SIEMENS

Издание 01/2021

Руководство по настройке

SIMATIC NET

Промышленные Ethernet коммутаторы

RUGGEDCOM ROS версия5.5

Для RST916C

https://www.siemens.com/ruggedcom

SIEMENS

SIMATIC NET

Промышленные Ethernet коммутаторы RUGGEDCOM ROS версия5.5

Руководство по настройке

Для RST916C

Предисловие

Введение 1

Использование операционной системы ROS 2

Начало работы 3

Управление устройством 4

Администрирование системы 5

Безопасность 6

Уровень 2 7

Уровень 3 8

Резервирование сети 9

Управление траффиком и его классификация 10

Службы времени 11

Исследование сетевого окружения и управление сетью 12

Назначение IP-адреса 13

Выявление и устранение проблем 14

01/2021
C79000-G8956-1486-02

Правовая справочная информация

Система предупреждений

Данная инструкция содержит указания, которые Вы должны соблюдать для Вашей личной безопасности и для предотвращения материального ущерба. Указания по Вашей личной безопасности выделены предупреждающим треугольником, общие указания по предотвращению материального ущерба не имеют этого треугольника. В зависимости от степени опасности, предупреждающие указания представляются в убывающей последовательности следующим образом:

⚠ ОПАСНОСТЬ

означает, что непринятие соответствующих мер предосторожности **приводит** к смерти или получению тяжелых телесных повреждений.

⚠ ПРЕДУПРЕЖДЕНИЕ

означает, что непринятие соответствующих мер предосторожности **может** привести к смерти или получению тяжелых телесных повреждений.

⚠ ВНИМАНИЕ

означает, что непринятие соответствующих мер предосторожности может привести к получению незначительных телесных повреждений.

⚠ ЗАМЕТКА

означает, что непринятие соответствующих мер предосторожности может привести к материальному ущербу.

При возникновении нескольких степеней опасности всегда используется предупреждающее указание, относящееся к наивысшей степени. Если в предупреждении с предупреждающим треугольником речь идет о предупреждении ущерба, причиняемому людям, то в этом же предупреждении дополнительно могут иметься указания о предупреждении материального ущерба.

Квалифицированный персонал

Работать с изделием или системой, описываемой в данной документации, должен только **квалифицированный персонал**, допущенный для выполнения поставленных задач и соблюдающий соответствующие указания документации, в частности, указания и предупреждения по технике безопасности. Квалифицированный персонал в силу своих знаний и опыта в состоянии распознать риски при обращении с данными изделиями или системами и избежать возникающих угроз.

Использование изделий Siemens по назначению

Соблюдайте следующее:

⚠ ПРЕДУПРЕЖДЕНИЕ

Изделия Siemens разрешается использовать только для целей, указанных в каталоге и в соответствующей технической документации. Если предполагается использовать изделия и компоненты других производителей, то обязательным является получение рекомендации и/или разрешения на это от фирмы Siemens. Исходными условиями для безупречной и надежной работы изделий являются надлежащая транспортировка, хранение, размещение, монтаж, оснащение, ввод в эксплуатацию, обслуживание и поддержание в исправном состоянии. Необходимо соблюдать допустимые условия окружающей среды. Обязательно учитывайте указания в соответствующей документации.

Товарные знаки

Все наименования, обозначенные символом защищенных авторских прав ®, являются зарегистрированными товарными знаками компании Siemens Canada Ltd.. Другие наименования в данной документации могут быть товарные знаки, использование которых третьими лицами для их целей могут нарушать права владельцев.

Исключение ответственности

Мы проверили содержимое документации на соответствие с описанным аппаратным и программным обеспечением. Тем не менее, отклонения не могут быть исключены, в связи с чем мы не гарантируем

Copyright © Siemens 2021
Все права защищены

полное соответствие. Данные в этой документации регулярно проверяются и соответствующие корректуры вносятся в последующие издания.

Digital Industries
Process Automation
300 Applewood Crescent
Concord, Ontario, L4K 4E5
Canada

C79000-G8956-1486-02
© 01/2021 Возможны изменения

Copyright © Siemens 2021
Все права защищены

Digital Industries
Process Automation
300 Applewood Crescent
Concord, Ontario, L4K 4E5
Canada

C79000-G8956-1486-02
© 01/2021 Возможны изменения

Copyright © Siemens 2021
Все права защищены

Содержание

Предисловие xv
Синтаксис команд CLI xv
Дополнительная документация xvi
Системные требования xviii
Доступ к документации xviii
Обучение xviii
Клиентская поддержка xviii

1 Введение 1

1.1 Особенности и преимущества 1
1.2 Рекомендации по обеспечению безопасности 5
1.3 Сообщения в системном журнале, относящиеся к системе безопасности 9
1.4 Сравнение контролируемых и неконтролируемых устройств 12
1.5 Поддерживаемые сетевые стандарты 13
1.6 Поддержка сетевого протокола интернета 14
1.6.1 Функции, поддерживаемые протоколами IPv4 и/или IPv6 14
1.6.2 Адрес IPv4 14
1.6.3 Адрес IPv6 15
1.7 Схема нумерации портов 15
1.8 Службы, доступные на портах TCP или UDP 16
1.9 Съемное запоминающее устройство 18

2 Использование операционной системы ROS 21

2.1 Вход в систему 22
2.2 Выход из системы 23
2.3 Использование веб-интерфейса 24
2.4 Использование консольного интерфейса 25
2.5 Использование интерфейса командной строки 27
2.5.1 Доступные CLI-команды 27
2.5.2 Трассировка событий 36
2.5.3 Удаленное исполнение команд через RSH 37
2.5.4 Использование команд SQL 38
2.5.4.1 Поиск нужной таблицы 38
2.5.4.2 Извлечение информации 39
2.5.4.3 Изменение значений в таблице 41
2.5.4.4 Сброс таблицы 41
2.5.4.5 Использование RSH и SQL 41
2.6 Определение выборки портов в RUGGEDCOM ROS 42
2.7 Администрирование файловой системы на флеш-диске 42

2.7.1 Просмотр списка файлов флеш-памяти 42
2.7.2 Просмотр сведений о файле флеш-памяти 43
2.7.3 Дефрагментирование файловой системы на флеш-диске 43

2.8 Доступ к режиму BIST 44

2.9 Управление доступом к интерфейсу загрузчика операционной системы 45
2.9.1 Включение/отключение доступа к интерфейсу загрузчика операционной системы 45
2.9.2 Доступ к интерфейсу загрузчика операционной системы 47
2.9.3 Настройка источника загрузки 47

2.10 Включение/отключение автоматического доступа к съемному запоминающему устройству 48

2.11 Включение/отключение консольной службы 48

3 Начало работы 51

3.1 Подключение к операционной системе ROS 51
3.1.1 IP-адрес по умолчанию 51
3.1.2 Подключение напрямую 51
3.1.3 Удаленное подключение 52

3.2 Установка USB-драйвера последовательной консоли RUGGEDCOM (только Windows) 53

3.3 Конфигурирование основной сети 54

4 Управление устройством 55

4.1 Просмотр информации об изделии 55

4.2 Просмотр диагностических сообщений процессора 56

4.3 Просмотр состояния источников питания 57

4.4 Восстановление заводских настроек по умолчанию 57

4.5 Выгрузка/загрузка файлов 59
4.5.1 Выгрузка/загрузка файлов с помощью протокола XMODEM 60
4.5.2 Выгрузка/загрузка файлов с помощью клиента TFTP 61
4.5.3 Выгрузка/загрузка файлов с помощью сервера TFTP 62
4.5.4 Выгрузка/загрузка файлов с помощью сервера SFTP 63
4.5.5 Выгрузка/загрузка файлов с помощью RUGGEDCOM CLP 63

4.6 Управление журналами 65
4.6.1 Просмотр локальных и системных журналов 65
4.6.2 Очистка локальных и системных журналов 65
4.6.3 Конфигурирование локального системного журнала 66
4.6.4 Управление удаленной регистрацией 66
4.6.4.1 Форма системного журнала 66
4.6.4.2 Конфигурирование удаленного Syslog-клиента 68
4.6.4.3 Просмотр списка удаленных Syslog-серверов 69
4.6.4.4 Добавление удаленного Syslog-сервера 69
4.6.4.5 Удаление удаленного Syslog-сервера 70

4.7 Управление Ethernet-портами 70

4.7.1 Защита контроллера с помощью Link Fault Indication (LFI — индикация отказа канала связи) 70
4.7.2 Просмотр состояния Ethernet-портов 72
4.7.3 Вывод диагностики для всех Ethernet-портов 72
4.7.4 Вывод диагностики для конкретных Ethernet-портов 73
4.7.5 Очистка статистики для конкретных Ethernet-портов 76
4.7.6 Конфигурирование Ethernet-порта 76
4.7.7 Конфигурирование ограничения скорости передачи через порт 79
4.7.8 Конфигурирование зеркалирования портов 80
4.7.9 Конфигурирование определения состояния канала связи 82
4.7.10 Управление трансиверами SFP 84
4.7.10.1 Требования к трансиверам SFP 84
4.7.10.2 Мониторинг порта SFP 85
4.7.10.3 Отображение информации для порта SFP 86
4.7.11 Обнаружение неисправностей кабеля 87
4.7.11.1 Просмотр результатов диагностики кабеля 87
4.7.11.2 Выполнение диагностики кабеля 89
4.7.11.3 Очистка диагностики кабеля 90
4.7.11.4 Определение расчетного расстояния до неисправности (DTF) 90
4.7.12 Сброс Ethernet-портов 90

4.8 Управление IP-интерфейсами 91
4.8.1 Просмотр списка IP-интерфейсов 92
4.8.2 Добавление IP-интерфейса 92
4.8.3 Удаление IP-интерфейса 94

4.9 Управление IP-шлюзами 94
4.9.1 Просмотр списка IP-шлюзов 94
4.9.2 Добавление IP-шлюза 95
4.9.3 Удаление IP-шлюза 95

4.10 Конфигурирование IP-сервисов 96

4.11 Управление дистанционным мониторингом 98
4.11.1 Управление средствами работы с данными, собираемыми при помощи RMON 98
4.11.1.1 Просмотр списка средств работы с данными, собираемыми при помощи RMON 98
4.11.1.2 Добавление средства работы с данными, собираемыми при помощи RMON ... 98
4.11.1.3 Удаление средства работы с данными, собираемыми при помощи RMON 99
4.11.2 Управление оповещениями RMON 99
4.11.2.1 Просмотр списка оповещений RMON 101
4.11.2.2 Добавление оповещения RMON 101
4.11.2.3 Удаление оповещения RMON 104
4.11.3 Управление событиями RMON 104
4.11.3.1 Просмотр списка событий RMON 104
4.11.3.2 Добавление события RMON 104
4.11.3.3 Удаление события RMON 105

4.12 Обновление микропрограммного обеспечения/возврат к более ранней версии микропрограммного обеспечения 105
4.12.1 Проверка хеш-сумм 106

4.12.2 Обновление микропрограммного обеспечения 106
4.12.3 Возврат к более ранней версии микропрограммного обеспечения 107
4.13 Перезапуск устройства 108
4.14 Вывод устройства из эксплуатации 109
5 Администрирование системы 111
5.1 Конфигурирование системной информации 111
5.2 Настройка экрана входа в систему 112
5.3 Включение/отключение веб-интерфейса 112
5.4 Управление оповещениями 112
5.4.1 Просмотр списка предварительно сконфигурированных оповещений 113
5.4.2 Просмотр и сброс фиксированных оповещений 114
5.4.3 Конфигурирование оповещения 114
5.4.4 Конфигурирование оповещений цифрового входа 115
5.4.5 Оповещения системы защиты для аутентификации при входе в систему 116
5.4.6 Список оповещений 119
5.5 Управление файлом конфигурации 123
5.5.1 Конфигурирование шифрования данных 123
5.5.2 Обновление файла конфигурации 125
5.6 Управление MMS 125
5.6.1 Основные сведения о протоколе MMS 125
5.6.1.1 Составление отчетов MMS 126
5.6.1.2 Отчеты/наборы данных 126
5.6.1.3 Поддерживаемые логические узлы 127
5.6.2 Просмотр списка предварительно сконфигурированных отчетов MMS 128
5.6.3 Конфигурирование отчета MMS 128
5.6.4 Пример: Конфигурирование отчетов MMS 129
6 Безопасность 131
6.1 Конфигурирование паролей 131
6.2 Очистка конфиденциальных данных 133
6.3 Управление аутентификацией пользователей 134
6.3.1 Методы аутентификации 134
6.3.2 Конфигурирование расширений имен пользователей 136
6.3.3 Управление аутентификацией RADIUS 137
6.3.3.1 Конфигурирование сервера RADIUS 138
6.3.3.2 Конфигурирование клиента RADIUS на устройстве 138
6.3.4 Управление аутентификацией TACACS+ 139
6.3.4.1 Конфигурирование TACACS+ 140
6.3.4.2 Конфигурирование привилегий пользователей 141
6.4 Управление безопасностью на уровне порта 142
6.4.1 Концепция безопасности на уровне порта 142
6.4.1.1 Аутентификация на базе статического MAC-адреса 142
6.4.1.2 Аутентификация на базе статического MAC-адреса в кольце MRP 143
6.4.1.3 Аутентификация IEEE 802.1x 143

6.4.1.4 Аутентификация IEEE 802.1X с аутентификацией на базе статического MAC-адреса 144
6.4.1.5 Ограниченные сети VLAN 145
6.4.1.6 Определение сетей VLAN с использованием туннельных атрибутов 146
6.4.2 Просмотр списка авторизованных MAC-адресов 147
6.4.3 Конфигурирование безопасности на уровне порта 147
6.4.4 Конфигурирование IEEE 802.1X 149

6.5 Управление ключами и сертификатами SSH/SSL 151
6.5.1 SSL-сертификаты 152
6.5.2 Хост-ключ SSH 153
6.5.3 Управление открытыми ключами SSH 153
6.5.3.1 Требования к открытым ключам 154
6.5.3.2 Добавление открытого ключа 155
6.5.3.3 Просмотр списка открытых ключей 156
6.5.3.4 Обновление открытого ключа 156
6.5.3.5 Удаление открытого ключа 157
6.5.4 Примеры сертификатов и ключей 157

7 Уровень 2 159

7.1 Управление виртуальными сетями LAN 159
7.1.1 Концепция сетей VLAN 159
7.1.1.1 Сравнение тегированных и нетегированных кадров 160
7.1.1.2 Native VLAN (VLAN, в которой кадры не тегируются) 160
7.1.1.3 Административная сеть VLAN 160
7.1.1.4 Вспомогательные административные сети VLAN 160
7.1.1.5 Типы граничных и транковых портов 161
7.1.1.6 Правила для входящего и исходящего трафика сети 162
7.1.1.7 Список запрещенных портов 163
7.1.1.8 Режимы VLAN-aware (VLAN-осведомленный) и VLAN-unaware (VLAN-неосведомленный) 163
7.1.1.9 Протокол регистрации GARP VLAN (GVRP) 164
7.1.1.10 Граничная сеть Private VLAN (PVLAN) 166
7.1.1.11 QinQ 166
7.1.1.12 Преимущества сети VLAN 168
7.1.2 Просмотр списка сетей VLAN 170
7.1.3 Глобальное конфигурирование сетей VLAN 170
7.1.4 Конфигурирование сетей VLAN для конкретных Ethernet-портов 171
7.1.5 Управление статическими сетями VLAN 173
7.1.5.1 Просмотр списка статических сетей VLAN 174
7.1.5.2 Добавление статической сети VLAN 174
7.1.5.3 Удаление статической сети VLAN 175
7.1.6 Пример: Конфигурирование поддержки управления на нескольких сетях VLAN 175

7.2 Управление MAC-адресами 178
7.2.1 Просмотр списка MAC-адресов 178
7.2.2 Конфигурирование опций определения MAC-адреса 178
7.2.3 Конфигурирование опций лавинной рассылки MAC-адресов 179
7.2.4 Управление статическими MAC-адресами 180

7.2.4.1 Просмотр списка статических MAC-адресов 180
7.2.4.2 Добавление статического MAC-адреса 180
7.2.4.3 Удаление статического MAC-адреса 181
7.2.5 Очистка всех динамических MAC-адресов 182

7.3 Управление многоадресной фильтрацией 182
7.3.1 Управление IGMP 182
7.3.1.1 Концепция IGMP 182
7.3.1.2 Просмотр списка составов многоадресных групп 188
7.3.1.3 Просмотр информации о пересылке для многоадресных групп 188
7.3.1.4 Конфигурирование IGMP 189
7.3.2 Управление GMRP 191
7.3.2.1 Концепция GMRP 191
7.3.2.2 Просмотр сводных сведений о многоадресных группах 194
7.3.2.3 Глобальное конфигурирование GMRP 195
7.3.2.4 Конфигурирование GMRP для конкретных Ethernet-портов 195
7.3.2.5 Просмотр списка статических многоадресных групп 196
7.3.2.6 Добавление статической многоадресной группы 196
7.3.2.7 Удаление статической многоадресной группы 197

8 Уровень 3 199

8.1 Управление коммутацией 3-го уровня 199
8.1.1 Основные сведения о коммутации 3-го уровня 199
8.1.1.1 Таблица переадресации коммутатора 3-го уровня 199
8.1.1.2 Правила статической коммутации 3-го уровня 200
8.1.1.3 Динамическое запоминание коммутации 3-го уровня 201
8.1.1.4 Взаимодействие между пересылкой IP и коммутацией 3-го уровня 201
8.1.1.5 Таблица ARP коммутатора 3-го уровня 202
8.1.1.6 Маршрутизируемые интерфейсы коммутатора 3-го уровня 204
8.1.2 Конфигурирование коммутации 3-го уровня 204
8.1.3 Конфигурирование опций коммутации 3-го уровня 205
8.1.4 Управление правилами одноадресной статической передачи 206
8.1.4.1 Просмотр правил одноадресной статической передачи 206
8.1.4.2 Добавление правила одноадресной статической передачи 206
8.1.4.3 Удаление правила одноадресной статической передачи 207
8.1.5 Управление статическими записями в таблице ARP 207
8.1.5.1 Просмотр списка записей в таблице ARP 207
8.1.5.2 Добавление статической записи в таблицу ARP 208
8.1.5.3 Удаление статической записи в таблице ARP 209
8.1.6 Просмотр правил маршрутизации 209
8.1.7 Очистка правил динамической маршрутизации аппаратного обеспечения .. 210
8.1.8 Пример: Конфигурирование коммутации 3-го уровня 210
8.1.9 Пример: Конфигурирование коммутации 3-го уровня с использованием нескольких коммутаторов 212

9 Резервирование сети 217

9.1 Управление протоколом связующего дерева 217
9.1.1 Функционирование протокола RSTP 217
9.1.1.1 Состояния и роли в RSTP 218
9.1.1.2 Граничные порты 220

9.1.1.3 Сетевые сегменты точка-точка и сегменты с множественным доступом 220
9.1.1.4 Стоимость пути и сумма стоимости портов на этом пути 221
9.1.1.5 Диаметр моста 222
9.1.1.6 eRSTP 223
9.1.1.7 Быстрый перехват роли корневого коммутатора в случае отказа 223
9.1.2 Применения RSTP 225
9.1.2.1 Структурированные кабельные сети с RSTP 225
9.1.2.2 Кольцевые магистральные сети с RSTP 227
9.1.2.3 Дублирование RSTP-портов 229
9.1.3 Функционирование протокола MSTP 230
9.1.3.1 MSTP-регионы и совместимость с другими протоколами 231
9.1.3.2 Роли мостов и портов в MSTP 232
9.1.3.3 Преимущества протокола MSTP 234
9.1.3.4 Реализация протокола MSTP в коммутируемой сети 235
9.1.4 Глобальное конфигурирование STP 236
9.1.5 Конфигурирование STP для конкретных Ethernet-портов 238
9.1.6 Конфигурирование eRSTP 241
9.1.7 Вывод глобальной диагностики для STP 244
9.1.8 Вывод диагностики STP для Ethernet-портов 245
9.1.9 Управление экземплярами множественного связующего дерева 247
9.1.9.1 Вывод диагностики для глобальных MSTI 247
9.1.9.2 Вывод диагностики для MSTI портов 248
9.1.9.3 Конфигурирование идентификатора MST-региона 250
9.1.9.4 Конфигурирование глобального MSTI 251
9.1.9.5 Конфигурирование MSTI для Ethernet-порта 252
9.1.10 Очистка статистики протокола связующего дерева 253

9.2 Управление протоколом резервирования среды передачи (MRP) 253
9.2.1 Основные сведения о протоколе MRP 253
9.2.1.1 Сравнение устройств MRM и MRC 254
9.2.1.2 Устройства MRA 254
9.2.1.3 Состояния портов кольцевой сети 254
9.2.1.4 Сравнение замкнутого кольца и разомкнутого кольца 255
9.2.2 Глобальное конфигурирование MRP 256
9.2.3 Просмотр состояния экземпляров MRP 256
9.2.4 Добавление экземпляра MRP 258
9.2.5 Удаление экземпляра MRP 260
9.2.6 Пример: Конфигурирование кольцевой сети MRP 261

9.3 Управление агрегированием каналов связи 263
9.3.1 Концепция агрегирования каналов связи 263
9.3.1.1 Сравнение статического и динамического агрегирования каналов связи 264
9.3.1.2 Правила и ограничения 265
9.3.1.3 Агрегирование каналов связи и особенности 2-го уровня 266
9.3.1.4 Агрегирование каналов связи и особенности физического уровня 266
9.3.2 Конфигурирование агрегирования каналов связи 267
9.3.3 Управление группами агрегирования каналов связи 267
9.3.3.1 Просмотр списка групп агрегирования каналов связи 268
9.3.3.2 Добавление группы агрегирования каналов связи 268
9.3.3.3 Удаление группы агрегирования каналов связи 269

9.3.3.4 Просмотр состояния групп агрегирования каналов связи 269
9.3.4 Управление протоколом управления агрегированием каналов связи 270
9.3.4.1 Просмотр информации о партнере LACP 271
9.3.4.2 Конфигурирование глобальных настроек LACP 272
9.3.4.3 Конфигурирование LACP на каждом порте 272
9.3.4.4 Вывод диагностики LACP 274
9.3.5 Очистка статистики агрегирования каналов связи 274

10 Управление траффиком и его классификация 275

10.1 Управление классами сервиса 275
10.1.1 Глобальное конфигурирование классов сервиса 277
10.1.2 Конфигурирование классов сервиса для конкретных Ethernet-портов 277
10.1.3 Конфигурирование определения класса сервиса по битам приоритета 278
10.1.4 Конфигурирование определения класса сервиса по битам приоритета DSCP 279

11 Службы времени 281

11.1 Конфигурирование даты и времени 281

11.2 Управление протоколом точного времени (PTP) 283
11.2.1 Глобальное конфигурирование протокола PTP 284
11.2.2 Конфигурирование прозрачных часов 286
11.2.3 Конфигурирование интервала запросов задержки протокола PTP 287
11.2.4 Вывод диагностики часов PTP 287
11.2.5 Вывод диагностики задержки между узлами 288

11.3 Конфигурирование источника времени 289

11.4 Управление NTP 289
11.4.1 Включение/отключение службы NTP 289
11.4.2 Конфигурирование серверов NTP 290

11.5 Просмотр состояния подсистемы синхронизации времени 290

12 Исследование сетевого окружения и управление сетью 291

12.1 Включение/отключение RCDP 291

12.2 Управление LLDP 293
12.2.1 Глобальное конфигурирование LLDP 294
12.2.2 Конфигурирование LLDP для Ethernet-порта 295
12.2.3 Вывод глобальной диагностики и рассылаемой системной информации 295
12.2.4 Вывод диагностики для соседних устройств LLDP 296
12.2.5 Вывод диагностики для портов LLDP 296

12.3 Управление SNMP 297
12.3.1 Поддержка базы интерфейса управления (MIB) SNMP 298
12.3.1.1 Поддерживаемые стандартные MIB 298
12.3.1.2 Поддерживаемые проприетарные базы RUGGEDCOM MIB 393
12.3.1.3 Поддерживаемые возможности агента 431
12.3.2 Trap-уведомления SNMP 432
12.3.3 Управление пользователями SNMP 438
12.3.3.1 Просмотр списка пользователей SNMP 438
12.3.3.2 Добавление пользователя SNMP 438

12.3.3.3 Удаление пользователя SNMP 441
12.3.4 Управление соответствиями групп пользователей моделям и уровням безопасности 441
12.3.4.1 Просмотр соответствий групп пользователей моделям и уровням безопасности 441
12.3.4.2 Добавление соответствия группы пользователей модели и уровню безопасности 441
12.3.4.3 Удаление соответствия группы пользователей модели и уровню безопасности 442
12.3.5 Управление группами SNMP 442
12.3.5.1 Просмотр списка групп SNMP 442
12.3.5.2 Добавление группы SNMP 443
12.3.5.3 Удаление группы SNMP 444

12.4 Поддержка управления ModBus 444
12.4.1 Функциональные коды ModBus 444
12.4.2 Распределение адресного пространства ModBus 445
12.4.3 Форматы памяти ModBus 450
12.4.3.1 Текстовый 450
12.4.3.2 Cmd 451
12.4.3.3 Uint16 451
12.4.3.4 Uint32 451
12.4.3.5 PortCmd 452
12.4.3.6 Оповещение 453
12.4.3.7 PSStatusCmd 453
12.4.3.8 TruthValues 454

13 Назначение IP-адреса 455

13.1 Управление DHCP 455
13.1.1 Концепция DHCP 455
13.1.1.1 Отслеживание DHCP 455
13.1.1.2 Надежные и ненадежные порты 456
13.1.1.3 Агент ретрансляции DHCP (Опция 82) 456
13.1.1.4 Динамический контроль ARP 457
13.1.1.5 Таблица привязки DHCP 457
13.1.1.6 Предотвращаемые сетевые атаки 458
13.1.2 Конфигурирование агента ретрансляции DHCP 461
13.1.3 Включение информации агента ретрансляции DHCP (Опция 82) для конкретных портов 461
13.1.4 Конфигурирование отслеживания DHCP 462
13.1.5 Конфигурирование доверенных/недоверенных портов 463
13.1.6 Управление динамическим контролем ARP 463
13.1.6.1 Включение/отключение динамического контроля ARP 464
13.1.6.2 Вывод диагностики контроля ARP 464
13.1.6.3 Очистка статистики контроля ARP 464
13.1.7 Управление таблицей привязки DHCP 465
13.1.7.1 Добавление записей в таблицу привязки DHCP 465
13.1.7.2 Просмотр таблицы привязки DHCP 465
13.1.7.3 Сохранение таблицы привязки DHCP 466
13.1.7.4 Пример: Конфигурирование устройства в качестве агента ретрансляции 466

14 Выявление и устранение проблем 471
14.1 Общее 471
14.2 Ethernet-порты 472
14.3 Связующее дерево 473
14.4 Сети VLAN 475

Предисловие

В настоящем руководстве приведено описание операционной системы ROS v5.5 (Rugged Operating System), работающей на устройствах RUGGEDCOM RST916C. Здесь содержатся инструкции и рекомендации по использованию программного обеспечения, а также немного общей теории.

Руководство предназначено для использования персоналом служб технической поддержки сетей, хорошо знакомым с функционированием сетей. Оно также рекомендовано для проектировщиков сетей и систем, системных программистов и линейных технических специалистов.

Примечание
Некоторые описанные параметры и опции могут быть не доступны, в зависимости от варианта аппаратной части устройства. Мы приложили все усилия для приведения точного описания конкретных параметров и опций, но данное руководство следует использовать совместно с текстом справочного документа, входящего в программное обеспечение.

Синтаксис команд CLI

В настоящем документе подробно рассмотрены команды CLI. Команда CLI состоит из ключевой команды, параметров, опций и/или пользовательских переменных.

Элементы команды CLI
В следующей команде CLI `interface` — ключевая команда, { *`name`* } — определяемое пользователем значение, `vlan` и `type` — параметры, а `access` и `trunk` — фиксированные опции.

`interface` { *`name`* } `vlan type [ access | trunk ]`

Форматирование команды
В настоящем документе команды CLI отображаются в соответствии со следующими правилами синтаксиса:

Условные обозначения	Описание	Пример
Шрифт	Все команды, параметры и опции отображаются моноширинным шрифтом.	**`command`** `parameter`
Определяемые пользователем значения	Некоторые параметры требуют определяемого пользователем значения. Значения, которые должны быть определены пользователем, заключены в скобки (фигурные скобки).	**`command`** `parameter { value }`

Условные обозначения	Описание	Пример
	Значение может быть строкой, такой как имя или описание. Значение может быть компонентом системы, таким как идентификатор или интерфейс. Во всех случаях ключевое слово между скобок обозначает тип вводимого значения.	
Диапазоны чисел	Когда значением параметра является число в определенном диапазоне, этот диапазон заключен в скобки (фигурные скобки).	**command** parameter { *0 - 10* }
Опции	Когда для параметра параметра доступен выбор из нескольких значений, все варианты заключены в квадратные скобки. Вариантами для выбора часто являются фиксированные значения, но также могут быть значения, определяемые пользователями, и/или диапазоны чисел.	**command** parameter [option1 | option2 | { *value* } | { *0 - 10* }]

Дополнительная документация

Ниже приведены прочие документы, относящиеся к данному продукту. Если не указано иное, все документы доступны на сайте поддержки Siemens Industry Online Support (SIOS) [https://support.industry.siemens.com].

В списке указаны документы, доступные на момент публикации. Могут быть доступны более новые версии этих документов или связанных продуктов. Для получения дополнительных сведений посетите сайт поддержки SIOS или обратитесь в представительство службы поддержки клиентов Siemens.

Примечания по продукту

Примечания по продукту доступны на сайте SIOS [https://support.industry.siemens.com/cs/ca/en/ps/16008/pm].

Руководства по конфигурированию

Название документа	Ссылка
Руководство пользователя RUGGEDCOM NMS v2.1 для Windows	https://support.industry.siemens.com/cs/ww/en/view/109737564
Руководство пользователя RUGGEDCOM NMS v2.1 для Linux	https://support.industry.siemens.com/cs/ww/en/view/109737563
Руководство по конфигурированию RUGGEDCOMDIRECTOR v1.5	https://support.industry.siemens.com/cs/ww/en/view/97691648

Название документа	Ссылка
Руководство пользователя RUGGEDCOM EXPLORER V1.5	https://support.industry.siemens.com/cs/ww/en/view/109480804
Руководство пользователя RUGGEDCOM PING v1.2	https://support.industry.siemens.com/cs/ww/en/view/97674073

Каталоги

Название документа	Ссылка
Каталог SFP-трансиверов RUGGEDCOM	https://support.industry.siemens.com/cs/ww/en/view/109482309

Вопросы и ответы

Название документа	Ссылка
Как сконфигурировать функцию SMP в коммутаторе RUGGEDCOM с RUGGEDCOM ROS?	https://support.industry.siemens.com/cs/ww/en/view/109474615
Как защитить устройства под управлением RUGGEDCOM ROS до и после развертывания на площадке?	https://support.industry.siemens.com/cs/ww/en/view/99858806
Как реализовать устойчивую кольцевую сеть с использованием RSTP и eRSTP?	https://support.industry.siemens.com/cs/ww/en/view/109738240
Как реализовать защищенный автоматический вход в систему ROS?	https://support.industry.siemens.com/cs/ww/en/view/109756843
Как управлять двунаправленным трафиком при использовании зеркалирования портов?	https://support.industry.siemens.com/cs/ww/en/view/109759351
Хэш-суммы RUGGEDCOM ROS	https://support.industry.siemens.com/cs/ww/en/view/109779935

Официальные описания

Название документа	Ссылка
Работа протокола быстрого связующего дерева в топологии кольцевой сети	https://assets.new.siemens.com/siemens/assets/api/uuid:d4af5d17-728c-493f-b00a-9c4db67b23ed/RSTP-whitepaper-EN-09-2020.pdf

Справочные руководства

Название документа	Ссылка
Справочное руководство по поддержке синхронизации времени	https://support.industry.siemens.com/cs/us/en/view/109780448

Руководства по установке

Название документа	Ссылка
Руководство по установке RUGGEDCOM RST916C	https://support.industry.siemens.com/cs/ww/en/view/109782150

Системные требования

Каждая рабочая станция, используемая для подключения к интерфейсу RUGGEDCOM ROS, должна удовлетворять следующим системным требованиям:

- Должен присутствовать Ethernet-интерфейс, совместимый хотя бы с одним типом портов на устройстве RUGGEDCOM
- Должна существовать возможность конфигурировать IP-адрес и маску сети на Ethernet-интерфейсе компьютера

Доступ к документации

Актуальная пользовательская документация для RUGGEDCOM ROS v5.5 доступна на сайте https://support.industry.siemens.com. По вопросам, касающимся пользовательской документации, обращайтесь в службу клиентской поддержки Siemens.

Обучение

Siemens предлагает широкий спектр образовательных услуг от стандартных курсов по сетевым технологиям, коммутаторам Ethernet и роутерам, проводимых на собственной базе, до специализированных выездных курсов, разработанных в соответствии с потребностями, опытом и сферой деятельности клиента.

Siemens имеет команду тренеров, которые стремятся поделиться с нашими клиентами важными практическими навыками, знаниями и опытом, необходимыми пользователям для понимания различных технологий, связанных с ключевыми технологиями инфраструктуры коммуникационных сетей.

Siemens обладает уникальным опытом в области ИТ/телекоммуникаций в сочетании с предметными знаниями на рынке коммунальных, транспортных и производственных услуг, что позволяет компании Siemens проводить обучение, ориентированное на конкретное применения клиента.

Для получения дополнительной информации об обучении и доступности курсов посетите сайт https://www.siemens.com или обратитесь к представителю компании Siemens.

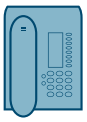
Клиентская поддержка

Клиентская поддержка доступна 24 часа в сутки 7 дней в неделю для всех клиентов Siemens. За технической поддержкой или для получения общей

информации обращайтесь в службу клиентской поддержки Siemens любым из следующим способов:

Онлайн

Чтобы отправить запрос в службу клиентской поддержки или проверить статус отправленного запроса, перейдите по ссылке http://www.siemens.com/automation/support-request.



Телефон

Чтобы отправить запрос в службу клиентской поддержки, позвоните по телефону местной горячей линии. Телефон местной горячей линии см. на сайте https://w3.siemens.com/aspa_app/?lang=ru.

Через мобильное приложение

Установите приложение Industry Online Support компании Siemens AG на любое мобильное устройство на базе Android, Apple iOS или Windows, чтобы:

- Получить доступ к обширной библиотеке документов Siemens, включая разделы с часто задаваемыми вопросами и инструкциями
- Отправить запрос в службу клиентской поддержки или проверить статус отправленного запроса
- Обратиться к региональному представителю отдела продаж, технической поддержки, обучения компании Siemens и т. д.
- Задать вопросы и поделиться знаниями с другими клиентами Siemens и сообществом поддержки клиентов

1 Введение

Это Руководство по настройке программного обеспечения RUGGEDCOM ROS v5.5 для устройств RUGGEDCOM RST916C. В этом руководстве описывается широкий спектр функций операторского класса, доступных операционной системе RUGGEDCOM ROS (Rugged Operating System).

В данном разделе представлен базовый обзор программного обеспечения RUGGEDCOM ROS.

1.1 Особенности и преимущества

Ниже приведено описание функций, доступных в RUGGEDCOM ROS, и их преимущества.

- **Функции кибербезопасности**

  Кибербезопасность является крайне важным аспектом для многих отраслей промышленности, в критических областях которых широко применяется автоматизация и сети связи. Ключевые особенности RUGGEDCOM ROS, направленные на решение проблем безопасности на уровне локальной вычислительной сети, включают следующие аспекты:

Пароли	Многоуровневые пароли пользователей предотвращают неавторизованное конфигурирование
SSH/SSL	Расширение возможностей защиты паролем для добавления шифрования паролей и данных по мере пересечения ими сети
Включение/отключение портов	Возможность отключения портов для предотвращения прохождения трафика
802.1Q VLAN	Обеспечивает возможность логического разделения трафика между предопределенными портами на коммутаторах
SNMPv3	Шифрованная аутентификация и защита доступа
HTTPS	Безопасный доступ к веб-интерфейсу

- **Усовершенствованный протокол связующего дерева (eRSTP)™**

  Протокол eRSTP компании Siemens позволяет создавать отказоустойчивые кольцевые и многосвязные сети Ethernet, включающие резервированные каналы связи, которые *отсекаются* для предотвращения образования петель. Протокол eRSTP реализует как STP, так и RSTP для обеспечения совместимости с коммерческими коммутаторами, в отличие от других проприетарных *кольцевых* решений. Функция быстрого перехвата роли корневого коммутатора в случае отказа корневого коммутатора RSTP в многосвязной топологии обеспечивает быструю конвергенцию сетей.

- **Класс сервиса (IEEE 802.1p)**

  Некоторые сетевые приложения, такие как протокол управления в реальном времени или протокол VoIP (Voice over IP), требуют прогнозируемого времени доставки Ethernet-кадров. Коммутаторы могут приводить к задержкам из-за внутренних запросов, которые буферизируют кадры, а затем передают их по принципу "первым пришёл — первым обслужен". RUGGEDCOM ROS поддерживает *класс сервиса (Class of Service)*, который позволяет трафику, для которого время является критическим, попадать в начало очереди, минимизируя задержку и снижая *эффект дрожания*, обеспечивая надлежащую работу требовательных приложений. RUGGEDCOM ROS обеспечивает классификацию приоритета по порту, тегам, MAC-адресу и типу сервиса (Type of Service, ToS) IP. Конфигурируемый алгоритм *взвешенной "справедливой" организации очередей* регулирует способ выхода кадров из очереди.

- **VLAN (IEEE 802.1Q)**

  Virtual Local Area Networks (VLAN — виртуальные локальные вычислительные сети) обеспечивают разделение физической сети на несколько отдельных логических сетей с независимыми широковещательными доменами. Уровень безопасности обеспечивается тем, что хосты могут получать доступ только к другим хостам в той же сети VLAN, а также изолированием лавин трафика. RUGGEDCOM ROS поддерживает Ethernet-кадры, тегированные 802.1Q, и транковые группы VLAN. Классификация на основе порта обеспечивает назначение устаревших устройств соответствующим сетям VLAN. Кроме того, предусмотрена поддержка GVRP для упрощения конфигурации коммутаторов в сети VLAN.

- **Дистанционный мониторинг и настройка с помощью системы управления сетью SINEC NMS**

  SINEC NMS — это программная система управления сетью компании Siemens для обнаружения, мониторинга и управления продуктами RUGGEDCOM, а также другими устройствами с поддержкой IP в сети. Данный полнофункциональный продукт характеризуется высокой степенью конфигурирования и обеспечивает отчеты о доступности и характеристиках сетевых компонентов и служб. Отказы устройств, сети и служб быстро выявляются, а информация о них оперативно передается пользователю, позволяя сократить время простоя.

  Система SINEC NMS особенно подходит для дистанционного мониторинга и конфигурирования маршрутизаторов Siemens, коммутаторов, последовательных серверов и беспроводного сетевого оборудования WiMAX. Для получения дополнительной информации см. https://www.siemens.com/sinec.

- **Простой протокол сетевого управления (SNMP)**

  Протокол SNMP обеспечивает станции управления сетью стандартизированным методом опроса устройств от различных поставщиков. Поддерживаемые версии протокола SNMP: v1, v2c и v3. Протокол SNMPv3, в частности, обеспечивает функции защиты (такие как

аутентификация, конфиденциальность и контроль доступа), отсутствующие в более ранних версиях SNMP. Поддержка многочисленных стандартов Management Information Base (MIB — база управляющей информации), делает возможной простую интеграцию с любой Network Management System (NMS — система управления сетью). Еще одной особенностью SNMP, поддерживаемой RUGGEDCOM ROS, является возможность генерировать *trap-уведомления* во время системных событий. Система управления сетью SINEC NMS от компании Siemens может записывать trap-уведомления от различных устройств, предоставляя мощный инструмент для решения сетевых проблем. Кроме того, она позволяет выполнять графическую визуализацию сети и полностью интегрируется со всеми продуктами Siemens.

- **Network Time Protocol (NTP — сетевой протокол времени)**

  Протокол NTP автоматически синхронизирует внутренние часы всех устройств под управлением RUGGEDCOM ROS в сети. Это позволяет соотнести события, имеющие метки даты и времени, для поиска и устранения неисправностей.

- **Ограничение скорости передачи через порт**

  RUGGEDCOM ROS поддерживает конфигурируемое ограничение скорости передачи данных на каждый порт для ограничения одноадресного и многоадресного трафика. Это может быть крайне важно в части управления пропускной способностью сети для поставщиков услуг. Кроме того, это обеспечивает граничную защиту от атак типа "отказ в обслуживании" (DoS-атак).

- **Фильтрация широковещательного шторма ("лавин")**

  Широковещательные штормы "лавины" приносят хаос в сеть и могут привести к выходу присоединенных устройств из строя. Это может оказывать катастрофическое влияние на критически важное оборудование. RUGGEDCOM ROS позволяет ограничить это явление путем фильтрации широковещательных кадров, используя установленное пользователем пороговое значение.

- **Агрегирование каналов связи**

  Ethernet-порты могут агрегироваться в единый логический канал связи либо статически, либо динамически, для увеличения пропускной способности сети и уравновешивания сетевой нагрузки.

- **Зеркалирование портов**

  RUGGEDCOM ROS можно сконфигурировать на дублирование всего трафика на одном порту на назначенный зеркальный порт. В сочетании с сетевым анализатором это формирует мощное средство поиска и устранения неисправностей.

- **Конфигурирование порта и его статус**

  RUGGEDCOM ROS позволяет *на аппаратном уровне* сконфигурировать для отдельных портов скорость, дуплексный режим, автосогласование, управление потоком данных и многое другое. Это обеспечивает

надлежащее соединение с устройствами, которые не осуществляют согласование или имеют необычные настройки. Детальный статус портов с аварийным оповещением и trap-уведомлением SNMP о проблемах канала связи значительно упрощают поиск и устранение неисправностей.

- **Статистика портов и Remote Monitoring (RMON — дистанционный мониторинг)**

  RUGGEDCOM ROS обеспечивает постоянное обновление статистики по портам, которая включает счетчики байтов входящих и исходящих пакетов, а также детализацию по ошибкам.

  Кроме того предусмотрена полная поддержка статистики RMON. RMON обеспечивает комплексный сбор данных, анализ и обнаружение моделей трафика.

- **Фильтрация многоадресных рассылок**

  RUGGEDCOM ROS поддерживает многоадресные группы и возможность динамически присоединяться к многоадресным группам и покидать их с помощью Internet Group Management Protocol (IGMP — протокол группового управления сети интернет) или GARP Multicast Registration Protocol (GMRP — протокол многоадресной регистрации).

- **Регистрация событий и оповещения**

  RUGGEDCOM ROS регистрирует все важные события в энергонезависимом системном журнале, обеспечивая возможность аналитического поиска и устранения неисправностей. К событиям, помимо прочего, относятся отказ и восстановление канала связи, неавторизованный доступ, обнаружение широковещательного шторма ("лавины"), а также самодиагностика. Оповещения обеспечивают отображение моментального состояния недавних событий, которые еще ожидают подтверждения сетевым администратором. Питание внешнего аппаратного реле отключается в присутствии критических оповещений, обеспечивая возможность вмешательства внешнего контроллера.

- **Пользовательский HTML-интерфейс веб-браузера**

  RUGGEDCOM ROS обеспечивает простой, интуитивно-понятный пользовательский интерфейс для конфигурирования и мониторинга с помощью стандартного графического веб-браузера или стандартного телекоммуникационного интерфейса. Все параметры системы включают подробную интерактивную справку для упрощения настройки и конфигурирования. RUGGEDCOM ROS обеспечивает типовой интерфейс и стандартизированный процесс конфигурации, что упрощает миграцию на другие продуктыRUGGEDCOM.

- **Предотвращение атак "грубой силы"**

  Защита от Brute Force Attacks (BFA — атака "грубой силы") является стандартом для RUGGEDCOM ROS. В случае фиксированного количества неудачных попыток входа внешнего хоста в систему через интерфейс терминала или веб-интерфейс служба блокируется на один час.

- **Поддержка IPv4/IPv6**

  RUGGEDCOM ROS поддерживает как адреса IPv4, так и адреса IPv6 (для отдельных функций). Дополнительную информацию о поддержке по каждому протоколу см. в разделе "Поддержка сетевого протокола интернета (Страница 14)".

- **Коммутация 3-го уровня**

  Устройство может функционировать в качестве коммутатора 3-го уровня. Дополнительную информацию о конфигурировании правил коммутации 3-го уровня в для RUGGEDCOM ROS см. в разделе "*Уровень 3* (Страница 199)".

1.2 Рекомендации по обеспечению безопасности

Чтобы предотвратить несанкционированный доступ к устройству, воспользуйтесь следующими рекомендациями по обеспечению безопасности.

Аутентификация

- Смените пароли по умолчанию для всех учетных записей пользователей и процессов (если применимо) до развертывания устройства.
- Используйте надежные пароли с высокой степенью рандомизации (энтропии) и без повторяющихся символов. Не используйте ненадежные пароли, такие как *password1*, *123456789*, *abcdefgh*, а также словарные слова или имена собственные в любой комбинации. Для получения дополнительной информации о создании надежных паролей см. требования к паролям в "Конфигурирование паролей (Страница 131)".
- Необходимо убедиться, что пароли защищены и не известны неавторизованному персоналу.
- Пароли не должны использоваться повторно для разных имен пользователя или систем, а также после истечения их срока действия.
- Если аутентификация RADIUS выполняется дистанционно, необходимо убедиться, что весь обмен данными происходит в пределах защищенного периметра или на защищенном канале.
- Сгенерируйте и обеспечьте пользовательский SSL-сертификат и хостовый ключ SSH перед вводом устройства в эксплуатацию. Для получения дополнительной информации см. "Управление ключами и сертификатами SSH/SSL (Страница 151)".
- Используйте аутентификацию с помощью общественного ключа SSH. Для получения дополнительной информации см. "Управление открытыми ключами SSH (Страница 153)".
- Протокол аутентификации по паролю (PAP) не считается безопасным протоколом и, по возможности, должен использоваться в защищенной сетевой среде.

- Обратите внимание на любые протоколы канального уровня, которые не обеспечивают внутреннюю аутентификацию между конечными точками, такими как ARP в IPv4, обнаружение соседних устройств/DAD в IPv6 и Wi-Fi в беспроводных сетях. Злоумышленники могут использовать слабые места в этих протоколах для атаки на хосты, коммутаторы и маршрутизаторы, подключенные к сети 2-го уровня, путем порчи ARP-кэша систем в подсети, и путем последовательного перехвата трафика. Необходимо предусмотреть подходящие средства защиты от небезопасных протоколов 2-го уровня, такие как защита физического доступа к локальной сети и использование защищенных протоколов более высокого уровня, чтобы предотвратить неавторизованный доступ к сети.

Физический/удаленный доступ

- Не подключайте устройство к сети Интернет. Развертывание устройства должно осуществляться только в пределах защищенного сетевого периметра.
- Физический доступ к устройству должен иметь только авторизованный персонал. Злоумышленники могут извлечь критически важную информацию, такую как сертификаты, ключи и т. д. (пароли пользователей защищены хэш-кодами) или перепрограммировать устройство.
- Если он не требуется, автоматический доступ к съемным запоминающим устройствам должен быть отключен, чтобы предотвратить неавторизованный доступ. Для получения дополнительной информации об отключении доступа к съемному запоминающему устройству см. "Включение/отключение автоматического доступа к съемному запоминающему устройству (Страница 48)".
- Ограничьте доступ к последовательной консоли также как и любой физический доступ к устройству. Доступ к последовательной консоли потенциально позволяет получить неавторизованный доступ к загрузчику операционной системы RUGGEDCOM ROS, включающему в себя инструментальные средства, которые могут быть использованы для получения полного доступа к устройству. Для получения дополнительной информации об ограничении доступа к интерфейсу загрузчика операционной системы см. "Управление доступом к интерфейсу загрузчика операционной системы (Страница 45)".
- Включайте только службы, которые будут использоваться на устройстве, включая физические порты. Неиспользуемые физические порты потенциально могут служить для получения доступа к сети за устройством.
- Зеркальные порты допускают двунаправленный трафик (т. е. устройство не будет блокировать трафик, входящий через зеркальные порты). Для повышения безопасности сконфигурируйте входную фильтрацию для управления потоком трафика, когда зеркалирование портов включено. Для получения дополнительной информации о включении зеркалирования портов см. "Конфигурирование зеркалирования портов (Страница 80)". Для получения дополнительной информации о включении входной

фильтрации см. "Глобальное конфигурирование сетей VLAN (Страница 170)".

- Для повышенной безопасности включите входную фильтрацию на всех портах по умолчанию. Для получения дополнительной информации о включении входной фильтрации см. "Глобальное конфигурирование сетей VLAN (Страница 170)".
- Если разрешен протокол SNMP, то ограничьте число IP-адресов, которые могут подключаться к устройству, а также измените имена строк-ключей. Кроме того, сконфигурируйте SNMP для выдачи trap-уведомления при ошибках аутентификации. Для получения дополнительной информации см. "Управление SNMP (Страница 297)".
- Избегайте использовать незащищенные службы, например, Telnet и TFTP, либо полностью отключите их, если это возможно. Эти службы присутствуют по исторически сложившимся причинам и по умолчанию отключены.
- Отключите протокол RCDP, если его использование не предполагается.
- Ограничьте число разрешенных одновременных сеансов служб веб-сервер, Telnet и SSH.
- Сконфигурируйте удаленный вход в систему таким образом, чтобы пересылать все журналы регистрации в центральный пункт. Для получения дополнительной информации см. "Управление журналами (Страница 65)" а также часто задаваемые вопросы по теме ""Как реализовать защищенный автоматический вход в систему ROS"" (https://support.industry.siemens.com/cs/ww/en/view/109756843).
- Файлы конфигурации представлены в формате CSV (значения с разделителями-запятыми) для удобства использования. Обеспечьте надлежащую защиту этих файлов конфигурации, если они существуют вне устройства. Например, шифруйте файлы, храните их в безопасном месте и не передавайте их через незащищенные коммуникационные каналы.
- Администрирование файлов конфигурации, сертификатов и ключей является обязанностью владельца устройства. Для повышения криптографической стойкости используйте ключи RSA длиной не менее 2048 бит и сертификаты, подписанные с помощью SHA256. Перед возвратом устройства в компанию Siemens ддля ремонта убедитесь в том, что шифрование отключено (чтобы создать версию файла конфигурации в виде открытого текста), а также замените текущие сертификаты и ключи временными *одноразовыми* сертификатами и ключами, которые могут быть уничтожены после возврата устройства.
- Принимайте во внимание наличие включенных на устройстве незащищенных протоколов. Некоторые протоколы, такие как HTTPS и SSH, является безопасными, а другие, такие как HTTP, MMS, Telnet и RSH, не были разработаны для этой цели. Необходимо предусмотреть подходящие средства защиты от незащищенных протоколов, чтобы предотвратить неавторизованный доступ к устройству/сети.

- Включите функции безопасности на портах доступа, для предотвращения самовольного физического подключения посторонних. Для получения дополнительной информации см. "Управление безопасностью на уровне порта (Страница 142)".

Аппаратное/программное обеспечение

- Всегда устанавливайте последнюю версию микропрограммного обеспечения, включая все исправления уязвимости. Актуальная информация об исправлениях уязвимости продуктов Siemens доступна на сайте промышленной безопасности [https://www.siemens.com/global/en/home/company/topic-areas/future-of-manufacturing/industrial-security.html] или на на сайте с рекомендациями по безопасности службы ProductCERT [http://www.siemens.com/innovation/en/technology-focus/siemens-cert/cert-security-advisories.htm]. Для получения обновлений рекомендаций по безопасности продуктов Siemens подпишитесь на RSS-рассылку на сайте Siemens ProductCERT Security Advisories или присоединяйтесь к нам в Twitter — @ProductCert.
- Включите функцию BPDU Guard для портов, на которых не ожидаются сообщения BPDU RSTP.
- Используйте последнюю версию веб-браузера, совместимую с RUGGEDCOM ROS, для обеспечения использования наиболее безопасных версий протокола безопасности транспортного уровня (TLS) и кодов.
- Если протокол Modbus не требуется пользователю, его можно деактивировать. Если необходимо активировать протокол Modbus, рекомендуется следовать рекомендациям по обеспечению безопасности, указанным в настоящем руководстве, а также сконфигурировать окружающую среду в соответствии с передовыми практиками защиты.
- Примите меры по предотвращению доступа к внешним ненадежным веб-страницам во время доступа к устройству через веб-браузер. Это может помочь в предотвращении потенциальных угроз безопасности, таких как перехват сеанса.
- Для обеспечения оптимального уровня безопасности используйте SNMPv3 при любой возможности. Используйте надежные ключи аутентификации и частные ключи без повторяющихся строк (например, *abc* или *abcabc*) с данной функцией. Для получения дополнительной информации о создании надежных паролей см. требования к паролям в "Конфигурирование паролей (Страница 131)".
- Если это не требуется в конкретной схеме сети, параметр *IP Forward (пересылка IP)* должен быть установлен в `Disabled` (Отключено), чтобы предотвратить маршрутизацию пакетов.

Политика

- Периодически производите аудит устройства, чтобы гарантировать его соответствие этим рекомендациям и/или любым внутренним политикам безопасности.
- Изучите прочую пользовательскую документацию для других продуктов Siemens, используемых по согласованию с устройством, для получения дополнительных рекомендаций по обеспечению безопасности.

1.3 Сообщения в системном журнале, относящиеся к системе безопасности

Ниже приведены сообщения о событиях системы защиты, которые могут генерироваться RUGGEDCOM ROS.

Категория	Сообщение о событии	Категория	Серьезность	Условие
SE_LOCAL_SUCCESSFUL_LOGON	{date} {time} INFO {temperature} Console user '{username}' logged in with admin level	local0 (локальные0)	Info (Информация)	Пользователь успешно вошел в систему через локальный интерфейс устройства.
SE_LOCAL_UNSUCCESSFUL_LOGON	{date} {time} INFO {temperature} Failed Console user '{username}' login attempt	local0 (локальные0)	Info (Информация)	Неудачная попытка входа в систему через локальный интерфейс устройства.
SE_NETWORK_SUCCESSFUL_LOGON	{date} {time} INFO {temperature} {protocol} user '{username}' logged in with admin level {ip address}	local0 (локальные0)	Info (Информация)	Пользователь успешно вошел в систему через сетевой интерфейс устройства.
SE_NETWORK_UNSUCCESSFUL_LOGON	{date} {time} INFO {temperature} Failed {protocol} user '{username}' login attempt {ip address}	local0 (локальные0)	Info (Информация)	Неудачная попытка входа в систему через сетевой интерфейс устройства.
SE_LOGOFF	{date} {time} INFO {temperature} console user '{username}, cmd: Logged out	local0 (локальные0)	Info (Информация)	Пользователь вышел из системы вручную или автоматически из-за таймаута через локальный интерфейс.
	{date} {time} INFO {temperature} {protocol} user '{username}' ({ip address}), cmd: Logged out	local0 (локальные0)	Info (Информация)	Пользователь вышел из системы вручную или автоматически

Категория	Сообщение о событии	Категория	Серьезность	Условие
				из-за тайм-аута через сетевой интерфейс.
SE_USER_AUTH_RADIUS_SERVER_NOT_AVAILABLE	{date} {time} INFO {temperature} RADIUS Primary server is unreachable	local0 (локальные0)	Info (Информация)	Неудачная попытка доступа к серверу RADIUS или отсутствие ответа от RADIUS.
SE_ACCESS_PWD_CHANGED	{date} {time} INFO {temperature} 'admin' level password changed {date} {time} INFO {temperature} {protocol} user {'username'} {(ip address)} Passwords Admin Password — MODIFIED.	local0 (локальные0)	Info (Информация)	Аутентифицированный пользователь изменил собственный пароль.
	{date} {time} INFO {temperature} 'guest' level password changed {date} {time} INFO {temperature} {protocol} user {'username'} {(ip address)} Passwords Guest Password — MODIFIED.	local0 (локальные0)	Info (Информация)	Аутентифицированный пользователь изменил пароль другого пользователя.
SE_USER_ACCOUNT_CHANGED	{date> {time} INFO {temperature} {protocol} user {username} {ip address}, Passwords Guest Username, old: {guest}, new: {new username} — MODIFIED.	local0 (локальные0)	Info (Информация)	Учетная запись пользователя изменена или назначена на другую роль.
SE_USER_ACCOUNT_DELETED	date> {time} INFO {temperature} {protocol} user {username} {ip address}, Passwords Guest Username, old: {username}, new:- MODIFIED.	local0 (локальные0)	Info (Информация)	Учетная запись пользователя удалена.
SE_ACCOUNT_LOCKED_TEMP	{date} {time} WARN {temperature} Excessive failed {protocol} access/ login attempts, service locked.	local0 (локальные0)	Warning (Предупреждение)	Предотвращение атаки "грубой силы" через временную блокировку учетной записи пользователя.
SE_SESSION_LOCKED_INACTIVITY	{date} {time} INFO 37C Console user 'admin' , cmd: Logged out	local0 (локальные0)	Info (Информация)	Сеанс был заблокирован через некоторое время отсутствия активности.
SE_RAS_SESSION_TERMINATED_INACTIVITY	{date} {time} INFO 37C HTTPS user 'admin' logged out (IP:192.168.0.200).	local0 (локальные0)	Info (Информация)	Удаленный сеанс завершен через некоторое время отсутствия активности.

Категория	Сообщение о событии	Категория	Серьезность	Условие
SE_UNSUCCESSFUL_RAS_LOGON	{date} {time} INFO {temperature} Failed {protocol} user '{username}' login attempt {ip address}	local0 (локальные0)	Info (Информация)	Неудачная попытка входа удаленного пользователя в систему через устройство удаленного доступа.
SE_RAS_LOGOFF	{date} {time} INFO {temperature} {protocol} user '{username}' {ip address}, cmd: loggd out	local0 (локальные0)	Info (Информация)	Удаленный пользователь вышел из системы через устройство удаленного доступа.
SE_RAS_CONNECTION_CLOSED	{date} {time} INFO {protocol} user {'username'} closing connection {(ip address)}	local0 (локальные0)	Info (Информация)	Соединение удаленного доступа закрыто.
SE_SUCCESSFUL_DEVICE_ IDENTIFICATION	{date} {time} INFO {temperature} {protocol} port 1 authorized addr {MAC address}, {VLAN ID} {date} {time} INFO{temperature} Secure port 1 learned addr {MAC address}, {VLAN ID}	local0 (локальные0)	Info (Информация)	Доступ к устройству получен через успешную аутентификацию порта 802.1X.
SE_UNSUCCESSFUL_DEVICE_ IDENTIFICATION	{date} {time}WARN 43C 802.1X port 1 auth failed, addr {MAC address}, {VLAN ID}	local0 (локальные0)	Warning (Предупреждение)	Доступ к устройству запрещен из-за неудачной аутентификации порта 802.1X.
SE_SUCCESSFUL_DEVICE_ AUTHENTICATION	{date} {time} INFO {temperature}{protocol} user {username} (pub id 1 fingerprint:{value}) logged in with {role} access {ip address}	local0 (локальные0)	Info (Информация)	Успешная аутентификация устройства через аутентификацию на базе сертификата.
SE_AUDIT_LOG_CLEARED	{date} {time}INFO {temperature} Console user 'admin' , cmd: clearlogs {date} {time} INFO {temperature} clearlogs	local0 (локальные0)	Info (Информация)	Пользователь удалил локальный буфер регистрации.
SE_CONFIG_CHANGE	{date} {time} INFO {temperature} Console user '{username}', IP Services Inactivity Timeout, old: 5 min, new: Disable — MODIFIED {date} {time} INFO {temperature} Configuration changed	local0 (локальные0)	Info (Информация)	Пользователь изменил определенные параметры конфигурации.
	{date} {time} INFO {temperature} Console user '{username}', Load	local0 (локальные0)	Info (Информация)	Пользователь инициировал сброс до

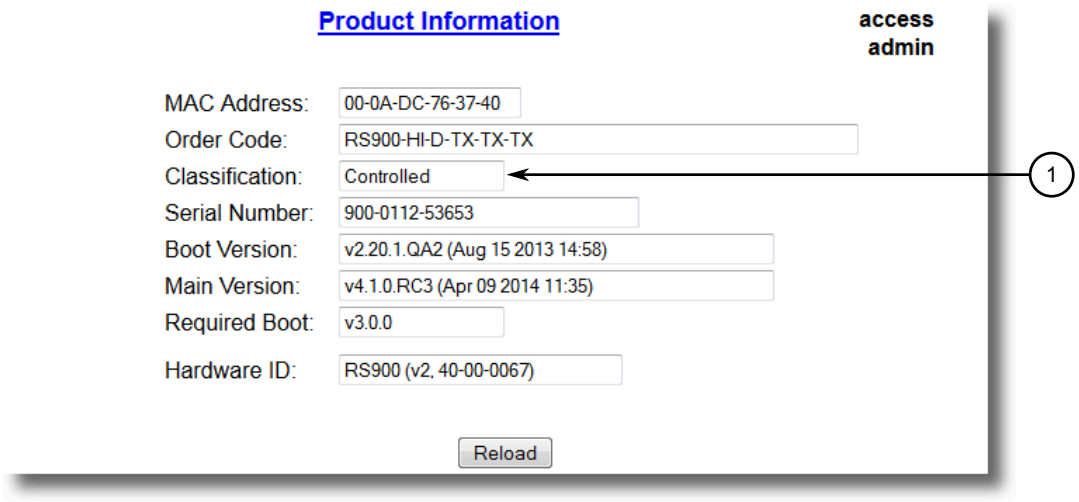
Категория	Сообщение о событии	Категория	Серьезность	Условие
	Factory Defaults Defaults Choice, old: None, new: All — MODIFIED.			заводских настроек.
SE_SOFTWARE_INTEGRITY_CHECK_ FAILED	{date} {time} NOTE {temperature} SFTP put file main.bin from {ip address} by user {date} {time} INFO Console user '{username}', cmd: xmodem receive main.bin {date} {time} ERRO Downloaded file main.bin is invalid: Bad signature {date} {time} NOTE Downloaded file with invalid signature (-7711) {date} {time} Downloaded file main.bin is invalid: Body CRC invalid	local0 (локальные0)	Ошибка	Проверка целостности микропрограммного/ программного обеспечения выявила ошибку целостности.
SE_BACKUP_SUCCESSFULLY_DONE	{date} {time} NOTE {temperature} config.csv copied to A:\config.csv	local0 (локальные0)	Notice (Замечание)	Система успешно создала резервную копию при установке съемного носителя.

1.4 Сравнение контролируемых и неконтролируемых устройств

Устройства под управлением RUGGEDCOM ROS могут быть контролируемыми (C) или неконтролируемыми (NC).

- **Контролируемые** коммутаторы имеют больше криптографических функций.
- **Неконтролируемые** коммутаторы имеют ограниченную криптографическую функциональность.

Чтобы определить, относится устройство к контролируемым или неконтролируемым, перейдите в***Diagnostics » View Product Information***. Параметр `Classification` в форме **Product Information** указывает, является устройство контролируемым или неконтролируемым.



① Поле классификации

Рисунок 1.1 Пример формы "Product Information" (Информация о продукте)

1.5 Поддерживаемые сетевые стандарты

RUGGEDCOM ROS поддерживает следующие сетевые стандарты:

Стандарт	10 Мбит/с	100 Мбит/с	1000 Мбит/с	10000 Мбит/с	Описание
IEEE 802.1AB	•	•	•	•	Протокол обнаружения канального уровня (LLDP)
IEEE 802.1D	•	•	•	•	MAC-мосты, протокол связующего дерева (STP)
IEEE 802.1Q	•	•	•	•	VLAN (виртуальная ЛВС)
IEEE 802.1Q-2005	•	•	•	•	Протокол множественных связующих деревьев (MSTP)
IEEE 802.1w	•	•	•	•	Протокол быстрого связующего дерева (RSTP)
IEEE 802.1p	•	•	•	•	Класс сервиса (CoS)
IEEE 802.1x	•	•	•	•	Управление сетевым доступом на базе портов
IEEE 802.3	•				10Base-T
IEEE 802.3u		•			100Base-TX/100Base-FX
IEEE 802.3z			•		1000Base-SX/LX
IEEE 802.3ab			•		1000Base-TX
IEEE 802.3ad	•	•	•	•	Агрегирование каналов связи
IEEE 802.3ae				•	10GBase
IEEE 802.3x	•	•	•	•	Управление потоком данных
IEEE 1588-2008	•	•	•	•	Управление точным временем (PTP), версия 2

Стандарт	10 Мбит/с	100 Мбит/с	1000 Мбит/с	10000 Мбит/с	Описание
МЭК 62439-2:2016	•	•	•	•	Протокол резервирования среды передачи (MRP)

1.6 Поддержка сетевого протокола интернета

RUGGEDCOM ROS поддерживает как адреса IPv4, так и глобальные индивидуальные адреса IPv6 для отдельных функций. Для получения дополнительной информации см. "Функции, поддерживаемые протоколами IPv4 и/или IPv6 (Страница 14)".

1.6.1 Функции, поддерживаемые протоколами IPv4 и/или IPv6

В таблице ниже указаны функции, поддерживаемые протоколами IPv4 и/или IPv6.

Функция	IPv4	IPv6
Ping	•	•
Сервер Telnet	•	•
SSH-сервер	•	•
SFTP-сервер	•	•
Доступ к веб-серверу	•	•
Клиент SNMP (v1, v2c, v3)	•	•
Клиент Radius	•	•
Клиент TACACS+	•	•
TFTP	•	•
Сервер/клиент NTP	•	•
Клиент DHCP	•	
Удаленный syslog-сервер	•	•
RSH	•	•
Протокол последовательной передачи	•	
ARP	•	
Сообщения сетевого обнаружения[a]		•

[a] Поддерживает сетевые запросы и сетевую рассылку.

1.6.2 Адрес IPv4

Адрес IPv4 составляет 32 бита в длину и записывается в виде точечно-цифрового выражения, состоящего из четырех октетов, разделенных точками. Каждое число может быть равным значению от нуля до 255.

Пример: 192.168.0.1

1.6.3 Адрес IPv6

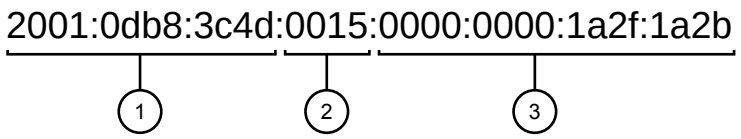
RUGGEDCOM ROS поддерживает глобальные индивидуальные адреса IPv6 для управления.

Длина адреса IPv6 составляет 128 бит. Он состоит из восьми 16-битных октетов, разделенных двоеточием.

Адреса IPv6 часто содержат последовательные шестнадцатеричные поля с нулями. Двойное двоеточие *(::)* может использоваться для сжатия нулей в адресе. Например, адрес IPv6 FF00:5402:0:0:0:0:0:32 можно представить в виде FF00:5402::32.

Формат адреса IPv6:

- Три крайних левых поля (48 бит) содержат префикс объекта. Префикс обычно определяет часть общей сети, которую Интернет провайдер резервирует для определенного объекта.
- Центральное поле — это 16-битный идентификатор подсети, который распределяется на конкретный объект. Идентификатор подсети описывает частную топологию, также известную как топология объекта, поскольку она является внутренней для объекта.
- Четыре последние поля справа правых (64 бита) содержат идентификатор интерфейса.



① Префикс объекта
② Идентификатор подсети
③ Идентификатор интерфейса

Рисунок 1.2 Пример глобального индивидуального адреса IPv6

1.7 Схема нумерации портов

Для быстрой идентификации каждому порту устройства RUGGEDCOM RST916C присваивается идентификатор. Все номера портов на устройстве нанесены методом трафаретной печати.

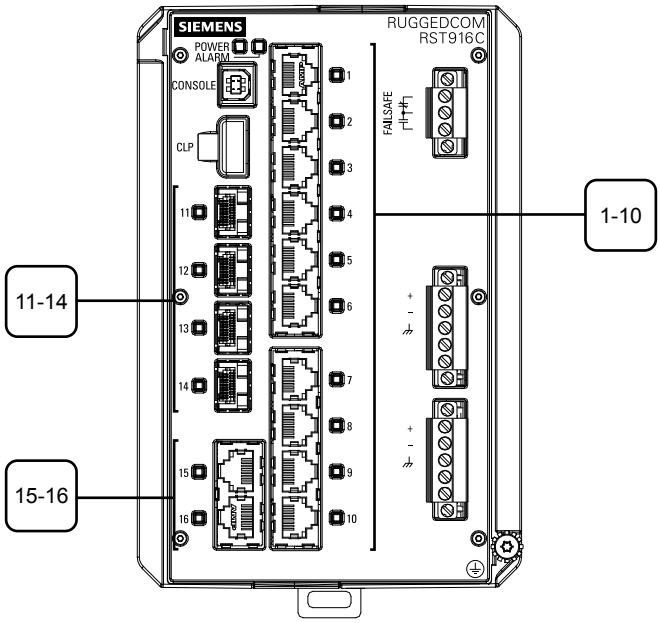


Рисунок 1.3 RUGGEDCOMRST916C Нумерация портов (стандартная)

Рекомендуется использовать эти идентификаторы для настройки применимых функций на выбранных портах.

1.8 Службы, доступные на портах TCP или UDP

В приведенной ниже таблице указаны службы, доступные в RUGGEDCOM ROS. Таблица содержит следующую информацию:

- **Службы**

  Службы, которые поддерживает устройство.

- **Номер порта**

  Номер порта, ассоциированный с соответствующей службой.

- **Порт открыт**

  Состояние порта: является ли порт открытым или закрытым по умолчанию, и можно ли его состояние изменить в настройках.

  Примечание
  В некоторых случаях службу можно отключить, но порт может оставаться открытым (например, TFTP).

- **Состояние порта по умолчанию**

  Состояние порта по умолчанию (т. е. открыт или закрыт).

- **Авторизация при доступе**

  Указывает, производится ли аутентификация портов/служб во время доступа.

Службы	Номер порта	Служба включена/ отключена	Авторизация при доступе	Примечание
Telnet	TCP/23	Отключено	Да	Доступно только через интерфейсы управления.
HTTP	TCP/80	Включена, перенаправляет на 443	—	Перенаправляет на 443 только на контролируемых версиях
HTTPS	TCP/443	Включена (допускает конфигурирование)	Да	Применимо только к конфигурируемым версиям
RSH	TCP/514	Отключена (допускает конфигурирование)	Да	Доступно только через интерфейсы управления.
TFTP	UDP/69	Отключена (допускает конфигурирование)	Нет	Доступно только через интерфейсы управления.
SFTP	TCP/22	Включено	Да	Доступно только через интерфейсы управления.
SNMP	UDP/161	Отключена (допускает конфигурирование)	Да	Доступно только через интерфейсы управления.
SNTP	UDP/123	Включена (допускает конфигурирование)	Нет	Доступно только через интерфейсы управления.
SSH	TCP/22	Включено	Да	Доступно только через интерфейсы управления.
ICMP	—	Включено	Нет	
TACACS+	TCP/49 (допускает конфигурирование)	Отключена (допускает конфигурирование)	Да	
RADIUS	UDP/1812 для передачи (допускает конфигурирование), открывает случайный порт для прослушивания	Отключена (допускает конфигурирование)	Да	Доступно только через интерфейсы управления.
Удаленный системный журнал	UDP/514 (допускает конфигурирование)	Отключена (допускает конфигурирование)	Нет	Доступно только через интерфейсы управления.
TCP Modbus (сервер)	TCP/502	Отключена (допускает конфигурирование)	Нет	Доступно только через интерфейсы управления.
TCP Modbus (коммутатор)	TCP/502	Отключена (допускает конфигурирование)	Нет	

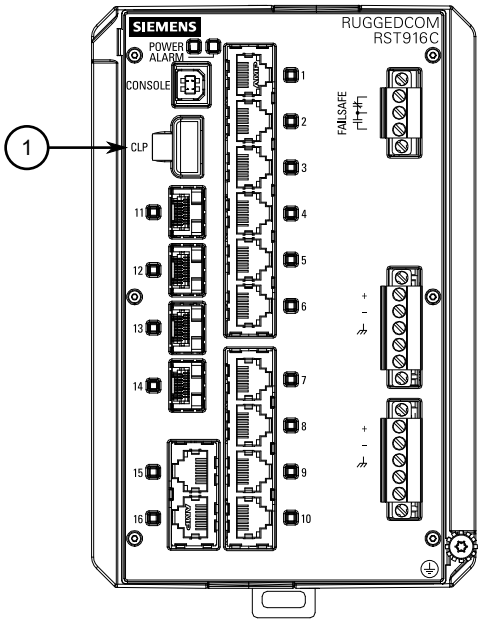
Службы	Номер порта	Служба включена/ отключена	Авторизация при доступе	Примечание
DHCP, агент DHCP	UDP/67, 68 посылает сообщение, если разрешено. Если сообщение принято, то оно всегда приходит на процессор; отбрасывается, если служба не сконфигурирована.	Отключена (допускает конфигурирование)	Нет	
RCDP	—	Включена (допускает конфигурирование)	Да	
PTP (IEEE 1588)	UDP/319 UDP/320	Отключена (допускает конфигурирование)	Нет	

1.9 Съемное запоминающее устройство

RST916C имеет доступный для пользователя слот памяти, поддерживающий стандартную ISO/МЭК 9293-совместимую файловую систему FAT16 или FAT32 (таблица размещения файлов) на CLP — съемном сменном носителе, используемом для данных конфигурации устройства.RUGGEDCOM

Важным преимуществом использования файловой системы на базе FAT является возможность изменения ее содержимого на любом компьютере с интерфейсом USB Type C.

Примечание
Карта CLP будет автоматически отформатирована в файловой системе FAT16 или FAT32, если на CLP загружена какая-либо файловая система, кроме FAT16 или FAT32.



① Съемный носитель CLP

Рисунок 1.4 Слот памяти

Основной задачей съемной карты CLP является предоставление места для автоматического резервирования основного образа микропрограммного обеспечения, а также способность автоматически восстанавливать образ микропрограммного обеспечения и/или конфигурацию из резервной копии.Его также можно использовать для восстановления доступа к устройству в случае повреждения данных во внутренней флеш-памяти.

Во время нормальной работы устройство автоматически синхронизирует файлы `main.bin` и `config.csv` на устройстве и карте microSD/microSDHC. Если действительный файл микропрограммного обеспечения (`main.bin`) существует на CLP, RUGGEDCOM ROS загрузит и выполнит микропрограммное обеспечение с CLP.

При перезагрузке устройства система сравнивает файлы `main.bin` и `config.csv` на устройстве и на CLP. Если файлы на устройстве отличаются от имеющихся на CLP, устройство загрузит файлы с CLP в свою файловую систему и применит их.

Другие варианты применения съемной карты CLP включают:

- быстрое восстановление после отказа аппаратного обеспечения в поле;
- резервное копирование и восстановление микропрограммного обеспечения и данных конфигурации;
- копирование микропрограммного обеспечения и конфигурации с одного устройства на другое;
- выполнение автоматического обновления микропрограммного обеспечения;

- восстановление после отказа обновления микропрограммного обеспечения или реконфигурации;
- автоматическое резервное копирование системных журналов.

Помимо возможности автоматического резервного копирования и восстановления микропрограммного обеспечения и конфигурации с помощью съемного носителя, RUGGEDCOM ROS поддерживает расширенный набор утилит командной строки для манипулирования файлами системы. Съемный носитель — это диск формата, привычного пользователям файловой системы на базе FAT, с поддержкой команд через интерфейсы командной строки CLI (CLI-команд), таких как **`dir`**, **`copy`** и**`move`**. Полный перечень доступных CLI-команд см. в "Доступные CLI-команды (Страница 27)".

Примечание
Инструкции по отключению автоматического доступа к карте CLP см. в"Включение/отключение автоматического доступа к съемному запоминающему устройству (Страница 48)".

2 Использование операционной системы ROS

В данном разделе рассматривается использование RUGGEDCOM ROS.

2.1 Вход в систему

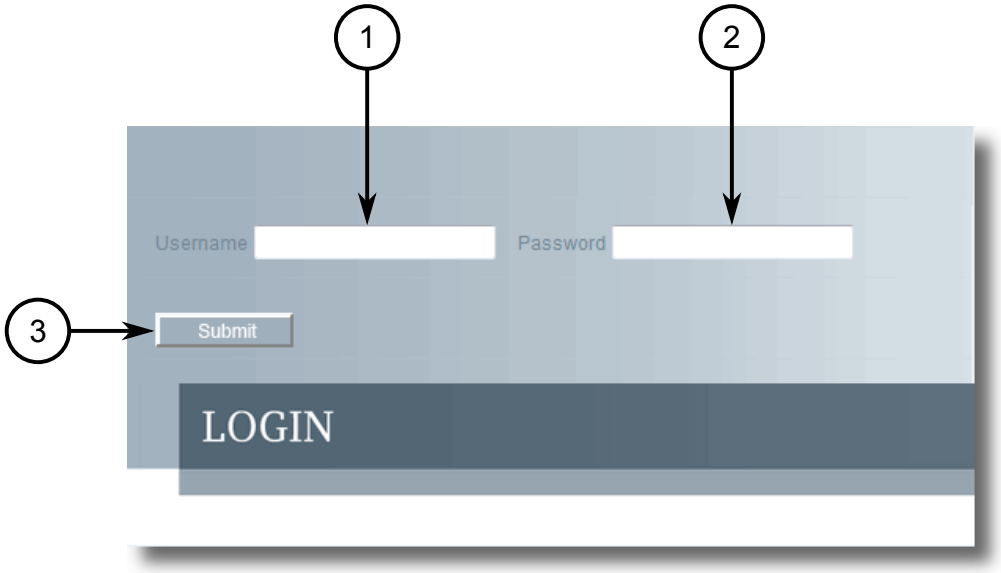
Чтобы войти в систему устройства, сделайте следующее:

1. Подключитесь к устройству напрямую или через веб-браузер. Для получения дополнительной информации о подключении к устройству см. "Подключение к операционной системе ROS (Страница 51)".

   После установки соединения появляется форма входа в систему.

① Поле имени пользователя
② Поле пароля

Рисунок 2.1 Экран входа в систему SSH (консольный интерфейс)



① Поле имени пользователя
② Поле пароля
③ Кнопка подтверждения

Рисунок 2.2 Экран входа в систему (веб-интерфейс)

Примечание
По умолчанию на устройстве установлены следующие имя пользователя и пароль:

Имя пользователя	Пароль
admin	admin

⚠ ЗАМЕТКА
Угроза безопасности — риск неавторизованного доступа и/или использования Перед вводом устройства в эксплуатацию необходимо сменить пароль администратора по умолчанию, чтобы предотвратить неавторизованный доступ. Для получения дополнительной информации об изменении паролей см. "Конфигурирование паролей (Страница 131)".

2. В поле **User Name** введите имя учетной записи, существующей на устройстве.
3. В поле **Password** введите пароль для учетной записи.
4. Нажмите **Enter** или **Submit** (только веб-интерфейс).

2.2 Выход из системы

Чтобы выйти из системы устройства, перейдите на основной экран и сделайте следующее:

- Чтобы выйти из подключения через консоль или из подключения по протоколу SSH, нажмите **CTRL** + **X**.
- Чтобы выйти из веб-интерфейса, нажмите **Logout**.

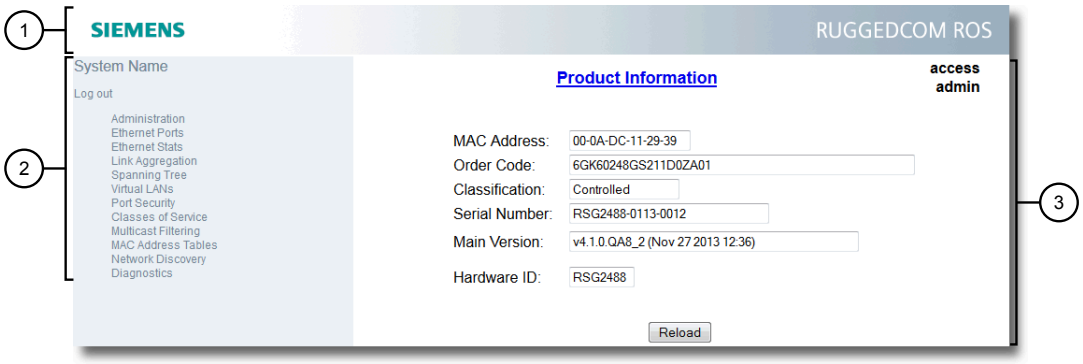
① Выход из системы

Рисунок 2.3 Пример веб-интерфейса

Примечание
При наличии ожидающих подтверждения изменений конфигурации RUGGEDCOM ROS запросит подтверждение перед отменой изменений и выхода из системы устройства.

2.3 Использование веб-интерфейса

Веб-интерфейс представляет собой Graphical User Interface (GUI — графический интерфейс пользователя) на веб-основе, отображающий важную информацию и средства управления в веб-браузере. Интерфейс разделен на три области: баннер, меню и основная область.



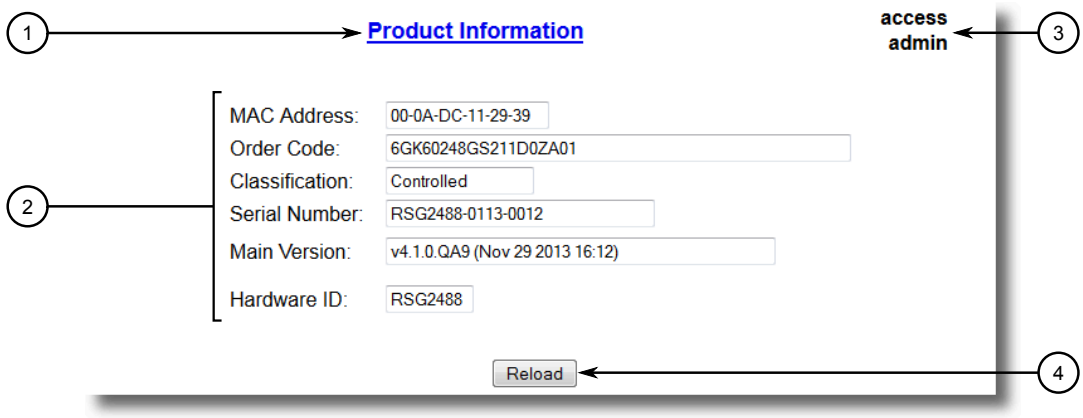
① Верхняя область
② Боковая область
③ Основная область

Рисунок 2.4 Пример раскладки веб-интерфейса

Область	Описание
Верхняя	В верхней области отображается имя системы для устройства.
Боковая	В боковой области расположена кнопка выхода из системы и сворачиваемый список ссылок, который открывает различные экранные формы в основной области. Информацию о выходе из системы RUGGEDCOM ROS, см. в "Выход из системы (Страница 23)".
Основная	В основной области отображаются параметры и/или данные, относящиеся к выбранной функции.

Каждая экранная форма основной области содержит заголовок, уровень доступа текущего пользователя, параметры и/или данные (в виде формы или таблицы) и средства управления (например, add (добавить), delete (удалить), refresh (обновить) и т. д.). В заголовке предусмотрен доступ к зависящей от контекста справочной системе (Help) для экранной формы, которая предоставляет важную информацию о доступных параметрах и/или данных. Щелкните ссылку, чтобы открыть справочную информацию в новом окне.

Если генерируется оповещение, на каждой экранной форме вместо уровня доступа пользователя отображается соответствующее уведомление до тех пор, пока аварийный сигнал не будет сброшен. В уведомлении указывается количество активных в данный момент оповещений. Для получения дополнительной информации об оповещениях см. "Управление оповещениями (Страница 112)".



① Заголовок
② Параметры и/или данные
③ Уровень доступа или уведомление об оповещении
④ Кнопка "Перезагрузить"

Рисунок 2.5 Пример элементов типовой экранной формы

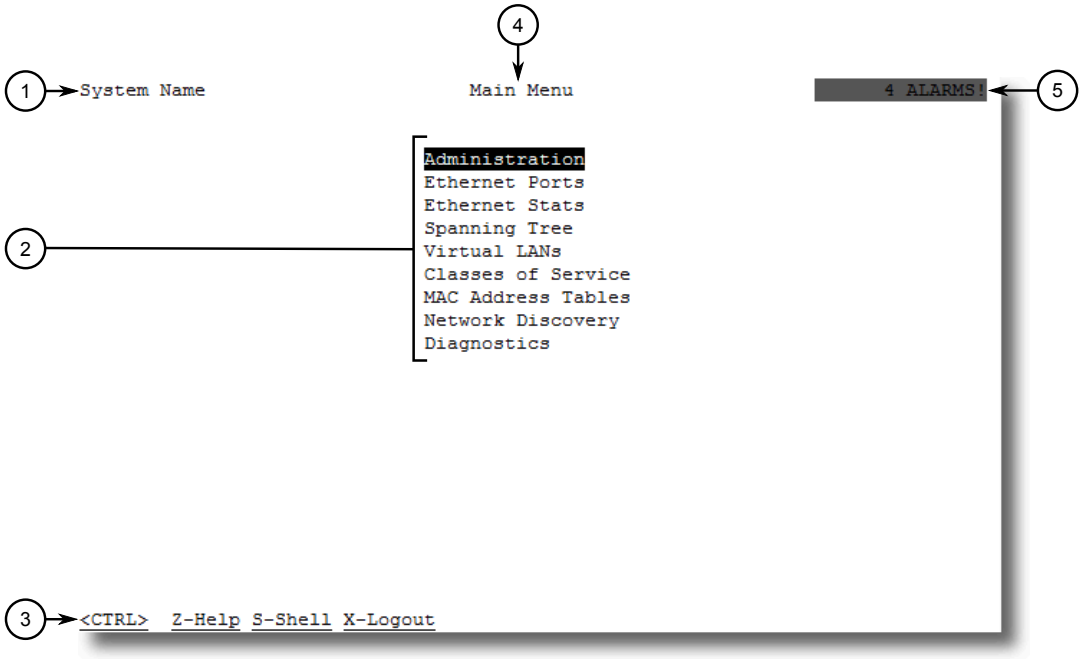
Примечание
При желании веб-интерфейс можно отключить. Для получения дополнительной информации см. "Включение/отключение веб-интерфейса (Страница 112)".

2.4 Использование консольного интерфейса

Консольный интерфейс представляет собой графический интерфейс пользователя (GUI), организованный в виде последовательности меню. В основном им пользуются через подключение по консоли, а также через подключение с использованием различных IP-сервисов, таких как сессии Telnet, RSH (Remote Shell) и SSH (Secure Shell), а также удаленное исполнение команд через SSH.

Примечание
IP-сервисы можно ограничить в целях регулирования доступа к устройству. Для получения дополнительной информации см. "Конфигурирование IP-сервисов (Страница 96)".

Каждая экранная форма состоит из системного идентификатора, названия текущего меню и панели команд. В правом верхнем углу каждой экранной формы указываются оповещения.



① Идентификация системы
② Различные меню
③ Панель команд
④ Имя меню
⑤ Индикатор оповещения

Рисунок 2.6 Пример консольного интерфейса

Примечание
Системный идентификатор может конфигурироваться пользователем. Для получения дополнительной информации о настройке имени системы см. "Конфигурирование системной информации (Страница 111)".

Навигация по интерфейсу

Используйте следующие средства управления для навигации между экранными формами в консольном интерфейсе:

Enter	Выберите элемент меню и нажмите **Enter**, чтобы перейти в подменю или в экранную форму снизу.
Esc	Нажмите **Esc**, чтобы вернуться к предыдущей экранной форме.

Конфигурирование параметров

Используйте следующие средства управления для выбора и конфигурирования параметров в консольном интерфейсе:

Стрелки вверх/ вниз	Используйте стрелки вверх и вниз для выбора параметров.

Enter	Выберите параметр и нажмите **Enter**, чтобы перейти к его редактированию. Нажмите **Enter** еще раз, чтобы подтвердить изменение.
Esc	При редактировании параметра нажмите **Esc**, чтобы отменить все изменения.

Команды

Панель команд содержит список различных команд, которые можно подавать в консольном интерфейсе. Некоторые команды являются специальными для конкретных экранных форм. Список стандартных команд:

Ctrl + A	Подтвердить изменения, внесенные в конфигурацию на текущей экранной форме. **Примечание** Перед выходом из экранной формы RUGGEDCOM ROS автоматически запросит пользователя подтвердить внесенные изменения. **Примечание** При наличии съемного носителя (т. е. CLP) изменения конфигурации приводят к обновлению файла `config.csv` как во флеш-памяти, так и на съемном носителе.
Ctrl + I	Вставить новую запись.
Ctrl + L	Удалить запись.
Ctrl + S	Открыть CLI-интерфейс.
Ctrl + X	Завершает текущий сеанс. Команда доступна только в главном меню.
Ctrl + Z	Отобразить важную информацию о текущей экранной форме или выбранном параметре.

2.5 Использование интерфейса командной строки

Command Line Interface (CLI — интерфейс командной строки) обеспечивает комплекс команд для обновления RUGGEDCOM ROS, генерирования сертификатов и ключей, отслеживания событий, поиска и устранения неисправностей и т. д. Доступ к командной строке осуществляется через консольный интерфейс с помощью комбинации клавиш **Ctrl-S**.

2.5.1 Доступные CLI-команды

В командной строке доступны следующие команды:

Команда	Описание	Авторизованные пользователи
alarms `all`	Показывает список доступных оповещений. Опциональные и/или необходимые параметры включают: • `all` отображает все доступные оповещения	Guest (Гость), Operator (Оператор), Admin (Администратор)

Команда	Описание	Авторизованные пользователи
arp	Показывает таблицу соответствия MAC-адресов IP-адресам.	Admin (Администратор)
attrib { *filename* } [+ | -] [W | H]	Устанавливает и удаляет атрибуты файла.	Admin (Администратор)
banner { *-?* } { *-c* } { *-l* } { *-f* } { -s <enter>{ *text* } | -s { *text* } } -e { *line_number* } -d { *line_number* }	Изменяет файл баннера `banner.txt`. Опциональные и/или необходимые параметры включают: • { *-?* } Отображает справочную информацию об опциях команд. • { *-c* } Очищает содержимое файла баннера. • { *-l* } Отображает файл баннера с индексированными номерами строк. • { *-f* } Восстанавливает заводской баннер по умолчанию. • -s <enter> { *text* } Вводит текст в файл баннера. Существующий текст баннера стирается и заменяется на новый. Принимает до 8190 символов и поддерживает наборы управляющих символов для редактирования текста. • -s { *text* } Вводит текст в файл баннера. Используется для изменения файла через терминал. Существующий текст баннера стирается и заменяется на новый. Принимает до 500 символов, максимум 250 слов. • -e { *line_number* } Редактирует выбранную строку файла баннера. • -d { *line_number* } Удаляет выбранную строку файла баннера.	Admin (Администратор)
chkdsk	Проверяет файловую систему на ошибки диска.	Admin (Администратор)
clearalarms	Удаляет все оповещения.	Operator (Оператор), Admin (Администратор)
clearethstats [all | { *port* }]	Удаляет статистику подключений по Ethernet для одного или нескольких портов. Опциональные и/или необходимые параметры включают: • all очищает статистику для всех портов • { *port* } список номеров портов с разделителем-запятой (например, 1,3-5,7)	Operator (Оператор), Admin (Администратор)
clearlogs	Удаляет системные журналы и журналы фатальных сбоев.	Admin (Администратор)
clrstpstats	Очищает статистику для всех портов.	Operator (Оператор), Admin (Администратор)
cls	Очищает экран.	Guest (Гость), Operator (Оператор), Admin (Администратор)
copy	Копирует целевой файл во внутреннюю память или на съемную карту памяти. Примеры:	Admin (Администратор)

Команда	Описание	Авторизованные пользователи

	• Копирование файла со съемной карты памяти на внутреннюю память
	`copy a:\config.csv config.csv`
	• Копирование файла из внутренней памяти на съемную карту памяти
	`copy config.csv a:\config.csv`	

delete { *filename* }	Удаляет указанный файл на съемной карте памяти.	Admin (Администратор)
dir	Распечатывает листинг директории внутренней памяти.	Guest (Гость), Operator (Оператор), Admin (Администратор)
dir { *A:* }	Распечатывает листинг директории съемной карты памяти, если она установлена.	Guest (Гость), Operator (Оператор), Admin (Администратор)
exit	Завершает сеанс.	Guest (Гость), Operator (Оператор), Admin (Администратор)
factory	Активирует заводской режим, в котором доступны дополнительные заводские команды, используемые для тестирования и устранения проблем. Доступно только для пользователей категории admin (администратор). **⚠ ЗАМЕТКА** **Опасность для конфигурации — риск повреждения микропрограммного обеспечения** Неправильное использование заводских команд может нарушить работу устройства и/или перевести его в нерабочее состояние, вывести из которого устройство смогут только специалисты предприятия-изготовителя.	Admin (Администратор)
flashfiles { info { *filename* } | defrag }	Набор диагностических команд для отображения информации о файловой системе и для дефрагментации флеш-памяти. Опциональные и/или необходимые параметры включают: • info { *filename* } показывает информацию об указанном файле в файловой системе на флеш-диске • defrag дефрагментирует файлы в файловой системе на флеш-диске Дополнительную информацию о команде **flashfiles** см. в разделе "Администрирование файловой системы на флеш-диске (Страница 42)".	Admin (Администратор)
flashleds { *timeout* }	Зажигает светодиодные индикаторы на устройстве на указанное количество секунд. Опциональные и/или необходимые параметры включают: • { *timeout* } продолжительность в секундах режима мерцания светодиодных индикаторов. Чтобы остановить мерцание светодиодных индикаторов, задайте для тайм-аута значение 0 (ноль).	Admin (Администратор)

Команда	Описание	Авторизованные пользователи
format { *disk* }	Форматирует указанный диск (например, A:).	Admin (Администратор)
fpgacmd	Предоставляет доступ к инструменту управления FPGA для поиска неисправностей, связанных с синхронизацией времени	Admin (Администратор)
help { *command* }	Отображает краткое описание указанной команды. Если команда не указана, отображает список всех доступных команд, включая описание для каждой. Опциональные и/или необходимые параметры включают: • { *command* } — имя команды.	Guest (Гость), Operator (Оператор), Admin (Администратор)
ipconfig	Отображает текущий IP-адрес, маску подсети и шлюз по умолчанию.	Guest (Гость), Operator (Оператор), Admin (Администратор)
label { *disk* } { *string* }	Применяет метку к указанному диску (например, A:).	Admin (Администратор)
loaddflts	Сбрасывает конфигурации до заводских настроек.	Admin (Администратор)
logout	Выход из оболочки.	Guest (Гость), Operator (Оператор), Admin (Администратор)
logs	Отображает записи в системном журнале в оболочке CLI.	Admin (Администратор)
passwd { *user_name* } { *new_password* }	Изменяет пароль выбранного пользователя. Опциональные и/или необходимые параметры включают: • { *user_name* } — существующее имя пользователя (user_name) в RUGGEDCOM ROS. • { *new_password* } — новый пароль, который заменит существующий пароль выбранного пользователя. Данная команда недоступна в сеансах Telnet.	Admin (Администратор)
ping { *address* } { { *count* } | { *timeout* } }	Посылает эхо-запрос ICMP на удаленное подключенное устройство. Для каждого принятого ответа отображается время прохождения сигнала в обоих направлениях. Команда может применяться для проверки возможности соединения с соседним подключенным устройством. Это также полезный инструмент для тестирования арендованных каналов связи. Эта команда также включает возможность отправки конкретного числа ping-команд с указанным интервалом времени, в течение которого необходимо ждать ответа. Опциональные и/или необходимые параметры включают: • { *address* } — целевой IP-адрес. • { *count* } — количество эхо-запросов для отправки. По умолчанию 4. • { *timeout* } — интервал времени в миллисекундах для ожидания каждого ответа. Диапазон от 2 до 5000 секунд. По умолчанию 300 миллисекунд.	Guest (Гость), Operator (Оператор), Admin (Администратор)

Команда	Описание	Авторизованные пользователи
	Примечание Устройство, проверяемое с помощью ping-команды, должно поддерживать эхо-запросы и эхо-ответы ICMP. В начале исполнения ping-команды выдается ARP-запрос для определения MAC-адреса устройства. Если устройство, проверяемое с помощью ping-команды, не находится в одной сети с устройством, передающим ping-запросы на другие устройства, то должен быть задан шлюз по умолчанию.	
purgemac	Очищает таблицу MAC-адресов.	Operator (Оператор), Admin (Администратор)
random	Выдает случайные числа или число для инициализации.	Admin (Администратор)
rename { *source* } { *destination* }	Переименовывает указанный файл. Необходимо добавить путь к новому имени файла, чтобы одновременно переместить файл.	Admin (Администратор)
reset	Выполняет аппаратный перезапуск коммутатора.	Operator (Оператор), Admin (Администратор)
resetport { all | { *ports* } }	Сбрасывает один или несколько Ethernet-портов, что может быть полезным для принудительного повторного согласования скорости передачи и дуплексного режима, либо в ситуациях, когда партнер по соединению фиксируется в неверном состоянии. Опциональные и/или необходимые параметры включают: • `all` сбрасывает все порты • { *ports* } список номеров портов с разделителем-запятой (например, 1,3-5,7)	Operator (Оператор), Admin (Администратор)
rmon	Показывает имена всех допустимых объектов для оповещений RMON.	Guest (Гость), Operator (Оператор), Admin (Администратор)
route	Показывает конфигурацию шлюзов.	Guest (Гость), Operator (Оператор), Admin (Администратор)
sql { default | delete | help | info | insert | save | select | update }	Обеспечивает SQL-подобный интерфейс для управления всей системной конфигурацией и параметрами состояния. Все имена команд, операторов, таблицы и столбцов нечувствительны к регистру. Опциональные и/или необходимые параметры включают: • `default` устанавливает для всех записей в таблице (таблицах) заводские значения по умолчанию • `delete` позволяет удалять записи из таблицы • `help` предоставляет справку для какой-либо команды или оператора SQL • `info` показывает различную информацию о таблицах в базе данных • `insert` позволяет вставлять новые записи в таблицу • `save` сохраняет базу данных в энергонезависимой памяти	Admin (Администратор)

Команда	Описание	Авторизованные пользователи
	• `select` обращается с запросом к базе данных и выводит на экран выбранные записи • `update` позволяет обновлять существующие записи в таблице Дополнительную информацию о команде **`sql`** см. в разделе "Использование команд SQL (Страница 38)".	
`sshdigest`	Отображает идентификационную метку хост-ключа устройства.	Admin (Администратор)
`sshkeygen` `[ rsa | dsa ] [ 1024 | 2048 | 3072 ] { N }`	Генерирует новые ключи RSA или DSA в `ssh.keys`. Длина ключей может составлять 1024, 2048 или 3072 бит.	Admin (Администратор)
`sshpubkey`	Составляет список, удаляет и обновляет записи ключей в файле sshpub.keys.	Admin (Администратор)
`sslkeygen` `{ keytype } { N }`	Генерирует новый SSL-сертификат в `ssl.crt`. Опциональные и/или необходимые параметры включают: • { *keytype* } — тип ключа: rsa или ecc • { *N* } — количество бит в длине. Допустимые размеры для ключей RSA: 1024, 2048 или 3072. Допустимые размеры для ключей ECC: 256, 384 или 521.	Admin (Администратор)
`svcmod` `-s { snmpaccess } { -i { GroupName } | -d { GroupName } } -sm { SecurityModel } -sl { SecurityLevel } -rv { ReadViewName } -wv { WriteViewName } -nv { NotifyViewName }`	Изменяет группы доступа SNMP. Опциональные и/или необходимые параметры включают: • `-i { GroupName }` создает новую группу доступа с указанным именем группы или изменяет параметры, связанные с указанной группой доступа, если она уже существует • `-d { GroupName }` удаляет указанную группу доступа • `-sm { SecurityModel }` указывает модель безопасности для использования • `-sl { SecurityLevel }` указывает уровень безопасности SNMP для назначения указанной группе доступа. Допустимые значения: authPriv (связь с аутентификацией и конфиденциальностью), authNoPriv (связь с аутентификацией и без конфиденциальности) или noAuthnoPriv (связь без аутентификации и конфиденциальности). • `-rv { ReadViewName }` идентифицирует подраздел (подразделы) MIB, к которым эта запись разрешает доступ для чтения. Допустимые значения: noView, V1Mib или allOfMib. • `-wv { WriteViewName }` идентифицирует подраздел (подразделы) MIB, к которым эта запись разрешает доступ для записи. Допустимые значения: noView, V1Mib или allOfMib. • `-nv { NotifyViewName }` идентифицирует подраздел (подразделы) MIB, к которым эта запись разрешает доступ для уведомлений. Допустимые значения: noView, V1Mib или allOfMib.	Admin (Администратор)

Команда	Описание	Авторизованные пользователи
svcmod -s { *snmpgroup* } { -i { *UserName* } | -d { *UserName* } } -sm { *SecurityModel* } -g { *group* }	Изменяет соответствия групп пользователей моделям и уровням безопасности SNMP. Опциональные и/или необходимые параметры включают: • -i { *UserName* } -sm { *SecurityModel* } создает новое имя пользователя и профиль защиты, как указано, или изменяет параметры, связанные с указанным именем пользователя и профилем защиты, если они уже существуют • -d { *UserName* } -sm { *SecurityModel* } удаляет указанное имя пользователя и профиль защиты • -g { *group* } указывает группу, которой принадлежат имя пользователя и профиль защиты	Admin (Администратор)
svcmod -s { *snmpuser* } { -i { *UserName* } | -d { *UserName* } } -c { *Community* } -ip { *IP* } -ap { *protocol* } -ak { *key* } -pp { *protocol* } -pk { *key* }	Изменяет пользователей SNMP. Опциональные и/или необходимые параметры включают: • -i { *UserName* } создает новое имя пользователя, как указано, или изменяет параметры, связанные с указанным именем пользователя, если оно уже существует • -d { *UserName* } удаляет указанное имя пользователя • -c { *Community* } указывает строку доступа SNMP (для SNMPv1 или SNMPv2c). • -ip { *IP* } конфигурирует указанный IP-адрес, подлежащий использованию для аутентификации SNMP • -ap { *protocol* } конфигурирует аутентификацию SNMP с помощью указанного протокола аутентификации. Допустимые значения: noAuth, HMACMD5 или HMACSHA. • -ak { *key* } устанавливает секретный ключ (из 0 или 6+ символов), подлежащий использованию для аутентификации SNMP • -pp { *protocol* } конфигурирует шифрование данных через указанный протокол конфиденциальности. Допустимые значения: noPriv или CBC-DES. • -ak { *key* } устанавливает секретный ключ (из 0 или 6+ символов), подлежащий использованию для шифрования данных	Admin (Администратор)
svcmod -s { *radius* } { -ip { *1* } | -ip { *2* } } -ip { *IP* } -ak { *AuthKey* } -pt { *Port* } -ux { *UsernameExtension* } -mr { *MaxRetries* } -to { *timeout* }	Изменяет сервер защиты RADIUS. Опциональные и/или необходимые параметры включают: • -ip { *1* } устанавливает указанный сервер в качестве основного сервера RADIUS • -ip { *2* } устанавливает указанный сервер в качестве резервного сервера RADIUS • -ip { *2* } -ip удаляет основной сервер RADIUS • -ip { *1* } -ip удаляет резервный сервер RADIUS	Admin (Администратор)

Команда	Описание	Авторизованные пользователи
	• `-ip { IP }` указывает IP-адрес сервера RADIUS • `-ak { AuthKey }` указывает ключ аутентификации для совместного использования с сервером RADIUS • `-pt { Port }` указывает номер IP-порта на сервере RADIUS • `-ux { UsernameExtension }` определяет аффикс, добавляемый при отправке имени пользователя на сервер RADIUS для аутентификации. Значения могут включать предопределенные ключевые слова (заключенные в ограничители %) или определенные пользователем строки. Предопределенные ключевые слова: %Username % (имя, связанное с профилем пользователя), %IPaddr% (административный IP-адрес сервера сетевого доступа), %SysName% (системное имя, назначенное устройству) и %SysLocation% (физическое расположение устройства). • `-mr { MaxRetries }` указывает максимальное количество попыток аутентификатора аутентифицировать пользователя в случае какой-либо ошибки. При превышении указанного значения происходит сбой аутентификации. • `-to { timeout }` указывает сколько миллисекунд (мс) аутентификатор будет ждать ответа от сервера RADUS перед повторной попыткой аутентификации.	
svcmod `-s { tacacsplus } { -ip { 1 } | -ip { 2 } } -ip { IP } -ak { AuthKey } -pt { Port } -ux { UsernameExtension } -mr { MaxRetries } -to { timeout } -apl { AdminPrivilege } -opl { OperPrivilege } -gpl { GuestPrivilege }`	Изменяет сервер защиты TACACS+. Опциональные и/или необходимые параметры включают: • `-ip { 1 }` устанавливает указанный сервер в качестве основного сервера TACACS • `-ip { 2 }` устанавливает указанный сервер в качестве резервного сервера TACACS+ • `-ip { 2 } -ip` удаляет основной сервер TACACS+ • `-ip { 1 } -ip` удаляет резервный сервер TACACS+ • `-ip { IP }` указывает IP-адрес сервера TACACS+ • `-ak { AuthKey }` указывает ключ аутентификации для совместного использования с сервером TACACS+ • `-pt { Port }` указывает номер IP-порта на сервере TACACS+ • `-ux { UsernameExtension }` определяет аффикс, добавляемый при отправке имени пользователя на сервер TACACS+ для аутентификации. Значения могут включать предопределенные ключевые слова (заключенные в ограничители %) или определенные пользователем строки. Предопределенные ключевые слова: %Username % (имя, связанное с профилем пользователя), %IPaddr% (административный IP-адрес сервера сетевого доступа), %SysName% (системное имя, назначенное устройству) и %SysLocation% (физическое расположение устройства). • `-mr { MaxRetries }` указывает максимальное количество попыток аутентификатора	Admin (Администратор)

Команда	Описание	Авторизованные пользователи
	аутентифицировать пользователя в случае какой-либо ошибки. При превышении указанного значения происходит сбой аутентификации. • `-to { timeout }` указывает сколько миллисекунд (мс) аутентификатор будет ждать ответа от сервера TACACS+ перед повторной попыткой аутентификации. • `-apl { AdminPrivilege }` указывает уровень, до которого административные пользователи могут конфигурировать сервер TACACS+. Значения должны соответствовать одной или нескольким опциям, численно определенным (от 0 до 15) в файле конфигурации TACACS+. • `-opl { OperPrivilege }` указывает уровень, до которого пользователи могут конфигурировать сервер TACACS+. Значения должны соответствовать одной или нескольким опциям, численно определенным (от 0 до 15) в файле конфигурации TACACS+. • `-gpl { GuestPrivilege }` указывает уровень, до которого гостевые пользователи могут конфигурировать сервер TACACS+. Значения должны соответствовать одной или нескольким опциям, численно определенным (от 0 до 15) в файле конфигурации TACACS+.	
telnet { *dest* }	Запускает сеанс Telnet. Нажмите **Ctrl-C**, чтобы завершить сеанс. Опциональные и/или необходимые параметры включают: • { *dest* } — IP-адрес сервера	Guest (Гость), Operator (Оператор), Admin (Администратор)
tftp { *address* } [put | get] { *source* } { *target* }	Запускает сеанс TFTP. Нажмите **Ctrl-C**, чтобы завершить сеанс. Опциональные и/или необходимые параметры включают: • { *address* } — IP-адрес удаленного сервера TFTP • `put` указывает, что TFTP будет выгружать исходный файл для замены файла назначения • `get` указывает, что TFTP будет загружать исходный файл для замены файла назначения • { *source* } - имя исходного файла • { *target* } - имя файла, который будет заменен	Admin (Администратор)
trace	Запускает трассировку событий. Выполните команду **trace ?** для получения дополнительной справочной информации.	Operator (Оператор), Admin (Администратор)
type { *filename* }	Показывает содержимое текстового файла. Опциональные и/или необходимые параметры включают: • { *filename* } - имя файла для чтения	Guest (Гость), Operator (Оператор), Admin (Администратор)
usermod { -b | -r { *username* } |	Набор команд для отображения удаления и изменения существующих имен пользователей.	Admin (Администратор)

Команда	Описание	Авторизованные пользователи
`{ old_user_name } { new_user_name } }`	Опциональные и/или необходимые параметры включают: • `-b` просматривает существующие имена пользователей в RUGGEDCOM ROS. • `-r { username }` удаляет указанное имя пользователя для отключения учетной записи • { *old_user_name* } и { *new_user_name* } определяет имя пользователя, подлежащее изменению Данная команда недоступна в сеансах Telnet.	
version	Распечатывает версию программного обеспечения.	Guest (Гость), Operator (Оператор), Admin (Администратор)
xmodem `{ send | receive } { filename }`	Открывает сеанс XModem. Опциональные и/или необходимые параметры включают: • `send` отправляет файл клиенту. • `receive` получает файл от клиента. • { *filename* } - имя файла для чтения.	Operator (Оператор), Admin (Администратор)

2.5.2 Трассировка событий

CLI-команда трассировки предусматривает средства для прослеживания работы различных протоколов, поддерживаемых устройством. Трассировка обеспечивает подробную информацию, включая отображение результатов декодирования STP-пакетов, активности IGMP-протокола и MAC-адресов.

Примечание
Трассировка предназначена для того, чтобы предоставлять подробную информацию опытным пользователям. Следует иметь в виду, что любая трассировка отключена при начальном запуске устройства.

Порядок выполнения трассировки события:

1. Войдите в систему устройства в качестве администратора и перейдите в командную оболочку CLI. Для получения дополнительной информации о порядке доступа к командной оболочке CLI см. "Использование интерфейса командной строки (Страница 27)".

2. Определите протоколы и доступные связанные опции путем ввода:

   trace ?

   Если необходима опция, такая как `alloff` или `allon`, определите какие опции доступны для желаемого протокола, введя с клавиатуры:

   trace { *protocol* } ?

   Примечание
   Если необходимо, расширьте объем трассировки путем связывания протоколов и соответствующих им опций вместе с помощью вертикальной линии (|).

3. Выберите тип трассировки, введя с клавиатуры:

   trace { *protocol* } { *option* }

   где:

   - { *protocol* } — протокол для трассировки
   - { *option* } — опция для использования во время трассировки

   Пример:

   ```
   >trace transport allon
                        TRANSPORT: Logging is enabled
   ```

4. Начните трассировку, введя с клавиатуры:

   trace

2.5.3 Удаленное исполнение команд через RSH

Функцию удаленной командной оболочки (Remote Shell, RSH) можно использовать с рабочей станции, чтобы устройство выполняло команды таким же образом, как если бы они вводились по приглашению Command Line Interface (CLI — интерфейс командной строки). Синтаксис команды RSH обычно имеет следующий вид:

rsh { *ipaddr* } -l { *auth_token* } { *command_string* }

где:

- { *ipaddr* } — адрес или преобразованное имя устройства.
- { *auth_token* } — имя пользователя (guest (гость), operator (обычный пользователь, оператор) или admin (администратор)) и соответствующий пароль, разделенные запятой. Например, *admin,secret*.
- { *command_string* } — CLI-команда RUGGEDCOM ROS для выполнения.

Примечание
Выбранный уровень доступа (соответствует имени пользователя) должен поддерживать данную команду.

Примечание
Все выходные данные команды будут возвращены на рабочую станцию, передавшую команду. Нельзя использовать команды, которые запускают интерактивные диалоги (например, **`trace`**).

2.5.4 Использование команд SQL

В RUGGEDCOM ROS предусмотрен *SQL-подобный* командный процессор, который позволяет опытным пользователям выполнять некоторые операции, которые невозможны в традиционном веб- или CLI-интерфейсе. Например:

- Восстановление заводских значений по умолчанию для содержания определенной таблицы, но не конфигурации в целом.
- Поиск таблиц в базе данных для определенных конфигураций.
- Внесение в таблицы изменений, обусловленных существующими конфигурациями.

В комбинации с RSH команды SQL обеспечивают средства, позволяющие запрашивать и конфигурировать большое число устройств из одного центра.

Примечание
Перечень всех параметров, доступных по команде **`sql`** см. в"Доступные CLI-команды (Страница 27)".

Примечание
Права чтения/записи для таблиц, содержащих пароли или совместно используемую секретную информацию, недоступны с помощью команд SQL.

2.5.4.1 Поиск нужной таблицы

Многие SQL-команды работают с конкретными таблицами в базе данных и требуют указывать имя таблицы. После перехода в системе меню к требуемому меню и нажатия комбинации клавиш **Ctrl-Z** будет показано имя таблицы. Будут приведены имя меню и соответствующее ему имя таблицы в базе данных.

Другим способом получить имя таблицы является запуск следующей команды:

```
sql info tables
```

Эта команда также показывает имена меню и соответствующие им имена таблиц в базе данных, в зависимости от поддерживаемых устройством функций. Например:

```
Table Description
```

```
--------------------------------------------------------------------------------
alarms Alarms
cpuDiags CPU Diagnostics
ethPortCfg Port Parameters
ethPortStats Ethernet Statistics
ethPortStatus Port Status
ipCfg IP Services
```

2.5.4.2 Извлечение информации

В данном разделе рассматриваются различные методы извлечения информации о таблицах и параметрах.

Извлечение информации из таблицы

Используйте следующие команды для отображения сводной информации о параметрах в таблице, а также об их значениях:

sql select from { *table* }

где:

- { *table* } — имя таблицы

Пример:

```
>sql select from ipAddrtable

IP Address      Subnet          IfIndex    IfStats    IfTime     IfName
172.30.146.88   255.255.224.0   1001       17007888   2994       vlan1

1 records selected
```

Извлечение информации о параметре из таблицы

Используйте следующую команду для извлечения информации о конкретном параметре из таблицы:

Примечание
Имя параметра должно быть таким же, как отображаемое в системе меню, если только имя не содержит пробелы (например, ip-адрес). Пробелы необходимо заменять на нижние подчеркивания (например, ip_address). Другой вариант: имя параметра необходимо заключить в двойные кавычки (например, "ip address").

sql select { *parameter* } from { *table* }

где:

- { *parameter* } — имя параметра
- { *table* } — имя таблицы

Пример:

```
>sql select "ip address" from ipSwitchIfCfg
```

```
IP Address
192.168.0.1

1 records selected
```

Извлечение информации из таблицы с помощью оператора Where

Используйте следующую команду для отображения конкретных параметров из таблицы, имеющей особое значение:

sql select from { *table* } where { *parameter* } = { *value* }

где:

- { *table* } — имя таблицы
- { *parameter* } — имя параметра
- { *value* } — значение параметра

Пример:

```
>sql select from ethportcfg where media = 1000T

Port Name            ifName          Media       State    AutoN Speed Dupx  FlowCtrl
 LFI Alarm
   1  Port 1          1             1000T       Enabled  On    Auto  Auto  Off
 Off On
   2  Port 2          2             1000T       Enabled  On    Auto  Auto  Off
 Off On
   3  Port 3          3             1000T       Enabled  On    Auto  Auto  Off
 Off On
   4  Port 4          4             1000T       Enabled  On    Auto  Auto  Off
 Off On

4 records selected
```

Дополните уточните результаты с помощью операторов and или or:

sql select from { *table* } where { *parameter* } = { *value* } { and | or } { *parameter* } = { *value* }

где:

- { *table* } — имя таблицы
- { *parameter* } — имя параметра
- { *value* } — значение параметра

Пример:

```
>sql select from ethportcfg where media = 1000T and State = enabled

Port Name            ifName          Media       State    AutoN Speed Dupx  FlowCtrl
 LFI Alarm
   1  Port 1          1             1000T       Enabled  On    Auto  Auto  Off
 Off on
   2  Port 2          2             1000T       Enabled  On    Auto  Auto  Off
 Off On
   3  Port 3          3             1000T       Enabled  On    Auto  Auto  Off
 Off On
   4  Port 4          4             1000T       Enabled  On    Auto  Auto  Off
 Off On
```

```
4 records selected
```

2.5.4.3 Изменение значений в таблице

Используйте следующую команду для изменения значения параметров в таблице:

sql update { *table* } set { *parameter* } = { *value* }

где:

- { *table* } — имя таблицы
- { *parameter* } — имя параметра
- { *value* } — значение параметра

Пример:

```
>sql update iplcfg set IP_Address_Type = static
1 records updated
```

Условия также можно включить в команду, чтобы применить изменения только к параметрам, которые соответствуют конкретным требованиям. В приведенном ниже примере управление потоками информации включено на портах, которые работают со скоростью 100 Мбит/с в полнодуплексном режиме с отключенным управлением потоками:

```
>sql update ethportcfg set FlowCtrl = Off where ( Media = 100TX and FlowCtrl = On )
2 records updated
```

2.5.4.4 Сброс таблицы

Используйте следующую команду для сброса таблицы к заводским настройкам по умолчанию:

sql default into { *table* }

где:

- { *table* } — имя таблицы

2.5.4.5 Использование RSH и SQL

Комбинирование сценариев удаленной командной оболочки и команд SQL обеспечивает средства, позволяющие опрашивать и администрировать большое число устройств. С помощью этого метода может быть проверена однородность конфигурации по узлам сети. Ниже представлен простой пример, когда опрашиваемые устройства извлекаются из файла `Devices`:

```
C:> type Devices
10.0.1.1
10.0.1.2
```

```
C:\> for /F %i in (devices) do rsh %i -l admin,admin sql select from ipAddrtable

C:\>rsh 10.0.1.1 -l admin,admin sql select from ipAddrtable

IP Address      Subnet          IfIndex    IfStats    IfTime     IfName
192.168.0.31    255.255.255.0   1001       274409096  2218       vlan1

1 records selected

C:\>rsh 10.0.1.2 -l admin,admin sql select from ipAddrtable
0 records selected
C:\
```

2.6 Определение выборки портов в RUGGEDCOM ROS

Многие функции в операционной системе ROS можно сконфигурировать для одного и более портов на устройстве. Ниже описывается как указать один порт, несколько портов, все порты.

Выберите один порт, указав номер порта:

2

Выберите диапазон портов, используя знак дефиса (-) между первым и последним портами в списке:

1-4

Выберите несколько портов, определив перечень с разделителем в виде запятой:

1,4,6,9

Используйте опцию `All` для выбора всех портов устройства или, если доступно, опцию `None`, чтобы не выбрать ни один из портов.

2.7 Администрирование файловой системы на флеш-диске

В данном разделе рассматривается управление файловой системой.

2.7.1 Просмотр списка файлов флеш-памяти

Чтобы просмотреть список файлов, хранящихся в данный момент на флеш-памяти, сделайте следующее:

1. Войдите в систему устройства в качестве администратора и перейдите в командную оболочку CLI. Для получения дополнительной информации о порядке доступа к командной оболочке CLI см. "Использование интерфейса командной строки (Страница 27)".
2. Введите **`flashfiles`**. Отобразится список файлов, которые в данный момент находятся на флеш-памяти, а также их расположение и размер занимаемой ими памяти. Например:

```
>flashfiles
------------------------------------------------------------------
Filename                      Base          Size
------------------------------------------------------------------
main.bin                   0xFE959AE0   0x002C5493 (2905235)
syslog.txt                 0xFE100080   0x001BFF80 (1834880)
.
.
.

Free Space: 19792360
Used Space: 11664720
Fragmented Space: 5830423
------------------------------------------------------------------
```

2.7.2 Просмотр сведений о файле флеш-памяти

Чтобы просмотреть сведения о файле, хранящемся в данный момент на флеш-памяти, сделайте следующее:

1. Войдите в систему устройства в качестве администратора и перейдите в командную оболочку CLI. Для получения дополнительной информации о порядке доступа к командной оболочке CLI см. "Использование интерфейса командной строки (Страница 27)".
2. Отобразите информацию о файле, введя с клавиатуры:

   `flashfiles` `info { filename }`

   где:

   - `{ filename }` — имя файла, хранящегося во флеш-памяти

   Отображаются сведения, аналогичные указанным ниже.

```
>flashfiles info main.bin

Flash file information for main.bin:
Header version   : 4

            Platform         : ROS-MPC83
File name        : main.bin
Firmware version : v5.5.0
Build date       : Sep 27 2014 15:50
File length      : 2624659
Board IDs        :  3d
Header CRC       : 73b4
Header CRC Calc  : 73b4
Body CRC         : b441
Body CRC Calc    : b441
```

2.7.3 Дефрагментирование файловой системы на флеш-диске

Дефрагментация флеш-памяти осуществляется автоматически, когда отсутствует достаточное количество памяти для бинарного обновления. Однако фрагментация может произойти при любой выгрузке нового файла в блок. Из-за фрагментации секторы доступной памяти оказываются разделены

секторами, выделенными под файлы. В некоторых случаях доступной памяти может быть достаточно для бинарного обновления, но эта память может быть не доступна в одной сплошной области.

Чтобы выполнить дефрагментацию флеш-памяти, сделайте следующее:

1. Войдите в систему устройства в качестве администратора и перейдите в командную оболочку CLI. Для получения дополнительной информации о порядке доступа к командной оболочке CLI см. "Использование интерфейса командной строки (Страница 27)".
2. Выполните дефрагментацию флеш-памяти, введя:

   ```
   flashfiles defrag
   ```

2.8 Доступ к режиму BIST

Режим BIST (Built-In-Self-Test— встроенное самотестирование) используется техниками по обслуживанию для тестирования и конфигурирования внутренних функций устройства. Режим предназначен для использования только в целях поиска и устранения неисправностей.

⚠ ЗАМЕТКА

Механическая опасность — риск физического повреждения устройства

Чрезмерное использование функций режима BIST может привести к износу устройства, что в свою очередь может привести к аннулированию гарантии. Не используйте функции BIST, если иное не указано представителями службы технической поддержки Siemens.

Примечание
По умолчанию доступ к режиму BIST отключен. Все вводимые на консоли команды игнорируются, а пользователи автоматически направляются на интерфейс пользователя RUGGEDCOM ROS.

Чтобы впервые открыть доступ к режиму BIST, сделайте следующее:

1. С помощью ПК/ноутбука создайте файл с именем `bootoption.txt` и включите в него следующую строку:

   ```
   Security=no
   ```

2. Выгрузите файл на устройство, а затем перезагрузите устройство.

Примечание
Доступ к режиму BIST и загрузчику операционной системы позже можно отменить, изменив `no` на `yes`.

Чтобы получить доступ к режиму BIST, сделайте следующее:

⚠ ЗАМЕТКА

Опасность для конфигурации — риск нарушения обмена данными

Не подключайте устройство к сети, когда оно находится в режиме BIST. В этом режиме устройство создает чрезмерный многоадресный трафик.

1. Отключите устройство от сети.
2. Подключитесь к RUGGEDCOM ROS через консольное USB-соединение RS-232 и приложение терминала. Для получения дополнительной информации см. "Подключение напрямую (Страница 51)".
3. Перезапустите устройство. Для получения дополнительной информации см. "Перезапуск устройства (Страница 108)".
4. При появлении соответствующего запроса во время загрузки нажмите **Ctrl-C**. Появится приглашение на ввод команды для BIST.

   >
5. Введите **`help`** для просмотра списка всех доступных опций в режиме BIST.

Другой вариант: к функциям BIST можно получить доступ через заводской режим. Для получения дополнительной информации о заводском режиме см. "Доступные CLI-команды (Страница 27)".

2.9 Управление доступом к интерфейсу загрузчика операционной системы

В приведенных ниже разделах описывается, как включить, отключить и получить доступ к интерфейсу загрузчика операционной системы RUGGEDCOM ROS.

Примечание
Доступ к интерфейсу загрузчика операционной системы по умолчанию отключен на заводе на всех устройствах RUGGEDCOM ROS версии v5.5 . Все вводимые на консоли команды игнорируются, а пользователи автоматически направляются на интерфейс пользователя RUGGEDCOM ROS.

Примечание
Siemens рекомендует отключить доступ к интерфейсу загрузчика после обновления с более ранней версии RUGGEDCOM ROS до RUGGEDCOM ROS версии v5.5. Для получения дополнительной информации об отключении загрузчика операционной системы см. "Включение/отключение доступа к интерфейсу загрузчика операционной системы (Страница 45)".

2.9.1 Включение/отключение доступа к интерфейсу загрузчика операционной системы

Чтобы включить или отключить доступ к интерфейсу загрузчика операционной системы, сделайте следующее:

Создайте файл bootoption.txt

Чтобы включить или отключить доступ к загрузчику операционной системы, на устройстве должен присутствовать файл `bootoption.txt`.

Если файл недоступен, сделайте следующее:

1. С помощью ПК/ноутбука создайте файл с именем `bootoption.txt`.

   ⚠ ЗАМЕТКА

   Если параметр *Security* отмечен символом решетки (#) или не существует в файле, он будет создан RUGGEDCOM ROS со значением по умолчанию после перезагрузки.

2. Включите в файл следующую строку:

   ```
   Security = [No | Yes]
   ```

   - *Security = No* включает доступ к загрузчику операционной системы.
   - *Security = Yes* отключает доступ к загрузчику операционной системы. Это значение по умолчанию.

3. Выгрузите файл на устройство, а затем перезагрузите устройство.

Включение загрузчика операционной систем

Чтобы включить доступ к загрузчику операционной системы, сделайте следующее:

1. Используя ПК/ноутбук перейдите к файлу `bootoption.txt`.
2. Найдите следующую строку и измените с

   ```
   Security = Yes
   ```

   на

   ```
   Security = No
   ```

3. Выгрузите файл на устройство, а затем перезагрузите устройство.

Выключение загрузчика операционной систем

Чтобы отключить доступ к загрузчику операционной системы, сделайте следующее:

1. Используя ПК/ноутбук перейдите к файлу `bootoption.txt`.
2. Найдите следующую строку и измените с

   ```
   Security = No
   ```

   на

   ```
   Security = Yes
   ```

3. Выгрузите файл на устройство, а затем перезагрузите устройство.

2.9.2 Доступ к интерфейсу загрузчика операционной системы

Чтобы получить доступ к интерфейсу загрузчика операционной системы, сделайте следующее:

1. Подключитесь к RUGGEDCOM ROS через консольное соединение RS-232 и приложение терминала. Для получения дополнительной информации см. "Подключение напрямую (Страница 51)".
2. Перезапустите устройство. Для получения дополнительной информации см. "Перезапуск устройства (Страница 108)".
3. Как только устройство начнет загружаться, нажмите **Ctrl-Z**. Появится приглашение на ввод команды для Uboot.

   ```
   =>
   ```
4. Введите **`help`** для просмотра списка всех доступных опций в Uboot.

2.9.3 Настройка источника загрузки

По умолчанию устройство загружается с собственной флеш-памяти. Однако RUGGEDCOM ROS при необходимости поддерживает также возможность загрузки с .

Чтобы выбрать источник загрузки, сделайте следующее:

⚠ ЗАМЕТКА

Чтобы разрешить загрузку с CLP, необходимо включить автоматический доступ к съемным запоминающим устройствам. Для получения дополнительной информации см. "Включение/отключение автоматического доступа к съемному запоминающему устройству (Страница 48)".

1. С помощью ПК/ноутбука создайте файл с именем `bootoption.txt`.

   ⚠ ЗАМЕТКА

   Если параметр *BootOrderFirstRemovable* отмечен символом решетки (#) или не существует в файле, он будет создан RUGGEDCOM ROS со значением по умолчанию после перезагрузки.

2. Включите в файл следующую строку:

   ```
   BootOrderFirstRemovable = [No | Yes]
   ```

   - *BootOrderFirstRemovable = No* — выполняет загрузку с внутренней флеш-памяти. Это значение по умолчанию.
   - *BootOrderFirstRemovable = Yes* выполняет загрузку с CLP.
3. Выгрузите файл на устройство, а затем перезагрузите устройство.

2.10 Включение/отключение автоматического доступа к съемному запоминающему устройству

RUGGEDCOM ROS может автоматически синхронизировать микропрограммное обеспечение, конфигурацию и файлы журнала между устройством и используемыми им картами памяти CLP RUGGEDCOM ROS.

⚠ ЗАМЕТКА

Угроза безопасности — риск неавторизованного доступа и/или использования

Если он не требуется, автоматический доступ к съемным запоминающим устройствам должен быть отключен.

Чтобы сконфигурировать автоматический доступ к съемному носителю, сделайте следующее:

1. С помощью ПК/ноутбука создайте файл с именем `bootoption.txt`.

   ⚠ ЗАМЕТКА

   Если параметр *DisableAutoAccessRemovable* отмечен символом решетки (#) или не существует в файле, он будет создан RUGGEDCOM ROS со значением по умолчанию после перезагрузки.

2. Чтобы отключить автоматический доступ к съемному носителю, добавьте в файл следующую строку:

   ```
   DisableAutoAccessRemovable = Yes
   ```

   Примечание
   Команда **`DisableAutoAccessRemovable`** влияет только на автоматические действия. Даже если автоматический доступ к съемному носителю отключен, пользователи могут вручную копировать файлы с устройства на CLP и наоборот.

3. Чтобы заново включить автоматический доступ к съемному носителю, добавьте в файл следующую строку:

   ```
   DisableAutoAccessRemovable = No.
   ```

   Нет — значение по умолчанию.

4. Выгрузите файл на устройство.
5. Перезагрузите устройство.

2.11 Включение/отключение консольной службы

Локальная консольная служба в RUGGEDCOM ROS по умолчанию включена. Для обеспечения дополнительной безопасности пользователь-администратор по

желанию может отключить и повторно включить доступ к последовательной консоли .

Примечание
Включение/отключение консольной службы доступно только с помощью команд SQL. Для получения дополнительной информации см. "Использование команд SQL (Страница 38)".

Чтобы включить/отключить доступ к консольной службе, сделайте следующее:

1. Войдите в систему устройства в качестве администратора и перейдите в командную оболочку CLI. Для получения дополнительной информации о порядке доступа к командной оболочке CLI см. "Использование интерфейса командной строки (Страница 27)".
2. Включите или отключите консольную службу, введя:

   Включение

   ```
   sql update consoleServices SET Local Console Service =
   Enabled
   ```

   Отключение

   ```
   sql update consoleServices SET Local Console Service =
   Disabled
   ```

Изменения вступят в силу немедленно при следующем входе в локальную консоль.

3 Начало работы

В данном разделе приведено описание задач по запуску во время первоначального ввода устройства в эксплуатацию. Эти задачи включают подключение к устройству и доступ к RUGGEDCOM ROS, а также конфигурирование основной сети.

⚠ ЗАМЕТКА

Угроза безопасности — риск неавторизованного доступа и/или использования

Siemens рекомендует выполнить следующие действия перед вводом устройства в эксплуатацию:

- Заменить заводской самоподписанный сертификат SSL на сертификат, подписанный доверенным центром сертификации (CA)
- Сконфигурировать клиент SSH на использование *diffie-hellman-group14-sha1* или лучше

3.1 Подключение к операционной системе ROS

В данном разделе приведено описание различных методов подключения к устройству.

3.1.1 IP-адрес по умолчанию

IP-адрес устройства по умолчанию: 192.168.0.1/24.

3.1.2 Подключение напрямую

Доступ к RUGGEDCOM ROS для управления, а также поиска и устранения проблем можно осуществить напрямую через , или-соединения. Консольное соединение обеспечивает доступ к консольному интерфейсу и CLI.

Для дополнительной безопасности консольную службу можно отключить. Для получения дополнительной информации об отключении консольной службы см. "Включение/отключение консольной службы (Страница 48)".

Использование консольного порта для

Чтобы установить консольное соединение с устройством, сделайте следующее:

3.1.3 Удаленное подключение

Безопасный и удаленный доступ к RUGGEDCOM ROS можно получить через веб-браузер, терминал или рабочую станцию с ПО эмуляции терминала.

Использование веб-браузера

Веб-браузеры обеспечивают безопасное подключение к веб-интерфейсу для использования RUGGEDCOM ROS метода связи SSL (уровень защищенных сокетов). SSL шифрует трафик, которым обменивается со своими клиентами.

Веб-сервер RUGGEDCOM ROS гарантирует, что весь обмен информацией с клиентом являются конфиденциальным. Если клиент запрашивает доступ через небезопасный HTTP-порт, клиент автоматически перенаправляется на безопасный порт. Доступ к веб-серверу через SSL будет обеспечиваться только для тех клиентов, которые предоставляют действительное имя пользователя и пароль.

Чтобы установить соединение через веб-браузер, сделайте следующее:

1. На рабочей станции, используемой для доступа к устройству, настройте Ethernet-порт для использования IP-адреса в подсети устройства. IP-адрес по умолчанию: 192.168.0.1/24.

   Например, чтобы сконфигурировать устройство для подключения к одному из доступных Ethernet-портов, назначьте IP-адрес Ethernet-порту на рабочей станции в диапазоне от 192.168.0.3 до 192.168.0.254.

2. Откройте веб-браузер. Список рекомендуемых веб-браузеров см. в "Системные требования (Страница xviii)".

   ⚠ ЗАМЕТКА

   При подключении к устройству некоторые веб-браузеры могут сообщить, что сертификат веб-сервера не может быть проверен по каким-либо известным сертификатам. Это ожидаемое поведение, и можно безопасно дать указание браузеру принять сертификат. Как только сертификат будет принят, обмен данными с веб-сервером через этот браузер будет безопасным.

   ⚠ ЗАМЕТКА

   Адреса IPv6 должны быть заключены в квадратные скобки (например, **https://[2001:db8:123::2228]**).

3. В адресной строке введите IP-адрес подключенного к сети порта. Например, чтобы получить доступ к устройству, используя его IP-адрес

по умолчанию, введите **`https://192.168.0.1`** и нажмите **Enter**. После установления соединения появится экран входа в веб-интерфейс.

Для получения дополнительной информации о входе в систему устройства см. "Вход в систему (Страница 22)". Для получения дополнительной информации о веб-интерфейсе см. "Использование веб-интерфейса (Страница 24)".

Использование оконечного устройства или программного обеспечения эмуляции оконечного устройства

Оконечное устройство или компьютер с программным обеспечением эмуляции оконечного устройства обеспечивают доступ к консольному интерфейсу для RUGGEDCOM ROS через сервисы Telnet, RSH (Remote Shell) или SSH (Secure Shell).

Примечание
IP-сервисы можно ограничить в целях регулирования доступа к устройству. Для получения дополнительной информации см. "Конфигурирование IP-сервисов (Страница 96)".

Чтобы установить соединение через оконечное устройство или программное обеспечение эмуляции оконечного устройства, сделайте следующее:

1. Выберите сервис (например, Telnet, RSH или SSH).
2. Введите IP-адрес подключенного к сети порта.
3. Подключите устройство. После установки соединения появляется форма входа в систему. Для получения дополнительной информации о входе в систему устройства см. "Вход в систему (Страница 22)".

3.2 Установка USB-драйвера последовательной консоли RUGGEDCOM (только Windows)

На рабочих станциях под управлением ОС Microsoft Windows должен быть установлен USB-драйвер последовательной консоли RUGGEDCOM перед подключением к консольному интерфейсу через порт последовательной консоли USB Type-B. Этот драйвер можно получить у Службы поддержки клиентов Siemens.

Чтобы установить USB-драйвер последовательной консоли RUGGEDCOM вручную, сделайте следующее:

1. Получите установочный пакет у Службы поддержки клиентов Siemens. Для получения дополнительной информации об обращении в Службу поддержки клиентов см. "Клиентская поддержка (Страница xviii)".
2. Удалите с рабочей станции все ранее установленные драйверы "USB-последовательная передача данных".

3. Убедитесь, что USB-порт последовательной консоли не подключен к рабочей станции.
4. Дважды щелкните `Setup.exe`. Появится мастер установки.
5. Следуйте инструкциям на экране, чтобы установить драйвер.
6. Подключите рабочую станцию к устройству с помощью кабеля USB Standard-A к Standard-B.
7. Откройте Device Manager (Диспетчер устройств): нажмите кнопку **Start**, щелкните **Control Panel**, затем нажмите **System and Security**, а затем в **System** щелкните **Device Manager**.
8. Убедитесь, что порты распознаны в **Ports (COM & LPT)**.

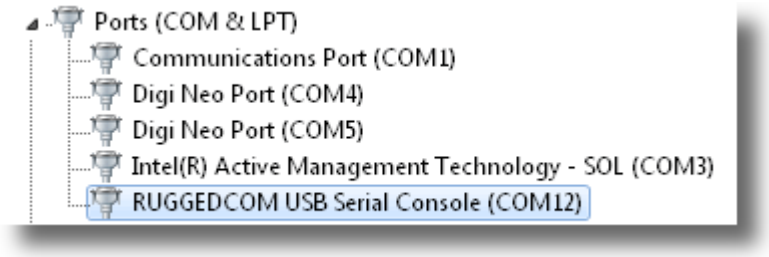


Рисунок 3.1 Порт последовательной консоли RUGGEDCOM

3.3 Конфигурирование основной сети

Чтобы сконфигурировать основную сеть, сделайте следующее:

1. Подключите компьютер к одному из портов коммутатора и сконфигурируйте компьютер таким образом, чтобы он находился в той же подсети, что и порт.
2. Сконфигурируйте компьютер на использование адреса VLAN1 в качестве шлюза по умолчанию.
3. Подключите второй компьютер к другому порту того же коммутатора и сконфигурируйте компьютер таким образом, чтобы он находился в той же подсети, что и порт.
4. Сконфигурируйте второй компьютер на использование адреса VLAN1 в качестве шлюза по умолчанию. IP-адрес по умолчанию: 192.168.0.1.
5. Убедитесь, что оба подключенных к устройству компьютера могут отправлять друг другу ping-запросы.

4 Управление устройством

В данном разделе описывается как конфигурировать и управлять устройством и его компонентами, такими как модульные интерфейсы, системные журналы и файлы.

4.1 Просмотр информации об изделии

Во время поиска и устранения неисправностей и при заказе нового устройства сотрудники Siemens могут запрашивать специальную информацию, такую как модель, код заказа или серийный номер.

Чтобы просмотреть информацию об устройстве, перейдите в ***Diagnostics » View Product Information***. Появится форма **Product Information**.

На экране отображается следующая информация:

Параметр	Описание
`MAC Address`	**Краткий обзор:** ##-##-##-##-##-## where ## ranges 0 to FF Показывает уникальный MAC-адрес устройства.
`Order Code`	**Краткий обзор:** Строка длиной 57 символа(ов) Показывает код заказа данного устройства.
`Classification`	**Краткий обзор:** Строка длиной 15 символа(ов) Обеспечивает классификацию системы. Значение `Controlled (Контролируемое)` указывает, что основное микропрограммное обеспечение представляет собой контролируемую версию операционной системы. Значение `Non-Controlled (Неконтролируемое)` указывает, что основное микропрограммное обеспечение представляет собой неконтролируемую версию. `Controlled (Контролируемое)` основное микропрограммное обеспечение может работать на контролируемых устройствах, но не может работать на не контролируемых устройствах. `Non-Controlled (Неконтролируемое)` основное микропрограммное обеспечение может работать как на контролируемых устройствах, так и на не контролируемых устройствах.
`Serial Number`	**Краткий обзор:** Строка длиной 31 символа(ов) Показывает серийный номер устройства.
`Main Version`	**Краткий обзор:** Строка длиной 47 символа(ов) Показывает версию и дату сборки основного программного обеспечения операционной системы.

Параметр	Описание
`Hardware ID`	Показывает тип, номер по каталогу и аппаратную ревизию оборудования. Пример: RST916C, RST916Cv2
`Descr`	**Краткий обзор:** Строка длиной 57 символа(ов) Описание продукта основано на идентификаторе аппаратного обеспечения, коде заказа и классификации.

4.2 Просмотр диагностических сообщений процессора

Чтобы просмотреть диагностическую информацию ЦПУ, полезную для поиска и устранения неисправностей, перейдите в ***Diagnostics » View CPU Diagnostics***. Появится форма **CPU Diagnostics**.

На экране отображается следующая информация:

Параметр	Описание
`Running Time`	**Краткий обзор:** DDDD days, HH:MM:SS Продолжительность времени, в течение которого устройство находилось во включенном состоянии в последний раз.
`CPU Usage`	**Краткий обзор:** Целое число от 0.0 до 100.0 Процентная доля доступных циклов процессора, используемая для работы устройства по измерениям за последнюю секунду.
`RAM Total`	**Краткий обзор:** Целое число от 0 до 4294967295 Суммарное количество байтов оперативной памяти в системе.
`RAM Free`	**Краткий обзор:** Целое число от 0 до 4294967295 Суммарное количество байтов свободной оперативной памяти.
`RAM Low Watermark`	**Краткий обзор:** Целое число от 0 до 4294967295 Суммарное количество байтов оперативной памяти, которые не были использованы во время работы системы.
`Temperature`	**Краткий обзор:** Целое число от -32768 до 32767 Температуры платы процессора.
`Free Rx Bufs`	**Краткий обзор:** Целое число от 0 до 4294967295 Свободные буферы передачи (Rx).
`Free Tx Bufs`	**Краткий обзор:** Целое число от 0 до 4294967295 Свободные буферы приема (Tx).

4.3 Просмотр состояния источников питания

Чтобы просмотреть текущее состояние источников питания, перейдите в ***Diagnostics » Power Supply Status***. Появится таблица **Power Supply Status**.

В этой таблице отображается следующая информация:

Параметр	Описание
`ID`	**Краткий обзор:** Целое число от 1 до 2 Идентификатор блока питания.
`Voltage`	**Краткий обзор:** Целое число от 0 до 4294967295 Выходное напряжение в милливольтах.
`Current`	**Краткий обзор:** Целое число от 0 до 4294967295 Выходной ток в миллиамперах.
`Temperature`	**Краткий обзор:** Целое число от -32768 до 32767 Температура источника питания.
`InStatus`	**Краткий обзор:** [---- | Out of range | Good] Указывает, входит ли входное напряжение источника питания в диапазон. Для двойных источников питания пост. тока/пост. тока диапазон входного напряжения составляет от 36 до 72 В. Для двойных источников питания перем. тока/пост. тока диапазон входного напряжения переменного тока составляет от 85 до 264 В перем. тока, а для постоянного тока — от 95 до 300 В пост. тока.
`OutStatus`	**Краткий обзор:** [---- | Out of range | Good] Указывает, входит ли выходное напряжение источника питания в диапазон. Диапазон выходного напряжения: 12 В +/- 1%.
`Calibration`	**Краткий обзор:** [---- | Bad | Good] Указывает правильно ли откалиброван источник питания.

4.4 Восстановление заводских настроек по умолчанию

Настройки устройства можно полностью или частично вернуть к заводским. Исключение групп параметров из сброса к заводским настройкам, например, регулирующие базовые возможности соединения и относящиеся к управлению SNMP, может оказаться полезным, если необходимо сохранить обмен данными с устройством во время сброса.

Выборочный сброс конфигурации не затрагивает следующие группы параметров:

- IP-интерфейсы
- IP-шлюзы
- SNMP-пользователи

- Таблица соответствия групп пользователей моделям и уровням безопасности SNMP
- SNMP-доступ

Полный или выборочный сброс конфигурации также не затрагивает следующие группы параметров:

- Часовой пояс
- Сдвиг летнего времени
- Правило перехода на летнее время

Примечание
Менеджеры резервирования среды передачи (устройства MRM) или автоматические менеджеры резервирования среды передачи (устройства MRA) необходимо отключить физически или отключить кольцевой порт (разомкнуть кольцо MRP), иначе конфигурация по умолчанию может не восстановиться для следующих параметров:

- RSTP-параметры порта
- Глобальные параметры MRP
- Экземпляры MRP

Для получения дополнительной информации о кольцах MRP см. "Управление протоколом резервирования среды передачи (MRP) (Страница 253)".

Для получения дополнительной информации о конфигурировании параметров порта см. "Конфигурирование Ethernet-порта (Страница 76)".

Чтобы восстановить заводские настройки, сделайте следующее:

1. Перейдите в ***Diagnostics » Load Factory Defaults***. Появится форма **Load Factory Defaults**.
2. Необходимо сконфигурировать следующие параметры:

   Примечание
   Если идентификатор VLAN для административного IP-интерфейса не `1`, настройка **Defaults Choice** на `Selected` автоматически установит его на `1`.

Параметр	Описание
`Defaults Choice`	**Краткий обзор:** [None | Selected | All] Установка некоторых записей, например, интерфейса управления IP-интерфейсами, шлюза по умолчанию, настроек SNMP на значение по умолчанию приведет к тому, что коммутатор будет недоступен для приложений управления. Этот параметр позволяет пользователю принять решение: загрузить настройки по умолчанию только в выбранные таблицы, что сохранит конфигурацию таблиц, критичных для базовых приложений управления коммуникацией и коммутацией, либо принудительно привести все таблицы к настройкам по умолчанию.

3. Нажмите **Apply**.

4.5 Выгрузка/загрузка файлов

Существует несколько механизмов передачи файлов с устройства на хост-компьютер и наоборот:

- Xmodem с использованием оболочки CLI в сеансе консоли Telnet, SSH или RS-232
- TFTP-клиент с использованием оболочки CLI в сеансе консоли и удаленного TFTP-сервера
- TFTP-сервер от удаленного TFTP-клиента
- SFTP (защищенный протокол FTP через SSH) от удаленного SFTP-клиента
- RUGGEDCOM CLP

Примечание
Для автоматизации управления файлами на устройстве можно использовать сценарии. Однако в зависимости от размера целевого файла (или файлов) может потребоваться задержка между любой последовательной командой записи и чтения, поскольку файл мог быть не полностью сохранен до подачи команды на считывание. Рекомендуется общая задержка, равная пяти секундам, но следует провести тестирование для оптимизации задержки целевого файла (или файлов) и условий эксплуатации.

Примечание
Содержимое внутренней файловой системы зафиксировано. Создание новых файлов и директорий, а также удаление существующих файлов невозможно. Перезаписать можно только файлы, которые могут быть выгружены на устройство.

RUGGEDCOM ROS будет генерировать SNMP-ловушку и регистрировать сообщение в системном журнале для указания деталей передачи и состояния при передаче файлов на удаленный компьютер или внешний носитель или с них.

Файлы, которые могут быть загружены или выгружены, включают:

- `main.bin` — основной образ микропрограммы приложения RUGGEDCOM ROS
- `config.csv` — полная база данных конфигурации в виде текстового файла ASCII с разделителями-запятыми
- `factory.txt` — содержит MAC-адрес, артикул и серийный номер. Заводские данные должны быть подписаны.
- `banner.txt` — содержит текст, который появляется на экране входа в систему

- `ssl.crt` — SSL-сертификат. Содержит как файл SSL-сертификата, так и соответствующий файл секретного ключа RSA.
- `ssh.keys` — SSH-ключи для устройства

4.5.1 Выгрузка/загрузка файлов с помощью протокола XMODEM

Чтобы выгрузить или загрузить файл с использованием XMODEM, сделайте следующее:

Примечание
Для данного метода требуется хост-компьютер с эмулятором терминала или программное обеспечение Telnet, а также возможность передачи данных по протоколу XMODEM.

1. Установите соединение между устройством и хост-компьютером. Для получения дополнительной информации см. "Подключение к операционной системе ROS (Страница 51)".
2. Войдите в систему устройства в качестве администратора и перейдите в командную оболочку CLI. Для получения дополнительной информации о порядке доступа к командной оболочке CLI см. "Использование интерфейса командной строки (Страница 27)".
3. В командной строке CLI наберите:

   xmodem [send | receive] { *filename* }

   где:

   - `send` — отправляет файл хост-компьютеру
   - `receive` — извлекает файл из хост-компьютера
   - { *filename* } — имя файла (т. е. main.bin)

   Примечание
   Если в эмуляторе терминала или программном обеспечении Telnet доступен протокол *XModem 1K*, выберите для передачи данных его вместо стандартной опции *XModem*.

4. Когда устройство ответит, `Press Ctrl-X to cancel`, запустите передачу XMODEM с хост-компьютера. Устройство укажет, когда передача информации будет завершена.

   Примечание
   Если для установления соединения между устройством RST916C и хост-компьютером используется SSH, загрузка образа по протоколу XMODEM займет много времени.

   Ниже приведен пример командной оболочки CLI успешной передачи файла XMODEM:

   ```
   >xmodem receive main.bin
   Press Ctrl-X to cancel
   Receiving data now ...C
   Received 1428480 bytes. Closing file main.bin ...
   main.bin transferred successfully
   ```

5. Если файл выгрузился, перезапустите устройство. Для получения дополнительной информации см. "Перезапуск устройства (Страница 108)".

4.5.2 Выгрузка/загрузка файлов с помощью клиента TFTP

Чтобы выгрузить или загрузить файл с использованием клиента TFTP, сделайте следующее:

⚠ ЗАМЕТКА

Угроза безопасности — риск неавторизованного доступа и/или использования

В протоколе TFTP нет механизмов аутентификации. Любое использование клиента или сервера TFTP следует рассматривать как в высшей степени небезопасное.

Примечание
Для данного метода требуется TFTP-сервер, который доступен через сеть.

1. Определите IP-адрес компьютера, на котором выполняется TFTP-сервер.
2. Установите соединение между устройством и хост-компьютером. Для получения дополнительной информации см. "Подключение к операционной системе ROS (Страница 51)".
3. Войдите в систему устройства в качестве администратора и перейдите в командную оболочку CLI. Для получения дополнительной информации о порядке доступа к командной оболочке CLI см. "Использование интерфейса командной строки (Страница 27)".

4. В командной строке CLI наберите:

   `tftp` `{ address } [ get | put ] { source-filename } { destination-filename }`

   где:

   - `get` — копирует файлы с хост-компьютера на устройство
   - `put` — копирует файлы с устройства на хост-компьютер
   - `{ address }` — IP-адрес компьютера, на котором выполняется TFTP-сервер
   - `{ source-filename }` — имя файла для передачи
   - `{ destination-filename }` — имя файла (на устройстве или TFTP-сервере), который будет заменен во время передачи данных

   Ниже приведен пример успешной передачи файла TFTP-клиента:

   ```
   >tftp 10.0.0.1 get ROS-MPC83_Main_v5.5.0.bin main.bin
   TFTP CMD: main.bin transfer ok. Please wait, closing file ...
   TFTP CMD: main.bin loading successful.
   ```

5. Если файл выгрузился, перезапустите устройство. Для получения дополнительной информации см. "Перезапуск устройства (Страница 108)".

4.5.3 Выгрузка/загрузка файлов с помощью сервера TFTP

Чтобы выгрузить или загрузить файл с использованием TFTP-сервера, сделайте следующее:

⚠ ЗАМЕТКА

Угроза безопасности — риск неавторизованного доступа и/или использования

В протоколе TFTP нет механизмов аутентификации. Любое использование клиента или сервера TFTP следует рассматривать как в высшей степени небезопасное.

1. Установите соединение между устройством и хост-компьютером. Для получения дополнительной информации см. "Подключение к операционной системе ROS (Страница 51)".
2. Инициализируйте TFTP-сервер на устройстве и запустите передачу данных по протоколу TFTP. Сервер укажет, когда передача информации будет завершена.

   Ниже приведен пример успешного обмена данными с TFTP-сервером:

   ```
   C:\>tftp -i 10.1.0.1 put C:\files\ROS-MPC83_Main_v5.5.0.bin main.bin
       Transfer successful: 1428480 bytes in 4 seconds, 375617 bytes/s
   ```

3. Если файл выгрузился, перезапустите устройство. Для получения дополнительной информации см. "Перезапуск устройства (Страница 108)".

4.5.4 Выгрузка/загрузка файлов с помощью сервера SFTP

SFTP (Secure File Transfer Protocol) — это протокол защищенной передачи файлов, представляющий собой механизм передачи файлов, в котором используется SSH для шифрования каждого компонента передачи файла между сетевым клиентом и сервером.

Примечание
Устройство не имеет SFTP-клиента и, следовательно, может только принимать файлы по протоколу SFTP от внешнего источника. SFTP требует аутентификации для передачи файла.

Чтобы выгрузить или загрузить файл с использованием SFTP-сервера, сделайте следующее:

Примечание
Для данного метода требуется хост-компьютер, на котором установлено программное обеспечение SFTP-клиента.

1. Установите SFTP-соединение между устройством и хост-компьютером.
2. Запустите передачу данных по протоколу SFTP. Клиент укажет, когда передача данных будет завершена.

   Ниже приведен пример успешного обмена данными с SFTP-сервером:

   ```
   user@host$ sftp admin@ros_ip
   Connecting to ros_ip...
   admin@ros_ip's password:


   sftp>
   ```

3. Если файл выгрузился, перезапустите устройство. Для получения дополнительной информации см. "Перезапуск устройства (Страница 108)".

4.5.5 Выгрузка/загрузка файлов с помощью RUGGEDCOM CLP

Съемный носитель RUGGEDCOM можно использовать для передачи файлов между устройством, хост-компьютером и/или другим устройством для различных целей. Для получения дополнительной информации о съемном носителе CLP и его использовании см. "Съемное запоминающее устройство (Страница 18)".

Примечание
Для повышения безопасности храните файлы на зашифрованном носителе CLP. Для получения дополнительной информации о включении шифрования данных см. "Конфигурирование шифрования данных (Страница 123)".

⚠ ЗАМЕТКА

Опасность для конфигурации — риск нарушения обмена данными

Перед совместным использованием зашифрованного файла конфигурации с другим устройством необходимо убедиться, что оба устройства используют один пароль/одну парольную строку для расшифровки файлов конфигурации. Для получения дополнительной информации о включении шифрования данных см. "Конфигурирование шифрования данных (Страница 123)".

⚠ ЗАМЕТКА

Опасность для конфигурации — риск потери данных.

После выгрузки или загрузки файла необходимо подождать не менее 20 секунд перед извлечением CLP, чтобы обеспечить полную передачу данных.

Примечание
Файлы можно переименовать во время их передачи между CLP и устройством. Это может быть полезно при наличии нескольких версий бинарного файла микропрограммного обеспечения на CLP. Необходимую версию можно перенести на устройство и переименовать на `main.bin`, чтобы заменить версию, которая в данный момент присутствует на устройстве.

Чтобы выгрузить файл на устройство или загрузить файл с устройства, сделайте следующее:

1. Вставьте съемный носитель CLP в устройство. Для получения дополнительной информации см. "Руководство по установке" устройства.
2. Войдите в систему устройства в качестве администратора и перейдите в командную оболочку CLI. Для получения дополнительной информации о порядке доступа к командной оболочке CLI см. "Использование интерфейса командной строки (Страница 27)".
3. В командной строке CLI наберите:
   - **Выгрузка**

     copy `a:\{` *sourceFile* `}` `{` *destinationFile* `}`

   - **Загрузка**

     copy `{` *sourceFile* `}` `a:\{` *destinationFile* `}`
4. Если файл выгрузился, перезапустите устройство. Для получения дополнительной информации см. "Перезапуск устройства (Страница 108)".

4.6 Управление журналами

Файлы журналов фатальных сбоев (`crashlog.txt`) и системных журналов (`syslog.txt`) содержат историческую информацию о событиях, которые произошли во время работы устройства.

Журнал фатальных сбоев содержит отладочную информацию, связанную с проблемами, которые могут приводить к незапланированным перезапускам устройства или влиять на его работу. Размер файла 0 байт указывает на то, что подобных непредвиденных событий не происходило.

Системный журнал содержит запись важных событий, включая запуски, изменения конфигурации, обновления микропрограммного обеспечения и повторные инициализации баз данных в связи с добавлениями функциональных возможностей. Системный журнал будет накапливаться информация до его переполнения, пока он не будет содержать приблизительно 2 мегабайта данных.

Примечание
Файлы системных журналов, резервная копия которых создается на CLP содержат временные метки в формате: год, месяц и дата (например, syslog.txt.20140101). Это позволяет сохранить несколько файлов системных журналов на одной карте памяти.

4.6.1 Просмотр локальных и системных журналов

Локальные журналы фатальных сбоев и системные журналы можно загрузить с устройства и просмотреть в текстовом редакторе. Для получения дополнительной информации о загрузке файлов журналов см. "Выгрузка/загрузка файлов (Страница 59)".

Чтобы просмотреть системный журнал через веб-интерфейс, перейдите в ***Diagnostics » View System Log***. Появится форма **syslog.txt**.

4.6.2 Очистка локальных и системных журналов

Чтобы очистить как локальные протоколы фатальных событий, так и системные журналы, войдите в командную оболочку CLI и введите:

```
clearlogs
```

Чтобы очистить только локальный системный журнал, войдите в веб-интерфейс и сделайте следующее:

1. Перейдите в ***Diagnostics » Clear System Log***. Появится форма **Clear System Log**.
2. Нажмите **Confirm**.

4.6.3 Конфигурирование локального системного журнала

Чтобы сконфигурировать уровень серьезности для локального системного журнала, сделайте следующее:

Примечание
Для максимальной надежности используйте дистанционный вход в систему. Для получения дополнительной информации см. "Управление удаленной регистрацией (Страница 66)".

1. Перейдите в ***Administration » Configure Syslog » Configure Local Syslog***. Появится форма **Local Syslog**.
2. Необходимо сконфигурировать следующие параметры:

Параметр	Описание
`Local Syslog Level`	**Краткий обзор:** [EMERGENCY | ALERT | CRITICAL | ERROR | WARNING | NOTICE | INFORMATIONAL | DEBUGGING] **Значение по умолчанию:** INFORMATIONAL Серьезность сообщения, которое было создано. Нужно отметить, что выбранный уровень серьезности рассматривается как минимальный уровень серьезности для данной системы. Например, если выбран уровень ERROR (Ошибка), то система посылает все сообщения системного журнала, созданные с уровнем серьезности ERROR (Ошибка), CRITICAL (Критический), ALERT (Тревога) и EMERGENCY (Авария).

3. Нажмите **Apply**.

4.6.4 Управление удаленной регистрацией

Дополнительно к локальному системному журналу, который ведется на устройстве, можно сконфигурировать удаленный системный журнал, а также собрать важные сообщения о событиях. Syslog-клиент представляет собой резидентную программу на устройстве и поддерживает до 5 сборщиков (или Syslog-серверов).

Протокол удаленного системного журнала представляет собой транспорт на основе UDP/IP, позволяющий устройству посылать по IP-сетям сообщения с уведомлениями о событиях для сборщиков сообщений о событиях, которые также называются syslog-серверами (серверами системных журналов). Данный протокол предназначен для простого транспорта этих сообщений о событиях от генерирующего устройства к собирающему.

4.6.4.1 Форма системного журнала

RUGGEDCOM ROS поддерживает форматы системных журналов RFC 3164 и RFC 5424, используемые для передачи уведомлений о событиях.

Поскольку RFC 3164 был замещен RFC 5424, этот раздел посвящен формату RFC 5424.

Каждое сообщение удаленного системного журнала, совместимое с RFC 5424, разделено на три части следующим образом:

- Заголовок
- Структурированный элемент
- Сообщение

Заголовок

Заголовок сообщения включает следующие поля:

Рисунок 4.1 Поля заголовков сообщения

Область	Описание
PRI	Значение приоритета (PRIVAL) представляет собой как "категорию", так и "серьезность". PRIVAL = (Категория * 8) + Серьезность.
ВЕРСИЯ	Версия протокола системного журнала RFC 5424 (например, "1").
SP	Это поле используется для представления пространства ASCII.
TS	Метка времени в формате YYYY-MM-DDTHH-MM-SSuZ. Пример: "2020-10-06T20:14:47.476406-5:00" означает 6 октября 2020 года в 20:14:47, 476406 микросекунд на следующую секунду. Метка времени указывает, что местное время -5 часов от UTC.
HN	Имя хоста. Оно устанавливается для статического или динамического IP-адреса устройства (в зависимости от типа IP-адреса, выбранного пользователем во время конфигурации интерфейса). Если устройству не назначен динамический адрес, для обозначения поля используется NILVALUE (т.е. "-").
AN	APP-NAME. Для этого поля используется тип шасси устройства. Например, "RST916C".
PID	Идентификатор процесса
MID	Идентификатор сообщения

Структурированный элемент

Структурированный элемент состоит из имени и пар параметра-значения в формате "["SD-ID SP SD-PARAM) "]". Имя обозначается SD-ID. Пары параметра-значения обозначаются "SD-PARAM".

В RUGGEDCOM ROS информация о качестве времени отправляется с использованием SD-ID "timeQuality" и 2 пар параметра-значения:

- **tzKnown**: Указывает, знает ли отправитель свой часовой пояс. Поскольку RUGGEDCOM ROS совместим с часовым поясом, tzKnown всегда имеет значение "1".
- **isSynced**: Указывает, синхронизирован ли отправитель с надежным внешним источником времени. Значение "1" указывает, что в качестве источника времени выбраны вешние ведущие часы и достигнута синхронизация между ведущим и ведомым устройствами. Значение "0" указывает, что локальные часы выбраны в качестве источника времени.

Сообщение

Сообщение содержит сообщение в свободной форме с информацией о событии.

Примеры

Следующее сообщение указывает на то, что источник времени сконфигурирован на локальные часы:

```
<190>1 2020-10-08T23:48:57.582209-5:00 192.168.2.102 RSG2488 - - [timeQuality
  tzKnown="1" isSynced="0"] RemoteSyslog update collector 192.168.2.101
```

Следующее сообщение указывает, что источник времени сконфигурирован на внешние часы:

```
<190>1 2020-10-08T23:40:31.534206-5:00 192.168.2.102 RSG2488R - - [timeQuality
  tzKnown="1" isSynced="1"] RemoteSyslog update collector 192.168.2.101
```

Для получения дополнительной информации о конфигурировании формата системного журнала см. "Добавление удаленного Syslog-сервера (Страница 69)".

4.6.4.2 Конфигурирование удаленного Syslog-клиента

Чтобы сконфигурировать удаленный Syslog-клиент, сделайте следующее:

1. Перейдите в ***Administration » Configure Syslog » Configure Remote Syslog Client***. Появится форма **Remote Syslog Client**.
2. Необходимо сконфигурировать следующие параметры:

Параметр	Описание
`UDP Port`	**Краткий обзор:** Целое число от 1025 до 65535 или [514] **Значение по умолчанию:** 514 Локальный UDP-порт, через который клиент посылает информацию серверу (серверам).

3. Нажмите **Apply**.

4.6.4.3 Просмотр списка удаленных Syslog-серверов

Чтобы просмотреть список известных удаленных серверов системных журналов, перейдите в ***Administration » Configure Syslog » Configure Remote Syslog Server***. Появится таблица **Remote Syslog Server**.

Если удаленные Syslog-серверы не были сконфигурированы, добавьте серверы в соответствии с необходимостью. Для получения дополнительной информации см. "Добавление удаленного Syslog-сервера (Страница 69)".

4.6.4.4 Добавление удаленного Syslog-сервера

RUGGEDCOM ROS поддерживает до 5 удаленных Syslog-серверов (или сборщиков). Аналогично локальному системному журналу удаленный Syslog-сервер можно сконфигурировать на регистрацию информации при конкретном уровне серьезности. В журнал записываются только сообщения с уровнем серьезности, который равен сконфигурированному уровню серьезности или превышает его.

Чтобы добавить удаленный Syslog-сервер в список известных серверов, сделайте следующее:

1. Перейдите в ***Administration » Configure Syslog » Configure Remote Syslog Server***. Появится таблица **Remote Syslog Server**.
2. Нажмите **InsertRecord**. Появится форма **Remote Syslog Server**.
3. Необходимо сконфигурировать следующие параметры:

Параметр	Описание
`IP Address`	**Краткий обзор:** Any valid IP address IP-адрес syslog-сервера.
`UDP Port`	**Краткий обзор:** Целое число от 1025 до 65535 или [514] **Значение по умолчанию:** 514 Номер UDP-порта, на котором производит прослушивание удаленный сервер.
`Facility`	**Краткий обзор:** [USER | LOCAL0 | LOCAL1 | LOCAL2 | LOCAL3 | LOCAL4 | LOCAL5 | LOCAL6 | LOCAL7] **Значение по умолчанию:** LOCAL7 Компонент приложения или операционной системы, который формирует сообщение журнала. RUGGEDCOM ROS сопоставляет всю информацию системных журналов с одной категорией, настраиваемой пользователем.
`Severity`	**Краткий обзор:** [EMERGENCY | ALERT | CRITICAL | ERROR | WARNING | NOTICE | INFORMATIONAL | DEBUGGING] **Значение по умолчанию:** DEBUGGING Серьезность сообщения, которое было создано. Следует отметить, что выбранный пользователем уровень серьезности принимается в качестве минимального уровня серьезности для данной системы. Например, если выбран уровень ERROR (Ошибка), то система посылает все

Параметр	Описание
	сообщения системного журнала, созданные с уровнем серьезности ERROR (Ошибка), CRITICAL (Критический), ALERT (Тревога) и EMERGENCY (Авария).
`Format`	**Краткий обзор:** [RFC3164 | RFC5424] **Значение по умолчанию:** RFC3164 Формат сообщений системного журнала, которые отправляются на удаленный syslog-сервер.

4. Нажмите **Apply**.

4.6.4.5 Удаление удаленного Syslog-сервера

Чтобы удалить удаленный Syslog-сервер из списка известных серверов, сделайте следующее:

1. Перейдите в ***Administration » Configure Syslog » Configure Remote Syslog Server***. Появится таблица **Remote Syslog Server**.
2. Выберите сервер из таблицы. Появится форма **Remote Syslog Server**.
3. Нажмите **Delete**.

4.7 Управление Ethernet-портами

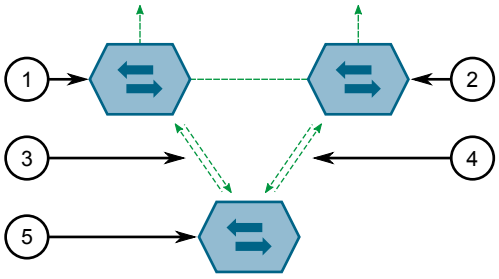
В данном разделе рассматривается управление Ethernet-портами.

Примечание
Информацию о конфигурировании дистанционного мониторинга для Ethernet-портов см. в "Управление дистанционным мониторингом (Страница 98)".

4.7.1 Защита контроллера с помощью Link Fault Indication (LFI — индикация отказа канала связи)

Современные промышленные контроллеры часто бывают оборудованы резервными Ethernet-портами, которые используются в случае отказа канала связи. Если в этих интерфейсах используется среда передачи данных (например, оптоволоконная), которая имеет раздельные тракты для передачи и приема, то такой интерфейс может быть уязвимым в случае возникновения физических повреждений только в одном из двух трактов.

Рассмотрим пример с двумя коммутаторами (A и B), подключенными к контроллеру. Коммутатор A подключен к основному порту контроллера, а коммутатор B подключен к резервному порту, который контроллер удерживает в неактивном состоянии, пока активен коммутатор A. Коммутатор B должен пересылать кадры в направлении контроллера через коммутатор A.



① Коммутатор A
② Коммутатор B
③ Основной тракт передачи
④ Резервный тракт передачи
⑤ Контроллер

Рисунок 4.2 Пример

Если происходит сбой тракта передачи от контроллер к коммутатору A, коммутатор A продолжает генерировать сигнал канала связи с контроллером через тракт приема. Контроллер продолжает видеть канал связи с коммутатором A и не переключается на резервный порт.

На рисунке показана необходимость в методе уведомления партнера по соединению о пропадании сигнала, подтверждающего целостность канала. Такой метод способ исходно существует в одних средах передачи данных, но отсутствует в других.

100Base-TX, 1000Base-T, 1000Base-X	Встроенная функция автоматического согласования (в передаваемом сигнале автоматического согласования устанавливается специальный флаг Remote Fault Indication (Удаленная индикация отказа)).
Каналы связи 100Base-FX	Индикация отказа на дальнем конце Far-End-Fault-Indication (FEFI) представляет собой стандартную функцию, определяемую стандартом IEEE 802.3 для каналов связи этого типа. Эта функция включает в себя следующее: • **Передача FEFI** Передача модифицированного сигнала целостности линии связи в случае обнаружения отказа канала связи (т. е. в том случае, когда сигнал наличия связи не принимается от партнера по соединению). • **Детектирование FEFI** Индикация потери связи в том случае, когда сигнал FEFI принимается от партнера по соединению.
Каналы связи 10Base-FL	Отсутствует стандартная поддержка.

Каналы связи 10Base-FL не имеют собственного механизма оповещения партнера по соединению. Кроме того, поддержка FEFI в каналах связи 100Base-FX является необязательной согласно стандарту IEEE 802.3, а это означает, что некоторые партнеры по соединению могут не обеспечивать такой поддержки.

Siemens предлагает расширенную функцию индикации отказа канала связи (LFI) для каналов связи, которые не имеют собственного механизма

оповещения партнера по соединению. Если функция LFI включена, то сигнал целостности линии связи генерируется устройством на основании приема сигнала связи. Если коммутатору A в приведенном ранее примере не удается принять сигнал наличия связи от контроллера, то он прекратит генерировать сигнал связи. Контроллер обнаружит отказ канала связи и переключится на резервный порт.

⚠ ЗАМЕТКА

Опасность для конфигурации — риск нарушения обмена данными

Если оба партнера по связи поддерживают функцию LFI, то она *не должна* быть включена на обеих сторонах канала связи. Если эта функция включена на обеих сторонах, то связь никогда не будет установлена, поскольку каждая сторона будет ждать передачи сигнала связи от партнера по соединению.

Коммутатор также можно настроить таким образом, чтобы он удалял записи для порта контроллера из таблицы MAC-адресов. Кадры, предназначенные для контроллера, будут передаваться на коммутатор B, откуда они будут пересылаться на контроллер (после того как контроллер передаст свой первый кадр).

4.7.2 Просмотр состояния Ethernet-портов

Чтобы просмотреть текущее состояние каждого Ethernet-порта, перейдите в ***Ethernet Ports » View Port Status***. Появится таблица **Port Status**.

В этой таблице отображается следующая информация:

Параметр	Описание
`Port`	**Краткий обзор:** 1 to maximum port number Номер порта.
`Name`	**Краткий обзор:** Строка длиной 15 символа(ов) Описательное имя, которое может использоваться для идентификации устройства, подключенного к этому порту.
`Link`	**Краткий обзор:** [---- | Down | Up] Состояние связи порта.
`Speed`	**Краткий обзор:** [--- | 10M | 100M | 1G | 10G] Текущая скорость передачи порта.
`Duplex`	**Краткий обзор:** [---- | Half | Full] Текущий дуплексный режим порта.

4.7.3 Вывод диагностики для всех Ethernet-портов

Чтобы просмотреть статистику для всех Ethernet-портов, перейдите в ***Ethernet Stats » View Ethernet Statistics***. Появится таблица **Ethernet Statistics**.

В этой таблице отображается следующая информация:

Параметр	Описание
`Port`	**Краткий обзор:** 1 to maximum port number Номер порта.
`State`	**Краткий обзор:** [---- | Down | Up] Коммуникационный статус порта.
`InOctets`	**Краткий обзор:** Целое число от 0 до 4294967295 Количество октетов в принятых и не содержащих ошибок пакетах (направленные+групповые+широковещательные) и отброшенных пакетах.
`OutOctets`	**Краткий обзор:** Целое число от 0 до 4294967295 Количество октетов в успешно переданных пакетах.
`InPkts`	**Краткий обзор:** Целое число от 0 до 4294967295 Количество принятых успешно переданных пакетов (направленные + групповые + широковещательные) и отброшенных пакетов.
`OutPkts`	**Краткий обзор:** Целое число от 0 до 4294967295 Количество успешно переданных пакетов.
`ErrorPkts`	**Краткий обзор:** Целое число от 0 до 4294967295 Количество и тип ошибочных пакетов.

4.7.4 Вывод диагностики для конкретных Ethernet-портов

Чтобы просмотреть статистику для конкретных Ethernet-портов, перейдите в ***Ethernet Stats » View Ethernet Port Statistics***. Появится таблица **Ethernet Port Statistics**.

В этой таблице отображается следующая информация:

Параметр	Описание
`Port`	**Краткий обзор:** 1 to maximum port number Номер порта.
`InOctets`	**Краткий обзор:** Целое число от 0 до 18446744073709551615 Количество октетов в принятых и не содержащих ошибок пакетах (направленные+групповые+широковещательные) и отброшенных пакетах.
`OutOctets`	**Краткий обзор:** Целое число от 0 до 18446744073709551615 Количество октетов в успешно переданных пакетах.
`InPkts`	**Краткий обзор:** Целое число от 0 до 18446744073709551615 Количество принятых успешно переданных пакетов (направленные + групповые + широковещательные) и отброшенных пакетов.

Параметр	Описание
`OutPkts`	**Краткий обзор:** Целое число от 0 до 18446744073709551615 Количество успешно переданных пакетов.
`TotalInOctets`	**Краткий обзор:** Целое число от 0 до 18446744073709551615 Суммарное количество октетов во всех принятых пакетах. Включает в себя октеты, отброшенные из-за ошибок, а также октеты в составе тех пакетов, которые были приняты но не были переданы в матрицу коммутации для дальнейшей обработки. Это число должно отражать все октеты данных, принятые по каналу связи.
`TotalInPkts`	**Краткий обзор:** Целое число от 0 до 18446744073709551615 Количество полученных пакетов. Включает в себя пакеты, отброшенные из-за ошибок, а также пакеты, которые были приняты, но не были переданы в матрицу коммутации для дальнейшей обработки. Это число должно отражать все пакеты, принятые по каналу связи.
`InBroadcasts`	**Краткий обзор:** Целое число от 0 до 18446744073709551615 Количество принятых широковещательных пакетов.
`InMulticasts`	**Краткий обзор:** Целое число от 0 до 18446744073709551615 Количество принятых групповых пакетов.
`CRCAlignErrors`	**Краткий обзор:** Целое число от 0 до 4294967295 Количество принятых пакетов, которые удовлетворяют следующим условиям: • Длина данных пакета данных находится в интервале от 64 до 1536 октетов включительно. • Циклический избыточный код (CRC) неправильный, то есть не соответствует содержимому пакета. • Событие коллизии не было обнаружено. • Событие поздней коллизии не было обнаружено.
`OversizePkts`	**Краткий обзор:** Целое число от 0 до 4294967295 Количество принятых пакетов, которые имеют длину данных больше 1536 октетов и правильный CRC.
`Fragments`	**Краткий обзор:** Целое число от 0 до 4294967295 Количество принятых пакетов, которые удовлетворяют следующим условиям: • Длина данных пакета меньше 64 октетов или пакета без SFD и меньше 64 октетов. • Событие коллизии не было обнаружено. • Событие поздней коллизии не было обнаружено. • Циклический избыточный код (CRC) неправильный, то есть не соответствует содержимому пакета.
`Jabbers`	**Краткий обзор:** Целое число от 0 до 4294967295 Количество пакетов, которые удовлетворяют следующим условиям. • Длина данных пакета данных больше 1536 октетов.

Параметр	Описание
	• Циклический избыточный код (CRC) неправильный, то есть не соответствует содержимому пакета.
`Collisions`	**Краткий обзор:** Целое число от 0 до 4294967295 Количество принятых пакетов, для которых была обнаружена коллизия.
`LateCollisions`	**Краткий обзор:** Целое число от 0 до 4294967295 Количество принятых пакетов, для которых была обнаружена поздняя коллизия.
`Pkt64Octets`	**Краткий обзор:** Целое число от 0 до 4294967295 Количество принятых и переданных пакетов с размером 64 октета. Включает в себя принятые и переданные пакеты, а также отброшенные пакеты и локальные принятые пакеты. Не включает в себя отклоненные полученные пакеты.
`Pkt65to127Octets`	**Краткий обзор:** Целое число от 0 до 4294967295 Количество принятых и переданных пакетов с размером от 65 до 127 октетов. Включает в себя принятые и переданные пакеты, а также отброшенные пакеты и локальные принятые пакеты. Не включает в себя отклоненные полученные пакеты.
`Pkt128to255Octets`	**Краткий обзор:** Целое число от 0 до 4294967295 Количество принятых и переданных пакетов с размером от 128 до 257 октетов. Включает в себя принятые и переданные пакеты, а также отброшенные пакеты и локальные принятые пакеты. Не включает в себя отклоненные полученные пакеты.
`Pkt256to511Octets`	**Краткий обзор:** Целое число от 0 до 4294967295 Количество принятых и переданных пакетов с размером от 256 до 511 октетов. Включает в себя принятые и переданные пакеты, а также отброшенные пакеты и локальные принятые пакеты. Не включает в себя отклоненные полученные пакеты.
`Pkt512to1023Octets`	**Краткий обзор:** Целое число от 0 до 4294967295 Количество принятых и переданных пакетов с размером от 512 до 1023 октетов. Включает в себя принятые и переданные пакеты, а также отброшенные пакеты и локальные принятые пакеты. Не включает в себя отклоненные полученные пакеты.
`Pkt1024to1536Octets`	**Краткий обзор:** Целое число от 0 до 4294967295 Количество принятых и переданных пакетов с размером от 1024 до 1536 октетов. Включает в себя принятые и переданные пакеты, а также отброшенные пакеты и локальные принятые пакеты. Не включает в себя отклоненные полученные пакеты.
`DropEvents`	**Краткий обзор:** Целое число от 0 до 4294967295 Количество принятых пакетов, которые были отброшены из-за нехватки буферов приема.
`OutMulticasts`	**Краткий обзор:** Целое число от 0 до 18446744073709551615 Количество переданных групповых пакетов. Не включает в себя широковещательные пакеты.

Параметр	Описание
`OutBroadcasts`	**Краткий обзор:** Целое число от 0 до 18446744073709551615 Количество переданных широковещательных пакетов.
`UndersizePkts`	**Краткий обзор:** Целое число от 0 до 4294967295 Количество принятых пакетов, которые удовлетворяют следующим условиям. • Длина данных пакета данных меньше 64 октетов. • Событие коллизии не было обнаружено. • Событие поздней коллизии не было обнаружено. • Пакет имеет правильный циклический избыточный код (CRC).

4.7.5 Очистка статистики для конкретных Ethernet-портов

Чтобы очистить статистику, собранную для одного или нескольких Ethernet-портов, сделайте следующее:

1. Перейдите в ***Ethernet Stats » Clear Ethernet Port Statistics***. Появится форма **Clear Ethernet Port Statistics**.
2. Выберите один или несколько Ethernet-портов.
3. Нажмите **Apply**.

4.7.6 Конфигурирование Ethernet-порта

Чтобы сконфигурировать Ethernet-порт, сделайте следующее:

Примечание
В зависимости от требуемого типа среды передачи данных порт SFP может нуждаться в некоторой явной настройке. Перед выполнением конфигурирования порта SFP см. "Требования к трансиверам SFP (Страница 84)".

1. Перейдите в ***Ethernet Ports » Configure Port Parameters***. Появится таблица **Port Parameters**.
2. Выберите Ethernet-порт. Появится форма **Port Parameters**.
3. Необходимо сконфигурировать следующие параметры:

Параметр	Описание
`Port`	**Краткий обзор:** 1 to maximum port number **Значение по умолчанию:** 1 Номер порта.

Параметр	Описание
Name	**Краткий обзор:** Строка длиной 15 символа(ов) **Значение по умолчанию:** Port x Описательное имя, которое может использоваться для идентификации устройства, подключенного к этому порту.
Media	**Краткий обзор:** [100TX | 10FL | 100FX | 1000X | 1000T | 802.11g | EoVDSL | 100TX Only | 10FL/100SX | 10GX] **Значение по умолчанию:** 100TX Тип среды передачи для данного порта.
State	**Краткий обзор:** [Disabled | Enabled] **Значение по умолчанию:** Enabled Отключение порта приведет к невозможности передачи и приема любых кадров через этот порт. Также при отключении порта не посылаются импульсные сигналы целостности линии связи, так что светодиодный индикатор связи/активности никогда не будет гореть. Отключение порта может потребоваться для выявления и устранения проблем, либо для его защиты от несанкционированных соединений. **Примечание** Отключение порта, для которого задан тип передающей среды 802.11g, отключает соответствующий беспроводной модуль.
AutoN	**Краткий обзор:** [Off | On] **Значение по умолчанию:** On Включает или выключает автоматическое согласование IEEE 802.3. Включение автоматического согласования приводит к согласованию скорости передачи и дуплексного режима при обнаружении канала связи; оба оконечных устройства должны быть совместимыми с функцией автоматического согласования для получения наилучших результатов. Оптоволоконные среды передачи данных со скоростью 10 Мбит/с и 100 Мбит/с не поддерживают автоматическое согласование, так что эти среды передачи данных должны явным образом конфигурироваться для полудуплексного или полнодуплексного режима. Работа в полнодуплексном режиме требует конфигурирования обеих сторон для этого режима, иначе при интенсивном сетевом трафике будут иметь место существенные потери кадров.
Speed	**Краткий обзор:** [Auto | 10M | 100M | 1G] **Значение по умолчанию:** Auto Скорость передачи (мегабиты в секунду или гигабиты в секунду). Если включено автоматическое согласование, то данный параметр представляет собой скорость передачи из числа возможных, предлагаемую в процессе автоматического согласования. Если автоматическое согласование отключено, то для порта устанавливается эта скорость передачи данных.

Параметр	Описание
	AUTO означает уведомление о всех поддерживаемых режимах скорости передачи.
`Dupx`	**Краткий обзор:** [Auto | Half | Full] **Значение по умолчанию:** Auto Дуплексный режим. Если включено автоматическое согласование, то данный параметр представляет собой дуплексный режим из числа возможных, предложенный в процессе автоматического согласования. Если автоматическое согласование отключено, то для порта устанавливается этот дуплексный режим. AUTO означает объявление всех поддерживаемых дуплексных режимов.
`LFI`	**Краткий обзор:** [Off | On] **Значение по умолчанию:** Off Включение индикации отказа канала связи (LFI) подавляет передачу сигнала целостности линии связи, если принимающий канал связи вышел из строя. Это позволяет устройству на дальнем конце линии обнаруживать отказ канала связи при любых обстоятельствах. **Примечание** Эта функция не должна быть включена на обеих сторонах канала связи.
`Alarm`	**Краткий обзор:** [On | Off] **Значение по умолчанию:** On Отключение сигналов тревоги по состоянию канала связи приведет к прекращению передачи оповещений, а также SNMP trap-уведомлений LinkUp и LinkDown для этого порта.
`Act on LinkDown`	**Краткий обзор:** [Do nothing | Admin Disable] **Значение по умолчанию:** Do nothing Действие, выполняемое при событии LinkDown (Соединение прервано) порта. Опции включают: • `Do nothing (Без действий)` - Никаких действий не предпринимается. • `Admin Disable (Отключение со стороны администратора)` - Состояние порта Disabled (Отключено). Для параметра State (Состояние) должно быть установлено значение Enabled (Ввключено) перед восстановлением связи.
`Downshift`	**Краткий обзор:** [Disabled | Enabled] **Значение по умолчанию:** Enabled Включение или отключение автоматического согласования на гигабитном (1000Base-T) порту с помощью двухпарного витого кабеля. Если эта опция включена, устройство может осуществлять автоматическое согласование с другим партнером по каналу связи 1000Base-T с помощью

Параметр	Описание
	двухпарного кабеля и устанавливать соединение со скоростью 100 Мбит/с или 10 Мбит/с.

Примечание
Если на одной стороне канала связи жестко установлены скорость передачи и тип дуплексного режима, а партнер по связи производит автоматическое согласование, то существует большая вероятность, что связь не удастся установить, либо она будет установлена с неверными настройками на стороне, где производилось автоматическое согласование. Партнер, выполняющий автосогласование, автоматически переключится на полудуплексный режим даже в том случае, если фиксированная сторона находится в полнодуплексном режиме. Работа в полнодуплексном режиме требует конфигурирования обеих сторон для этого режима, иначе при интенсивном сетевом трафике будут иметь место большое количество испорченных кадров из-за ошибок. При небольшом объеме трафика канал связи может демонстрировать меньше ошибок или даже их отсутствие. По мере роста объема трафика на стороне с фиксированным согласованием параметров связи начнут теряться пакеты, тогда как на стороне с автоматическим согласованием будут иметь место чрезмерные коллизии. И наконец, по мере приближения интенсивности трафика к 100 % канал связи станет полностью непригодным для использования. Этих проблем можно избежать, всегда жестко настраивая на обоих соединяемых портах одинаковые параметры.

4. Нажмите **Apply**.

4.7.7 Конфигурирование ограничения скорости передачи через порт

Чтобы сконфигурировать ограничение скорости передачи через порт, сделайте следующее:

1. Перейдите в ***Ethernet Ports » Configure Port Rate Limiting***. Появится таблица **Port Rate Limiting**.
2. Выберите Ethernet-порт. Появится форма **Port Rate Limiting**.
3. Необходимо сконфигурировать следующие параметры:

Параметр	Описание
`Port`	**Краткий обзор:** 1 to maximum port number **Значение по умолчанию:** 1 Номер порта.
`Ingress Limit`	**Краткий обзор:** [Disabled] **Значение по умолчанию:** 1000 Максимальная скорость, при превышении которой принятые кадры (того типа, который описан параметром "входящие кадры") будут отброшены коммутатором.

Параметр	Описание
`Ingress Frames`	**Значение по умолчанию:** Broadcast Этот параметр определяет типы кадров, скорость поступления которых на данный порт должна быть ограничена. Ограничение применяется только к принимаемым кадрам: • `Broadcast` - только широковещательные кадры • `Bcast&Mcast` - широковещательные и групповые кадры • `Bcast&FloodUcast` - широковещательные кадры и направленные кадры с веерной рассылкой • `FloodUcast` - только направленные кадры с веерной рассылкой
`Egress Limit`	**Краткий обзор:** [Disabled] **Значение по умолчанию:** Disabled Максимальная скорость, с которой коммутатор передает (групповые, широковещательные и направленные) кадры через данный порт. При необходимости коммутатор будет отбрасывать кадры, чтобы средняя скорость исходящего трафика соответствовала этой максимальной скорости.

4. Нажмите **Apply**.

4.7.8 Конфигурирование зеркалирования портов

Зеркалирование портов представляет собой инструмент для выявления и устранения проблем, который дублирует, или зеркалирует, весь трафик, принимаемый или передаваемый через выделенный порт, на указанный "зеркальный" порт. Если к порту назначения подключен анализатор протокола, то поток трафика не содержащих ошибок кадров через любой порт-источник становится доступным для анализа.

⚠ ЗАМЕТКА

Опасность для конфигурации — риск нарушения обмена данными

Выбирайте порт назначения, который имеет более высокую скорость, чем порт-источник. Зеркалирование порта, имеющего скорость 100 Мбит/с, на порт, имеющий скорость 10 Мбит/с, приведет к неверному зеркалированию потока кадров.

⚠ ЗАМЕТКА

Опасность для конфигурации — риск нарушения обмена данными

Кадры будут отбрасываться, если скорость прохождения кадров через порт-источник с учетом дуплекса превышает скорость передачи порта назначения. Поскольку на порт назначения дублируются как передаваемые, так и принимаемые через порт-источник кадры, то кадры будут теряться, если суммарный трафик превышает скорость передачи порта назначения.

Эта проблема достигает своего крайнего проявления в том случае, когда трафик через полнодуплексный порт, имеющий скорость передачи 100 Мбит/с, зеркалируется на полудуплексный порт, имеющий скорость передачи 10 Мбит/с.

⚠ ЗАМЕТКА

Перед конфигурированием зеркалирования портов обратите внимание на следующее:

- Зеркальные порты допускают двунаправленный трафик (т. е. устройство не будет блокировать трафик, входящий через зеркальные порты). Для повышения безопасности сконфигурируйте входную фильтрацию для управления потоком трафика, когда зеркалирование портов включено. Для получения дополнительной информации о включении входной фильтрации см. "Глобальное конфигурирование сетей VLAN (Страница 170)".
- Трафик будет зеркалироваться на порт назначения независимо от сети VLAN, которой он принадлежит. Эта может быть как та же сеть, что и у порта-источника, так и другая.
- Кадры управления сетью (например, RSTP, GVRP и т. п.) не могут зеркалироваться.
- Кадры управления коммутаторами, генерируемые коммутатором (например, Telnet, HTTP, SNMP и т. п.) не могут зеркалироваться.

Примечание
Кадры неверного формата, принимаемые на порт-источник, не будут зеркалироваться. Сюда относятся ошибки CRC, пакеты избыточного и неполного размера, фрагменты, бессмысленные пакеты, коллизии и поздние коллизии, а также отброшенные события.

Чтобы сконфигурировать зеркалирование порта, сделайте следующее:

1. Перейдите в ***Ethernet Ports » Configure Port Mirroring***. Появится форма **Port Mirroring**.
2. Необходимо сконфигурировать следующие параметры:

Параметр	Описание
`Port Mirroring`	**Краткий обзор:** [Disabled | Enabled] **Значение по умолчанию:** Disabled Включение зеркалирования портов приводит к тому, что все кадры, принимаемые и передаваемые через порты-источники, передаются на порт назначения.
`Source Ports Egr`	**Краткий обзор:** Comma-separated list of ports Контролируемый(-е) порт(-ы).
`Source Ports Ingr`	**Краткий обзор:** Comma-separated list of ports Контролируемый(-е) порт(-ы).

Параметр	Описание
`Target Port`	**Краткий обзор:** 1 to maximum port number **Значение по умолчанию:** 1 Устройство для мониторинга должно быть подключено к порту назначения.

3. Нажмите **Apply**.

4.7.9 Конфигурирование определения состояния канала связи

Чтобы сконфигурировать определение состояния канала связи, сделайте следующее:

1. Перейдите в ***Ethernet Ports » Configure Link Detection***. Появится форма **Link Detection**.
2. Необходимо сконфигурировать следующие параметры:

Примечание
Если включено быстрое определение состояния канала связи, то система предотвращает захват процедурой обработки изменений состояния канала связи всех доступных ресурсов процессора. Однако, если не используется функция Port Guard, то почти все рабочее время центрального процессора будет занято обработкой частых изменений состояния канала связи, что может оказывать отрицательное влияние на быстроту реагирования системы в целом.

Параметр	Описание
`Fast Link Detection`	**Краткий обзор:** [Off | On | On_withPortGuard] **Значение по умолчанию:** On_withPortGuard Этот параметр обеспечивает защиту от неисправных оконечных устройств, генерирующих неправильный сигнал целостности линии связи. При подключении неисправного оконечного устройства или несоответствующего волоконного порта к устройству, в течение короткого периода времени может быть сообщено о большом количестве непрерывных изменений состояния линии связи. Такое большое количество ложных изменений состояния линии связи может привести к отсутствию реакции системы, так как большая часть (если не все) ресурсов системы используются для обработки изменений состояния линии связи. Это, в свою очередь, может вызвать серьезные проблемы в сети, поскольку обработка RSTP устройства может не выполняться, что позволяет формировать петлю в сети. Для данного параметра доступны три различные настройки: • `Off (Выключено)` - значение Off (Выключено) для этого параметра полностью отключает функцию быстрого определения рабочего состояния линии. Коммутатору будет необходимо больше времени для обнаруже-

Параметр	Описание
	ния отказа канала связи. Это приведет к более продолжительному времени восстановления сети, до двух секунд. • `On (Включено)` - в особых случаях, когда в течение длительных интервалов времени имеют место частые изменения состояния линии, которые являются нормальными для этой линии, такая настройка предотвращает отключение системой функции быстрого определения рабочего состояния линии для порта. Если чрезмерно частые изменения состояния канала связи имеют место более двух минут для определенного порта, то генерируется оповещение, чтобы предупредить о нарушении синхронизации канала связи. Если впоследствии чрезмерно частые изменения состояния линии будут устранены, то оповещение сбрасывается автоматически. Поскольку эта опция не отключает функцию быстрого определения рабочего состояния линии, то устойчивое нарушение синхронизации линии может влиять на время реакции системы. Эту настройку следует применять с осторожностью. • `On_withPortGuard` - это рекомендуемая настройка. При этой настройке продолжительный период (более двух минут) чрезмерно частых изменений состояния линии, о которых сообщает порт, служит указанием для функции защиты порта произвести постоянное отключение быстрого определения рабочего состояния линии и приводит к выдаче оповещения. При отключении функции быстрого определения рабочего состояния линии чрезмерно частые изменения состояния линии больше не могут приводить к расходованию существенного количества системных ресурсов. При отключенной функции быстрого определения рабочего состояния линии порту потребуется больше времени для обнаружения отказа канала связи. Это может привести к более продолжительному времени восстановления сети, до двух секунд. После того как функция защиты порта отключит быстрое определение рабочего состояния линии для конкретного порта, вы снова можете его включить, удаляя соответствующее оповещение.
`Link Detection Time`	**Краткий обзор:** Целое число от 100 до 1000 **Значение по умолчанию:** 100 Интервал времени, в течение которого канал связи должен непрерывно находиться в активном состоянии, пока устройство не сделает вывод, что "связь установлена". Устройство производит устранение ложных повторных сигналов при обнаружении канала связи Ethernet, чтобы избежать множественных реакций на случайное событие дребезга контактов в линии связи (например, когда кабель образует прерывистый контакт при его подсоединении или отсоединении).

3. Нажмите **Apply**.

4.7.10 Управление трансиверами SFP

RUGGEDCOM ROS поддерживает компактные модульные приемопередатчики (трансиверы SFP) для обеспечения каналов связи 1000Base-X, 100Base-FX, 1000Base-T или 100Base-TX link.

Примечание
Поскольку волоконно-оптические трансиверы SFP 1000Base-X являются стандартизированными, RUGGEDCOM ROS поддерживает большую часть моделей данного типа. Для получения дополнительной информации см. RUGGEDCOMкаталог трансиверов SFP [https://support.industry.siemens.com/cs/ww/en/view/109482309].

Настоятельно рекомендуется использовать только модели трансиверов SFP, одобренные компанией Siemens. Siemens проводит широкое испытание этих трансиверов, чтобы убедиться в их способности выдерживать тяжелые условия эксплуатации. При использовании другой модели SFP-трансивера в обязанности пользователя входит проверка ее соответствия требованиям к окружающей среде и эксплуатационным требованиям.

Медные SFP трансиверы 1000Base-T не являются стандартизированными. RUGGEDCOM ROS поддерживает только некоторые модели данного типа.

Примечание
SFP-трансиверы поддерживают замену в горячем режиме.

При установке трансивера SFP в соответствующий слот настройки скорости и автосогласования автоматически корректируются на соответствующие значения. Например, при установке трансивера SFP 1 G скорость порта автоматически меняется на 1 G, а автосогласование устанавливается на *Вкл.*.

Примечание
Из-за неопределенного времени ожидания, вызванного встроенным PHY, точность выдерживания времени IEEE 1588 может значительно снижаться на медном порте SFP.

4.7.10.1 Требования к трансиверам SFP

В зависимости от требуемого типа среды передачи данных порт SFP может нуждаться в некотором явном конфигурировании:

- Для каналов связи 10GBase-X скорость должна быть установлена на уровне 10 Гбит/с, а автосогласование — на *Выкл.* .
- Для каналов связи 100Base-FX или 100Base-TX скорость должна быть установлена на уровне 100 Мбит/с.
- Для каналов связи 1000Base-X или 1000Base-T, скорость порта SFP должна быть установлена на уровне 1 Гбит/с.

- Автоматическое согласование может быть сконфигурировано на *Вкл.*, когда скорость порта установлена на 1 Гбит/с, или на *Выкл.*, когда скорость порта установлена на 100 Мбит/с.
- Дуплексный режим не может конфигурироваться для порта SFP, так что всегда принудительно устанавливается полнодуплексный режим.
- Дуплексный режим не может конфигурироваться для порта 10G SFP+, так что всегда принудительно устанавливается полнодуплексный режим.

Для получения дополнительной информации о конфигурировании SFP-трансиверов и других Ethernet-портов на устройстве см. "Конфигурирование Ethernet-порта (Страница 76)".

4.7.10.2 Мониторинг порта SFP

RUGGEDCOM ROS поддерживает "горячую" замену SFP-трансиверов на портах SFP и автоматически обнаруживает, когда SFP-трансивер удаляется или вставляется.

Когда RUGGEDCOM ROS обнаруживает, что SFP-трансивер вставлен в порт SFP, она считывает информацию трансивера и определяет тип трансивера. В результате этого решения порт SFP будет *принят*, *принят и реконфигурирован* или *отвергнут* в RUGGEDCOM ROS.

Следующая таблица показывает, в каких случаях SFP-трансивер *принимается* или *принимается и реконфигурируется*.

Сконфигурированная скорость	Тип обнаруженного SFP: 1000Base-X	Тип обнаруженного SFP: 100Base-FX	Тип обнаруженного SFP: 1000Base-T
1 Гбит/с	Принять	Принять и автоматически установить скорость 100 Мбит/с и установить автоматическое согласование на *Выкл.*.	Принять
100 Мбит/с	Принять и автоматически установить скорость 1 Гбит/с и установить автоматическое согласование на *Вкл.*.	Принять	Сравнить модель трансивера со списком поддерживаемых моделей. Принять, если присутствует в списке. В ином случае автоматически установить скорость 1 Гбит/с и установить автоматическое согласование на *Вкл.*.

Если трансивер *принят*, `Media` параметр состояния ***Ethernet Ports » Configure Port Parameters*** показывает подробную информацию об этом SFP-трансивере, в том числе код соответствия Gigabit Ethernet, среду передачи данных, тип разъема и длину линии связи. Например:

```
SFP 1000LX SM LC 10 km
SFP 1000T 100 m
```

Если трансивер не распознан, он *отвергается*. Также генерируется оповещение, а порт будет заблокирован, так что связь не может быть установлена, пока не будет заменен трансивер. Параметр `Media` будет показывать, что отвергнутый SFP-трансивер не определен. Например:

```
SFP Unidentified
```

Если на порт SFP не установлен трансивер, то параметр `Media` будет показывать, что SFP-трансивер не подключен:

```
SFP Unplugged
```

4.7.10.3 Отображение информации для порта SFP

Чтобы отобразить детальную информацию о порте SFP, сделайте следующее:

1. Войдите в систему и перейдите в командную оболочку CLI. Для получения дополнительной информации о порядке доступа к командной оболочке CLI см. "Использование интерфейса командной строки (Страница 27)".
2. Введите следующую команду:

   sfp { *port* }

   где:

   - { *port* } — номер порта

   Отобразится информация о порте. Например:

```
>sfp


ID: SFP
Extended ID: GBIC/SFP function is defined by serial ID only
Connector: LC
Transceiver:
Gigabit Ethernet Compliance Codes:
1000LX
Fibre Channel link length:
Long Distance (L)
Fibre Channel transmitter technology:
Longwave laser (LC)
Fibre Channel transmission media:
Single Mode (SM)
Fibre Channel speed:
100 MBytes/Sec
Baud Rate, nominal: 1300 MBits/sec
Encoding type: 8B10B
Length(9um): 10 km
Length(9um): 10000 m
Length(50um): 550 m
Length(62.5um): 550 m
Length(Copper): Not specified
Vendor: xxxxxxx
IEEE company ID: xxxxxxx
Part number: xxxxxxxxxx
Revision: 0000
Laser wavelength: 1310 nm
```

>

4.7.11 Обнаружение неисправностей кабеля

Проблемы с подключением иногда могут быть связаны с неисправностями в Ethernet-кабелях. Для упрощения поиска неисправностей вроде коротких замыканий, обрывов и слишком длинных кабелей, в RUGGEDCOM ROS предусмотрена встроенная утилита диагностики кабелей.

4.7.11.1 Просмотр результатов диагностики кабеля

Чтобы просмотреть результаты предыдущих диагностических тестов, перейдите в ***Ethernet Ports » Configure/View Cable Diagnostics Parameters***. Появится таблица **Cable Diagnostics Parameters**.

Примечание
Для получения информации о том, как запустить диагностический тест см. "Выполнение диагностики кабеля (Страница 89)".

В этой таблице отображается следующая информация:

Параметр	Описание
`Port`	**Краткий обзор:** 1 to maximum port number Номер порта.
`State`	**Краткий обзор:** [Stopped | Started] Запускает или останавливает диагностику кабеля для выбранного порта. Если порт не поддерживает диагностику кабеля, то для параметра "состояние" будет отображаться значение N/A (недоступно).
`Runs`	**Краткий обзор:** Целое число от 0 до 65535 Общее число попыток выполнения диагностики кабеля, которое должно быть произведено для выбранного порта. Если задано значение 0, то диагностика кабеля выполняется до тех пор, пока процедура диагностики не будет остановлена явным образом.
`Calib.`	**Краткий обзор:** Целое число от -100.0 до 100.0 Для коррекции расчетного расстояния до места отказа может использоваться калибровочное значение. Пользователь может выполнить следующие действия для калибровки расчетного расстояния до неисправности при диагностике кабеля: 1. Выберите конкретный порт, калибровка которого необходима. 2. Подключите Ethernet-кабель известной длины (например, 50 м) к порту. 3. НЕ ПОДКЛЮЧАЙТЕ другой конец этого кабеля к партнеру по связи.

Параметр	Описание
	4. Выполните диагностику кабеля для порта несколько раз. Неисправности типа ОБРЫВА ЛИНИИ должны выявляться. 5. Найдите среднее расстояние до неисправности типа ОБРЫВА ЛИНИИ, зарегистрированной в журнале, и сравните его с известной длиной кабеля. Разница может использоваться в качестве калибровочного значения. 6. Введите калибровочное значение и выполните диагностику кабеля еще несколько раз. 7. Расстояние до неисправности типа ОБРЫВА ЛИНИИ должно быть таким же, что и длина кабеля. 8. Расстояние до неисправности для выбранного порта теперь откалибровано.
`Good`	**Краткий обзор:** Целое число от 0 до 65535 Число повторений, в ходе которых состояние GOOD TERMINATION (отсутствие отказа) было определено на кабельных парах выбранного порта.
`Open`	**Краткий обзор:** Целое число от 0 до 65535 Число повторений, в ходе которых состояние OPEN (обрыв линии) было определено на кабельных парах выбранного порта.
`Short`	**Краткий обзор:** Целое число от 0 до 65535 Число повторений, в ходе которых состояние SHORT (короткое замыкание) было определено на кабельных парах выбранного порта.
`Imped`	**Краткий обзор:** Целое число от 0 до 65535 Число повторений, в ходе которых состояние IMPEDANCE MISMATCH (рассогласование полных сопротивлений) было детектировано на кабельных парах выбранного порта.
`Pass /Fail /Total`	**Краткий обзор:** Строка длиной 19 символа(ов) Это поле содержит итоговые результаты выполненной диагностики кабеля на текущий момент. • `Pass (испытание пройдено)` - число успешных попыток выполнения диагностики кабеля для выбранного порта. • `Fail (испытание не пройдено)` - число неуспешных попыток выполнения диагностики кабеля для выбранного порта. • `Total (итого)` - общее число попыток выполнения диагностики кабеля для выбранного порта.

Примечание
Для каждого успешного диагностического испытания значения для **Good**, **Open**, **Short** или **Imped** будут увеличиваться на основе числа кабельных пар, подключенных к порту. Для порта 100Base-T, имеющего две кабельные пары, количество будет увеличиваться на два. Для порта 1000Base-T, имеющего четыре кабельные пары, количество будет увеличиваться на четыре.

Примечание
При обнаружении неисправности кабеля рассчитывается расчетное расстояние до неисправности, которое регистрируется в системном журнале. В журнале указывается кабельная пара, обнаруженная неисправность и значение расстояния до неисправности. Для получения дополнительной информации о системном журнале см. "Просмотр локальных и системных журналов (Страница 65)".

4.7.11.2 Выполнение диагностики кабеля

Для проведения диагностического теста кабеля на одном или нескольких Ethernet-портах, сделайте следующее:

1. Подключите Ethernet-кабель категории CAT-5 (или лучше) к выбранному Ethernet-порту.

   ⚠ ЗАМЕТКА
   Выбранный Ethernet-порт и его порт-партнер могут быть оба сконфигурированы на работу в режиме *Enabled (Включено)* с автосогласованием или в режиме *Disabled (Отключено)*. Другие режимы не рекомендуются, поскольку они могут создавать помехи процедуре диагностики кабеля.

2. Подключите другой конец этого кабеля к аналогичному сетевому порту. Например, подключайте порт 100Base-T к порту 100Base-T, а порт 1000Base-T подключайте к порту 1000Base-T.
3. В RUGGEDCOM ROS перейдите в ***Ethernet Ports » Configure/View Cable Diagnostics Parameters***. Появится таблица **Cable Diagnostics Parameters**.
4. Выберите Ethernet-порт. Появится форма **Cable Diagnostics Parameters**.
5. В пункте **Runs** введите число диагностических тестов для последовательного выполнения. Значение 0 указывает, что тест будет выполняться бесконечно до тех пор, пока его не остановит пользователь.
6. В пункте **Calib.** введите расчетное значение расстояния до неисправности (DTF). Для получения информации о том, как определить значение DTF см. "Определение расчетного расстояния до неисправности (DTF) (Страница 90)".
7. Выберите **Started**.

   ⚠ ЗАМЕТКА
   Диагностический тест можно остановить, выбрав **Stopped** и нажав **Apply**. Однако если остановить тест в процессе диагностики, он продолжится до завершения.

8. Нажмите **Apply**. Состояние Ethernet-порта автоматически изменится на `Stopped` после завершения испытания. Для получения информации о текущем контроле теста и просмотре результатов см. "Просмотр результатов диагностики кабеля (Страница 87)".

4.7.11.3 Очистка диагностики кабеля

Чтобы очистить результаты диагностики кабеля, сделайте следующее:

1. Перейдите в ***Ethernet Ports » Clear Cable Diagnostics Statistics***. Появится форма **Clear Cable Diagnostics Statistics**.
2. Выберите один или несколько Ethernet-портов.
3. Нажмите **Apply**.

4.7.11.4 Определение расчетного расстояния до неисправности (DTF)

Чтобы определить расчетное расстояние до неисправности (DTF), сделайте следующее:

1. Подключите Ethernet-кабель категории CAT-5 (или лучше) известной длины к устройству. Не подключайте другой конец этого кабеля к другому порту.
2. Сконфигурируйте утилиту диагностики кабеля на несколько выполнений с выбранным Ethernet-портом и запустите тест. Для получения дополнительной информации см. "Выполнение диагностики кабеля (Страница 89)". Неисправности типа обрыва линии должны выявляться и регистрироваться в системном журнале.
3. Ознакомьтесь с ошибками, зарегистрированными в системном журнале и определите среднее расстояние неисправностей типа обрыва линии. Для получения дополнительной информации о системном журнале см. "Просмотр локальных и системных журналов (Страница 65)".
4. Отбросьте среднее расстояние от длины кабеля для определения калибровочного значения.
5. Сконфигурируйте утилиту диагностики кабеля на выполнение в течение нескольких раз с новым калибровочным значением. Расстояние до неисправности типа обрыва линии должно быть таким же, что и фактическая длина кабеля. Расчетное расстояние до неисправности (DTF) теперь скалибровано для выбранного Ethernet-порта.

4.7.12 Сброс Ethernet-портов

Иногда бывает необходимо сбросить конкретный Ethernet-порт, например, если партнер по соединению фиксируется в неверном состоянии. Это также бывает полезно для принудительного пересогласования скоростных и дуплексных режимов.

Чтобы сбросить конкретные Ethernet-порты, сделайте следующее:

1. Перейдите в ***Ethernet Ports » Reset Port(s)***. Появится форма **Reset Port(s)**.
2. Выберите один или несколько Ethernet-портов для сброса.
3. Нажмите **Apply**. Выбранные Ethernet-порты сбрасываются.

4.8 Управление IP-интерфейсами

RUGGEDCOM ROS позволяет сконфигурировать по одному IP-интерфейсу для каждой подсети (или VLAN) всего до 255 интерфейсов.

Один интерфейс должен быть сконфигурирован как интерфейс управления. По умолчанию только на интерфейсе управления, могут работать IP-сервисы, такие как DHCP, IEEE1588, последовательный сервер и LLDP, которые влияют на устройство Тем не менее, RUGGEDCOM ROS можно сконфигурировать таким образом, чтобы вспомогательные интерфейсы управления запускали следующие сервисы:

- Коммутация 3-го уровня
- MMS
- Modbus
- Radius/TacPlus
- Удаленная оболочка
- Удаленный системный журнал
- SNMP
- SNTP
- SSH
- TFTP
- Telnet
- Веб-сервер

Для получения дополнительной информации см. "Конфигурирование IP-сервисов (Страница 96)".

Каждому IP-интерфейсу должен быть назначен IP-адрес. В случае интерфейса управления тип IP-адреса может быть статическим, DHCP, BOOTP или динамическим. Для всех остальных интерфейсов IP-адрес должен быть статическим.

⚠ ЗАМЕТКА

Опасность для конфигурации — риск нарушения обмена данными

Изменение идентификатора для сети VLAN с передачей трафика управления коммутаторами приведет к разрыву любого активного TCP-соединения

RawSocket (неструктурированный сокет). Если это произойдет, сбросьте все последовательные порты.

4.8.1 Просмотр списка IP-интерфейсов

Чтобы просмотреть список IP-интерфейсов, сконфигурированных на устройстве, перейдите в ***Administration » Configure IP Interfaces » Configure IP Interfaces***. Появится таблица **IP Interfaces**.

Если IP-интерфейсы не были сконфигурированы, добавьте необходимые IP-интерфейсы. Для получения дополнительной информации см. "Добавление IP-интерфейса (Страница 92)".

4.8.2 Добавление IP-интерфейса

Чтобы добавить IP-интерфейс, сделайте следующее:

1. Перейдите в ***Administration » Configure IP Interfaces***. Появится **IP Interfaces Table**.
2. Нажмите **InsertRecord**. Появится форма **IP Interfaces**.
3. Необходимо сконфигурировать следующие параметры:

⚠ ЗАМЕТКА

Угроза безопасности — риск неавторизованного доступа и/или использования

IP-интерфейсы, которые принадлежат сети VLAN с передачей трафика управления коммутаторами или вспомогательной сети VLAN с передачей трафика управления коммутаторами, должны быть подключены к доверенной сети.

⚠ ЗАМЕТКА

Опасность для конфигурации — риск нарушения обмена данными.

Изменение идентификатора для сети VLAN с передачей трафика управления коммутаторами приведет к разрыву любого активного TCP-соединения по протоколу RawSocket (неструктурированный сокет). Если это произойдет, сбросьте все последовательные порты.

Примечание

При сбросе всех параметров конфигурации в настройки по умолчанию IP-адрес и маска подсети, сконфигурированные для сети VLAN с передачей трафика управления коммутаторами, не изменяются; также для них будет назначен по умолчанию идентификатор сети VLAN ID, равный 1.

Изменения IP-адреса вступают в силу немедленно. Все IP-соединения, имеющие место во время изменения IP-адреса, будут потеряны.

Примечание
При использовании синтаксического представления 32-битовых адресов в виде четырех 8-битовых целых чисел, разделенных точками для IPv4, например, 255.255.255.0, оно будет автоматически преобразовано в эквивалентное число битов (например, 24 бита).

Параметр	Описание
`Type`	**Краткий обзор:** [VLAN] **Значение по умолчанию:** VLAN Указывает тип интерфейса, для которого создан этот IP-интерфейс.
`ID`	**Краткий обзор:** Целое число от 1 до 4094 **Значение по умолчанию:** 1 Указывает идентификатор интерфейса, для которого создан этот IP-интерфейс. Если тип интерфейса — VLAN, представляет идентификатор беспроводной ЛВС.
`Mgmt`	**Краткий обзор:** [No | Yes | Aux] **Значение по умолчанию:** No Указывает, является ли данный IP-интерфейс интерфейсом административного управления устройством. • `Aux (Вспомогательный)` - поддерживает функции управления • `Yes (Да)` - поддерживает функции управления и назначения динамических адресов, например, DHCP • `No (Нет)` - не поддерживает функции управления или назначения динамических адресов
`IP Address Type`	**Краткий обзор:** [Static | Dynamic | DHCP | BOOTP] **Значение по умолчанию:** Static Указывает, является ли IP-адрес статическим, либо назначается динамически через DHCP или BOOTP. Опция DYNAMIC (динамический) является общим случаем динамически назначаемого IP-адреса. Она обеспечивает переключение между протоколами BOOTP и DHCP, пока не будет получен ответ от соответствующего сервера. Для интерфейсов, не являющихся интерфейсами административного управления, должно быть выбрано Static (статический).
`IP Address`	**Краткий обзор:** Any valid IP address **Значение по умолчанию:** 192.168.0.1 Указывает IP-адрес этого интерфейса. IP-адрес это 128-битное число, которое записывается с помощью восьми полей из четырех шестнадцатеричных цифр, для которых начальные нули могут быть опущены, разделенных знаками двоеточия. Дополнительную информацию см. в документации для чтения в автономном режиме.

Параметр	Описание
	Адрес 4 версии может быть зашифрован четырьмя десятичными числами от 0 до 255, разделенными точками. Допускается только индивидуальный IP-адрес, который не начинается с "FF" или находится в диапазоне от 1.0.0.0 до 233.255.255.255 для версии 4.
`Subnet`	**Краткий обзор:** Целое число от 0 до 128 **Значение по умолчанию:** 24 Указывает число смежных старших битов, составляющих маску подсети для текущего интерфейса. Например, 24 будет соответствовать маске подсети IPv4 255.255.255.0, а 64 будет указывать, что маска подсети состоит из 64 старших бит (действительно для IPv6). **⚠ ЗАМЕТКА** Каждый IP-интерфейс должен иметь уникальный сетевой адрес.

4. Нажмите **Apply**.

4.8.3 Удаление IP-интерфейса

Для удаления IP-интерфейса, сконфигурированного на устройстве, сделайте следующее:

1. Перейдите в ***Administration » Configure IP Interfaces***. Появится таблица **IP Interfaces**.
2. Выберите IP-интерфейс из таблицы. Появится форма **IP Interfaces**.
3. Нажмите **Delete**.

4.9 Управление IP-шлюзами

RUGGEDCOM ROS позволяет сконфигурировать до десяти IP-шлюзов. Если оба параметра **Destination** и **Subnet** пусты, шлюз считается шлюзом по умолчанию.

Примечание
Шлюз по умолчанию не изменяется при выборочном сбросе конфигурации до заводских настроек.

4.9.1 Просмотр списка IP-шлюзов

Чтобы просмотреть список IP-шлюзов, сконфигурированных на устройстве, перейдите в ***Administration » Configure IP Gateways***. Появится таблица **IP Gateways**.

Если IP-шлюзы не были сконфигурированы, добавьте необходимые IP-шлюзы. Для получения дополнительной информации см. "Добавление IP-шлюза (Страница 95)".

4.9.2 Добавление IP-шлюза

Примечание
Предоставленные DHCP адреса IP-шлюза будут иметь приоритет над сконфигурированными вручную значениями.

Чтобы добавить IP-шлюз, сделайте следующее:

1. Перейдите в ***Administration » Configure IP Gateways***. Появится таблица **IP Gateways**.
2. Нажмите **InsertRecord**. Появится форма **IP Gateways**.
3. Необходимо сконфигурировать следующие параметры:

Параметр	Описание
`Destination`	**Краткий обзор:** Any valid IP address Указывает IP-адрес целевой сети или хоста. Для шлюза по умолчанию оба параметра (адресат и подсеть) установлены на 0.
`Subnet`	**Краткий обзор:** Целое число от 0 до 128 **Значение по умолчанию:** 0 Указывает маску IP-подсети устройства-адресата. Для шлюза по умолчанию оба параметра (адресат и подсеть) установлены на 0.
`Gateway`	**Краткий обзор:** Any valid IP address Указывает шлюз, который будет использоваться для доступа к адресату.

4. Нажмите **Apply**.

4.9.3 Удаление IP-шлюза

Для удаления IP-шлюза, сконфигурированного на устройстве, сделайте следующее:

1. Перейдите в ***Administration » Configure IP Gateways***. Появится таблица **IP Gateways**.
2. Выберите IP-шлюз из таблицы. Появится форма **IP Gateways**.
3. Нажмите **Delete**.

4.10 Конфигурирование IP-сервисов

Чтобы сконфигурировать IP-сервисы, обеспечиваемые устройством, сделайте следующее:

1. Перейдите в ***Administration » Configure IP Services***. Появится форма **IP Services**.
2. Необходимо сконфигурировать следующие параметры:

Параметр	Описание
`Inactivity Timeout`	**Краткий обзор:** Целое число от 1 до 60 или [Disabled] **Значение по умолчанию:** 5 Указывает, когда консоль произведет блокировку по времени и будет отображаться экран входа в систему, если отсутствует активность пользователя. Если значение равно нулю, то тайм-ауты отключены. Для пользователей веб-сервера максимальное значение тайм-аута ограничено 30 минутами.
`Telnet Sessions Allowed`	**Краткий обзор:** Целое число от 1 до 4 или [Disabled] **Значение по умолчанию:** Disabled Ограничивает число сеансов Telnet. Если значение равно нулю, то любой Telnet-доступ исключен.
`Web Server Users Allowed`	**Краткий обзор:** Целое число от 1 до 4 или [Disabled] **Значение по умолчанию:** 4 Ограничивает число одновременных пользователей веб-сервера.
`TFTP Server`	**Краткий обзор:** [Disabled | Get Only | Enabled] **Значение по умолчанию:** Disabled Поскольку это нестойкий протокол, данный параметр позволяет пользователю ограничивать или отключать службу. `Disabled (Отключено)` - отключает доступ для чтения и записи через эту службу `Get Only (Только прием)` - позволяет только читать файлы через эту службу `Enabled (Включено)` - позволяет читать и записывать файлы через эту службу
`ModBus Address`	**Краткий обзор:** Целое число от 1 до 255 или [Disabled] **Значение по умолчанию:** Disabled Определяет адрес Modbus, который следует использовать для административного управления через Modbus.
`SSH Sessions Allowed (Controlled Version Only)`	**Краткий обзор:** Целое число от 1 до 4 **Значение по умолчанию:** 4 Ограничивает число сеансов SSH.

Параметр	Описание
`MMS Sessions Allowed`	**Краткий обзор:** Целое число от 1 до 4 **Значение по умолчанию:** Disabled Ограничивает число сеансов MMS. Если выбрано значение Disabled (Отключено), то любой MMS-доступ исключен.
`RSH Server`	**Краткий обзор:** [Disabled | Enabled] **Значение по умолчанию:** Disabled Отключает/включает доступ через удаленную командную оболочку.
`IP Forward`	**Краткий обзор:** [Disabled | Enabled] **Значение по умолчанию:** Disabled Регулирует возможность пересылки IP между сетями VLAN в последовательном сервере или IP-сегментах. **Примечание** При обновлении до RUGGEDCOM ROS версии5.5, по умолчанию установлено значение { Enabled }.
`Max Failed Attempts`	**Краткий обзор:** Целое число от 1 до 20 **Значение по умолчанию:** 10 Максимальное количество неудачных попыток доступа на каждую службу в пределах окна неудачных попыток до блокировки службы. Для каждой службы допускается максимальное количество попыток до блокировки. Этот параметр сбрасывается на значение по умолчанию при сбросе конфигурации в заводские настройки, однако счетчик неудачных попыток для конкретной службы не сбрасывается.
`Failed Attempts Window`	**Краткий обзор:** Целое число от 1 до 30 **Значение по умолчанию:** 5 Время в минутах (мин), в течение которого должно быть превышено максимальное количество неудачных попыток входа в систему до блокировки системы. Когда время истекает, счетчик неудачных попыток сбрасывается на 0. Данный параметр сбрасывается на значение по умолчанию при сбросе конфигурации в заводские настройки.
`Lockout Time`	**Краткий обзор:** Целое число от 1 до 120 **Значение по умолчанию:** 60 Время в минутах (мин) в течение которого служба остается заблокированной после достижения максимального числа неудачных попыток доступа. Данный параметр сбрасывается на значение по умолчанию при сбросе конфигурации в заводские настройки, за исключением интерфейса управления устройством.

3. Нажмите **Apply**.

4.11 Управление дистанционным мониторингом

Дистанционный мониторинг (RMON) используется для сбора и просмотра накопленных статистических данных, относящихся к производительности и работе Ethernet-портов. Он также позволяет регистрировать записи системного журнала и/или генерировать trap-уведомление SNMP, когда превышена частота возникновения заданных событий.

4.11.1 Управление средствами работы с данными, собираемыми при помощи RMON

Средства работы с данными, собираемыми при дистанционном мониторинге (RMON), с регулярными интервалами создают выборки из накапливаемых статистических данных RMON-MIB для заданных Ethernet-портов.

4.11.1.1 Просмотр списка средств работы с данными, собираемыми при помощи RMON

Чтобы просмотреть список средства работы с хронологическими данными, собираемыми при помощи RMON, перейдите в ***Ethernet Stats » Configure RMON History Controls***. Появится таблица **RMON History Controls**.

Если средства работы с собираемыми данными не были сконфигурированы, добавьте необходимые средства управления. Для получения дополнительной информации см. "Добавление средства работы с данными, собираемыми при помощи RMON (Страница 98)".

4.11.1.2 Добавление средства работы с данными, собираемыми при помощи RMON

Чтобы добавить средство работы с данными, собираемыми при помощи RMON, сделайте следующее:

1. Перейдите в ***Ethernet Stats » Configure RMON History Controls***. Появится таблица **RMON History Controls**.
2. Нажмите **InsertRecord**. Появится форма **RMON History Controls**.
3. Необходимо сконфигурировать следующие параметры:

Параметр	Описание
`Index`	**Краткий обзор:** Целое число от 1 до 65535 **Значение по умолчанию:** 1 Указатель на запись в данной таблице RMON History Control.
`Port`	**Краткий обзор:** 1 to maximum port number **Значение по умолчанию:** 1 Номер порта.

Параметр	Описание
`Requested Buckets`	**Краткий обзор:** Целое число от 1 до 5000 **Значение по умолчанию:** 50 Максимальное число сегментов памяти, запрашиваемых для накапливания этой серии статистических выборок RMON. Интервал: 1–4000. По умолчанию 50.
`Granted Buckets`	**Краткий обзор:** Целое число от 0 до 65535 Число сегментов памяти, предоставленных для накапливания этой серии статистических выборок RMON. Это поле не редактируемое.
`Interval`	**Краткий обзор:** Целое число от 1 до 3600 **Значение по умолчанию:** 1800 Число секунд, в течение которых производится выборка данных для каждого сегмента. Интервал: 1–3600. По умолчанию 1800.
`Owner`	**Краткий обзор:** Строка длиной 127 символа(ов) **Значение по умолчанию:** Monitor Владелец этой записи. Рекомендуется начинать эту строку словом "monitor".

4. Нажмите **Apply**.

4.11.1.3 Удаление средства работы с данными, собираемыми при помощи RMON

Чтобы удалить средство работы с данными, собираемыми при помощи RMON, сделайте следующее:

1. Перейдите в ***Ethernet Stats » Configure RMON History Controls***. Появится таблица **RMON History Controls**.
2. Выберите в таблице средство работы с собираемыми данными. Появится форма **RMON History Controls**.
3. Нажмите **Delete**.

4.11.2 Управление оповещениями RMON

Если сконфигурированы оповещения дистанционного мониторинга, RUGGEDCOM ROS проверяет состояние конкретной статистической переменной.

Оповещения дистанционного мониторинга (RMON) определяют верхнюю и нижнюю границы для допустимых значений конкретных статистических переменных в заданном интервале. Это позволяет RUGGEDCOM ROS обнаруживать происходящие события быстрее, чем указанная максимальная скорость, и медленнее, чем минимальная скорость.

Если скорость изменения статистики значения выходит за пределы, всегда генерируется оповещение типа INFO (Информационное). Для получения информации о просмотре оповещений см. "Просмотр и сброс фиксированных оповещений (Страница 114)".

Кроме того, выход статистического параметра за пределы пороговых значений может привести к дальнейшим действиям. Оповещение RMON может быть настроено таким образом, чтобы указывать на конкретное событие RMON, которое способно генерировать trap-уведомление SNMP, запись в журнале событий, либо выполнять оба этих действия. Событие RMON также может направлять оповещения в сторону различных пользователей, определенных для SNMP.

Оповещение может указывать на различное событие для каждого порогового значения. Таким образом, возможны такие комбинации, как *trap on rising threshold (trap-уведомление при пороге по росту)* или *trap on rising threshold, log and trap on falling threshold (trap-уведомление при пороге по росту, регистрация и trap-уведомление при пороге по спаду)*.

Каждое оповещение RMON может быть настроено таким образом, чтобы его первый экземпляр возникал только при выходе за верхний предел, при выходе за нижний предел, либо при выходе за любое пороговое значение.

Возможность задавать верхнее и нижнее пороговые значения для величины измеряемого статистического параметра позволяет добавлять гистерезис к процессу генерирования оповещений.

Если величина измеряемого в течение некоторого времени статистического параметра сравнивается с единственным порогом, то оповещения будут генерироваться каждый раз, когда данный статистический параметр пересекает это единственное пороговое значение. Если величина статистического параметра совершает колебания возле порогового значения, то оповещение может генерироваться в течение каждого периода измерения. Программирование верхнего и нижнего пороговых значений устраняет ложные оповещения. Величина статистического параметра должна *переместиться* между порогами, прежде чем смогут генерироваться оповещения. Следующий рисунок иллюстрирует сильно различающиеся модели генерирования оповещения, которые являются результатом статистической выборки и той же статистической выборки с примененным гистерезисом.

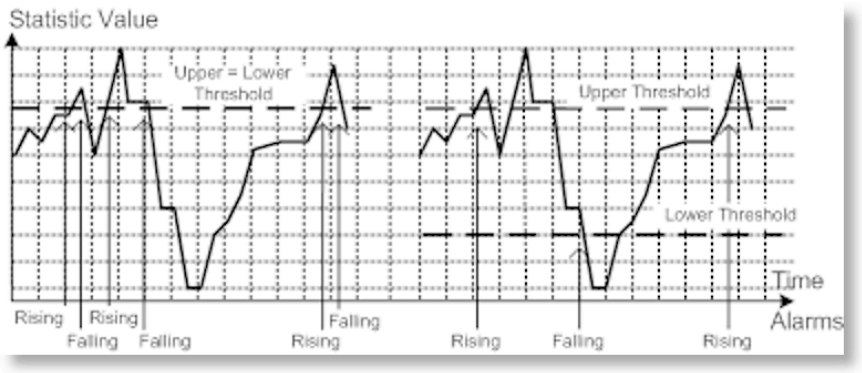


Рисунок 4.3 Процесс генерирования оповещений

Существует два способа оценки статистики, чтобы определить момент, когда нужно генерировать оповещение: разностный и абсолютный.

Для большинства статистических данных, например, ошибок линии связи, целесообразно генерировать оповещение, когда превышена определенная частота ошибок. По умолчанию регистрация записи оповещения настроена с *delta (разностным)* методом измерения, который рассматривает изменения статистического параметра в начале и в конце периода измерения.

Оповещение может потребоваться в случае, когда общее или абсолютное число событий выходит за определенное пороговое значение. В этом случае установите тип периода измерения *absolute (абсолютный)*.

4.11.2.1 Просмотр списка оповещений RMON

Чтобы просмотреть список оповещений RMON, перейдите в ***Ethernet Stats » Configure RMON Alarms***. Появится таблица **RMON Alarms**.

Если оповещения не были сконфигурированы, добавьте необходимые оповещения. Для получения дополнительной информации см. "Добавление оповещения RMON (Страница 101)".

4.11.2.2 Добавление оповещения RMON

Чтобы добавить оповещение RMON, сделайте следующее:

1. Перейдите в ***Ethernet Stats » Configure RMON Alarms***. Появится таблица **RMON Alarms**.
2. Нажмите **InsertRecord**. Появится форма **RMON Alarms**.

3. Необходимо сконфигурировать следующие параметры:

Параметр	Описание
`Index`	**Краткий обзор:** Целое число от 1 до 65535 **Значение по умолчанию:** 1 Указатель данной записи оповещения RMON.
`Variable`	**Краткий обзор:** Целое число Идентификатор объекта SNMP (OID) конкретного переменного параметра, выборка которого должна производиться. Может производиться выборка только тех переменных параметров, которые разрешаются в предусмотренный ASN.1 тип примитивов INTEGER (INTEGER, Integer32, Counter32, Counter64, Gauge, или TimeTicks). Список объектов можно увидеть, введя команду "rmon" в интерфейсе командной строки. Формат OID: objectName.index1.index2... , где формат указателя зависит от типа индексного объекта.
`Rising Thr`	**Краткий обзор:** Целое число от -2147483647 до 2147483647 **Значение по умолчанию:** 0 Пороговое значение переменного параметра, для которого производится выборка. Если текущее значение параметра, для которого производится выборка, больше этого порога или равно ему, а также значение на последнем интервале выборки было меньше этого порога, то будет генерироваться единственное событие. Кроме того, единственное событие будет генерироваться, если первая выборка, созданная после регистрации данной записи, превышает этот порог или равна ему, а также параметр "Startup Alarm" в этой записи имеет значение Rising (Рост). После генерирования оповещения о росте другое такое же событие не будет генерироваться, пока значение, выборка которого производится, не спадет ниже порогового и не достигнет значения порога по спаду.
`Falling Thr`	**Краткий обзор:** Целое число от -2147483647 до 2147483647 **Значение по умолчанию:** 0 Пороговое значение переменного параметра, для которого производится выборка. Если текущее значение параметра, для которого производится выборка, меньше этого порога или равно ему, а также значение на последнем интервале выборки было больше этого порога, то будет генерироваться единственное событие. Кроме того, единственное событие будет генерироваться, если первая выборка, созданная после регистрации данной записи, меньше этого порога или равна ему, а также параметр "Startup Alarm" в этой записи имеет значение Falling (Спад). После генерирования оповещения о спаде другое такое же событие не будет генерироваться, пока значение, выборка которого производится, не возрастет выше порогового и не достигнет значения порога по росту.

Параметр	Описание
`Value`	**Краткий обзор:** Целое число от -2147483647 до 2147483647 Значение объекта, мониторинг которого производится, в течение последнего периода выборки. Представление этого значения зависит от типа выборки ("абсолютная" или "разностная").
`Type`	**Краткий обзор:** [absolute | delta] **Значение по умолчанию:** delta Метод выборки для выбранного переменного параметра и вычисления значения для сравнения с пороговыми значениями. Значение типа выборки может быть "абсолютный" или "разностный".
`Interval`	**Краткий обзор:** Целое число от 0 до 2147483647 **Значение по умолчанию:** 60 Число секунд, в течение которых производится выборка данных и сравнивается с порогами по росту и по спаду.
`Startup Alarm`	**Краткий обзор:** [rising | falling | risingOrFalling] **Значение по умолчанию:** risingOrFalling Оповещение, которое может быть послано при первоначальном создании этой записи, если соблюдено условие для выдачи оповещения. Значение оповещения при запуске может быть "рост", "спад", "рост или спад".
`Rising Event`	**Краткий обзор:** Целое число от 0 до 65535 **Значение по умолчанию:** 0 Указатель события, которое используется при выходе за порог по спаду. Если в таблице событий нет соответствующей записи, то никаких ассоциаций не существует. В частности, если это значение равно нулю, то не будет генерироваться никакого ассоциированного события.
`Falling Event`	**Краткий обзор:** Целое число от 0 до 65535 **Значение по умолчанию:** 0 Указатель события, которое используется при выходе за порог по росту. Если в таблице событий нет соответствующей записи, то никаких ассоциаций не существует. В частности, если это значение равно нулю, то не будет генерироваться никакого ассоциированного события.
`Owner`	**Краткий обзор:** Строка длиной 127 символа(ов) **Значение по умолчанию:** Monitor Владелец этой записи. Рекомендуется начинать эту строку словом "monitor".

4. Нажмите **Apply**.

4.11.2.3 Удаление оповещения RMON

Чтобы удалить оповещение RMON, сделайте следующее:

1. Перейдите в ***Ethernet Stats » Configure RMON Alarms***. Появится таблица **RMON Alarms**.
2. Выберите оповещение из таблицы. Появится форма **RMON Alarms**.
3. Нажмите **Delete**.

4.11.3 Управление событиями RMON

События дистанционного мониторинга (RMON) определяют поведение профилей, используемых при регистрации событий. Эти профили используются оповещениями RMON для отправки trap-уведомлений и регистрации событий.

Каждый раз при возникновении события каждая регистрация записи может указывать, что запись в журнале сигналов тревоги создается от ее имени. Каждая запись также может указывать, что должно производиться уведомление посредством trap-уведомлений SNMP. В этом случае пользователь для trap-уведомления указывается как *Community (Строка-ключ)*.

Определены два trap-уведомления: risingAlarm (оповещение о росте) и fallingAlarm (оповещение о спаде)

4.11.3.1 Просмотр списка событий RMON

Чтобы просмотреть список событий RMON, перейдите в ***Ethernet Stats » Configure RMON Events***. Появится таблица **RMON Events**.

Если события не были сконфигурированы, добавьте необходимые события. Для получения дополнительной информации см. "Добавление события RMON (Страница 104)".

4.11.3.2 Добавление события RMON

Чтобы добавить оповещение RMON, сделайте следующее:

1. Перейдите в ***Ethernet Stats » Configure RMON Events***. Появится таблица **RMON Events**.
2. Нажмите **InsertRecord**. Появится форма **RMON Events**.
3. Необходимо сконфигурировать следующие параметры:

Параметр	Описание
`Index`	**Краткий обзор:** Целое число от 1 до 65535 **Значение по умолчанию:** 3 Указатель данной записи события RMON.

Параметр	Описание
`Type`	**Краткий обзор:** [none | log | snmpTrap | logAndTrap] **Значение по умолчанию:** logAndTrap Тип оповещения, которое модуль проверки будет выдавать об этом событии. В случае значения "log" для каждого события делается запись в таблице системного журнала RMON. В случае значения "snmp_trap" посылается trap-уведомление SNMP на одну или несколько станций администрирования.
`Community`	**Краткий обзор:** Строка длиной 31 символа(ов) **Значение по умолчанию:** public Если должно быть отправлено trap-уведомление SNMP, то этот параметр будет вписан в поле строки-ключа этого уведомления.
`Last Time Sent`	**Краткий обзор:** DDDD days, HH:MM:SS Значение времени (отсчитывается от последней перезагрузки) в тот момент, когда эта запись события в последний раз генерировала событие. Если эта запись не генерировала событий, то данное значение будет равно 0.
`Description`	**Краткий обзор:** Строка длиной 127 символа(ов) **Значение по умолчанию:** EV2-Rise Комментарий, описывающий это событие.
`Owner`	**Краткий обзор:** Строка длиной 127 символа(ов) **Значение по умолчанию:** Monitor Владелец этой записи события. Рекомендуется начинать эту строку словом "monitor".

4. Нажмите **Apply**.

4.11.3.3 Удаление события RMON

Чтобы удалить событие RMON, сделайте следующее:

1. Перейдите в ***Ethernet Stats » Configure RMON Events***. Появится таблица **RMON Events**.
2. Выберите событие из таблицы. Появится форма **RMON Events**.
3. Нажмите **Delete**.

4.12 Обновление микропрограммного обеспечения/возврат к более ранней версии микропрограммного обеспечения

В данном разделе описано, как обновить микропрограммное обеспечение для RUGGEDCOM ROS или вернуться к его более ранней версии.

4.12.1 Проверка хеш-сумм

Перед установкой нового микропрограммного обеспечения RUGGEDCOM ROS рекомендуется проверить хеш-сумму, чтобы убедиться, что микропрограммное обеспечение является подлинным и безошибочным.

Инструкции по проверке хеш-суммы, включая список хеш-сумм для всех устройств и версий RUGGEDCOM ROS, см. в FAQ по "хеш-суммам RUGGEDCOM ROS" (https://support.industry.siemens.com/cs/ww/en/view/109779935).

4.12.2 Обновление микропрограммного обеспечения

Чтобы получить доступ к новейшим функциям и исправлениям, может потребоваться обновить микропрограммное обеспечение RUGGEDCOM ROS включая основное микропрограммное обеспечение, микропрограммное обеспечение загрузчика операционной системы и микропрограммное обеспечение FPGA. Выпуски микропрограммного обеспечения, включая обновления, доступны при обращении в Службу поддержки на сайте Siemens Industry Online Support [https://support.industry.siemens.com]. Для получения дополнительной информации см. https://support.industry.siemens.com/My/ww/en/requests.

Двоичные образы микропрограммного обеспечения, переданные на устройство, хранятся в энергонезависимой флеш-памяти и требуют сброса устройства, чтобы вступить в действие.

⚠ ЗАМЕТКА
Если во время обновления установлен CLP, новая микропрограмма будет сохранена как во внутреннюю флэш-память, так и на CLP.

Примечание
В случае прерывания процесса обновления, возможно, из-за сбоя питания, RUGGEDCOM ROS можно восстановить, если до следующей перезагрузки установлен CLP с действительным образом микропрограммы (`main.bin`). RUGGEDCOM ROS скопирует образ микропрограммы во внутреннюю память и загрузится из нее.

Примечание
IP-адрес, заданный устройству, не будет изменен после обновления микропрограммы.

Примечание
Рекомендуется включить доступ к интерфейсу загрузчика во время этого процесса в случае необходимости аварийного восстановления (например, при отключении питания во время обновления). Для повышения безопасности Siemens рекомендует отключить доступ к загрузчику операционной системы после обновления. Для получения дополнительной информации об управление доступом к загрузчику операционной системы см. "Включение/

отключение доступа к интерфейсу загрузчика операционной системы (Страница 45)".

Чтобы обновить микропрограмму RUGGEDCOM ROS, сделайте следующее:

1. Включите доступ к интерфейсу загрузчика операционной системы. Для получения дополнительной информации см. "Включение/отключение доступа к интерфейсу загрузчика операционной системы (Страница 45)".
2. Загрузите на устройство другую версию двоичного образа микропрограммы или вставьте CLP, который содержит необходимый образ. Для получения дополнительной информации о выгрузке файлов см. "Выгрузка/загрузка файлов (Страница 59)".
3. Перезапустите устройство, чтобы завершить установку. Для получения дополнительной информации см. "Перезапуск устройства (Страница 108)".
4. Войдите в оболочку CLI и убедитесь, что новая версия программного обеспечения установлена, введя **`version`**. Отображаются текущие установленные версии основной микропрограммы и микропрограммы начальной загрузки.

   ```
   >version
   Current ROS-MPC83 Main Software v5.5.0 (Jan 01 5.5 00:01)
   ```

5. Отключите доступ к интерфейсу загрузчика операционной системы. Для получения дополнительной информации см. "Включение/отключение доступа к интерфейсу загрузчика операционной системы (Страница 45)".

4.12.3 Возврат к более ранней версии микропрограммного обеспечения

Как правило, возврат к более ранней версии микропрограммного обеспечения RUGGEDCOM ROS не рекомендуется, поскольку это может иметь непредсказуемые последствия. Если, тем не менее, вы хотите вернуться к более ранней версии, то сделайте следующее:

Примечание
Перед возвратом к более ранней версии микропрограммного обеспечения убедитесь в том, что коды типов аппаратного обеспечения и FPGA, установленных в устройстве, поддерживаются старой версией микропрограммного обеспечения. Обратитесь за подтверждением к документации с информацией о соответствующей версии микропрограммного обеспечения.

Примечание
Не производите возврат к более ранней версии для загрузчика RUGGEDCOM ROS.

1. Отключите устройство от сети.
2. Войдите в систему устройства в качестве администратора. Для получения дополнительной информации см. "Вход в систему (Страница 22)".

3. Сделайте локальную копию текущего файла конфигурации. Для получения дополнительной информации см. "Выгрузка/загрузка файлов (Страница 59)".

   ⚠ ЗАМЕТКА

   Опасность для конфигурации — риск нарушения обмена данными

   Не понижайте версию микропрограммного обеспечения при включенном шифровании до версии, не поддерживающей шифрование.

4. Восстановите на устройстве заводские настройки по умолчанию. Для получения дополнительной информации см. "Восстановление заводских настроек по умолчанию (Страница 57)".
5. Загрузите и приведите в активное состояние старую версию микропрограммного обеспечения и связанные с ней файлы FPGA, используя те же методы, которые применяются для установки новых версий микропрограммного обеспечения. Для получения дополнительной информации см. "Обновление микропрограммного обеспечения (Страница 106)".
6. Нажмите **Ctrl-S**, чтобы перейти к командной строке.
7. Очистите все журналы, введя:

   ```
   clearlogs
   ```

8. Очистите все оповещения, введя:

   ```
   clearalarms
   ```

   ⚠ ЗАМЕТКА

   Угроза безопасности — риск неавторизованного доступа и/или использования

   После возврата к более ранней версии микропрограммного обеспечения и файлов FPGA имейте в виду, что некоторые настройки из предыдущей конфигурации могут быть потеряны или сброшены в настройки по умолчанию (включая пароли пользователя при возврате от защищенной версии), поскольку соответствующие таблицы или поля могут отсутствовать в старой версии микропрограммного обеспечения. По этой причине после возврата к старой версии устройство должно быть сконфигурировано.

9. Сконфигурируйте устройство требуемым образом.

4.13 Перезапуск устройства

Чтобы перезагрузить устройство, сделайте следующее:

1. Перейдите в ***Diagnostics » Reset Device***. Появится форма **Reset Device**.

2. Нажмите **Confirm**.

4.14 Вывод устройства из эксплуатации

Перед отключением устройства на постоянной основе или для проведения технического обслуживания третьей стороной необходимо проделать процедуру его полного вывода из эксплуатации. Это включает удаление всей конфиденциальной информации.

Чтобы снять устройство с эксплуатации, сделайте следующее:

1. Отключите от устройства все сетевые кабели.
2. Подключитесь к устройству через последовательный консольный порт RS-232. Для получения дополнительной информации см. "Подключение напрямую (Страница 51)".
3. Восстановите заводские настройки устройства. Для получения дополнительной информации см. "Восстановление заводских настроек по умолчанию (Страница 57)".
4. Перейдите в командную строку. Для получения дополнительной информации см. "Использование интерфейса командной строки (Страница 27)".
5. Выгрузите на устройство пустую версию файла `banner.txt`, чтобы заменить существующий файл. Для получения дополнительной информации о выгрузке файлов см. "Выгрузка/загрузка файлов (Страница 59)".
6. Убедитесь в успешной выгрузке, введя:

   ```
   type banner.txt
   ```

7. Удалите системные журналы и журналы фатальных сбоев, введя:

   ```
   clearlog
   ```

8. Сгенерируйте случайный SSL-сертификат, введя:

   ```
   sslkeygen
   ```

   На завершение этой операции может потребоваться несколько минут. Чтобы убедиться, что сертификат был сгенерирован, введите:

   ```
   type syslog.txt
   ```

   Когда в журнале появляется фраза `Generated ssl.crt was saved`, это означает, что SSL-сертификат был создан.

9. Сгенерируйте случайные SSH-ключи, введя:

   sshkeygen

   На завершение этой операции может потребоваться несколько минут. Чтобы убедиться, что ключи были сгенерированы, введите:

   type syslog.txt

   Когда в журнале появляется фраза Generated ssh.keys was saved, это означает, что SSH-ключи были сгенерированы.

10. Выполните дефрагментацию и стирание всей свободной флеш-памяти, введя:

    flashfile defrag

    На завершение этой операции может потребоваться несколько минут.

5 Администрирование системы

В данном разделе описывается выполнение различных административных задач, связанных с идентификацией устройства, разрешениями пользователей, конфигурированием оповещений, сертификатами и ключами и т. д.

5.1 Конфигурирование системной информации

Чтобы сконфигурировать базовую информацию, которая может использоваться для идентификации устройства, его расположения и/или владельца, сделайте следующее:

1. Перейдите в ***Administration » Configure System Identification***. Появится форма **System Identification**.
2. Необходимо сконфигурировать следующие параметры:

Параметр	Описание
`System Name`	**Краткий обзор:** Строка длиной 24 символа(ов) Имя системы отображается на всех RUGGEDCOM ROS экранах меню. Это может облегчить идентификацию коммутаторов в вашей сети при том условии, что каждому коммутатору присвоено уникальное имя.
`Location`	**Краткий обзор:** Строка длиной 49 символа(ов) Этот параметр можно использовать для указания физического местонахождения коммутатора. Местонахождение отображается на экране входа в систему в качестве дополнительного средства, позволяющего убедиться в том, что вы имеете дело с требуемым коммутатором.
`Contact`	**Краткий обзор:** Строка длиной 49 символа(ов) Контактные данные можно использовать для облегчения идентификации лица, отвечающего за администрирование данного коммутатора. Вы можете ввести имя, номер телефона, адрес электронной почты и т. п. Эти сведения отображаются на экране входа в систему, чтобы к данному лицу можно было обратиться, если потребуется помощь.

3. Нажмите **Apply**.

5.2 Настройка экрана входа в систему

Чтобы показать созданное пользователем сообщение-приветствие, информацию об устройстве или любую другую информацию на странице входа в систему для веб- и консольных интерфейсов, добавьте текст в файл `banner.txt`.

Если файл `banner.txt` пуст, то на странице входа в систему появятся только поля для ввода **Username** и **Password**.

Чтобы обновить файл `banner.txt`, загрузите его с устройства, измените и снова загрузите на устройство. Для получения информации о загрузке и выгрузке файлов см. "Выгрузка/загрузка файлов (Страница 59)".

Кроме того, файл `banner.txt` можно обновить с помощью CLI-команды **`banner`**. Для получения дополнительной информации см. "Доступные CLI-команды (Страница 27)".

5.3 Включение/отключение веб-интерфейса

В некоторых случаях пользователю может потребоваться отключить веб-интерфейс для повышения кибербезопасности.

Чтобы отключить или включить веб-интерфейс, сделайте следующее:

Примечание
Веб-интерфейс можно отключить через веб-интерфейс пользователя, сконфигурировав параметр Web Server Users Allowed (Допустимое количество пользователей веб-сервера) в форме **IP Services form**. Для получения дополнительной информации см. "Конфигурирование IP-сервисов (Страница 96)".

---

1. Войдите в систему устройства в качестве администратора и перейдите в командную оболочку CLI. Для получения дополнительной информации о порядке доступа к командной оболочке CLI см. "Использование интерфейса командной строки (Страница 27)".
2. Перейдите в ***Administration » Configure IP Services » Web Server Users Allowed***.
3. Выберите **Disabled**, чтобы отключить веб-интерфейс, или укажите допустимое количество пользователей веб-сервера, чтобы включить интерфейс.

5.4 Управление оповещениями

Оповещения указывают на регистрируемые устройством происходящие важные или значимые события.

Существует два типа оповещений:

- **Активные оповещения** обозначают состояния функционирования, которые не соответствуют нормальному режиму работы. К примерам активных оповещений относятся ситуации, когда не действуют каналы связи, по которым должно быть установлено соединение, либо постоянно имеют место частоты появления ошибок, превосходящие определенный порог. Активные оповещения активны постоянно и удаляются (очищаются) только путем устранения исходной причины соответствующего оповещения.
- **Пассивные оповещения** являются ретроспективными по своей природе. Они обозначают события, представляющие собой аномальные условия в прошлом и не влияющие на текущее рабочее состояние. К примерам пассивных оповещений относятся ошибки аутентификации, генерируемые базой MIB дистанционного мониторинга (RMON) оповещения или частоты появления ошибок, которые лишь временно превышают определенный порог. Эти оповещения можно сбросить из списка оповещений.

Примечание
Для получения дополнительной информации об оповещениях RMON см. "Управление оповещениями RMON (Страница 99)".

Когда имеет место любое из этих оповещений, в правом верхнем углу интерфейса пользователя отображается сообщение. Если имеет место более одного оповещения, в сообщении будет показано количество оповещений. Активные оповещения также приводят к срабатыванию светодиодного индикатора сухих контактов аварийной сигнализации. Сообщение и индикатор будут активны до тех пор, пока оповещение не будет сброшено.

Примечание
Оповещения являются непостоянными по своей природе. Все оповещения (активные и пассивные) удаляются при запуске.

5.4.1 Просмотр списка предварительно сконфигурированных оповещений

Чтобы просмотреть оповещения, предварительно сконфигурированные для устройства, перейдите в ***Diagnostic » Configure Alarms***. Появится таблица **Alarms**.

Примечание
Этот список оповещений (конфигурируемых и неконфигурируемых) доступен через интерфейс командной строки с помощью команды **`alarms`**. Для получения дополнительной информации см. "Доступные CLI-команды (Страница 27)".

Для получения информации об изменении предварительно сконфигурированного оповещения см. "Конфигурирование оповещения (Страница 114)".

5.4.2 Просмотр и сброс фиксированных оповещений

Чтобы просмотреть список оповещений, предварительно сконфигурированных на фиксацию, перейдите в ***Diagnostics » View Latched Alarms***. Появится таблица **Latched Alarms**.

Чтобы сбросить пассивные оповещения из списка, сделайте следующее:

1. Перейдите в ***Diagnostics » Clear Latched Alarms***. Появится форма **Clear Latched Alarms**.
2. Нажмите **Confirm**.

5.4.3 Конфигурирование оповещения

Все оповещения предварительно сконфигурированы на устройстве, однако их можно изменить под конкретное применение. К таким изменениям относятся включение/отключение определенных функций и изменение времени обновления.

Чтобы сконфигурировать оповещение, сделайте следующее:

⚠ ЗАМЕТКА

Оповещения уровней Critical (Критические) и Alert (Предупреждающие) нельзя сконфигурировать или отключить.

1. Перейдите в ***Diagnostic » Configure Alarms***. Появится таблица **Alarms**.
2. Выберите оповещение. Появится форма **Alarms**.
3. Необходимо сконфигурировать следующие параметры:

Параметр	Описание
`Name`	**Краткий обзор:** Строка длиной 34 символа(ов) или [sys_alarm] **Значение по умолчанию:** sys_alarm Имя оповещения (например, в том виде, как оно получено через команду CLI: **`alarms`**).
`Level`	**Краткий обзор:** [EMRG | ALRT | CRIT | ERRO | WARN | NOTE | INFO | DEBG] Уровень серьезности оповещения: • `EMRG (АВАРИЯ)` - серьезный отказ устройства, который привел к перезагрузке системы. • `ALRT (ТРЕВОГА)` - серьезный отказ устройства, который не привел к перезагрузке системы. • `CRIT (КРИТИЧЕСКИЙ)` - имеет место серьезная неустранимая проблема с устройством. • `ERRO (ОШИБКА)` - имеет место устранимая проблема с устройством, которая не оказывает серьезного влияния на функционирование.

Параметр	Описание
	• `WARN (ПРЕДУПРЕЖДЕНИЕ)` - возможная серьезная проблема, влияющая на функционирование системы в целом. • `NOTE (УВЕДОМЛЕНИЕ)` - обнаружено условие, которое не предусмотрено или не разрешено. • `INFO (ИНФОРМАЦИЯ)` - событие, которое является элементом нормального функционирования, например, холодный запуск, вход пользователя в систему и т.п. • `DEBG (ОТЛАДКА)` - предназначен только для отладки на заводе-изготовителе. Этот параметр не конфигурируется.
`Latch`	**Краткий обзор:** [On | Off] **Значение по умолчанию:** Off Включает фиксацию появления данного оповещения в таблице оповещений.
`Trap`	**Краткий обзор:** [On | Off] **Значение по умолчанию:** Off Разрешает отправку SNMP-уведомления для данного оповещения.
`Log`	**Краткий обзор:** [On | Off] **Значение по умолчанию:** Off Разрешает регистрацию появления данного оповещения в файле syslog.txt.
`LED & Relay`	**Краткий обзор:** [On | Off] **Значение по умолчанию:** Off Включает светодиодную индикацию и срабатывание реле для этого оповещения. Если фиксация не включена, то это поле останется пустым.
`Refresh Time`	**Краткий обзор:** Целое число от 0 до 60 **Значение по умолчанию:** 60 Время обновления для данного оповещения.

4. Нажмите **Apply**.

5.4.4 Конфигурирование оповещений цифрового входа

Оповещения цифрового входа позволяют пользователям контролировать внешнее оборудование, такое как реле, пассивные коммутаторы или входы прямого напряжения. Система CyberKnife RUGGEDCOM RST916C предлагает два изолированных независимых цифровых входа, каждый из которых связан со специальным оповещением, определенным вRUGGEDCOM ROS. Первый цифровой вход (DI1+ и DI-) связан с оповещением 1, а второй цифровой вход (DI2+ и DI-) связан с оповещением 2.

Каждое оповещение срабатывает, когда соответствующий цифровой вход находится в состоянии "высокий" или "низкий", в зависимости от конфигурации оповещения.

Примечание
Для получения дополнительной информации о подключении цифровых входов к RUGGEDCOM RST916C см. Руководство по установке.

Чтобы сконфигурировать оповещение цифрового входа, сделайте следующее:

1. Перейдите в ***Diagnostics » Configure Digital Input Alarm***. Появится таблица **Digital Input Alarm**.
2. Выберите оповещение. Появится форма **Digital Input Alarm**.
3. Необходимо сконфигурировать следующие параметры:

Параметр	Описание
`ID`	**Краткий обзор:** Целое число от 1 до 2 Идентификатор оповещения для этого цифрового входа.
`Alarm`	**Краткий обзор:** [Disabled | Enabled] Включение или отключение оповещения для этого цифрового входа.
`Active`	**Краткий обзор:** [Low | High] Состояние, которое активирует оповещение для этого цифрового входа.
`Delay On`	**Краткий обзор:** Целое число от 10 до 3600 или [0] Время, в течение которого вход должен быть неактивен, прежде чем оповещение будет отключено.
`Delay Off`	**Краткий обзор:** Целое число от 10 до 3600 или [0] Время, в течение которого вход должен быть неактивен, прежде чем оповещение будет отключено.
`Description`	**Краткий обзор:** Строка длиной 24 символа(ов) Строка описания для оповещения.
`Input`	**Краткий обзор:** [Low | High] Текущее состояние входа считывается с аппаратного обеспечения.
`Status`	**Краткий обзор:** [On | Off] Текущее состояние оповещения.

4. Нажмите **Apply**.

5.4.5 Оповещения системы защиты для аутентификации при входе в систему

В RUGGEDCOM ROS предусмотрены различные опции входа в систему, связанные с аутентификацией при входе в систему. Пользователь может войти

в систему устройства под управлением RUGGEDCOM ROS, используя один из 4 методов: Web, консоль, SSH или Telnet. RUGGEDCOM ROS может регистрировать сообщения в системном журнале, посылать trap-уведомление для извещения SNMP-администратора и/или выдавать оповещение, когда имеет место событие успешного и неуспешного входа в систему. Кроме того, когда на устройстве сконфигурирован ненадежный пароль, либо недоступен первичный сервер аутентификации для TACACS+ или RADIUS, RUGGEDCOM ROS будет выдавать оповещения, отправлять trap-уведомления SNMP и регистрировать сообщения в системном журнале.

Ниже приведен список сообщений системного журнала и сообщений-оповещений, относящихся к аутентификации пользователя:

- Создан ненадежный пароль
- Информация о входе в систему и выходе из системы
- Чрезмерно много неудачных попыток входа в систему
- Сервер RADIUS недоступен
- Сервер TACACS недоступен
- Неправильный ответ сервера TACACS
- Ошибка SNMP-аутентификации

Примечание
Все оповещения и сообщения системного журнала, относящиеся к аутентификации при входе в систему, являются конфигурируемыми. Для получения дополнительной информации о конфигурировании оповещений см. "Конфигурирование оповещения (Страница 114)".

Создан ненадежный пароль

RUGGEDCOM ROS генерирует это оповещение и регистрирует сообщение в системном журнале, когда в таблице **Passwords** создается ненадежный пароль.

Имя сообщения	Оповещение	SNMP trap-уведомление	Системный журнал
Создан ненадежный пароль	Да	Да	Да

Используются ключи по умолчанию

RUGGEDCOM ROS генерирует это оповещение и регистрирует сообщение в системном журнале, когда используются ключи шифрования по умолчанию. Для получения дополнительной информации о ключах по умолчанию см. "Управление ключами и сертификатами SSH/SSL (Страница 151)".

Примечание
Для неконтролируемых (NC) версий RUGGEDCOM ROS это оповещение генерируется лишь в том случае, когда используются ключи SSL по умолчанию.

Имя сообщения	Оповещение	SNMP trap-уведомление	Системный журнал
Используются ключи по умолчанию	Да	Да	Да

Информация о входе в систему и выходе из системы

RUGGEDCOM ROS генерирует это оповещение и регистрирует сообщение в системном журнале, когда имеют место успешные и неуспешные попытки входа в систему. Также в системном журнале регистрируется сообщение, когда пользователь с определенным уровнем привилегий выходит из системы.

Попытки входа в систему регистрируются независимо от способа, посредством которого пользователь получает доступ к устройству (т. е. SSH, Web, консоль, Telnet или RSH). Однако при выходе пользователя из системы сообщение регистрируется лишь в том случае, когда пользователь осуществлял доступ к устройству через SSH, Telnet или консоль.

Имя сообщения	Оповещение	SNMP trap-уведомление	Системный журнал
Успешный вход в систему	Да	Да	Да
Вход в систему не выполнен	Да	Да	Да
Выход пользователя из системы	Нет	Нет	Да

Чрезмерно много неудачных попыток входа в систему

RUGGEDCOM ROS генерирует это оповещение и регистрирует сообщение в системном журнале после 10 неудачных попыток входа пользователя в систему в течение пяти минут. Кроме того, служба, к которой попытался получить доступ пользователь, будет заблокирована на один час, чтобы предотвратить дальнейшие попытки.

Имя сообщения	Оповещение	SNMP trap-уведомление	Системный журнал
Чрезмерно много неудачных попыток входа в систему	Да	Да	Да

Сервер RADIUS недоступен

RUGGEDCOM ROS генерирует это оповещение и регистрирует сообщение в системном журнале, когда первичный сервер RADIUS недоступен.

Имя сообщения	Оповещение	SNMP trap-уведомление	Системный журнал
Первичный сервер RADIUS недоступен	Да	Да	Да

Сервер TACACS+ недоступен

RUGGEDCOM ROS генерирует это оповещение и регистрирует сообщение в системном журнале, когда первичный сервер TACACS+ недоступен.

Имя сообщения	Оповещение	SNMP trap-уведомление	Системный журнал
Первичный сервер TACACS недоступен	Да	Да	Да

Неправильный ответ сервера TACACS+

RUGGEDCOM ROS генерирует это оповещение и регистрирует сообщение в системном журнале, когда от сервера TACACS+ получен ответ с неправильным CRC.

Имя сообщения	Оповещение	SNMP trap-уведомление	Системный журнал
Неправильный ответ сервера TACACS	Да	Да	Да

Ошибка SNMP-аутентификации

RUGGEDCOM ROS генерирует это оповещение, посылает trap-уведомление об ошибке аутентификации и регистрирует сообщение в системном журнале, когда программный продукт для управления сетью пытается взаимодействовать с SNMP-агентом RUGGEDCOM ROS, используя неверные идентификационные данные.

Имя сообщения	Оповещение	SNMP trap-уведомление	Системный журнал
Ошибка SNMP-аутентификации	Да	Да	Да

5.4.6 Список оповещений

В следующей таблице перечислены все возможные оповещения RUGGEDCOM ROS и указано, может ли пользователь сконфигурировать оповещение.

Для получения дополнительной информации о конфигурировании оповещений см. "Конфигурирование оповещения (Страница 114)".

Имя	Уровень	Фиксация	Trap-уведомление	Системный журнал	Светодиоды и реле	Конфигурируется пользователем
Пароль администратора изменен	Примечание	Выкл.	Вкл.	Вкл.	Выкл.	Y

Имя	Уровень	Фиксация	Trap-уведомление	Системный журнал	Светодиоды и реле	Конфигурируется пользователем
Передача Bootp — cfg не выполнена	Ошибка	Вкл.	Вкл.	Вкл.	Вкл.	N
Ошибка начальной загрузки	Критический	Вкл.	Выкл.	Вкл.	Вкл.	N
Дребезг контактов в линии связи	Критический	Вкл.	Вкл.	Вкл.	Вкл.	N
Защита BPDU активирована	Ошибка	Вкл.	Вкл.	Вкл.	Вкл.	Y
Несогласованная скорость портов группы	Ошибка	Вкл.	Вкл.	Вкл.	Вкл.	N
Недостаточно ресурсов для ClkMgr	Предупреждение	Вкл.	Нет	Вкл.	Вкл.	N
Ошибка основного источника ClkMgr	Предупреждение	Вкл.	Выкл.	Вкл.	Вкл.	N
Конфигурация изменена	Info (Информация)	Выкл.	Вкл.	Вкл.	Выкл.	Y
Журнал фатальных сбоев создан	Критический	Вкл.	Выкл.	Нет	Вкл.	N
Парольная строка хранилища данных изменена	Примечание	Выкл.	Вкл.	Вкл.	Выкл.	Y
Ошибка чтения дочерней платы	Критический	Вкл.	Вкл.	Вкл.	Вкл.	N
Ошибка устройства	Критический	Вкл.	Вкл.	Выкл.	Вкл.	N
Оповещение безопасности DHCP	Предупреждение	Вкл.	Вкл.	Вкл.	Вкл.	Y
Чрезмерно много неудачных попыток входа в систему	Предупреждение	Вкл.	Вкл.	Вкл.	Вкл.	Y
Быстрое определение ганала связи отключено	Критический	Вкл.	Вкл.	Вкл.	Вкл.	N
Передача файла выполнена	Примечание	Выкл.	Вкл.	Вкл.	Выкл.	N
GMRP не может запомнить больше адресов	Предупреждение	Вкл.	Вкл.	Вкл.	Вкл.	Y
Пароль уровня "гость" изменен	Примечание	Выкл.	Вкл.	Вкл.	Выкл.	Y
Ошибка массива данных	Предупреждение	Вкл.	Выкл.	Вкл.	Вкл.	N
Ошибка BMC IEEE1588	Предупреждение	Вкл.	Вкл.	Выкл.	Выкл.	Y
Состояние удержания IEEE1588	Предупреждение	Вкл.	Вкл.	Выкл.	Выкл.	Y
Таблица состава групп IGMP заполнена	Предупреждение	Вкл.	Вкл.	Вкл.	Вкл.	Y
Таблица пересылки IGMP Mcast заполнена	Предупреждение	Вкл.	Вкл.	Вкл.	Вкл.	Y
Несоответствие скорости/dpx в транке	Ошибка	Вкл.	Вкл.	Вкл.	Вкл.	Y
Прерывистый канал связи	Ошибка	Вкл.	Вкл.	Вкл.	Вкл.	N
Недопустимая конфигурации	Критический	Вкл.	Выкл.	Выкл.	Вкл.	N
Канал связи работоспособен/не работоспособен	Предупреждение	Вкл.	Вкл.	Вкл.	Вкл.	Y

Имя	Уровень	Фиксация	Trap-уведомление	Системный журнал	Светодиоды и реле	Конфигурируется пользователем
Таблица удаленного LLDP изменена	Info (Информация)	Выкл.	Вкл.	Вкл.	Выкл.	N
Локальная консоль отключена	Примечание	Выкл.	Вкл.	Вкл.	Выкл.	N
Локальная консоль включена	Примечание	Выкл.	Вкл.	Вкл.	Выкл.	N
Вход в систему не выполнен	Info (Информация)	Вкл.	Вкл.	Вкл.	Выкл.	Y
Информация о входе в систему	Info (Информация)	Вкл.	Вкл.	Вкл.	Выкл.	Y
Авторизации MAC-адреса не выполнена	Ошибка	Вкл.	Выкл.	Вкл.	Вкл.	Y
MAC-адрес не запомнен	Предупреждение	Вкл.	Вкл.	Вкл.	Вкл.	Y
Таблица фильтрации Mcast CPU заполнена	Предупреждение	Вкл.	Вкл.	Вкл.	Вкл.	Y
Многократная ошибка MRM кольца MRP Inst 1	Предупреждение	Вкл.	Вкл.	Вкл.	Вкл.	Y
Односторонняя ошибка Rx кольца MRP Inst 1	Предупреждение	Вкл.	Вкл.	Вкл.	Вкл.	Y
Кольцо MRP Inst 1 разомкнуто	Предупреждение	Вкл.	Вкл.	Вкл.	Вкл.	Y
Порт кольца MRP Inst 1 разъединен	Предупреждение	Вкл.	Вкл.	Вкл.	Вкл.	Y
Многократная ошибка MRM кольца MRP Inst 2	Предупреждение	Вкл.	Вкл.	Вкл.	Вкл.	Y
Односторонняя ошибка Rx кольца MRP Inst 2	Предупреждение	Вкл.	Вкл.	Вкл.	Вкл.	Y
Кольцо MRP Inst 2 разомкнуто	Предупреждение	Вкл.	Вкл.	Вкл.	Вкл.	Y
Порт кольца MRP Inst 2 разъединен	Предупреждение	Вкл.	Вкл.	Вкл.	Вкл.	Y
Многократная ошибка MRM кольца MRP Inst 3	Предупреждение	Вкл.	Вкл.	Вкл.	Вкл.	Y
Односторонняя ошибка Rx кольца MRP Inst 3	Предупреждение	Вкл.	Вкл.	Вкл.	Вкл.	Y
Кольцо MRP Inst 3 разомкнуто	Предупреждение	Вкл.	Вкл.	Вкл.	Вкл.	Y
Порт кольца MRP Inst 3 разъединен	Предупреждение	Вкл.	Вкл.	Вкл.	Вкл.	Y
Многократная ошибка MRM кольца MRP Inst 4	Предупреждение	Вкл.	Вкл.	Вкл.	Вкл.	Y
Односторонняя ошибка Rx кольца MRP Inst 4	Предупреждение	Вкл.	Вкл.	Вкл.	Вкл.	Y
Кольцо MRP Inst 4 разомкнуто	Предупреждение	Вкл.	Вкл.	Вкл.	Вкл.	Y
Порт кольца MRP Inst 4 разъединен	Предупреждение	Вкл.	Вкл.	Вкл.	Вкл.	Y
Новая активная топология STP	Info (Информация)	Выкл.	Вкл.	Выкл.	Выкл.	N
Новый корень STP	INFO (ИНФОРМАЦИЯ)	Выкл.	Выкл.	Выкл.	Выкл.	Y

Имя	Уровень	Фиксация	Trap-уведомление	Системный журнал	Светодиоды и реле	Конфигурируется пользователем
Состояние службы NTP изменено	Info (Информация)	Вкл.	Вкл.	Вкл.	Выкл.	Y
Пароль уровня "оператор" изменен	Примечание	Выкл.	Вкл.	Вкл.	Выкл.	Y
Порт помещен в карантинную VLAN	Примечание	Вкл.	Выкл.	Вкл.	Вкл.	Y
Нарушена защита порта	Предупреждение	Вкл.	Вкл.	Вкл.	Вкл.	Y
Смещение часов PTP превышает допустимый предел	Info (Информация)	Выкл.	Вкл.	Вкл.	Выкл.	N
Гроссмейстерские часы PTP изменены	Info (Информация)	Выкл.	Вкл.	Вкл.	Выкл.	N
Шаг времени ведущего устройства PTP изменен	Info (Информация)	Выкл.	Вкл.	Вкл.	Выкл.	N
Служба PTP запущена	Info (Информация)	Выкл.	Вкл.	Вкл.	Выкл.	N
Служба PTP остановлена	Info (Информация)	Выкл.	Вкл.	Вкл.	Выкл.	N
Ключ аутентификации RADIUS изменен	Примечание	Выкл.	Вкл.	Вкл.	Выкл.	Y
Состояние службы RADIUS изменено	Info (Информация)	Вкл.	Вкл.	Вкл.	Выкл.	Y
Сбой часов реального времени	Ошибка	Вкл.	Выкл.	Вкл.	Вкл.	N
BPDU с обратной связью	Ошибка	Вкл.	Вкл.	Вкл.	Вкл.	Y
Оповещение RMON	Info (Информация)	Вкл.	Выкл.	Вкл.	Вкл.	N
Оповещение совместимости с ROS FPGA	Предупреждение	Вкл.	Выкл.	Вкл.	Выкл.	N
Низкий уровень буфера Rx	Примечание	Вкл.	Выкл.	Вкл.	Вкл.	N
Оповещение SFP	Ошибка	Вкл.	Вкл.	Вкл.	Вкл.	N
Ключ аутентификации SNMP изменен	Примечание	Выкл.	Вкл.	Вкл.	Выкл.	Y
Ошибка SNMP-аутентификации	Предупреждение	Вкл.	Вкл.	Вкл.	Выкл.	Y
Строка-ключ SNMP изменена	Примечание	Выкл.	Вкл.	Вкл.	Выкл.	Y
Секретный ключ SNMP изменен	Примечание	Выкл.	Вкл.	Вкл.	Выкл.	Y
Ошибка добавления открытого ключа пользователя SSH	Предупреждение	Вкл.	Вкл.	Вкл.	Вкл.	Y
Переполнение стека	Предупреждение	Вкл.	Выкл.	Вкл.	Вкл.	N
События STP	Info (Информация)	Выкл.	Выкл.	Вкл.	Выкл.	Y
Изменение топологии STP	Info (Информация)	Выкл.	Выкл.	Выкл.	Выкл.	Y
Ключ аутентификации Tacacs+ изменен	Примечание	Выкл.	Вкл.	Вкл.	Выкл.	Y
Неправильный ответ TACACS+	Предупреждение	Вкл.	Вкл.	Вкл.	Вкл.	Y
Состояние службы TACACS+ изменено	Info (Информация)	Вкл.	Вкл.	Вкл.	Выкл.	Y

Имя	Уровень	Фиксация	Trap-уведомление	Системный журнал	Светодиоды и реле	Конфигурируется пользователем
Не удалось получить IP-адрес	Критический	Вкл.	Вкл.	Вкл.	Вкл.	N
Неизвестный privKey от пользователя SNMPv3	Предупреждение	Вкл.	Вкл.	Вкл.	Выкл.	Y
Неразрешенная скорость	Ошибка	Вкл.	Вкл.	Вкл.	Вкл.	N
Сброс сторожевого таймера	Предупреждение	Вкл.	Выкл.	Вкл.	Вкл.	N
WeakPswdAdmin	Предупреждение	Вкл.	Вкл.	Вкл.	Выкл.	Y
WeakPswdGuest	Предупреждение	Вкл.	Вкл.	Вкл.	Выкл.	Y
WeakPswdOper	Предупреждение	Вкл.	Вкл.	Вкл.	Выкл.	Y
WeakRadiusBackupKey	Предупреждение	Вкл.	Вкл.	Вкл.	Выкл.	Y
WeakRadiusPrimaryKey	Предупреждение	Вкл.	Вкл.	Вкл.	Выкл.	Y
WeakSnmpAuthKey	Предупреждение	Вкл.	Вкл.	Вкл.	Выкл.	Y
WeakSnmpPrivKey	Предупреждение	Вкл.	Вкл.	Вкл.	Выкл.	Y
WeakSSHKey	Предупреждение	Вкл.	Вкл.	Вкл.	Выкл.	Y
WeakSSLKey	Предупреждение	Вкл.	Вкл.	Вкл.	Выкл.	Y
WeakTacacsBackupKey	Предупреждение	Вкл.	Вкл.	Вкл.	Выкл.	Y
WeakTacacsPrimaryKey	Предупреждение	Вкл.	Вкл.	Вкл.	Выкл.	Y

5.5 Управление файлом конфигурации

Файл конфигурации устройства для RUGGEDCOM ROS — это текстовый ASCII файл с расширением CSV (значение, разделенное запятой) с именем `config.csv`. Его можно загрузить с устройства для просмотра и сравнения с другими файлами конфигурации, а также для сохранения резервной копии. Его также можно перезаписать путем выгрузки на устройство полного или частичного файла конфигурации.

Чтобы предотвратить неавторизованный доступ к содержимому файла конфигурации, его можно зашифровать с помощью пароля/парольной строки.

5.5.1 Конфигурирование шифрования данных

Чтобы зашифровать файл конфигурации и защитить его с помощью пароля/парольной строки, сделайте следующее:

Примечание
Шифрование данных недоступно для неконтролируемых (NC) версий RUGGEDCOM ROS . При переключении между контролируемой и неконтролируемой (NC) версиями RUGGEDCOM ROS убедитесь в том, что

шифрование отключено. В противном случае NC-версия RUGGEDCOM ROS будет игнорировать зашифрованный файл конфигурации и загрузит заводские настройки по умолчанию.

Примечание
Шифруются только конфигурационные данные. Все команды и имена таблиц в файле конфигурации сохраняются в виде нешифрованного текста.

Примечание
Если файл конфигурации переносится на другие устройства, то убедитесь в том, что на всех устройствах сконфигурирована одна и та же парольная строка. В противном случае файл конфигурации будет отвергнут.

Примечание
Шифрование должно быть отключено перед возвратом устройства в компанию Siemens или передачей файла конфигурации в Службу поддержки клиентов.

⚠ ЗАМЕТКА

Опасность для конфигурации — риск нарушения обмена данными

Не понижайте версию программного обеспечения RUGGEDCOM ROS ниже RUGGEDCOM ROS v5.5 при включенном шифровании. Перед возвратом к более ранней версии программного обеспечения убедитесь в том, что на устройстве были восстановлены заводские настройки по умолчанию.

1. Перейдите в ***Administration » Configure Data Storage***. Появится форма **Data Storage**.
2. Необходимо сконфигурировать следующие параметры:

Параметр	Описание
`Encryption`	**Краткий обзор:** [On | Off] Включает/выключает шифрование данных в файле конфигурации.
`Passphrase`	**Краткий обзор:** Строка длиной 31 символа(ов) Эта парольная строка используется в качестве секретного ключа для шифрования конфигурационных данных. Зашифрованные данные могут быть дешифрованы любым устройством, сконфигурированным с такой же парольной строкой.
`Confirm Passphrase`	**Краткий обзор:** Строка длиной 31 символа(ов) Эта парольная строка используется в качестве секретного ключа для шифрования конфигурационных данных. Зашифрованные данные могут быть дешифрованы любым устройством, сконфигурированным с такой же парольной строкой.

3. Нажмите **Apply**.

5.5.2 Обновление файла конфигурации

После загрузки с устройства файл конфигурации может быть обновлен с помощью различных инструментов:

Примечание
Для получения информации о выгрузке и загрузке файлов см. "Выгрузка/загрузка файлов (Страница 59)".

- Любые программы для редактирования текста, способные читать и записывать файлы в кодировке ASCII
- Инструменты для обнаружения различий/коррекции файлов (например, утилиты командной строки UNIX *diff* и *patch*)
- Системы управления исходным кодом (например, CVS, SVN)

⚠ ЗАМЕТКА

Опасность для конфигурации — риск потери данных

Не редактируйте зашифрованный файл конфигурации. Любая строка, которая редактировалась вручную, будет игнорироваться.

RUGGEDCOM ROS также способна принимать частичные обновления конфигурации. Например, чтобы обновить параметры конфигурации только для Ethernet-порта 1 без изменения каких-либо других параметров, передайте на устройство файл, который содержит лишь следующие строки:

```
# Port Parameters
ethPortCfg
Port,Name,Media,State,AutoN,Speed,Dupx,FlowCtrl,LFI,Alarm,
1,Port 1,100TX,Enabled,On,Auto,Auto,Off,Off,On,
```

5.6 Управление MMS

RUGGEDCOM ROS поддерживает протокол MMS (спецификация производственных сообщений) стандарта МЭК 61850.

5.6.1 Основные сведения о протоколе MMS

RUGGEDCOM ROS поддерживает стандарт МЭК 61850 — протокол управления и мониторинга для интеллектуальных электронных устройств (ИЭУ) на электрических подстанциях. Стандарт использует в качестве транспортного протокола протокол MMS (спецификация производственных сообщений), а объектная модель коммутатора определяет объекты, подлежащие опросу или конфигурированию.

Протокол MMS указывает службы для обмена данными в реальном времени между сетевыми устройствами и компьютерными приложениями. Он обеспечивает базовую систему обмена сообщениями между промышленными устройствами.

Модель данных, используемая протоколом MMS, основана на логических узлах, содержащих набор объектов данных. Эти объекты данных содержат набор атрибутов данных.

5.6.1.1 Составление отчетов MMS

Функция отчета МЭК 61850 используется для агрегирования объектов данных из логических узлов. Эти объекты данных можно отправлять клиенту в виде необусловленного событийно-управляемого отчета, инициируемого клиентом.

Отчет MMS основывается на параметре *MMS Sessions Allowed (Допустимое количество сеансов MMS)*, который контролирует количество клиентов, которые могут одновременно создать соединения MMS с коммутатором под управлением RUGGEDCOM ROS. Для получения дополнительной информации о конфигурировании составления отчетов MMS см. "Конфигурирование IP-сервисов (Страница 96)".

5.6.1.2 Отчеты/наборы данных

RUGGEDCOM ROS поддерживает следующие типы отчетов/наборов данных:

- **LLDPStatus**

  Основанный на времени отчет, принадлежащий логическому узлу LPLD, указывающий состояние LLDP устройства. Он включает три объекта данных: LPLD.RemPortId (идентификатор удаленного порта), LPLD.RemChsId (идентификатор шасси удаленного порта) и LPLD.RemAddr (адрес управления удаленной системой).

- **PortLinkStatus**

  Основанный на событиях отчет, принадлежащий логическому узлу LPCP, который указывает состояние блока доступа к среде (MAU) физического порта. Он включает объект данных LPCP.Mau (статус канала связи блока доступа к среде).

- **PortStatistics**

  Основанный на времени отчет, принадлежащий логическому узлу LPCP, который указывает рабочее состояние физического порта. Он включает четыре объекта данных: LPCP.AutoNgt (при значении true (истина), порт находится в режиме автосогласования), LPCP.RxCnt (количество сообщений, полученных с момента прошлого сброса), LPCP.TxCnt (количество сообщений, отправленных с момента прошлого сброса) и LPCP.FerPort (частота появления ошибочных кадров на порте).

- **RSTPStatus**

  Основанный на событиях отчет, принадлежащий логическому узлу LBRI, указывающий состояние RSTP устройства. Он включает три объекта данных: LBRI.RstpRoot (устройство является корнем RSTP или нет), LBRI.RstpTopoCnt (счетчик изменений топологи RSTP) и LBSP.RstpSt (состояние порта RSTP).

- **SystemStatus**

  Основанный на событиях отчет, принадлежащий логическому узлу LPHD, который указывает рабочее состояние устройства. Он включает два объекта данных: LPHD.PhyHealth (состояние устройства) и LPHD.PwrSupAlm (состояние оповещения источника питания устройства).

Примечание
Файлы `ruggedcom.icd` (МЭК 61850, описание возможностей ИЭУ для устройства) и `ruggedcom.iid` (МЭК 61850, инстанциированное описание ИЭУ для устройства) содержат список логических узлов, поддерживаемых RUGGEDCOM ROS. Для получения информации о загрузке этих файлов см. "Выгрузка/загрузка файлов (Страница 59)".

5.6.1.3 Поддерживаемые логические узлы

RUGGEDCOM ROS поддерживает следующие логические узлы:

Логический узел	Описание
LLN0	Общий логический узел, обеспечивающий общую информацию об устройстве в целом, например, информация о поставщике и версия программного обеспечения.
LPHD (физическое устройство)	Информация об уровне системы, несущем логические узлы, относящаяся к физическому устройству, например, имя системы и описание системы.
LBRI (мост)	Логический узел, обеспечивающий информацию, относящуюся к связующему дереву, если устройство используется в качестве моста, например, приоритет RSTP и интервал между приветствиями RSTP.
LPCP (порт физической связи)	Логический узел, который обеспечивает относящуюся к порту информацию для каждого физического интерфейса устройства, например, состояние администрирования порта и состояние автосогласования порта.
LPLD (обнаружение канала порта)	Логический узел, который предоставляет относящуюся к порту информацию о протоколе обнаружения канального уровня (LLDP) для каждого физического интерфейса устройства, например, идентификатор локального порта и идентификатор удаленного порта.
LBSP (Порт связующего дерева моста)	Логический узел, который обеспечивает относящуюся к порту информацию о связующем дереве для каждого физического интерфейса устройства, например, состояние порта RSTP и состояние граничного порта RSTP.
LCMF (фильтрация MAC-адреса канала связи)	Логический узел, несущий информацию о фильтрации групповых MAC-адресов, например, список разрешенных групповых MAC-адресов и связанных идентификаторов сетей VLAN.
LCVF (фильтрация каналов связи сети VLAN)	Логический узел, обеспечивающий относящуюся к порту информацию о конфигурации сети VLAN, например, идентификатор порта VLAN или приоритет CoS.

5.6.2 Просмотр списка предварительно сконфигурированных отчетов MMS

Чтобы просмотреть отчеты MMS, предварительно сконфигурированные для устройства, перейдите в ***Administration » Configure MMS***. Появится таблица **MMS Report Configuration**.

В этой таблице отображается следующая информация:

Параметр	Описание
`Name`	**Краткий обзор:** Строка длиной 32 символа(ов) или [SysStatus] **Значение по умолчанию:** SysStatus Имя отчета MMS (например, имя набора данных).
`Status`	**Краткий обзор:** [Disabled | Enabled] **Значение по умолчанию:** Disabled Статус составления отчетов MMS, запущенный или измененный клиентским приложением. Если какое-либо клиентское приложение активирует функцию составления отчетов о наборе данных, статус этого набора данных устанавливается на Enabled (Включено). Если ни одно клиентское приложение не активирует функцию составления отчетов о наборе данных, статус этого набора данных устанавливается на Disabled (Отключено).
`EventDriven`	**Краткий обзор:** [False | True] **Значение по умолчанию:** True Критерий составления отчетов: • `True (Истинно)` - составление отчета основано на событиях • `False (Ложно)` - составление отчета основано на времени
`Period`	**Краткий обзор:** Целое число от 30 до 1080 или [Disabled] **Значение по умолчанию:** 300 Интервал составления отчета в секундах для отчетов, основанных на времени. Этот параметр установлен на Disabled (Отключено) для отчетов, основанных на событиях.

Для получения информации об изменении отчета MMS см. "Конфигурирование отчета MMS (Страница 128)".

5.6.3 Конфигурирование отчета MMS

Все отчеты MMS предварительно сконфигурированы на устройстве, однако их можно изменить под конкретное применение. К таким изменениям относятся включение/отключение определенных отчетов и изменение интервала составления отчетов.

Чтобы сконфигурировать отчет MMS, сделайте следующее:

1. Перейдите в ***Administration » Configure MMS***. Появится таблица **MMS Report Configuration**.

2. Выберите отчет. Появится форма **MMS Report Configuration**.
3. Необходимо сконфигурировать следующие параметры:

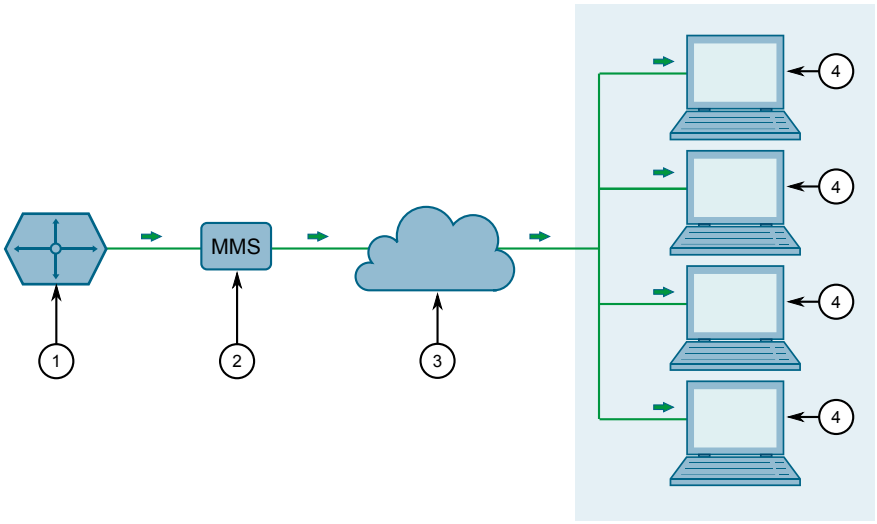
Параметр	Описание
`Period`	**Краткий обзор:** Целое число от 30 до 1080 или [Disabled] **Значение по умолчанию:** 300 Интервал составления отчета в секундах для отчетов, основанных на времени. Этот параметр установлен на Disabled (Отключено) для отчетов, основанных на событиях.

4. Нажмите **Apply**.

5.6.4 Пример: Конфигурирование отчетов MMS

В данном примере рассматривается, как сконфигурировать устройство на генерирование отчетов MMS.

Приведенная ниже топология описывает сценарий, при котором четырем клиентам в ЛВС отправляются отчеты MMS от RUGGEDCOM ROS:



① RUGGEDCOM ROS
② Отчет MMS
③ LAN
④ Клиент

Рисунок 5.1 Топология — MMS

Чтобы сконфигурировать устройство на получение отчетов MMS, выполните указанные ниже действия:

1. Действия на стороне клиента:

   Примечание
   Конфигурация клиента зависит от используемого клиента MMS. Подробные сведения о конфигурации см. в руководстве по эксплуатации от OEM-производителя.

   a. Включите или отключите отчеты MMS в соответствии с вашими предпочтениями. Список доступных в RUGGEDCOM ROS отчетов см. в "Отчеты/наборы данных (Страница 126)".

   b. Сконфигурируйте устройство на предоставление отчетов на основе событий или отчетов на основе времени.

2. Выполните следующие действия в RUGGEDCOM ROS:

   a. Сконфигурируйте допустимое количество сеансов MMS, чтобы указать, сколько клиентов будут получать отчеты. На каждую топологию допускается 4 сеанса. Для получения дополнительной информации о конфигурировании сеансов MMS см. "Конфигурирование IP-сервисов (Страница 96)".

   b. Если на стороне клиента выбраны отчеты на основе времени, сконфигурируйте необходимый временной интервал составления отчетов. Для получения дополнительной информации см. "Конфигурирование отчета MMS (Страница 128)".

3. Чтобы проверить конфигурацию, необходимо убедиться, что каждый клиент получает отчеты MMS от устройства в соответствии с конфигурацией.

6 Безопасность

В данном разделе описывается конфигурирование функций безопасности RUGGEDCOM ROS и управление ими.

6.1 Конфигурирование паролей

Чтобы сконфигурировать пароли для одного или нескольких профилей пользователя, сделайте следующее:

1. Перейдите в ***Administration » Configure Passwords***. Появится форма **Configure Passwords**.

Примечание
Все пароли пользователей в RUGGEDCOM ROS должны соответствовать установленным требованиям, чтобы не допустить использования ненадежных паролей. При создании нового пароля убедитесь в том, что он соответствует следующим требованиям:

- Длина должна быть не менее 8 символов.
- Не должен содержать в себе имя пользователя или любые 4 символа, которые присутствуют в имени пользователя и идут один за другим. Например, в случае имени пользователя *Subnet25* нельзя использовать пароль *subnet25admin*, *subnetadmin* или *net25admin*. Однако допускаются пароли *net-25admin* или *Sub25admin*.
- Должен содержать хотя бы один буквенный символ и одну цифру. Допускаются специальные символы.
- Не должен содержать более 3 последовательно возрастающих или убывающих цифр. Например, пароли *Sub123* и *Sub19826* допускаются, а *Sub12345* не допускается.

Если сконфигурирован ненадежный пароль, то будет генерироваться оповещение. Оповещение в связи с ненадежным паролем может быть отключено пользователем. Для получения дополнительной информации об отключении оповещений см. "Управление оповещениями (Страница 112)".

---

2. Необходимо сконфигурировать следующие параметры:

Параметр	Описание
`Auth Type`	**Краткий обзор:** [Local | RADIUS | TACACS+ | RADIUSorLocal | TACACS+orLocal] **Значение по умолчанию:** Local Аутентификация по паролю может осуществляться с использованием локально сконфигурированных значений, удаленного сервера RADIUS или удаленного сервера TACACS+. Настройка этого значения для одной из комбинаций, которые включают в себя RADIUS или TACACS +, требует наличия сконфигурированной таблицы сервера защиты. Настройки: • `Local` - аутентификация из локальной таблицы паролей. • `RADIUS` - аутентификация с использованием сервера RADIUS только для сетевого доступа (HTTP/HTTPS, SSH, RSH, Telnet). Для консольного доступа аутентификацию необходимо выполнить из локальной таблицы паролей. Если при локальной аутентификации произойдет сбой, выполните аутентификацию с помощью сервера RADIUS. • `TACACS+` - аутентификация с использованием сервера TACACS+ только для сетевого доступа (HTTP/HTTPS, SSH, RSH, Telnet). Для консольного доступа аутентификацию необходимо выполнить из локальной таблицы паролей. Если при локальной аутентификации произойдет сбой, выполните аутентификацию с помощью сервера TACACS+. • `RADIUSOrLocal` - аутентификация с использованием RADIUS. Если сервер недоступен, то аутентификация производится из локальной таблицы паролей. • `TACACS+OrLocal` - аутентификация с использованием TACACS+. Если сервер недоступен, то аутентификация производится из локальной таблицы паролей.
`Guest Username`	**Краткий обзор:** Строка длиной 15 символа(ов) **Значение по умолчанию:** guest Соответствующий пароль находится в поле пароля пользователя из категории "гость"; разрешен только просмотр, не может изменять настройки или запускать какие-либо команды.
`Guest Password`	**Краткий обзор:** Строка длиной 19 символа(ов) Соответствующее имя пользователя находится в поле имени пользователя из категории "гость"; разрешен только просмотр, не может изменять настройки или запускать какие-либо команды.
`Confirm Guest Password`	**Краткий обзор:** Строка длиной 19 символа(ов) Соответствующее имя пользователя находится в поле имени пользователя из категории "гость"; разрешен только

Параметр	Описание
	просмотр, не может изменять настройки или запускать какие-либо команды.
`Operator Username`	**Краткий обзор:** Строка длиной 15 символа(ов) **Значение по умолчанию:** operator Соответствующий пароль находится в поле пароля пользователя из категории "оператор"; не может изменять настройки, может сбрасывать оповещения, статистику, системные журналы и т. п.
`Operator Password`	**Краткий обзор:** Строка длиной 19 символа(ов) Соответствующее имя пользователя находится в поле имени пользователя из категории "оператор"; не может изменять настройки, может сбрасывать оповещения, статистику, системные журналы и т. п.
`Confirm Operator Password`	**Краткий обзор:** Строка длиной 19 символа(ов) Соответствующее имя пользователя находится в поле имени пользователя из категории "оператор"; не может изменять настройки, может сбрасывать оповещения, статистику, системные журналы и т. п.
`Admin Username`	**Краткий обзор:** Строка длиной 15 символа(ов) **Значение по умолчанию:** admin Соответствующий пароль находится в поле пароля пользователя из категории "администратор"; полный доступ для чтения/записи ко всем настройкам и командам.
`Admin Password`	**Краткий обзор:** Строка длиной 19 символа(ов) Соответствующее имя пользователя находится в поле имени пользователя из категории "администратор"; полный доступ для чтения/записи ко всем настройкам и командам.
`Confirm Admin Password`	**Краткий обзор:** Строка длиной 19 символа(ов) Соответствующее имя пользователя находится в поле имени пользователя из категории "администратор"; полный доступ для чтения/записи ко всем настройкам и командам.
`Password Minimum Length`	**Краткий обзор:** Целое число от 1 до 17 **Значение по умолчанию:** 1 Сконфигурируйте минимальную длину строки пароля. Новый пароль, не соответствующий требованиям к длине, будет отклонен.

3. Нажмите **Apply**.

6.2 Очистка конфиденциальных данных

Если параметр установлен на enabled (включено), во время загрузки системы пользователь сможет удалить все хранящиеся на устройстве конфиденциальные данные и ключи, а также сбросить все имена пользователей и пароли к заводским настройкам.

Чтобы очистить конфиденциальные данные, сделайте следующее:

Примечание
Команды, используемые в следующей процедуре, являются чувствительными по времени. При превышении указанных пределов времени до предоставления подходящего ответа устройство продолжит выполнять нормальную загрузку.

1. Подключитесь к устройству через последовательный консольный порт RS-232. Для получения дополнительной информации см. "Подключение напрямую (Страница 51)".
2. Выключите и снова включите питание устройства. Во время загрузки появится следующий запрос:

   ```
   Press any key to start
   ```

3. В течение четырех секунд нажмите **CTRL** + **r**. Появится баннер доступа, за которым последует приглашение на ввод команды:

   ```
   >
   ```

4. Введите следующую команду и нажмите **Enter** в течение 30 секунд:

   ```
   clear private data
   ```

5. При запросе "Вы уверены, что хотите очистить конфиденциальные данные? (Да/Нет)?", ответьте *yes (да)* и нажмите **Enter** в течение пяти секунд. Вся конфигурация и ключи во флеш-памяти будут обнулены. В журнале событий будет создана запись. Файлы crashlog.txt (если имеются) и файлы syslog.txt будут сохранены. Устройство автоматически перезагрузится.

6.3 Управление аутентификацией пользователей

В данном разделе приведено описание различных методов аутентификации пользователей.

6.3.1 Методы аутентификации

RUGGEDCOM ROS поддерживает следующие варианты аутентификации: локальную, на RADIUS сервере, на TACACS+ сервере, на RADIUS сервере или локальную и на TACAS+ сервере или локальную. Выбранный метод настраивается с помощью параметра `Auth Type`.

Для получения дополнительной информации о конфигурировании параметра `Auth Type` см. "Конфигурирование паролей (Страница 131)".

В следующей таблице показаны возможности доступа пользователей в различных сценариях с использованием поддерживаемых методов аутентификации.

Тип аутентификации	Метод/сценарий аутентификации	Учетные данные для доступа в систему	Метод доступа	
			Локальная консоль	Сеть (SSH/ Telnet/WebUI)
Локальный	Локальная аутентификация	Локальный	✓	✓
	Аутентификация сервера RADIUS	RADIUS	×	×
RADIUS	Аутентификация сервера RADIUS	RADIUS	✓	✓
	Локальная аутентификация	Локальный	✓	✓
	Сервер недоступен	Локальный	✓	×
		RADIUS	×	×
	Неверный общий ключ	Локальный	✓	×
		RADIUS	×	×
	Неправильный порт назначения	Локальный	✓	×
		RADIUS	×	×
TACACS+	Аутентификация сервера TACACS+	TACACS+	✓	✓
	Локальная аутентификация	Локальный	✓	✓
	Сервер недоступен	Локальный	✓	×
		TACACS+	×	×
	Неверный общий ключ	Локальный	✓	×
		TACACS+	×	×
	Неправильный порт назначения	Локальный	✓	×
		TACACS+	×	×
RADIUSorLocal	Аутентификация сервера RADIUS	RADIUS	✓	✓
	Локальная аутентификация	Локальный	×	×
	Сервер недоступен	Локальный	✓	✓
		RADIUS	×	×
	Неверный общий ключ	Локальный	×	×
		RADIUS	×	×
	Неправильный порт назначения	Локальный	✓	✓
		RADIUS	×	×
TACACS+ или локальный	Аутентификация сервера TACACS+	TACACS+	✓	✓
	Локальная аутентификация	Локальный	×	×
	Сервер недоступен	Локальный	✓	✓
		TACACS+	×	×
	Неверный общий ключ	Локальный	×	×
		TACACS+	×	×

Тип аутентификации	Метод/сценарий аутентификации	Учетные данные для доступа в систему	Метод доступа	
			Локальная консоль	Сеть (SSH/ Telnet/WebUI)
	Неправильный порт назначения	Локальный	✓	✓
		TACACS+	×	×

6.3.2 Конфигурирование расширений имен пользователей

Если настроена аутентификация пользователей с помощью RADIUS или TACACS +, RUGGEDCOM ROS можно настроить на добавление важной для сервера аутентификации информации к каждому имени пользователя. Сюда может входить IP-адрес NAS, имя системы, расположение системы или любой другой определенный пользователем текст.

Если параметр **Username Extension** оставлен пустым, на сервер аутентификации будет посылаться только имя пользователя.

Примечание
Расширения игнорируются, если включена аутентификация IEEE 802.1x на базе порта. RUGGEDCOM ROS останется прозрачной и не будет вносить изменений в имя пользователя. Для получения дополнительной информации об аутентификации IEEE 802.1x см. "Концепция безопасности на уровне порта (Страница 142)".

Чтобы сконфигурировать расширение имени пользователя, сделайте следующее:

1. Перейдите в ***Administration » Configure Security Server » Configure Common Security Parameters***. Появится форма **Common Security Parameters**.
2. Необходимо сконфигурировать следующие параметры:

Параметр	Описание
`Username Extension`	**Краткий обзор:** Строка длиной 127 символа(ов) Определяет формат всех имен пользователей, отправленных на RADIUS или сервер TACACS+ для аутентификации. К имени пользователя можно добавить префикс или суффикс с помощью предопределенных ключевых слов (заключенных в ограничители %) или определенные пользователем строки. Заключенные в ограничители значения включают: %Username%: имя, связанное с профилем пользователя (например, admin, oper и т. д.) %IPaddr%: управляющий IP-адрес коммутатора, действующий в качестве сервера сетевого доступа (NAS). %SysName%: имя системы, присвоенное устройству. %SysLocation%: расположение системы, присвоенное устройству.

Параметр	Описание
	Все предопределенные ключевые слова чувствительны к регистру. Примеры: %Username%@ABC.com %Username%_%SysLocation% Если расширение не определено, на сервер аутентификации посылается только имя пользователя.

3. Нажмите **Apply**.

6.3.3 Управление аутентификацией RADIUS

RUGGEDCOM ROS можно сконфигурировать на функционирование в качестве клиента RADIUS и переслать учетные данные пользователя на сервер RADIUS (служба дистанционной аутентификации пользователей) для удаленной аутентификации и авторизации.

Служба RADIUS представляет собой протокол прикладного уровня, работающий поверх UDP транспорта, используемый для переноса аутентификационной, авторизационной и конфигурационной информации между сервером сетевого доступа (NAS), которому требуется аутентифицировать свои каналы связи, и коллективно используемым сервером аутентификации. Она обеспечивает аутентификацию и авторизацию для сетевого доступа.

Служба RADIUS также широко используется в сочетании со стандартом IEEE 802.1X для обеспечения безопасности на уровне портов с использованием расширяемого протокола аутентификации (EAP).

Примечание
RADIUS-сообщения передаются как UDP-сообщения. Коммутатор и сервер RADIUS должны использовать одинаковый ключ аутентификации и шифрования.

Примечание
RUGGEDCOM ROS поддерживает как защищенный расширяемый протокол аутентификации (PEAP), так и протокол EAP-MD5. Протокол PEAP является более защищенным и рекомендован к использованию, если его поддерживает запрашивающее устройство.

Примечание
Для получения дополнительной информации о протоколе RADIUS см. RFC 2865 [http://tools.ietf.org/html/rfc2865].

Для получения дополнительной информации о расширяемом протоколе аутентификации (EAP) см. RFC 3748 [http://tools.ietf.org/html/rfc3748].

6.3.3.1 Конфигурирование сервера RADIUS

Примечание
Информацию по конфигурированию сервера RADIUS см. в инструкции изготовителя конфигурируемого сервера.

Специфический для производителя атрибут (VSA), посылаемый на сервер RADIUS как часть запроса, используется для определения уровня доступа от сервера RADIUS. Этот атрибут можно сконфигурировать в рамках сервера RADIUS со следующей информацией:

Атрибут	Значение
Специфический для производителя	Идентификатор производителя: 15004 Формат: String 2 Атрибут: { Guest, Operator, Admin } (Гость, Оператор, Администратор)

Примечание
Если в ответном пакете от сервера RADIUS отсутствует уровень доступа, доступ не разрешается.

6.3.3.2 Конфигурирование клиента RADIUS на устройстве

Клиент RADIUS можно сконфигурировать на использование двух серверов RADIUS: первичного и резервного. Если первичный сервер недоступен, устройство автоматически попытается подключиться к резервному серверу.

⚠ ЗАМЕТКА

RADIUS-клиент использует протокол аутентификации по паролю (PAP) для проверки корректности доступа. Другие протоколы аутентификации не поддерживаются.

CLI-команды, относящиеся к конфигурированию RADIUS-клиента на устройстве, см. в "Доступные CLI-команды (Страница 27)".

Чтобы сконфигурировать доступ к первичному или резервному серверу RADIUS, сделайте следующее:

1. Перейдите в ***Administration » Configure Security Server » Configure RADIUS Server***. Появится **RADIUS Server Table**.
2. Выберите в таблице **Primary** или **Backup**. Появится форма **RADIUS Server**.

3. Необходимо сконфигурировать следующие параметры:

Параметр	Описание
`Server`	**Краткий обзор:** Строка длиной 8 символа(ов) или [Primary] **Значение по умолчанию:** Primary Это поле указывает, предназначена ли данная настройка для первичного или для резервного сервера.
`IP Address`	**Краткий обзор:** Any valid IP address IP-адрес сервера.
`Auth UDP Port`	**Краткий обзор:** Целое число от 1 до 65535 **Значение по умолчанию:** 1812 IP-порт на сервере.
`Max Retry`	**Краткий обзор:** Целое число от 1 до 10 **Значение по умолчанию:** 2 Максимальное количество попыток аутентификатора связаться с сервером аутентификации, чтобы аутентифицировать пользователя в случае какой-либо ошибки.
`Timeout`	**Краткий обзор:** Целое число от 1000 до 120000 **Значение по умолчанию:** 10000 Время в миллисекундах, в течение которого аутентификатор будет ожидать ответа от сервера аутентификации.
`Reachable`	**Краткий обзор:** [No | Yes] Статус сервера.
`Auth Key`	**Краткий обзор:** Строка длиной 31 символа(ов) Ключ аутентификации для совместного использования с сервером.
`Confirm Auth Key`	**Краткий обзор:** Строка длиной 31 символа(ов) Ключ аутентификации для совместного использования с сервером.

4. Нажмите **Apply**.

6.3.4 Управление аутентификацией TACACS+

TACACS+ (Система управления доступом к терминалам и контроллерам) представляет собой протокол управления доступом на основе TCP, который обеспечивает сервисы аутентификации, авторизации и учета на маршрутизаторах, серверах сетевого доступа (NAS) и других сетевых вычислительных устройствах через один или несколько центральных серверов.

6.3.4.1 Конфигурирование TACACS+

RUGGEDCOM ROS можно сконфигурировать на использование двух серверов TACACS+: первичного и резервного. Если первичный сервер недоступен, устройство автоматически попытается подключиться к резервному серверу.

CLI-команды, относящиеся к конфигурированию TACACS+, см. в "Доступные CLI-команды (Страница 27)".

Чтобы сконфигурировать доступ к первичному или резервному серверу TACACS+, сделайте следующее:

1. Перейдите в ***Administration » Configure Security Server » Configure TacPlus Server » Configure TACACS Plus Server***. Появится **TACACS Plus Server Table**.
2. Выберите в таблице **Primary** или **Backup**. Появится форма **TACACS Plus Server**.
3. Необходимо сконфигурировать следующие параметры:

Параметр	Описание
`Server`	**Краткий обзор:** Строка длиной 8 символа(ов) или [Primary] **Значение по умолчанию:** Primary Это поле указывает, предназначена ли данная настройка для первичного или для резервного сервера.
`IP Address`	**Краткий обзор:** Any valid IP address IP-адрес сервера.
`Auth TCP Port`	**Краткий обзор:** Целое число от 1 до 65535 **Значение по умолчанию:** 49 IP-порт на сервере.
`Max Retry`	**Краткий обзор:** Целое число от 1 до 10 **Значение по умолчанию:** 3 Максимальное количество попыток аутентификатора связаться с сервером аутентификации, чтобы аутентифицировать пользователя в случае какой-либо ошибки.
`Timeout`	**Краткий обзор:** Целое число от 1000 до 120000 **Значение по умолчанию:** 10000 Время в миллисекундах, в течение которого аутентификатор будет ожидать ответа от сервера аутентификации.
`Reachable`	**Краткий обзор:** [No | Yes] Статус сервера.
`Auth Key`	**Краткий обзор:** Строка длиной 31 символа(ов) или [mySecret] **Значение по умолчанию:** mySecret Ключ аутентификации для совместного использования с сервером.

Параметр	Описание
`Confirm Auth Key`	**Краткий обзор:** Строка длиной 31 символа(ов) Ключ аутентификации для совместного использования с сервером.

4. Установите уровни привилегий для каждого типа пользователя (администратор, оператор или гость). Для получения дополнительной информации см. "Конфигурирование привилегий пользователей (Страница 141)".
5. Нажмите **Apply**.

6.3.4.2 Конфигурирование привилегий пользователей

Каждый запрос TACACS+ на аутентификацию включает атрибут *priv_lvl*, который используется для предоставления доступа к устройству. По умолчанию атрибут использует следующие диапазоны, как определено в файле конфигурации TACACS+:

- `15` представляет уровень доступа *admin* (администратор)
- `2-14` представляет уровень доступа *operator (оператор)*
- `1` представляет уровень доступа *guest (гость)*

CLI-команда `svcmod` используется для конфигурирования привилегий пользователя. Вводимые значения должны соответствовать одной или нескольким опциям, численно определенным (от 0 до 15) в файле конфигурации TACACS+, расположенном на сервере TACACS+.

Для получения дополнительной информации о CLI-команде `svcmod` см. "Доступные CLI-команды (Страница 27)".

Чтобы сконфигурировать уровни привилегий для каждого типа пользователя, сделайте следующее:

1. Перейдите в ***Administration » Configure Security Server » Configure TacPlus Server » Configure TACPLUS Serv Privilege Config***. Появится форма **TACPLUS Serv Privilege Config**.
2. Необходимо сконфигурировать следующие параметры:

Параметр	Описание
`Admin Priv`	**Краткий обзор:** Целое число от 0 до 15 или a range (e.g. 2-14) **Значение по умолчанию:** 15 Уровень привилегий, присвоенный пользователю.
`Oper Priv`	**Краткий обзор:** Целое число от 0 до 15 или a range (e.g. 2-14) **Значение по умолчанию:** 2-14 Уровень привилегий, присвоенный пользователю.

Параметр	Описание
`Guest Priv`	**Краткий обзор:** Целое число от 0 до 15 или a range (e.g. 2-14) **Значение по умолчанию:** 1 Уровень привилегий, присвоенный пользователю.

3. Нажмите **Apply**.

6.4 Управление безопасностью на уровне порта

Система безопасности на уровне порта или контроль доступа к портам предусматривает возможности фильтровать или принимать трафик от определенных MAC-адресов.

Система безопасности на уровне порта контролирует MAC-адреса источника в принимаемых кадрах и проверяет их соответствие списку MAC-адресов, разрешенных для данного порта. Неразрешенные кадры будут отфильтрованы и, в качестве варианта, принявший такие кадры порт будет отключен постоянно или на указанный период времени. Будет выдано оповещение, указывающее на обнаруженный неавторизованный MAC-адрес.

Кадры для неизвестных адресов назначения рассылаются через защищенные порты.

6.4.1 Концепция безопасности на уровне порта

В данном разделе рассматриваются некоторые принципы, имеющие значение для реализации безопасности на уровне порта в RUGGEDCOM ROS.

6.4.1.1 Аутентификация на базе статического MAC-адреса

Используя этот метод, коммутатор сравнивает MAC-адреса источника в принятых кадрах с содержанием таблицы статических MAC-адресов.

RUGGEDCOM ROS также поддерживает очень гибкую конфигурацию защиты порта, которая обеспечивает сетевым администраторам удобные средства для использования этой функции в различных сетевых сценариях.

Статический MAC-адрес можно сконфигурировать, не указывая явно номер порта. В этом случае сконфигурированный MAC-адрес будет автоматически разрешен для того порта, на котором он обнаружен. Это позволяет подключать устройства к любому защищенному порту коммутатора, не требуя какого-либо реконфигурирования.

Коммутатор можно также настроить для запоминания (и, следовательно, авторизации) предварительно заданного числа первых MAC-адресов источника, поступивших на защищенный порт. Это позволяет накапливать

надлежащие безопасные адреса при первоначальной настройке авторизации на базе статического MAC-адреса для определенного порта. Эти MAC-адреса автоматически вставляются в таблицу статических MAC-адресов и остаются там, пока пользователь не удалит их явным образом.

6.4.1.2 Аутентификация на базе статического MAC-адреса в кольце MRP

Если безопасность на уровне порта сконфигурирована на MRC, MAC-адрес портов кольца MRM должен быть сконфигурирован в таблице **Static MAC Addresses**, чтобы кольцо оставалось замкнутым.

Чтобы разрешить связь (ping) между устройствами MRP в кольце, каждое устройство с включенной на его портах MRP безопасностью на уровне порта должно содержать MAC-адреса всех устройств в кольце в его таблице **Static MAC Addresses**.

Для получения информации о конфигурировании MRP см. "Управление протоколом резервирования среды передачи (MRP) (Страница 253)".

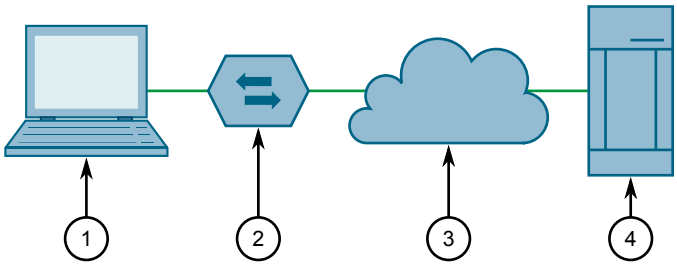
Для получения информации о конфигурировании статического MAC-адреса см. "Добавление статического MAC-адреса (Страница 180)".

6.4.1.3 Аутентификация IEEE 802.1x

Стандарт IEEE 802.1x определяет механизм для контроля доступа к сети на базе портов, а также предусматривает средства аутентификации и авторизации устройств, присоединяемых к портам локальной сети.

Хотя стандарт IEEE 802.1x чаще всего используется в беспроводных сетях, этот метод также реализован в коммутаторах с проводными соединениями.

В стандарте IEEE 802.1x определены три основных компонента метода аутентификации: Supplicant (запрашивающее устройство), Authenticator (аутентификатор) и Authentication server (сервер аутентификации). RUGGEDCOM ROS поддерживает компонент Authenticator (аутентификатор).



① Запрашивающее устройство
② Коммутатор-аутентификатор
③ LAN

④ Сервер аутентификации

Рисунок 6.1 Общая топология стандарта IEEE 802.1x

⚠ ЗАМЕТКА

RUGGEDCOM ROS поддерживает защищенный расширяемый протокол аутентификации (PEAP), EAP-протокол безопасности транспортного уровня (EAP-TLS) и протокол EAP-MD5. Протоколы PEAP и EAP-TLS являются более защищенным и рекомендованы к использованию, если их поддерживает запрашивающее устройство.

В стандарте IEEE 802.1x используется расширяемый протокол аутентификации (EAP), который представляет собой настраиваемый PPP протокол аутентификации, который поддерживает различные методы аутентификации. Стандарт IEEE 802.1x определяет протокол для коммуникации между запрашивающим устройством и аутентификатором; этот протокол называют EAP через локальную сеть (EAPOL).

RUGGEDCOM ROS поддерживает связь с сервером аутентификации, используя протокол EAP через RADIUS.

Примечание
Коммутатор поддерживает аутентификацию только одного хоста для каждого порта.

Примечание
Если MAC-адрес хоста сконфигурирован в таблице статических MAC-адресов, то он будет авторизован даже в том случае, когда сервером аутентификации не была подтверждена аутентификация хоста.

6.4.1.4 Аутентификация IEEE 802.1X с аутентификацией на базе статического MAC-адреса

Данный метод, также называемый обходом аутентификации MAC-адресов (MAB), широко используется для устройств, таких как телефоны VoIP и Ethernet-принтеры, которые не поддерживают протокол 802.1x. Этот метод позволяет выполнять аутентификацию подобных устройств с использованием той же инфраструктуры базы данных, какая применяется в 802.1x.

IEEE 802.1x с обходом аутентификации MAC-адресов работает следующим образом:

1. Устройство подключается к порту коммутатора.
2. Коммутатор запоминает MAC-адрес устройства, приняв первый кадр от этого устройства (при первом соединении устройство обычно посылает сообщение с DHCP-запросом).
3. Коммутатор посылает на данное устройство сообщение EAP-запрос, пытаясь начать аутентификацию по протоколу 802.1X.

4. У коммутатора истекает время тайм-аута при ожидании EAP-ответа, поскольку устройство не поддерживает протокол 802.1x.
5. Коммутатор посылает сообщение аутентификации на сервер аутентификации, используя MAC-адрес данного устройства в качестве имени пользователя и пароля.
6. Коммутатор выполняет аутентификацию устройства или отвергает его в соответствии с ответом от сервера аутентификации.

6.4.1.5 Ограниченные сети VLAN

RUGGEDCOM ROS позволяет пользователям сконфигурировать порты 802.1X в режиме *Guest VLAN (Гостевая ЛВС)* или *Quarantine VLAN (Карантинная ЛВС)*, чтобы ограничить службы клиентам, когда происходит сбой аутентификации IEEE 802.1x или 802.1x/MAC-Auth. Например, администратор может решить ограничить доступ только к принтерам, интернету или конкретным загрузкам для неаутентифицированных пользователей.

После указанного числа неудачных попыток аутентификации, сконфигурированный порт автоматически переключится на карантинную (Quarantine) или гостевую (Guest) сеть VLAN, в зависимости от режима безопасности на уровне порта и настроек безопасности клиента:

- Если подключенное устройство поддерживает безопасность 802.1x, но не прошло аутентификацию, порт переключится на Quarantine VID.
- Если подключенное устройство несовместимо с 802.1X, а безопасность на уровне порта установлена на 802.1X, порт станет членом гостевой (Guest) сети VLAN, когда истечет время аутентификации.

Если устройство-клиент помещается в карантинную (Quarantine) или гостевую (Guest) сеть VLAN, генерируется trap-уведомление SNMP. Оповещение предупредит пользователя об изменении статуса порта.

Если порт является членом карантинной (Quarantine) сети VLAN, операционная система ROS попытается выполнить повторную аутентификацию клиента с установленным интервалом. Клиенты, не прошедшие аутентификацию, остаются в карантинной (Quarantine) сети VLAN до тех пор, пока успешно не пройдут повторную аутентификацию или пока физическая связь не пропадет. Если повторная аутентификация заканчивается неудачей, порт остается членом карантинной (Quarantine) сети VLAN.

В гостевых (Guest) сетях VLAN попытки повторной аутентификации не предпринимаются. При получении кадра EAPOL-старт от клиента порт вернется в неаутентифицированное состояние и удалит доступ клиента из гостевой (Guest) сети VLAN, чтобы продолжить процесс аутентификации.

В приведенной ниже таблице указано, как происходит определение порта в карантинную (Quarantine) или гостевую (Guest) сеть после неудачной аутентификации:

Режим безопасности на уровне порта	Безопасность клиента	Размещение после неудачной попытки аутентификации
802.1x	Поддерживает 802.1x	Карантинная сеть VLAN
	Не поддерживает 802.1x	Гостевая сеть VLAN
802.1x/MAC-Auth	Поддерживает 802.1x	Карантинная сеть VLAN
	Не поддерживает 802.1x	Карантинная сеть VLAN

Для получения дополнительной информации о конфигурировании гостевой/карантинной сети VLAN см. "Конфигурирование безопасности на уровне порта (Страница 147)".

6.4.1.6 Определение сетей VLAN с использованием туннельных атрибутов

RUGGEDCOM ROS поддерживает определение VLAN для авторизованного порта с использованием туннельных атрибутов, как определено в RFC 3580 [http://tools.ietf.org/html/rfc3580], когда для режима безопасности на уровне порта задано значение 802.1x или 802.1x/MAC-Auth.

В некоторых случаях может потребоваться разрешить размещение порта в конкретной сети VLAN, исходя из результата аутентификации. Например:

- чтобы при перемещениях в пределах сети конкретное устройство, имеющее определенный MAC-адрес, могло оставаться в одной и той же VLAN, сконфигурируйте коммутаторы для режима 802.1X/MAC-Auth
- чтобы при входе в систему из различных мест конкретный пользователь, имеющий определенные идентификационные данные для входа в систему, мог оставаться в одной и той же VLAN, сконфигурируйте коммутаторы для режима 802.1X

Если RADIUS-сервер желает использовать эту функцию, то он указывает требуемую сеть VLAN, включая туннельные атрибуты в сообщение Access-Accept (доступ-допуск). RADIUS-сервер использует следующие туннельные атрибуты для назначения VLAN:

- тип туннеля Tunnel-Type=VLAN (13)
- тип среды передачи туннеля Tunnel-Medium-Type=802
- идентификатор приватной группы туннеля Tunnel-Private-Group-ID=VLANID

Обратите внимание, что параметр VLANID 12-разрядный и принимает значения от 1 до 4094 включительно. Атрибут Tunnel-Private-Group-ID представляет собой строку, как определено в стандарте RFC 2868 [http://tools.ietf.org/html/rfc2868], так что целочисленное значение VLANID кодируется в виде строки символов.

Если туннельные атрибуты не возвращены сервером аутентификации, то назначенная для порта коммутатора сеть VLAN остается неизменной.

6.4.2 Просмотр списка авторизованных MAC-адресов

Чтобы просмотреть список MAC-адресов, полученных от защищенных портов, перейдите в ***Network Access Control » Port Security » View Authorized MAC Addresses***. Появится таблица **Authorized MAC Addresses**.

Примечание
Отображаются только MAC-адреса, авторизованные на статических MAC-портах. MAC-адреса, авторизованные с помощью IEEE 802.1X, не отображаются.

В этой таблице отображается следующая информация:

Параметр	Описание
`Port`	**Краткий обзор:** 1 to maximum port number Порт, на котором был запомнен MAC-адрес.
`MAC Address`	**Краткий обзор:** ##-##-##-##-##-## where ## ranges 0 to FF Авторизованный MAC-адрес, запомненный коммутатором.
`VID`	**Краткий обзор:** Целое число от 0 до 65535 VLAN-идентификатор той сети VLAN, в которой функционирует данный MAC-адрес.
`Sticky`	**Краткий обзор:** [No | Yes] Этот параметр описывает, могут ли авторизованные MAC-адрес/устройство быть перемещены на незащищенный порт или нет. • `Да` - авторизованные MAC-адрес/устройство не могут быть перемещены на другой порт коммутатора • `Нет` - авторизованные MAC-адрес/устройство могут быть перемещены на незащищенный порт коммутатора

Если MAC-адрес не указан в списке, сделайте следующее:

- Сконфигурируйте безопасность на уровне порта. Для получения дополнительной информации см. "Конфигурирование безопасности на уровне порта (Страница 147)".
- Сконфигурируйте IEEE 802.1X. Для получения дополнительной информации см. "Конфигурирование IEEE 802.1X (Страница 149)".

6.4.3 Конфигурирование безопасности на уровне порта

Чтобы сконфигурировать безопасность порта, сделайте следующее:

1. Перейдите в ***Network Access Control » Port Security » Configure Ports Security***. Появится таблица **Ports Security**.
2. Выберите Ethernet-порт. Появится форма **Ports Security**.

3. Необходимо сконфигурировать следующие параметры:

Параметр	Описание
`Port`	**Краткий обзор:** 1 to maximum port number **Значение по умолчанию:** 1 Номер порта.
`Security`	**Краткий обзор:** [Off | Static MAC | 802.1X | 802.1x/MAC-Auth] **Значение по умолчанию:** Off Включает или выключает функцию защиты порта. Доступны два типа контроля доступа к порту: • На базе статического MAC-адреса. При использовании этого метода разрешенные MAC-адреса должны быть указаны в таблице статических MAC-адресов. Если некоторые MAC-адреса неизвестны заранее (или неизвестно, с каким портом они будут соединены), то остается вариант сконфигурировать коммутатор для автоматического запоминания некоторого числа MAC-адресов. После запоминания эти адреса не устаревают, пока не произведен перезапуск устройства или не прервано соединение. • Аутентификация по стандарту IEEE 802.1X. • IEEE 802.1X с MAC-аутентификацией, также называемой обход MAC-аутентификации. При использовании этой опции устройство может выполнять аутентификацию клиентов на основании MAC-адреса клиента, если истекло время тайм-аута для аутентификации IEEE 802.1X.
`Quarantine VID`	**Краткий обзор:** Целое число от 1 до 4096 или [None] **Значение по умолчанию:** None Идентификатор VLAN для карантинной сети VLAN. Применимо лишь в том случае, когда в поле "защита" задано значение "802.1x" или "802.1x/MAC-Auth". Порт будет помещен в карантинную сеть VLAN, если клиент не прошел аутентификацию.
`Guest VID`	**Краткий обзор:** Целое число от 1 до 4096 или [None] **Значение по умолчанию:** None Идентификатор VLAN для гостевой сети VLAN. Применимо лишь в том случае, когда в поле "защита" задано значение "802.1x". Порт будет помещен в гостевую сеть VLAN, если клиент не поддерживает стандарт 802.1x.
`Autolearn`	**Краткий обзор:** Целое число от 1 до 16 или [None] **Значение по умолчанию:** None Применимо лишь в том случае, когда в поле "защита" задано значение "статический MAC-адрес". Этот параметр определяет максимальное количество MAC-адресов, которые могут быть динамически запомнены для данного порта. Если для порта сконфигурированы статические адреса, то фактическое число адресов, которые разрешено запомнить, будет равно значению этого параметра за вычетом числа статических MAC-адресов.

Параметр	Описание
`Sticky`	**Краткий обзор:** [No | Yes] **Значение по умолчанию:** Yes Применимо лишь в том случае, когда в поле "защита" задано значение "статический MAC-адрес". Изменение поведения порта на Sticky (привязка) или Non-sticky (без привязки). Если параметр Sticky (привязка) имеет значение "Да", то разрешенные для данного порта статические MAC-адреса "привязываются" к этому порту, а коммутатор не позволит удалить их из порта (в случае отсутствия соединения с этим портом) или переместить на другой порт. Если параметр Sticky (привязка) имеет значение "Нет", то разрешенные для данного порта статические MAC-адреса могут быть перемещены на незащищенный порт.
`Shutdown Time`	**Краткий обзор:** Целое число от 1 до 86400 или [Until reset | Don't shutdown] **Значение по умолчанию:** Don't shutdown Указывает продолжительность времени отключения порта, если имеет место нарушение безопасности.
`Status`	**Краткий обзор:** Строка длиной 31 символа(ов) Описывает состояние безопасности порта.

Примечание
Существует несколько сценариев, при которых статические MAC-адреса могут быть перемещены:

- Если канал связи работоспособен/не работоспособен на защищенном порте *без привязки адресов*
- Если трафик переключается с защищенного порта *без привязки адресов* или на него.

Примечание
Трафик теряется до тех пор, пока исходный MAC-адрес входящего трафика не будет авторизован вновь в соответствии с таблицей статических MAC-адресов.

4. Нажмите **Apply**.

6.4.4 Конфигурирование IEEE 802.1X

Порядок конфигурирования аутентификации IEEE 802.1X на базе порта:

1. Перейдите в ***Network Access Control » Port Security » Configure 802.1X***. Появится таблица **802.1X Parameters**.
2. Выберите Ethernet-порт. Появится форма **802.1X Parameters**.

3. Необходимо сконфигурировать следующие параметры:

Параметр	Описание
`Port`	**Краткий обзор:** 1 to maximum port number **Значение по умолчанию:** 1 Номер порта.
`txPeriod`	**Краткий обзор:** Целое число от 1 до 65535 **Значение по умолчанию:** 30 Время ожидания пакета EAP Response/Identity (ответ/идентификация) от супликанта до повторной передачи пакета EAP Request/Identity (запрос/идентификация).
`quietPeriod`	**Краткий обзор:** Целое число от 0 до 65535 **Значение по умолчанию:** 60 Период времени, в течение которого не производятся попытки получить информацию супликанта после неудачного сеанса авторизации.
`reAuthEnabled`	**Краткий обзор:** [No | Yes] **Значение по умолчанию:** No Включение или отключение периодической повторной аутентификации.
`reAuthPeriod`	**Краткий обзор:** Целое число от 60 до 86400 **Значение по умолчанию:** 3600 Интервал времени между периодическими повторными аутентификациями супликанта.
`reAuthMax`	**Краткий обзор:** Целое число от 1 до 10 **Значение по умолчанию:** 2 Число попыток повторной аутентификации, которые разрешается сделать до того как порт перейдет в неавторизованное состояние.
`suppTimeout`	**Краткий обзор:** Целое число от 1 до 300 **Значение по умолчанию:** 30 Время ожидания ответа супликанта на пакет EAP от сервера аутентификации.
`serverTimeout`	**Краткий обзор:** Целое число от 1 до 300 **Значение по умолчанию:** 30 Время ожидания ответа сервера аутентификации на пакет EAP от супликанта.
`maxReq`	**Краткий обзор:** Целое число от 1 до 10 **Значение по умолчанию:** 2 Максимальное число повторных передач пакета EAP Request (запрос) от сервера аутентификации супликанту до прекращения сеанса аутентификации по тайм-ауту.

4. Нажмите **Apply**.

6.5 Управление ключами и сертификатами SSH/SSL

RUGGEDCOM ROS использует сертификаты и ключи X.509v3, чтобы создавать защищенные соединения для удаленного входа в систему (SSH) и веб-доступа (SSL).

⚠ ЗАМЕТКА

Угроза безопасности — риск неавторизованного доступа и/или использования

Siemens рекомендует выполнить следующие действия перед вводом устройства в эксплуатацию:

- Заменить заводской самоподписанный сертификат SSL на сертификат, подписанный доверенным центром сертификации (CA)
- Сконфигурировать клиент SSH на использование *diffie-hellman-group14-sha1* или лучше

Примечание
Только административные пользователи могут записывать на устройство сертификаты и ключи.

Каждое устройство RUGGEDCOM ROS поставляется с уникальным самоподписанным SSL-сертификатом ECC 256 и парой хост-ключей SSH RSA 2048, которые генерируются на заводе. Администратор может выгрузить новый сертификат и ключи в систему в любое время, что приведет к перезаписи существующих. Кроме того, доступны CLI-команды для последовательного генерирования SSL-сертификата и пары хост-ключей SSH.

В RUGGEDCOM ROS используется три типа сертификатов и ключей:

Примечание
Следует избегать присутствие в сети устройства под управлением ROS с ключами по умолчанию, даже временно. Лучше всего как можно скорее создать собственные сертификаты и ключи, предпочтительно ещё до подключения устройства к сети.

Примечание
Сертификат и ключи по умолчанию являются общими для всех версий RUGGEDCOM ROS без сертификата или файлов ключей. Поэтому важно либо разрешить выполнение автоматического генерирования ключей, либо предоставить пользовательские ключи. Таким образом, при установлении защищенного соединения с устройством будут иметь место, по меньшей мере, уникальные, а в лучшем случае — прослеживаемые и проверяемые ключи.

- **По умолчанию**

  Стандартные сертификат и ключи SSL/SSH встроены в RUGGEDCOM ROS и являются общими для всех устройств RUGGEDCOM ROS с одним и тем же микропрограммным обеспечением. Если действительные файлы SSL-сертификата или ключей SSL/SSH отсутствуют на устройстве (что обычно

происходит при обновлении с более старой версии ROS, которая не поддерживает конфигурируемые пользователем ключи и, следовательно, не поставлялась с уникальными сгенерированными на заводе ключами), то *временно* используются сертификат и ключи по умолчанию; это сделано для того, чтобы к устройству можно было подключиться с использованием SSH и SSL (HTTPS).

- **Автоматически генерируемые**

  Если используются SSL-сертификат и ключи SSL/SSH по умолчанию, то RUGGEDCOM ROS немедленно начинает генерировать в фоновом режиме уникальный сертификат и ключи SSL/SSH. Если во время автоматической генерации сертификатов и ключей загружаются пользовательские сертификат и ключи, то процедура генерации прерывается, так что будут использоваться пользовательские сертификат и ключи.

- **Генерируемые пользователем (рекомендуется)**

  Пользовательские сертификаты и ключи — это самый безопасный вариант. Они дают пользователю полный контроль над администрированием сертификата и ключей, позволяют обеспечивать сертификаты, подписанные публичным или местным центром сертификации, активируют жестко контролируемый доступ к частным ключам, а также обеспечивают полномочное распространение SSL-сертификатов, любых сертификатов CA и открытых SSH-ключей.

Примечание
Частный ключ RSA или EC, соответствующий SSL-сертификату, должен быть добавлен к сертификату в файле `ssl.crt`.

6.5.1 SSL-сертификаты

RUGGEDCOM ROS поддерживает SSL-сертификаты, которые соответствуют следующим спецификациям:

- Формат цифровых сертификатов X.509 v3
- Формат PEM
- Для контролируемых версий RUGGEDCOM ROS: пара ключей RSA, длина 1024, 2048 или 3072 бита; или NIST P-256, P-384 или P-521
- Для неконтролируемых (NC) версий RUGGEDCOM ROS: Пара ключей RSA, длина от 512 до 2048 бит

Примечание
Ключи эллиптической кривой длиной менее P-256 бит не поддерживаются.

Примечание
Не рекомендуется применять ключи RSA с длиной менее 2048 бит.

Требуются два стандартных файла PEM: файл SSL-сертификата и соответствующий файл секретного ключа RSA. Эти файлы последовательно

соединяются в результирующий `ssl.crt`, который может быть затем загружен в RUGGEDCOM ROS. Для получения дополнительной информации о передаче файлов между устройством и хост-компьютером см. "Выгрузка/загрузка файлов (Страница 59)".

Несмотря на то, что RUGGEDCOM ROS может использовать самоподписанные сертификаты, созданные с помощью команды **`sslkeygen`**, Siemens рекомендует использовать сертификат X.509, выпускаемый собственным центром сертификации (CA) организации.

6.5.2 Хост-ключ SSH

Примечание
SSH не поддерживается для неконтролируемых (NC) версий RUGGEDCOM ROS.

Контролируемые версии RUGGEDCOM ROS поддерживают пары открытых/секретных SSH-ключей, которые соответствуют следующим спецификациям:

- Формат PEM
- Пара ключей DSA, длина 1024, 2048 ли 3072 бита
- Пара ключей RSA, длина 1024, 2048 ли 3072 бита

Примечание
Время генерирования ключа DSA или RSA увеличивается в зависимости от длины ключа. Ключи RSA длиной 1024 бита генерируются менее, чем за 5 минут, на слегка нагруженном блоке, а на генерирование ключей длиной 2048 бит уходит значительно больше времени. Однако типичная современная компьютерная система может генерировать такие ключи за несколько секунд.

В следующем фрагменте shell-скрипта (командная оболочка bash) используется утилита командной строки `ssh-keygen` для генерации 2048-битного ключа RSA, пригодного для использования в RUGGEDCOM ROS. В результате получается файл `ssh.keys`, который может быть затем загружен в RUGGEDCOM ROS.

```
# RSA key size:
BITS=2048

# Make an SSH key pair:
ssh-keygen -t RSA -b $BITS -N '' -f ssh.keys
```

Пример ключа SSH, сгенерированного RUGGEDCOM ROS, см. в "Примеры сертификатов и ключей (Страница 157)".

6.5.3 Управление открытыми ключами SSH

RUGGEDCOM ROS позволяет административным пользователям составлять список, добавлять и удалять открытые ключи SSH. Открытые ключи

добавляются в виде файлов энергонезависимого хранилища на устройства RUGGEDCOM ROS и извлекаются во время аутентификации SSH-клиента.

6.5.3.1 Требования к открытым ключам

Открытые ключи хранятся во флеш-файле *sshpub.keys*. Файл *sshpub.keys* состоит из записей открытых ssh-ключей пользователя. Аналогично файлу config.csv, каждая запись должна отделяться пустой строкой. Запись должна включать два компонента. в следующей последовательности:

- Заголовок
- Ключ

Заголовок содержит параметры записи, разделенные запятой. Порядок параметров:

- Идентификатор: Число от 0 до 9999
- Тип записи: UserKey
- Уровень доступа: Admin, Operator или Guest (администратор, оператор или гость)
- Статус отмены: активен/неактивен (всегда активен для ключей)
- Имя пользователя: Имя пользователя клиента (не имя пользователя RUGGEDCOM ROS). Будет использоваться клиентами в будущем для SSH в устройство RUGGEDCOM ROS.

Ключ должен иметь формат RFC4716 или PEM со следующими строками заголовка и примечания:

```
-----BEGIN PUBLIC KEY-----
-----END PUBLIC KEY-----

-----BEGIN SSH2 PUBLIC KEY-----
-----END SSH2 PUBLIC KEY-----

-----BEGIN RSA PUBLIC KEY-----
-----END RSA PUBLIC KEY-----
```

Ниже приведен пример действительной записи в файле *sshpub.keys* в формате PEM:

```
1,userkey,admin,active,alice
---- BEGIN SSH2 PUBLIC KEY ----
AAAAB3NzaC1yc2EAAAABIwAAAQEA4mRrqfk+RKXnmGRvzMyWVDsbq5VwpGGrlLQYCrjVEa
NdbXsphqYKop8V5VUeXFRAUFzOy82yk8TF/5JxGPWq6wRNjhnYR7IY2AiMBq0+K8XeURl/
z5K2XNRjnqTZSFwkhaUVJeduvjGgOlNN4yvgUwF3n0idU9k3E1q/na+LmYIeGhOwzCqoAc
ipHAdR4fhD5u0jbmvjv+gDikTSZIbj9eFJfP09ekImMLHwbBry0SSBpqAKbwVdWEXIKQ47
zz7ao2/rs3rSV16IXSq3Qe8VZh2irah0Md6JFMOX2qm9fo1I62q1DDgheCOsOiGPf4xerH
rI2cs6FT31rAdx2JOjvw==
---- END SSH2 PUBLIC KEY ----
```

Ниже приведен пример действительной записи в файле *sshpub.keys* в формате RFC4716:

```
2,userkey,admin,active,bob
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDH0NivR8zzbTxlecvFPzR/
GR24NrRJa0Lc7scNsWRgi0XulHuGrRLRB5RoQ39+spdig88Y8CqhRI49XJx7uLJe0Su3RvyNYz1jkdSwHq2h
```

```
SZCpukJxJ6CK95Po/sVa5Gq2gMaHowiYDSkcx+AJywzK/eM6i/jc125lRxFPdfkj74u
+ob3PCvmIWz5z3WAJBrQU1IDPHDets511WMu8O9/mAPZRwjqrWhRsqmcXZuv5oo54wIopCAZ
So20SPzM2VmXFuUsEwDkvYMXLJK1koJPbDjH7yFFC7mwK2eMU/oMFFn934cbO5N6etsJSvplYQ4pMCw6Ok8Q/
bB5cPSOa/rAt bob@work
```

RUGGEDCOM ROS позволяет хранить 16 записей ключей пользователя. Каждая запись ключа должна соответствовать следующим ограничениям:

- Тип ключа должен быть RSA 2048-битовый или RSA 3072-битовый
- Размер ключа не должен превышать 4000 символов с кодированием base64
- Тип записи в заголовке не должен превышать 8 символов ASCII
- Уровень доступа в заголовке не должен превышать 8 символов ASCII (максимум — *оператор*)
- Статус отмены в заголовке не должен превышать 8 символов ASCII (максимум — *неактивен*)
- Имя пользователя не должно превышать 12 символов ASCII

6.5.3.2 Добавление открытого ключа

Администраторы могут добавлять один или несколько открытых ключей в RUGGEDCOM ROS.

Существует два способа обновления файла *sshpub.keys*:

- Напрямую выгрузить созданный локально файл в *sshpub.keys*. Содержимое файла заменяет содержимое, которое хранится в настоящий момент во флеш-памяти.
- Выгрузить созданный локально файл к файлу *sshaddpub.keys*. Содержимое файла добавляется к существующим записям в файле *sshpub.keys*.

⚠ ЗАМЕТКА

Опасность для конфигурации — риск нарушения обмена данными

Содержимое файла *sshaddpub.keys* должно иметь такой же синтаксис, что и файл *sshpub.keys*.

Чтобы добавить ключи, сделайте следующее:

1. Создайте файл открытого ключа через хост-компьютер.
2. Передайте файл открытого ключа на устройство с помощью SFTP или Xmodem. Для получения дополнительной информации о передаче файлов см. "Выгрузка/загрузка файлов (Страница 59)".
3. Войдите в систему устройства в качестве администратора и перейдите в командную оболочку CLI. Для получения дополнительной информации о порядке доступа к командной оболочке CLI см. "Использование интерфейса командной строки (Страница 27)".

4. Проверьте системный журнал, чтобы убедиться в том, что файлы были надлежащим образом переданы. Для получения дополнительной информации о просмотре системного журнала см. "Просмотр локальных и системных журналов (Страница 65)".

6.5.3.3 Просмотр списка открытых ключей

Административные пользователи могут просматривать список существующих открытых ключей на устройстве.

Чтобы просмотреть открытые ключи, сделайте следующее:

1. Войдите в систему устройства в качестве администратора и перейдите в командную оболочку CLI. Для получения дополнительной информации о порядке доступа к командной оболочке CLI см. "Использование интерфейса командной строки (Страница 27)".
2. В командной строке CLI наберите:

   `sshpubkey` `list`

   Появится список открытых ключей, включая их идентификатор ключа, уровень доступа, статус отмены, имя пользователя и отпечаток ключа.

6.5.3.4 Обновление открытого ключа

Административные пользователи могут обновлять открытые ключи.

Чтобы обновить открытые ключи, сделайте следующее:

1. Войдите в систему устройства в качестве администратора и перейдите в командную оболочку CLI. Для получения дополнительной информации о порядке доступа к командной оболочке CLI см. "Использование интерфейса командной строки (Страница 27)".
2. В командной строке CLI наберите:

   `sshpubkey` `list`

   Появится список открытых ключей, включая их идентификатор ключа, уровень доступа, статус отмены, имя пользователя и отпечаток ключа.
3. Введите следующие команды, чтобы обновить открытые ключи:

Команда	Описание
`sshpubkey` `update_id { current_ID } { new_ID }`	Обновляет идентификатор открытого ключа пользователя. **Примечание** Идентификатор открытого ключа пользователя должен являться числом от 0 до 9999. • `{ current_ID }` — это идентификатор, назначенный открытому ключу в данный момент

Команда	Описание
	• { *new_ID* } — это идентификатор, который будет использоваться для идентификации открытого ключа в дальнейшем
sshpubkey update_al { *AL* }	Обновляет уровень доступа открытого ключа пользователя. • { *AL* } — это уровень доступа (администратор, оператор или гость) открытого ключа, подлежащего обновлению
sshpubkey update_rs { *RS* }	Обновляет состояние отмены (активен, неактивен) пользовательского открытого ключа. • { *RS* } — состояние отмены открытого ключа, подлежащего обновлению
sshpubkey update_un { *UN* }	Обновляет имя пользователя открытого ключа пользователя. • { *UN* } — имя пользователя открытого ключа, подлежащего обновлению

6.5.3.5 Удаление открытого ключа

Административные пользователи могут удалить один или несколько открытых ключей.

Чтобы удалить открытый ключ, сделайте следующее:

1. Войдите в систему устройства в качестве администратора и перейдите в командную оболочку CLI. Для получения дополнительной информации о порядке доступа к командной оболочке CLI см. "Использование интерфейса командной строки (Страница 27)".
2. В командной строке CLI наберите:

   sshpubkey list

   Появится список открытых ключей, включая уровень доступа, статус отмены, имя пользователя и отпечаток ключа.
3. Введите следующие команды, чтобы удалить открытый ключ или несколько открытых ключей:

Команда	Описание
sshpubkey remove { *ID* }	Удаляет ключ из энергонезависимой памяти. • { *ID* } — идентификатор открытого ключа, подлежащего удалению

6.5.4 Примеры сертификатов и ключей

Для SSL сертификаты должны соответствовать требованиям, указанным в "SSL-сертификаты (Страница 152)".

Сертификат и ключи должны быть объединены в одном файле `ssl.crt` и загружены на устройство.

Ниже приведен пример объединения SSL-сертификата и ключа:

```
-----BEGIN CERTIFICATE-----
MIIC9jCCAl+gAwIBAgIJAJh6rrehMt3iMA0GCSqGSIb3DQEBBQUAMIGuMQswCQYD
VQQGEwJDQTEQMA4GA1UECBMHT250YXJpbzEQMA4GA1UEBxMHQ29uY29yZDESMBAG
A1UEChMJUnVnZ2VkY29tMRkwFwYDVQQLExBDdXN0b21lciBTdXBwb3J0MSYwJAYD
VQQDEx1XUy1NSUxBTkdPVkFOLlJVR0dFRENPTS5MT0NBTDEkMCIGCSqGSIb3DQEJ
ARYVc3VwcG9ydEBydWdnZWRjb20uY29tMB4XDTEyMTAyMzIxMTA1M1oXDTE3MTAy
MjIxMTA1M1owgZwxCzAJBgNVBAYTAlVTMRAwDgYDVQQIEwdPbnRhcmlvMRAwDgYD
VQQHEwdDb25jb3JkMRIwEAYDVQQKEwlSdWdnZWRDb20xGTAXBgNVBAsTEEN1c3Rv
bWVyIFN1cHBvcnQxFDASBgNVBAMTCzE5Mi4xNjguMS4yMSQwIgYJKoZIhvcNAQkB
FhVTdXBwb3J0QHJ1Z2dlZGNvbS5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJ
AoGBALfE4eh2aY+CE3W5a4Wz1Z1RGRP02COHt153wFFrU8/fFQXNhKlQirlAHbNT
RSwcTR8ZFapivwYDivn0ogOGFXknYP90gv2oIaSVY08FqZkJW77g3kzkv/8Zrw3m
W/cBsZJ8SyKLIDfy401HkHpDOle5NsQFSrziGUPjAOIvvx4rAgMBAAGjLDAqMAkG
A1UdEwQCMAAwHQYDVR0OBBYEFER0utgQOifnrflnDtsqNcnvRB0XMA0GCSqGSIb3
DQEBBQUAA4GBAHtBsNZuh8tB3kdqR7Pn+XidCsD70YnI7w0tiy9yiRRhARmVXH8h
5Q1rOeHceri3JFFIOxIxQt4KgCUYJLu+c9Esk/nXQQar3zR7IQCt0qOABPkviiY8
c3ibVbhJjLpR2vNW4xRAJ+HkNNtBOg1xUlp4vOmJ2syYZR+7XAy/OP/S
-----END CERTIFICATE-----
-----BEGIN RSA PRIVATE KEY-----
MIIEpQIBAAKCAQEAn3UT94ZjlmBjygLXaA21ULum7EDmgsvFvg2tKYyaMj1en5UW
x172GvlDLUm5EwGmcG9u6DyuO3wOyv/taD1OUFkZA1W7cPu9NjeTtZjIQCx33xSU
1d6INMi2oOzwJmWzqwqIkIgy0uMdw78be4n7359U0UOOEtCStOmUfdw34jv6c38J
8sb+lC/FktX8Eilka4mDr07tf/ivC2kdwpPlGZIKt/xjcwjOsNHIBSfqbEbg5mO3
9OAPqsPRWKhBQZ6rM8aqEQjGPlrSTTNHrxO/CYVxAh0gtz+6qUytL3zi7Z9P7EzD
H8V8qNdXRNN0w5hsh2A5ZJj6+cbQJm0JHQeOowIDAQABAoIBAH2zXqUfBLyTibbC
3KoDPG7DLwhI9S4gkuaKg3ogg6GdLU2hys4p9to2qxU1a7cm8tzpi0V6KGNuHX87
lxw4T9cZFZXCbLvZR0RJNaDPKvUj2O87m0SpYzgxDX74qSuruqHX8OX26BHExj78
FR8jHDIhuUwp9AKy9yO0isFY65jkLov6tdRpNy5A+QrGyRVBilCIT6YFYKSzEEI8
6+29FkLtX+ERjqxJs+aGHyEPDWE4Zy7dBsuTk1Fwz8F6/rOz4PS2pNQXc2sWmomn
muQXv0hwKY5gMcovCkC3y/op3kNuc/3qeBHjeCBYEMLR0o25hZHGrKOrQahFsy+R
V48sgIECgYEA0H66Ijfcc7NpgKOQwyvCt9/uhRZ3RkeABoSBLb/wYfQjw4pMadqr
RMMzVPzOLC459Giv4m8GeikNPl53rYdTCRmd/t1nZClU/UQKhgj+RRt4xY2cJNsg
j2CTZDr5SJO8H957K1IbvN5mxdsWZuDc5dtf0wBMIaCJoXR/iDMcf2MCgYEAw8oK
Dkpz9PdhGkbTE0ARLeUv7okelBkfDIGgucXBFHUElHAGe+XLF5dMppmzRDHXi2NG
gSNPJsDOlgSyLJjKX7HapYeAJWm91w5kJEX+oERr1EnEPWPvOHI+OW5DjM6eR1s9
xRJ87e3ymgLIF7G5rmf0p3OlnVvCaQvIVYTB98ECgYEAl+sPI2nCp0eeY05LZ/rV
6fcwLCdfh4UHwzf/jF9j/2vON2fpH+RmkTcOiymd7NFOB0nUhtBRTufkr4JT/8wv
89yHpDKdaH05YUWXyWx6Ic7PpFr34F8OjYpYO1tBUuHa3PnWk41Dis4e4qIt446L
Rq0fWHbKAmKghlWFq69aX3MCgYEArKU2JM/mXHbfe0pEyk7OV0gn8hGbk0Brrp2H
2wjUb3OYbEQ0k4BYjB7wimAyQcoppVIPU8SNAUE3afYOH2FD4wp0IU7Q4yzRKBga
mhnWpABxjSrXDsNWqNGkqQPgMQPpcka0u1jILQ6LxN77Dlm7wF0O0bIash292t92
8mI0oIECgYEAql8/uRHGtwSk64rXWXI+uq+x4ewwZkVc+mMmJ0yCMuQsOzbQTxhx
v9GEi3xsFbNazGCx4b56+/6Bi6gf7aH+NeK2+7C4ddlpHGEawoEcW1CW8hRQ2brp
vWgC+m5nmQ2SaYGzlilzZVK3JE6qOZ/AG8k+ZEG9tsvakMliG1SoJXk=
-----END RSA PRIVATE KEY-----
```

Для SSH, DSA или RSA пары хост-ключей должны соответствовать требованиям, указанным в "Хост-ключ SSH (Страница 153)".

Ниже приведен пример SSH-ключа в формате PEM:

```
-----BEGIN DSA PRIVATE KEY-----
MIIBuwIBAAKBgQD0gcGbXx/rrEMu2913UW4cYo1OlcbnuUz7OZyd2mBLDx/GYbD8
X5TnRcMraJ0RuuGK+chqQJW5k3zQmZa/BS6q9U7wYwIAx8JSxxpwfPfl/t09VwKG
rtSJIMpLRoDq3qEwEVyR4kDUo4LFQDsljtiyhcz1n6kd6gqsd5Xu1vdh4wIVANXb
SBi97GmZ6/9f4UCvIIBtXLEjAoGAAfmhkcCCEnRJitUTiCE+MurxdFUr3mFs/d31
4cUDaLStQEhYYmx5dbFdQuapl4Y32B7lZQkohi5q1T1iUAa40/nUnJx1hFvblkYT
8DLwxcuDAaiu0VqsaPtJ+baL2dYNp96tFisj/475PEEWBGbP6GSe5kKa1Zdgwuie
9LyPb+ACgYBv856v5tb9UVG5+tX5Crfv/Nd8FFlSSFKmVWW3yzguhHajg2LQg8UU
sm1/zPSwYQ0SbQ9aOAJnpLc2HUkK0lji/0oKVI7y9MMc4B+bGu4W4OnryP7oFpnp
YYHt5PJY+zvLw/Wa+u3NOVFHkF1tGyfVBMXeV36nowPo+wrVMolAEgIVALLTnfpW
maV6uh6RxeE1d4XoxSg2
-----END DSA PRIVATE KEY-----
```

7 Уровень 2

В данной главе описаны возможности RUGGEDCOM ROS, относящиеся ко 2-му уровню (@@уровень канала данных (DLL)).

7.1 Управление виртуальными сетями LAN

Виртуальная локальная сеть (или VLAN) представляет собой группу устройств на одном или нескольких сегментах локальной сети, которые поддерживают между собой связь таким образом, как если бы они были соединены с одним и тем же сегментом физической локальной сети. Использование VLAN дает очень большую гибкость, так как разделение сетей основано на логических, а не на физических соединениях.

Когда применяются VLAN, каждый из видов трафика оказывается принадлежащим той или другой VLAN. Трафик в одной сети VLAN не может быть передан в другую никаким иным образом, кроме как через межсетевой маршрутизатор или коммутатор уровня 3.

Сети VLAN создают двумя способами:

- **Явно**

  Статические сети VLAN могут создаваться в коммутаторе. Для получения дополнительной информации о статических сетях VLAN см. "Управление статическими сетями VLAN (Страница 173)".

- **Неявно**

  Если идентификатор сети VLAN (VID) устанавливается для сети VLAN с использованием портов, статического MAC-адреса или IP-интерфейса, автоматически создается соответствующая сеть VLAN, если она уже не существует.

Для получения дополнительной информации о сетях VLAN см. "Концепция сетей VLAN (Страница 159)".

7.1.1 Концепция сетей VLAN

В данном разделе рассматриваются некоторые принципы, имеющие значение для реализации сетей VLAN в RUGGEDCOM ROS.

7.1.1.1 Сравнение тегированных и нетегированных кадров

Теги сети VLAN идентифицируют кадры как часть сети VLAN. Если коммутатор получает кадр с тегом сети VLAN (или 802.1Q), идентификатор сети VLAN (VID) извлекается, а кадр пересылается на другие порты той же сети VLAN.

Если кадр не содержит тега сети VLAN или содержит тег 802.1p (приоритизация), содержащий только информацию о приоритизации и VID равный 0, такой кадр считается нетегированным.

7.1.1.2 Native VLAN (VLAN, в которой кадры не тегируются)

Для каждого порта задается номер native VLAN (номер виртуальной локальной сети, к которой относятся все нетегированные кадры или кадры от не включенных в какую-либо VLAN портов), идентификатор порта VLAN ID (PVID). Когда нетегированный кадр поступает на порт, он ассоциируется с native VLAN этого порта.

По умолчанию, когда коммутатор передает кадр в native VLAN, он посылает нетегированный кадр. Коммутатор можно настроить для передачи тегированных кадров в native VLAN.

7.1.1.3 Административная сеть VLAN

По умолчанию весь трафик управления принадлежит административной сети VLAN. Вспомогательные сети VLAN с поддержкой функции управления можно сконфигурировать на перемещение трафика управления; однако трафик BOOTP, DHCP и LLDP может принадлежать только административной сети VLAN.

Административная сеть VLAN является конфигурируемой и всегда по умолчанию настроена как VLAN 1. Она также по умолчанию является Native VLAN для всех портов.. Ее изменение может использоваться с целью ограничения административного доступа для определенной группы пользователей.

⚠ ЗАМЕТКА

Угроза безопасности — риск неавторизованного доступа и/или использования

IP-интерфейсы, принадлежащие сети VLAN с передачей трафика управления коммутаторами, должны быть подключены к доверенной сети.

7.1.1.4 Вспомогательные административные сети VLAN

В дополнение к административной сети VLAN вспомогательные сети VLAN с поддержкой функции управления могут пересылать трафик управления, связанный со следующими службами:

- MMS
- Modbus
- Radius/TacPlus
- Удаленная оболочка
- Удаленный системный журнал
- SNMP
- SNTP
- SSH
- TFTP
- Telnet
- Веб-сервер

Однако в отличие от административной сети VLAN, вспомогательные сети VLAN не могут пересылать трафик BOOTP, DHCP или LLDP.

По умолчанию вспомогательные сети VLAN с передачей трафика управления коммутаторами не сконфигурированы. Можно сконфигурировать до 254 вспомогательных административных сетей VLAN. Конфигурирование вспомогательных сетей VLAN с передачей трафика управления коммутаторами может использоваться для ограничения или расширения административного доступа между набором пользователей.

⚠ ЗАМЕТКА

Угроза безопасности — риск неавторизованного доступа и/или использования

IP-интерфейсы, которые принадлежат вспомогательной сети VLAN с передачей трафика управления коммутаторами, должны быть подключены к доверенной сети.

7.1.1.5 Типы граничных и транковых портов

Каждый порт можно сконфигурировать как граничный или транковый порт.

Граничный порт подключается к одному оконечному устройству, такому как ПК или интеллектуальное электронное устройство (ИЭУ). Граничный порт переносит трафик на native VLAN.

Транковые порты являются частью сети и передают трафик для всех сетей VLAN между коммутаторами. Транковые порты автоматически становятся участниками всех сетей VLAN, настроенных в коммутаторе.

Коммутатор может "ретранслировать" трафик, пересылая кадры, принятые на один транковый порт с другого транкового порта. Транковые порты должны быть участниками всех сетей VLAN, составной частью которых является "транзитный" трафик, даже если ни одна из этих сетей VLAN не используется на граничных портах.

Кадры, передаваемые с порта по всем сетям VLAN, кроме native VLAN этого порта, всегда посылаются тегированные.

Примечание
Иногда бывает нужно вручную ограничить трафик в транке определенной группой сетей VLAN. Например, если транк подключен к устройству (такому как маршрутизатор уровня 3), которое поддерживает подмножество из доступных сетей VLAN. Можно предотвратить участие транкового порта в сети VLAN, включая его в список запрещенных портов этой VLAN.

Для получения дополнительной информации о списке запрещенных портов см. "Список запрещенных портов (Страница 163)".

Тип порта	Поддерживаемые сети VLAN	Формат PVID	Использование
Граничный	Сконфигурирован 1 (native VLAN)	Нетегированный	*Сети VLAN Unaware (с передачей в теге номера VLAN)*: Все кадры посылаются и принимаются без тегов VLAN.
		Тегированный	*Сети VLAN Aware (с передачей в теге только информации о приоритете)*: Весь трафик включается в одну VLAN.
Транковый	Все сконфигурированные	Тегированные или нетегированные	*Межкоммутаторные соединения*: Сети VLAN должны создаваться и администрироваться вручную, либо могут динамически запоминаться через GVRP. *Оконечные устройства с множественными VLAN*: Реализуются соединения с оконечными устройствами, которые поддерживают несколько сетей VLAN одновременно.

7.1.1.6 Правила для входящего и исходящего трафика сети

Правила для входящего и исходящего трафика сети определяют, как коммутатор получает и пересылает трафик.

Правила для входящего трафика сети применяются следующим образом ко всем кадрам при получении коммутатором:

- Если входящий кадр является нетегированным или имеет VID, равный 0 (тегированный приоритетом), кадр ассоциируется с PVID входного порта
- Если входящий кадр является тегированным, разрешается прохождение кадра с сохранением его VID
- Входящие кадры отбрасываются только в случае, если активирована входная фильтрация и кадр тегирован с помощью VID, который не совпадает ни с одной сетью VLAN, членом которой является входящий порт

Правила для исходящего трафика сети применяются следующим образом ко всем кадрам при передаче коммутатором:

- Если тегирование PVID включено, исходящие кадры тегируются, если они ассоциированы с native VLAN выходного порта, независимо от типа его принадлежности (граничный или транковый)

- Кадры, выходящие на граничном интерфейсе отбрасываются, если они связаны с сетью VLAN, отличной от native VLAN выходного порта
- Кадры, выходящие на транковом интерфейсе тегируются, если они связаны с сетью VLAN, членом которой является выходной порт

7.1.1.7 Список запрещенных портов

Каждая сеть VLAN может быть сконфигурирована на исключение портов из сети VLAN с помощью списка запрещенных портов. Для получения дополнительной информации см. "Добавление статической сети VLAN (Страница 174)".

7.1.1.8 Режимы VLAN-aware (VLAN-осведомленный) и VLAN-unaware (VLAN-неосведомленный)

Естественным режимом работы для IEEE 802.1Q-совместимого коммутатора является VLAN-aware (VLAN-осведомленный). Даже в том случае, когда в сетевой архитектуре не используются виртуальные локальные сети (VLAN), настройки VLAN по умолчанию в RUGGEDCOM ROS все же позволяют коммутатору работать в режиме VLAN-aware, обеспечивая при этом функциональность почти для любого сетевого приложения. Однако стандарт IEEE 802.1Q определяет набор правил, которым должны следовать все VLAN-aware коммутаторы:

- Допустимый интервал идентификаторов VID от 1 до 4094. VID=0 и VID=4095 не допускаются.
- Каждый кадр, входящий на VLAN-aware коммутатор, связан с допустимым VID.
- Каждый кадр, выходящий из VLAN-aware коммутатора, является нетегированным или тегирован с использованием допустимого VID. Приоритетно-тегированные кадры с недопустимым VID никогда не посылаются VLAN-aware коммутатором.

Примечание
Иногда оказывается, что некоторые приложения имеют требования, конфликтующие с естественным режимом работы IEEE 802.1Q. Например, некоторые приложения явным образом требуют приоритетно-тегированных кадров для приема оконечными устройствами.

Чтобы обеспечить полную совместимость с устаревшими VLAN-unaware (VLAN-неосведомленными) устройствами, RUGGEDCOM ROS может быть сконфигурирована для работы в режиме VLAN-unaware.

В этом режиме:

- Кадры, входящие на VLAN-unaware устройство, не ассоциированы с какой-либо сетью VLAN

- Кадры, выходящие из VLAN-unaware устройства, посылаются без изменений (то есть в том же нетегированном, 802.1Q-тегированном или приоритетно-тегированном формате, в каком они были получены)

7.1.1.9 Протокол регистрации GARP VLAN (GVRP)

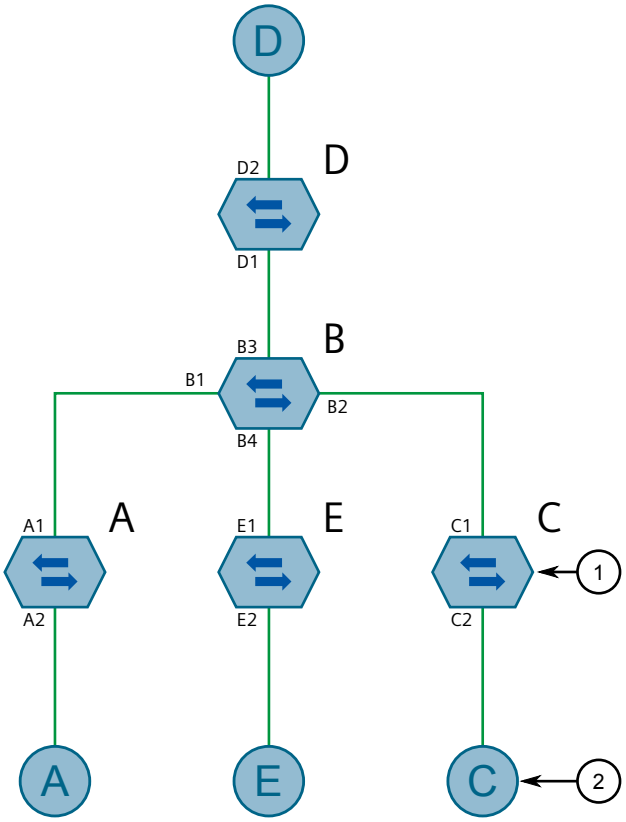
Протокол регистрации VLAN GVRP представляет собой стандартный протокол, построенный на основе GARP (базовый протокол регистрации атрибутов), чтобы автоматически распространять конфигурационную информацию VLAN в сети. Каждый коммутатор в сети необходимо сконфигурировать только с теми сетями VLAN, которые требуются для него локально. Сети VLAN, сконфигурированные в другой части сети, запоминаются через GVRP. Поддерживающая GVRP оконечная станция (например, ПК или интеллектуальное электронное устройство), настроенная для работы с определенным VID, может быть подключена к транку коммутатора, поддерживающего GVRP, и способна автоматически становиться частью требуемой сети VLAN.

Когда коммутатор посылает сообщения BPDU протокола GVRP со всех понимающих GVRP портов, сообщения BPDU протокола GVRP уведомляют остальную сеть о всех известных этому коммутатору сетях VLAN (сконфигурированных вручную или запоминаемых динамически через GVRP).

Когда GVRP-совместимый коммутатор принимает сообщение BPDU протокола GVRP, уведомляющее о группе сетей VLAN, то принимающий порт становится участником этих объявленных VLAN и начинает уведомлять об этих VLAN через понимающие GVRP порты (кроме порта, через который была получена эта информация о VLAN).

Чтобы повысить уровень безопасности сети, в которой используются виртуальные локальные сети (VLAN), понимающие GVRP порты можно настроить таким образом, чтобы запретить прием любых новых динамических VLAN, но при этом разрешить рассылку о сетях VLAN, настроенных на коммутаторе.

Ниже приведен пример использования GVRP:



① Коммутатор
② Конечный узел

Рисунок 7.1 Использование GVRP

- Коммутатор B является центральным, а все остальные коммутаторы — граничными
- Порты A1, с B1 по B4, C1, D1, D2 и E1 являются понимающими GVRP
- Порты с B1 по B4, D1 и D2 установлены на оповещение и на запоминание
- Порты A1, C1 и E1 установлены только на оповещение
- Порты A2, C2 и E2 — граничные порты
- Конечный узел D поддерживает GVRP
- Конечные узлы A, E и C не поддерживают GVRP
- Порты A2 и C2 сконфигурированы с идентификатором PVID 7
- Порт E2 сконфигурирован с идентификатором PVID 20
- Конечный узел D участвует в сети VLAN 20, поскольку он производит рассылку о сети VLAN 20 в направлении коммутатора D
- D2 становится участником VLAN 20

- Порты A1 и C1 производят рассылку об идентификаторе VID 7
- Порты B1 и B2 становятся участниками сети VLAN 7
- Порты B1, B2 и D1 производят рассылку об идентификаторе VID 20
- Порты B3, B4 и D1 становятся участниками сети VLAN 20

Для получения дополнительной информации о конфигурировании GVRP см. "Конфигурирование сетей VLAN для конкретных Ethernet-портов (Страница 171)".

7.1.1.10 Граничная сеть Private VLAN (PVLAN)

Реализация частных VLAN (PVLAN) для пограничных коммутаторов изолирует множество граничных портов VLAN друг от друга в пределах одного устройства. Если граничные порты сети VLAN сконфигурированы как *защищенные*, им запрещается отправлять кадры друг другу, но разрешается отправлять кадры на другие, незащищенные порты в пределах одной сети VLAN. Эта защита распространяется на весь трафик в сети VLAN, включая одноадресный, многоадресный и широковещательный трафик.

Для получения дополнительной информации о конфигурировании порта в качестве *защищенного* см. "Конфигурирование сетей VLAN для конкретных Ethernet-портов (Страница 171)".

Примечание
Данная функция является строго локальной для коммутатора. Граничные порты PVLAN не имеют препятствий для связи с портами за пределами коммутатора, независимо от наличия удаленной защиты.

7.1.1.11 QinQ

Технология QinQ также называется Stacked VLANs, port bridging, двойным тегированием VLAN или вложенными сетями VLAN. Она используется для наложения частной сети уровня 2 поверх публичной сети уровня 2.

Крупный оператор связи может иметь, например, несколько клиентов, в каждой из сетей которых используется множество VLAN. Существует вероятность, что идентификаторы VLAN ID, используемые этими различными клиентскими сетями, будут конфликтовать между собой при объединении в сети провайдера. При использовании двойного QinQ каждая клиентская сеть может дополнительно тегироваться с применением специфических для клиента идентификаторов VID на границах, где клиентские сети подключены к инфраструктуре оператора связи.

Любые кадры, входящие на граничный порт коммутатора оператора связи, тегируются идентификаторами VID частной сети клиента. Когда эти кадры выходят с QinQ-совместимого порта в сеть оператора связи, коммутатор всегда добавляет дополнительный тег (называемый *внешним тегом*) поверх исходного VLAN-тега кадров (называемого *внутренним тегом*). Идентификатор

VID внешнего тега является идентификатором PVID входного граничного порта для этих кадров. Это значит, что трафик от конкретного клиента тегируется его уникальным идентификатором VID и, таким образом, отделяется от трафика других клиентов. Для нетегированных входящих кадров, коммутатор добавит только наружный тег VLAN.

В пределах сети оператора связи коммутация базируется на идентификаторе VID во внешнем теге.

Оператор связи удаляет наружный VID из кадра на входе, оставляя кадр с его исходным тегом VLAN ID. Затем эти кадры пересылаются на соответствующие сети VLAN.

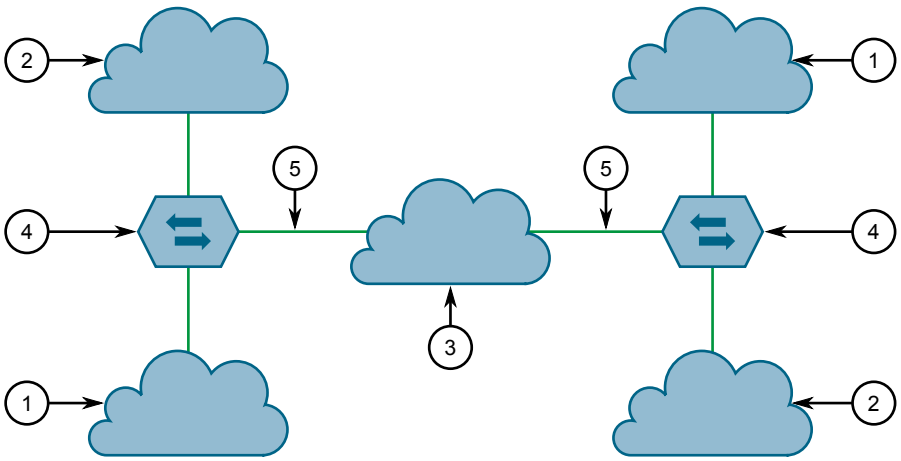
На рисунке ниже приведен пример потока трафика с использованием QinQ.

Для тегированных кадров:

- Кадры, полученные от клиента 1 с VID 100 будут нести внутренний тег 100 и внешний тег VID X (например, VLAN 110), который конфигурируется на граничном порте, подключенном к клиенту 1.
- Затем кадры от клиента 1 пересылаются через порт QinQ, неся внутренний и наружный тег.
- И наконец, когда кадры поступают на одноранговый коммутатор, наружный тег VLAN удаляется, а кадры пересылаются с внутренним тегом VLAN в сторону клиента 1.

Для нетегированных кадров:

- Кадры, полученные от клиента 2, будут нести наружный тег VID Y (например, VLAN 220), который конфигурируется на граничном порте, подключенном к клиенту 2.
- Затем кадры от клиента 2 пересылаются через порт QinQ, неся наружный тег.
- И наконец, когда кадры поступают на одноранговый коммутатор, наружный тег VLAN удаляется перед пересылкой кадров в сторону клиента 2.



① Клиент 1 (PVID — X)
② Клиент 2 (PVID — Y)
③ Инфраструктура оператора связи
④ Коммутатор
⑤ QinQ

Рисунок 7.2 Использование QinQ

Примечание
У некоторых коммутаторов, из-за их аппаратной платформы, одновременно только один порт может быть настроен в режим QinQ.

Примечание
Если для QinQ установлено enabled (включено), теги всех портов, не являющихся QinQ портами, будут отменены и их нельзя будет изменить, а все порты QinQ будут тегированы и их нельзя будет изменить.

7.1.1.12 Преимущества сети VLAN

Ниже приведено несколько преимуществ обеспечиваемых сетями VLAN.

Изоляция трафика определенного домена

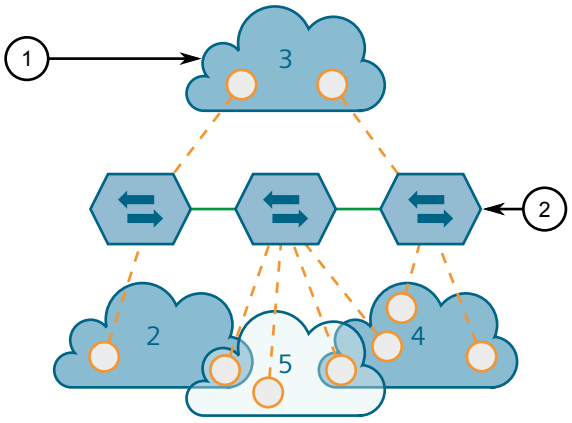
Виртуальные локальные сети (VLAN) чаще всего используются в связи с их способностью ограничивать потоки трафика между группами устройств.

Излишний широковещательный трафик можно ограничить сетью VLAN, в которой он необходим. Широковещательные штормы в одной VLAN не влияют на пользователей в других VLAN.

Для хостов в одной сети VLAN можно предотвратить случайное или преднамеренное получение IP-адреса хоста в другой сети VLAN.

Использование хитроумной фильтрации на 2-м уровне и нескольких VLAN позволяет разделить вроде бы единую IP-подсеть на несколько областей с различными политиками безопасности/доступа.

Хосты с подключением к нескольким VLAN могут передавать трафик различного типа через разные сети VLAN.



① VLAN
② Коммутатор

Рисунок 7.3 Несколько перекрывающихся VLAN

Удобство администрирования

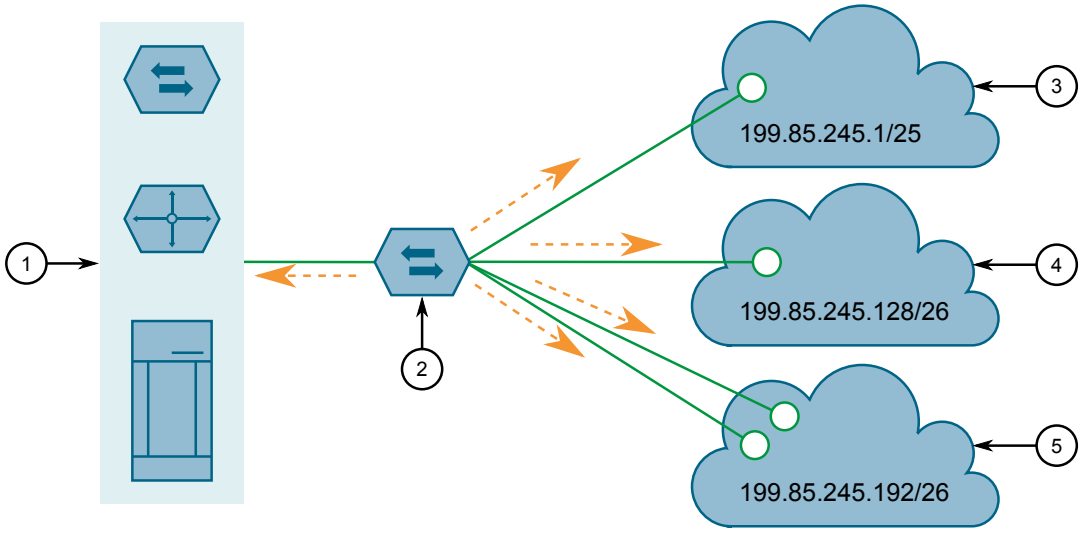
Виртуальные локальные сети (VLAN) обеспечивают адаптацию к перемещению оконечного оборудования за счет простого изменения конфигурации сетевого оборудования вместо физической реорганизации кабельной системы. Когда изменяется физическое расположение хоста, то часто также меняется его точка подключения. В этом случае при использовании VLAN достаточно просто скопировать настройки VLAN и приоритетов на новый порт.

Сокращение количества используемого оборудования

Без сетей VLAN изоляция областей трафика требует использования отдельных мостов для разделения сетей. Сети VLAN исключают необходимость в отдельных мостах.

Часто удается сократить и количество хостов сети. Нередко сервер назначается с целью обеспечения сервиса для независимых сетей. Все серверы могут быть заменены единственным сервером, с доступом ко всем VLAN через единственное подключение. Этот сервер может осуществлять маршрутизацию между сетями VLAN.

Хосты с подключением к нескольким VLAN могут передавать трафик различного типа через разные сети VLAN.



① Сервер, маршрутизатор или коммутатор уровня 3
② Коммутатор
③ VLAN 2
④ VLAN 3
⑤ VLAN 4

Рисунок 7.4 Коммуникации между виртуальными локальными сетями

7.1.2 Просмотр списка сетей VLAN

Чтобы просмотреть список всех сетей VLAN, созданных статически или неявно, перейдите в ***Virtual LANs » View VLAN Summary***. Появится таблица **VLAN Summary**.

Если сети VLAN не указаны в списке, добавьте необходимые статические сети VLAN. Для получения дополнительной информации см. "Добавление статической сети VLAN (Страница 174)".

7.1.3 Глобальное конфигурирование сетей VLAN

Чтобы сконфигурировать глобальные настройки для всех сетей VLAN, сделайте следующее:

1. Перейдите в ***Virtual LANs » Configure Global VLAN Parameters***. Появится форма **Global VLAN Parameters**.

2. Необходимо сконфигурировать следующие параметры:

Параметр	Описание
`VLAN-aware`	**Краткий обзор:** [No | Yes] **Значение по умолчанию:** Yes Устанавливает режим функционирования VLAN-осведомленный или VLAN-неосведомленный.
`Ingress Filtering`	**Краткий обзор:** [Disabled | Enabled] **Значение по умолчанию:** Disabled Включает или отключает входную фильтрацию VLAN на всех портах. Если этот параметр включен, любой тегированный пакет, поступающий на порт, который не является участником виртуальной сети, с которой связан этот пакет, отбрасывается. Если параметр отключен, пакеты не отбрасываются. **Примечание** Входная фильтрация не имеет влияния, когда порты находятся в режиме VLAN-unaware (VLAN-неосведомленный) или в режиме Q-in-Q.
`QinQ Outer TPID`	**Краткий обзор:** [0x8100 | 0x88A8] **Значение по умолчанию:** 0x8100 Выбор Ethertype для использования в качестве идентификатора протокола тегирования (TPID) на портах QinQ сети VLAN, когда для QinQ выбрано значение "включено". Кадры, входящие в порт QinQ сети VLAN будут идентифицироваться как тегированные, если первый Ethertype совпадает с этим значением; тег внешней сети VLAN с полем TPID, назначенным этому значению, будет вставлен в кадры, входящие в порт QinQ сети VLAN. **Примечание** Если для QinQ установлено enabled (включено), теги всех портов, не являющихся QinQ портами, будут отменены и их нельзя будет изменить, а все порты QinQ будут тегированы и их нельзя будет изменить.

3. Нажмите **Apply**.

7.1.4 Конфигурирование сетей VLAN для конкретных Ethernet-портов

Если VLAN ID присваивается Ethernet-порту, сеть VLAN отображается в таблице сводных сведений по VLAN, где ее можно дополнительно сконфигурировать.

Чтобы сконфигурировать VLAN для конкретного Ethernet-порта, сделайте следующее:

1. Перейдите в ***Virtual LANs » Configure Port VLAN Parameters***. Появится таблица **Port VLAN Parameters**.

2. Выберите порт. Появится форма **Port VLAN Parameters**.
3. Необходимо сконфигурировать следующие параметры:

Параметр	Описание
`Port(s)`	**Краткий обзор:** Any combination of numbers valid for this parameter Номер порта устройства (или список портов, если они объединены в группу).
`Type`	**Краткий обзор:** [Edge | Trunk | PVLANEdge | QinQ] **Значение по умолчанию:** Edge Этот параметр указывает, каким образом порт определяет свое участие в виртуальных локальных сетях (VLAN). Существует несколько типов портов: • `Edge (Граничный)` - порт является участником только одной сети VLAN (это его native VLAN, задаваемая параметром PVID). • `Trunk (Транковый)` – порт автоматически становится участником всех сконфигурированных сетей VLAN. Кадры, передаваемые с данного порта по всем сетям VLAN, кроме native VLAN этого порта, всегда будут тегированными. Этот порт также можно настроить для использования GVRP в целях автоматического конфигурирования VLAN. • `PVLANEdge` - порт является участником только одной сети VLAN (это его native VLAN, задаваемая параметром PVID) и не пересылает трафик на другие порты PVLANedge в той же VLAN. • `QinQ` - порт является транковым портом, использующим двойное тегирование VLAN, или вложенные сети VLAN. Во все кадры, выходящие из этого порта, всегда добавляется дополнительный тег VLAN. Идентификатор VID в добавляемом дополнительном теге, представляет собой идентификатор PVID входного порта кадра. Тег VLAN всегда удаляется из кадров, поступающих на этот порт. **Примечание** В зависимости от установленной аппаратной части некоторые модели коммутаторов позволяют конфигурировать только один порт коммутатора на режим QinQ за один раз.
`PVID`	**Краткий обзор:** Целое число от 1 до 4094 **Значение по умолчанию:** 1 Идентификатор порта виртуальной локальной сети (VLAN) определяет идентификатор сети VLAN, ассоциированной с нетегированными (и тегированными приоритетом 802.1p) кадрами, принимаемыми на этот порт. Кадры, тегированные ненулевым идентификатором VLAN, всегда будут ассоциированы с этим идентификатором VLAN, который извлекается из тега кадра.

Параметр	Описание
	Изменяйте этот параметр с осторожностью! По умолчанию коммутатор настроен таким образом, чтобы использовать VLAN 1 для управления, и каждый порт коммутатора настроен для использования VLAN 1. Если изменить настройки порта коммутатора таким образом, чтобы для трафика управления коммутаторами использовалась не одна VLAN, а другая, то устройства, подключенные к портам в первой VLAN, не смогут управлять этим коммутатором.
`PVID Format`	**Краткий обзор:** [Untagged | Tagged] **Значение по умолчанию:** Untagged Указывает, будут ли тегированными или нетегированными кадры, передаваемые через порт в его native VLAN (которая определена параметром `PVID`). **Примечание** Если для QinQ установлено enabled (включено), теги всех портов, не являющихся QinQ портами, будут отменены и их нельзя будет изменить, а все порты QinQ будут тегированы и их нельзя будет изменить.
`GVRP`	**Краткий обзор:** [Adv&Learn | Adv Only | Disabled] **Значение по умолчанию:** Disabled Конфигурирует режим работы протокола GVRP (базовый протокол регистрации VLAN) для порта. Существует несколько режимов работы GVRP. • `Adv&Learn (Рассылка и прием)` - через порт посылаются оповещения о всех сетях VLAN, существующих в коммутаторе (настроенные или известные из рассылки), но порт не принимает информацию о сетях VLAN. • `Adv Only (Только рассылка)` - через порт посылаются оповещения о всех сетях VLAN, существующих в коммутаторе (настроенные или известные из рассылки), но порт не принимает информацию о сетях VLAN. • `Disabled (Отключено)` - порт не способен производить какую-либо обработку по протоколу GVRP. Только транковые порты являются GVRP-совместимыми.

4. Нажмите **Apply**.

7.1.5 Управление статическими сетями VLAN

В данном разделе описывается процесс конфигурирования статических сетей VLAN и управления ими.

7.1.5.1 Просмотр списка статических сетей VLAN

Чтобы просмотреть список статических сетей VLAN, перейдите в ***Virtual LANs » Configure Static VLANs***. Появится таблица **Static VLANs**.

Если статическая сеть VLAN не указана в списке, добавьте ее. Для получения дополнительной информации см. "Добавление статической сети VLAN (Страница 174)".

7.1.5.2 Добавление статической сети VLAN

Чтобы добавить статическую сеть VLAN, сделайте следующее:

1. Перейдите в ***Virtual LANs » Configure Static VLANs***. Появится таблица **Static VLANs**.
2. Нажмите **InsertRecord**. Появится форма **Static VLANs**.
3. Необходимо сконфигурировать следующие параметры:

Примечание
Если **IGMP Options** не включены для данной сети VLAN, то сообщения IGMP и многоадресные потоки будут пересылаться непосредственно всем участникам этой VLAN. Если любой из участников сети VLAN подписывается на многоадресную рассылку, то все участники этой VLAN будут получать групповой трафик.

Параметр	Описание
`VID`	**Краткий обзор:** Целое число от 1 до 4094 **Значение по умолчанию:** 1 Идентификатор VLAN, используемый для идентификации сети VLAN в тегированных Ethernet-кадрах в соответствии с IEEE 802.1Q.
`VLAN Name`	**Краткий обзор:** Строка длиной 19 символа(ов) Имя сети VLAN представляет собой описание назначения данной VLAN (например, виртуальная локальная сеть технического назначения).
`Forbidden Ports`	**Краткий обзор:** Any combination of numbers valid for this parameter или [None] Это порты, которым не разрешается быть участниками виртуальной локальной сети (VLAN). Примеры: • `None (Отсутствует)` - всем портам коммутатора разрешается быть участниками виртуальной локальной сети (VLAN). • `2, 4-6, 8` - всем портам, за исключением портов 2, 4, 6, 7 и 8, разрешается быть участниками VLAN.

Параметр	Описание
IGMP	**Краткий обзор:** [Off | On] **Значение по умолчанию:** Off Этот параметр включает или выключает отслеживание сетевого трафика IGMP в данной сети VLAN.
DHCP	**Краткий обзор:** [Off | On] **Значение по умолчанию:** Off Этот параметр включает или выключает отслеживание сетевого трафика DHCP в данной сети VLAN.
MSTI	**Краткий обзор:** Целое число от 0 до 16 **Значение по умолчанию:** 0 Этот параметр является существенным только для протокола множественного связующего дерева (MSTP) и не оказывает влияния, если MSTP не используется. Данным параметром определяется экземпляр множественного связующего дерева (MSTI), на который должна отображаться сеть VLAN.

4. Нажмите **Apply**.

7.1.5.3 Удаление статической сети VLAN

Чтобы удалить статическую сеть VLAN, сделайте следующее:

1. Перейдите в ***Virtual LANs » Configure Static VLANs***. Появится таблица **Static VLANs**.
2. Выберите статическую сеть VLAN из таблицы. Появится форма **Static VLANs**.
3. Нажмите **Delete**.

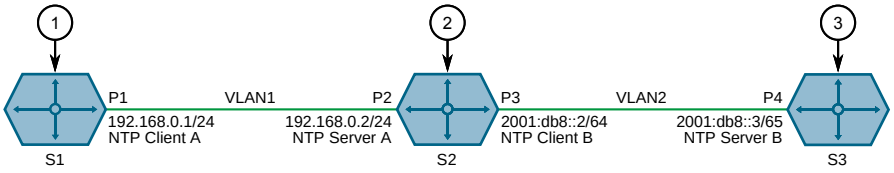
7.1.6 Пример: Конфигурирование поддержки управления на нескольких сетях VLAN

В данном примере показано, как осуществлять перемещение трафика управления по нескольким сетям VLAN.

Следующая топология соответствует сценарию, при котором системное время синхронизируется на трех устройствах RUGGEDCOM ROS в двух сетях VLAN. SNTP-пакеты отправляются назад и вперед между устройствами RUGGEDCOM ROS в модели "клиент-сервер".

⚠ ЗАМЕТКА

Указанные значения характерны для представленной топологии. Фактические значения могут отличаться, в зависимости от конфигурации пользователя.



① Коммутатор S1
② Коммутатор S2
③ Коммутатор S3

Рисунок 7.5 Топология — конфигурирование поддержки управления на нескольких сетях VLAN

Чтобы воспроизвести эту топологию, сделайте следующее:

1. Сконфигурируйте коммутатор S1 следующим образом:
   a. Подключите порт P1 к порту P2 на коммутаторе S2.
   b. Назначьте IP-адрес *192.168.0.1/24* порту P1.
   c. Сконфигурируйте порт P1 в качестве интерфейса управления. Для получения дополнительной информации см. "Добавление IP-интерфейса (Страница 92)".
   d. Назначьте порт P1 сети VLAN 1. Для получения дополнительной информации см. раздел "Конфигурирование сетей VLAN для конкретных Ethernet-портов (Страница 171)".
   e. Сконфигурируйте NTP-сервер на коммутаторе S1 следующим образом:

Сервер	Первичный
IP-адрес	192.168.0.2
Период обновления данных	1 минута

   Для получения дополнительной информации см. "Конфигурирование серверов NTP (Страница 290)".

2. Сконфигурируйте коммутатор S2 следующим образом:
   a. Подключите порт P3 к порту P4 на коммутаторе S3.
   b. Назначьте IP-адрес *192.168.0.2/24* порту P2.
   c. Назначьте IP-адрес *2001:db8::2/64* порту P3.
   d. Сконфигурируйте порт P2 в качестве вспомогательного интерфейса управления. Для получения дополнительной информации см. "Добавление IP-интерфейса (Страница 92)".
   e. Сконфигурируйте порт P3 в качестве интерфейса, не являющегося управляющим. Для получения дополнительной информации см. "Добавление IP-интерфейса (Страница 92)".
   f. Назначьте порт P2 сети VLAN 1. Для получения дополнительной информации см. раздел "Конфигурирование сетей VLAN для конкретных Ethernet-портов (Страница 171)".
   g. Назначьте порт P3 сети VLAN 2. Для получения дополнительной информации см. раздел "Конфигурирование сетей VLAN для конкретных Ethernet-портов (Страница 171)".
   h. Сконфигурируйте NTP-сервер на коммутаторе S2 следующим образом:

Сервер	Первичный
IP-адрес	2001:db8::3
Период обновления данных	1 минута

   Для получения дополнительной информации см. "Конфигурирование серверов NTP (Страница 290)".
3. Сконфигурируйте коммутатор S3 следующим образом:
   a. Назначьте IP-адрес *2001:db8::3/64* порту P4.
   b. Сконфигурируйте порт P4 в качестве интерфейса, не являющегося управляющим. Для получения дополнительной информации см. "Добавление IP-интерфейса (Страница 92)".
   c. Назначьте порт P4 сети VLAN 2. Для получения дополнительной информации см. раздел "Конфигурирование сетей VLAN для конкретных Ethernet-портов (Страница 171)".
   d. Установите SNTP на enabled (включено) на коммутаторе S3. Для получения дополнительной информации см. раздел "Включение/отключение службы NTP (Страница 289)".

4. Убедитесь в следующем:
   a. Локальные часы коммутатора S1 синхронизированы с локальными часами коммутатора S2. Для получения дополнительной информации см. "Управление NTP (Страница 289)".
   b. Локальные часы коммутатора S2 *не* синхронизированы с локальными часами коммутатора S3. Для получения дополнительной информации см. "Управление NTP (Страница 289)".
   c. SNTP-сервер не доступен на коммутаторе S2 с первичного NTP-сервера (поскольку сеть VLAN 2 не является управляющей). Для получения дополнительной информации см. "Управление NTP (Страница 289)".

7.2 Управление MAC-адресами

В данном разделе рассматривается управление MAC-адресами.

7.2.1 Просмотр списка MAC-адресов

Чтобы просмотреть список всех статических и динамически полученных MAC-адресов, перейдите в ***MAC Address Tables » View MAC Addresses***. Появится таблица **MAC Addresses**.

Если MAC-адрес не указан в списке, сделайте следующее:

1. Сконфигурируйте опции определения MAC-адресов на регулирование времени устаревания динамически определяемых MAC-адресов других устройств в сети. Для получения дополнительной информации см. "Конфигурирование опций определения MAC-адреса (Страница 178)".
2. Сконфигурируйте адрес на устройстве в качестве статического MAC-адреса. Для получения дополнительной информации см. "Добавление статического MAC-адреса (Страница 180)".

7.2.2 Конфигурирование опций определения MAC-адреса

Опции определения MAC-адреса регулируют как и когда MAC-адреса автоматически удаляются из таблицы MAC-адресов. Отдельные адреса удаляются при превышении времени таймера устаревания. Адреса также могут удаляться при отказе канала связи или изменении топологии.

Чтобы сконфигурировать опции определения MAC-адресов, сделайте следующее:

1. Перейдите в ***MAC Address Tables » Configure MAC Address Learning Options***. Появится форма **MAC Address Learning Options**.

2. Необходимо сконфигурировать следующие параметры:

Параметр	Описание
`Aging Time`	**Краткий обзор:** Целое число от 15 до 800 **Значение по умолчанию:** 300 Этот параметр задает время, в течение которого запомненный MAC-адрес хранится, пока не будет сочтен устаревшим.
`Age Upon Link Loss`	**Краткий обзор:** [No | Yes] **Значение по умолчанию:** Yes Если установлено на "Да", все запомненные MAC-адреса на отказавшем порту мгновенно будут сочтены устаревшими после обнаружения отказа канала связи. Когда возникает отказ канала связи, то коммутатор может хранить некоторые MAC-адреса, ранее запомненные через неработоспособный порт. Поскольку эти адреса не устарели, то коммутатор продолжит пересылку трафика на этот порт, препятствуя тем самым прохождению трафика к узлу назначения через новую топологию сети. Обратите внимание, что при включенном на коммутаторе протоколе резервирования сети, например, RSTP/MSTP, этот протокол резервирования может очистить запомненные на отказавшем порту MAC-адреса при отказе канала связи, независимо от настройки данного параметра.

3. Нажмите **Apply**.

7.2.3 Конфигурирование опций лавинной рассылки MAC-адресов

Чтобы сконфигурировать опции лавинной рассылки MAC-адресов, сделайте следующее:

1. Перейдите в ***MAC Address Tables » Configure MAC Address Flooding Options***. Появится таблица **Flooding Options**.
2. Выберите порт. Появится форма **Flooding Options**.
3. Необходимо сконфигурировать следующие параметры:

Параметр	Описание
`Port(s)`	**Краткий обзор:** Comma-separated list of ports Номер порта устройства (или список портов, если они объединены в группу).
`Flood Unknown Unicast`	**Краткий обзор:** [On | Off] **Значение по умолчанию:** On Обычно направленный трафик с неизвестными адресами узлов назначения рассылается через все порты. Если порт сконфигурирован таким образом, чтобы отключать лавинную рассылку такого типа, то направленный трафик

Параметр	Описание
	с неизвестными адресами не рассылается через указанный порт.

4. Нажмите **Apply**.

7.2.4 Управление статическими MAC-адресами

Статические MAC-адреса должны быть сконфигурированы, когда устройство может только получать кадры, но не передавать их. Их также может потребоваться сконфигурировать, если безопасность на уровне порта (если поддерживается) должна быть принудительной.

Также можно настроить статические MAC-адреса, указав для них высокий приоритет в ситуации, когда для трафика к определенному устройству или от него в каком-либо сегменте локальной сети должен быть назначен более высокий приоритет CoS, чем для других устройств в этом сегменте локальной сети.

Примечание
MAC-адрес не может быть определен в сети VLAN, которая не сконфигурирована в таблице статических сетей VLAN. При получении кадра с тегом неизвестной сети VLAN на защищенный порт это считается нарушением безопасности и RUGGEDCOM ROS автоматически генерирует оповещение безопасности на уровне порта.

7.2.4.1 Просмотр списка статических MAC-адресов

Чтобы просмотреть список статических MAC-адресов, перейдите в ***MAC Address Tables » Configure Static MAC Addresses***. Появится таблица **Static MAC Addresses**.

Если статические MAC-адреса не были сконфигурированы, добавьте необходимые адреса. Для получения дополнительной информации см. "Добавление статического MAC-адреса (Страница 180)".

7.2.4.2 Добавление статического MAC-адреса

Чтобы добавить статический MAC-адрес в таблицу статических MAC-адресов, сделайте следующее:

1. Перейдите в ***MAC Address Tables » Configure Static MAC Addresses***. Появится таблица **Static MAC Addresses**.
2. Нажмите **InsertRecord**. Появится форма **Static MAC Addresses**.

3. Необходимо сконфигурировать следующие параметры:

Параметр	Описание
`MAC Address`	**Краткий обзор:** ##-##-##-##-##-## where ## ranges 0 to FF MAC-адрес, запомненный коммутатором. Не более 6 символов подстановки можно использовать для указания диапазона MAC-адресов, запоминание которых модулем обеспечения безопасности на уровне порта разрешено (когда для параметра Port Security установлен режим статических MAC-адресов "Static MAC"). Символы подстановки должны начинаться с конца MAC-адреса, причем все подстановочные символы должны следовать непрерывно. Примеры: • 00-0A-DC-**-* * - * * означает все пространство MAC-адресов RuggedCom. • 00-0A-DC-12-3*-** означает диапазон, который начинается с 00-0A-DC-12-30-00 и заканчивается значением 00-0A-DC-12-3F-FF.
`VID`	**Краткий обзор:** Целое число от 1 до 4094 или [ANY] **Значение по умолчанию:** 1 VLAN-идентификатор той сети VLAN, в которой функционирует данный MAC-адрес. Опция "Любой" позволяет запоминать MAC-адрес через модуль безопасности на уровне порта на любых сетях VLAN, которые сконфигурированы на коммутаторе.
`Port`	**Краткий обзор:** 1 to maximum port number или [Learn] **Значение по умолчанию:** Learn Введите номер порта, на котором находится устройство с данным адресом. Выбираемый режим безопасности порта не должен быть "802.1X". Если порт должен производить автоматическое запоминание адресов, то установите для этого параметра значение "запоминать". Опция "Запоминать" применима для безопасности на уровне порта в режиме "Статический MAC-адрес".

4. Нажмите **Apply**.

7.2.4.3 Удаление статического MAC-адреса

Чтобы удалить статический MAC-адрес из таблицы статических MAC-адресов, сделайте следующее:

1. Перейдите в ***MAC Address Tables » Configure Static MAC Addresses***. Появится таблица **Static MAC Addresses**.
2. Выберите MAC-адрес из таблицы. Появится форма **Static MAC Addresses**.
3. Нажмите **Delete**.

7.2.5 Очистка всех динамических MAC-адресов

Чтобы очистить список динамических MAC-адресов, сделайте следующее:

1. Перейдите в ***MAC Address Tables » Purge MAC Address Table***. Появится форма **Purge MAC Address Table**.
2. Нажмите **Confirm**.

7.3 Управление многоадресной фильтрацией

Групповой (многоадресный) трафик можно фильтровать с помощью отслеживания протокола группового управления сети интернет (IGMP) или протокола многоадресной регистрации GARP (GMRP).

7.3.1 Управление IGMP

Протокол IGMP используется IP-хостами, чтобы сообщать многоадресным маршрутизаторам о своей принадлежности к группе хостов. По мере того, как хосты подписываются на конкретные многоадресные рассылки или отписываются от них, потоки трафика направляются к этим хостам или минуют их.

Протокол IGMP работает между многоадресными маршрутизаторами и IP-хостами. Если неуправляемый коммутатор размещается между многоадресными маршрутизаторами и их хостами, то многоадресные потоки будут распределены по всем портам. Это может привести к существенному трафику на тех портах, где он не требуется и где от него нет никаких выгод.

Если функция отслеживания сетевого трафика IGMP включена, она будет воздействовать на сообщения IGMP, посылаемые с маршрутизатора и хоста, ограничивая потоки трафика к соответствующим сегментам локальной сети.

⚠ ЗАМЕТКА

RUGGEDCOM ROS запрещает хостам IGMP подписку на следующие особые многоадресные адреса:

- от 224.0.0.0 до 224.0.0.255
- 224.0.1.129

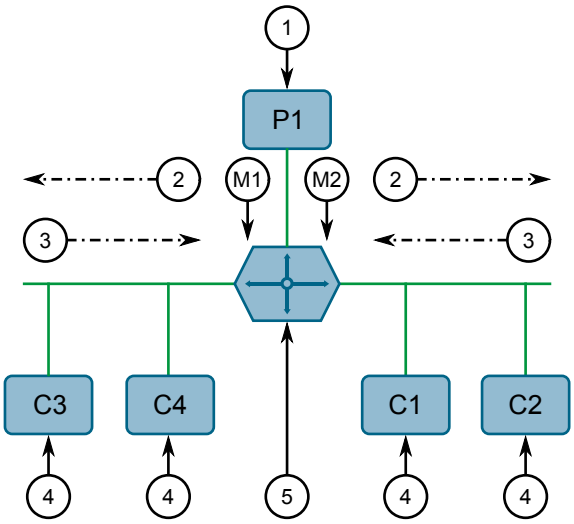
Эти адреса зарезервированы для протоколов маршрутизации и IEEE 1588. Если отчет о принадлежности IGMP содержит один из этих адресов, отчет пересылается коммутатором без запоминания информации о хосте.

7.3.1.1 Концепция IGMP

В данном разделе рассматриваются некоторые принципы, имеющие значение для реализации фильтрации многоадресных рассылок с помощью IGMP.

Работа IGMP

На приведенной ниже схеме показан простой пример использования IGMP.



① Источник
② Запросы принадлежности
③ Отчеты о принадлежности
④ Потребитель
⑤ Многоадресный маршрутизатор

Рисунок 7.6 Пример работы IGMP

Один IP-хост *источник* (P1) генерирует два многоадресных потока IP-трафика, M1 и M2. Существует четыре потенциальных *потребителя* этих потоков, C1-C4. Многоадресный маршрутизатор выясняет, какой хост желает подписаться на тот или иной поток, посылая общие запросы о принадлежности в каждый из сегментов.

В этом примере на общий запрос о принадлежности, отправленный на сегмент C1-C2, приходит ответ в виде отчета о принадлежности (или *подписке*), указывающий, что требуется подписка на поток M2. Маршрутизатор будет перенаправлять поток M2 в сегмент C1-C2. Аналогичным образом маршрутизатор определяет, что он должен перенаправлять поток M1 в сегмент C3-C4.

Потребитель может подписаться на любое число многоадресных рассылок, выдавая отчет о принадлежности для каждой группы. Когда какой-либо хост выдает отчет о принадлежности, другие хосты в том же сегменте сети, которым также требуется принадлежность к той же группе, подавляют свои собственные запросы, поскольку они будут дублироваться. Таким образом, протокол IGMP гарантирует, что сегмент будет запрашивать только один отчет о принадлежности для каждой группы.

Маршрутизатор периодически опрашивает каждый из своих сегментов, чтобы определить, подписан хотя бы один потребитель на определенный поток. Если маршрутизатор не получает ответа в течение заданного периода

времени (обычно два интервала времени запроса), то он прекратит передачу группового потока в данный сегмент.

Более общий метод отсечения имеет место, когда потребители, желающие отписаться, отправляют сообщение IGMP *leave group (покинуть группу)*. Маршрутизатор моментально отправит специфичный для группы запрос о принадлежности, чтобы определить, остались ли еще в сегменте подписчики этой группы. После того как отпишется последний потребитель групповой рассылки, маршрутизатор прекратит передачу группового потока в данный сегмент.

Функционирование IGMP на коммутаторе

Функция IGMP Snooping (отслеживание сетевого трафика IGMP) предусматривает средства, позволяющие коммутаторам отслеживать (то есть наблюдать) работу маршрутизаторов, отвечать сообщениями о подписке/отписке от имени портов потребителя трафика и соответствующим образом отсекать многоадресные потоки. Существует два режима IGMP, под которые можно сконфигурировать коммутатор: активный и пассивный.

- **Активный режим**

  Протокол IGMP поддерживает режим работы *без маршрутизатора*.

  Если коммутатор в этом режиме используется без многоадресного маршрутизатора, то он способен функционировать таким образом, как если бы он был многоадресным маршрутизатором, посылающим общие запросы IGMP.

- **Пассивный режим**

  Если коммутатор в этом режиме используется в сети с многоадресным маршрутизатором, то коммутатор можно сконфигурировать для работы в пассивном режиме IGMP. Этот режим предотвращает передачу коммутатором запросов, которые могут создать помехи маршрутизатору, приводя к прекращению выдачи IGMP-запросов.

Примечание
Коммутатор, работающий в пассивном режиме, требует присутствия многоадресного маршрутизатора, иначе он вообще не сможет пересылать групповые потоки.

Примечание
Для функционирования IGMP хотя бы один коммутатор отслеживания сетевого трафика IGMP должен находиться в активном режиме.

Правила отслеживания сетевого трафика IGMP

Отслеживание сетевого трафика IGMP подчиняется следующим правилам:

- Когда групповой источник начинает многоадресную рассылку, поток трафика будет немедленно блокирован для сегментов, от которых не были получены подписки.

- Коммутатор будет пересылать весь групповой трафик на порты, с которыми соединены многоадресные маршрутизаторы, если не предусмотрена иная конфигурация.
- Пакеты с групповым IP-адресом назначения в диапазоне 224.0.0.X, которые не являются IGMP-пакетами, всегда пересылаются на все порты. Такой режим работы основан на том факте, что многие системы не посылают отчетов о принадлежности на групповые IP-адреса в этом диапазоне, хотя продолжают анализировать такие пакеты.
- Коммутатор реализует *прокси-отчетность* IGMPv2 (т. е. отчеты о принадлежности, полученные от устройств в нисходящем направлении, суммируются и используются коммутатором для выдачи собственных отчетов).
- Коммутатор будет посылать IGMP-отчеты о принадлежности только с тех портов, с которыми соединены многоадресные маршрутизаторы, поскольку передача отчетов о принадлежности на хосты может привести к непредусмотренному исключению хоста из подписки на конкретную групповую рассылку.
- Многоадресные маршрутизаторы используют IGMP для выбора главного маршрутизатора, называемого *querier (запрашивающее устройство)*. *Запрашивающее устройство* — это маршрутизатор с самым нижним IP-адресом. Все остальные маршрутизаторы становятся незапрашивающими устройствами, участвующими только в пересылке группового трафика. Коммутаторы, работающие в активном режиме, участвуют в выборе запрашивающего устройства подобно многоадресным маршрутизаторам.
- Когда процесс выбора запрашивающего устройства завершен коммутатор просто ретранслирует IGMP-запросы, полученные от запрашивающего устройства.
- Посылая пакеты IGMP, коммутатор использует свой собственный IP-адрес, если имеет его для сети VLAN, в которой посылаются пакеты, либо адрес 0.0.0.0, если коммутатору не назначен IP-адрес.

Примечание
Коммутаторы, отслеживающие сетевой трафик IGMP, осуществляют отсечение группового трафика, используя групповой MAC-адрес назначения многоадресных кадров, который зависит от группового IP-адреса группы. IP-адрес W.X.Y.Z соответствует MAC-адресу 01-00-5E-XX-YY-ZZ, где XX — нижние 7 бит X, а YY и ZZ — просто Y и Z, закодированные в шестнадцатеричной системе.

Также следует отметить, что такие групповые IP-адреса как, например, 224.1.1.1 и 225.1.1.1, будут отображаться на один и тот же MAC-адрес 01-00-5E-01-01-01. Это проблема, для которой рабочая группа IETF по вопросам сетей в настоящее время еще не опубликовала решения. Пользователям рекомендуется принять это к сведению и избегать данной проблемы.

IGMP и RSTP

Изменение топологии посредством RSTP может привести к некорректности маршрутов, выбранных для транспорта группового трафика. В результате трафик многоадресных рассылок будет теряться.

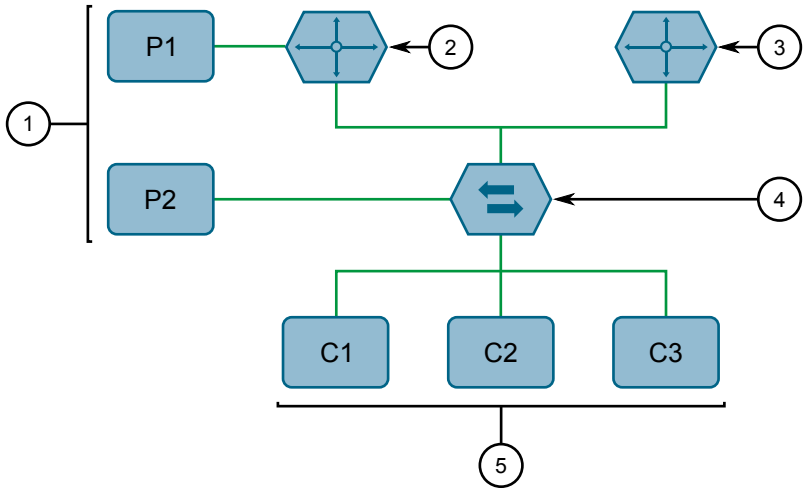
Если RSTP обнаруживает изменение в сетевой топологии, то IGMP будет предпринимать определенные действия, чтобы избежать утраты способности доставлять многоадресные рассылки и сократить время сходимости:

- Коммутатор немедленно начнет выдавать IGMP-запросы (если он находится в активном режиме IGMP), чтобы получить информацию о потенциальной принадлежности к новой группе.
- Коммутатор может быть настроен для временной веерной рассылки многоадресных потоков со всех портов, которые не сконфигурированы в качестве граничных портов RSTP.

Взаимодействие коммутатора и маршрутизатора посредством протокола IGMP

Приведенный ниже пример иллюстрирует задачи, связанные с использованием нескольких маршрутизаторов, поддержкой VLAN и коммутацией.

Источник трафика P1 находится в сети VLAN 2, тогда как P2 находится в сети VLAN 3. Потребитель трафика C1 находится в обеих VLAN, тогда как C2 и C3 находятся в сетях VLAN 3 и 2 соответственно. Маршрутизатор 2 находится в сети VLAN 2, предположительно для перенаправления группового трафика в удаленную сеть, либо сам действует в качестве источника группового трафика.



① Источник
② Многоадресный маршрутизатор 1
③ Многоадресный маршрутизатор 2
④ Коммутатор

⑤ Хост

Рисунок 7.7 Пример взаимодействия коммутатора и маршрутизатора посредством протокола IGMP

В данном примере:

- P1, маршрутизатор 1, маршрутизатор 2 и C3 находятся в сети VLAN 2
- P2 и C2 расположены в сети VLAN 3
- C1 находится в обеих сетях — VLAN 2 и VLAN 3

В этом примере мы будем предполагать, что все устройства рассматривают маршрутизатор 1 в качестве запрашивающего для VLAN 2, а маршрутизатор 2 представляет собой простое не запрашивающее устройство. В данном случае коммутатор будет периодически принимать запросы от маршрутизатора 1 и, таким образом, поддерживать обмен информацией относительно того, какие из его портов соединены с многоадресным маршрутизатором. Однако порт коммутатора, который соединен с маршрутизатором 2, должен быть вручную сконфигурирован как *порт маршрутизатора*. В противном случае коммутатор не будет передавать многоадресные потоки или сообщения о подписке/отписке на маршрутизатор 2.

Обратите внимание, что VLAN 3 не имеет внешнего многоадресного маршрутизатора. Коммутатор необходимо сконфигурировать для работы в режиме *без маршрутизатора*, а также он должен выдавать общие запросы принадлежности, как если бы он был маршрутизатором.

- **Обработка подписок**

  Если хосту C1 нужно подписаться на многоадресные потоки P1 и P2, то он будет генерировать два отчета о принадлежности. Подписка от C1 в сети VLAN 2 приведет к тому, что коммутатор немедленно инициирует собственную подписку на рассылку многоадресного маршрутизатора 1 (и будет выдавать сообщение о собственной подписке в ответ на запросы).

  Отчет о принадлежности от C1 для VLAN 3 приведет к тому, что коммутатор немедленно начнет пересылать групповой трафик от P2 к C2.

- **Обработка отписок**

  Когда хост C1 принимает решение отписаться от групповой рассылки, он выдает запрос отписки на коммутатор. Коммутатор опрашивает соответствующий порт, чтобы определить, не является ли хост C1 последним участником группы от этого порта. Если хост C1 является последним (или единственным) участником, то данная группа будет немедленно отсечена от порта.

  Если хост C1 отписался от групповой рассылки без выдачи сообщения об отписке от группы, а затем не ответил на общий запрос принадлежности, то коммутатор прекратит ретрансляцию трафика после двух запросов.

  Когда последний порт отпишется от групповой рассылки (или устареет информация о его принадлежности к группе), коммутатор выдаст IGMP-отчет об отписке на маршрутизатор.

7.3.1.2 Просмотр списка составов многоадресных групп

С помощью отслеживания сетевого трафика IGMP RUGGEDCOM ROS регистрирует информацию о групповой принадлежности для каждого порта по отдельности на основании отчетов о принадлежности, наблюдаемых ею между маршрутизатором и хостом.

Чтобы просмотреть список многоадресных принадлежностей, перейдите в ***Multicast Filtering » View IGMP Group Membership***. Появится таблица **IGMP Group Membership**.

Таблица содержит следующую информацию:

Параметр	Описание
`Port`	**Краткий обзор:** 1 to maximum port number Номер порта.
`VID`	**Краткий обзор:** Целое число от 0 до 65535 VLAN-идентификатор той сети VLAN, в которой действует данная групповая рассылка.
`Group`	**Краткий обзор:** ###.###.###.### where ### ranges from 0 to 255 Адрес групповой рассылки.
`Ver`	**Краткий обзор:** [v3 | v2 | v1] Указывает версию IGMP запомненной многоадресной группы.
`Reporter`	**Краткий обзор:** ###.###.###.### where ### ranges from 0 to 255 Указывает IP-адрес источника, который сообщает о подписке на многоадресную группу.
`Age`	**Краткий обзор:** Целое число от 0 до 7210 Указывает текущий возраст в секундах многоадресной группы IP, запомненной на порте.

Если таблица пуста, сделайте следующее:

- Убедитесь, что на устройство посылается трафик.
- Убедитесь, что на устройстве надлежащим образом выполнено конфигурирование IGMP. Для получения дополнительной информации см. "Конфигурирование IGMP (Страница 189)".

7.3.1.3 Просмотр информации о пересылке для многоадресных групп

Информация о многоадресной пересылке для каждой комбинации источника, группы и сети VLAN, запомненной RUGGEDCOM ROS, регистрируется в таблице многоадресной пересылки IGMP.

Чтобы просмотреть таблицу многоадресной пересылки IGMP, перейдите в ***Multicast Filtering » View IGMP Multicast Forwarding***. Появится таблица **IGMP Multicast Forwarding**.

Таблица содержит следующую информацию:

Параметр	Описание
`VID`	**Краткий обзор:** Целое число от 0 до 65535 VLAN-идентификатор той сети VLAN, в которой действует данная групповая рассылка.
`Group`	**Краткий обзор:** ###.###.###.### where ### ranges from 0 to 255 Адрес групповой рассылки.
`Source`	**Краткий обзор:** ###.###.###.### where ### ranges from 0 to 255 или [*] Адрес источника. * означает все возможные адреса источников.
`Joined Ports`	**Краткий обзор:** Comma-separated list of ports Все порты, которые в настоящее время получают многоадресный трафик для указанной групповой рассылки.
`Router Ports`	**Краткий обзор:** Comma-separated list of ports Все порты, которые были сконфигурированы вручную или обнаружены динамически (путем анализа трафика, идущего от маршрутизатора) в качестве портов, обеспечивающих связь с многоадресными маршрутизаторами.

Если таблица пуста, сделайте следующее:

- Убедитесь, что на устройство посылается трафик.
- Убедитесь, что на устройстве надлежащим образом выполнено конфигурирование IGMP. Для получения дополнительной информации см. "Конфигурирование IGMP (Страница 189)".

7.3.1.4 Конфигурирование IGMP

Чтобы сконфигурировать IGMP, сделайте следующее:

1. Убедитесь, что существует не менее одной статической сети VLAN с включенным IGMP. Для получения дополнительной информации см. "Управление статическими сетями VLAN (Страница 173)".
2. Перейдите в ***Multicast Filtering » Configure IGMP Parameters***. Появится форма **IGMP Parameters**.
3. Необходимо сконфигурировать следующие параметры:

Параметр	Описание
`Mode`	**Краткий обзор:** [Passive | Active] **Значение по умолчанию:** Passive Определяет режим IGMP. Опции включают: • `Passive (Пассивный)` - коммутатор пассивно отслеживает сетевой трафик IGMP и никогда не посылает IGMP-запросы.

Параметр	Описание
	• `Active (Активный)` - коммутатор генерирует IGMP-запросы, если в течение некоторого времени не обнаружены запросы от лучшего кандидата на роль запрашивающего устройства.
`IGMP Version`	**Краткий обзор:** [v2 | v3] **Значение по умолчанию:** v2 Указывает сконфигурированную версию IGMP на коммутаторе. Опции включают: • `v2` - Устанавливает версию IGMP на версию 2. При выборе для коммутатора отслеживания сетевого трафика все отчеты и запросы IGMP выше v2, пересылаются, но не добавляются в таблицу многоадресной пересылки IGMP. • `v3` - Устанавливает версию IGMP на версию 3. Общие запросы генерируются в формате IGMPv3, все версии IGMP-сообщений обрабатываются коммутатором, а трафик отсекается только на основе группового адреса групповой рассылки.
`Query Interval`	**Краткий обзор:** Целое число от 10 до 3600 **Значение по умолчанию:** 60 Интервал времени между IGMP-запросами, которые генерирует коммутатор. **Примечание** Этот параметр также влияет на интервал времени принадлежности к группе (то есть время устаревания подписки на групповую рассылку), поэтому он оказывает воздействие даже в PASSIVE (ПАССИВНОМ) режиме.
`Router Ports`	**Краткий обзор:** Comma-separated list of ports **Значение по умолчанию:** None Этот параметр определяет порты, которые подключены к многоадресным маршрутизаторам. Если известные порты маршрутизатора не сконфигурированы, то коммутатор может оказаться в состоянии определить их, однако рекомендуется предварительно конфигурировать порты.
`Router Forwarding`	**Краткий обзор:** [Off | On] **Значение по умолчанию:** On Этот параметр определяет, будут ли групповые потоки всегда ретранслироваться на многоадресные маршрутизаторы.
`RSTP Flooding`	**Краткий обзор:** [Off | On] **Значение по умолчанию:** Off Этот параметр определяет, будут ли RSTP-порты, не являющиеся граничными, временно переходить в режим лавинной рассылки при обнаружении изменения топологии. Такая лавинная рассылка желательна, если

Параметр	Описание
	важнее всего гарантированная доставка группового потока после изменения топологии.

4. Нажмите **Apply**.

7.3.2 Управление GMRP

GMRP представляет собой приложение базового протокола регистрации атрибутов (GARP), который обеспечивает на уровне 2 механизм для управления принадлежностью к групповой рассылке в сети с коммутацией уровня 2. Этот протокол позволяет Ethernet-коммутаторам и оконечным станциям регистрировать и отменять регистрацию принадлежности к групповым рассылкам с помощью других коммутаторов в локальной сети, а также распространять соответствующую информацию по всем коммутаторам в локальной сети, которые поддерживают работу расширенных служб фильтрации.

GMRP представляет собой принятый в качестве промышленного стандарта сетевой протокол, первоначально определенный в стандарте IEEE 802.1D-1998 и расширенный в IEEE 802.1Q-2005. Протокол GARP был определен в стандарте IEEE 802.1D-1998 и обновлен в 802.1D-2004.

7.3.2.1 Концепция GMRP

В данном разделе рассматриваются некоторые принципы, имеющие значение для реализации фильтрации многоадресных рассылок с помощью GMRP:

Подписка на групповую рассылку

Чтобы подписаться на групповую рассылку, оконечная станция передает GMRP-сообщение *о подписке*. Коммутатор, принявший сообщение *о подписке*, добавляет порт, через который было получено это сообщение, к групповой рассылке, указанной в сообщении. Затем коммутатор распространяет это сообщение *о подписке* по всем остальным хостам в сети VLAN, один из которых предполагается в качестве источника группового трафика.

Когда коммутатор передает обновления GMRP (от портов, поддерживающих протокол GMRP), то коммутатор уведомляет остальную часть сети обо всех известных ему многоадресных рассылках, сконфигурированных вручную или запомненных динамически через GMRP.

Пока хотя бы один хост в сети с коммутацией уровня 2 зарегистрирован для данной групповой рассылки, трафик от соответствующего группового источника будет переноситься по сети. Групповой трафик от источника направляется каждым коммутатором в сети лишь к тем портам, от которых были получены сообщения о подписке на данную групповую рассылку.

Отписка от групповой рассылки

Периодически коммутатор посылает GMRP-запросы в форме сообщений *отписаться от всех подписок*. Если хост (коммутатор или оконечная станция) намерен сохранить подписку на групповую рассылку, то он повторно подтверждает принадлежность к группе, отвечая соответствующим запросом *подписаться*. В противном случае он может ответить сообщением *отписаться* или просто не ответить. Если коммутатор принимает сообщение *отписаться* или не получает ответа от хоста в период тайм-аута, то коммутатор удаляет этот хост из групповой рассылки.

Замечания по GMRP

Поскольку протокол GMRP является приложением GARP, транзакции производятся с использованием протокола GARP. GMRP определяет следующие два типа атрибутов:

- Тип атрибута группы — используется для идентификации MAC-адресов группы
- Тип атрибута требований к сервису — используется с целью идентификации требований к сервису для группы

Атрибуты требований к сервису используются для изменения режима работы принимающего порта при фильтрации многоадресных рассылок на один из следующих вариантов:

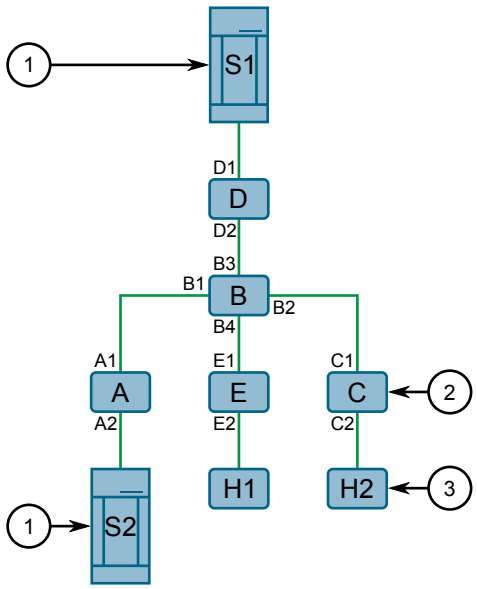
- Ретранслировать весь трафик групповой рассылки в заданную сеть VLAN, либо
- Ретранслировать весь неизвестный трафик (многоадресных рассылок), для которого нет подписчиков, зарегистрированных на данном устройстве в сети VLAN

Если для GMRP выбрано disabled (отключено), полученные пакеты GMRP будут пересылаться как любой другой трафик. В противном случае пакеты GMRP будут обрабатываться и не пересылаться.

Установление принадлежности с помощью GMRP

Следующий пример показывает, как сеть хостов и коммутаторов может динамически присоединиться к двум многоадресным группам с помощью GMRP.

В данном примере имеется два многоадресных источника, S1 и S2, производящих многоадресные рассылки 1 и 2 соответственно. Сеть из пяти коммутаторов, включая один центральный коммутатор (B), соединяет источники с двумя хостами, H1 и H2, которые принимают многоадресные потоки от S1 и S2 соответственно.



① Источник групповой рассылки
② Коммутатор
③ Хост групповой рассылки

Рисунок 7.8 Пример установления принадлежности с помощью GMRP

Хосты и коммутаторы устанавливают принадлежность к многоадресным группам 1 и 2 следующим образом:

1. Хост H1 не поддерживает GMRP, но ему необходимо видеть трафик для групповой рассылки 1. Поэтому порт E2 на коммутаторе E статически настроен таким образом, чтобы ретранслировать трафик групповой рассылки 1.
2. Коммутатор E уведомляет сеть о принадлежности к групповой рассылке 1 через порт E1, делая порт B4 на коммутаторе B участником групповой рассылки 1.
3. Коммутатор B распространяет сообщение *о подписке*; это приводит к тому, что порты A1, C1 и D1 становятся участниками групповой рассылки 1.
4. Хост H2 поддерживает протокол GMRP и посылает запрос *подписаться* на групповую рассылку 2 на порт C2, который становится, таким образом, участником групповой рассылки 2.
5. Коммутатор C распространяет сообщение *о подписке*; это приводит к тому, что порты A1, B2, D1 и E1 становятся участниками групповой рассылки 2.

После того как сведения о регистрации на базе GMRP будут распространены через сеть, как описано выше, многоадресный трафик от S1 и S2 сможет достигать своих получателей, как описано ниже:

- Источник S1 передает на порт D2 групповой трафик, который затем ретранслируется через порт D1, предварительно ставший участником групповой рассылки 1.

- Коммутатор B ретранслирует трафик групповой рассылки 1 через порт B4 в направлении коммутатора E.
- Коммутатор E ретранслирует трафик групповой рассылки 1 через порт E2, который был статически сконфигурирован для участия в групповой рассылке 1.
- Хост H1, подключенный к порту E2, получает, таким образом, групповую рассылку 1.
- Источник S2 передает на порт A2 групповой трафик, который затем ретранслируется через порт A1, предварительно ставший участником групповой рассылки 2.
- Коммутатор B ретранслирует трафик групповой рассылки 2 через порт B2 в направлении коммутатора C.
- Коммутатор C ретранслирует трафик групповой рассылки 2 через порт C2, предварительно ставший участником групповой рассылки 2.
- И наконец, хост H2, подключенный к порту C2, получает групповую рассылку 2.

7.3.2.2 Просмотр сводных сведений о многоадресных группах

Чтобы просмотреть сводную информацию обо всех многоадресных группах, перейдите в ***Multicast Filtering » View Multicast Group Summary***. Появится таблица **Multicast Group Summary**.

Таблица содержит следующую информацию:

Параметр	Описание
`VID`	**Краткий обзор:** Целое число от 0 до 65535 VLAN-идентификатор той сети VLAN, в которой действует данная групповая рассылка.
`MAC Address`	**Краткий обзор:** ##-##-##-##-##-## where ## ranges 0 to FF Групповой MAC-адрес.
`Static Ports`	**Краткий обзор:** Any combination of numbers valid for this parameter Порты, которые статически подписаны на эту групповую рассылку посредством статической конфигурации в таблице статических MAC-адресов и на которые ретранслируется трафик групповой рассылки.
`GMRP Dynamic Ports`	**Краткий обзор:** Any combination of numbers valid for this parameter Порты, которые динамически подписаны на эту групповую рассылку посредством приложения GMRP и на которые ретранслируется трафик групповой рассылки.

7.3.2.3 Глобальное конфигурирование GMRP

Чтобы сконфигурировать глобальные настройки для GMRP, сделайте следующее:

1. Перейдите в ***Multicast Filtering » Configure Global GMRP Parameters***. Появится форма **Global GMRP Parameters**.
2. Необходимо сконфигурировать следующие параметры:

Параметр	Описание
`GMRP Enable`	**Краткий обзор:** [No | Yes] **Значение по умолчанию:** No Глобальное включение или отключение GMRP. Когда GMRP глобально отключен, конфигурации GMRP на отдельных портах игнорируются. Если GMRP глобально включен, то каждый порт можно сконфигурировать индивидуально.
`RSTP Flooding`	**Краткий обзор:** [On | Off] **Значение по умолчанию:** Off Этот параметр определяет, будут ли RSTP-порты, не являющиеся граничными, временно переходить в режим лавинной рассылки при обнаружении изменения топологии. Такая лавинная рассылка желательна, если важнее всего гарантированная доставка группового потока после изменения топологии.
`Leave Timer`	**Краткий обзор:** Целое число от 600 до 300000 **Значение по умолчанию:** 4000 Период времени ожидания в миллисекундах после выдачи сообщения "Отписаться" или "Отменить все подписки" и до удаления зарегистрированных многоадресных рассылок. Если для определенных адресов будут получены сообщения с запросом подписки до истечения времени этого таймера, то регистрация таких адресов будет сохранена.

3. Нажмите **Apply**.

7.3.2.4 Конфигурирование GMRP для конкретных Ethernet-портов

Чтобы сконфигурировать GMRP для конкретного Ethernet-порта, сделайте следующее:

1. Убедитесь, что для GMRP сконфигурированы глобальные настройки. Для получения дополнительной информации см. "Глобальное конфигурирование GMRP (Страница 195)".
2. Перейдите в ***Multicast Filtering » Configure Port GMRP Parameters***. Появится таблица **Port GMRP Parameters**.
3. Выберите Ethernet-порт. Появится форма **Port GMRP Parameters**.

4. Необходимо сконфигурировать следующие параметры:

Параметр	Описание
`Port(s)`	**Краткий обзор:** Any combination of numbers valid for this parameter Номер порта устройства (или список портов, если они объединены в группу).
`GMRP`	**Краткий обзор:** [Disabled | Adv Only | Adv&Learn] **Значение по умолчанию:** Disabled Конфигурируется функционирование протокола GMRP (протокол групповой регистрации GARP) для порта. Существует несколько режимов функционирования протокола GMRP: • `Disabled (Отключено)` - порт не способен производить какую-либо обработку по протоколу GMRP. • `Adv Only (Только рассылка)` - через порт посылаются оповещения обо всех групповых адресах, существующих в коммутаторе (настроенные или известные из рассылки), но порт не принимает информацию о групповых адресах. • `Adv&Learn (Рассылка и прием)` - через порт посылаются оповещения обо всех групповых адресах, существующих в коммутаторе (настроенные или известные из рассылки), и порт принимает информацию о групповых адресах.

5. Нажмите **Apply**.

7.3.2.5 Просмотр списка статических многоадресных групп

Чтобы просмотреть список статических многоадресных групп, перейдите в ***Multicast Filtering » Configure Static Multicast Groups***. Появится таблица **Static Multicast Groups**.

Если статическая многоадресная группа отсутствует в списке, добавьте ее. Для получения дополнительной информации см. "Добавление статической многоадресной группы (Страница 196)".

7.3.2.6 Добавление статической многоадресной группы

Чтобы добавить статическую многоадресную группу с другого устройства, сделайте следующее:

1. Перейдите в ***Multicast Filtering » Configure Static Multicast Groups***. Появится таблица **Static Multicast Groups**.
2. Нажмите **InsertRecord**. Появится форма **Static Multicast Groups**.

3. Необходимо сконфигурировать следующие параметры:

Параметр	Описание
`MAC Address`	**Краткий обзор:** ##-##-##-##-##-## where ## ranges 0 to FF **Значение по умолчанию:** 00-00-00-00-00-00 Групповой MAC-адрес.
`VID`	**Краткий обзор:** Целое число от 1 до 4094 **Значение по умолчанию:** 1 VLAN-идентификатор той сети VLAN, в которой действует данная групповая рассылка.
`Ports`	**Краткий обзор:** Any combination of numbers valid for this parameter **Значение по умолчанию:** None Список с разделителями-запятыми всех портов, на которые пересылается трафик многоадресной группы. Если порт является частью группы агрегирования каналов (LAG) или транкового порта, укажите все порты в группе агрегирования каналов.

4. Нажмите **Apply**.

7.3.2.7 Удаление статической многоадресной группы

Чтобы удалить статическую многоадресную группу, сделайте следующее:

1. Перейдите в ***Multicast Filtering » Configure Static Multicast Groups***. Появится таблица **Static Multicast Groups**.
2. Выберите группу из таблицы. Появится форма **Static Multicast Groups**.
3. Нажмите **Delete**.

8 Уровень 3

В данной главе приведено описание особенностей RUGGEDCOM ROS 3-го уровня (сетевого уровня).

8.1 Управление коммутацией 3-го уровня

В данном разделе рассматривается управление коммутацией 3-го уровня.

Примечание
Коммутация 3-го уровня поддерживает только адреса IPv4 (и не поддерживает адреса IPv6).

Примечание
Коммутация 3-го уровня поддерживает трафик, направляемый на индивидуальные адреса. Коммутация 3-го уровня для многоадресного и широковещательного трафика не поддерживается.

8.1.1 Основные сведения о коммутации 3-го уровня

Традиционная коммутация работает на 2-ом уровне модели OSI, где пакеты отправляются на конкретный порт коммутатора на основании целевых MAC-адресов и сетей VLAN. Маршрутизация работает на 3-ем уровне, где пакеты отправляются на конкретный IP-адрес следующего транзитного участка на основании целевого IP-адреса.

RUGGEDCOM ROS поддерживает настройку правил коммутации 3-го уровня, дающих возможность пересылать IP-трафик между двумя существующими сетями VLAN на аппаратном уровне.

В данном разделе рассматриваются некоторые принципы, имеющие значение для реализации коммутации 3-го уровня в RUGGEDCOM ROS.

8.1.1.1 Таблица переадресации коммутатора 3-го уровня

Чтобы направить пакет с конкретным целевым IP-адресом, устройству необходима следующая информация:

- **Выходной интерфейс (подсеть)**

  Эта информация хранится в таблице маршрутизации устройства.

  Примечание
  В коммутируемом сетевом сегменте 2-го уровня сеть VLAN представляет собой IP-подсеть.

- **Следующий транзитный участок или MAC-адрес**

  Данная информация хранится в таблице ARP, относящейся к коммутации 3-го уровня.

  Примечание
  Если следующим транзитным участком является сама целевая подсеть, требуется MAC-адрес целевого хоста.

Коммутация 3-го уровня преобразует эту информацию о маршрутизации в правила коммутации 3-го уровня. Эти правила также называют *информационная база пересылки (FIB) коммутации 3-го уровня* или *информационная таблица пересылки коммутации 3-го уровня*. Коммутация 3-го уровня определяет, как переключать конкретный поток трафика.

Специализированные интегральные схемы (ASIC) 3-го уровня коммутации хранят правила коммутации 3-го уровня в отдельных таблицах троичной памяти с адресацией по содержимому (TCAM) для хостов и подсетей. Правила коммутации 3-го уровня могут статически конфигурироваться или динамически запоминаться (или *автоматически запоминаться*).

Примечание
Правила коммутации 3-го уровня могут динамически определяться только для соседних хостов. Для удаленных хостов и подсетей правила необходимо статически конфигурировать.

Примечание
Максимальное число правил коммутации 3-го уровня составляет , включая правил для хостов и правила для подсетей.

8.1.1.2 Правила статической коммутации 3-го уровня

При создании статического маршрута через управление коммутацией можно явно сконфигурировать ускорение аппаратной части. Если выбрано аппаратное ускорение, соответствующее правило коммутации 3-го уровня устанавливается в таблицу TCAM схемы ASIC и никогда не устаревает.

Примечание
Только потоки трафика ICMP, TCP и UDP будут ускоряться IP/схемой ASIC коммутации 3-го уровня.

Примечание
При использовании статически сконфигурированных правил коммутации 3-го уровня пересылка IP может быть включена (enabled) или отключена (disabled). Для получения информации о конфигурировании пересылки IP см. "Конфигурирование IP-сервисов (Страница 96)".

8.1.1.3 Динамическое запоминание коммутации 3-го уровня

Для статических маршрутов без аппаратного ускорения или для динамических маршрутов правила коммутации 3-го уровня могут динамически запоминаться на основании программных решений маршрутизатора.

После успешной маршрутизации определенного количества для одного потока схема ASIC коммутации 3-го уровня начинает коммутировать остальные пакеты, принадлежащие тому же потоку. Поток — это однонаправленный трафик между двумя хостами. Например, трафик, протекающий между портами от одного хоста к другому, считается потоком. Трафик, протекающий в противоположном направлении между теми же портами, считается другим потоком.

RUGGEDCOM ROS поддерживает хост-ориентированный метод автоматического запоминания, при котором устройство использует IP-адреса источника и пункта назначения для идентификации потока трафика.

Каждый поток составляет одно правило.

Коммутатор 3-го уровня постоянно отслеживает активность (т. е. наличие трафика) для динамически запомненных правил. По этой причине динамически запомненные правила могут удаляться через конфигурируемое время из-за неактивности.

8.1.1.4 Взаимодействие между пересылкой IP и коммутацией 3-го уровня

Чтобы использовать правила статической коммутации 3-го уровня, пересылка IP может быть включена (enabled) или отключена (disabled). Однако для использования динамически запомненных правил коммутации 3-го уровня пересылка IP должна быть включена (enabled). Для получения информации о конфигурировании пересылки IP см. "Конфигурирование IP-сервисов (Страница 96)".

Ниже показано как пересылка IP взаимодействует с коммутацией 3-го уровня в RUGGEDCOM ROS.

Пересылка IP	Коммутация 3-го уровня отключена	Статическая коммутация 3-го уровня	Динамическая коммутация 3-го уровня
Отключено	Обе функции отключены	Статическая коммутация 3-го уровня	Невозможно

Пересылка IP	Коммутация 3-го уровня отключена	Статическая коммутация 3-го уровня	Динамическая коммутация 3-го уровня
Включено	Без аппаратного ускорения	Статическая коммутация 3-го уровня	Статическая и динамическая коммутация 3-го уровня

8.1.1.5 Таблица ARP коммутатора 3-го уровня

Маршрутизатору необходимо знать хост назначения или MAC-адрес шлюза следующего транзитного участка. Таким образом, программное обеспечение поддерживает таблицу протокола преобразования адресов (ARP), которая привязывает IP-адреса к MAC-адресам. Эта же информация также необходима схеме ASIC коммутации 3-го уровня при переключении IP-пакетов между подсетями.

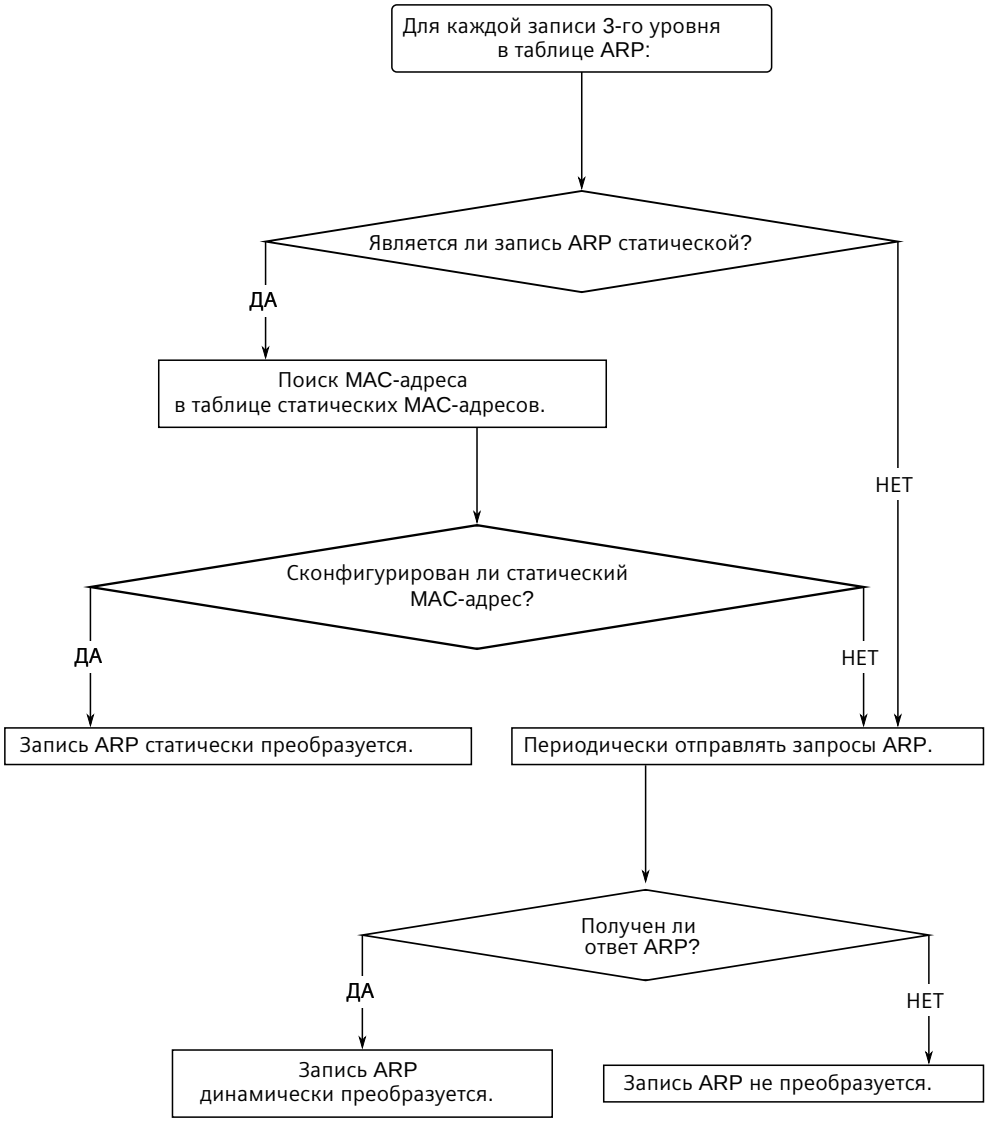
Примечание
Записи ARP могут статически конфигурироваться и преобразовываться, если статические MAC-адреса, которым они соответствуют, конфигурируются в **Static MAC Address Table**. В противном случае записи ARP будут динамически преобразовываться каждые 60 секунд.

Получение MAC-адреса пункта назначения или шлюза обычно происходит через ARP. Однако записи ARP также могут статически конфигурироваться в коммутаторе 3-го уровня, благодаря чему не происходит их тайм-аута. При конфигурировании статической записи ARP, если для параметра MAC Address (MAC-адрес) не введено значение, адрес автоматически преобразуется через ARP, а затем статически сохраняется. Он сохраняется при перезагрузках устройства.

Если для конкретного пункта назначения не сконфигурирована статическая запись ARP, будет создана динамическая запись ARP и произойдет автоматическое преобразование MAC-адреса пункта назначения.

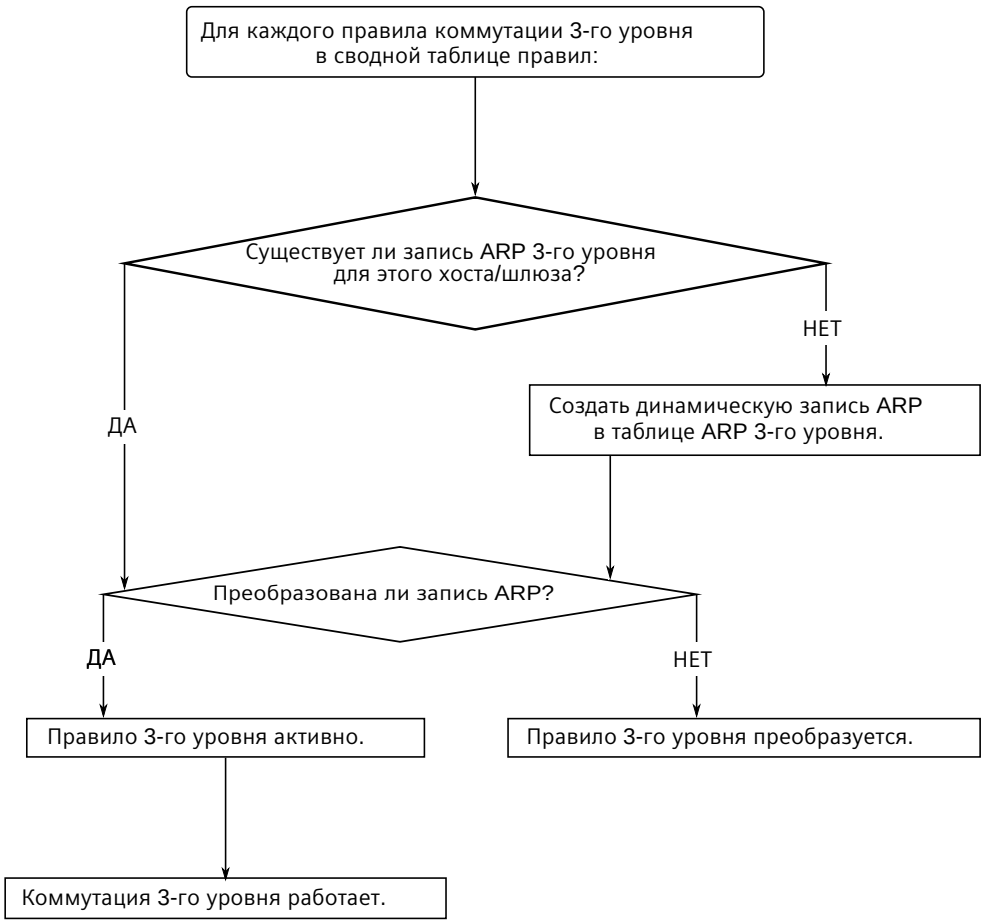
Преобразование ARP 3-го уровня

На приведенной ниже схеме показано преобразование записей ARP в RUGGEDCOM ROS.



Преобразование правил коммутации 3-го уровня

На приведенной ниже схеме показано преобразование правил коммутации 3-го уровня в RUGGEDCOM ROS.



8.1.1.6 Маршрутизируемые интерфейсы коммутатора 3-го уровня

RUGGEDCOM ROS позволяет сконфигурировать до 255 интерфейсов (сетей VLAN). Чтобы сделать интерфейс маршрутизируемым для одноадресного трафика IPv4, адрес IPv4 необходимо сконфигурировать статически или присвоить интерфейсу через DHCP. Для получения дополнительной информации см. "Управление IP-интерфейсами (Страница 91)".

8.1.2 Конфигурирование коммутации 3-го уровня

Чтобы сконфигурировать коммутацию 3-го уровня, сделайте следующее:

Примечание
Избегайте конфигурирования групп агрегирования каналов связи (LAG), если включена коммутация 3-го уровня. Для получения дополнительной

информации см. "Управление группами агрегирования каналов связи (Страница 267)".

1. Добавьте необходимые сети VLAN. Для получения дополнительной информации см. "Добавление статической сети VLAN (Страница 174)".
2. Назначьте IP-адреса сконфигурированным сетям VLAN. Для получения дополнительной информации см. "Добавление IP-интерфейса (Страница 92)".
3. Назначьте необходимые порты сконфигурированным сетям VLAN. Для получения дополнительной информации см. "Конфигурирование сетей VLAN для конкретных Ethernet-портов (Страница 171)".
4. Сконфигурируйте режим одноадресной передачи и время устаревания. Для получения дополнительной информации см. "Конфигурирование опций коммутации 3-го уровня (Страница 205)".
5. Если выбран статический режим одноадресной передачи, добавьте необходимые целевые IP-адреса и шлюзы следующего транзитного участка. Для получения дополнительной информации см. "Управление правилами одноадресной статической передачи (Страница 206)".
6. Если выбран режим статической одноадресной передачи, добавьте необходимые статические записи таблицы ARP. Для получения дополнительной информации см. "Управление статическими записями в таблице ARP (Страница 207)".
7. Протестируйте конфигурацию путем отправления трафика и проверки следующего:
   a. Записи ARP преобразованы в **ARP Table**. Для получения дополнительной информации см. "Просмотр списка записей в таблице ARP (Страница 207)".
   b. Правила активны в **Rule Summary Table**. Для получения дополнительной информации см. "Просмотр правил маршрутизации (Страница 209)".
   c. Осуществляется отправка и прием трафика. Для получения дополнительной информации см. "Вывод диагностики для конкретных Ethernet-портов (Страница 73)".

Примеры конфигурирования см. в "Пример: Конфигурирование коммутации 3-го уровня (Страница 210)" и "Пример: Конфигурирование коммутации 3-го уровня с использованием нескольких коммутаторов (Страница 212)".

8.1.3 Конфигурирование опций коммутации 3-го уровня

Чтобы сконфигурировать опции коммутации 3-го уровня, сделайте следующее:

1. Перейдите в ***Layer 3 Switching » Configure Switch Options***. Появится форма **Switch Options**.

2. Необходимо сконфигурировать следующие параметры:

Параметр	Описание
`Unicast Mode`	**Краткий обзор:** [Disabled | Static | Auto] **Значение по умолчанию:** Disabled Disabled (Отключено) — коммутация 3-го уровня отключена. Static (Статический) — будут использоваться только статически сконфигурированные правила коммутации 3-го уровня. Auto (Автоматический) — будут использоваться как статически сконфигурированные, так и динамически запомненные правила коммутации 3-го уровня. В этом режиме используется максимальное аппаратное ускорение маршрутизации.
`Aging Time`	**Краткий обзор:** Целое число от 16 до 600 **Значение по умолчанию:** 32 Этот параметр конфигурирует время удержания динамически запомненного правила для потока трафика, который стал неактивным, после которого это правило удаляется из таблицы пересылки коммутации 3-го уровня.

3. Нажмите **Apply**.

8.1.4 Управление правилами одноадресной статической передачи

В данном разделе рассматривается управление правилами одноадресной статической передачи.

8.1.4.1 Просмотр правил одноадресной статической передачи

Чтобы просмотреть список правил одноадресной статической передачи, перейдите в ***Layer 3 Switching » Configure Static Unicast Rules***. Если элементы таблицы были сконфигурированы, появится таблица **Static Unicast Rules**.

При необходимости правила одноадресной статической передачи можно сконфигурировать. Для получения дополнительной информации о добавлении правил одноадресной статической передачи см. "Добавление правила одноадресной статической передачи (Страница 206)".

8.1.4.2 Добавление правила одноадресной статической передачи

Чтобы добавить правило одноадресной статической передачи, сделайте следующее:

1. Перейдите в ***Layer 3 Switching » Configure Static Unicast Rules***. Появится **Static Unicast Rules Table**.

2. Нажмите **InsertRecord**. Появится форма **Static Unicast Rules**.
3. Необходимо сконфигурировать следующие параметры:

Параметр	Описание
`Destination`	**Краткий обзор:** ###.###.###.###/## where ### ranges from 0 to 255 and ## ranges from 0 to 32 **Значение по умолчанию:** ANY IP-адрес или подсеть назначения. Для соответствия правилу IP-адрес назначения входящего пакета должен принадлежать подсети.
`Gateway`	**Краткий обзор:** ###.###.###.### where ### ranges from 0 to 255 IP-адрес следующего транзитного участка, на который будут пересылаться совпадающие одноадресные пакеты. **Примечание** Если **"Адресат"** является напрямую связанным соседним устройством, для параметра **Gateway (Шлюз)** не должно поставляться значение.

4. Нажмите **Apply**.

8.1.4.3 Удаление правила одноадресной статической передачи

Чтобы удалить правило одноадресной статической передачи, сделайте следующее:

1. Перейдите в ***Layer 3 Switching » Configure Static Unicast Rules***. Появится таблица **Static Unicast Rules**.
2. Выберите запись, которую необходимо удалить. Появится форма **Static Unicast Rules**.
3. Нажмите **Delete**.

8.1.5 Управление статическими записями в таблице ARP

В данном разделе рассматривается управление статическими записями в таблице ARP.

8.1.5.1 Просмотр списка записей в таблице ARP

Чтобы просмотреть список записей коммутации 3-го уровня в таблице ARP, перейдите в ***Layer 3 Switching » Configure/View ARP Table***. Если элементы таблицы были сконфигурированы, появится **ARP Table**.

После конфигурирования правил одноадресной передачи таблица ARP коммутации 3-го уровня автоматически заполнится по мере динамического запоминания записей ARP. При необходимости статические записи в таблицу ARP также можно добавить. Для получения дополнительной информации о добавлении статических записей в таблицу ARP см. "Добавление статической записи в таблицу ARP (Страница 208)".

8.1.5.2 Добавление статической записи в таблицу ARP

Чтобы добавить статическую запись в таблицу ARP, сделайте следующее:

1. Перейдите в ***Layer 3 Switching » Configure/View ARP Table***. Появится форма **ARP Table**.
2. Нажмите **InsertRecord**. Появится форма **ARP Table**.
3. Необходимо сконфигурировать следующие параметры:

Параметр	Описание
`IP Address`	**Краткий обзор:** ###.###.###.### where ### ranges from 0 to 255 IP-адрес сетевого устройства, которое описывает запись.
`VID`	**Краткий обзор:** Целое число от 0 до 65535 **Значение по умолчанию:** N/A VLAN-идентификатор той сети VLAN, в которой функционирует данный MAC-адрес.
`MAC Address`	**Краткий обзор:** ##-##-##-##-##-## where ## ranges 0 to FF **Значение по умолчанию:** 00-00-00-00-00-00 MAC-адрес сетевого устройства, указанный IP-адресом.
`Static`	**Краткий обзор:** [True | False] **Значение по умолчанию:** True Указывает, является запись статической или динамической. Статические записи конфигурируются в результате действия управления. Динамические записи автоматически запоминаются устройством и могут быть запомнены повторно.
`Status`	**Краткий обзор:** [Unresolved | Resolved] Статус преобразования записи ARP: Resolved (Преобразовано) — адресная пара MAC-IP преобразована и работает. Unresolved (Не преобразовано) — устройство не преобразовало адресную пару MAC-IP и продолжает периодически посылать запросы ARP.

4. Нажмите **Apply**.

8.1.5.3 Удаление статической записи в таблице ARP

Чтобы удалить статическую запись в таблицу ARP, сделайте следующее:

1. Перейдите в ***Layer 3 Switching » Configure/View ARP Table***. Появится форма **ARP Table**.
2. Выберите запись, которую необходимо удалить. Появится форма **ARP Table**.
3. Нажмите **Delete**.

8.1.6 Просмотр правил маршрутизации

Чтобы просмотреть список правил маршрутизации, перейдите в ***Layer 3 Switching » View Rule Summary***. При наличии сконфигурированных статических или динамических правил одноадресной статической передачи появится **Rule Summary Table**.

Таблица содержит следующую информацию:

Параметр	Описание
`Destination`	**Краткий обзор:** Строка длиной 20 символа(ов) IP-адрес или подсеть назначения. Для соответствия правилу IP-адрес назначения входящего пакета должен принадлежать подсети.
`Out-VLAN(s)`	**Краткий обзор:** Comma separated list of up to 2 numbers ranging from 1 to 4095 Исходящие сети VLAN. Совпадающие одноадресные или многоадресные пакеты будут отправляться на эту сеть/эти сети VLAN.
`Gateway`	**Краткий обзор:** ###.###.###.### where ### ranges from 0 to 255 IP-адрес следующего транзитного участка, на который будут пересылаться совпадающие одноадресные пакеты.
`Static`	**Краткий обзор:** [True | False] Указывает, является правило статическим или динамическим. Статические правила конфигурируются в результате действия управления. Динамические правила автоматически запоминаются устройством и могут быть запомнены повторно в соответствии с параметром Aging Time (Время устаревания).
`Status`	**Краткий обзор:** [Active | Resolving] Указывает, является правило рабочим в настоящий момент или нет: Active (Активно) — правило является полностью рабочим и может быть применено, поэтому выполняется аппаратное ускорение.

Параметр	Описание
	Resolving (Преобразуется) — правило еще не работает из-за частично непреобразованной информации, например, ARP или MAC-адрес шлюза в таблице MAC-адресов. Аппаратное ускорение не выполняется.

8.1.7 Очистка правил динамической маршрутизации аппаратного обеспечения

Очистка правил динамической маршрутизации аппаратного обеспечения удаляет все динамически запомненные правила из **Layer 3 Switch Forwarding Table**.

Примечание
Очистить можно только динамические правила. Статичные правила, сконфигурированные в **Layer 3 Switch Forwarding Table**, никогда не устаревают. Для получения дополнительной информации о включении аппаратного ускорения см. "Основные сведения о коммутации 3-го уровня (Страница 199)".

Чтобы очистить динамические правила маршрутизации аппаратной части, сделайте следующее:

1. Перейдите в ***Layer 3 Switching*** и выберите **Flush Learned Rules**. Появится форма **Flush Learned Rules**.
2. Нажмите **Confirm**.

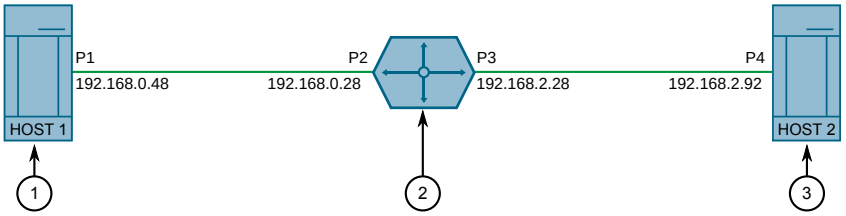
8.1.8 Пример: Конфигурирование коммутации 3-го уровня

В данном примере показано, как сконфигурировать коммутацию 3-го уровня.

Следующая топология соответствует сценарию, при котором два хоста в отдельных сетях подключаются к устройству RUGGEDCOM ROS, сконфигурированному в качестве коммутатора 3-го уровня. Отправка двунаправленного трафика между двумя хостами осуществляется через RUGGEDCOM ROS.

⚠ ЗАМЕТКА

Указанные значения характерны для представленной топологии. Фактические значения могут отличаться, в зависимости от конфигурации пользователя.



① Хост 1
② Устройство RUGGEDCOM ROS
③ Хост 2

Рисунок 8.1 Базовая топология коммутации 3-го уровня

Чтобы воспроизвести эту топологию, сделайте следующее:

Примечание
Хосты 1 и 2 могут являться устройствами 2-го уровня или ПК. Конкретные инструкции по конфигурированию см. в документации производителя оригинального оборудования (OEM).

1. Сконфигурируйте Хост 1 в соответствии с топологией следующим образом:
   a. Подключите P1 к P2 устройства RUGGEDCOM ROS.
   b. Назначьте IP-адрес *192.168.0.48* интерфейсу P1.
   c. Установите шлюз по умолчанию *192.168.0.28*.
2. Сконфигурируйте Хост 2 в соответствии с топологией следующим образом:
   a. Подключите P4 к P3 устройства RUGGEDCOM ROS.
   b. Назначьте IP-адрес *192.168.2.92* интерфейсу P4.
   c. Установите шлюз по умолчанию *192.168.2.28*.

3. Сконфигурируйте устройство RUGGEDCOM ROS в качестве коммутатора 3-го уровня:
   a. Добавьте сети VLAN 1 и VLAN 2. Для получения дополнительной информации см. "Добавление статической сети VLAN (Страница 174)".
   b. Назначьте IP-адрес *192.168.0.28* сети VLAN 1 и IP-адрес *192.168.2.28* сети VLAN 2. Для получения дополнительной информации см. "Добавление IP-интерфейса (Страница 92)".
   c. Назначьте P2 сети VLAN1 и P3 сети VLAN2. Для получения дополнительной информации см. "Конфигурирование сетей VLAN для конкретных Ethernet-портов (Страница 171)".
   d. Включите режим одноадресной передачи. Для получения дополнительной информации см. "Конфигурирование опций коммутации 3-го уровня (Страница 205)".
   e. Если для режима одноадресной передачи выбрано *Автоматический*, переходите к шагу Шаг 4. В ином случае сконфигурируйте правила одноадресной статической передачи для адресата и шлюза следующим образом:

Адресат	Шлюз
192.168.0.48	0.0.0.0
192.168.2.92	0.0.0.0

   Для получения дополнительной информации о конфигурировании правил одноадресной статической передачи см. "Добавление правила одноадресной статической передачи (Страница 206)".
   f. Отправьте несколько запросов/ответов ARP от Хостов 1 и 2 на устройство RUGGEDCOM ROS.
4. Отправьте двунаправленный трафик (например, UDP, TCP, ICMP) между Хостом 1 и Хостом 2, а затем убедитесь в следующем:
   a. Записи ARP преобразованы в **ARP Table**. Для получения дополнительной информации см. "Просмотр списка записей в таблице ARP (Страница 207)".
   b. Правила активны в **Rule Summary Table**. Для получения дополнительной информации см. "Просмотр правил маршрутизации (Страница 209)".
   c. Отправка и прием трафика осуществляются на двух конечных хостах. Для получения дополнительной информации см. "Вывод диагностики для конкретных Ethernet-портов (Страница 73)".

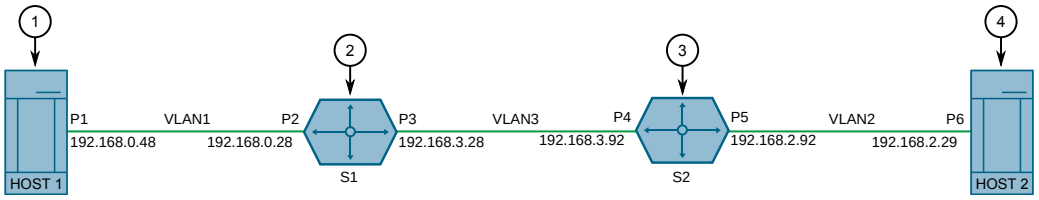
8.1.9 Пример: Конфигурирование коммутации 3-го уровня с использованием нескольких коммутаторов

В данном примере показано, как сконфигурировать коммутацию 3-го уровня с использованием нескольких коммутаторов.

Следующая топология соответствует сценарию, при котором два хоста отдельных сетях подключаются к двум устройствам RUGGEDCOM ROS, сконфигурированным в качестве коммутаторов 3-го уровня. Отправка двунаправленного трафика между двумя хостами осуществляется через устройства RUGGEDCOM ROS.

⚠ ЗАМЕТКА

Указанные значения характерны для представленной топологии. Фактические значения могут отличаться, в зависимости от конфигурации пользователя.



① Хост 1
② S1
③ S2
④ Хост 2

Рисунок 8.2 Топология — коммутация 3-го уровня с помощью двух коммутаторов

Чтобы воспроизвести эту топологию, сделайте следующее:

Примечание

Хосты 1 и 2 могут являться устройствами 2-го уровня или ПК. Конкретные инструкции по конфигурированию см. в документации производителя оригинального оборудования (OEM).

1. Сконфигурируйте Хост 1 в соответствии с топологией следующим образом:
   a. Подключите P1 к P2 устройства 1 RUGGEDCOM ROS.
   b. Назначьте IP-адрес *192.168.0.48* интерфейсу P1.
   c. Установите шлюз по умолчанию *192.168.0.28*.
2. Сконфигурируйте Хост 2 в соответствии с топологией следующим образом:
   a. Подключите P6 к P5 коммутатора S2.
   b. Назначьте IP-адрес *192.168.2.29* интерфейсу P6.
   c. Установите шлюз по умолчанию *192.168.2.92*.

3. Сконфигурируйте S1 в качестве коммутатора 3-го уровня:
   a. Подключите P3 к P4 коммутатора S2.
   b. Добавьте сети VLAN 1 и VLAN 3. Для получения дополнительной информации см. "Добавление статической сети VLAN (Страница 174)".
   c. Назначьте IP-адрес *192.168.0.28* сети VLAN 1 и IP-адрес *192.168.3.28* сети VLAN 3. Для получения дополнительной информации см. "Добавление IP-интерфейса (Страница 92)".
   d. Назначьте P2 сети VLAN1 и P3 сети VLAN3. Для получения дополнительной информации см. "Конфигурирование сетей VLAN для конкретных Ethernet-портов (Страница 171)".
   e. Установите режим одноадресной передачи на *Автоматический*. Для получения дополнительной информации см. "Конфигурирование опций коммутации 3-го уровня (Страница 205)".
   f. Сконфигурируйте правила одноадресной статической передачи для адресата и шлюза следующим образом:

Адресат	Шлюз
192.168.2.0/24	192.168.3.92

   Для получения дополнительной информации о конфигурировании правил одноадресной статической передачи см. "Добавление правила одноадресной статической передачи (Страница 206)".
4. Сконфигурируйте S2 в качестве коммутатора 3-го уровня:
   a. Добавьте сети VLAN 3 и VLAN 2. Для получения дополнительной информации см. "Добавление статической сети VLAN (Страница 174)".
   b. Назначьте IP-адрес *192.168.3.92* сети VLAN 3 и IP-адрес *192.168.2.92* сети VLAN 2. Для получения дополнительной информации см. "Добавление IP-интерфейса (Страница 92)".
   c. Установите режим одноадресной передачи на *Автоматический*. Для получения дополнительной информации см. "Конфигурирование опций коммутации 3-го уровня (Страница 205)".
   d. Сконфигурируйте правила одноадресной статической передачи для адресата и шлюза следующим образом:

Адресат	Шлюз
192.168.0.0/24	192.168.3.28

   Для получения дополнительной информации о конфигурировании правил одноадресной статической передачи см. "Добавление правила одноадресной статической передачи (Страница 206)".
5. Отправьте несколько запросов/ответов ARP от Хоста 1 на коммутатор S1 и от Хоста 2 на коммутатор S2.

6. Отправьте двунаправленный трафик (например, UDP, TCP, ICMP) между Хостом 1 и Хостом 2, а затем убедитесь в следующем:
   a. Записи ARP преобразованы в **ARP Table**. Для получения дополнительной информации см. "Просмотр списка записей в таблице ARP (Страница 207)".
   b. Правила активны в **Rule Summary Table**. Для получения дополнительной информации см. "Просмотр правил маршрутизации (Страница 209)".
   c. Отправка и прием трафика осуществляются на двух конечных хостах. Для получения дополнительной информации см. "Вывод диагностики для конкретных Ethernet-портов (Страница 73)".

8.1.9 Пример: Конфигурирование коммутации 3-го уровня с использованием нескольких коммутаторов

9 Резервирование сети

В данном разделе описывается конфигурирование функций резервирования RUGGEDCOM ROS и управление ими.

9.1 Управление протоколом связующего дерева

В данном разделе рассматривается управление протоколом связующего дерева.

9.1.1 Функционирование протокола RSTP

Протокол связующего дерева (STP) стандарта 802.1D был разработан для создания устойчивых к сбоям сетей, в которых имеются резервные связи, но в то же время из активной топологии удалено лишнее для предотвращения образования петель. Если протокол STP запущен, то он обеспечивает, чтобы передача кадров останавливалась после перебоя в работе канала связи, пока все мосты в сети не будут гарантированно оповещены о новой топологии. При использовании значений, рекомендуемых в стандарте 802.1D, продолжительность этого периода составляет 30 секунд.

Протокол быстрого связующего дерева (RSTP, IEEE 802.1w) был дальнейшим развитием протокола связующего дерева 802.1D. В нем период стабилизации топологии заменен активным обменом сигналами для установления связи между мостами, который гарантирует быстрое распространение информации о топологии по сети. RSTP также предлагает ряд других важных инноваций, которые включают в себя следующее:

- Оповещения об изменении топологии в RSTP могут исходить от любого моста и рассылаться далее любыми его соседями, что приводит к более быстрому распространению информации об адресах, в отличие от изменений топологии в STP, которые должны пройти через корневой мост, прежде чем они могут быть распространены в сети.
- Протокол RSTP в явной форме распознает две роли блокирования — альтернативный и резервный порт, которые включаются в процесс вычисления момента, когда следует производить запоминание адресов и пересылку информации. В то же время STP распознает только одно состояние — блокировку для портов, которые не должны производить пересылку информации.
- Мосты RSTP генерируют собственные конфигурационные сообщения, даже если они не могут принять что-либо от корневого моста. Это приводит

к быстрому обнаружению отказа. Напротив, протокол STP должен ретранслировать только конфигурационные сообщения, принятые на корневой порт с выделенных портов. Если коммутатор STP не может принять сообщение от своего соседа, то он не в состоянии узнать достоверно, где именно на пути возникла неисправность.

- RSTP обеспечивает распознавание граничного порта, позволяя портам на границе сети пересылать кадры сразу после активизации, одновременно предохраняя их от возникновения петель.

Имея существенно лучшие характеристики, чем STP, определяемый стандартом IEEE 802.1w протокол RSTP все же требует несколько секунд для восстановления связности сети после возникновения изменений в топологии.

Переработанная и хорошо оптимизированная версия протокола RSTP была определена в издании 802.1D-2004 стандарта IEEE. Версия IEEE 802.1D-2004 RSTP уменьшает время восстановления сети всего лишь до нескольких миллисекунд и оптимизирует функционирование RSTP для различных сценариев.

RUGGEDCOM ROS поддерживает IEEE 802.1D-2004 RSTP.

9.1.1.1 Состояния и роли в RSTP

Мосты RSTP исполняют роль корневого или выделенного моста. Один мост (корневой) является логическим центром сети. Все остальные мосты в сети являются выделенными мостами. Протокол RSTP также назначает каждому порту моста состояние и роль. Состояние RSTP описывает, что происходит с данным портом в плане запоминания адресов и пересылки кадров. Роль RSTP описывает, главным образом, следующее: действует ли порт в направлении центра или границ сети, а также может ли он использоваться в данный момент.

Состояние

Существует три состояния RSTP: "сбрасывание", "запоминание" и "пересылка".

Порт входит в состояние сбрасывания сразу после включения. В этом состоянии порт не запоминает адреса и не участвует в передаче кадров. Порт ищет трафик RSTP, чтобы определить свою роль в сети. Если определено, что порт будет играть активную роль в сети, то состояние изменится на состояние запоминания.

Вход в состояние запоминания производится, когда порт готов играть активную роль в сети. В этом состоянии порт запоминает адреса, но не участвует в передаче кадров. В сети с RSTP-мостами время, затрачиваемое в этом состоянии, обычно очень короткое. RSTP-мосты, работающие в режиме совместимости с STP, будут затрачивать от шести до 40 секунд в этом состоянии.

После *запоминания* мост переведет устройство в состояние пересылки данных. В этом состоянии порт определяет адреса и участвует в передаче кадров.

⚠ ЗАМЕТКА

В RUGGEDCOM ROS вводится еще два состояния: "отключено" и "соединение отсутствует". Эти состояния используются для мониторинга сети и поиска и устранения неисправностей.

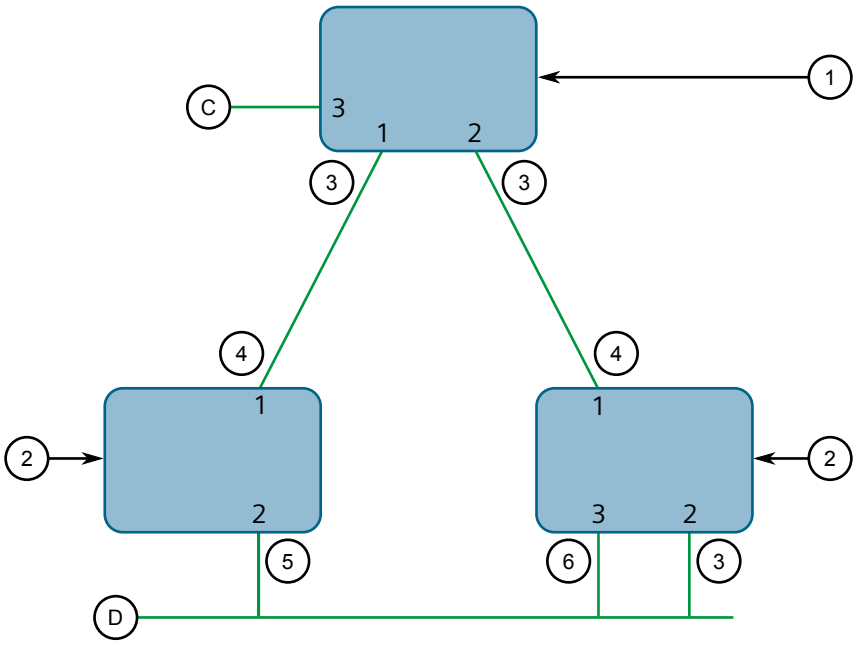
Состояние "отключено" относится к соединениям, для которых протокол RSTP был отключен. В состоянии "отключено" порт всегда находится в состоянии "пересылка".

Состояние "соединение отсутствует" относится к соединениям, для которых протокол RSTP был включен, однако на данный момент неактивен.

Роль

Существуют четыре роли порта RSTP: корневой, выделенный, альтернативный и резервный. Если мост не является корневым, то он должен иметь единственный корневой порт. Корневой порт — это наилучший (то есть самый быстрый) путь для передачи трафика к корневому мосту.

Порт отмечается как выделенный, если это наилучший порт для обслуживания данного сегмента локальной сети из подключенных к этому сегменту. Все мосты в одном и том же сегменте локальной сети прослушивают сообщения друг от друга и согласуют между собой, порт какого моста является корневым. Порты остальных мостов данного сегмента должны стать корневыми, альтернативными или резервными портами.



① Корневой мост
② Выделенный мост
③ Выделенный порт
④ Корневой порт

⑤ Альтернативный порт
⑥ Резервный порт

Рисунок 9.1 Роли моста и порта

Порт является альтернативным, если для него выгоднее принимать сообщения от другого моста в сегменте локальной сети, к которому этот порт подключен. Прием сообщений альтернативным портом выгоднее, чем отправка сообщений, которые может генерировать сам этот порт, но недостаточно выгоден, чтобы данный порт стал корневым. Данный порт становится альтернативным по отношению к текущему корневому порту, а при отказе текущего корневого порта станет новым корневым портом. Альтернативный порт не участвует в работе сети.

Порт является резервным, если для него выгоднее принимать сообщения от сегмента локальной сети, к которому этот порт подключен, исходящие от другого порта того же моста. Данный порт является резервным для другого порта того же моста и станет активным при отказе этого порта. Резервный порт не участвует в работе сети.

9.1.1.2 Граничные порты

Порт может быть выделен в качестве граничного порта, если он непосредственно подключен к оконечной станции. В этом качестве он не может образовать петли мостовых соединений в сети и, таким образом, способен сразу переходить к пересылке информации, пропуская этапы прослушивания и запоминания.

Если граничные порты принимают конфигурационные сообщения, то они немедленно теряют свой статус граничного порта и становятся обычными портами связующего дерева. Таким образом, образованная из-за неправильно подключенного граничного порта петля очень быстро устраняется.

Поскольку граничный порт обслуживает только оконечные станции, то при переключении состояний его линии связи сообщения об изменении топологии не генерируются.

9.1.1.3 Сетевые сегменты точка-точка и сегменты с множественным доступом

В RSTP используется одноранговый протокол под названием "предложение-соглашение", чтобы обеспечить переход к другой топологии в случае отказа какого-либо канала связи. Это протокол точка-точка, который прекращает работать в ситуациях множественного доступа, то есть при наличии белее чем двух мостов, подключенных к одному сегменту сети.

Если RSTP обнаруживает такую ситуацию (на основании полудуплексного статуса порта после установления соединения), то протокол предложение-соглашение отключается. Порт должен пройти через состояния запоминания и пересылки, находясь в каждом из этих состояний в течение времени, которое называется временем для перехода в режим пересылки.

Существуют ситуации, в которых RSTP принимает неправильное решение о состоянии соединения точка-точка при простом анализе полудуплексного статуса, а именно:

- Порт подключен к единственному партнеру, но через полудуплексный канал связи.
- Порт подключен к общему медиа-концентратору через полнодуплексный канал связи. К образованному этим концентратором сегменту с множественным доступом подключен более чем один мост, поддерживающий протокол RSTP.

В этих случаях пользователь может настроить коммутатор таким образом, чтобы переопределить механизм, определенный на основе полудуплексного режима, и принудительно обрабатывать состояние соединения правильным образом.

9.1.1.4 Стоимость пути и сумма стоимости портов на этом пути

Стоимость пути STP представляет собой основной показатель, с помощью которого выбираются корневой порт и выделенные порты. Стоимость пути для выделенного коммутатора представляет собой сумму стоимостей отдельных портов на линиях связи между корневым коммутатором и этим выделенным коммутатором. Порт с наименьшей стоимостью пути представляет собой наилучший маршрут к корневому коммутатору и выбирается в качестве корневого порта.

Примечание
В действительности основным определяющим фактором выбора корневого порта служит идентификатор корневого моста. Идентификатор моста важен, главным образом, при запуске сети, когда коммутатор с наименьшим идентификатором выбирается в качестве корневого моста. После запуска (когда со всеми мостами согласован идентификатор корневого моста), стоимость пути используется для выбора корневых портов. Если стоимость пути у кандидатов на роль корневого порта одинаковая, то для выбора порта используется идентификатор однорангового моста. И, наконец, если стоимость пути и идентификатора однорангового моста у кандидатов на роль корневого порта одинаковы, то для выбора порта используется идентификатор порта однорангового моста. Во всех случаях в качестве наилучшего варианта выбираются наименьшие идентификаторы, стоимость пути или идентификатор порта.

Как определяется стоимость порта

Значения стоимости порта могут определяться в результате автоматического согласования параметров соединения или ручного конфигурирования. Когда используется метод автоматического согласования параметров соединения, стоимость порта вычисляется на основании скорости соединения. Этот метод полезен в том случае, если создана сеть с хорошей связностью. Его можно

использовать, когда для разработчика не особо важна получаемая в результате топология, если обеспечивается связность сети.

Ручная настройка полезна в случае, когда точная топология сети должна быть предсказуемой при любых обстоятельствах. Стоимость пути можно использовать для создания топологии сети, которая в точности соответствует намерениям разработчика.

Сравнение стоимостей STP и RSTP

Спецификация IEEE 802.1D-1998 ограничивает стоимость порта значениями в интервале от 1 до 65536. Разработанный еще в те времена, когда высшим техническим достижением были каналы связи со скоростью передачи 9600 бит/с, этот метод плохо работает в современных условиях эксплуатации, поскольку в нем невозможно представить скорость канала связи выше десяти гигабит в секунду.

Чтобы устранить эту проблему в будущих приложениях, спецификация IEEE 802.1w ограничивает стоимость порта значениями в интервале от 1 до 20000000, а скорость связи до 10 Тбайт в секунду можно представить со значением 2.

Мосты RUGGEDCOM поддерживают совместимость с устаревшими коммутаторами STP за счет выбора используемого типа значений. На практике неважно, какой именно тип значений используется, если он последовательно применяется в масштабах всей сети, либо значения стоимости назначаются вручную.

9.1.1.5 Диаметр моста

Диаметр моста представляет собой максимальное количество мостов между двумя возможными точками подключения оконечных станций к сети.

Диаметр моста служит отражением того очевидного факта, что для распространения информации о топологии требуется время, в течение которого она проходит один транзитный участок сети за другим. Если распространение конфигурационных сообщений из конца в конец сети занимает слишком много времени, то результатом будет нестабильная сеть.

Существует взаимосвязь между диаметром моста и параметром максимального возраста сообщения. Чтобы обеспечить увеличенные размеры кольцевых топологий, в Siemens eRSTP™ возраст сообщения увеличивается на ¼ секунды на каждом мосту. Таким образом, максимальный диаметр моста численно равен умноженному на 4 параметру максимального возраста сообщения, который задан в конфигурации.

Примечание
Алгоритм в RSTP следующий:

- Конфигурационные сообщения STP содержат информацию об их *возрасте*.

- Сообщения, передаваемые через корневой мост, имеют возраст 0. Передавая конфигурационное сообщение, каждый последующий выделенный мост должен увеличить его возраст хотя бы на 1 секунду.
- Если возраст превысит значение параметра максимального возраста, то следующий мост, принимающий это сообщение, немедленно его отбросит.

⚠ ЗАМЕТКА

Увеличьте значение параметра максимального возраста сообщения, если создаются очень большие коммутируемые или кольцевые сети.

9.1.1.6 eRSTP

Усовершенствованный протокол связующего дерева (eRSTP) компании Siemens обеспечивает улучшение протокола RSTP в двух направлениях:

- сокращает время устранения неисправности (< 5 мс на транзитный участок)
- повышает эффективность крупных кольцевых сетевых топологий (до 160 коммутаторов).

Протокол eRSTP также совместим с протоколом, что обеспечивает возможность взаимодействия с коммерческими коммутаторами.

9.1.1.7 Быстрый перехват роли корневого коммутатора в случае отказа

Реализованная Siemens функция *быстрого перехвата роли корневого коммутатора* в случае отказа является расширением протокола RSTP, которое можно включить или отключить. Быстрый перехват роли корневого коммутатора в случае отказа улучшает обработку отказов корневого моста в протоколе RSTP для сетей с ячеистой топологией.

⚠ ЗАМЕТКА

Опасность для конфигурации — риск нарушения обмена данными

В смешанных сетях, где присутствуют коммутаторы RUGGEDCOM и коммутаторы не производства RUGGEDCOM, либо реализованы различные алгоритмы быстрого перехвата роли корневого коммутатора в случае отказа, функция быстрого перехвата роли корневого коммутатора RSTP не будет работать корректно, а при отказе корневого моста время перехвата его роли будет непредсказуемым. Чтобы избежать потенциальных проблем, обратите внимание на следующее:

- При использовании алгоритма Robust (Стойкий) необходимо, чтобы все коммутаторы были коммутаторами RUGGEDCOM.

- При использовании алгоритма Relaxed (Смягченный), все коммутаторы должны быть под коммутаторами RUGGEDCOM, кроме корневого коммутатора.
- Все коммутаторы RUGGEDCOM в сети должны использовать алгоритм Fast Root Failover (быстрый перехват роли корневого коммутатора в случае отказа).

Существует два алгоритма быстрого перехвата роли корневого коммутатора в случае отказа.

- **Robust (Стойкий):** гарантирует детерминированное время перехвата роли корневого коммутатора в случае отказа, но требуется его поддержка всеми коммутаторами в сети, включая корневой коммутатор.
- **Relaxed (Смягченный):** обеспечивает детерминированное время перехвата роли корневого коммутатора в случае отказа для большинства сетевых топологий, но позволяет использовать стандартный мост в роли корневого.

Примечание
Минимальный интервал для корневых отказов составляет одну секунду. Множественные, практически одновременные корневые отказы (с интервалом менее одной секунды) не поддерживаются алгоритмом быстрого перехвата роли корневого коммутатора в случае отказа.

Быстрый перехват роли корневого коммутатора в случае отказа и производительность RSTP

- Запуск RSTP с отключенной функцией быстрого перехвата роли корневого коммутатора в случае отказа не влияет на функционирование RSTP в кольцевых сетях.
- Функция быстрого перехвата роли корневого коммутатора не влияет на функционирование RSTP в случае отказов, которые не касаются корневого моста или одной из его линий связи.
- Дополнительная обработка, вводимая функцией быстрого перехвата роли корневого коммутатора, существенно уменьшает время переключения при отказе в худшем случае для сетей с ячеистой топологией.

Рекомендации по использованию быстрого перехвата роли корневого коммутатора в случае отказа

- Не рекомендуется активизировать функцию быстрого перехвата роли корневого коммутатора в сетевой топологии, где все коммутаторы соединены в составе единого кольца.
- Настоятельно рекомендуется всегда подключать корневой мост к каждому из его соседних мостов, используя более одной линии связи, при включении в кольцевой сети.

9.1.2 Применения RSTP

В данном разделе описывается различное применение RSTP.

9.1.2.1 Структурированные кабельные сети с RSTP

Протокол RSTP позволяет проектировать структурированные кабельные сети, в которых сохраняется связность в случае отказа каналов связи. Например, при одиночном отказе любой из линий связи от A до N на Рисунок 9.2, «Пример топологии структурированной кабельной сети» все порты коммутаторов от 555 до 888 останутся подключенными к сети.

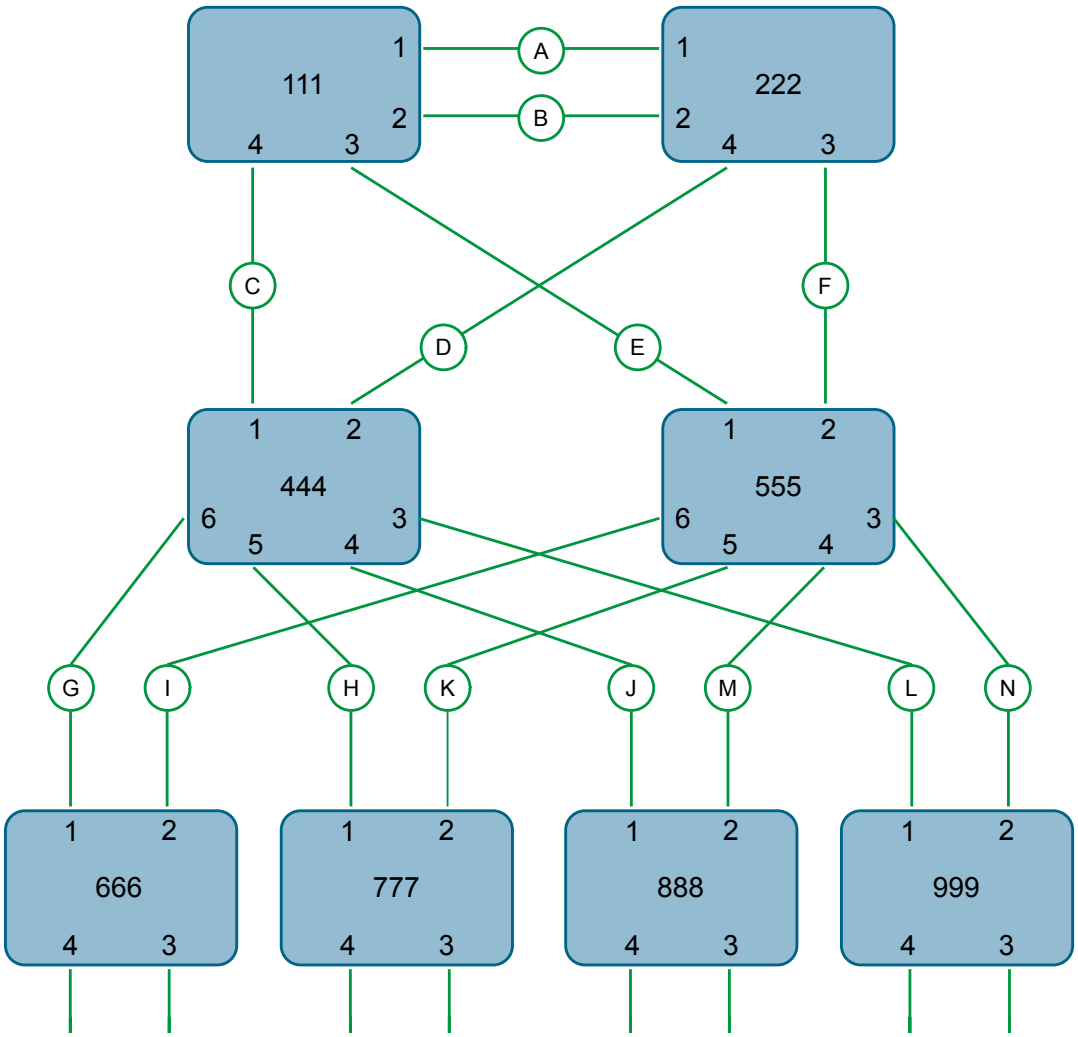


Рисунок 9.2 Пример топологии структурированной кабельной сети

Чтобы спроектировать структурированную кабельную сеть, сделайте следующее:

1. **Выберите параметры проектирования для сети.**

   Каковы требования к отказоустойчивости и времени переключения при отказе/времени восстановления? Существуют ли специальные требования для различной маршрутизации к центральному серверу? Существуют ли специальные требования к дублированию портов?

2. **Определите, требуется ли поддержка устаревшего оборудования.**

   Используются ли в сети STP-мосты? Эти мосты не поддерживают быстрый переход в режим пересылки информации. Если эти мосты присутствуют, то нельзя ли их перегруппировать ближе к границе сети?

3. **Определите граничные порты и порты с ограничениями полудуплексного режима/общей среды передачи данных.**

   Порты, которые подключены к серверам, интеллектуальным электронным устройствам (ИЭУ) и контроллерам, могут быть настроены в качестве граничных портов, чтобы гарантировать быстрый переход к пересылке информации, а также сократить количество оповещений об изменении топологии в сети. Порты с ограничениями полудуплексного режима/общей среды передачи данных требуется особое внимание, чтобы эти ограничения не приводили к увеличенному времени переключения при отказе/времени восстановления.

4. **Тщательно выберите корневой мост и резервный корневой мост.**

   Корневой мост следует выбирать таким образом, чтобы он находился в точке концентрации сетевого трафика. Найдите резервный корневой мост вблизи от корневого моста. Одна из стратегий, которую можно использовать, состоит в настройке приоритета моста, чтобы назначить корневой мост, а затем настраивается приоритет каждого моста в соответствии с его расстоянием от корневого моста.

5. **Определите требуемую топологию стабильного состояния.**

   Идентифицируйте требуемую топологию стабильного состояния, принимая в расчет скорости передачи по каналам связи, обеспечиваемый трафик и класс сервиса (QOS). Исследуйте эффекты в результате прерывания выбранных соединений, принимая во внимание загрузку сети и качество альтернативных соединений.

6. **Примите решение относительно стратегии вычисления стоимости порта.**

   Выберите, будут ли использоваться фиксированные стоимости или будет производиться их автоматическое согласование? Рекомендуется использовать автоматическое согласование, если только нет необходимости в изменении автоматического согласования проектом сети. Выберите тип значений стоимости STP или RSTP, который должен использоваться. Необходимо сконфигурировать одинаковый тип согласования на всех устройствах сети.

7. **Активируйте опцию быстрого перехвата роли корневого коммутатора в случае отказа.**

   Это проприетарная функция Siemens. В ячеистой сети, ядро которой содержит только устройства RUGGEDCOM, рекомендуется включить опцию быстрого перехвата роли корневого коммутатора в случае отказа, чтобы минимизировать время простоя сети в случае отказа корневого моста.

8. **Вычислите и введите в конфигурацию значения приоритетов и стоимостей.**
9. **Реализуйте сеть и протестируйте ее в условиях загрузки.**

9.1.2.2 Кольцевые магистральные сети с RSTP

Протокол RSTP может использоваться в кольцевых конфигурациях магистрали, когда требуется быстрое восстановление после отказа канала связи. В нормальном режиме работы RSTP будет блокировать трафик на одном или нескольких каналах связи, например, как показывает двойная черта, перечеркивающая канал связи H на Рисунок 9.3, «Пример кольцевой конфигурации магистрали». В случае отказа канала связи D коммутатор 444 разблокирует канал связи H. Коммутатор 333 будет взаимодействовать с сетью через канал связи F.

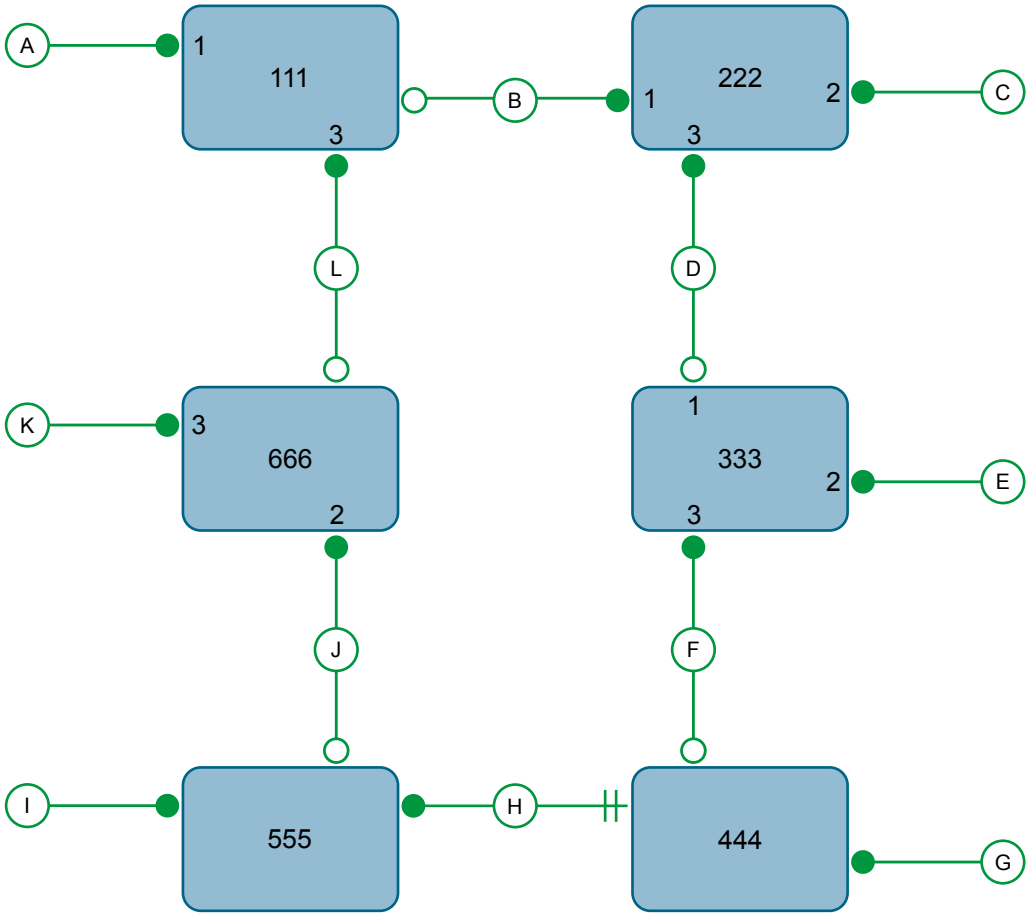


Рисунок 9.3 Пример кольцевой конфигурации магистрали

Чтобы спроектировать кольцевую конфигурацию магистрали с использованием RSTP, сделайте следующее:

1. **Выберите параметры проектирования для сети.**

   Каковы требования к отказоустойчивости и времени переключения при отказе/времени восстановления? Обычно кольцевые магистральные сети выбираются для того, чтобы построение сети обеспечивало отказоустойчивость при относительно невысокой стоимости.

2. **Определите, требуется ли поддержка устаревшего оборудования, а также определите порты с ограничениями полудуплексного режима/общей среды передачи данных.**

   Эти коммутаторы не должны использоваться, если для сети нужно минимизировать время переключения при отказе/время восстановления.

3. **Определите граничные порты.**

   Порты, которые подключены к серверам, интеллектуальным электронным устройствам (ИЭУ) и контроллерам, могут быть настроены в качестве граничных портов, чтобы гарантировать быстрый переход к пересылке

информации, а также сократить количество оповещений об изменении топологии в сети.

4. **Выберите корневой мост.**

   Корневой мост можно выбрать для уравнивания количества мостов, количества станций или объема трафика в каждой из половин кольца, разделяемых этим мостом. Важно понимать, что кольцевая магистраль всегда будет разорвана в одной точке и что трафик всегда проходит через корневой мост.

5. **Назначьте приоритеты мостов для кольцевой магистрали.**

   Для получения дополнительной информации см. официальное описание RUGGEDCOM ""Работа протокола быстрого связующего дерева в топологии кольцевой сети"", доступное по адресу https://assets.new.siemens.com/siemens/assets/api/uuid:d4af5d17-728c-493f-b00a-9c4db67b23ed/RSTP-whitepaper-EN-09-2020.pdf.

6. **Примите решение относительно стратегии вычисления стоимости порта.**

   Рекомендуется использовать автоматическое согласование, если только нет необходимости в изменении автоматического согласования проектом сети. Выберите тип значений стоимости STP или RSTP, который должен использоваться. Необходимо сконфигурировать одинаковый тип согласования на всех устройствах сети.

7. **Отключите опцию быстрого перехвата роли корневого коммутатора в случае отказа.**

   Это проприетарная функция Siemens. В RUGGEDCOM ROS опция быстрого перехвата роли корневого коммутатора в случае отказа включена по умолчанию. При работе в кольцевой сети рекомендуется отключать эту функцию.

8. **Реализуйте сеть и протестируйте ее в условиях загрузки.**

9.1.2.3 Дублирование RSTP-портов

В случаях, когда резервирование (дублирование) портов имеет важное значение, протокол RSTP позволяет использовать более одного порта моста для обслуживания сегмента сети. В следующем примере, если порт 3 выделен для передачи сетевого трафика локальной сети A, то порт 4 заблокирует трафик. Если возникает отказ интерфейса порта 3, то порт 4 принимает на себя контроль над сегментом сети.

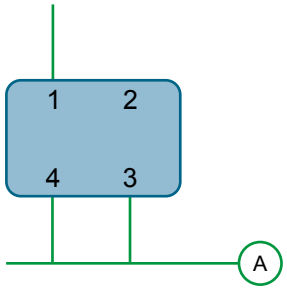


Рисунок 9.4 Пример дублирования RSTP-портов

9.1.3 Функционирование протокола MSTP

Алгоритм и протокол множественного связующего дерева (MST) обеспечивает более высокую степень контроля и гибкости, чем RSTP и устаревший STP. Протокол множественного связующего дерева (MSTP) представляет собой расширение протокола RSTP, при помощи которого в одной и той же коммутируемой сети можно поддерживать множество связующих деревьев. Трафик данных назначается на то или иное из связующих деревьев путем отображения одной или нескольких виртуальных локальных сетей (VLAN) на данную сеть.

Уровень сложности и полезности реализации множественного связующего дерева на данной коммутируемой сети пропорционален объему трудозатрат на планирование и разработку, вложенных в настройку MSTP.

Если протокол MSTP активизирован на некоторых или на всех коммутаторах в сети без дополнительной настройки, то результатом будет сеть с полной и простой связностью, но этот результат в лучшем случае будет с сетью, в которой используется только протокол RSTP. Извлечение всех преимуществ, которые обеспечивает MSTP, требует потенциально большого числа конфигурационных переменных параметров, которые выводятся из анализа трафика данных в коммутируемой сети, а также из требований к разделению нагрузки, к резервированию, а также к оптимизации пути. После того как все эти параметры будут определены, также очень важно последовательно их применять и администрировать на всех коммутаторах в MST-регионе.

Исходя из принципа построения протокола, время обработки в MSTP пропорционально числу активных экземпляров STP. Это значит, что MSTP, скорее всего, будет работать существенно медленнее, чем RSTP. Следовательно, в случае ответственных приложений протокол RSTP следует рассматривать как лучшее решение для обеспечения избыточности сети, чем MSTP.

9.1.3.1 MSTP-регионы и совместимость с другими протоколами

В дополнение к поддержке множественных связующих деревьев в сети из MSTP-совместимых мостов, протокол MSTP способен взаимодействовать с мостами, которые поддерживают только протокол RSTP или устаревший STP, не требуя никакого специального конфигурирования.

MST-регион может быть определен как заданное множество соединенных между собой мостов, у которых совпадает идентификация MST-региона. Интерфейс между MSTP-мостами и мостами, не поддерживающими протокол MSTP, либо между MSTP-мостами с различной идентификационной информацией MST-региона, становится частью границы MST-региона.

Коммутаторы за пределами MST-региона будут видеть весь этот регион как единственный мост (R)STP; внутренние детали MST-региона скрыты от остальной коммутируемой сети. Для этого MSTP поддерживает отдельные *счетчики транзитных участков* для информации связующего дерева, обмен которой производится на границе MST-региона, в отличие от информации, распространяемой внутри этого региона. Для информации, принимаемой на границе MST-региона, возраст сообщения (R)STP инкрементно увеличивается лишь один раз. Внутри региона поддерживается отдельный счетчик остающихся транзитных участков, по одному для каждого экземпляра связующего дерева. Внешний параметр возраста сообщения сравнивается с временем максимального возраста сообщения (R)STP, тогда как внутренние счетчики остающихся транзитных участков сравниваются с параметром максимального числа транзитных участков в масштабах MST-региона.

MSTI

Экземпляр множественного связующего дерева (MSTI) представляет собой один из шестнадцати независимых экземпляров связующего дерева, которые могут быть определены в MST-регионе (исключая IST — см. ниже). MSTI создается путем отображения определенного множества сетей VLAN (в RUGGEDCOM ROS — путем конфигурирования VLAN) на заданный идентификатор MSTI ID. Такое же отображение должно быть настроено на всех коммутаторах, которые должны быть составным элементом MSTI. Более того, все отображения VLAN на MSTI должны быть идентичными для всех коммутаторов в MST-регионе.

RUGGEDCOM ROS поддерживает 16 экземпляров MSTI в дополнение к IST.

Каждый MSTI имеет топологию, которая не зависит от других экземпляров. Трафик данных, исходящий от одного источника и направленный к одному и тому же адресату, но по разным сетям VLAN в различных MSTI, может, таким образом, проходить через сеть по разным путям.

IST

MST-регион всегда определяет внутреннее связующее дерево (IST). Дерево IST охватывает весь MST-регион и переносит весь трафик данных, который не назначен специально (посредством VLAN) для конкретного MSTI. IST всегда вычисляется и определяется таким образом, чтобы оно было нулевым MSTI.

IST также является расширением CIST (см. ниже) внутри MST-региона, которое охватывает всю коммутируемую сеть, внутри и за пределами MST-региона, все остальные коммутаторы RSTP и STP, а также все прочие MST-регионы.

CST

Общее связующее дерево (CST) охватывает всю коммутируемую сеть, включая MST-регионы, а также все подключенные мосты STP или RSTP. CST рассматривает MST-регион как отдельный мост, с единственным значением стоимости, которое ассоциировано с его прохождением.

CIST

Общее и внутреннее связующее дерево (CIST) представляет собой объединение дерева CST и деревьев IST во всех MST-регионах. Таким образом, CIST охватывает всю коммутируемую сеть, проникая в каждый MST-регион через IST последнего, чтобы иметь доступ к каждому мосту в сети.

9.1.3.2 Роли мостов и портов в MSTP

Протокол множественного связующего дерева (MSTP) поддерживает следующие роли мостов и портов:

Роли мостов

Роль	Описание
Корневой мост CIST	Корневой мост CIST — это выбранный корневой мост дерева CIST, которое охватывает все подключенные мосты STP и RSTP, а также MSTP-регионы.
Региональный корневой мост CIST	Корневой мост дерева IST в пределах MSTP-региона. Региональный корневой мост CIST — это мост в пределах MSTP-региона с наименьшей стоимостью пути к корневому мосту CIST. Обратите внимание, что региональный корневой мост CIST будет находиться на границе MSTP-региона. Также имейте в виду, что региональный корневой мост CIST может быть корневым мостом CIST.
Региональный корневой мост MSTI	Корневой мост для MSTI в пределах MSTP-региона. Корневой мост выбирается независимо для каждого MSTI в MSTP-регионе.

Роли портов

Каждый порт MSTP-моста может иметь более одной роли CIST в зависимости от количества и топологии экземпляров связующего дерева, определенных для этого порта.

Роль	Описание
Роли портов CIST	• Корневой порт обеспечивает минимальную стоимость пути от моста к корневому мосту CIST через региональный корневой мост CIST. Если этот мост сам оказывается региональным корневым мостом CIST, то его корневой порт также является ведущим портом для всех MSTI и обеспечивает минимальную стоимость пути к корневому мосту CIST, расположенному вне данного региона. • Выделенный порт обеспечивает минимальную стоимость пути от присоединенной локальной сети через мост к региональному корневому мосту CIST. • Альтернативный и резервный порты совпадают с аналогичными портами в RSTP, но по отношению к региональному корневому мосту CIST.
Роли портов MSTI	Для каждого MSTI на мосту: • Корневой порт обеспечивает минимальную стоимость пути от моста к региональному корневому мосту MSTI, если сам этот мост не является региональным корневым мостом MSTI. • Выделенный порт обеспечивает минимальную стоимость пути от присоединенной локальной сети через мост к региональному корневому мосту MSTI. • Альтернативный и резервный порты совпадают с аналогичными портами в RSTP, но по отношению к региональному корневому мосту MSTI. Ведущий порт, который является уникальным в MSTP-регионе, служит корневым портом CIST регионального корневого моста CIST и обеспечивает минимальную стоимость пути к корневому мосту CIST для всех MSTI.
Граничные порты	Граничный порт — это порт на мосту в MSTP-регионе, который подключен к любому из следующих устройств: мост, принадлежащий к другому MSTP-региону, либо мост, поддерживающий только протокол RSTP или устаревший STP. Граничный порт блокирует или перенаправляет все сети VLAN от всех MSTI и, аналогичным образом, от CIST. Граничный порт может представлять собой: • Корневой порт CIST регионального корневого моста CIST (и, следовательно, ведущий порт MSTI). • Выделенный порт CIST, альтернативный/ резервный порт CIST, либо находиться в состоянии "отключен". На границе MST-

Роль	Описание
	региона роль порта MSTI аналогична роли порта CIST. Граничный порт, подключенный к мосту STP, будет посылать только блок данных протокола коммутаторов (BPDU) для протокола STP. Граничный порт, подключенный к мосту RSTP, нет необходимости удерживать от отправки сообщений BPDU для протокола MSTP. Это возможно в связи с тем фактом, что протокол MSTP передает идентификатор регионального корневого коммутатора CIST в поле данных, которое RSTP анализирует как идентификатор выделенного коммутатора.

9.1.3.3 Преимущества протокола MSTP

Несмотря на то, что протокол MSTP по умолчанию устроен таким образом, чтобы автоматически приходить к некоторому решению со связующим деревом для каждого сконфигурированного MSTI, можно извлечь преимущества, оказывая влияние на топологию экземпляров MSTI в MST-регионе. Тот факт, что приоритет моста и стоимость каждого порта могут конфигурироваться для отдельного MST, позволяет управлять топологией каждого MSTI в пределах региона.

Баланс загрузки

MSTP можно использовать для равномерного распределения интенсивности трафика между множествами сетей VLAN, обеспечивая более полное использование коммутируемой сети с множественными межсоединениями.

Коммутируемая сеть, которая управляется единственным связующим деревом, будет блокировать избыточные соединения, чтобы избежать образования нежелательных петель. Однако при использовании протокола MSTP любое заданное соединение может иметь различное состояние блокировки для экземпляра связующего дерева, поскольку это поддерживается протоколом MSTP. Любое заданное соединение может, таким образом, находиться в состоянии блокировки для одних сетей VLAN и в состоянии пересылки информации для других сетей VLAN, в зависимости от способа отображения виртуальных локальных сетей на экземпляры MSTI.

Можно контролировать построение решения связующего дерева для каждого MSTI, особенно множество активных соединений для каждого дерева, манипулируя для отдельного MSTI приоритетом моста и стоимостями соединений через данный порт в сети. Если трафик разумным образом распределяется по нескольким сетям VLAN, то теперь для передачи трафика могут создаваться избыточные межсоединения в коммутируемой сети, которые в случае единственного связующего дерева стали бы неиспользуемыми.

Изолированность реконфигурации связующего дерева.

Отказ канала связи в MSTP-регионе, не влияющий на роли граничных портов, не приведет к повторному конфигурированию CST, а также не повлияет на другие MSTP-регионы. Это связано с тем фактом, что информация MSTP не распространяется за границу региона.

Сравнение протоколов MSTP и PVST

Преимущество протокола MSTP по сравнению с проприетарным протоколом PVST компании Cisco Systems Inc. состоит в способности первого из них отображать множество сетей VLAN на единственный MSTI. Поскольку каждое связующее дерево требует обработки с участием процессора и памяти для хранения, то издержки на отслеживание возрастающего числа сетей VLAN растут быстрее для протокола PVST, чем для MSTP.

Совместимость с протоколами STP и RSTP

Не требуется никакого специального конфигурирования мостов MST-региона для полноценного и простого подключения к мостам той же коммутируемой сети, которые не поддерживают MST. Однако для получения оптимальной сети рекомендуется тщательное планирование и настройка.

9.1.3.4 Реализация протокола MSTP в коммутируемой сети

Настройку MSTP в сети рекомендуется производить в описанной ниже последовательности.

Естественно, также рекомендуется, чтобы при анализе и планировании сети предоставлялась информация, в частности, об этапах настройки параметров VLAN и MSTP.

Начните с перевода в неактивное состояние MSTP-совместимых Ethernet-мостов и протокола MSTP. Для каждого моста в сети сделайте следующее.

Примечание
Чтобы привязать сеть VLAN к экземпляру MSTI не нужно включать MSTP. Однако привязка должна быть идентичной для каждого моста, принадлежащего MSTP-региону.

1. Сконфигурируйте и включите STP глобально и/или для конкретных Ethernet-портов. Для получения дополнительной информации см. "Глобальное конфигурирование STP (Страница 236)" или "Конфигурирование STP для конкретных Ethernet-портов (Страница 238)".

   Примечание
   В настройке MSTP должны использоваться статические виртуальные локальные сети. GVRP не поддерживается.

2. Добавьте статические сети VLAN и привяжите их к экземплярам MSTI. Для получения дополнительной информации см. "Добавление статической сети VLAN (Страница 174)".

Примечание
Идентификатор региона и уровень версии должны быть одинаковыми для каждого моста в MST-регионе.

3. Сконфигурируйте уровень версии для идентификатора MST-региона. Для получения дополнительной информации см. "Конфигурирование идентификатора MST-региона (Страница 250)".
4. Убедитесь, что дайджест "только для чтения" для идентификатора MST-региона идентичен для каждого моста в MST-регионе. Если дайджест отличается, набор привязок от сетей VLAN к экземплярам MSTI отличается.
5. Сконфигурируйте приоритет коммутатора для глобального MSTI. Для получения дополнительной информации см. "Конфигурирование глобального MSTI (Страница 251)".
6. Сконфигурируйте стоимость порта и приоритетность по порту для каждого MSTI. Для получения дополнительной информации см. "Конфигурирование MSTI для Ethernet-порта (Страница 252)".
7. Установите версию протокола STP на MSTP и включите STP. Для получения дополнительной информации см. "Глобальное конфигурирование STP (Страница 236)".

9.1.4 Глобальное конфигурирование STP

Чтобы сконфигурировать глобальные настройки для протокола связующего дерева (STP), сделайте следующее:

1. Перейдите в ***Network Redundancy » Spanning Tree » Configure Bridge RSTP Parameters***. Появится форма **Bridge RSTP Parameters**.
2. Необходимо сконфигурировать следующие параметры:

Параметр	Описание
`State`	**Краткий обзор:** [Disabled | Enabled] **Значение по умолчанию:** Enabled Глобально активирует протокол STP/RSTP/MSTP для коммутатора. Обратите внимание, что чтобы активизировать протокол STP/RSTP/MSTP для конкретного порта, этот протокол необходимо активизировать глобально и для отдельного порта.
`Version Support`	**Краткий обзор:** [STP | RSTP | MSTP] **Значение по умолчанию:** RSTP Выберите версию протокола связующего дерева, которая будет поддерживаться: STP (протокол связующего дерева), Rapid STP (протокол быстрого связующего дерева) или

Параметр	Описание
	Multiple STP (протокол множественного связующего дерева).
`Bridge Priority`	**Краткий обзор:** [0 | 4096 | 8192 | 12288 | 16384 | 20480 | 24576 | 28672 | 32768 | 36864 | 40960 | 45056 | 49152 | 53248 | 57344 | 61440] **Значение по умолчанию:** 32768 Параметр Bridge Priority (приоритет моста) обеспечивает способ управления топологией сети с соединениями по протоколу STP. Требуемые корневые и выделенные мосты могут быть сконфигурированы для конкретной топологии. Мост с наименьшим приоритетом станет корневым мостом. В случае отказа корневого моста корневым станет мост с последующим наименьшим приоритетом. Выделенные мосты, которые (в целях дублирования) обслуживают общую локальную сеть, также используют приоритет для определения того, какой мост активен. Таким образом, при тщательном подборе приоритетов мостов можно определить пути передачи трафика как для нормального состояния сети, так и на случай отказа какого-либо соединения.
`Hello Time`	**Краткий обзор:** Целое число от 1 до 10 **Значение по умолчанию:** 2 Интервал времени между конфигурационными сообщениями, которые посылает корневой мост. Более короткие интервалы времени между конфигурационными сообщениями, подтверждающими работоспособность устройства, приводят к более быстрому обнаружению изменений топологии ценой умеренного возрастания трафика STP.
`Max Age Time`	**Краткий обзор:** Целое число от 6 до 40 **Значение по умолчанию:** 20 Время, в течение которого конфигурационное сообщение остается не устаревшим после его отправки корневым мостом. Настраивайте этот параметр с осторожностью, когда существуют множественные звенья мостов, либо при наличии в составе сети каналов связи с низкой скоростью передачи данных (например, как у каналов связи, применяемых в глобальных сетях).
`Transmit Count`	**Краткий обзор:** Целое число от 3 до 100 или [Unlimited] **Значение по умолчанию:** Unlimited Максимальное количество сообщений BPDU для каждого порта, которое может быть передано за одну секунду. Чем больше эти значения, тем быстрее может происходить восстановление сети после отказа каналов связи/мостов.
`Forward Delay`	**Краткий обзор:** Целое число от 4 до 30 **Значение по умолчанию:** 15 Интервал времени, затрачиваемого мостом на запоминание MAC-адреса или активацию порта перед началом пересылки трафика. Меньшие значения позволяют порту быстрее достигать состояния пересылки,

Параметр	Описание
	но за счет веерной рассылки неизвестных адресов на все порты.
`Max Hops`	**Краткий обзор:** Целое число от 6 до 40 **Значение по умолчанию:** 20 Этот параметр применим только для MSTP. Этот параметр определяет максимально возможный диаметр коммутируемой сети внутри MST-региона. Сообщения BPDU протокола MSTP, распространяемые внутри MST-региона, несут в себе параметр времени жизни сообщения, который уменьшается на единицу каждым коммутатором, который распространяет это сообщение BPDU. Если максимальное число транзитных участков внутри данного региона превышает заданное в конфигурации максимальное значение, то сообщения BPDU могут отбрасываться из-за содержащейся в них информации о времени жизни.

3. Нажмите **Apply**.

9.1.5 Конфигурирование STP для конкретных Ethernet-портов

Чтобы сконфигурировать протокол связующего дерева (STP) для конкретного Ethernet-порта, сделайте следующее:

1. Перейдите в ***Network Redundancy » Spanning Tree » Configure Port RSTP Parameters***. Появится таблица **Port RSTP Parameters**.
2. Выберите Ethernet-порт. Появится форма **Port RSTP Parameters**.
3. Необходимо сконфигурировать следующие параметры:

Параметр	Описание
`Port(s)`	**Краткий обзор:** Comma-separated list of ports Номер порта устройства (или список портов, если они объединены в группу).
`Enabled`	**Краткий обзор:** [Disabled | Enabled] **Значение по умолчанию:** Enabled Включение STP активизирует протокол STP или RSTP для этого порта в соответствии с конфигурацией в меню конфигурации STP. Протокол STP может быть отключен для порта ТОЛЬКО в том случае, если данный порт не присоединен каким-либо образом к мосту, который поддерживает протокол STP. Несоблюдение этого требования НЕИЗБЕЖНО приведет к возникновению петли трафика в сети, которое невозможно обнаружить. Лучшая альтернатива отключению порта — оставить протокол STP активным, но сконфигурировать данный порт в качестве граничного порта. Хорошим кандидатом на отключение STP может быть порт, которым обслуживается только единственный сервер.

Параметр	Описание
`Priority`	**Краткий обзор:** [0 | 16 | 32 | 48 | 64 | 80 | 96 | 112 | 128 | 144 | 160 | 176 | 194 | 208 | 224 | 240] **Значение по умолчанию:** 128 Выбор приоритета для STP-порта. Порт для использования будет выбираться из портов с одинаковой стоимостью, подключенных к общей локальной сети, на основании приоритета этого порта.
`STP Cost`	**Краткий обзор:** Целое число от 0 до 65535 или [Auto] **Значение по умолчанию:** Auto Выбор значения стоимости, используемого при вычислениях стоимости, когда для параметра Cost Style (тип значений стоимости) выбран вариант STP в конфигурации RSTP-параметров моста. Настройка значений стоимости вручную обеспечивает возможность выбирать определенные порты для преимущественной передачи трафика через них, минуя остальные порты. Оставьте для этого порта значение "автоматически", чтобы использовать стандартные согласованные значения стоимости STP-порта (4 для скорости передачи 1 Гбит/с, 19 для каналов связи со скоростью передачи 100 Мбит/с и 100 для каналов связи со скоростью передачи 10 Мбит/с). В случае MSTP этот параметр применим к стоимости внешнего и внутреннего пути.
`RSTP Cost`	**Краткий обзор:** Целое число от 0 до 2147483647 или [Auto] **Значение по умолчанию:** Auto Выбор значения стоимости, используемого при вычислениях стоимости, когда для параметра Cost Style (тип значений стоимости) выбран вариант RSTP в конфигурации RSTP-параметров моста. Настройка значений стоимости вручную обеспечивает возможность выбирать определенные порты для преимущественной передачи трафика через них, минуя остальные порты. Оставьте для этого порта значение "автоматически", чтобы использовать стандартные значения стоимости RSTP-порта, полученные при автоматическом согласовании (20000 для скорости передачи 1 Гбит/с, 200000 для каналов связи со скоростью передачи 100 Мбит/с и 2000000 для каналов связи со скоростью передачи 10 Мбит/с). В случае MSTP этот параметр применим к стоимости внешнего и внутреннего пути.
`Edge Port`	**Краткий обзор:** [False | True | Auto] **Значение по умолчанию:** Auto Граничные порты — это порты, которые не являются частью связующего дерева, но посылают конфигурационные сообщения. Граничные порты переходят непосредственно к пересылке кадров, без каких-либо задержек для прослушивания и запоминания адресов. Таблицы MAC-адресов для граничных портов не требуется очищать, когда в сети STP возникают изменения топологии. В отличие от порта с отключенным протоколом

Параметр	Описание
	STP, случайное соединение граничного порта с другим портом в связующем дереве приведет к возникновению петли трафика, которую можно обнаружить. Статус "граничности" такого порта будет отменен и будут применяться стандартные правила RSTP (до следующего перебоя в работе канала связи).
`Point to Point`	**Краткий обзор:** [False | True | Auto] **Значение по умолчанию:** Auto RSTP использует одноранговый протокол, который обеспечивает быстрое согласование топологии для соединений точка-точка. Этот протокол автоматически отключается в ситуациях, когда множество STP-мостов взаимодействует через общую сеть (не с соединением точка-точка). Мост будет автоматически устанавливать для параметра point-to-point (точка-точка) значение "истинно" при обнаружении канала связи, пригодного для работы в полнодуплексном режиме. Параметр point-to-point (точка-точка) разрешает эти действия или отменяет их, принудительно устанавливая для соединения точка-точка статус "истинно" или "ложно". Установите для этого параметра фиксированное значение "истинно", когда порт работает с каналом связи, используя соединение точка-точка, но не может перевести этот канал связи в полнодуплексный режим. Установите для этого параметра фиксированное значение "ложно", когда порт работает с каналом связи в полнодуплексном режиме, но не используется соединение точка-точка (например, полнодуплексный канал связи к неуправляемому мосту, который служит концентратором для двух других STP-мостов).
`Restricted Role`	**Краткий обзор:** [True | False] **Значение по умолчанию:** False Логическое значение, задаваемое администратором. Значение "ИСТИННО" приводит к тому, что данный порт не выбирается в качестве корневого порта для CIST или любого MSTI, даже если он имеет наилучший вектор приоритета в связующем дереве. Такой порт будет выбран в качестве альтернативного порта после выбора корневого порта. Этот параметр должен иметь значение "ЛОЖНО" по умолчанию. Если данный параметр установлен, это может привести к недостаточной связности связующего дерева. Этот параметр устанавливается сетевым администратором, чтобы мосты, которые являются внешними по отношению к области ядра сети, не влияли на активную топологию связующего дерева. Это может быть необходимым, например, если упомянутые мосты не находятся под полным контролем администратора.
`Restricted TCN`	**Краткий обзор:** [True | False] **Значение по умолчанию:** False Логическое значение, задаваемое администратором. Значение "ИСТИННО" приводит к тому, что данный порт не распространяет принимаемые оповещения об изменении топологии и изменения топологии на

Параметр	Описание
	другие порты. Если данный параметр установлен, это может привести к временной потере связности после изменений в активной топологии связующего дерева в результате устойчиво некорректно запоминаемой информации о расположении станции. Этот параметр устанавливается сетевым администратором, чтобы мосты, которые являются внешними по отношению к области ядра сети, не вызывали очистки таблицы адресов в этой области. Это может быть необходимым, например, если упомянутые мосты не находятся под полным контролем администратора, либо в случае частых изменений параметра статуса MAC_Operational для присоединенных локальных сетей.

4. Нажмите **Apply**.

9.1.6 Конфигурирование eRSTP

Чтобы сконфигурировать eRSTP, сделайте следующее:

1. Перейдите в ***Network Redundancy » Spanning Tree » Configure eRSTP Parameters***. Появится форма **eRSTP Parameters**.
2. Необходимо сконфигурировать следующие параметры:

Параметр	Описание
`Max Network Diameter`	**Краткий обзор:** [MaxAgeTime | 4*MaxAgeTime] **Значение по умолчанию:** 4*MaxAgeTime Стандарт RSTP налагает ограничение на максимальный размер сети, которой можно управлять с помощью протокола RSTP. Размер сети описывается в терминах "максимального диаметра сети", представляющего собой число коммутаторов в составе самого длинного пути, который способны проходить сообщения BPDU в случае протокола RSTP. Поддерживаемый стандартом максимальный диаметр сети равен значению RSTP-параметра MaxAgeTime (время максимального возраста сообщения). eRSTP обеспечивает расширение стандарта RSTP, которое позволяет охватывать сети большего размера, чем сети, определяемые данным стандартом. Этот конфигурационный параметр служит для выбора максимального поддерживаемого размера сети.
`BPDU Guard Timeout`	**Краткий обзор:** Целое число от 1 до 86400 или [Until reset | Don't shutdown] **Значение по умолчанию:** Don't shutdown В стандарте RSTP не решен вопрос обеспечения безопасности сети. Протокол RSTP должен обрабатывать каждый принятое сообщение BPDU и предпринимать соответствующее действие. Это позволяет атакующему влиять на топологию RSTP, передавая в сеть сообщения BPDU протокола RSTP.

Параметр	Описание
	BPDU Guard представляет собой функцию защиты сети от сообщений BPDU, принимаемых на порт, к которому не предполагается подключение RSTP-совместимых устройств. Если сообщение BPDU принимается портом, для параметра "Edge" (граничный) которого установлено значение "ИСТИННО", либо протокол RSTP отключен, то данный порт будет отключаться на период времени, определяемый этим параметром. • `Don't shutdown (Не отключать)` - функция BPDU Guard неактивна. • `Until reset (До сброса)` - порт будет оставаться в отключенном состоянии, пока оператор не выдаст команду сброса порта.
`Fast Root Failover`	**Краткий обзор:** [On | On with standard root | Off] **Значение по умолчанию:** On В сетях с ячеистой топологией стандартный алгоритм RSTP не гарантирует детерминированное время восстановления сети в случае отказа корневого коммутатора. Это время восстановления с трудом поддается вычислению и может быть различным (в том числе относительно продолжительным) для заданной ячеистой топологии. Этот конфигурационный параметр активирует функцию расширения протокола RSTP, разработанную Siemens, которая обнаруживает отказ корневого коммутатора и выполняет ряд дополнительных шагов обработки в RSTP, сокращая время восстановления сети и делая его детерминированным. **Примечание** • Эта функция доступна только в режиме RSTP. В режиме MSTP этот конфигурационный параметр игнорируется. • В топологии с одним кольцом эта функция не является необходимой и должна быть отключена, чтобы избежать увеличения времени восстановления сети из-за дополнительной обработки в протоколе RSTP. Чтобы гарантировать оптимальные характеристики, алгоритм Fast Root Failover должен поддерживаться всеми коммутаторами в сети, включая корневой коммутатор. Однако нередко встречаются ситуации, когда роль корневого коммутатора назначается коммутатору от другого поставщика, нежели остальные коммутаторы в сети. В этом случае возможно, что корневой коммутатор не поддерживает алгоритма Fast Root Failover. Для такого сценария используйте "смягченный" алгоритм, который допускает недостаточную поддержку алгоритма корневым коммутатором. Далее приведены поддерживаемые опции конфигурации: • `Off (Выключено)` - алгоритм Fast Root Failover (быстрый перехват роли корневого коммутатора в случае отказа) неактивен, поэтому отказ корневого коммутатора может привести к чрезмерно большому времени восстановления связности.

Параметр	Описание
	• `On (Включено)` - функция Fast Root Failover (быстрый перехват роли корневого коммутатора в случае отказа) активна, а также используется самый надежный алгоритм, который требует соответствующей поддержки в корневом коммутаторе. • `On with standard root (Включено со стандартным корневым коммутатором)` - функция Fast Root Failover (быстрый перехват роли корневого коммутатора в случае отказа) активна, но используется "смягченный" алгоритм, позволяющий использовать стандартный коммутатор в роли корневого.
`IEEE802.1w Interoperability`	**Краткий обзор:** [On | Off] **Значение по умолчанию:** On Исходный протокол RSTP, который определен в стандарте IEEE 802.1w, имеет небольшие расхождения с более новыми, расширенными стандартами. Эти расхождения порождают проблемы из-за несовместимости, которые, не вызывая полного прекращения работы RSTP, могут приводить к более продолжительному времени восстановления после отказов в сети. eRSTP предусматривает некоторые расширения протокола, которые делают коммутатор полностью совместимым с коммутаторами от других поставщиков, способными работать с протоколом IEEE 802.2w RSTP. Эти расширения не влияют на совместимость с более новыми версиями протокола RSTP. Этот конфигурационный параметр активирует вышеупомянутый режим совместимости.
`Cost Style`	**Краткий обзор:** [STP (16 bit) | RSTP (32 bit)] **Значение по умолчанию:** STP (16 bit) В стандарте RSTP определены два типа значений стоимости пути. STP использует 16-разрядные значения стоимости пути, исходя из отношения 1x10E9/скорость передачи канала связи (4 для 1 Гбит/с, 19 для 100 Мбит/с и 100 для 10 Мбит/с), тогда как RSTP использует 32-разрядные значения стоимости пути, исходя из отношения 2x10E13/скорость передачи канала связи (20000 для 1 Гбит/с, 200000 для 100 Мбит/с и 2000000 для 10 Мбит/с). Однако коммутаторы от некоторых поставщиков используют тип значений стоимости пути STP даже в режиме RSTP, что может приводить к недоразумениям и проблемам из-за несовместимости. Этот конфигурационный параметр служит для выбора используемого типа значений стоимости пути. Обратите внимание, что значения стоимости пути RSTP используются лишь в том случае, когда настроенная на коммутаторе поддержка версий разрешает RSTP, а порт не мигрирует к STP.

3. Нажмите **Apply**.

9.1.7 Вывод глобальной диагностики для STP

Чтобы просмотреть глобальную статистику для STP, перейдите в ***Network Redundancy » Spanning Tree » View Bridge RSTP Statistics***. Появится форма **Bridge RSTP Statistics**.

В этой таблице отображается следующая информация:

Параметр	Описание
`Bridge Status`	**Краткий обзор:** [Designated Bridge | Not Designated For Any LAN | Root Bridge] Статус моста в связующем дереве. Статус может иметь значение "корневой" или "выделенный". В этом поле может отображаться "не выделено для LAN", если мост не является выделенным для какого-либо из своих портов.
`Bridge ID`	**Краткий обзор:** $$ / ##-##-##-##-##-## where $$ is 0 to 65535, ## is 0 to FF Идентификатор данного моста.
`Root ID`	**Краткий обзор:** $$ / ##-##-##-##-##-## where $$ is 0 to 65535, ## is 0 to FF Идентификатор моста для корневого моста.
`Root Port`	**Краткий обзор:** 1 to maximum port number или [<empty string>] Если коммутатор выделенный, то это порт, который обеспечивает связность в направлении корневого моста сети.
`Root Path Cost`	**Краткий обзор:** Целое число от 0 до 4294967295 Полная стоимость пути к корневому мосту, состоящая из суммы стоимостей каждого канала связи на этом пути. Если значения стоимости не были заданы специально, то порты со скоростью передачи 1 Гбит/с добавляют стоимость, равную четырем, порты со скоростью передачи 100 Мбит/с добавляют стоимость 19, а порты со скоростью передачи 10 Мбит/с добавляют стоимость 100. В случае CIST-экземпляра MSTP это стоимость пути к внешнему корневому мосту, которая представляет собой стоимость пути от корневого моста IST (т. е. регионального моста) к корневому мосту CST (т. е. "глобальному" корневому мосту сети).
`Configured Hello Time`	**Краткий обзор:** Целое число от 0 до 65535 Сконфигурированный параметр Hello time (интервал времени между конфигурационными сообщениями, подтверждающими работоспособность устройства) из формы Bridge RSTP Parameters (RSTP-параметры моста).
`Learned Hello Time`	**Краткий обзор:** Целое число от 0 до 65535 Фактический интервал времени между конфигурационными сообщениями, подтверждающими работоспособность устройства, настроенный на корневом мосте и полученный в конфигурационных сообщениях. Этот интервал времени используется в выделенных мостах.

Параметр	Описание
`Configured Forward Delay`	**Краткий обзор:** Целое число от 0 до 65535 Сконфигурированный интервал времени Forward Delay (задержка пересылки) из формы Bridge RSTP Parameters (RSTP-параметры моста).
`Learned Forward Delay`	**Краткий обзор:** Целое число от 0 до 65535 Фактическое время задержки пересылки, настроенное на корневом мосте и полученное в конфигурационных сообщениях. Этот интервал времени используется в выделенных мостах.
`Configured Max Age`	**Краткий обзор:** Целое число от 0 до 65535 Сконфигурированный параметр Maximum Age (максимальный возраст сообщения) из формы Bridge RSTP Parameters (RSTP-параметры моста).
`Learned Max Age`	**Краткий обзор:** Целое число от 0 до 65535 Фактическое значение параметра Maximum Age (максимальный возраст сообщения), настроенное на корневом мосте и полученное в конфигурационных сообщениях. Этот интервал времени используется в выделенных мостах.
`Total Topology Changes`	**Краткий обзор:** Целое число от 0 до 65535 Счетчик изменений топологии в сети, которые были обнаружены на данном мосте в виде отказов каналов связи или о которых сообщили другие мосты. Чрезмерно большие или быстро растущие значения счетчиков сигнализируют о проблемах с сетью.
`Time since Last TC`	**Краткий обзор:** DDDD days, HH:MM:SS Время с момента последнего изменения топологии, обнаруженного мостом.

9.1.8 Вывод диагностики STP для Ethernet-портов

Чтобы просмотреть статистику STP для Ethernet-портов, перейдите в ***Network Redundancy » Spanning Tree » View Port RSTP Statistics***. Появится таблица **Port RSTP Statistics**.

В этой таблице отображается следующая информация:

Параметр	Описание
`Port(s)`	**Краткий обзор:** Comma-separated list of ports Номер порта устройства (или список портов, если они объединены в группу).
`Status`	**Краткий обзор:** [Disabled | Listening | Learning | Forwarding | Blocking | Link Down | Discarding] Статус этого порта в связующем дереве. Может иметь одно из следующих значений:

Параметр	Описание
	• `Disabled (Отключено)` - STP отключен для данного порта. • `Listening (Прослушивание)` - это состояние не используется • `Learning (Запоминание)` - порт запоминает MAC-адреса, чтобы исключить избыточную рассылку, когда он начнет пересылать трафик. • `Forwarding (Пересылка)` - порт пересылает трафик. • `Blocking (Блокировка)` - порт блокирует трафик. • `Link Down (Соединение отсутствует)` - STP включен для данного порта, но сам порт физически не работает. • `Discarding (Сбрасывание)` - данный канал связи не используется в топологии STP, но находится в дежурном режиме.
`Role`	**Краткий обзор:** [Root | Designated | Alternate | Backup | Master] Роль этого порта в связующем дереве. Может иметь одно из следующих значений: • `Designated (Выделенный)` - порт является выделенным (то есть передает трафик в направлении корневого моста) для сегмента локальной сети, к которой подключен. • `Root (Корневой)` - единственный порт данного моста, который обеспечивает связность в направлении корневого моста. • `Backup (Резервный)` - порт подключен к сегменту локальной сети, который обслуживается другим портом этого моста. Не используется, но находится в дежурном режиме. • `Alternate (Альтернативный)` - порт подключен к коммутатору, который обеспечивает связность с корневым мостом. Не используется, но находится в дежурном режиме. • `Master (Главный)` - существует только в MSTP. Это граничный порт MST-региона и единственный порт моста, который обеспечивает связность для экземпляра множественного связующего дерева в направлении корневого порта общего связующего дерева (т. е. этот порт является корневым портом для экземпляра общего связующего дерева).
`Cost`	**Краткий обзор:** Целое число от 0 до 4294967295 Стоимость, обеспечиваемая этим портом. Если в форме Bridge RSTP Parameters (RSTP-параметры моста) для параметра Cost Style (тип значения стоимости) выбран вариант STP, то порты со скоростью передачи 1 Гбит/с добавляют стоимость, равную четырем, порты со скоростью передачи 100 Мбит/с добавляют стоимость 19, а порты со скоростью передачи 10 Мбит/с добавляют стоимость 100. Если для параметра Cost Style выбран вариант RSTP, то порты со скоростью передачи 1 Гбит/с добавляют стоимость 20000, порты со скоростью передачи 100 Мбит/с добавляют стоимость 200000, а порты со скоростью передачи 10 Мбит/с добавляют стоимость 2000000. Обратите внимание, что даже в том случае, когда для параметра Cost Style задано значение RSTP, при миграции порта к STP его стоимость будет ограничена максимальной величиной 65535.

Параметр	Описание
RX RSTs	**Краткий обзор:** Целое число от 0 до 4294967295 Счетчик конфигурационных сообщений RSTP, принятых на этот порт.
TX RSTs	**Краткий обзор:** Целое число от 0 до 4294967295 Счетчик конфигурационных сообщений RSTP, переданных с этого порта.
RX Configs	**Краткий обзор:** Целое число от 0 до 4294967295 Счетчик конфигурационных сообщений STP, принятых на этот порт.
TX Configs	**Краткий обзор:** Целое число от 0 до 4294967295 Счетчик конфигурационных сообщений STP, переданных с этого порта.
RX Tcns	**Краткий обзор:** Целое число от 0 до 4294967295 Счетчик оповещающих сообщений об изменениях топологии, принятых на этот порт. Чрезмерно большие или быстро растущие значения счетчиков сигнализируют о проблемах с сетью.
TX Tcns	**Краткий обзор:** Целое число от 0 до 4294967295 Счетчик оповещающих сообщений об изменениях топологии, переданных с этого порта.
Desig Bridge ID	**Краткий обзор:** $$ / ##-##-##-##-##-## where $$ is 0 to 65535, ## is 0 to FF Доступно на корневых портах назначенных мостов, идентификатор моста, к которому подключен этот порт.
operEdge	**Краткий обзор:** [True | False] Работает ли данный порт в качестве граничного порта.

9.1.9 Управление экземплярами множественного связующего дерева

В данном разделе описывается конфигурирование экземпляров множественного связующего дерева (MSTI) и управление ими.

9.1.9.1 Вывод диагностики для глобальных MSTI

Чтобы просмотреть статистику для глобальных MSTI, перейдите в ***Network Redundancy » Spanning Tree » View Bridge MSTI Statistics***. Появится форма **Bridge MSTI Statistics**.

Чтобы просмотреть статистику для глобальных MSTI, перейдите в ***Spanning Tree » View Bridge MSTI Statistics***. Появится форма **Bridge MSTI Statistics**.

В этой таблице отображается следующая информация:

Параметр	Описание
`Bridge Status`	**Краткий обзор:** [Designated Bridge | Not Designated For Any LAN | Root Bridge] Статус моста в связующем дереве. Статус может иметь значение "корневой" или "выделенный". В этом поле может отображаться "не выделено для LAN", если мост не является выделенным для какого-либо из своих портов.
`Bridge ID`	**Краткий обзор:** $$ / ##-##-##-##-##-## where $$ is 0 to 65535, ## is 0 to FF Идентификатор данного моста.
`Root ID`	**Краткий обзор:** $$ / ##-##-##-##-##-## where $$ is 0 to 65535, ## is 0 to FF Идентификатор моста для корневого моста.
`Root Port`	**Краткий обзор:** 1 to maximum port number или [<empty string>] Если коммутатор выделенный, то это порт, который обеспечивает связность в направлении корневого моста сети.
`Root Path Cost`	**Краткий обзор:** Целое число от 0 до 4294967295 Полная стоимость пути к корневому мосту, состоящая из суммы стоимостей каждого канала связи на этом пути. Если значения стоимости не были заданы специально, то порты со скоростью передачи 1 Гбит/с добавляют стоимость, равную четырем, порты со скоростью передачи 100 Мбит/с добавляют стоимость 19, а порты со скоростью передачи 10 Мбит/с добавляют стоимость 100. В случае CIST-экземпляра MSTP это стоимость пути к внешнему корневому мосту, которая представляет собой стоимость пути от корневого моста IST (т. е. регионального моста) к корневому мосту CST (т. е. "глобальному" корневому мосту сети).
`Total Topology Changes`	**Краткий обзор:** Целое число от 0 до 65535 Счетчик изменений топологии в сети, которые были обнаружены на данном мосте в виде отказов каналов связи или о которых сообщили другие мосты. Чрезмерно большие или быстро растущие значения счетчиков сигнализируют о проблемах с сетью.

9.1.9.2 Вывод диагностики для MSTI портов

Чтобы просмотреть статистику для MSTI портов, перейдите в ***Network Redundancy » Spanning Tree » View Port MSTI Statistics***. Появится форма **Port MSTI Statistics**.

В этой таблице отображается следующая информация:

Параметр	Описание
`Port(s)`	**Краткий обзор:** Comma-separated list of ports Номер порта устройства (или список портов, если они объединены в группу).
`Status`	**Краткий обзор:** [Disabled | Listening | Learning | Forwarding | Blocking | Link Down | Discarding] Статус этого порта в связующем дереве. Может иметь одно из следующих значений: • `Disabled (Отключено)` - STP отключен для данного порта. • `Listening (Прослушивание)` - это состояние не используется • `Learning (Запоминание)` - порт запоминает MAC-адреса, чтобы исключить избыточную рассылку, когда он начнет пересылать трафик. • `Forwarding (Пересылка)` - порт пересылает трафик. • `Blocking (Блокировка)` - порт блокирует трафик. • `Link Down (Соединение отсутствует)` - STP включен для данного порта, но сам порт физически не работает. • `Discarding (Сбрасывание)` - данный канал связи не используется в топологии STP, но находится в дежурном режиме.
`Role`	**Краткий обзор:** [Root | Designated | Alternate | Backup | Master] Роль этого порта в связующем дереве. Может иметь одно из следующих значений: • `Designated (Выделенный)` - порт является выделенным (то есть передает трафик в направлении корневого моста) для сегмента локальной сети, к которой подключен. • `Root (Корневой)` - единственный порт данного моста, который обеспечивает связность в направлении корневого моста. • `Backup (Резервный)` - порт подключен к сегменту локальной сети, который обслуживается другим портом этого моста. Не используется, но находится в дежурном режиме. • `Alternate (Альтернативный)` - порт подключен к коммутатору, который обеспечивает связность с корневым мостом. Не используется, но находится в дежурном режиме. • `Master (Главный)` - существует только в MSTP. Это граничный порт MST-региона и единственный порт моста, который обеспечивает связность для экземпляра множественного связующего дерева в направлении корневого порта общего связующего дерева (т. е. этот порт является корневым портом для экземпляра общего связующего дерева).
`Cost`	**Краткий обзор:** Целое число от 0 до 4294967295 Стоимость, обеспечиваемая этим портом. Если в форме Bridge RSTP Parameters (RSTP-параметры моста) для параметра Cost Style (тип значения стоимости) выбран вариант STP, то порты со скоростью передачи 1 Гбит/с добавляют стоимость, равную четырем, порты со скоростью передачи 100 Мбит/с

Параметр	Описание
	добавляют стоимость 19, а порты со скоростью передачи 10 Мбит/с добавляют стоимость 100. Если для параметра Cost Style выбран вариант RSTP, то порты со скоростью передачи 1 Гбит/с добавляют стоимость 20000, порты со скоростью передачи 100 Мбит/с добавляют стоимость 200000, а порты со скоростью передачи 10 Мбит/с добавляют стоимость 2000000. Обратите внимание, что даже в том случае, когда для параметра Cost Style задано значение RSTP, при миграции порта к STP его стоимость будет ограничена максимальной величиной 65535.
`Desig Bridge ID`	**Краткий обзор:** $$ / ##-##-##-##-##-## where $$ is 0 to 65535, ## is 0 to FF Доступно на корневых портах назначенных мостов, идентификатор моста, к которому подключен этот порт.

9.1.9.3 Конфигурирование идентификатора MST-региона

Конфигурирование идентификатора региона и уровня версии ставит мост MSTP в определенную группу. Другие мосты, имеющие такой же идентификатор и уровень версии, взаимосвязаны в пределах этого региона. Для получения дополнительной информации см. "MSTP-регионы и совместимость с другими протоколами (Страница 231)".

Чтобы сконфигурировать идентификатор региона множественного связующего дерева (MST), сделайте следующее:

1. Перейдите в ***Network Redundancy » Spanning Tree » Configure MST Region Identifier***. Появится форма **MST Region Identifier**.
2. Необходимо сконфигурировать следующие параметры:

Параметр	Описание
`Name`	**Краткий обзор:** Строка длиной 32 символа(ов) **Значение по умолчанию:** 00-0A-DC-92-00-00 Имя MST-региона. Все устройства в одном и том же MST-регионе должны иметь одно и то же сконфигурированное имя региона.
`Revision Level`	**Краткий обзор:** Целое число от 0 до 65535 **Значение по умолчанию:** 0 Уровень версии для конфигурации MST. Как правило, все устройства в одном и том же MST-регионе сконфигурированы с одним и тем же уровнем версии. Однако для создания субрегионов с одним именем региона могут использоваться разные уровни версий.
`Digest`	**Краткий обзор:** Строка длиной 32 символа(ов) **Значение по умолчанию:** 0 Это параметр только для чтения, который стоит использовать лишь в целях выявления и устранения проблем с сетью. Чтобы обеспечить корректное отображение сетей VLAN на экземпляр связующего

Параметр	Описание
	дерева, протокол должен быть в состоянии точно идентифицировать границы MST-регионов. С этой целью характеристики региона включаются в сообщения BPDU. Нет необходимости распространять в сообщениях BPDU точную информацию об отображении сетей VLAN на экземпляр связующего дерева, поскольку коммутаторам нужно иметь сведения лишь о том, находятся ли они в одном регионе со своим соседом. Поэтому в сообщениях BPDU посылается только этот 16-октетный дайджест, создаваемый из информации об отображения сетей VLAN на экземпляр связующего дерева.

3. Нажмите **Apply**.

9.1.9.4 Конфигурирование глобального MSTI

Чтобы сконфигурировать глобальный экземпляр множественного связующего дерева (MSTI) для протокола связующего дерева (STP), сделайте следующее:

1. Перейдите в ***Network Redundancy » Spanning Tree » Configure Bridge MSTI Parameters***. Появится форма **Bridge MSTI Parameters**.
2. В поле **Instance ID** введите идентификационный номер для MSTI и нажмите **GET**. Отобразятся настройки для MSTI. Любые изменения, внесенные в конфигурацию, будут применены конкретно к идентификатору этого экземпляра.
3. Необходимо сконфигурировать следующие параметры:

Параметр	Описание
`Bridge Priority`	**Краткий обзор:** [0 | 4096 | 8192 | 12288 | 16384 | 20480 | 24576 | 28672 | 32768 | 36864 | 40960 | 45056 | 49152 | 53248 | 57344 | 61440] **Значение по умолчанию:** 32768 Параметр Bridge Priority (приоритет моста) обеспечивает способ управления топологией сети с соединениями по протоколу STP. Требуемые корневые и выделенные мосты могут быть сконфигурированы для конкретной топологии. Мост с наименьшим приоритетом станет корневым мостом. В случае отказа корневого моста корневым станет мост с последующим наименьшим приоритетом. Выделенные мосты, которые (в целях дублирования) обслуживают общую локальную сеть, также используют приоритет для определения того, какой мост активен. Таким образом, при тщательном подборе приоритетов мостов можно определить пути передачи трафика как для нормального состояния сети, так и на случай отказа какого-либо соединения.

4. Нажмите **Apply**.

9.1.9.5 Конфигурирование MSTI для Ethernet-порта

Чтобы сконфигурировать глобальный экземпляр множественного связующего дерева (MSTI) для Ethernet-порта, сделайте следующее:

1. Перейдите в ***Network Redundancy » Spanning Tree » Configure Port MSTI Parameters***. Появится таблица **Port MSTI Parameters**.
2. Выберите Ethernet-порт. Появится форма **Port MSTI Parameters**.
3. В поле **Instance ID** введите идентификационный номер для MSTI и нажмите **GET**. Отобразятся настройки для MSTI. Любые изменения, внесенные в конфигурацию, будут применены конкретно к идентификатору этого экземпляра.
4. Необходимо сконфигурировать следующие параметры:

Параметр	Описание
`Port(s)`	**Краткий обзор:** Comma-separated list of ports Номер порта устройства (или список портов, если они объединены в группу).
`Priority`	**Краткий обзор:** [0 | 16 | 32 | 48 | 64 | 80 | 96 | 112 | 128 | 144 | 160 | 176 | 192 | 208 | 224 | 240] **Значение по умолчанию:** 128 Выбор приоритета для STP-порта. Порт для использования будет выбираться из портов с одинаковой стоимостью, подключенных к общей локальной сети, на основании приоритета этого порта.
`STP Cost`	**Краткий обзор:** Целое число от 0 до 65535 или [Auto] **Значение по умолчанию:** Auto Выбор значения стоимости, используемого при вычислениях стоимости, когда для параметра Cost Style (тип значений стоимости) выбран вариант STP в конфигурации RSTP-параметров моста. Настройка значений стоимости вручную обеспечивает возможность выбирать определенные порты для преимущественной передачи трафика через них, минуя остальные порты. Оставьте для этого порта значение "автоматически", чтобы использовать стандартные согласованные значения стоимости STP-порта (4 для скорости передачи 1 Гбит/с, 19 для каналов связи со скоростью передачи 100 Мбит/с и 100 для каналов связи со скоростью передачи 10 Мбит/с). В случае MSTP этот параметр применим к стоимости внешнего и внутреннего пути.
`RSTP Cost`	**Краткий обзор:** Целое число от 0 до 2147483647 или [Auto] **Значение по умолчанию:** Auto Выбор значения стоимости, используемого при вычислениях стоимости, когда для параметра Cost Style (тип значений стоимости) выбран вариант RSTP в конфигурации RSTP-параметров моста. Настройка значений стоимости вручную обеспечивает возможность выбирать определенные порты для преимущественной передачи трафика через них, минуя остальные порты.

Параметр	Описание
	Оставьте для этого порта значение "автоматически", чтобы использовать стандартные значения стоимости RSTP-порта, полученные при автоматическом согласовании (20000 для скорости передачи 1 Гбит/с, 200000 для каналов связи со скоростью передачи 100 Мбит/с и 2000000 для каналов связи со скоростью передачи 10 Мбит/с). В случае MSTP этот параметр применим к стоимости внешнего и внутреннего пути.

5. Нажмите **Apply**.

9.1.10 Очистка статистики протокола связующего дерева

Чтобы полностью очистить статистику протокола связующего действия, сделайте следующее:

1. Перейдите в ***Network Redundancy » Spanning Tree » Clear Spanning Tree Statistics***. Появится форма **Clear Spanning Tree Statistics**.
2. Нажмите **Confirm**.

9.2 Управление протоколом резервирования среды передачи (MRP)

RUGGEDCOM ROS поддерживает протокол резервирования среды передачи (MRP).

9.2.1 Основные сведения о протоколе MRP

Протокол резервирования среды передачи (MRP) — это сетевой протокол, разработанный для реализации резервирования и восстановления в кольцевой топологии, содержащей до 50 устройств. Он позволяет кольцам Ethernet-коммутаторов быстро преодолевать любой одиночный отказ межкоммутаторного канала связи или коммутатора в кольце MRP или соединительной топологии.

MRP работает между 2-м уровнем и прикладным уровнем и использует функции ISO/МЭК/IEEE 8802-3 (IEEE 802.3) и IEEE 802.1Q, включая базу данных фильтрации (FDB).

Протокол MRP стандартизирован Международной электротехнической комиссией как МЭК 62439-2.

9.2.1.1 Сравнение устройств MRM и MRC

В кольце MRP менеджер резервирования среды передачи (MRM) действует как менеджер кольца, а клиент резервирования среды передачи (MRC) — как узлы, принадлежащие кольцу.

MRM периодически отправляет сообщения тестирования MRP через оба своих порта кольцевой сети. Эти сообщения передаются устройствами MRC между их портами кольцевой сети. Поскольку коммутаторы соединены в кольцо, сообщение тестирования MRP циркулирует через кольцо и возвращается на MRM. Это позволяет MRM определить состояние кольцевой сети.

Если сообщения тестирования MRP возвращаются на MRM, резервирование присутствует, а кольцо объявляется замкнутым. Если сообщения тестирования MRP не возвращаются, то резервирование потеряно, а кольцо объявляется разомкнутым.

Если кольцо замкнуто, MRM отбрасывает (блокирует) все пакеты на одном из своих двух выделенных кольцевых портов, а другой порт пересылает пакеты. При отказе канала связи клиенты MRC отправляют уведомление об отказе канала связи на менеджер MRM, который в свою очередь разблокирует заблокированный порт, активируя связь между всеми устройствами.

9.2.1.2 Устройства MRA

Устройства, являющиеся автоматическими менеджерами резервирования среды передачи (MRA), автоматически решают, какое устройство возьмет на себя роль менеджера в кольце. Это осуществляется в процессе выбора между всеми MRA в сети. После того, как менеджер будет выбран, остальные MRA выступают в качестве клиентов.

Если в кольцевой сети присутствует MRA, все остальные устройства в сети должны быть устройствами MRA или MRC (но не MRM).

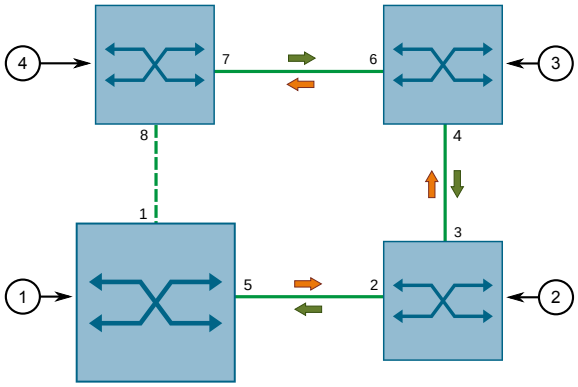
9.2.1.3 Состояния портов кольцевой сети

Порты кольцевой сети MRM и MRC поддерживают три состояния: *отключено*, *заблокировано* и *пересылка*:

- **Отключенные** порты кольцевой сети отбрасывают все полученные пакеты.
- **Заблокированные** порты кольцевой сети отбрасывают все полученные пакеты, кроме пакетов управления MRP.
- **Пересылающие** порты кольцевой сети пересылают все полученные пакеты.

9.2.1.4 Сравнение замкнутого кольца и разомкнутого кольца

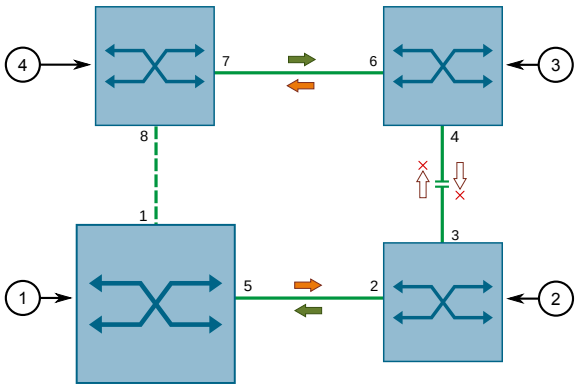
При нормальном режиме работы сеть работает в состоянии замкнутой кольцевой сети. В этом состоянии один из портов кольцевой сети устройства MRM блокируется, а другие являются пересылающими. Оба порта кольцевой сети всех устройств MRC являются пересылающими.



① Устройство MRM или MRA, действующее в качестве менеджера
② Клиент MRP 1
③ Клиент MRP 2
④ Клиент MRP 3

Рисунок 9.5 Состояние замкнутой кольцевой сети MRP

В случае отказа сеть работает в режиме разомкнутой кольцевой сети. Если в этом состоянии отказывает канал связи двух устройств, оба порта кольцевой сети устройства MRM становятся пересылающими. У устройств MRC, расположенных рядом с отказом, один порт кольцевой сети является заблокированным, а другой — пересылающим; у остальных устройств MRC оба порта кольцевой сети являются пересылающими.



① Устройство MRM или MRA, действующее в качестве менеджера
② Клиент MRP 1

③ Клиент MRP 2
④ Клиент MRP 3

Рисунок 9.6 Состояние разомкнутой кольцевой сети MRP

9.2.2 Глобальное конфигурирование MRP

Чтобы сконфигурировать протокол резервирования среды передачи данных (MRP) глобально, сделайте следующее:

1. Перейдите в ***Network Redundancy » Ring Redundancy » Configure Global MRP Parameters***. Появится форма **Global MRP Parameters**.
2. Необходимо сконфигурировать следующие параметры:

Параметр	Описание
`State`	**Краткий обзор:** [Disabled | Enabled] **Значение по умолчанию:** Disabled Глобально включает/отключает MRP. Обратите внимание, что MRP может быть отключен для каждого порта в отдельности.
`Auto Generate UUID`	**Краткий обзор:** [Disabled | Enabled] **Значение по умолчанию:** Enabled Включает/отключает автоматическое генерирование универсальный уникальный идентификатор MRP (UUID). Если этот параметр включен, любой существующий пользовательский идентификатор домена будет перезаписан сгенерированным UUID. Сгенерированный UUID — это MD5-хэш доменного имени.

3. Нажмите **Apply**.

9.2.3 Просмотр состояния экземпляров MRP

Чтобы просмотреть состояние экземпляров MRP, перейдите в ***Network Redundancy » Ring Redundancy » View MRP Instance Status***. Появится таблица **MRP Instance Status**.

В этой таблице отображается следующая информация:

Параметр	Описание
`Index`	Номер экземпляров MRP.
`Name`	**Краткий обзор:** Строка длиной 24 символа(ов) или [default-mrpdomain] **Значение по умолчанию:** default-mrpdomain Имя домена/кольца MRP. Все экземпляры MRP, принадлежащие одному и тому же кольцу, должны иметь одно и то же доменное имя.

Параметр	Описание
Role	Роль, назначенная экземпляру MRP: • Disabled (Отключено) - Назначенная роль отсутствует. Экземпляр MRP отключен. • Client (Клиент) - Клиент MRP. • Manager (Менеджер) - Менеджер MRP. • ManagerAuto (Автоматический менеджер) - Экземпляр MRP автоматически определяет роль.
Ring Status	Состояние кольца MRP. Возможные значения включают: • Неприменимо - Состояние кольца неизвестно. Отображается, если устройство является MRC. • Разомкнуто - Кольцо MRP разомкнуто. Оба порта кольца пересылают пакеты. • Замкнуто - Кольцо MRP замкнуто. Один порт кольца пересылает пакеты, а другой — блокирует.
PRM Port	Номер порта и состояние порта кольца MRP. Возможные значения включают: • { *порт* }- OFF (ВЫКЛ.) - MRP не выполняется. • { *порт* }- DWN - порт кольца не работает. • { *порт* }- BLK - порт кольца блокирует пакеты. • { *порт* }- FWD - порт кольца пересылает пакеты.
SEC Port	Номер порта и состояние порта кольца MRP. Возможные значения включают: • { *порт* }- OFF (ВЫКЛ.) - MRP не выполняется. • { *порт* }- DWN - порт кольца не работает. • { *порт* }- BLK - порт кольца блокирует пакеты. • { *порт* }- FWD - порт кольца пересылает пакеты.
Multi-MRM Err	Ошибка, указываемая MRM, если активно более одного устройства MRM в кольцевой сети MRP. Возможные значения включают: • ложно - ошибка Multi-MRM отсутствует. • истинно - в кольцевой сети присутствует больше одного устройства MRM.
One Side Rx Err	Ошибка, указываемая устройством MRM, если тестовые кадры MRM поступают только на один порт кольца. Возможные значения включают: • ложно - ошибка One Side Rx отсутствует. • истинно - тестовый кадр поступает только на один порт кольца.

9.2.4 Добавление экземпляра MRP

Чтобы сконфигурировать экземпляр MRP, сделайте следующее:

1. Перейдите в ***Network Redundancy » Ring Redundancy » Configure MRP Instances***. Появится таблица **MRP Instances**.
2. Нажмите **InsertRecord**. Появится форма **MRP Instances**.

Примечание
RUGGEDCOM ROS допускает наличие нескольких экземпляров MRP, если все экземпляры являются менеджерами. Устройство может иметь до четырех экземпляров, являющихся менеджерами.

⚠ ЗАМЕТКА

Опасность для конфигурации — риск нарушения обмена данными

RUGGEDCOM ROS допускает наличие нескольких экземпляров MRP, если устройство является менеджером кольца в каждом экземпляре. Устройство может иметь до четырех экземпляров, являющихся менеджерами кольца.

⚠ ЗАМЕТКА

Опасность для конфигурации — риск нарушения обмена данными

Прежде чем конфигурация экземпляра MRM сможет быть изменена, устройства MRM или MRA, действующие в качестве менеджера, либо должны быть физически отключены, либо их порт кольцевой сети должен быть отключен (т. е. кольцевая сеть MRP разомкнута).

Для получения дополнительной информации о конфигурировании параметров порта см. "Конфигурирование Ethernet-порта (Страница 76)".

Для получения дополнительной информации о разомкнутых и замкнутых кольцах MRP см. "Управление протоколом резервирования среды передачи (MRP) (Страница 253)".

Примечание
Чтобы избежать потенциальных ошибок конфигурации, которые могут привести к потере сетевого доступа, Siemens рекомендует отключать порт кольцевой сети устройства MRC перед его конфигурированием. Для получения дополнительной информации о конфигурировании параметров порта см. "Конфигурирование Ethernet-порта (Страница 76)".

Примечание
При использовании безопасности на уровне порта в кольцевой сети MRP необходимо сконфигурировать MAC-адреса устройств в кольцевой сети для обеспечения связи между ними. Кроме того, порт кольцевой сети устройства MRM должен быть сконфигурирован в таблице **Static MAC Addresses**, чтобы кольцевая сеть оставалась в замкнутом состоянии. Для

получения дополнительной информации см. "Аутентификация на базе статического MAC-адреса в кольце MRP (Страница 143)".

3. Необходимо сконфигурировать следующие параметры:

Параметр	Описание
`Index`	**Краткий обзор:** Целое число от 1 до 4 **Значение по умолчанию:** 1 Номер экземпляров MRP.
`Name`	**Краткий обзор:** Строка длиной 24 символа(ов) **Значение по умолчанию:** default-mrpdomain Имя домена/кольца MRP. Все экземпляры MRP, принадлежащие одному и тому же кольцу, должны иметь одно и то же доменное имя.
`Role`	**Краткий обзор:** [Disabled | Client | Manager | ManagerAuto] **Значение по умолчанию:** Client Роль, назначенная экземпляру MRP: • `Disabled (Отключено)` - Назначенная роль отсутствует. Экземпляр MRP отключен. • `Client (Клиент)` - Клиент MRP. • `Manager (Менеджер)` - Менеджер MRP. • `ManagerAuto (Автоматический менеджер)` - Экземпляр MRP автоматически определяет роль.
`PRM Port`	**Краткий обзор:** 1 to maximum port number **Значение по умолчанию:** 1 Номер порта кольца MRP. Номер порта в том виде, как он записан на устройстве.
`SEC Port`	**Краткий обзор:** 1 to maximum port number **Значение по умолчанию:** 1 Номер порта кольца MRP. Номер порта в том виде, как он записан на устройстве.
`Priority`	**Краткий обзор:** Строка длиной 4 символа(ов) **Значение по умолчанию:** 8000 Приоритет, назначенная экземпляру MRP. Используется при согласовании с другими устройствами MRP, чтобы определить, которое из них является менеджером MRP. Возможные значения включают: • `0000` - Наивысший приоритет, менеджер (Manager) • `1000` – 7000 — Высокий приоритет, менеджер (Manager) • `8000` - Приоритет по умолчанию, менеджер (Manager) • `9000 – E000` - Низкий приоритет, автоматический менеджер (ManagerAuto) • `F000` - Низший приоритет, автоматический менеджер (ManagerAuto)

Параметр	Описание
	Приоритет применяется только в том случае, если параметр Role (Роль) установлен на "менеджер" или "автоматический менеджер".
`ID`	**Краткий обзор:** Строка длиной 32 символа(ов) **Значение по умолчанию:** FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF 128-битовый доменный идентификатор UUID, уникальный для домена/кольцевой сети. Все экземпляры MRP, принадлежащие одной кольцевой сети, должны иметь одинаковый доменный идентификатор. Если включен параметр Auto Generate UUID (автоматическое генерирование универсального уникального идентификатора), ROS автоматически генерирует доменный идентификатор как MD5-хэш доменного имени. В этом случае любая попытка изменить доменный идентификатор будет отклонена. Если параметр Auto Generate UUID отключен, доменный идентификатор может быть изменен пользователем.

4. Нажмите **Apply**.

9.2.5 Удаление экземпляра MRP

Чтобы удалить экземпляр MRP, сделайте следующее:

1. Перейдите в ***Network Redundancy » Ring Redundancy » Configure MRP Instances***. Появится таблица **MRP Instances**.
2. Выберите необходимую запись. Появится форма **MRP Instances**.

⚠ ЗАМЕТКА

Прежде чем конфигурация экземпляра MRM сможет быть изменена, устройства MRM или MRA, действующие в качестве менеджера, либо должны быть физически отключены, либо их порт кольцевой сети должен быть отключен (т. е. кольцевая сеть MRP разомкнута).

Для получения дополнительной информации о конфигурировании параметров порта см. "Конфигурирование Ethernet-порта (Страница 76)".

Для получения дополнительной информации о разомкнутых и замкнутых кольцах MRP см. "Управление протоколом резервирования среды передачи (MRP) (Страница 253)".

Примечание
Чтобы избежать потенциальных ошибок конфигурации, которые могут привести к потере сетевого доступа, Siemens рекомендует отключать порт кольцевой сети устройства MRC перед его конфигурированием. Для получения дополнительной информации о конфигурировании параметров порта см. "Конфигурирование Ethernet-порта (Страница 76)".

3. Нажмите **Delete**.

9.2.6 Пример: Конфигурирование кольцевой сети MRP

В данном примере показано, как сконфигурировать кольцевую сеть MRP с использованием четырех устройств RUGGEDCOM ROS.

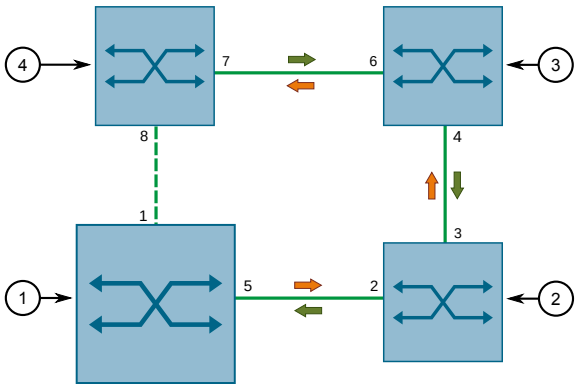
В следующей топологии кольцевая сеть MRP работает в замкнутом состоянии. Менеджер MRP (MRM) выполняет роль менеджера кольцевой сети, а клиенты MRP (MRC) действуют как узлы, принадлежащие кольцевой сети. У каждого MRM или узла MRC есть два порта, участвующих в кольцевой сети.

Устройство MRM блокирует все пакеты, пересылаемые на один из его двух выделенных портов кольцевой сети. Если один из двух каналов связи на любом их других узлов кольцевой сети обнаруживает отказ, кольцевая сеть MRP перейдет в разомкнутое состояние. В этом состоянии устройство MRC посылает сообщение на устройство MRM, которое затем разблокирует свой заблокированный порт, обеспечивая связь всех коммутаторов.

Для получения дополнительной информации о разомкнутых и замкнутых кольцах см. "Управление протоколом резервирования среды передачи (MRP) (Страница 253)".

⚠ ЗАМЕТКА

Указанные значения характерны для представленной топологии. Фактические значения могут отличаться, в зависимости от конфигурации пользователя.



① Менеджер MRP
② Клиент MRP 1
③ Клиент MRP 2
④ Клиент MRP 3

Рисунок 9.7 Топология — кольцевая сеть MRP

Чтобы сконфигурировать кольцевую сеть MRP в соответствии с топологией, сделайте следующее:

1. Убедитесь, что протокол RSTP отключен на портах, действующих как порты PRM и SEC в кольцевой сети. Для получения дополнительной информации см. "Конфигурирование Ethernet-порта (Страница 76)".
2. Включите MRP на менеджере MRP и всех клиентских устройствах MRP. Для получения дополнительной информации см. "Глобальное конфигурирование MRP (Страница 256)".
3. Сконфигурируйте экземпляр MRP для менеджера MRP следующим образом:

Параметр	Значение
Имя	{ name }
Роль	Менеджер
PRM-порт	5
SEC-порт	1
Приоритет	1000

   Для получения дополнительной информации о конфигурировании экземпляров MRP см. "Добавление экземпляра MRP (Страница 258)".
4. Сконфигурируйте экземпляр MRP для каждого клиента MRP следующим образом:

   Примечание
   В данном примере используется три устройства. Протокол MRP поддерживается в кольцевых топологиях до 50 устройств.

Устройство	Параметр	Значение
Клиент MRP 1	Имя	{ name }
	Роль	Клиент
	PRM-порт	2
	SEC-порт	3
	Приоритет	A000
Клиент MRP 2	Имя	{ name }
	Роль	Клиент
	PRM-порт	4
	SEC-порт	6
	Приоритет	A000
Клиент MRP 3	Имя	{ name }
	Роль	Клиент
	PRM-порт	7
	SEC-порт	8
	Приоритет	A000

   Для получения дополнительной информации о конфигурировании экземпляров MRP см. "Добавление экземпляра MRP (Страница 258)".

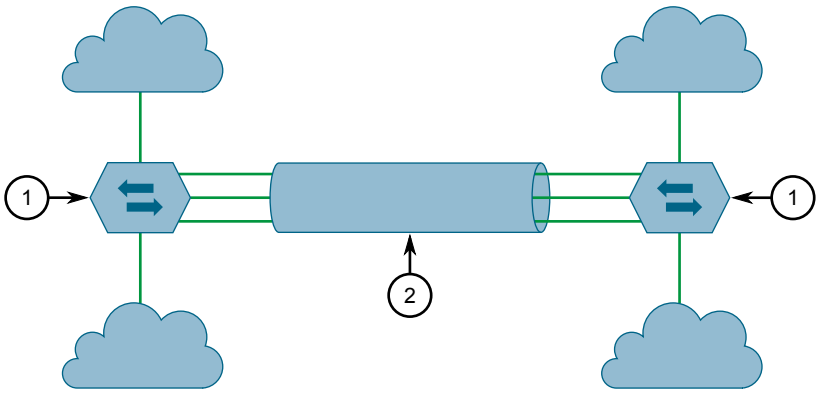
5. Чтобы проверить конфигурацию, необходимо убедиться, что идентификатор экземпляра MRP автоматически генерируется на менеджере MRP и на каждом клиенте MRP. Для получения дополнительной информации об идентификаторе экземпляра MRP см. "Добавление экземпляра MRP (Страница 258)".

9.3 Управление агрегированием каналов связи

Агрегирование каналов связи также известно как *транкинг/объединение портов* или *связывание портов*. Оно обеспечивает способность агрегировать или комбинировать несколько Ethernet-портов в один логический канал связи (группу агрегирования каналов связи) с более высокой пропускной способностью. Это обеспечивает высоко рандомизированный баланс загрузки между агрегированными каналами связи на основе MAC-адресов отправителя и получателя в пересылаемых кадрах.

Агрегирование каналов связи может использоваться для двух целей:

- Для получения повышенной, линейно возрастающей пропускной способности канала связи.
- Для повышения надежности сети за счет создания дублирующих каналов связи. Если один из агрегированных каналов связи выходит из строя, то коммутатор равномерно распределит трафик между остальными каналами связи.



① Устройство
② Группа агрегирования каналов связи (LAG)

Рисунок 9.8 Базовая топография агрегирования каналов связи

9.3.1 Концепция агрегирования каналов связи

В данном разделе рассматриваются некоторые принципы, имеющие значение для реализации агрегирования каналов связи в RUGGEDCOM ROS.

9.3.1.1 Сравнение статического и динамического агрегирования каналов связи

RUGGEDCOM ROS поддерживает либо статическое, либо динамическое агрегирование каналов связи. При **статическом** агрегировании каналов связи происходит сопряжение устройства с конкретным устройством-партнером, обладающего такими же возможностями и конфигурацией. То же самое необходимо для динамического агрегирования каналов связи, однако требуемый уровень вмешательства пользователя ниже. При **динамическом** агрегировании каналов связи протокол управления агрегированием каналов (LACP) самостоятельно выполняет поиск подходящего партнера после согласования со своими узлами, чтобы определить наилучшее совпадение.

Статическое агрегирование каналов связи идеально подходит для конфигураций коммутатор-коммутатор, но у него отсутствуют следующие ключевые характеристики, обеспечиваемые динамическим агрегированием каналов связи:

- **Переключение**

  При статическом агрегировании каналов связи устройства не могут сообщать статус своих групп агрегирования каналов связи. Если все порты в группе агрегирования каналов связи перестанут функционировать и при наличии преобразователя среды между устройствами устройство на другом конце не узнает и продолжит посылать трафик своему партнеру. Однако динамическое преобразование каналов связи будет обнаруживать отказавшие каналы связи и прекратит посылать трафик на другое устройство.

- **Повторное согласование**

  Если все порты на устройстве-партнере перестанут функционировать и/или отношение сигнал-шум (SNR) будет слишком высоким, LACP автоматически начнет искать другое устройство с поддержкой LACP в сети для формирования нового канала порта.

- **Режим ожидания**

  Если к группе агрегирования каналов связи добавляется большего количество портов, чем поддерживает устройство, протокол LACP автоматически переведет лишние порты в режим ожидания. Он определяет, какие порты перевести в режим ожидания, на основании критериев, определенных пользователем. Эти резервные порты будут ждать, пока не произойдет сбой активного порта, чтобы занять его место.

- **Проверка ссылок**

  При динамическом агрегировании каналов связи оба партнера могут взаимно проверять канал порта между ними, упрощая пользователям подтверждение конфигурации. При статическом агрегировании каналов связи такая проверка не выполняется.

Выбор между статическим и динамическим агрегированием каналов связи зависит от возможностей устройств, доступных в сети.

9.3.1.2 Правила и ограничения

При реализации агрегирования каналов связи необходимо учитывать следующие правила и ограничения:

- Порт может одновременно принадлежать только одной группе агрегирования каналов связи (LAG) или *транковой группе портов*.
- Зеркалируемый порт (порт назначения) не может принадлежать группе агрегирования каналов связи. А порт, который получает зеркалируемый трафик (исходный порт) — может.
- Если устройство поддерживает только один порт QinQ, работающий в режиме QinQ порт не может являться вторичным членом группы агрегирования каналов связи.
- Клиентский порт агента ретрансляции DHCP не может быть участником группы агрегирования каналов связи.
- Баланс загрузки между каналами группы является рандомизированным и может быть неидеальным. Например, если агрегировано три канала связи со скоростью передачи 100 Мбит/с, то результирующая пропускная способность группы агрегирования каналов связи может не быть в точности 300 Мбит/с.
- Статический MAC-адрес не должен конфигурироваться таким образом, чтобы он приходился на агрегированный порт — это может привести к отбрасыванию некоторых кадров, предназначенных для данного адреса.
- Защищенный порт не может быть участником транковой группы агрегирования каналов связи.
- Стандарт агрегации каналов связи IEEE 802.1AX (ранее IEEE 802.3ad) требует, чтобы все физические каналы связи в группе агрегирования каналов связи работали с одинаковой скоростью в полнодуплексном режиме. Если это требование нарушено, то производительность группы агрегирования каналов связи упадет.

  Коммутатор будет выдавать соответствующее оповещение при обнаружении такого несовпадения скорости/дуплексного режима.
- Протокол связующего дерева (STP) динамически рассчитывает стоимость пути группы агрегирования каналов связи на основании агрегированной пропускной способности. Однако, если агрегированные порты работают с разными скоростями, то стоимость пути не может быть вычислена правильно.
- Включенный протокол STP представляет собой наилучший способ поддерживать дублирование каналов связи в межкоммутаторных соединениях, состоящих из более чем одного физического канала связи. Если протокол STP разрешен, а увеличенная пропускная способность не требуется, то агрегацию каналов связи не стоит использовать, поскольку она обеспечивает большее время восстановления связи после отказа.

9.3.1.3 Агрегирование каналов связи и особенности 2-го уровня

Функции уровня 2 (например, STP, VLAN, CoS, фильтрация многоадресных рассылок) работают с группой агрегирования каналов связи как с единым каналом связи.

- Если протокол связующего дерева (STP) устанавливает статус агрегированного порта на `Blocking` или `Forwarding`, это выполняется для всей группы агрегирования каналов связи.
- Если один из агрегированных портов подписывается на групповую рассылку или отписывается от нее (например, через GMRP), то все остальные порты группы агрегирования каналов связи также подписываются или отписываются.
- Изменение параметра конфигурации любого порта (например, VLAN, CoS) будет автоматически применено ко всем портам группы агрегирования каналов связи.
- Параметры конфигурации/состояния вторичных портов не будут отображаться, а их номера портов будут просто перечисляться рядом с номером первичного порта в конфигурации/статусе соответствующих сеансов интерфейса пользователя.
- Когда вторичный порт добавляется в группу агрегирования каналов связи, он наследует все настройки конфигурации первичного порта. Когда вторичный порт удаляется из группы агрегирования каналов связи, восстанавливаются те настойки, которые он имел до агрегирования.

9.3.1.4 Агрегирование каналов связи и особенности физического уровня

Функции физического уровня (например, конфигурация физического канала связи, состояние соединения, ограничение скорости передачи, статистика Ethernet) будут продолжать работать с каждым агрегированным портом по-отдельности.

- Параметры физической конфигурации/состояния НЕ применяются автоматически к другим портам в группе агрегирования каналов связи и будут отображаться для каждого порта, как обычно.
- Убедитесь в том, что агрегированы только порты с одинаковыми настройками скорости и дуплексного режима. Если используется автоматическое согласование, то убедитесь в том, что оно приводит к одинаковой скорости передачи для всех портов в группе агрегирования каналов связи.
- Чтобы получить значение счетчика из статистики Ethernet для группы агрегирования каналов связи, просуммируйте значения счетчиков для всех портов группы агрегирования каналов связи.

9.3.2 Конфигурирование агрегирования каналов связи

Чтобы сконфигурировать статическое или динамическое агрегирование каналов связи, сделайте следующее:

1. Отключите или выключите каждый порт, подлежащий агрегированию. Для получения информации об отключении порта см. "Конфигурирование Ethernet-порта (Страница 76)".
2. Создайте одну или несколько групп агрегирования каналов связи (LAG) из двух или более портов. Для получения дополнительной информации см. "Добавление группы агрегирования каналов связи (Страница 268)".
3. Подключите или включите каждый порт в LAG. Для получения информации о включении порта см. "Конфигурирование Ethernet-порта (Страница 76)".
4. Если требуется динамическое агрегирование каналов связи, необходимо сконфигурировать настройки LACP глобально и для каждого порта. Для получения дополнительной информации см. "Конфигурирование глобальных настроек LACP (Страница 272)" и "Конфигурирование LACP на каждом порте (Страница 272)".
5. Повторите шаги с Шаг 1 до Шаг 4 для соседнего устройства, обладающего теми же возможностями (скорость порта, тип среды передачи и т. д.), обязательно руководствуясь сведениями в пользовательской документацией к устройству.

9.3.3 Управление группами агрегирования каналов связи

RUGGEDCOM ROS позволяет конфигурировать на одном устройстве до 15 групп агрегирования каналов связи (LAG) или *транковых групп портов*, каждая из которых может включать до восьми портов.

Примечание
Избегайте конфигурирования групп агрегирования каналов связи, если включена коммутация 3-го уровня. Для получения дополнительной информации о включении и выключении коммутации 3-го уровня см. "*Уровень 3* (Страница 199)".

Примечание
Максимальное количество групп агрегирования каналов связи для каждого устройства зависит от количества доступных портов. Для конфигурирования группы агрегирования каналов связи требуется не менее двух портов.

Примечание
Агрегированный порт с наименьшим номером порта называется *первичным* портом. Другие порты группы агрегирования каналов связи называются *вторичными* портами.

9.3.3.1 Просмотр списка групп агрегирования каналов связи

Чтобы просмотреть группы агрегирования каналов связи (LAG) или *транковые группы портов*, сконфигурированные на устройстве, перейдите в ***Link Aggregation » Configure Port Trunks***. Появится таблица **Port Trunks**.

Добавьте необходимые группы агрегирования каналов связи, если они не были сконфигурированы. Для получения дополнительной информации см. "Добавление группы агрегирования каналов связи (Страница 268)".

9.3.3.2 Добавление группы агрегирования каналов связи

Чтобы добавить группу агрегирования каналов связи (LAG) или *транковую группу портов*, сделайте следующее:

⚠ ЗАМЕТКА

Опасность для конфигурации — риск нарушения обмена данными

Группа агрегирования каналов связи должна быть надлежащим образом сконфигурирована на обеих сторонах канала порта. В межкоммутаторных соединениях, если конфигурация обеих сторон не совпадает (то есть некоторые порты по ошибке не включены в транковую группу портов), это приведет к возникновению петли. Поэтому для конфигурирования группы агрегирования каналов связи настоятельно рекомендуется следующая процедура:

1. Отсоедините или выключите в настройках все порты, участвующие в конфигурировании, то есть добавляемые в группу агрегирования каналов связи или удаляемые из нее.
2. Сконфигурируйте группу агрегирования каналов связи на обоих коммутаторах.
3. Перепроверьте конфигурацию группы агрегирования каналов связи портов на обоих коммутаторах.
4. Снова подсоедините или включите порты.

Если группа агрегирования каналов связи портов конфигурируется при неотсоединенных или неотключенных портах, то порт будет автоматически отключен на несколько секунд.

Примечание
Убедитесь в том, что агрегированы только порты с одинаковыми настройками скорости и дуплексного режима. Если используется автоматическое согласование, то убедитесь в том, что оно приводит к одинаковой скорости передачи для всех портов в группе агрегирования каналов связи.

1. Перейдите в ***Link Aggregation » Configure Port Trunks***. Появится таблица **Port Trunks**.
2. Нажмите **InsertRecord**. Появится форма **Port Trunks**.

3. Необходимо сконфигурировать следующие параметры:

Параметр	Описание
`Trunk ID`	**Краткий обзор:** Целое число от 1 до 5 **Значение по умолчанию:** 1 Идентификатор для группы агрегирования каналов связи (LAG) или транковой группы портов.
`Trunk Name`	**Краткий обзор:** Строка длиной 19 символа(ов) Имя для группы агрегирования каналов связи (LAG) или транковой группы портов. По возможности указывайте подробности, определяющие цель агрегированных каналов.
`Mode`	**Краткий обзор:** [LACP | Static] **Значение по умолчанию:** Static Определяет, как выполняется агрегирование каналов. Опции включают: • `LACP` - Агрегирование каналов осуществляется динамически с использованием LACP для обоих партнеров по агрегированию каналов. • `Static (Статический)` - Настройки агрегирования каналов для обоих партнеров по агрегированию каналов конфигурируются вручную. LACP не используется.
`Ports`	Список с разделителями-запятыми или диапазон портов для агрегирования в группе агрегирования каналов (LAG) или транковой группе портов.

4. Нажмите **Apply**.

9.3.3.3 Удаление группы агрегирования каналов связи

Чтобы удалить группу агрегирования каналов связи (LAG) или *транковую группу портов*, сделайте следующее:

1. Перейдите в ***Link Aggregation » Configure Port Trunks***. Появится таблица **Port Trunks**.
2. Выберите необходимую группу агрегирования каналов связи из таблицы. Появится форма **Port Trunks**.
3. Нажмите **Delete**.

9.3.3.4 Просмотр состояния групп агрегирования каналов связи

Чтобы просмотреть состояние каждой группы агрегирования каналов связи (LAG) или *транковые группы портов*, сконфигурированные на устройстве, перейдите в ***Link Aggregation » View Port Trunk Statistics***. Появится таблица **Port Trunk Statistics**.

В таблице отображается следующая информация для каждой группы агрегирования каналов связи:

Параметр	Описание
`Trunk ID`	Идентификатор для группы агрегирования каналов связи (LAG) или транковой группы портов.
`Mode`	Режим агрегирования каналов. Опции включают: • `LACP` - Агрегирование каналов осуществляется динамически с использованием LACP для обоих партнеров по агрегированию каналов. • `Static (Статический)` - Настройки агрегирования каналов для обоих партнеров по агрегированию каналов конфигурируются вручную. LACP не используется.
`State`	Рабочее состояние для группы агрегирования каналов (LAG) или транковой группы портов.
`Ports Aggregated`	Список с разделителями-запятыми или диапазон портов, которые агрегируются и функционируют в группе агрегирования каналов (LAG) или транковой группе портов.

9.3.4 Управление протоколом управления агрегированием каналов связи

Протокол управления агрегированием каналов связи (LACP) позволяет устройствам с поддержкой LACP динамически определять возможности друг друга и автоматически создавать каналы портов на основании максимальной скорости порта и транкингового состояния. Возможности и конфигурацию каждого устройства не нужно явно контролировать, как в случае со статическим агрегированием каналов связи.

Возможности устройств с поддержкой LACP определяются через обмен блоками данных LACP (LACPDU). Блоки LACPDU изначально распределяются портами, сконфигурированными на выполнение LACP в режиме `Active`. Если эти блоки LAPDU получает соседнее устройство с поддержкой LACP, блок LACPDU возвращается, а оба устройства согласовывают создание канала порта. Создание канала происходит только в случае согласования возможностей каждого устройства.

Примечание
Избегайте конфигурирования LACP, если включена коммутация 3-го уровня. Для получения дополнительной информации о включении и выключении коммутации 3-го уровня см. "*Уровень 3* (Страница 199)".

⚠ ЗАМЕТКА

Как минимум у одного устройства с поддержкой LACP должен быть порт, сконфигурированный на выполнение LACP в режиме `Active`. Порты, сконфигурированные на работу в режиме `Passive`, участвуют в процессе согласования, но не будут его начинать.

Конфигурируйте порт LACP, когда параметр `Mode` для любой транковой группы портов установлен на `LACP`.

9.3.4.1 Просмотр информации о партнере LACP

Чтобы просмотреть сведения о системе партнера LACP, перейдите в ***Link Aggregation » View Partner LACP Information***. Появится таблица **Partner LACP Information**.

В этой таблице отображается следующая информация:

Параметр	Описание
`Port`	Номер порта.
`System Priority`	Приоритет системы LACP системы-партнера.
`System ID`	MAC-адрес системы-партнера.
`Port Priority`	Приоритет порта LACP системы-партнера.
`Port Number`	Номер порта LACP системы-партнера.
`Key`	Ключ LACP, назначенный порту-партнеру системой-партнером.
`State`	Рабочее состояние LACP порта-партнера. Состояние выражается в виде строки длиной восемь символов. Например: `ASAO----` Слева направо: каждый символ в строке имеет следующее значение: 1. Активность LACP: A=активный LACP, P=пассивный LACP 2. Тайм-аут LACP: S=короткий тайм-аут, L=длительный тайм-аут 3. Агрегирование: A=агрегируемый, I=индивидуальный 4. Синхронизация: S=синхронизировано, O=несинхронизировано 5. Сбор: C=собирающий, -=несобирающий 6. Распределение: D=распределяющий, -= нераспределяющий 7. По умолчанию: D= информация по умолчанию, -=полученная информация 8. Истечение срока действия: E=срок действия истек, -=срок действия не истек
`Version`	**Краткий обзор:** Целое число от 0 до 255 Номер версии пакетов LACP, отправленных системой-партнером.

9.3.4.2 Конфигурирование глобальных настроек LACP

Чтобы сконфигурировать глобальные настройки для протокола управления агрегированием каналов (LACP), сделайте следующее:

1. Перейдите в ***Link Aggregation » Configure Global LACP Parameters***. Появится форма **Global LACP Parameters**.
2. Необходимо сконфигурировать следующие параметры:

Параметр	Описание
`Bridge LACP Priority`	**Краткий обзор:** Целое число от 0 до 65535 **Значение по умолчанию:** 32768 Приоритет системы LACP. Это комбинируется с MAC-адресом устройства для формирования идентификатора системы LACP, который используется при согласовании с другими устройствами с поддержкой LACP.
`LAG Ports Selection Rule`	**Краткий обзор:** [ActivePartner | LinkSpeed | LinkPriority] **Значение по умолчанию:** ActivePartner Определяет порядок, в котором порты в группе агрегирования каналов (LAG) или транковой группе портов выбираются для агрегирования посредством LACP. Этот параметр применяется, когда порты в LAG подключены к двум или более другим LAG. Опции включают: • `ActivePartner` - Выбор портов в зависимости от того, когда активируются порты-партнеры. • `LinkSpeed` - Выбор портов в зависимости от скорости соединения. Порт с более высокой скоростью соединения имеет приоритет. • `LinkPriority` - Выбор портов в зависимости от приоритета соединения LACP. Порт с более высоким приоритетом соединения LACP имеет приоритет.

3. Нажмите **Apply**.

9.3.4.3 Конфигурирование LACP на каждом порте

Чтобы сконфигурировать глобальные настройки протокола управления агрегированием каналов (LACP) для конкретного канала, сделайте следующее:

1. Перейдите в ***Link Aggregation » Configure Port LACP Parameters***. Появится таблица **Port LACP Parameters**.
2. Выберите необходимый порт. Появится форма **Port LACP Parameters**.
3. Необходимо сконфигурировать следующие параметры:

Параметр	Описание
`Port`	**Краткий обзор:** 1 to maximum port number Номер порта.

Параметр	Описание
`Mode`	**Краткий обзор:** [Active | Passive] **Значение по умолчанию:** Passive Определяет режим LACP для порта. Опции включают: • `Active (Активный)` - Порт активно отправляет пакеты LACP, независимо от режима порта-партнера. • `Passive (Пассивный)` - Порт не отправляет пакеты LACP, если порт-партнер не находится в режиме Active (Активный). **Примечание** Для каждого физического канала в группе агрегирования каналов (LAG) или транковой группе портов один порт-партнер должен находиться в активном режиме.
`Timeout`	**Краткий обзор:** [Short | Long] **Значение по умолчанию:** Short Определяет время (в секундах) ожидания пакетов LACP от порта-партнера. Если пакет LACP не принимается в течение требуемого периода времени, информация о порте-партнере аннулируется. Опции включают: Опции включают: • `Короткий` - 3 с • `Длительный` - 90 с **Примечание** Настройка тайм-аута должна быть одинаковой для всех портов в группе агрегирования каналов (LAG) или транковой группе портов.
`Individual`	**Краткий обзор:** [False | True] **Значение по умолчанию:** False Включает или отключает индивидуальный режим для порта. Порты в индивидуальном режиме не могут агрегироваться в группе агрегирования каналов (LAG) или транковой группе портов.
`Priority`	**Краткий обзор:** Целое число от 0 до 65535 **Значение по умолчанию:** 32768 Приоритет порта LACP. Это комбинируется с номером порта для формирования идентификатора порта LACP. Приоритет порта учитывается при определении того, должен ли порт находиться в режиме ожидания.

4. Нажмите **Apply**.

9.3.4.4 Вывод диагностики LACP

Чтобы просмотреть статистику, собранную протоколом управления агрегированием каналов связи (LACP), перейдите в ***Link Aggregation » View Port LACP Statistics***. Появится таблица **Port LACP Statistics**.

В этой таблице отображается следующая информация:

Параметр	Описание
`Port`	Номер порта.
`Link`	Коммуникационный статус порта.
`State`	**Краткий обзор:** Целое число от 0 до 255 Рабочее состояние LACP порта. Состояние выражается в виде строки длиной восемь символов. Например: `ASAO----` Слева направо: каждый символ в строке имеет следующее значение: 1. Активность LACP: A=активный LACP, P=пассивный LACP 2. Тайм-аут LACP: S=короткий тайм-аут, L=длительный тайм-аут 3. Агрегирование: A=агрегируемый, I=индивидуальный 4. Синхронизация: S=синхронизировано, O=несинхронизировано 5. Сбор: C=собирающий, -=несобирающий 6. Распределение: D=распределяющий, -= нераспределяющий 7. По умолчанию: D= информация по умолчанию, -=полученная информация 8. Истечение срока действия: E=срок действия истек, -=срок действия не истек
`Tx`	Число пакетов LACP, переданных портом.
`Rx`	Количество пакетов LACP, успешно полученных портом.
`RxUnknown`	Количество неизвестных пакетов LACP, полученных портом.
`RxIllegal`	Количество недопустимых пакетов LACP, полученных портом.

9.3.5 Очистка статистики агрегирования каналов связи

Чтобы очистить статистику агрегирования каналов связи, сделайте следующее:

1. Перейдите в ***Link Aggregation » Clear Link Aggregation Statistics***. Появится форма **Clear Link Aggregation Statistics**.
2. Нажмите **Confirm**.

10 Управление траффиком и его классификация

Используйте подсистемы управления траффиком и его классификации для регулирования потока пакета данных к подключенным сетевым интерфейсам.

10.1 Управление классами сервиса

Классы обслуживания (CoS) позволяют ускорить передачу некоторых кадров и трафика порта по сравнению с другими кадрами и трафиком. CoS кадра можно установить на "нормальный", "средний", "высокий" или "критический". По умолчанию, за исключением управляющих кадров, RUGGEDCOM ROS принудительно устанавливает "нормальный" CoS для всего входящего трафика, получаемого без тега приоритета.

⚠ ЗАМЕТКА

Используйте самый высокий поддерживаемый CoS с осторожностью, поскольку он всегда используется коммутатором для обслуживания трафика управления сетью, например, сообщений BPDU протокола RSTP.

Если такой CoS используется для обычного сетевого трафика, то при резком возрастании трафика это может привести к потере некоторых кадров управления сетью, что, в свою очередь, может иметь результатом потерю связности в масштабах сети.

Процесс управления трафиком на основании CoS происходит в два этапа:

1. **Этап определения класса сервиса**

   На этапе определения класса сервиса приоритет CoS принятого кадра определяется на основании следующих данных:

   - специальный CoS, основанный на MAC-адресе источника и получателя (как указано в таблице статических MAC-адресов)
   - поле приоритета в тегах IEEE 802.1Q
   - компонент Differentiated Services Code Point (DSCP) поля типа обслуживания (TOS) в IP-заголовке, если это IP-кадр
   - CoS по умолчанию для данного порта

   CoS каждого кадра будет определен при обнаружении первого же анализируемого параметра в этом кадре.

   Примечание
   Для получения информации о том, как конфигурировать параметр **Inspect TOS**, см. "Конфигурирование классов сервиса для конкретных Ethernet-портов (Страница 277)".

   Сначала проверяется заголовок каждого получаемого кадра, чтобы определить является ли кадр IP-пакетом и включен ли параметр **Inspect TOS** в RUGGEDCOM ROS. Класс сервиса определяется по полю DSCP.

   Если кадр не является IP-пакетом или параметр **Inspect TOS** отключен, кадр проверяется на наличие MAC-адреса его пункта назначения или источника в таблице статических MAC-адресов. При положительном результате используется CoS, сконфигурированный для данного статического MAC-адреса. Если MAC-адрес пункта назначения или источника отсутствует в таблице статических MAC-адресов, то кадр далее анализируется на предмет тегов 802.1Q и CoS определяется по битам поля приоритета. Если тег отсутствует, используется CoS по умолчанию для данного порта.

   После определения класса сервиса кадр пересылается на выходной порт для передачи.

2. **Этап пересылки**

   После определения CoS кадра он пересылается на выходной порт, где попадает в одну из очередей с разным приоритетом, в соответствии с назначенным для кадра значением CoS.

   Весовые коэффициенты CoS служат для определения требуемого вида обработки, которая связана с различными очередями разного приоритета. Отношение числа передаваемых кадров с более высоким CoS к числу передаваемых кадров с меньшим CoS может конфигурироваться. Если требуется, то пользователь может задать передачу кадров с меньшим CoS только после обслуживания всех кадров с более высоким CoS.

10.1.1 Глобальное конфигурирование классов сервиса

Чтобы сконфигурировать глобальные настройки для классов сервиса (CoS), сделайте следующее:

1. Перейдите в ***Classes of Service » Configure Global CoS Parameters***. Появится форма **Global CoS Parameters**.
2. Необходимо сконфигурировать следующие параметры:

Параметр	Описание
`CoS Weighting`	**Краткий обзор:** [8:4:2:1 | Strict] **Значение по умолчанию:** 8:4:2:1 Во время резкого возрастания трафика кадры, помещаемые в очередь коммутатора в ожидании передачи в направлении определенного порта, могут иметь различные приоритеты CoS. Этим параметром определяется алгоритм, использующий весовые коэффициенты для передачи кадров с различным приоритетом CoS. Примеры: • `8:4:2:1` - 8 кадров с критическим, 4 кадра с высоким, 2 кадра со средним и 1 кадр с нормальным приоритетом CoS • `Строгое правило` - кадры с меньшим приоритетом CoS будут передаваться только после передачи всех кадров с более высоким приоритетом CoS

3. Нажмите **Apply**.
4. Если необходимо, конфигурируйте привязку CoS на основании приоритета IEEE 802.1p или поля дифференцированных служб (DS), настроенного в IP-заголовке для каждого пакета. Для получения дополнительной информации см. "Конфигурирование определения класса сервиса по битам приоритета (Страница 278)" или "Конфигурирование определения класса сервиса по битам приоритета DSCP (Страница 279)".

10.1.2 Конфигурирование классов сервиса для конкретных Ethernet-портов

Чтобы сконфигурировать классы сервисов (CoS) для одного или нескольких Ethernet-портов, сделайте следующее:

1. Перейдите в ***Classes of Service » Configure Port CoS Parameters***. Появится таблица **Port CoS Parameters**.
2. Выберите Ethernet-порт. Появится форма **Port CoS Parameters**.

3. Необходимо сконфигурировать следующие параметры:

Параметр	Описание
`Port(s)`	**Краткий обзор:** Any combination of numbers valid for this parameter Номер порта устройства (или список портов, если они объединены в группу).
`Default Pri`	**Краткий обзор:** Целое число от 0 до 7 **Значение по умолчанию:** 0 Этот параметр позволяет осуществлять приоритизацию принимаемых на данный порт кадров, которые не приоритизированы на основании содержимого кадра (например, поля приоритета в теге VLAN, поля DiffServ в IP-заголовке, MAC-адреса с назначенным приоритетом).
`Inspect TOS`	**Краткий обзор:** [No | Yes] **Значение по умолчанию:** No Этот параметр разрешает или запрещает анализ поля "тип сервиса" (TOS) в IP-заголовке принимаемых кадров, чтобы определить класс сервиса, который должен быть назначен. Если анализ поля TOS разрешен, то коммутатор будет использовать биты DSCP в поле TOS.

4. Нажмите **Apply**.

10.1.3 Конфигурирование определения класса сервиса по битам приоритета

Кадрам, полученным без тегов, может автоматически присваиваться класс сервиса (CoS) на основании их уровня приоритета.

Чтобы привязать уровень приоритета к CoS, сделайте следующее:

1. Перейдите в ***Classes of Service » Configure Priority to CoS Mapping***. Появится таблица **Priority to CoS Mapping**.
2. Выберите уровень приоритета. Появится форма **Priority to CoS Mapping**.
3. Необходимо сконфигурировать следующие параметры:

Параметр	Описание
`Priority`	**Краткий обзор:** Целое число от 0 до 7 **Значение по умолчанию:** 0 Значение приоритета в спецификации IEEE 802.1p.
`CoS`	**Краткий обзор:** [Normal | Medium | High | Crit] **Значение по умолчанию:** Normal Класс сервиса, назначаемый принятым тегированным кадрам с заданным значением приоритета IEEE 802.1p.

4. Нажмите **Apply**.

10.1.4 Конфигурирование определения класса сервиса по битам приоритета DSCP

Привязка CoS к полю дифференцированных сервисов (DS), установленному в IP-заголовке для каждого пакета, осуществляется путем определения кодовых точек дифференцированных сервисов (DSCP) в конфигурации CoS.

Чтобы привязать DSCP к классу сервиса, сделайте следующее:

1. Перейдите в ***Classes of Service » Configure DSCP to CoS Mapping***. Появится таблица **DSCP to CoS Mapping**.
2. Выберите уровень DSCP. Появится форма **DSCP to CoS Mapping**.
3. Необходимо сконфигурировать следующие параметры:

Параметр	Описание
DSCP	**Краткий обзор:** Целое число от 0 до 63 **Значение по умолчанию:** 0 Точка кода дифференцированных услуг (DSCP) — значение 6-разрядного поля DiffServ в поле "тип сервиса" (TOS) IP-заголовка.

4. Нажмите **Apply**.
5. При необходимости сконфигурируйте параметры CoS на выбранных коммутируемых Ethernet-портах. Для получения дополнительной информации см. "Конфигурирование классов сервиса для конкретных Ethernet-портов (Страница 277)".

11 Службы времени

В данном разделе рассматриваются функции измерения и синхронизации времени в RUGGEDCOM ROS.

11.1 Конфигурирование даты и времени

Чтобы установить время, дату и другие параметры, связанные с измерением времени, сделайте следующее:

1. Перейдите в ***Administration » System Time Manager » Configure Time and Date***. Появится форма **Time and Date**.
2. Необходимо сконфигурировать следующие параметры:

Параметр	Описание
`Time`	**Краткий обзор:** HH:MM:SS Этот параметр позволяет просматривать и устанавливать локальное время.
`Date`	**Краткий обзор:** MMM DD, YYYY Этот параметр позволяет просматривать и устанавливать локальную дату.
`Time Zone`	**Краткий обзор:** [UTC-12:00 (Eniwetok, Kwajalein) | UTC-11:00 (Midway Island, Samoa) | UTC-10:00 (Hawaii) | UTC-9:00 (Alaska) | UTC-8:00 (Los Angeles, Vancouver) | UTC-7:00 (Calgary, Denver) | UTC-6:00 (Chicago, Mexico City) | UTC-5:00 (New York, Toronto) | UTC-4:30 (Caracas) | UTC-4:00 (Santiago) | UTC-3:30 (Newfoundland) | UTC-3:00 (Brasilia, Buenos Aires) | UTC-2:00 (Mid Atlantic) | UTC-1:00 (Azores) | UTC-0:00 (Lisbon, London) | UTC+1:00 (Berlin, Paris, Rome) | UTC+2:00 (Athens, Cairo, Helsinki) | ...] **Значение по умолчанию:** UTC-5:00 (New York, Toronto) Эта настройка обеспечивает преобразование времени UTC (всемирное координированное время) в местное время.
`DST Offset`	**Краткий обзор:** HH:MM:SS **Значение по умолчанию:** 00:00:00 Этот параметр указывает, насколько сдвигается время вперед/назад при переходе на летнее время и на зимнее время. Например, для большинства штатов США и для Канады сдвиг летнего времени составляет 1 час (01:00:00) вперед при переходе на летнее время и 1 час назад при переходе на зимнее время.

Параметр	Описание
`DST Rule`	**Краткий обзор:** mm.n.d/HH:MM:SS mm.n.d/HH:MM:SS Этот параметр определяет правило изменения времени и даты, когда имеет место переход между стандартным и летним временем. • `mm` - месяц года (01 — январь, 12 — декабрь) • `n` - день месяца (1 — 1-й день, 5 — 5-й/последний день) • `d` - день недели (0 — воскресенье, 6 — суббота) • `HH` - час суток (0–24) • `MM` - минута часа (0–59) • `SS` - секунда минуты (0–59) Пример: следующее правило применимо для большинства штатов США и Канады: `03.2.0/02:00:00 11.1.0/02:00:00` Летнее время начинается во второе воскресенье марта в 2:00. Летнее время заканчивается в первое воскресенье ноября в 2:00.
`Current UTC Offset`	**Краткий обзор:** Целое число от 0 до 1000 **Значение по умолчанию:** 36 Всемирное координированное время (UTC) представляет собой стандартное время, основанное на Международном атомном времени (TAI), с прибавлением секунд координации через нерегулярные интервалы времени, чтобы компенсировать замедление вращения Земли. Параметр текущего сдвига времени UTC позволяет пользователю корректировать разницу между UTC и TAI. Международная служба наблюдения за вращением и координатами Земли (IERS) наблюдает вращение Земли и приблизительно за шесть месяцев (в январе и июле) рассылает информационное сообщение Bulletin-C, в котором уведомляет о том, следует ли прибавлять секунду координации в конце июня и декабря. Имейте в виду, что изменение параметра текущего сдвига времени UTC приведет к временному нарушению в синхронизирующей сети.
`Leap Second Pending`	**Краткий обзор:** [No | Yes] **Значение по умолчанию:** No Этот параметр позволяет пользователю управлять событием прибавления секунд координации. Секунда координации представляет собой одну секунду, которая прибавляется к всемирному координированному времени (UTC), чтобы сохранить его синхронизацию с астрономическим временем. Международная служба наблюдения за вращением и координатами Земли (IERS) наблюдает вращение Земли и приблизительно за шесть месяцев (в январе и июле) рассылает информационное сообщение Bulletin-C, в котором уведомляет о том, следует ли прибавлять секунду координации в конце июня и декабря. Этот параметр должен быть определен не менее

Параметр	Описание
	чем за 5 минут до возникновения события, связанного с прибавлением секунды координации.

11.2 Управление протоколом точного времени (PTP)

Протокол точного времени (PTP) является стандартным методом синхронизации сетевых часов через Ethernet. RUGGEDCOM ROS поддерживает PTP v2, который определяется рабочей группой IEEE 1588 в стандарте IEEE 1588-2008.

PTP представляет собой распределенный протокол, который позволяет синхронизироваться друг с другом множеству часов в сети. Эти часы организованы в иерархию синхронизации ведущее-ведомое устройство, с *главными ведущими* часами на вершине иерархии, которые определяют эталонное время для всей системы. Синхронизация обеспечивается за счет обмена синхронизирующими PTP-сообщениями. *Ведомые* часы используют информацию о времени в PTP-сообщениях для коррекции своего внутреннего времени по времени *ведущего* устройства в своей части иерархии.

Протокол PTP поддерживается в пределах логической области под названием *домен*. Время, установленное через этот протокол в пределах одного домена, не зависит от времени в других доменах.

Система с протоколом PTP версии 2 может состоять из комбинации устройств, изменяющих проходящие PTP-сообщения и не изменяющих проходящего трафика PTP. В стандарте IEEE 1588-2008 определено пять основных типов PTP-устройств.

- Обычные часы
- Граничные часы
- Прозрачные часы с измерением сквозной задержки из конца в конец
- Прозрачные часы с измерением задержки между соседними узлами
- Администрирующие узлы

RUGGEDCOM ROS поддерживает режимы *прозрачных часов с измерением задержки между узлами* и *прозрачных часов с измерением сквозной задержки*:

- *Прозрачные часы с измерением задержки между узлами* транслируют все сообщения в точности так, как это делает обычный мост, маршрутизатор или репитер. Различие состоит в том, что прозрачные часы с измерением задержки между узлами также вычисляют продолжительность пребывания в коммутаторе (время отправки сообщения — время прибытия сообщения) и задержку канала связи (задержка распространения пакета между портами узлов сети) и добавляют эту информацию в PTP-сообщения о событиях (сообщения, которые несут в себе отметку времени). Ethernet-порты на прозрачных часах с измерением задержки между узлами

используют механизм измерения задержки между узлами для вычисления задержки распространения пакета между портами узлов сети.

- *Прозрачные часы измерением сквозной задержки* поддерживают использование механизма измерения сквозной задержки при передаче сигнала между ведомыми часами и ведущими часами. Они транслируют все сообщения в точности так, как это делает обычный мост, маршрутизатор или репитер. Различие состоит в том, что прозрачные часы с измерением сквозной задержки также вычисляют продолжительность пребывания в коммутаторе (время отправки сообщения — время прибытия сообщения) и добавляют эту информацию в PTP-сообщения о событиях (сообщения, которые несут в себе отметку времени).

11.2.1 Глобальное конфигурирование протокола PTP

Чтобы сконфигурировать глобальные настройки для PTP, сделайте следующее:

1. Перейдите в ***Administration » System Time Manager » Precision Time Protocol » Configure Global Parameters***. Появится форма **Global Parameters**.

> ⚠ **ЗАМЕТКА**
>
> Перед выполнением операций SNMP get или SNMP set для баз MIB IEEE C37.238-2011 и RUGGEDCOM-PTP1588-MIB.mib необходимо убедиться, что параметр "PTP Enable" установлен в *Да*. Для получения дополнительной информации о поддерживаемых базах MIB см. "Поддержка базы интерфейса управления (MIB) SNMP (Страница 298)".

2. Необходимо сконфигурировать следующие параметры:

Параметр	Описание
`PTP Enable`	**Краткий обзор:** [No | Yes] **Значение по умолчанию:** No Активирует протокол PTP (протокол точного времени).
`Clock Type`	**Краткий обзор:** [P2P TClock | E2E TClock] **Значение по умолчанию:** P2P TClock Выбор типа часов PTP (протокола точного времени). Обратите внимание, что обычные часы станут ведущими часами (MC) или ведомыми часами (SC) при условии согласования сети. Однако, если в качестве источника времени выбран IRIGB или GPS, устройство будет либо согласовывать статус ведущего устройства и действовать как гроссмейстерские часы (GMC), либо оставаться в пассивном состоянии PTP. Позволяет настраивать атрибуты ведомых граничных часов (BClock) PTP.

Параметр	Описание
`PTP Profile`	**Краткий обзор:** [Power Profile | Default P2P Profile | Utility Profile Level 1 | Default E2E Profile | Custom Profile | Power Profile v2] **Значение по умолчанию:** Power Profile Выбор профиля часов PTP (протокола точного времени). Профиль PTP представляет набор допустимых функций PTP, применимых к конкретной отрасли. **Примечание** `Power Profile` представляет C37.238.2011. **Примечание** `Power Profile v2` представляет C37.238.2017. **Примечание** `Utility Profile Level 1` представляет МЭК/IEEE 61850-9-3 Ed.1.
`Ethernet Ports`	**Краткий обзор:** Comma-separated list of ports или [All] **Значение по умолчанию:** All Выбор Ethernet-портов, которые будут участвовать в обмене сообщениями по протоколу PTP (протокол точного времени).
`VLAN ID`	**Краткий обзор:** Целое число от 1 до 4094 или [Disable] **Значение по умолчанию:** 1 Идентификатор виртуальной локальной сети (VLAN), ассоциированной с нетегированными (и тегированными приоритетом 802.1p) кадрами, принимаемыми на этот порт. Кадры, тегированные ненулевым идентификатором VLAN, всегда будут ассоциированы с этим идентификатором VLAN, который извлекается из тега кадра. Кадры, тегированные нулевым идентификатором VLAN, всегда будут ассоциированы с идентификатором VLAN 1, пока этот параметр не будет сконфигурирован.
`Class Of Service`	**Краткий обзор:** Целое число от 1 до 7 или [Disable] **Значение по умолчанию:** 4 Выбор приоритета сообщений PTP (протокола точного времени) на основании спецификации IEEE 802.1p. IEEE 802.1p определяет восемь различных классов сервиса, обычно представляемых через 3-разрядное поле приоритета в заголовке IEEE 802.1Q, который добавляется к Ethernet-кадру. Если опция VLAN включена, а опция класса сервиса установлена на "Отключить", это соответствует приоритету "0" согласно спецификации IEEE 802.1p.
`Transport Protocol`	**Краткий обзор:** [Layer 2 Multicast | Layer 3 Multicast] **Значение по умолчанию:** Layer 2 Multicast Выбор сетевого транспортного протокола для сообщений PTP (протокола точного времени).

Параметр	Описание
`Grandmaster ID`	**Краткий обзор:** Целое число от 3 до 255 **Значение по умолчанию:** 255 Этот параметр является специальным для профиля Power Profile (IEEE C37.238-2011) или профиля Power Profile v2 (IEEE C37.238-2017), в зависимости от сделанного выбора. Для всех устройств, способных работать в режиме ведущего устройства PTP, должно быть сконфигурировано уникальное в масштабах сети значение этого параметра в интервале от 3 до 254, чтобы обеспечить корректное функционирование.

3. Нажмите **Apply**.
4. Перезапустите устройство. Для получения дополнительной информации см. "Перезапуск устройства (Страница 108)".

11.2.2 Конфигурирование прозрачных часов

Чтобы сконфигурировать настройки прозрачных часов PTP, сделайте следующее:

1. Перейдите в ***Administration » System Time Manager » Precision Time Protocol » Configure Clock Parameters***. Появится форма **Clock Parameters**.
2. Необходимо сконфигурировать следующие параметры:

Параметр	Описание
`Domain Number`	**Краткий обзор:** Целое число от 0 до 127 или [254] **Значение по умолчанию:** 0 Выбор номера домена PTP (протокола точного времени). PTP-домен — это логическая группа PTP-часов, которые синхронизируются друг с другом, используя протокол PTP.
`Path Delay Mechanism`	**Краткий обзор:** [Disabled | Peer-to-Peer | End-to-End] **Значение по умолчанию:** Peer-to-Peer Выбор функциональности механизма измерения задержки PTP (протокола точного времени). Существует два механизма, которые применяются в PTP для измерения задержки распространения сигнала между портами PTP: Механизм измерения задержки между узлами P2P измеряет время распространения сигнала от порта к порту, а именно: задержку канала связи и время прохождения кадра. Механизм P2P не зависит от того, является ли порт PTP ведущим или ведомым. Механизм измерения задержки E2E (с измерением сквозной задержки) измеряет время распространения сообщений между ведущими и ведомыми часами по всей промежуточной сети. Обратите внимание, что механизм измерения задержки между узлами не взаимодействует с измерениями задержки тракта, основанными на механизме измерения

Параметр	Описание
	задержки E2E (который также имеет название "запрос-ответ").

3. Нажмите **Apply**.
4. Перезапустите устройство. Для получения дополнительной информации см. "Перезапуск устройства (Страница 108)".

11.2.3 Конфигурирование интервала запросов задержки протокола PTP

Чтобы сконфигурировать интервал запросов задержки PTP, сделайте следующее:

1. Перейдите в ***Administration » System Time Manager » Precision Time Protocol » Configure Path Delay***. Появится форма **Path Delay**.
2. Необходимо сконфигурировать следующие параметры:

Параметр	Описание
`P2P Request Interval`	**Краткий обзор:** [1 s | 2 s | 4 s | 8 s | 16 s | 32 s] **Значение по умолчанию:** 1 s Выбор интервала запроса задержки PTP (усредненный интервал времени между следующими друг за другом сообщениями с запросом задержки) в секундах. Механизм измерения задержки между узлами измеряет время распространения сигнала от порта к порту, а именно: задержку канала связи, между двумя взаимодействующими портами, которые поддерживают механизм измерения задержки между узлами.
`E2E Request Interval`	**Краткий обзор:** [1 s | 2 s | 4 s | 8 s | 16 s | 32 s] **Значение по умолчанию:** 1 s Выбор интервала запроса задержки PTP (усредненный интервал времени между следующими друг за другом сообщениями с запросом задержки) в секундах. Механизм измерения задержки E2E (также имеет название "запрос-ответ") измеряет время распространения сообщений между ведущими и ведомыми часами.

3. Нажмите **Apply**.
4. Перезапустите устройство. Для получения дополнительной информации см. "Перезапуск устройства (Страница 108)".

11.2.4 Вывод диагностики часов PTP

Чтобы просмотреть статистику для часов протокола точного времени (PTP), перейдите в ***Administration » System Time Manager » Precision Time Protocol » View PTP Statistics » View PTP Clock Stats***. Появится форма **PTP Clock Stats**.

В этой форме отображается следующая информация:

Примечание
Доступность параметров зависит от статуса устройства.

Параметр	Описание
`Status`	**Краткий обзор:** Строка длиной 31 символа(ов) Показывает статус узла PTP (протокола точного времени). Если устройство сконфигурировано в качестве обычных часов, то в этом поле отображается статус состояния PTP, а именно: ВЕДУЩЕЕ УСТРОЙСТВО, ВЕДОМОЕ УСТРОЙСТВО или ПРОСЛУШИВАЮЩЕЕ УСТРОЙСТВО. Если устройство сконфигурировано в качестве прозрачных часов, то в этом поле указаны настройки конфигурации.

11.2.5 Вывод диагностики задержки между узлами

Чтобы просмотреть статистику задержки между узлами протокола точного времени (PTP), сделайте следующее:

1. Перейдите в ***Administration » System Time Manager » Precision Time Protocol » View PTP Statistics » View Peer Delay Stats***. Появится таблица **PTP Delay Stats**.
2. Выберите Ethernet-порт. Появится форма **PTP Delay Stats**.

В этой таблице отображается следующая информация:

Параметр	Описание
`Port`	**Краткий обзор:** 1 to maximum port number Номер порта.
`State`	**Краткий обзор:** [On | Off] Показывает статус PTP-порта с точки зрения механизма измерения задержки P2P (между узлами).
`PeerDelay`	**Краткий обзор:** Целое число от 0 до 2147483647 Показывает задержку между узлами в наносекундах. Механизм измерения задержки между узлами измеряет время распространения сигнала от порта к порту, а именно: задержку канала связи, между двумя взаимодействующими портами, которые поддерживают механизм измерения задержки между узлами.

11.3 Конфигурирование источника времени

Чтобы сконфигурировать ссылочный источник времени, который будет использоваться устройством для локальных часов и для всех выходных данных синхронизации времени, сделайте следующее:

1. Перейдите в ***Administration » System Time Manager » Configure Time Source***. Появится форма **Time Source**.
2. Необходимо сконфигурировать следующие параметры:

Параметр	Описание
`Primary Time Source`	**Краткий обзор:** [LOCAL CLK | NTP Server] **Значение по умолчанию:** LOCAL CLK Служит для выбора источника времени, от которого будут синхронизироваться локальные часы. Обратите внимание, что выбор нового источника времени вызовет скачкообразное изменение показаний локальных часов, наблюдаемое на любых выходах точного времени.

3. Нажмите **Apply**.

11.4 Управление NTP

RUGGEDCOM ROS может быть настроена таким образом, чтобы производилось периодическое обращение к заданному NTP-серверу для коррекции накопившегося отклонения показаний внутренних часов. RUGGEDCOM ROS также будет передавать время через простой протокол сетевого времени (SNTP) на хосты, которые запросят его.

Для устройства можно настроить два сервера NTP (первичный и резервный). При каждой попытке обновить системное время сначала производится обращение к первичному серверу. Если первичный сервер не отвечает, то производится обращение к резервному серверу. Если первичный или резервный сервер не отвечает, то инициируется оповещение.

11.4.1 Включение/отключение службы NTP

Чтобы включить или отключить службу NTP, сделайте следующее:

Примечание
Если устройство работает в качестве сервера NTP, служба NTP должна быть включена.

1. Перейдите в ***Administration » System Time Manager » Configure NTP » Configure NTP Service***. Появится форма **SNTP Parameters**.
2. Выберите **Enabled** для включения SNTP или **Disabled** — для отключения.
3. Нажмите **Apply**.

11.4.2 Конфигурирование серверов NTP

Чтобы сконфигурировать первичный или резервный сервер NTP, сделайте следующее:

1. Перейдите в ***Administration » System Time Manager » Configure NTP » Configure NTP Servers***. Появится таблица **NTP Servers**.
2. Выберите **Primary** или **Backup**. Появится форма **NTP Servers**.
3. Необходимо сконфигурировать следующие параметры:

Параметр	Описание
`Server`	**Краткий обзор:** Строка длиной 8 символа(ов) **Значение по умолчанию:** Primary Это поле указывает, предназначена ли данная настройка для первичного или для резервного сервера.
`IP Address`	**Краткий обзор:** Any valid IP address IP-адрес сервера.
`Reachable`	**Краткий обзор:** [No | Yes] Статус сервера.
`Update Period`	**Краткий обзор:** Целое число от 1 до 1440 **Значение по умолчанию:** 60 Эта настройка определяет, насколько часто (S)NTP-сервер опрашивается для обновления времени. Если сервер недоступен, то производятся три попытки с одноминутными интервалами, а затем генерируется оповещение.

4. Нажмите **Apply**.

11.5 Просмотр состояния подсистемы синхронизации времени

Чтобы просмотреть текущее состояние каждой подсистемы временной синхронизации, перейдите в ***Administration » System Time Manager » View Time Sync Status***. Появится форма **Time Sync Status**. Эта форма меняется в зависимости от сконфигурированного источника времени.

В этой таблице отображается следующая информация:

Параметр	Описание
`Time Source`	**Краткий обзор:** [LOCAL CLK | IRIGB | IEEE1588 | NTP Server | GPS] Источник времени, который управляет локальными часами.
`Frequency Adjustment`	**Краткий обзор:** Целое число от -2147483647 до 2147483646 Показывает текущий уровень дисциплины, применяемый к локальной эталонной частоте (TCXO), т. е. объем корректировки в данной системе, необходимый для синхронизации с текущим эталонным значением.

Исследование сетевого окружения и управление сетью

12

Для автоматического исследования топологии сети и сетевого окружения, а также для управления сетевыми устройствами и их мониторинга RUGGEDCOM ROS поддерживает следующие протоколы:

- **Протокол обнаружения RUGGEDCOM (RCDP)**

  Протокол RCPD используется для обнаружения устройств под управлением RUGGEDCOM ROS в коммутируемой сети уровня 2.

- **Протокол обнаружения канального уровня (LLDP)**

  Протокол LLDP используется для рассылки характеристик и настроек устройства на соседствующие в сети устройства, а также для получения рассылаемых соседними устройствами характеристик и настроек.

- **Простой протокол сетевого управления (SNMP)**

  Протокол SNMP используется для отправки выбранным пользователям или группам уведомлений об определенных событиях, произошедших во время работы, например, об изменениях в сетевой топологии, состоянии канала связи, корень связующего дерева и т. д.

12.1 Включение/отключение RCDP

RUGGEDCOM ROS поддерживает протокол обнаружения RUGGEDCOM (RCDP). RCDP обеспечивает ввод в эксплуатацию устройств на базе RUGGEDCOM ROS, которые не были индивидуально настроены с момента отгрузки с завода. Все устройства RUGGEDCOM ROS, в фабричных настройках, имеют один и тот же IP-адрес (уровня 3) по умолчанию. Подключение более чем одного такого устройства к сети с коммутацией уровня 2 означает, что для их настройки и управления невозможно будет использовать стандартные средства конфигурирования на базе IP. Поведение таких IP механизмов как веб-интерфейс, SSH, telnet или SNMP непредсказуемо.

Поскольку RCDP функционирует на уровне 2, его можно применять для надежной и однозначной адресации множества устройств, даже на всех этих устройствах настроен один и тот же IP-адрес.

RUGGEDCOM EXPLORER компании Siemens представляет собой простое, самостоятельное приложение Windows, поддерживающее протокол RCDP. Оно способно выполнять через RCDP обнаружение, идентификацию и базовую настройку устройств под управлением RUGGEDCOM ROS. Протокол RCDP поддерживает следующие функции:

- обнаружение устройств под управлением RUGGEDCOM ROS в коммутируемой сети уровня 2;
- получение данных по конфигурации первичной сети, версии RUGGEDCOM ROS, артикулу и серийному номеру;
- управление светодиодными индикаторами устройства для облегчения его физической идентификации;
- настройка основных идентификационных, сетевых и аутентификационных параметров.

Из соображений безопасности приложение RUGGEDCOM EXPLORER попытается отключить протокол RCDP или переведет все устройства в режим *Только прием* при закрытии этого приложения.

Кроме того, RUGGEDCOM EXPLORER настроит все устройства на режим *Только прием* при выполнении следующих условий:

- 60 минут с момента получения последнего кадра RCDP;
- IP-адрес, подсеть, шлюз или один из паролей устройства изменены через SSH, RSH, Telnet, последовательную консоль или SNMP.

⚠ ЗАМЕТКА

Для повышения безопасности Siemens рекомендует отключить RCDP, если его использование не предполагается.

Примечание
Протокол RCDP несовместим с сетевыми конфигурациями на основе виртуальных локальных сетей (VLAN). Для корректной работы приложения RUGGEDCOM EXPLORER не должны быть сконфигурированы никакие сети VLAN (тегированные или нетегированные) Все элементы конфигурации VLAN должны иметь настройки по умолчанию.

Примечание
RUGGEDCOM ROS только отвечает на RCDP-запросы. Она ни при каких обстоятельствах не инициирует обмен данными при помощи протокола RCDP.

Чтобы включить или отключить протокол RCDP, сделайте следующее:

1. Перейдите в ***Network Discovery » RuggedCom Discovery Protocol » Configure RCDP Parameters***. Появится форма **RCDP Parameters**.

2. В **RCDP Discovery** выберите одну из следующих опций:

⚠ **ЗАМЕТКА**
Опция `Enabled` доступна только для устройств с загруженными заводскими настройками по умолчанию. Эта опция не будет выбрана после того, как устройство будет сконфигурировано.

   - `Disabled` — отключает доступ для чтения и записи
   - `Get Only` — включает только доступ для чтения
   - `Enabled` — включает доступ для чтения и записи
3. Нажмите **Apply**.

12.2 Управление LLDP

Протокол обнаружения канального уровня (LLDP), определенный IEEE 802.11AB, позволяет сетевому устройству производить рассылку собственных базовых сетевых возможностей и конфигурации.

Протокол LLDP позволяет сетевому устройству получать информацию о соседних устройствах через подключенные сетевые каналы связи, используя стандартный механизм. Устройства, поддерживающие протокол LLDP, способны сообщать информацию о себе, включая их возможности, конфигурацию, межсоединения, а также идентификационную информацию.

Функционирование агента LLDP обычно реализовано в виде двух модулей: модуля передачи LLDP и модуля приема LLDP. Модуль передачи LLDP, находящийся в активном состоянии, передает информацию о локальном устройстве через регулярные интервалы времени в формате стандарта IEEE 802.1AB. Если модуль передачи неактивен, то он передает LLDPDU (сообщение LLDP) с параметром времени жизни (TTL), в котором информационное поле атрибута "тип, длина, значение" (TLV) содержит "0". Это позволяет удаленным устройствам исключать из своих баз данных информацию, связанную с данным локальным устройством. Модуль приема LLDP, находящийся в активном состоянии, принимает информацию об удаленных устройствах и обновляет свою базу данных LLDP по удаленным системам. Когда принимается новая или обновленная информация, модуль приема запускает таймер на период времени актуальности этой информации, указанный в атрибуте TTL TLV принятого LLDPDU. Информация об удаленной системе исключается из базы данных, когда от этой системе принят LLDPDU с атрибутом TTL TLV, содержащим значение "0" в своем поле информации.

Примечание
Протокол LLDP реализован таким образом, чтобы регистрировать только одно устройство на один порт Ethernet. Таким образом, при наличии нескольких устройств, посылающих информацию LLDP на порт коммутатора, на котором активен протокол LLDP, информация о соседнем устройстве для этого порта будет постоянно изменяться.

12.2.1 Глобальное конфигурирование LLDP

Чтобы сконфигурировать глобальные настройки для LLDP, сделайте следующее:

1. Перейдите в ***Network Discovery » Link Layer Discovery Protocol » Configure Global LLDP Parameters***. Появится форма **Global LLDP Parameters**.
2. Необходимо сконфигурировать следующие параметры:

Параметр	Описание
`State`	**Краткий обзор:** [Disabled | Enabled] **Значение по умолчанию:** Enabled Активирует протокол LLDP. Обратите внимание, что протокол LLDP активен для того или иного пор-та, когда LLDP активизирован глобально наряду с настройками для отдельного порта в меню "LLDP-параметры порта".
`Tx Interval`	**Краткий обзор:** Целое число от 5 до 32768 **Значение по умолчанию:** 30 Интервал, через который кадры LLDP передаются от имени этого агента LLDP.
`Tx Hold`	**Краткий обзор:** Целое число от 2 до 10 **Значение по умолчанию:** 4 Значение этого параметра, будучи умноженным на параметр Tx Interval, определяет время жизни (TTL) сообщения LLDPDU, то есть время, в течение которого хранится информация, полученная о соседнем устройстве. Фактическое значение TTL можно выразить с помощью следующей формулы: `TTL = MIN(65535, (Tx Interval * Tx Hold)`
`Reinit Delay`	**Краткий обзор:** Целое число от 1 до 10 **Значение по умолчанию:** 2 Задержка в секундах, с того момента как параметр Admin Status (административный статус) конкретного порта приобретает значение "отключено" и до попытки повторной инициализации.
`Tx Delay`	**Краткий обзор:** Целое число от 1 до 8192 **Значение по умолчанию:** 2 Задержка в секундах между последовательными передачами кадра LLDP, которые инициируются изменением значения или статуса. Рекомендуемое значение вычисляется по следующей формуле: `1 <= txDelay <= (0.25 * Tx Interval)`

3. Нажмите **Apply**.

12.2.2 Конфигурирование LLDP для Ethernet-порта

Чтобы сконфигурировать LLDP для конкретного Ethernet-порта, сделайте следующее:

1. Перейдите в ***Network Discovery » Link Layer Discovery Protocol » Configure Port LLDP Parameters***. Появится таблица **Port LLDP Parameters**.
2. Выберите порт. Появится форма **Port LLDP Parameters**.
3. Необходимо сконфигурировать следующие параметры:

Параметр	Описание
`Port`	**Краткий обзор:** 1 to maximum port number **Значение по умолчанию:** 1 Номер порта.
`Admin Status`	**Краткий обзор:** [rxTx | txOnly | rxOnly | Disabled] **Значение по умолчанию:** rxTx rxTx: локальный агент LLDP может передавать и принимать кадры LLDP через порт. txOnly: локальный агент LLDP может только передавать кадры LLDP. rxOnly: локальный агент LLDP может только принимать кадры LLDP. disabled: локальный агент LLDP не может ни передавать, ни принимать кадры LLDP.
`Notifications`	**Краткий обзор:** [Disabled | Enabled] **Значение по умолчанию:** Disabled Отключение уведомлений предотвратит отправку уведомлений и генерирование оповещений для конкретного порта или от агента LLDP.

4. Нажмите **Apply**.

12.2.3 Вывод глобальной диагностики и рассылаемой системной информации

Чтобы просмотреть глобальную статистику для LLDP и системную информацию, которая рассылается соседним сетевым устройствам, перейдите в ***Network Discovery » Link Layer Discovery Protocol » View LLDP Global Remote Statistics***. Появится форма **LLDP Global Remote Statistics**.

В этой форме отображается следующая информация:

Параметр	Описание
`Inserts`	**Краткий обзор:** Целое число от 0 до 4294967295 Число операций вставки записи в таблицу информации о соседних устройствах LLDP.

Параметр	Описание
`Deletes`	**Краткий обзор:** Целое число от 0 до 4294967295 Число операций удаления записи из таблицы информации о соседних устройствах LLDP.
`Drops`	**Краткий обзор:** Целое число от 0 до 4294967295 Число операций удаления записи из таблицы информации о соседних устройствах LLDP по причине истечения интервала времени актуальности данной информации.
`Ageouts`	**Краткий обзор:** Целое число от 0 до 4294967295 Количество всех отброшенных TLV.

12.2.4 Вывод диагностики для соседних устройств LLDP

Чтобы просмотреть статистику для соседних устройствах LLDP, перейдите в ***Network Discovery » Link Layer Discovery Protocol » View LLDP Neighbor Information***. Появится таблица **LLDP Neighbor Information**.

В этой форме отображается следующая информация:

Параметр	Описание
`Port`	**Краткий обзор:** 1 to maximum port number Локальный порт, связанный с этой записью.
`ChassisId`	**Краткий обзор:** Строка длиной 45 символа(ов) Информация об идентификаторе шасси, полученная от удаленного агента LLDP.
`PortId`	**Краткий обзор:** Строка длиной 45 символа(ов) Информация об идентификаторе порта, полученная от удаленного агента LLDP.
`SysName`	**Краткий обзор:** Строка длиной 45 символа(ов) Информация о системном имени, полученная от удаленного агента LLDP.
`SysDesc`	**Краткий обзор:** Строка длиной 45 символа(ов) Информация о системном дескрипторе, полученная от удаленного агента LLDP.

12.2.5 Вывод диагностики для портов LLDP

Чтобы просмотреть статистику для портов LLDP, перейдите в ***Network Discovery » Link Layer Discovery Protocol » View LLDP Statistics***. Появится таблица **LLDP Statistics**.

В этой таблице отображается следующая информация:

Параметр	Описание
`Port`	**Краткий обзор:** 1 to maximum port number Номер порта.
`FrmDrop`	**Краткий обзор:** Целое число от 0 до 4294967295 Количество всех отброшенных кадров LLDP.
`ErrFrm`	**Краткий обзор:** Целое число от 0 до 4294967295 Количество всех принятых сообщений LLDPDU с обнаружимыми ошибками.
`FrmIn`	**Краткий обзор:** Целое число от 0 до 4294967295 Количество всех принятых сообщений LLDPDU.
`FrmOut`	**Краткий обзор:** Целое число от 0 до 4294967295 Количество всех переданных сообщений LLDPDU.
`Ageouts`	**Краткий обзор:** Целое число от 0 до 4294967295 Число операций удаления информации о соседних устройствах из базы MIB удаленной системы LLDP из-за истечения времени таймера txinfoTTL.
`TLVsDrop`	**Краткий обзор:** Целое число от 0 до 4294967295 Количество всех отброшенных TLV.
`TLVsUnknown`	**Краткий обзор:** Целое число от 0 до 4294967295 Количество всех TLV, принятых на данный порт, которые не были распознаны локальным LLDP-агентом.

12.3 Управление SNMP

RUGGEDCOM ROS поддерживает версии 1, 2 и 3 простого протокола сетевого управления (SNMP), иначе именуемые SNMPv1, SNMPv2c и SNMPv3 соответственно. SNMPv3 обеспечивает безопасный доступ к устройствам посредством сочетания аутентификации и шифрования пакетов по сети. Функции безопасности для этого протокола включают:

Функция	Описание
Целостность сообщений	Удостоверяет, что пакет не был изменен во время передачи.
Аутентификация	Определяет, получено ли сообщение из допустимого источника.
Шифрование	Шифрует содержимое пакета, чтобы предотвратить его просмотр несанкционированным источником.

SNMPv3 обеспечивает модели безопасности и уровни безопасности. Модель безопасности — это настройка стратегии аутентификации для пользователя и группы, в которой он находится. Уровень безопасности — это допустимый уровень безопасности в модели безопасности. Комбинация модели безопасности и уровня определяет, какой механизм безопасности используется при обработке пакета SNMP.

Перед конфигурированием SNMPv3 обратите внимание на следующее:

- Каждый пользователь принадлежит к группе
- Группа определяет политику доступа для определенной группы пользователей
- Политика доступа определяет, к каким объектам SNMP можно получить доступ (например, чтение, запись и создание уведомлений)
- Группа определяет список уведомлений, которые могут получать ее пользователи
- Группа также определяет модель безопасности и уровень безопасности для своих пользователей

Для SNMPv1 и SNMPv2c может быть сконфигурирована строка сообщества. Строка сопоставляется с группой и уровнем доступа с помощью имени безопасности, которое конфигурируется как **User Name**.

12.3.1 Поддержка базы интерфейса управления (MIB) SNMP

RUGGEDCOM ROS поддерживает различные стандартные базы MIB, проприетарные базы RUGGEDCOM MIB и базы MIB возможностей агента для простого протокола сетевого управления (SNMP).

12.3.1.1 Поддерживаемые стандартные MIB

RUGGEDCOM ROS поддерживает следующие стандартные базы MIB:

⚠ ЗАМЕТКА

В этом разделе перечислены все базы MIB, поддерживаемые RUGGEDCOM ROS, и он приводится исключительно в качестве справочной информации. Поддержка отдельных устройств может отличаться.

- **BRIDGE-MIB**

  Для получения дополнительной информации см. "BRIDGE-MIB".
- **IEC-62439-3-MIB**

  Для получения дополнительной информации см. "IEC-62439-3-MIB".
- **IEEEC37-238-MIB**

  Для получения дополнительной информации см. "IEEEC37-238-MIB".
- **IF-MIB**

  Для получения дополнительной информации см. "IF-MIB".
- **IP-MIB**

  Для получения дополнительной информации см. "IP-MIB".

- **LLDP-MIB**

  Для получения дополнительной информации см. "LLDP-MIB".
- **Q-BRIDGE-MIB**

  Для получения дополнительной информации см. "Q-BRIDGE-MIB".
- **RMON-MIB**

  Для получения дополнительной информации см. "RMON-MIB".
- **RS-232-MIB**

  Для получения дополнительной информации см. "RS-232-MIB".
- **RSTP-MIB**

  Для получения дополнительной информации см. "RSTP-MIB".
- **SNMP-FRAMEWORK-MIB**

  Для получения дополнительной информации см. "SNMP-FRAMEWORK-MIB".
- **SNMP-USER-BASED-SM-MIB**

  Для получения дополнительной информации см. "SNMP-USER-BASED-SM-MIB".
- **SNMPv2-MIB**

  Для получения дополнительной информации см. "SNMPv2-MIB".
- **SNMP-VIEW-BASED-ACM-MIB**

  Для получения дополнительной информации см. "SNMP-VIEW-BASED-ACM-MIB".
- **TCP-MIB**

  Для получения дополнительной информации см. "TCP-MIB".
- **UDP-MIB**

  Для получения дополнительной информации см. "UDP-MIB".

BRIDGE-MIB

Группа/Объект	Описание
Группа: dot1dBaseBridgeGroup **Объект:** dot1dBaseBridgeAddress	**Доступ:** Только для чтения **Синтаксическая структура:** Hex-String **Идентификатор объекта:** .1.3.6.1.2.1.17.1.1.0 **Определение:** MAC-адрес, используемый мостом в тех случаях, когда требуется обеспечить однозначность. Рекомендуется использовать для этого численно меньшее значение MAC-адреса среди всех портов моста. Однако требуется лишь уникальность значения. При конкатенации с dot1dStpPriority образуется уникальное значение BridgeIdentifier, используемое в протоколе связующего дерева.
Группа: dot1dBaseBridgeGroup **Trap-уведомление:** dot1dBaseNumPorts	**Доступ:** Только для чтения **Синтаксическая структура:** Integer **Идентификатор объекта:** .1.3.6.1.2.1.17.1.2.0

Группа/Объект	Описание
	Определение: Число портов, контролируемых данным мостом.
Группа: dot1dBasePortGroup **Trap-уведомление:** dot1dBasePort	**Доступ:** Только для чтения **Синтаксическая структура:** Integer **Идентификатор объекта:** .1.3.6.1.2.1.17.1.4.1.1.1 **Определение:** Номер порта, для которого эта запись содержит данные управления мостом.
Группа: dot1dBasePortGroup **Trap-уведомление:** dot1dBasePortCircuit	**Доступ:** Только для чтения **Синтаксическая структура:** Идентификатор объекта **Идентификатор объекта:** .1.3.6.1.2.1.17.1.3.1 **Определение:** Для порта, который (потенциально) имеет такое же значение dot1dBasePortIfIndex как у другого порта в том же мосту. Этот объект содержит имя экземпляра объекта, уникальное для этого порта. Например, в случае когда множество портов, взаимно-однозначно соответствует виртуальным устройствам X.25, это значение может указывать (например, первый) экземпляр объекта, связанного с виртуальным устройством X.25, соответствующим этому порту. Для порта, имеющего уникальное значение dot1dBasePortIfIndex, этот объект имеет значение { 0 0 }.
Группа: dot1dBasePortGroup **Trap-уведомление:** dot1dBasePortDelayExceededDiscards	**Функционал агента:** RC-BRIDGE-MIB-AC **Доступ:** Только для чтения **Синтаксическая структура:** Counter32 **Идентификатор объекта:** .1.3.6.1.2.1.17.1.4.1.4.1 **Определение:** Число кадров, отброшенных этим портом по причине избыточной задержки при передаче через мост. Счетчик инкрементируется прозрачными мостами и мостами с маршрутизацией от источника. **Примечание** Коммутатору не известно значение этого объекта. В ответ на запрос GET будет возвращено нулевое значение.
Группа: dot1dBasePortGroup **Trap-уведомление:** dot1dBasePortIfIndex	**Доступ:** Только для чтения **Синтаксическая структура:** Integer **Идентификатор объекта:** .1.3.6.1.2.1.17.1.4.1.2.1 **Определение:** Значение экземпляра объекта ifIndex, определенного в IF-MIB, для соответствующего этому порту интерфейса.
Группа: dot1dBasePortGroup **Trap-уведомление:** dot1dBasePortMtuExceededDiscards	**Доступ:** Только для чтения **Синтаксическая структура:** Counter32 **Идентификатор объекта:** .1.3.6.1.2.1.17.1.4.1.5.1 **Определение:** Число кадров, отброшенных этим портом по причине избыточного размера. Счетчик инкрементируется прозрачными мостами и мостами с маршрутизацией от источника.
Группа: dot1dBaseBridgeGroup **Trap-уведомление:** dot1dBaseType	**Доступ:** Только для чтения **Синтаксическая структура:** Integer **Идентификатор объекта:** .1.3.6.1.2.1.17.1.3.0 **Определение:** Указывает, какой тип маршрутизации может выполнять этот мост. Если мост фактически выполняет определенный тип

Группа/Объект	Описание
	маршрутизации, это обозначается записями в таблице портов для данного типа.
Группа: dot1dStpBridgeGroup **Trap-уведомление:** dot1dStpBridgeForwardDelay	**Функционал агента:** RC-BRIDGE-MIB-AC **Доступ:** Для чтения и записи **Синтаксическая структура:** Integer **Идентификатор объекта:** .1.3.6.1.2.1.17.2.14.0 **Определение:** Значение, которое все мосты используют в качестве ForwardDelay, когда мост работает в качестве корневого. Отметим, что 802.1D-1998 задает привязку диапазона для этого параметра к значению параметра dot1dStpBridgeMaxAge. Дискретность для этого таймера установлена стандартом 802.1D-1998 в 1 сек. Агент может возвращать ошибку badValue при попытке установить нецелое число секунд. **Примечание** Значение этого объекта округляется до ближайшего числа десятых долей секунды.
Группа: dot1dStpBridgeGroup **Trap-уведомление:** dot1dStpBridgeHelloTime	**Функционал агента:** RC-BRIDGE-MIB-AC **Доступ:** Для чтения и записи **Синтаксическая структура:** Integer **Идентификатор объекта:** .1.3.6.1.2.1.17.2.13.0 **Определение:** Значение, которое все мосты используют в качестве HelloTime, когда мост работает в качестве корневого. Дискретность для этого таймера установлена стандартом 802.1D-1998 в 1 сек. Агент может возвращать ошибку badValue при попытке установить нецелое число секунд. **Примечание** Значение этого объекта округляется до ближайшего числа десятых долей секунды.
Группа: dot1dStpBridgeGroup **Trap-уведомление:** dot1dStpBridgeMaxAge	**Функционал агента:** RC-BRIDGE-MIB-AC **Доступ:** Для чтения и записи **Синтаксическая структура:** Integer **Идентификатор объекта:** .1.3.6.1.2.1.17.2.12.0 **Определение:** Значение, которое все мосты используют в качестве MaxAge, когда мост работает в качестве корневого. Отметим, что 802.1D-1998 задает привязку диапазона для этого параметра к значению параметра dot1dStpBridgeHelloTime. Дискретность для этого таймера установлена стандартом 802.1D-1998 в 1 сек. Агент может возвращать ошибку badValue при попытке установить нецелое число секунд. **Примечание** Значение этого объекта округляется до ближайшего числа десятых долей секунды.
Группа: dot1dStpBridgeGroup **Trap-уведомление:** dot1dStpDesignatedRoot	**Доступ:** Только для чтения **Синтаксическая структура:** Hex-String **Идентификатор объекта:** .1.3.6.1.2.1.17.2.5.0

Группа/Объект	Описание
	Определение: Идентификатор моста, служащего корнем связующего дерева, определенный протоколом STP, выполняемым на этом узле. Это значение используется как параметр корневого идентификатора во всех конфигурационных блоках протокольных данных моста, создаваемых этим узлом.
Группа: dot1dStpBridgeGroup **Trap-уведомление:** dot1dStpForwardDelay	**Доступ:** Только для чтения **Синтаксическая структура:** Integer **Идентификатор объекта:** .1.3.6.1.2.1.17.2.11.0 **Определение:** Это значение (в сотых долях секунды) задает как быстро порт меняет свое состояние STP при переходе в направлении к состоянию Forwarding. Значение определяет время пребывания порта в каждом из состояний Listening и Learning, предшествующих состоянию Forwarding. Это значение используется также в случае обнаружения происходящей смены топологии, чтобы "состарить" все динамические записи в базе данных пересылки. [Отметим, что это значение является одним из тех, которые этот мост использует в настоящий момент в отличие от dot1dStpBridgeForwardDelay, с которым этот и все другие мосты начинают работу, когда мост становится корневым.]
Группа: dot1dStpBridgeGroup **Trap-уведомление:** dot1dStpHelloTime	**Доступ:** Только для чтения **Синтаксическая структура:** Integer **Идентификатор объекта:** .1.3.6.1.2.1.17.2.9.0 **Определение:** Интервал между передачей конфигурационных блоков протокольных данных моста через любой порт данного моста, когда он является или пытается стать корнем связующего дерева (в сотых долях секунды). Это значение, используемое мостом в данный момент.
Группа: dot1dStpBridgeGroup **Trap-уведомление:** dot1dStpHoldTime	**Доступ:** Только для чтения **Синтаксическая структура:** Integer **Идентификатор объекта:** .1.3.6.1.2.1.17.2.10.0 **Определение:** Это значение определяет интервал (в сотых долях секунды), в течение которого данным узлом должно передаваться не более двух конфигурационных блоков протокольных данных моста.
Группа: dot1dStpBridgeGroup **Trap-уведомление:** dot1dStpMaxAge	**Доступ:** Только для чтения **Синтаксическая структура:** Integer **Идентификатор объекта:** .1.3.6.1.2.1.17.2.8.0 **Определение:** Максимальный возраст информации протокола STP, полученной из сети на любом порту, по достижении которого данные отбрасываются (в сотых долях секунды). Это значение, используемое мостом в данный момент.
Группа: dot1dStpPortGroup **Trap-уведомление:** dot1dStpPort	**Доступ:** Только для чтения **Синтаксическая структура:** Integer **Идентификатор объекта:** .1.3.6.1.2.1.17.2.15.1.1.1 **Определение:** Номер порта, для которого эта запись содержит данные управления протоколом связующего дерева.
Группа: dot1dStpPortGroup **Trap-уведомление:** dot1dStpPortDesignatedBridge	**Доступ:** Только для чтения **Синтаксическая структура:** Hex-String **Идентификатор объекта:** .1.3.6.1.2.1.17.2.15.1.8.1

Группа/Объект	Описание
	Определение: Идентификатор моста, который данный порт считает выделенным мостом для сегмента данного порта.
Группа: dot1dStpPortGroup **Trap-уведомление:** dot1dStpPortDesignatedCost	**Доступ:** Только для чтения **Синтаксическая структура:** Integer **Идентификатор объекта:** .1.3.6.1.2.1.17.2.15.1.7.1 **Определение:** Стоимость пути выделенного порта для сегмента, подключенного к данному порту. Это значение сравнивается с полем стоимости корневого тракта в полученных блоках протокольных данных моста.
Группа: dot1dStpPortGroup **Trap-уведомление:** dot1dStpPortDesignatedPort	**Доступ:** Только для чтения **Синтаксическая структура:** Hex-String **Идентификатор объекта:** .1.3.6.1.2.1.17.2.15.1.9.1 **Определение:** Идентификатор порта выделенного моста для сегмента данного порта.
Группа: dot1dStpPortGroup **Trap-уведомление:** dot1dStpPortDesignatedRoot	**Доступ:** Только для чтения **Синтаксическая структура:** Hex-String **Идентификатор объекта:** .1.3.6.1.2.1.17.2.15.1.6.1 **Определение:** Уникальный идентификатор моста, записанного в качестве корневого в конфигурационных блоках протокольных данных моста, передаваемых выделенным мостом для сегмента, к которому порт подключен.
Группа: dot1dStpPortGroup **Trap-уведомление:** dot1dStpPortEnable	**Доступ:** Для чтения и записи **Синтаксическая структура:** Integer **Идентификатор объекта:** .1.3.6.1.2.1.17.2.15.1.4.1 **Определение:** Статус порта enabled/disabled (включен/отключен).
Группа: dot1dStpPortGroup **Trap-уведомление:** dot1dStpPortForwardTransitions	**Доступ:** Только для чтения **Синтаксическая структура:** Counter32 **Идентификатор объекта:** .1.3.6.1.2.1.17.2.15.1.10.1 **Определение:** Число переходов данного порта из состояния Learning в состояние Forwarding.
Группа: dot1dStpPortGroup **Trap-уведомление:** dot1dStpPortPathCost	**Доступ:** Для чтения и записи **Синтаксическая структура:** Integer **Идентификатор объекта:** .1.3.6.1.2.1.17.2.15.1.5.1 **Определение:** Вклад данного порта в стоимость пути к корню STP через этот порт. 802.1D-1998 рекомендует по умолчанию использовать значение, обратно пропорциональное скорости подключенной ЛВС. Новым реализациям следует поддерживать dot1dStpPortPathCost32. Если стоимость пути через порт превосходит максимальное значение для этого объекта, объекту следует возвращать максимальное значение 65535. Если данный объект возвращает максимальное значение, приложению следует выполнить чтение объекта dot1dStpPortPathCost32.
Группа: dot1dStpPortGroup **Trap-уведомление:** dot1dStpPortPriority	**Функционал агента:** RC-BRIDGE-MIB-AC **Доступ:** Для чтения и записи **Синтаксическая структура:** Integer **Идентификатор объекта:** .1.3.6.1.2.1.17.2.15.1.2.1

Группа/Объект	Описание
	Определение: Значение поля приоритета, содержащегося в первых 2 октетах идентификатора порта. Остальные октеты идентификатора порта задаются значением dot1dStpPort. Для мостов с поддержкой IEEE 802.1t или IEEE 802.1w допустимы значения от 0 до 240 с шагом 16. **Примечание** Согласно RFC 4188 допустимые значения для этого объекта составляют от 0 до 240 с шагом 16.
Группа: rstpPortGroup **Trap-уведомление:** dot1dStpPortProtocolMigration	**Доступ:** Для чтения и записи **TruthValue** **Идентификатор объекта:** .1.3.6.1.2.1.17.2.19.1.1 **Определение:** При работе в режиме RSTP (версия 2) запись значения true(1) для этого объекта приводит к принудительной передаче этим портом блока протокольных данных моста RSTP. Любая другая операция с этим объектом не оказывает никакого влияния и всегда возвращает значение false(2) при чтении.
Группа: dot1dStpPortGroup **Trap-уведомление:** dot1dStpPortState	**Доступ:** Только для чтения **Синтаксическая структура:** Integer **Идентификатор объекта:** .1.3.6.1.2.1.17.2.15.1.3.1 **Определение:** Текущее состояние порта, определенное приложением STP. Это состояние определяет действия порта при получении кадра. При обнаружении неработоспособного порта мост устанавливает для него состояние broken(6). Для отключенных портов (см. dot1dStpPortEnable) этот объект имеет значение disabled(1).
Группа: dot1dStpBridgeGroup **Trap-уведомление:** dot1dStpPriority	**Функционал агента:** RC-BRIDGE-MIB-AC **Доступ:** Для чтения и записи **Синтаксическая структура:** Integer **Идентификатор объекта:** .1.3.6.1.2.1.17.2.2.0 **Определение:** Значение разрешенной для записи части идентификатора моста (т. е. первые 2 октета 8-октетного идентификатора моста). Последние 6 октетов идентификатора моста заданы значением dot1dBaseBridgeAddress. На мостах, поддерживающих IEEE 802.1t или IEEE 802.1w, разрешены значения от 0 до 61440 с шагом 4096. **Примечание** Согласно RFC 4188 допустимые значения для этого объекта составляют от 0 до 61440 с шагом 4096.
Группа: dot1dStpBridgeGroup **Trap-уведомление:** dot1dStpProtocolSpecification	**Доступ:** Только для чтения **Синтаксическая структура:** Integer **Идентификатор объекта:** .1.3.6.1.2.1.17.2.1.0 **Определение:** Индикация используемой версии протокола STP. Значение decLb100(2) указывает протокол DEC LANbridge 100 STP. Реализации IEEE 802.1D будут возвращать значение ieee8021d(3). При выпуске в будущем новых версий протокола IEEE STP, не совместимых с текущей версией, будут определены новые значения.
Группа: dot1dStpBridgeGroup **Trap-уведомление:** dot1dStpRootCost	**Доступ:** Только для чтения **Синтаксическая структура:** Integer

Группа/Объект	Описание
	Идентификатор объекта: .1.3.6.1.2.1.17.2.6.0 **Определение:** Стоимость пути к корню со стороны этого моста.
Группа: dot1dStpBridgeGroup **Trap-уведомление:** dot1dStpRootPort	**Доступ:** Только для чтения **Синтаксическая структура:** Integer **Идентификатор объекта:** .1.3.6.1.2.1.17.2.7.0 **Определение:** Номер порта, который предлагает самый дешевый путь от данного моста к корневому мосту.
Группа: dot1dStpBridgeGroup **Trap-уведомление:** dot1dStpTimeSinceTopologyChange	**Функционал агента:** RC-BRIDGE-MIB-AC **Доступ:** Только для чтения **Синтаксическая структура:** Timeticks **Идентификатор объекта:** .1.3.6.1.2.1.17.2.3.0 **Определение:** Время (в сотых долях секунды) с момента последнего изменения топологии, обнаруженного мостом. Для RSTP это время с момента, когда таймер tcWhile любого из портов этого моста принял ненулевое значение. **Примечание** Согласно RFV 4188 это время с момента, когда таймер tcWhile любого из портов этого моста принял ненулевое значение.
Группа: dot1dStpBridgeGroup **Trap-уведомление:** dot1dStpTopChanges	**Доступ:** Только для чтения **Синтаксическая структура:** Counter32 **Идентификатор объекта:** .1.3.6.1.2.1.17.2.4.0 **Определение:** Общее число изменений топологии, обнаруженных этим мостом с момента последнего сброса или инициализации элемента управления.
Группа: dot1dTpBridgeGroup **Trap-уведомление:** dot1dTpAgingTime	**Доступ:** Для чтения и записи **Синтаксическая структура:** Integer **Идентификатор объекта:** .1.3.6.1.2.1.17.4.2.0 **Определение:** Время (в секундах) старения динамически определенной информации о пересылке. 802.1D-1998 рекомендует использовать по умолчанию 300 секунд. **Примечание** Диапазон допустимых значений ограничен интервалом от 15 до 800 секунд. Нижний предел 15 секунд является аппаратным ограничением.
Группа: dot1dTpFdbGroup **Trap-уведомление:** dot1dTpFdbAddress	**Доступ:** Только для чтения **Синтаксическая структура:** Hex-String **Идентификатор объекта:** .1.3.6.1.2.1.17.4.3.1.1.148.184.197.5.176.0 **Определение:** Информация о конкретном индивидуальном MAC-адресе, для которого мост имеет информацию о пересылке и/или фильтрации.
Группа: dot1dTpFdbGroup **Trap-уведомление:** dot1dTpFdbPort	**Доступ:** Только для чтения **Синтаксическая структура:** Integer **Идентификатор объекта:** .1.3.6.1.2.1.17.4.3.1.2.148.184.197.5.176.0 **Определение:** 0 или номер порта, на котором был обнаружен кадр с адресом отправителя, совпадающим со значением соответствующего

Группа/Объект	Описание
	экземпляра dot1dTpFdbAddress. 0 показывает, что номер порта не был определен, но у моста имеется некая информация о пересылке/фильтрации для этого адреса (например, в dot1dStaticTable). Разработчикам рекомендуется назначать этому объекту номер порта, когда он определен, даже для адресов, у которых соответствующее значение dot1dTpFdbStatus не равно learned(3).
Группа: dot1dTpFdbGroup **Trap-уведомление:** dot1dTpFdbStatus	**Доступ:** Только для чтения **Синтаксическая структура:** Integer **Идентификатор объекта:** .1.3.6.1.2.1.17.4.3.1.3.148.184.197.5.176.0 **Определение:** Статус этой записи. который может принимать значения: • other(1) — ни одно из перечисленных ниже. Это включает ситуации, когда некий другой объект MIB (не соответствующий экземпляру dot1dTpFdbPort и не запись в dot1dStaticTable) используется для определения пересылки кадра, направленного по адресу из соответствующего dot1dTpFdbAddress. • invalid(2) — запись больше не пригодна (например, она уже устарела), но еще остается в таблице. • learned(3) — значение соответствующего экземпляра dot1dTpFdbPort определено и используется. • self(4) — значение соответствующего экземпляра dot1dTpFdbAddress представляет один из адресов моста. Соответствующий экземпляр dot1dTpFdbPort показывает, какой из портов имеет этот адрес. • mgmt(5) — значение соответствующего экземпляра dot1dTpFdbAddress является также значением имеющегося экземпляра dot1dStaticAddress.
Группа: dot1dTpBridgeGroup **Trap-уведомление:** dot1dTpLearnedEntryDiscards	**Функционал агента:** RC-BRIDGE-MIB-AC **Доступ:** Только для чтения **Синтаксическая структура:** Counter32 **Идентификатор объекта:** .1.3.6.1.2.1.17.4.1.0 **Определение:** Общее число записей базы данных пересылки, которые были получены путем обучения, но отброшены по причине нехватки места в базе данных пересылки. Если значение счетчика растет, это показывает регулярное переполнение базы данных пересылки (негативное влияние на работу сети). Если значение счетчика достаточно велико, но не растет, это показывает, что проблема переполнения была временной. **Примечание** Коммутатору не известно значение этого объекта. В ответ на запрос GET будет возвращено нулевое значение.
Группа: dot1dTpGroup **Trap-уведомление:** dot1dTpPort	**Доступ:** Только для чтения **Синтаксическая структура:** Integer **Идентификатор объекта:** .1.3.6.1.2.1.17.4.4.1.1.1 **Определение:** Номер порта, для которого эта запись содержит данные управления прозрачным мостом.
Группа: dot1dTpGroup **Trap-уведомление:** dot1dTpPortInDiscards	**Доступ:** Только для чтения **Синтаксическая структура:** Counter32 **Идентификатор объекта:** .1.3.6.1.2.1.17.4.4.1.5.1

Группа/Объект	Описание
	Определение: Число принятых данным портом из своего сегмента корректных кадров, которые были отброшены (т. е., отфильтрованы) процессом пересылки.
Группа: dot1dTpGroup **Trap-уведомление:** dot1dTpPortInFrames	**Доступ:** Только для чтения **Синтаксическая структура:** Counter32 **Идентификатор объекта:** .1.3.6.1.2.1.17.4.4.1.3.1 **Определение:** Число кадров, полученных данным портом из его сегмента. Отметим, что кадры, полученные на соответствующем этому порту интерфейсе, учитываются этим объектом лишь в том случае, когда они относятся к протоколу, обрабатываемому локальной функцией моста (включая кадры управления мостом).
Группа: dot1dTpGroup **Trap-уведомление:** dot1dTpPortMaxInfo	**Доступ:** Только для чтения **Синтаксическая структура:** Integer **Идентификатор объекта:** .1.3.6.1.2.1.17.4.4.1.2.1 **Определение:** Максимальный размер поля INFO (не MAC), который этот порт будет принимать и передавать.
Группа: dot1dTpGroup **Trap-уведомление:** dot1dTpPortOutFrames	**Доступ:** Только для чтения **Синтаксическая структура:** Counter32 **Идентификатор объекта:** .1.3.6.1.2.1.17.4.4.1.4.1 **Определение:** Число кадров, переданных портом в свой сегмент. Отметим, что кадры, переданные соответствующим этому порту интерфейсом, учитываются этим объектом лишь в том случае, когда они относятся к протоколу, обрабатываемому локальной функцией моста (включая кадры управления мостом).

IEC-62439-3-MIB

Группа/Объект	Описание
Группа: lreStatisticsInterfaceGroup **Trap-уведомление:** lreCntDuplicateA	**Доступ:** Только для чтения **Синтаксическая структура:** Counter32 **Идентификатор объекта:** 1.0.62439.2.21.1.1.0.1.1.19.1 **Определение:** Число записей в механизме обнаружения дубликатов на порту A, для которых был получен один единственный дубликат.
Группа: lreStatisticsInterfaceGroup **Trap-уведомление:** lreCntDuplicateB	**Доступ:** Только для чтения **Синтаксическая структура:** Counter32 **Идентификатор объекта:** 1.0.62439.2.21.1.1.0.1.1.20.1 **Определение:** Число записей в механизме обнаружения дубликатов на порту B, для которых был получен один единственный дубликат.
Группа: lreStatisticsInterfaceGroup **Trap-уведомление:** lreCntDuplicateC	**Доступ:** Только для чтения **Синтаксическая структура:** Counter32 **Идентификатор объекта:** 1.0.62439.2.21.1.1.0.1.1.21.1 **Определение:** Число записей в механизме обнаружения дубликатов на порту C, для которых был получен один единственный дубликат.
Группа: lreStatisticsInterfaceGroup **Trap-уведомление:** lreCntErrorsA	**Доступ:** Только для чтения **Синтаксическая структура:** Counter32 **Идентификатор объекта:** 1.0.62439.2.21.1.1.0.1.1.11.1

Группа/Объект	Описание
	Определение: Число кадров с ошибками, полученных на этом LRE-порту A. Исходное значение = 0.
Группа: lreStatisticsInterfaceGroup **Trap-уведомление:** lreCntErrorsB	**Доступ:** Только для чтения **Синтаксическая структура:** Counter32 **Идентификатор объекта:** 1.0.62439.2.21.1.1.0.1.1.12.1 **Определение:** Число кадров с ошибками, полученных на этом LRE-порту B. Исходное значение = 0.
Группа: lreStatisticsInterfaceGroup **Trap-уведомление:** lreCntErrorsC	**Доступ:** Только для чтения **Синтаксическая структура:** Counter32 **Идентификатор объекта:** 1.0.62439.2.21.1.1.0.1.1.13.1 **Определение:** Число кадров с ошибками, полученных на интерфейсе приложения DANP или DANH или межсетевом соединении RedBox. Исходное значение = 0.
Группа: lreStatisticsInterfaceGroup **Trap-уведомление:** lreCntErrWrongLanA	**Доступ:** Только для чтения **Синтаксическая структура:** Counter32 **Идентификатор объекта:** 1.0.62439.2.21.1.1.0.1.1.5.1 **Определение:** Число кадров с неверным идентификатором ЛВС, полученных на LRE-порту A. Исходное значенпие = 0. Применимо только для PRP-портов.
Группа: lreStatisticsInterfaceGroup **Trap-уведомление:** lreCntErrWrongLanB	**Доступ:** Только для чтения **Синтаксическая структура:** Counter32 **Идентификатор объекта:** 1.0.62439.2.21.1.1.0.1.1.6.1 **Определение:** Число кадров с неверным идентификатором ЛВС, полученных на LRE-порту B. Исходное значение = 0. Применимо только для PRP-портов.
Группа: lreStatisticsInterfaceGroup **Trap-уведомление:** lreCntErrWrongLanC	**Функционал агента:** RC-IEC-62439-3-MIB-AC **Доступ:** не реализован **Синтаксическая структура:** Counter32 **Идентификатор объекта:** 1.0.62439.2.21.1.1.0.1.1.7.1 **Определение:** Число кадров с неверным идентификатором ЛВС, полученных на межсетевом соединении RedBox. Применимо только для RedBox HSR в конфигурации HSR-PRP.
Группа: lreStatisticsInterfaceGroup **Trap-уведомление:** lreCntMultiA	**Функционал агента:** RC-IEC-62439-3-MIB-AC **Доступ:** не реализован **Синтаксическая структура:** Counter32 **Идентификатор объекта:** 1.0.62439.2.21.1.1.0.1.1.22.1 **Определение:** Число записей в механизме обнаружения дубликатов на порту A, для которых было получено более одного дубликата.
Группа: lreStatisticsInterfaceGroup **Trap-уведомление:** lreCntMultiB	**Функционал агента:** RC-IEC-62439-3-MIB-AC **Доступ:** не реализован **Синтаксическая структура:** Counter32 **Идентификатор объекта:** 1.0.62439.2.21.1.1.0.1.1.23.1 **Определение:** Число записей в механизме обнаружения дубликатов на порту B, для которых было получено более одного дубликата.
Группа: lreStatisticsInterfaceGroup	**Функционал агента:** RC-IEC-62439-3-MIB-AC

Группа/Объект	Описание
Trap-уведомление: lreCntMultiC	**Доступ:** не реализован **Синтаксическая структура:** Counter32 **Идентификатор объекта:** 1.0.62439.2.21.1.1.0.1.1.24.1 **Определение:** Число записей в механизме обнаружения дубликатов в интерфейсе приложения DAN или межсетевом соединении RedBox, для которых было получено более одного дубликата.
Группа: lreStatisticsInterfaceGroup **Trap-уведомление:** lreCntNodes	**Доступ:** Только для чтения **Синтаксическая структура:** Integer **Идентификатор объекта:** 1.0.62439.2.21.1.1.0.1.1.14.1 **Определение:** Число узлов в таблице узлов.
Группа: lreStatisticsInterfaceGroup **Trap-уведомление:** lreCntOwnRxA	**Доступ:** Только для чтения **Синтаксическая структура:** Counter32 **Идентификатор объекта:** 1.0.62439.2.21.1.1.0.1.1.25.1 **Определение:** Количество кадров с тегами HSR, полученных на порту A, которые поступают от этого устройства. Кадры поступают от этого устройства, если MAC-адрес источника совпадает с MAC-адресом LRE или если MAC-адрес источника появляется в таблице прокси-узлов (в случае реализации). Применимо только для HSR. Исходное значение = 0.
Группа: lreStatisticsInterfaceGroup **Trap-уведомление:** lreCntOwnRxB	**Доступ:** Только для чтения **Синтаксическая структура:** Counter32 **Идентификатор объекта:** 1.0.62439.2.21.1.1.0.1.1.26.1 **Определение:** Количество кадров с меткой HSR, полученных на порту B, которые поступают от этого устройства. Кадры поступают от этого устройства, если MAC-адрес источника совпадает с MAC-адресом LRE или если MAC-адрес источника появляется в таблице прокси-узлов (в случае реализации). Применимо только для HSR. Исходное значение = 0.
Группа: lreStatisticsInterfaceGroup **Trap-уведомление:** lreCntProxyNodes	**Доступ:** Только для чтения **Синтаксическая структура:** Integer **Идентификатор объекта:** 1.0.62439.2.21.1.1.0.1.1.15.1 **Определение:** Число узлов в таблице прокси-узлов. Применимо только для RedBox. Исходное значение = 0.
Группа: lreStatisticsInterfaceGroup **Trap-уведомление:** lreCntRxA	**Доступ:** Только для чтения **Синтаксическая структура:** Counter32 **Идентификатор объекта:** 1.0.62439.2.21.1.1.0.1.1.8.1 **Определение:** Число кадров, полученных на LRE-порту A. Учитываются только кадры с меткой HSR или оснащенные концевой меткой управления резервированием PRP. Также учитываются кадры, которые никуда не пересылаются (например, потому что отправитель кадра находится в таблице прокси-узлов). Учитываются только кадры, полученные полностью и без ошибок. Исходное значение = 0.
Группа: lreStatisticsInterfaceGroup **Trap-уведомление:** lreCntRxB	**Доступ:** Только для чтения **Синтаксическая структура:** Counter32 **Идентификатор объекта:** 1.0.62439.2.21.1.1.0.1.1.9.1 **Определение:** Число кадров, полученных на LRE-порту B. Учитываются только кадры с меткой HSR или оснащенные концевой меткой

Группа/Объект	Описание
	управления резервированием PRP. Также учитываются кадры, которые никуда не пересылаются (например, потому что отправитель кадра находится в таблице прокси-узлов). Учитываются только кадры, полученные полностью и без ошибок. Исходное значение = 0.
Группа: lreStatisticsInterfaceGroup **Trap-уведомление:** lreCntRxC	**Функционал агента:** RC-IEC-62439-3-MIB-AC **Доступ:** Только для чтения **Синтаксическая структура:** Counter32 **Идентификатор объекта:** 1.0.62439.2.21.1.1.0.1.1.10.1 **Определение:** Число кадров с ошибками, полученных на интерфейсе приложения DANP или DANH или число кадров, полученных на межсетевом соединении RedBox. Учитываются кадры, оснащенные концевой меткой управления резервированием PRP или без нее, или с меткой HSR, но не кадры link-local. Учитываются только кадры, полученные полностью и без ошибок. Исходное значение = 0. **Примечание** Учитываются только кадры, полученные на локальном порту.
Группа: lreStatisticsInterfaceGroup **Trap-уведомление:** lreCntTxA	**Доступ:** Только для чтения **Синтаксическая структура:** Counter32 **Идентификатор объекта:** 1.0.62439.2.21.1.1.0.1.1.2.1 **Определение:** Число кадров, отправленных через LRE-порт A, которые являются кадрами с меткой HSR или оснащены концевой меткой управления резервированием PRP. Учитываются только кадры с меткой HSR или оснащенные концевой меткой управления резервированием PRP. Кадры, отброшенные во время передачи, не учитываются. Исходное значение = 0.
Группа: lreStatisticsInterfaceGroup **Trap-уведомление:** lreCntTxB	**Доступ:** Только для чтения **Синтаксическая структура:** Counter32 **Идентификатор объекта:** 1.0.62439.2.21.1.1.0.1.1.3.1 **Определение:** Число кадров, отправленных через LRE-порт B, которые являются кадрами с меткой HSR или оснащены концевой меткой управления резервированием PRP. Учитываются только кадры с меткой HSR или оснащенные концевой меткой управления резервированием PRP. Кадры, отброшенные во время передачи, не учитываются. Исходное значение = 0.
Группа: lreStatisticsInterfaceGroup **Trap-уведомление:** lreCntTxC	**Функционал агента:** RC-IEC-62439-3-MIB-AC **Доступ:** Только для чтения **Синтаксическая структура:** Counter32 **Идентификатор объекта:** 1.0.62439.2.21.1.1.0.1.1.4.1 **Определение:** Число кадров, отправленных на интерфейс приложения DANP или DANH или через межсетевое соединение RedBox. Учитываются кадры, оснащенные концевой меткой управления резервированием PRP или без нее, или с меткой HSR, но не кадры link-local. Кадры, отброшенные во время передачи, не учитываются. Исходное значение = 0. **Примечание** Учитываются только кадры, отправленные с локального порта.
Группа: lreStatisticsInterfaceGroup	**Функционал агента:** RC-IEC-62439-3-MIB-AC

Группа/Объект	Описание
Trap-уведомление: lreCntUniqueA	**Доступ:** не реализован **Синтаксическая структура:** Counter32 **Идентификатор объекта:** 1.0.62439.2.21.1.1.0.1.1.16.1 **Определение:** Число записей в механизме обнаружения дубликатов на порту A, для которых не было получено ни одного дубликата.
Группа: lreStatisticsInterfaceGroup **Trap-уведомление:** lreCntUniqueB	**Функционал агента:** RC-IEC-62439-3-MIB-AC **Доступ:** не реализован **Синтаксическая структура:** Counter32 **Идентификатор объекта:** 1.0.62439.2.21.1.1.0.1.1.17.1 **Определение:** Число записей в механизме обнаружения дубликатов на порту B, для которых не было получено ни одного дубликата.
Группа: lreStatisticsInterfaceGroup **Trap-уведомление:** lreCntUniqueC	**Функционал агента:** RC-IEC-62439-3-MIB-AC **Доступ:** не реализован **Синтаксическая структура:** Counter32 **Идентификатор объекта:** 1.0.62439.2.21.1.1.0.1.1.18.1 **Определение:** Число записей в механизме обнаружения дубликатов на порту C, для которых не было получено ни одного дубликата.
Группа: lreConfigurationInterfaceGroup **Trap-уведомление:** lreDuplicateDiscard	**Функционал агента:** RC-IEC-62439-3-MIB-AC **Доступ:** Только для чтения **Синтаксическая структура:** Integer **Идентификатор объекта:** 1.0.62439.2.21.0.1.0.1.1.11.1 **Определение:** Указывает, используется ли при приеме алгоритм исключения дубликатов. По умолчанию: исключение.
Группа: lreConfigurationInterfaceGroup **Trap-уведомление:** lreEvaluateSupervision	**Функционал агента:** RC-IEC-62439-3-MIB-AC **Доступ:** Только для чтения **Синтаксическая структура:** Integer **Идентификатор объекта:** 1.0.62439.2.21.0.1.0.1.1.16.1 **Определение:** True (истина), если LRE оценивает полученные контролирующие кадры. False (ложь), если он отбрасывает контролирующие кадры без оценки. Примечание: LRE необходимы для отправки контролирующих кадров, но прием не является обязательным. Значение по умолчанию зависит от реализации.
Группа: lreConfigurationInterfaceGroup **Trap-уведомление:** lreHsrLREMode	**Функционал агента:** RC-IEC-62439-3-MIB-AC **Доступ:** Только для чтения **Синтаксическая структура:** Integer **Идентификатор объекта:** 1.0.62439.2.21.0.1.0.1.1.13.1 **Определение:** Это перечисление применимо только в том случае, если LRE является узлом моста HSR или RedBox. Оно показывает режим работы LRE HSR: • (1): Режим по умолчанию: LRE HSR находится в режиме h и выполняет маршрутизацию трафика с меткой HSR. • (2): Опциональный режим: LRE HSR находится в режиме n, и маршрутизация между его портами HSR отключено. Трафик имеет метку HSR.

Группа/Объект	Описание
	• (3): Опциональный режим: LRE HSR находится в режиме t и выполняет маршрутизацию трафика без метки HSR между портами HSR. • (4): Опциональный режим: LRE HSR находится в режиме u его поведение аналогично режиму h, за исключением удаления одноадресных сообщений. • (5): Опциональный режим: LRE HSR сконфигурирован для комбинированного режима. Кадры HSR обрабатываются в соответствии с режимом h. Кадры не HSR обрабатываются в соответствии с правилами мостового соединения 802.1D. Когда коммутатор находится в режиме HSR, этот параметр конфигурации доступен, но только для чтения. Значение: modeh(1). Когда коммутатор находится в режиме PRP, этот параметр недоступен, так как не применяется.
Группа: lreConfigurationInterfaceGroup **Trap-уведомление:** lreInterfaceConfigEntry	**Доступ:** не реализован **Синтаксическая структура:** Integer **Идентификатор объекта:** 1.0.62439.2.21.0.1.0.1.1 **Определение:** Каждая запись содержит данные управления, применимые к конкретному LRE.
Группа: lreConfigurationInterfaceGroup **Trap-уведомление:** lreInterfaceConfigIndex	**Доступ:** не реализован **Синтаксическая структура:** Integer **Идентификатор объекта:** 1.0.62439.2.21.0.1.0.1.1.1 **Определение:** Уникальное значение для каждого LRE.
Группа: lreConfigurationInterfaceGroup **Trap-уведомление:** lreInterfaceConfigTable	**Доступ:** не реализован **Синтаксическая структура:** Integer **Идентификатор объекта:** 1.0.62439.2.21.0.1.0.1 **Определение:** Перечень LRE PRP/HSR. Каждая запись соответствует одному объекту протокола резервирования (LRE) PRP/HSR, каждый из которых представляет пару LAN-портов A и B. Базовые устройства, поддерживающие PRP/HSR, могут иметь только один LRE и, следовательно, одну запись в таблице, в то время как более сложные устройства могут иметь несколько записей для нескольких LRE.
Группа: lreConfigurationGeneralGroup **Trap-уведомление:** lreInterfaceCount	**Доступ:** Только для чтения **Синтаксическая структура:** Integer **Идентификатор объекта:** 1.0.62439.2.21.0.0.2.0 **Определение:** Общее число LRE в этой системе.
Группа: lreStatisticsInterfaceGroup **Trap-уведомление:** lreInterfaceStatsEntry	**Доступ:** не реализован **Синтаксическая структура:** Integer **Идентификатор объекта:** 1.0.62439.2.21.1.1.0.1.1 **Определение:** Запись, содержащая данные управления, применимые к конкретному LRE.
Группа: lreStatisticsInterfaceGroup **Trap-уведомление:** lreInterfaceStatsIndex	**Доступ:** не реализован **Синтаксическая структура:** Integer **Идентификатор объекта:** 1.0.62439.2.21.1.1.0.1.1.1 **Определение:** Уникальное значение для каждого LRE.
Группа: lreStatisticsInterfaceGroup **Trap-уведомление:** lreInterfaceStatsTable	**Доступ:** не реализован **Синтаксическая структура:** Integer

Группа/Объект	Описание
	Идентификатор объекта: 1.0.62439.2.21.1.1.0.1 **Определение:** Перечень LRE PRP/HSR. Каждая запись соответствует одному объекту протокола резервирования (LRE) PRP/HSR, каждый из которых представляет пару LAN-портов A и B, а также порт C в отношении приложения/межсетевого соединения. Базовые устройства, поддерживающие PRP/HSR, могут иметь только один LRE и, следовательно, одну запись в таблице, в то время как более сложные устройства могут иметь несколько записей для нескольких LRE.
Группа: lreConfigurationInterfaceGroup **Trap-уведомление:** lreLinkStatusA	**Доступ:** Только для чтения **Синтаксическая структура:** Integer **Идентификатор объекта:** 1.0.62439.2.21.0.1.0.1.1.9.1 **Определение:** Показывает фактический статус канала порта A LRE.
Группа: lreConfigurationInterfaceGroup **Trap-уведомление:** lreLinkStatusB	**Доступ:** Только для чтения **Синтаксическая структура:** Integer **Идентификатор объекта:** 1.0.62439.2.21.0.1.0.1.1.10.1 **Определение:** Показывает фактический статус канала порта B LRE.
Группа: lreConfigurationInterfaceGroup **Trap-уведомление:** lreMacAddress	**Функционал агента:** RC-IEC-62439-3-MIB-AC **Доступ:** Только для чтения **Синтаксическая структура:**MacAddress **Идентификатор объекта:** 1.0.62439.2.21.0.1.0.1.1.6.1 **Определение:** Указывает MAC-адрес для использования этим LRE. MAC-адреса идентичны для всех портов одного LRE.
Группа: lreConfigurationGeneralGroup **Trap-уведомление:** lreManufacturerName	**Доступ:** Только для чтения **Синтаксическая структура:**DisplayString **Идентификатор объекта:** 1.0.62439.2.21.0.0.1.0 **Определение:** Указывает наименование производителя устройства LRE.
Группа: lreConfigurationInterfaceGroup **Trap-уведомление:** lreNodeName	**Доступ:** Для чтения и записи **Синтаксическая структура:**DisplayString **Идентификатор объекта:** 1.0.62439.2.21.0.1.0.1.1.4.1 **Определение:** Указывает имя узла этого LRE.
Группа: lreConfigurationInterfaceGroup **Trap-уведомление:** lreNodesTableClear	**Доступ:** Для чтения и записи **Синтаксическая структура:** Integer **Идентификатор объекта:** 1.0.62439.2.21.0.1.0.1.1.17.1 **Определение:** Указывает, что таблица узлов должна быть очищена.
Группа: lreConfigurationInterfaceGroup **Trap-уведомление:** lreNodeType	**Доступ:** Для чтения и записи **Синтаксическая структура:** Integer **Идентификатор объекта:** 1.0.62439.2.21.0.1.0.1.1.3.1 **Определение:** Указывает режим работы LRE: • Режим PRP 1 (1) • Режим HSR (2)

Группа/Объект	Описание
	Примечание Режим PRP 0 считается устаревшим и не поддерживается этой версией MIB.
Группа: lreConfigurationInterfaceGroup **Trap-уведомление:** lrePortAdminStateA	**Доступ:** Для чтения и записи **Синтаксическая структура:** Integer **Идентификатор объекта:** 1.0.62439.2.21.0.1.0.1.1.7.1 **Определение:** Указывает, должен ли порт A быть активным или неактивным, с помощью действий по управлению. По умолчанию: активный
Группа: lreConfigurationInterfaceGroup **Trap-уведомление:** lrePortAdminStateB	**Доступ:** Для чтения и записи **Синтаксическая структура:** Integer **Идентификатор объекта:** 1.0.62439.2.21.0.1.0.1.1.8.1 **Определение:** Указывает, должен ли порт B быть активным или неактивным, с помощью действий по управлению. По умолчанию: активный
Группа: lreConfigurationInterfaceGroup **Trap-уведомление:** lreProxyNodeTableClear	**Функционал агента:** RC-IEC-62439-3-MIB-AC **Доступ:** не реализован **Синтаксическая структура:** Integer **Идентификатор объекта:** 1.0.62439.2.21.0.1.0.1.1.18 **Определение:** Указывает, что таблица прокси-узлов должна быть очищена.
Группа: lreConfigurationInterfaceGroup **Trap-уведомление:** lreRedBoxIdentity	**Функционал агента:** RC-IEC-62439-3-MIB-AC **Доступ:** не реализован **Синтаксическая структура:** Integer **Идентификатор объекта:** 1.0.62439.2.21.0.1.0.1.1.15 **Определение:** Применимо к HSR-PRP RedBox A и HSR-PRP RedBox B. Один идентификатор используется одной парой RedBox (один настроен на A, а другой настроен на B), соединяющей кольцо HSR с сетью PRP. Целочисленное значение задает значение поля пути, которое RedBox вставляет в каждый кадр, получаемый им от своего межсетевого соединения, и вводит в кольцо HSR. При определении в качестве двоичных значений наименьший значащий бит (LSB) обозначает конфигурацию RedBox (A или B), а следующие 3 бита обозначают идентификатор пары RedBox.
Группа: lreConfigurationInterfaceGroup **Trap-уведомление:** lreRowStatus	**Функционал агента:** RC-IEC-62439-3-MIB-AC **Доступ:** Только для чтения **Синтаксическая структура:** RowStatus **Идентификатор объекта:** 1.0.62439.2.21.0.1.0.1.1.2 **Определение:** Указывает статус записи таблицы LRE.
Группа: lreConfigurationInterfaceGroup **Trap-уведомление:** lreSwitchingEndNode	**Функционал агента:** RC-IEC-62439-3-MIB-AC **Доступ:** Только для чтения **Синтаксическая структура:** Integer **Идентификатор объекта:** 1.0.62439.2.21.0.1.0.1.1.14.1 **Определение:** Это перечисление показывает, какая функция включена в этом конкретном LRE:

Группа/Объект	Описание
	• (1): незаданный не-мостовой узел, например, SRP. • (2): незаданный мостовой узел, например, RSTP. • (3): узел PRP/RedBox. • (4): RedBox HSR с обычным трафиком Ethernet на межсетевом соединении. • (5): коммутационный узел HSR. • (6): RedBox HSR с трафиком с меткой HSR на межсетевом соединении. • (7): RedBox HSR с трафиком PRP для LAN A на межсетевом соединении. • (8): RedBox HSR с трафиком PRP для LAN B на межсетевом соединении.
Группа: lreConfigurationInterfaceGroup **Trap-уведомление:** lreTransparentReception	**Доступ:** Только для чтения **Синтаксическая структура:** Integer **Идентификатор объекта:** 1.0.62439.2.21.0.1.0.1.1.12.1 **Определение:** Если сконфигурировано removeRCT, RCT удаляется при пересылке на верхние уровни, применимо только для LRE PRP (по умолчанию: removeRCT).
Группа: lreConfigurationInterfaceGroup **Trap-уведомление:** lreVersionName	**Доступ:** Только для чтения **Синтаксическая структура:** String **Идентификатор объекта:** 1.0.62439.2.21.0.1.0.1.1.5.1 **Определение:** Указывает версию программного обеспечения LRE.

IEEEC37-238-MIB

Группа/Объект	Описание
Группа: ieeeC37238SystemCurrentGroup **Trap-уведомление:** ieeeC37238CurrentDSLocTimeInacc	**Доступ:** Только для чтения **Синтаксическая структура:** Gauge32 **Идентификатор объекта:** 1.3.111.3.37.238.9999.1.2.3 **Определение:** Вклад TimeInaccuracy устройства в наносекундах.
Группа: ieeeC37238SystemCurrentGroup **Trap-уведомление:** ieeeC37238CurrentDSOfstFrMaster	**Доступ:** Только для чтения **Синтаксическая структура:** IEEEC37238TimeInterval **Идентификатор объекта:** 1.3.111.3.37.238.9999.1.2.2 Зависящее от реализации представление текущего значения разницы во времени между ведущим и ведомым устройством, вычисленное ведомым устройством; т. е. <offsetFromMaster> = <Time on the slave clock> ? <Time on the master clock>. Старшие 4 байта. Тип данных должен быть TimeInterval.
Группа: ieeeC37238SystemCurrentGroup **Trap-уведомление:** ieeeC37238CurrentDSStepsRemoved	**Доступ:** Только для чтения **Синтаксическая структура:** Integer **Идентификатор объекта:** 1.3.111.3.37.238.9999.1.2.1 **Определение:** Число коммуникационных путей между локальными часами и гроссмейстерскими часами. Значение инициализации должно быть 0.
Группа: ieeeC37238SystemDefaultReqdGroup	**Доступ:** Только для чтения **Синтаксическая структура:** IEEEC37238ClockAccuracyValue

Группа/Объект	Описание
Trap-уведомление: ieeeC37238DefaultDSClkAccuracy	**Идентификатор объекта:** 1.3.111.3.37.238.9999.1.1.5 **Определение:**ClockAccuracy локальных часов.
Группа: ieeeC37238SystemDefaultReqdGroup **Trap-уведомление:** ieeeC37238DefaultDSClkClass	**Доступ:** Только для чтения **Синтаксическая структура:** IEEEC37238ClockAccuracyValue **Идентификатор объекта:** 1.3.111.3.37.238.9999.1.1.4 **Определение:**ClockClass локальных часов.
Группа: ieeeC37238SystemDefaultReqdGroup **Trap-уведомление:** ieeeC37238DefaultDSClkIdentity	**Доступ:** Только для чтения **Синтаксическая структура:** ClockIdentity **Идентификатор объекта:** 1.3.111.3.37.238.9999.1.1.2 **Определение:**ClockIdentity локальных часов.
Группа: ieeeC37238SystemDefaultReqdGroup **Trap-уведомление:** ieeeC37238DefaultDSDomainNumber	**Доступ:** Для чтения и записи **Синтаксическая структура:** Integer **Идентификатор объекта:** 1.3.111.3.37.238.9999.1.1.9 **Определение:**Стандартный домен локальных часов.
Группа: ieeeC37238SystemDefaultReqdGroup **Trap-уведомление:** ieeeC37238DefaultDSEngTimeInacc	**Функционал агента:** AC-IEEEC37-238-MIB-AC **Доступ:** не реализован **Синтаксическая структура:** Integer **Идентификатор объекта:** 1.3.111.3.37.238.9999.1.1.13 **Определение:**Спроектированное значение networkTimeInaccuracy в нс. Это значение представляет собой наихудший вариант networkTimeInaccuracy от этого устройства для всего.
Группа: ieeeC37238SystemDefaultReqdGroup **Trap-уведомление:** ieeeC37238DefaultDSGMIdentity	**Доступ:** Для чтения и записи **Синтаксическая структура:** Integer **Идентификатор объекта:** 1.3.111.3.37.238.9999.1.1.11 **Определение:**Идентификатор гроссмейстерских часов, передаваемый в TLV IEEE_C37_238 (2 байта). Старший байт зарезервирован и должен быть 0. Настраивается только для устройств с функцией гроссмейстерских часов.
Группа: ieeeC37238SystemDefaultReqdGroup **Trap-уведомление:** ieeeC37238DefaultDSLocTimeInacc	**Доступ:** Только для чтения **Синтаксическая структура:** Gauge32 **Идентификатор объекта:** 1.3.111.3.37.238.9999.1.1.14 **Определение:**Максимальное значение TimeInaccuracy, которое устройство вносит в общее значение networkTimeInaccuracy.
Группа: ieeeC37238SystemDefaultReqdGroup **Trap-уведомление:** ieeeC37238DefaultDSNetTimeInacc	**Доступ:** Для чтения и записи **Синтаксическая структура:** Gauge32 **Идентификатор объекта:** 1.3.111.3.37.238.9999.1.1.12 **Определение:**Значение networkTimeInaccuracy, передаваемое в TLV IEEE_C37_238.
Группа: ieeeC37238SystemDefaultReqdGroup **Trap-уведомление:** ieeeC37238DefaultDSNumberPorts	**Доступ:** Только для чтения **Синтаксическая структура:** Gauge32 **Идентификатор объекта:** 1.3.111.3.37.238.9999.1.1.3 **Определение:** Число PTP-портов на устройстве. Для стандартных часов это значение должно быть 1.

Группа/Объект	Описание
Группа: ieeeC37238SystemDefaultReqdGroup **Trap-уведомление:** ieeeC37238DefaultDSOfsScdLogVar	**Доступ:** Только для чтения **Синтаксическая структура:** Integer **Идентификатор объекта:** 1.3.111.3.37.238.9999.1.1.6 **Определение:** Значение масштабируется, представление смещения как оценки вариации PTP. Вариация PTP характеризует стабильность точности и частоты ведущих часов.
Группа: ieeeC37238SystemDefaultReqdGroup **Trap-уведомление:** ieeeC37238DefaultDSOfstFrMLimit	**Функционал агента:** RC-IEEEC37-238-MIB-AC **Доступ:** Только для чтения **Синтаксическая структура:** IEEEC37238TimeInterval **Идентификатор объекта:** 1.3.111.3.37.238.9999.1.1.15 **Определение:**Смещение от основного ограничения для генерации события OfstExceedsLimit.
Группа: ieeeC37238SystemDefaultReqdGroup **Trap-уведомление:** ieeeC37238DefaultDSPriority1	**Доступ:** Для чтения и записи **Синтаксическая структура:** Gauge32 **Идентификатор объекта:** 1.3.111.3.37.238.9999.1.1.7 **Определение:**Атрибут Priority1 локальных часов.
Группа: ieeeC37238SystemDefaultReqdGroup **Trap-уведомление:** ieeeC37238DefaultDSPriority2	**Доступ:** Для чтения и записи **Синтаксическая структура:** Gauge32 **Идентификатор объекта:** 1.3.111.3.37.238.9999.1.1.8 **Определение:**Атрибут Priority2 локальных часов.
Группа: ieeeC37238SystemDefaultReqdGroup **Trap-уведомление:** ieeeC37238DefaultDSSlaveOnly	**Доступ:** Для чтения и записи **Синтаксическая структура:** Integer **Идентификатор объекта:** 1.3.111.3.37.238.9999.1.1.10 **Определение:** True (истина), если локальные часы являются только ведомыми часами, в ином случае — False (ложь).
Группа: ieeeC37238SystemDefaultReqdGroup **Trap-уведомление:** ieeeC37238DefaultDSTwoStepFlag	**Доступ:** Для чтения и записи **Синтаксическая структура:** Integer **Идентификатор объекта:** 1.3.111.3.37.238.9999.1.1.1 **Определение:** True (истина), если часы являются только часами с двухэтапной синхронизацией, в ином случае — False (ложь).
Группа: ieeeC37238EventsPropertiesGroup **Trap-уведомление:** ieeeC37238EventFaultyState	**Функционал агента:** RC-IEEEC37-238-MIB-AC **Идентификатор объекта:** 1.3.111.3.37.238.9999.0.0.3.0 **Определение:** Указывает, что часы перешли в неисправное состояние. **Примечание** Это уведомление не поддерживается.
Группа: ieeeC37238EventsPropertiesGroup **Trap-уведомление:** ieeeC37238EventLeapSecAnnounced	**Функционал агента:** RC-IEEEC37-238-MIB-AC **Идентификатор объекта:** 1.3.111.3.37.238.9999.0.0.7.0 **Определение:** Указывает, что была заявлена секунда координации. **Примечание** Это уведомление не поддерживается.
Группа: ieeeC37238EventsPropertiesGroup	**Функционал агента:** RC-IEEEC37-238-MIB-AC

Группа/Объект	Описание
Trap-уведомление: ieeeC37238EventOtherProfileDetect	**Идентификатор объекта:** 1.3.111.3.37.238.9999.0.0.6.0 **Определение:** Указывает, что был обнаружен профиль PTP, отличный от C37.238. **Примечание** Это уведомление не поддерживается.
Группа: ieeeC37238EventsPropertiesGroup **Trap-уведомление:** ieeeC37238EventPortStateChange	**Функционал агента:** RC-IEEEC37-238-MIB-AC **Идентификатор объекта:** 1.3.111.3.37.238.9999.0.0.4.0 **Определение:** Указывает, что состояние порта изменилось. **Примечание** Это уведомление не поддерживается.
Группа: ieeeC37238SystemClockParentGroup **Trap-уведомление:** ieeeC37238ParentDSClkIdentity	**Доступ:** Только для чтения **Синтаксическая структура:** ClockIdentity **Идентификатор объекта:** 1.3.111.3.37.238.9999.1.3.1.0 **Определение:** Идентификатор ведущих часов для синхронизации этих часов.
Группа: ieeeC37238SystemClockParentGroup **Trap-уведомление:** ieeeC37238ParentDSGMClkAccuracy	**Доступ:** Только для чтения **Синтаксическая структура:** IEEEC37238ClockAccuracyValue **Идентификатор объекта:** 1.3.111.3.37.238.9999.1.3.8.0 **Определение:** ClockAccuracy гроссмейстерских часов
Группа: ieeeC37238SystemClockParentGroup **Trap-уведомление:** ieeeC37238ParentDSGMClkClass	**Доступ:** Только для чтения **Синтаксическая структура:** IEEEC37238ClockClassValue **Идентификатор объекта:** 1.3.111.3.37.238.9999.1.3.7.0 **Определение:** ClockClass гроссмейстерских часов
Группа: ieeeC37238SystemClockParentGroup **Trap-уведомление:** ieeeC37238ParentDSGMClkIdentity	**Доступ:** Только для чтения **Синтаксическая структура:** ClockIdentity **Идентификатор объекта:** 1.3.111.3.37.238.9999.1.3.6.0 **Определение:** ClockIdentity гроссмейстерских часов
Группа: ieeeC37238SystemClockParentGroup **Trap-уведомление:** ieeeC37238ParentDSGMIdentity	**Доступ:** Только для чтения **Синтаксическая структура:** Integer **Идентификатор объекта:** 1.3.111.3.37.238.9999.1.3.12.0 **Определение:** Идентификатор гроссмейстерских часов, полученный в TLV IEEE_C37_238.
Группа: ieeeC37238SystemClockParentGroup **Trap-уведомление:** ieeeC37238ParentDSGMOfstScdLVar	**Функционал агента:** RC-IEEEC37-238-MIB-AC **Доступ:** Только для чтения **Синтаксическая структура:** Integer **Идентификатор объекта:** 1.3.111.3.37.238.9999.1.3.4.0 **Определение:** Вариация OffsetScaledLog гроссмейстерских часов. **Примечание** Дальнейшая поддержка будет предоставлена. Текущее значение: 65535.

Группа/Объект	Описание
Группа: ieeeC37238SystemClockParentGroup **Trap-уведомление:** ieeeC37238ParentDSGMPriority1	**Доступ:** Только для чтения **Синтаксическая структура:** Gauge32 **Идентификатор объекта:** 1.3.111.3.37.238.9999.1.3.10.0 **Определение:** Атрибут Priority1 гроссмейстерских часов.
Группа: ieeeC37238SystemClockParentGroup **Trap-уведомление:** ieeeC37238ParentDSGMPriority2	**Доступ:** Только для чтения **Синтаксическая структура:** Gauge32 **Идентификатор объекта:** 1.3.111.3.37.238.9999.1.3.11.0 **Определение:** Атрибут Priority2 гроссмейстерских часов.
Группа: ieeeC37238SystemClockParentGroup **Trap-уведомление:** ieeeC37238ParentDSGMTimeInacc	**Функционал агента:** RC-IEEEC37-238-MIB-AC **Доступ:** Только для чтения **Синтаксическая структура:** Gauge32 **Идентификатор объекта:** 1.3.111.3.37.238.9999.1.3.13.0 **Определение:** Значение NetworkTimeInaccuracy, полученное в TLV IEEE_C37_238 в наносекундах. **Примечание** Дальнейшая поддержка будет предоставлена. Текущее значение: 0.
Группа: ieeeC37238SystemClockParentGroup **Trap-уведомление:** ieeeC37238ParentDSNetTimeInacc	**Функционал агента:** RC-IEEEC37-238-MIB-AC **Доступ:** Только для чтения **Синтаксическая структура:** Gauge32 **Идентификатор объекта:** 1.3.111.3.37.238.9999.1.3.14.0 **Определение:** Значение NetworkTimeInaccuracy, полученное в TLV IEEE_C37_238 в наносекундах. **Примечание** Дальнейшая поддержка будет предоставлена. Текущее значение: 0.
Группа: ieeeC37238SystemClockParentGroup **Trap-уведомление:** ieeeC37238ParentDSObsOfstScdLVar	**Функционал агента:** RC-IEEEC37-238-MIB-AC **Доступ:** Только для чтения **Синтаксическая структура:** Gauge32 **Идентификатор объекта:** 1.3.111.3.37.238.9999.1.3.4.0 **Определение:** Оценка отклонения PTP родительских часов, отмеченная ведомыми часами, вычисленная и представленная согласно описанию в стандарте IEEE 1588-2008 7.6.3.5. Значение инициализации должно быть FFFF. **Примечание** Дальнейшая поддержка будет предоставлена. Текущее значение: 65535.
Группа: ieeeC37238SystemClockParentGroup **Trap-уведомление:** ieeeC37238ParentDSObsPhChgRate	**Функционал агента:** RC-IEEEC37-238-MIB-AC **Доступ:** Только для чтения **Синтаксическая структура:** Gauge32 **Идентификатор объекта:** 1.3.111.3.37.238.9999.1.3.5.0 **Определение:** Оценка частоты изменения фазы синхронизации ведущего устройства, отмеченная ведомыми часами согласно

Группа/Объект	Описание
	описанию в стандарте IEEE 1588-2008 7.6.4.4. Если оценка превышает допустимый диапазон типа данных, это значение должно быть установлено на 7FFF FFFF или 8000 0000, в зависимости от ситуации. Знак плюса указывает, что частота изменения фазы синхронизации ведущего устройства больше, чем частота фазы синхронизации ведомого устройства. Значение инициализации должно быть 7FFF FFFF. **Примечание** Дальнейшая поддержка будет предоставлена. Текущее значение: 0x7FFF FFFF.
Группа: ieeeC37238SystemClockParentGroup **Trap-уведомление:** ieeeC37238ParentDSPortNumber	**Доступ:** Только для чтения **Синтаксическая структура:** Gauge32 **Идентификатор объекта:** 1.3.111.3.37.238.9999.1.3.2.0 **Определение:** Номер порта на ведущем устройстве, которое выдает сообщения синхронизации, используемые для синхронизации этих часов.
Группа: ieeeC37238SystemClockParentGroup **Trap-уведомление:** ieeeC37238ParentDSStats	**Функционал агента:** RC-IEEEC37-238-MIB-AC **Доступ:** Только для чтения **Синтаксическая структура:** Integer **Идентификатор объекта:** 1.3.111.3.37.238.9999.1.3.3.0 **Определение:** True (истина), если выполняются оба следующих условия: • Часы имеют порт в состоянии SLAVE (ведомый). • Часы вычислили статистически достоверные оценки отклонения parentDS.observedParentOffsetScaledLog и членов parentDS.observedParentClockPhaseChangeRate. В ином случае – False (ложь). Значение инициализации должно быть FALSE (ложь). **Примечание** Дальнейшая поддержка будет предоставлена. Текущее значение: false (ложь).
Группа: ieeeC37238TCPropertiesGroup **Trap-уведомление:** ieeeC37238TCDefaultDSClkIdentity	**Доступ:** Только для чтения **Синтаксическая структура:** ClockIdentity **Идентификатор объекта:** 1.3.111.3.37.238.9999.1.6.1 **Определение:** Идентификатор локальных часов.
Группа: ieeeC37238TCPropertiesGroup **Trap-уведомление:** ieeeC37238TCDefaultDSCurGMaster	**Доступ:** Только для чтения **Синтаксическая структура:** ClockIdentity **Идентификатор объекта:** 1.3.111.3.37.238.9999.1.6.6 **Определение:** Содержит текущий идентификатор гроссмейстерских часов.
Группа: ieeeC37238TCPropertiesGroup **Trap-уведомление:** ieeeC37238TCDefaultDSDelayMech	**Доступ:** Для чтения и записи **Синтаксическая структура:** Integer **Идентификатор объекта:** 1.3.111.3.37.238.9999.1.6.3 **Определение:** Механизм задержки, используемый устройством. Для реализаций, совместимых с IEEE C37.238, это значение должно быть 2 (p2p).
Группа: ieeeC37238TCPropertiesGroup	**Функционал агента:** RC-IEEEC37-238-MIB-AC

Группа/Объект	Описание
Trap-уведомление: ieeeC37238TCDefaultDSGMIdentity	**Доступ:** не реализован **Синтаксическая структура:** Integer **Идентификатор объекта:** 1.3.111.3.37.238.9999.1.6.8 **Определение:** Идентификатор гроссмейстерских часов, полученный в TLV GRANDMASTER_ID.
Группа: ieeeC37238TCPropertiesGroup **Trap-уведомление:** ieeeC37238TCDefaultDSGMTimeInacc	**Функционал агента:** RC-IEEEC37-238-MIB-AC **Доступ:** Только для чтения **Синтаксическая структура:** Gauge32 **Идентификатор объекта:** 1.3.111.3.37.238.9999.1.6.12 **Определение:** Значение GrandmasterTimeInaccuracy, полученное в TLV IEEE_C37_238. **Примечание** Дальнейшая поддержка будет предоставлена. Текущее значение: 0.
Группа: ieeeC37238TCPropertiesGroup **Trap-уведомление:** ieeeC37238TCDefaultDSLocTimeInacc	**Доступ:** Только для чтения **Синтаксическая структура:** Gauge32 **Идентификатор объекта:** 1.3.111.3.37.238.9999.1.6.14 **Определение:** Вклад TimeInaccuracy локальных часов в наносекундах.
Группа: ieeeC37238TCPropertiesGroup **Trap-уведомление:** ieeeC37238TCDefaultDSNetProtocol	**Доступ:** Для чтения и записи **Синтаксическая структура:** Integer **Идентификатор объекта:** 1.3.111.3.37.238.9999.1.6.9 **Определение:** Указывает используемый сетевой протокол. Для реализаций, совместимых с IEEE C37.238, это значение должно быть 1 (ieee8023).
Группа: ieeeC37238TCPropertiesGroup **Trap-уведомление:** ieeeC37238TCDefaultDSNetTimeInacc	**Функционал агента:** RC-IEEEC37-238-MIB-AC **Доступ:** Только для чтения **Синтаксическая структура:** Gauge32 **Идентификатор объекта:** 1.3.111.3.37.238.9999.1.6.13 **Определение:** Значение NetworkTimeInaccuracy, полученное в TLV IEEE_C37_238. **Примечание** Дальнейшая поддержка будет предоставлена. Текущее значение: 0.
Группа: ieeeC37238TCPropertiesGroup **Trap-уведомление:** ieeeC37238TCDefaultDSNumberPorts	**Доступ:** Только для чтения **Синтаксическая структура:** Gauge32 **Идентификатор объекта:** 1.3.111.3.37.238.9999.1.6.2 **Определение:** Число PTP-портов устройства.
Группа: ieeeC37238TCPropertiesGroup **Trap-уведомление:** ieeeC37238TCDefaultDSPriDomain	**Доступ:** Для чтения и записи **Синтаксическая структура:** Integer **Идентификатор объекта:** 1.3.111.3.37.238.9999.1.6.4 **Определение:** Номер первичного домена синтонизации. Значение инициализации должно быть 0.
Группа: ieeeC37238TCPropertiesGroup	**Доступ:** Для чтения и записи **Синтаксическая структура:** Gauge32

Группа/Объект	Описание
Trap-уведомление: ieeeC37238TCDefaultDSPriority	**Идентификатор объекта:** 1.3.111.3.37.238.9999.1.6.11 **Определение:** Указывает используемый приоритет тега VLAN.
Группа: ieeeC37238TCPropertiesGroup **Trap-уведомление:** ieeeC37238TCDefaultDSSyntonize	**Доступ:** Для чтения и записи **Синтаксическая структура:** Integer **Идентификатор объекта:** 1.3.111.3.37.238.9999.1.6.5 **Определение:** True (истина), если синтонизация включена.
Группа: ieeeC37238TCPropertiesGroup **Trap-уведомление:** ieeeC37238TCDefaultDSTwoStepFlag	**Доступ:** Для чтения и записи **Синтаксическая структура:** Integer **Идентификатор объекта:** 1.3.111.3.37.238.9999.1.6.7 **Определение:** True (истина), если часы являются часами с двухэтапной синхронизацией.
Группа: ieeeC37238TCPropertiesGroup **Trap-уведомление:** ieeeC37238TCDefaultDSVlanId	**Доступ:** Для чтения и записи **Синтаксическая структура:** Gauge32 **Идентификатор объекта:** 1.3.111.3.37.238.9999.1.6.10 **Определение:** Указывает используемый идентификатор VLAN.
Группа: ieeeC37238SystemTimePropGroup **Trap-уведомление:** ieeeC37238TimePropDSCurUTCOfst	**Доступ:** Только для чтения **Синтаксическая структура:** Integer **Идентификатор объекта:** 1.3.111.3.37.238.9999.1.4.1 **Определение:** Текущее смещение между TAI и UTC в секундах.
Группа: ieeeC37238SystemTimePropGroup **Trap-уведомление:** ieeeC37238TimePropDSCurUTCOfstVd	**Доступ:** Только для чтения **Синтаксическая структура:** Integer **Идентификатор объекта:** 1.3.111.3.37.238.9999.1.4.2 **Определение:** True (истина), если известно, что значение currentUtcOffset является верным.
Группа: ieeeC37238SystemTimePropGroup **Trap-уведомление:** ieeeC37238TimePropDSFrqTraceable	**Доступ:** Только для чтения **Синтаксическая структура:** Integer **Идентификатор объекта:** 1.3.111.3.37.238.9999.1.4.6 **Определение:** True (истина), если частота, определяющая шкалу времени, прослеживается до первичного эталона, в ином случае – False (ложь).
Группа: ieeeC37238SystemTimePropGroup **Trap-уведомление:** ieeeC37238TimePropDSLeap59	**Функционал агента:** RC-IEEEC37-238-MIB-AC **Доступ:** Только для чтения **Синтаксическая структура:** Integer **Идентификатор объекта:** 1.3.111.3.37.238.9999.1.4.3 **Определение:** Значение True (истина) указывает, что последняя минута текущего дня UTC содержит 59 секунд. **Примечание** Дальнейшая поддержка будет предоставлена. Текущее значение: false (ложь).
Группа: ieeeC37238SystemTimePropGroup **Trap-уведомление:** ieeeC37238TimePropDSLeap61	**Доступ:** Только для чтения **Синтаксическая структура:** Integer **Идентификатор объекта:** 1.3.111.3.37.238.9999.1.4.4

Группа/Объект	Описание
	Определение: Значение True (истина) указывает, что последняя минута текущего дня UTC содержит 61 секунду.
Группа: ieeeC37238SystemTimePropGroup **Trap-уведомление:** ieeeC37238TimePropDSLeapEvExpiry	**Функционал агента:** RC-IEEEC37-238-MIB-AC **Доступ:** не реализован **Синтаксическая структура:** Integer **Идентификатор объекта:** 1.3.111.3.37.238.9999.1.4.15 **Определение:** Секундная часть времени PTP для истечения последнего объявленного IERS события секунды координации. Если время PTP > LeapEvExpiry, устройство устанавливает значение CurUTCOfstVd на False (ложь).
Группа: ieeeC37238SystemTimePropGroup **Trap-уведомление:** ieeeC37238TimePropDSLeapEvLatest	**Функционал агента:** RC-IEEEC37-238-MIB-AC **Доступ:** не реализован **Синтаксическая структура:** Integer **Идентификатор объекта:** 1.3.111.3.37.238.9999.1.4.13 **Определение:** Секундная часть времени PTP для секунды до последнего объявленного IERS события секунды координации (может быть прошедшей или будущей).
Группа: ieeeC37238SystemTimePropGroup **Trap-уведомление:** ieeeC37238TimePropDSLocalTCurOfs	**Функционал агента:** RC-IEEEC37-238-MIB-AC **Доступ:** не реализован **Синтаксическая структура:** Integer **Идентификатор объекта:** 1.3.111.3.37.238.9999.1.4.9 **Определение:** Смещение альтернативного времени в секундах от времени узла. Альтернативное время – это сумма данного значения и времени узла.
Группа: ieeeC37238SystemTimePropGroup **Trap-уведомление:** ieeeC37238TimePropDSLocalTJumpS	**Функционал агента:** RC-IEEEC37-238-MIB-AC **Доступ:** не реализован **Синтаксическая структура:** Integer **Идентификатор объекта:** 1.3.111.3.37.238.9999.1.4.10 **Определение:** Размер следующего разрыва в значениях альтернативного времени в секундах. Нулевое значение указывает на отсутствие разрыва в значениях. Положительное значение указывает на то, что разрыв в значениях приведет к увеличению currentOffset альтернативного времени.
Группа: ieeeC37238SystemTimePropGroup **Trap-уведомление:** ieeeC37238TimePropDSLocalTName	**Функционал агента:** RC-IEEEC37-238-MIB-AC **Доступ:** не реализован **Синтаксическая структура:** String **Идентификатор объекта:** 1.3.111.3.37.238.9999.1.4.12 **Определение:** Значение displayName должно быть текстовым именем шкалы альтернативного времени.
Группа: ieeeC37238SystemTimePropGroup **Trap-уведомление:** ieeeC37238TimePropDSLocalTNtJump	**Функционал агента:** RC-IEEEC37-238-MIB-AC **Доступ:** не реализован **Синтаксическая структура:** Integer **Идентификатор объекта:** 1.3.111.3.37.238.9999.1.4.11 **Определение:** Значение секундной части времени передающего узла в момент наступления следующего разрыва в значениях. Разрыв в значениях возникает в начале секунды, указанной этим значением.

Группа/Объект	Описание
Группа: ieeeC37238SystemTimePropGroup **Trap-уведомление:** ieeeC37238TimePropDSPTPTimescale	**Доступ:** Только для чтения **Синтаксическая структура:** Integer **Идентификатор объекта:** 1.3.111.3.37.238.9999.1.4.7 **Определение:** True (истина), если шкала времени гроссмейстерских часов является PTP. Для реализаций, совместимых с IEEE C37.238, это значение должно быть True (истина).
Группа: ieeeC37238SystemTimePropGroup **Trap-уведомление:** ieeeC37238TimePropDSTimeSource	**Доступ:** Только для чтения **Синтаксическая структура:** IEEEC37238TimeSourceValue **Идентификатор объекта:** 1.3.111.3.37.238.9999.1.4.8 **Определение:** Источник времени, используемый гроссмейстерскими часами.
Группа: ieeeC37238SystemTimePropGroup **Trap-уведомление:** ieeeC37238TimePropDSTmeTraceable	**Доступ:** Только для чтения **Синтаксическая структура:** Integer **Идентификатор объекта:** 1.3.111.3.37.238.9999.1.4.5 **Определение:** True (истина), если шкала времени и значение currentUtcOffset прослеживаются до первичного эталона; в ином случае – False (ложь).
Группа: ieeeC37238SystemTimePropGroup **Trap-уведомление:** ieeeC37238TimePropDSUTCOfstNext	**Функционал агента:** RC-IEEEC37-238-MIB-AC **Доступ:** не реализован **Синтаксическая структура:** Integer **Идентификатор объекта:** 1.3.111.3.37.238.9999.1.4.14 **Определение:** Секунды смещаются между шкалой TAI и шкалой UTC после LeapEvLatest (аналогично CurUTCOfst после LeapEvLatest).
Группа: ieeeC37238PortDataSetGlobalGroup **Trap-уведомление:** IfIeeeC37238PortDSAnnounceRcTout	**Доступ:** Для чтения и записи **Синтаксическая структура:** Integer **Идентификатор объекта:** 1.3.111.3.37.238.9999.1.5.1.7 **Определение:** При повторной инициализации системы управления и в других случаях, указанных значением ifCounterDiscontinuityTime, могут возникать разрывы в значениях этого счетчика.
Группа: ieeeC37238PortDataSetGlobalGroup **Trap-уведомление:** IfIeeeC37238PortDSClkIdentity	**Доступ:** Только для чтения **Синтаксическая структура:** ClockIdentity **Идентификатор объекта:** 1.3.111.3.37.238.9999.1.5.1.2 **Определение:** Идентификатор локальных часов.
Группа: ieeeC37238PortDataSetGlobalGroup **Trap-уведомление:** IfIeeeC37238PortDSDelayMech	**Доступ:** Для чтения и записи **Синтаксическая структура:** Integer **Идентификатор объекта:** 1.3.111.3.37.238.9999.1.5.1.9 **Определение:** Опция измерения задержки распространения, используемая портом. Для реализаций, совместимых с IEEE C37.238, это значение должно быть 2 (p2p).
Группа: ieeeC37238PortDataSetGlobalGroup **Trap-уведомление:** IfIeeeC37238PortDSDlyAsymmetry	**Функционал агента:** RC-IEEEC37-238-MIB-AC **Доступ:** не реализован **Синтаксическая структура:** Integer **Идентификатор объекта:** 1.3.111.3.37.238.9999.1.5.1.13 **Определение:** Асимметрия задержки распространения сигнала

Группа/Объект	Описание
Группа: ieeeC37238PortDataSetGlobalGroup **Trap-уведомление:** IfIeeeC37238PortDSLogAnnounceInt	**Доступ:** Для чтения и записи **Синтаксическая структура:** Integer **Идентификатор объекта:** 1.3.111.3.37.238.9999.1.5.1.6 **Определение:** Логарифм по основанию 2 среднего announceInterval.
Группа: ieeeC37238PortDataSetGlobalGroup **Trap-уведомление:** IfIeeeC37238PortDSLogMinPdlyRInt	**Доступ:** Для чтения и записи **Синтаксическая структура:** Integer **Идентификатор объекта:** 1.3.111.3.37.238.9999.1.5.1.10 **Определение:** Логарифм по основанию 2 minPdelayReqInterval.
Группа: ieeeC37238PortDataSetGlobalGroup **Trap-уведомление:** IfIeeeC37238PortDSLogSyncInt	**Доступ:** Для чтения и записи **Синтаксическая структура:** Integer **Идентификатор объекта:** 1.3.111.3.37.238.9999.1.5.1.8 **Определение:** Логарифм по основанию 2 среднего SyncInterval для многоадресных сообщений.
Группа: ieeeC37238PortDataSetGlobalGroup **Trap-уведомление:** IfIeeeC37238PortDSMPathPDly	**Доступ:** Только для чтения **Синтаксическая структура:** IEEEC37238TimeInterval **Идентификатор объекта:** 1.3.111.3.37.238.9999.1.5.1.5 **Определение:** Оценка текущей односторонней задержки распространения по каналу связи, подключенному к этому порту, рассчитанная с использованием механизма одноранговой задержки. Значение инициализации должно быть нулем.
Группа: ieeeC37238PortDataSetGlobalGroup **Trap-уведомление:** IfIeeeC37238PortDSNetProtocol	**Доступ:** Для чтения и записи **Синтаксическая структура:** Integer **Идентификатор объекта:** 1.3.111.3.37.238.9999.1.5.1.15 **Определение:** Указывает используемый сетевой протокол. Для реализаций, совместимых с IEEE C37.238, это значение должно быть 1 (ieee8023).
Группа: ieeeC37238PortDataSetGlobalGroup **Trap-уведомление:** IfIeeeC37238PortDSPortNumber	**Доступ:** Только для чтения **Синтаксическая структура:** Gauge32 **Идентификатор объекта:** 1.3.111.3.37.238.9999.1.5.1.3 **Определение:** Номер локального порта.
Группа: ieeeC37238PortDataSetGlobalGroup **Trap-уведомление:** IfIeeeC37238PortDSPortState	**Доступ:** Только для чтения **Синтаксическая структура:** Integer **Идентификатор объекта:** 1.3.111.3.37.238.9999.1.5.1.4 **Определение:** Текущее состояние движка протокола PTP, связанного с этим портом.
Группа: ieeeC37238PortDataSetGlobalGroup **Trap-уведомление:** IfIeeeC37238PortDSPriority	**Доступ:** Для чтения и записи **Синтаксическая структура:** Gauge32 **Идентификатор объекта:** 1.3.111.3.37.238.9999.1.5.1.17 **Определение:** Указывает используемый приоритет тега VLAN.
Группа: ieeeC37238PortDataSetGlobalGroup **Trap-уведомление:** IfIeeeC37238PortDSProfileId	**Доступ:** Для чтения и записи **Синтаксическая структура:** Integer **Идентификатор объекта:** 1.3.111.3.37.238.9999.1.5.1.14 **Определение:** Указывает используемый профиль PTP.

Группа/Объект	Описание
Группа: ieeeC37238PortDataSetGlobalGroup **Trap-уведомление:** IfIeeeC37238PortDSPtpPortEnabled	**Доступ:** Для чтения и записи **Синтаксическая структура:** Integer **Идентификатор объекта:** 1.3.111.3.37.238.9999.1.5.1.12 **Определение:** True (истина), если порт подключен.
Группа: ieeeC37238PortDataSetGlobalGroup **Trap-уведомление:** IfIeeeC37238PortDSVersionNumber	**Доступ:** Только для чтения **Синтаксическая структура:** Gauge32 **Идентификатор объекта:** 1.3.111.3.37.238.9999.1.5.1.11 **Определение:** Используемая версия PTP на порту. Для реализаций, совместимых с IEEE C37.238, это значение должно быть 2.
Группа: ieeeC37238PortDataSetGlobalGroup **Trap-уведомление:** IfIeeeC37238PortDSVlanId	**Доступ:** Для чтения и записи **Синтаксическая структура:** Gauge32 **Идентификатор объекта:** 1.3.111.3.37.238.9999.1.5.1.16 **Определение:** Указывает используемый идентификатор VLAN.
Группа: ieeeC37238TCPortDataSetGroup **Trap-уведомление:** IfIeeeC37238TCPortDSDlyAsymm	**Функционал агента:** RC-IEEEC37-238-MIB-AC **Доступ:** не реализован **Синтаксическая структура:** Integer **Идентификатор объекта:** 1.3.111.3.37.238.9999.1.7.16 Асимметрия задержки распространения сигнала
Группа: ieeeC37238TCPortDataSetGroup **Trap-уведомление:** IfIeeeC37238TCPortDSFaulty	**Функционал агента:** RC-IEEEC37-238-MIB-AC **Доступ:** Только для чтения **Синтаксическая структура:** Integer **Идентификатор объекта:** 1.3.111.3.37.238.9999.1.7.1.4 **Определение:** True (истина), если порт неисправен, и False (ложь), если порт работает нормально. Значение инициализации должно быть False (ложь). **Примечание** Дальнейшая поддержка будет предоставлена. Текущее значение: false (ложь).
Группа: ieeeC37238TCPortDataSetGroup **Trap-уведомление:** IfIeeeC37238TCPortDSLMinPdlyRInt	**Доступ:** Для чтения и записи **Синтаксическая структура:** Integer **Идентификатор объекта:** 1.3.111.3.37.238.9999.1.7.1.3 **Определение:** Логарифм по основанию 2 minPdelayReqInterval.
Группа: ieeeC37238TCPortDataSetGroup **Trap-уведомление:** IfIeeeC37238TCPortDSMPathPDly	**Доступ:** Только для чтения **Синтаксическая структура:** IEEEC37238TimeInterval **Идентификатор объекта:** 1.3.111.3.37.238.9999.1.7.1.5 **Определение:** Оценка текущей задержки одностороннего распространения.
Группа: ieeeC37238TCPortDataSetGroup **Trap-уведомление:** IfIeeeC37238TCPortDSPortNumber	**Доступ:** Только для чтения **Синтаксическая структура:** Gauge32 **Идентификатор объекта:** 1.3.111.3.37.238.9999.1.7.1.2 **Определение:** Номер локального порта.

IF-MIB

Группа/Объект	Описание
Группа: IfGeneralInformationGroup **Trap-уведомление:** IfAdminStatus	**Функционал агента:** RC-IEEEC37-238-MIB-AC **Доступ:** Для чтения и записи **Синтаксическая структура:** Integer **Идентификатор объекта:** .1.3.6.1.2.1.2.2.1.7.1 **Определение:** Желаемый статус интерфейса. Состояние testing(3) указывает на то, что никакие операционные пакеты не могут быть переданы. Когда управляемая система инициализируется, все интерфейсы начинаются с ifAdminStatus в состоянии down(2). В результате либо явного действия системы управления, либо в соответствии с конфигурационной информацией, сохраненной управляемой системой, ifAdminStatus затем изменяется на состояние up(1) или testing(3) (или остается в состоянии down(2)). **Примечание** Поддержка значения testing(3) не реализована в соответствии с заявлением о соответствии RFC 2863.
Группа: IfGeneralInformationGroup **Trap-уведомление:** IfAlias	**Функционал агента:** RC-IF-MIB-AC **Синтаксическая структура:** String **Идентификатор объекта:** .1.3.6.1.2.1.31.1.1.1.18.1 **Определение:** Этот объект является псевдонимом интерфейса, согласно определению менеджера сети, и предоставляет энергонезависимый "дескриптор" для интерфейса. В первом экземпляре интерфейса значение ifAlias, связанное с этим интерфейсом, представляет собой строку нулевой длины. Когда значение записывается в экземпляр ifAlias через операцию набора управления сетью, агент должен сохранять указанное значение в экземпляре ifAlias, связанном с тем же интерфейсом, до тех пор, пока этот интерфейс остается экземпляром, в том числе при всех повторных инициализациях/перезагрузках системы управления сетью, включая те, которые приводят к изменению значения ifIndex интерфейса. Примером значения, которое менеджер сети может хранить в этом объекте для интерфейса WAN, является номер/идентификатор цепи (Telco) интерфейса. Некоторые агенты могут поддерживать доступ на запись только для интерфейсов, имеющих определенные значения ifType. Агент, поддерживающий доступ на запись к этому объекту, необходим для сохранения значения в энергонезависимом хранилище, но он может ограничить длину новых значений в зависимости от того, сколько памяти уже занято текущими значениями для других интерфейсов. **Примечание** Длина строки ограничена 15 символами.
Группа: IfGeneralInformationGroup **Trap-уведомление:** IfConnectorPresent	**Функционал агента:** RC-IF-MIB-AC **Доступ:** Только для чтения **Синтаксическая структура:** Integer **Идентификатор объекта:** .1.3.6.1.2.1.31.1.1.1.17.1 **Определение:** Этот объект имеет значение "true(1)", если подслой интерфейса имеет физический соединитель, и значение "false(2)" в ином случае.

Группа/Объект	Описание
Группа: IfCounterDiscontinuityGroup **Trap-уведомление:** IfCounterDiscontinuityTime	**Доступ:** Только для чтения **Синтаксическая структура:** Timeticks **Идентификатор объекта:** .1.3.6.1.2.1.31.1.1.1.19.1 **Определение:** Значение sysUpTime в последнем случае обнаружения разрывов в значениях для одного или нескольких счетчиков этого интерфейса. Соответствующие счетчики — это конкретные экземпляры, связанные с этим интерфейсом любого Counter32 или
Группа: IfGeneralInformationGroup **Trap-уведомление:** IfDescr	**Доступ:** Только для чтения **Синтаксическая структура:** String **Идентификатор объекта:** .1.3.6.1.2.1.2.2.1.2.1 **Определение:** Текстовая строка, содержащая информацию об интерфейсе Эта строка должна содержать имя производителя, название продукта и версию аппаратного/программного обеспечения интерфейса.
Группа: IfVHCPacketGroup **Trap-уведомление:** IfHCInBroadcastPkts	**Доступ:** Только для чтения **Определение:** Counter64 **Идентификатор объекта:** .1.3.6.1.2.1.31.1.1.1.9.1 **Определение:** Объект Counter64, содержащийся в ifTable или ifXTable. Если с момента последней повторной инициализации локальной подсистемы управления таких разрывов в значениях не возникло, то этот объект содержит нулевое значение.
Группа: IfVHCPacketGroup **Trap-уведомление:** IfHCInMulticastPkts	**Доступ:** Только для чтения **Определение:** Counter64 **Идентификатор объекта:** .1.3.6.1.2.1.31.1.1.1.8.1 **Определение:** Количество пакетов, доставленных этим подуровнем на более высокий уровень (подуровень), которые были адресованы на групповой адрес на этом подуровне. Для протокола уровня MAC это включает как групповые, так и функциональные адреса. Этот объект является 64-разрядной версией ifInMulticastPkts. При повторной инициализации системы управления и в других случаях, указанных значением ifCounterDiscontinuityTime, могут возникать разрывы в значениях этого счетчика.
Группа: IfVHCPacketGroup **Trap-уведомление:** IfHCInOctets	**Доступ:** Только для чтения **Определение:** Counter64 **Идентификатор объекта:** .1.3.6.1.2.1.31.1.1.1.6.1 **Определение:** Общее количество октетов, полученных на интерфейсе, включая символы кадровой синхронизации. Этот объект является 64-разрядной версией ifInOctets. При повторной инициализации системы управления и в других случаях, указанных значением ifCounterDiscontinuityTime, могут возникать разрывы в значениях этого счетчика.
Группа: IfVHCPacketGroup **Trap-уведомление:** IfHCInUcastPkts	**Доступ:** Только для чтения **Определение:** Counter64 **Идентификатор объекта:** .1.3.6.1.2.1.31.1.1.1.7.1 **Определение:** Количество пакетов, доставленных этим подуровнем на более высокий уровень (подуровень), которые не были адресованы на групповой или широковещательный адрес на этом подуровне. Этот объект является 64-разрядной версией ifInUcastPkts. При повторной инициализации системы управления и в других случаях, указанных

Группа/Объект	Описание
	значением ifCounterDiscontinuityTime, могут возникать разрывы в значениях этого счетчика.
Группа: IfVHCPacketGroup **Trap-уведомление:** IfHCOutBroadcastPkts	**Доступ:** Только для чтения **Определение:** Counter64 **Идентификатор объекта:** .1.3.6.1.2.1.31.1.1.1.13.1 **Определение:** Общее количество пакетов, которые запрашиваются протоколами более высокого уровня и которые были адресованы на широковещательный адрес на этом подуровне, включая те, которые были отброшены или не отправлены. Этот объект является 64-разрядной версией ifOutBroadcastPkts. При повторной инициализации системы управления и в других случаях, указанных значением ifCounterDiscontinuityTime, могут возникать разрывы в значениях этого счетчика.
Группа: IfVHCPacketGroup **Trap-уведомление:** IfHCOutMulticastPkts	**Доступ:** Только для чтения **Определение:** Counter64 **Идентификатор объекта:** .1.3.6.1.2.1.31.1.1.1.12.1 **Определение:** Общее количество пакетов, которые запрашиваются протоколами более высокого уровня и которые были адресованы на групповой адрес на этом подуровне, включая те, которые были отброшены или не отправлены. Для протокола уровня MAC это включает как групповые, так и функциональные адреса. Этот объект является 64-разрядной версией IfOutMulticastPkts. При повторной инициализации системы управления и в других случаях, указанных значением ifCounterDiscontinuityTime, могут возникать разрывы в значениях этого счетчика.
Группа: IfVHCPacketGroup **Trap-уведомление:** IfHCOutOctets	**Доступ:** Только для чтения **Определение:** Counter64 **Идентификатор объекта:** .1.3.6.1.2.1.31.1.1.1.10.1 **Определение:** Общее количество октетов, передаваемых из интерфейса, включая символы кадровой синхронизации. Этот объект является 64-разрядной версией ifOutOctets.
Группа: IfVHCPacketGroup **Trap-уведомление:** IfHCOutUcastPkts	**Доступ:** Только для чтения **Определение:** Counter64 **Идентификатор объекта:** .1.3.6.1.2.1.31.1.1.1.11.1 **Определение:** Общее количество пакетов, которые запрашиваются протоколами более высокого уровня и которые не были адресованы на групповой или широковещательный адрес на этом подуровне, включая те, которые были отброшены или не отправлены. Этот объект является 64-разрядной версией IfOutUcastPkts.
Группа: IfGeneralInformationGroup **Trap-уведомление:** IfHighSpeed	**Доступ:** Только для чтения **Синтаксическая структура:** Gauge32 **Идентификатор объекта:** .1.3.6.1.2.1.31.1.1.1.15.1 **Определение:** Оценка текущей пропускной способности интерфейса в единицах измерения 1 000 000 битов в секунду. Если этот объект сообщает значение "n", то скорость интерфейса находится приблизительно в диапазоне от "n-500 000" до "n+499 999". Для интерфейсов, которые не отличаются по ширине полосы пропускания или для интерфейсов, для которых невозможно произвести точную оценку, этот объект должен содержать номинальную ширину полосы

Группа/Объект	Описание
	пропускания. Для подуровня, который не содержит понятие полосы пропускания, этот объект должен быть равен нулю.
Группа: IfVHCPacketGroup **Trap-уведомление:** IfInBroadcastPkts	**Доступ:** Только для чтения **Синтаксическая структура:** Counter32 **Идентификатор объекта:** .1.3.6.1.2.1.31.1.1.1.3.1 **Определение:** Количество пакетов, доставленных этим подуровнем на более высокий уровень (подуровень), которые были адресованы на широковещательный адрес на этом подуровне. При повторной инициализации системы управления и в других случаях, указанных значением ifCounterDiscontinuityTime, могут возникать разрывы в значениях этого счетчика.
Группа: IfGeneralInformationGroup **Trap-уведомление:** IfIndex	**Функционал агента:** RC-IEEEC37-238-MIB-AC **Доступ:** Только для чтения **Синтаксическая структура:** Integer **Идентификатор объекта:** .1.3.6.1.2.1.2.2.1.1.1 **Определение:** Уникальное значение больше нуля для каждого интерфейса. Рекомендуется присваивать значения непрерывно, начиная с 1. Значение для каждого подуровня интерфейса должно оставаться постоянным, по крайней мере, от одной повторной инициализации системы управления сетью объекта до следующей повторной инициализации. **Примечание** Создание и удаление записи в ifTable не поддерживается.
Группа: IfVHCPacketGroup **Trap-уведомление:** IfInDiscards	**Доступ:** Только для чтения **Синтаксическая структура:** Counter32 **Идентификатор объекта:** .1.3.6.1.2.1.2.2.1.13.1 **Определение:** Количество входящих пакетов, которые были выбраны для удаления, даже если не было обнаружено ошибок, чтобы помешать их доставке в протокол более высокого уровня. Одной из возможных причин отказа от такого пакета может быть высвобождение буферного пространства. При повторной инициализации системы управления и в других случаях, указанных значением ifCounterDiscontinuityTime, могут возникать разрывы в значениях этого счетчика.
Группа: IfVHCPacketGroup **Trap-уведомление:** IfInErrors	**Доступ:** Только для чтения **Синтаксическая структура:** Counter32 **Идентификатор объекта:** .1.3.6.1.2.1.2.2.1.14.1 **Определение:** Для пакетно-ориентированных интерфейсов — количество входящих пакетов, содержащих ошибки, препятствующие их доставке в протокол более высокого уровня. Для интерфейсов, ориентированных на символы или фиксированную длину, — количество входящих блоков передачи, содержащих ошибки, препятствующие их доставке в протокол более высокого уровня. При повторной инициализации системы управления и в других случаях, указанных значением ifCounterDiscontinuityTime, могут возникать разрывы в значениях этого счетчика.
Группа: IfVHCPacketGroup **Trap-уведомление:** IfInMulticastPkts	**Доступ:** Только для чтения **Синтаксическая структура:** Counter32 **Идентификатор объекта:** .1.3.6.1.2.1.31.1.1.1.2.1

Группа/Объект	Описание
	Определение: Количество пакетов, доставленных этим подуровнем на более высокий уровень (подуровень), которые были адресованы на групповой адрес на этом подуровне. Для протокола уровня MAC это включает как групповые, так и функциональные адреса. При повторной инициализации системы управления и в других случаях, указанных значением ifCounterDiscontinuityTime, могут возникать разрывы в значениях этого счетчика.
Группа: IfVHCPacketGroup **Trap-уведомление:** IfInOctets	**Доступ:** Только для чтения **Синтаксическая структура:** Counter32 **Идентификатор объекта:** .1.3.6.1.2.1.2.2.1.10.1 **Определение:** Общее количество октетов, полученных на интерфейсе, включая символы кадровой синхронизации. При повторной инициализации системы управления и в других случаях, указанных значением ifCounterDiscontinuityTime, могут возникать разрывы в значениях этого счетчика.
Группа: IfVHCPacketGroup **Trap-уведомление:** IfInUcastPkts	**Доступ:** Только для чтения **Синтаксическая структура:** Counter32 **Идентификатор объекта:** .1.3.6.1.2.1.2.2.1.11.1 **Определение:** Количество пакетов, доставленных этим подуровнем на более высокий уровень (подуровень), которые не были адресованы на групповой или широковещательный адрес на этом подуровне. При повторной инициализации системы управления и в других случаях, указанных значением ifCounterDiscontinuityTime, могут возникать разрывы в значениях этого счетчика.
Группа: IfVHCPacketGroup **Trap-уведомление:** IfInUnknownProtos	**Доступ:** Только для чтения **Синтаксическая структура:** Counter32 **Идентификатор объекта:** .1.3.6.1.2.1.2.2.1.15.1 **Определение:** Для пакетно-ориентированных интерфейсов — количество пакетов, полученных через интерфейс, которые были отброшены из-за неизвестного или неподдерживаемого протокола. Для интерфейсов, ориентированных на символы, или интерфейсов фиксированной длины, поддерживающих мультиплексирование протоколов, количество блоков передачи, принятых через интерфейс, которые были отброшены из-за неизвестного или неподдерживаемого протокола. Для любого интерфейса, который не поддерживает мультиплексирование протоколов, этот счетчик всегда будет равен 0. При повторной инициализации системы управления и в других случаях, указанных значением ifCounterDiscontinuityTime, могут возникать разрывы в значениях этого счетчика.
Группа: IfGeneralInformationGroup **Trap-уведомление:** IfLastChange	**Доступ:** Только для чтения **Синтаксическая структура:** Timeticks **Идентификатор объекта:** .1.3.6.1.2.1.2.2.1.9.1 **Определение:** Значение sysUpTime на момент перехода интерфейса в текущее рабочее состояние. Если текущее состояние было введено до последней повторной инициализации подсистемы управления локальной сетью, то этот объект содержит нулевое значение.
Группа: IfGeneralInformationGroup **Trap-уведомление:** IfLinkUpDownTrapEnable	**Доступ:** Для чтения и записи **Синтаксическая структура:** Integer **Идентификатор объекта:** .1.3.6.1.2.1.31.1.1.1.14.1

Группа/Объект	Описание
	Определение: Указывает, следует ли создавать ловушки linkUp/linkDown для этого интерфейса. По умолчанию этот объект должен иметь значение enabled(1) для интерфейсов, которые не работают поверх любого другого интерфейса (как определено в ifStackTable), в противном случае — значение disabled(2).
Группа: IfVHCPacketGroup **Trap-уведомление:** IfMtu	**Доступ:** Только для чтения **Синтаксическая структура:** Integer **Идентификатор объекта:** .1.3.6.1.2.1.2.2.1.4.1 **Определение:** Размер самого большого пакета, который может быть отправлен/принят на интерфейсе, указанный в октетах. Для интерфейсов, которые используются для передачи сетевых датаграмм, это размер самой большой сетевой датаграммы, которая может быть отправлена на интерфейс.
Группа: IfGeneralInformationGroup **Trap-уведомление:** IfName	**Доступ:** Только для чтения **Синтаксическая структура:** String **Идентификатор объекта:** .1.3.6.1.2.1.31.1.1.1.1.1 **Определение:** Текстовое имя интерфейса. Значением этого объекта должно быть имя интерфейса, присвоенное локальным устройством, и должно быть пригодно для использования в командах, вводимых на "консоли" устройства. Это может быть текстовое имя, например, "le0" или простой номер порта, например "1", в зависимости от синтаксиса именования интерфейса устройства. Если несколько записей в ifTable вместе представляют один интерфейс с именем устройства, то каждая из них будет иметь одинаковое значение ifName. Обратите внимание, что для агента, который отвечает на SNMP-запросы относительно интерфейса на каком-либо другом (проксированном) устройстве, значение ifName для такого интерфейса является локальным именем проксированного устройства для него. Если локального имени нет или этот объект не применим иным образом, то этот объект содержит строку нулевой длины.
Группа: IfGeneralInformationGroup **Trap-уведомление:** IfNumber	**Доступ:** Только для чтения **Синтаксическая структура:** Integer **Идентификатор объекта:** .1.3.6.1.2.1.2.1.0 **Определение:** Количество сетевых интерфейсов (независимо от их текущего состояния), присутствующих в этой системе.
Группа: IfGeneralInformationGroup **Trap-уведомление:** IfOperStatus	**Функционал агента:** RC-IF-MIB-AC **Доступ:** Только для чтения **Синтаксическая структура:** Integer **Идентификатор объекта:** .1.3.6.1.2.1.2.2.1.8.1 **Определение:** Текущее рабочее состояние интерфейса. Состояние testing(3) указывает на то, что никакие операционные пакеты не могут быть переданы. Если ifAdminStatus находится в состоянии down(2), то ifOperStatus должен быть в состоянии down(2). Если ifAdminStatus изменен на up(1), то ifOperStatus должен измениться на up(1), если интерфейс готов к передаче и приему сетевого трафика; он должен измениться на dormant(5), если интерфейс ожидает внешних действий (например, последовательная линия ожидает входящего соединения); он должен оставаться в состоянии down(2), если и только если есть неисправность, которая мешает ему перейти в состояние up(1); он должен оставаться в состоянии notPresent(6), если интерфейс имеет отсутствующие (обычно аппаратные) компоненты.

Группа/Объект	Описание
	Примечание Информация, ограниченная агентом Rugged Switch для объекта только для чтения.
Группа: IfVHCPacketGroup **Trap-уведомление:** IfOutBroadcastPkts	**Доступ:** Только для чтения **Синтаксическая структура:** Counter32 **Идентификатор объекта:** .1.3.6.1.2.1.31.1.1.1.5.1 **Определение:** Общее количество пакетов, которые запрашиваются протоколами более высокого уровня и которые были адресованы на широковещательный адрес на этом подуровне, включая те, которые были отброшены или не отправлены. При повторной инициализации системы управления и в других случаях, указанных значением ifCounterDiscontinuityTime, могут возникать разрывы в значениях этого счетчика.
Группа: IfVHCPacketGroup **Trap-уведомление:** IfOutDiscards	**Доступ:** Только для чтения **Синтаксическая структура:** Counter32 **Идентификатор объекта:** .1.3.6.1.2.1.2.2.1.19.1 **Определение:** Количество исходящих пакетов, которые были выбраны для удаления, даже если не было обнаружено ошибок для предотвращения их передачи. Одной из возможных причин отказа от такого пакета может быть высвобождение буферного пространства. При повторной инициализации системы управления и в других случаях, указанных значением ifCounterDiscontinuityTime, могут возникать разрывы в значениях этого счетчика.
Группа: IfVHCPacketGroup **Trap-уведомление:** IfOutErrors	**Доступ:** Только для чтения **Синтаксическая структура:** Counter32 **Идентификатор объекта:** .1.3.6.1.2.1.2.2.1.20.1 **Определение:** Для пакетно-ориентированных интерфейсов — количество исходящих пакетов, которые не удалось передать из-за ошибок. Для интерфейсов, ориентированных на символы или фиксированную длину, — количество исходящих блоков передачи, которые не могут быть переданы из-за ошибок. При повторной инициализации системы управления и в других случаях, указанных значением ifCounterDiscontinuityTime, могут возникать разрывы в значениях этого счетчика.
Группа: IfVHCPacketGroup **Trap-уведомление:** IfOutMulticastPkts	**Доступ:** Только для чтения **Синтаксическая структура:** Counter32 **Идентификатор объекта:** .1.3.6.1.2.1.31.1.1.1.4.1 **Определение:** Общее количество пакетов, которые запрашиваются протоколами более высокого уровня и которые были адресованы на групповой адрес на этом подуровне, включая те, которые были отброшены или не отправлены. Для протокола уровня MAC это включает как групповые, так и функциональные адреса. При повторной инициализации системы управления и в других случаях, указанных значением ifCounterDiscontinuityTime, могут возникать разрывы в значениях этого счетчика.
Группа: IfVHCPacketGroup **Trap-уведомление:** IfOutOctets	**Доступ:** Только для чтения **Синтаксическая структура:** Counter32 **Идентификатор объекта:** .1.3.6.1.2.1.2.2.1.16.1

Группа/Объект	Описание
	Определение: Общее количество октетов, передаваемых из интерфейса, включая символы кадровой синхронизации. При повторной инициализации системы управления и в других случаях, указанных значением ifCounterDiscontinuityTime, могут возникать разрывы в значениях этого счетчика.
Группа: IfVHCPacketGroup **Trap-уведомление:** IfOutUcastPkts	**Доступ:** Только для чтения **Синтаксическая структура:** Counter32 **Идентификатор объекта:** .1.3.6.1.2.1.2.2.1.17.1 **Определение:** Общее количество пакетов, которые запрашиваются протоколами более высокого уровня и которые не были адресованы на групповой или широковещательный адрес на этом подуровне, включая те, которые были отброшены или не отправлены. При повторной инициализации системы управления и в других случаях, указанных значением ifCounterDiscontinuityTime, могут возникать разрывы в значениях этого счетчика.
Группа: IfGeneralInformationGroup **Trap-уведомление:** IfPhysAddress	**Доступ:** Только для чтения **Синтаксическая структура:** PhysAddress **Идентификатор объекта:** .1.3.6.1.2.1.2.2.1.6.1 **Определение:** Адрес интерфейса на подуровне протокола. Например, для интерфейса 802.x этот объект обычно содержит MAC-адрес. MIB интерфейса, зависящий от носителя, должен определять порядок битов и байтов и формат значения этого объекта. Для интерфейсов, не имеющих такого адреса (например, последовательной линии), этот объект должен содержать октетную строку нулевой длины.
Группа: IfVHCPacketGroup **Trap-уведомление:** IfPromiscuousMode	**Функционал агента:** RC-IF-MIB-AC **Доступ:** Только для чтения **Синтаксическая структура:** Integer **Идентификатор объекта:** .1.3.6.1.2.1.31.1.1.1.16.1 **Определение:** Этот объект имеет значение false(2), если этот интерфейс принимает только пакеты/кадры, адресованные этой станции. Этот объект имеет значение true(1), когда станция принимает все пакеты/кадры, переданные на носителе. Значение true(1) является законным только для определенных типов носителей. Если это законно, установка этого объекта на значение true(1) может потребовать сброса интерфейса перед вступлением в силу. Значение ifPromiscuousMode не влияет на прием широковещательных и групповых пакетов/кадров интерфейсом. **Примечание** Доступ для записи не реализован в соответствии с заявлением о соответствии RFC 2863. Этот режим всегда "false(1)".
Группа: IfGeneralInformationGroup **Trap-уведомление:** IfSpeed	**Функционал агента:** RC-IF-MIB-AC **Доступ:** Только для чтения **Синтаксическая структура:** Integer **Идентификатор объекта:** .1.3.6.1.2.1.2.2.1.5.1 **Определение:** Оценка текущей пропускной способности интерфейса в битах в секунду. Для интерфейсов, которые не отличаются по ширине полосы пропускания или для интерфейсов, для которых невозможно произвести точную оценку, этот объект должен содержать номинальную ширину полосы пропускания. Если ширина полосы

Группа/Объект	Описание
	пропускания интерфейса превышает максимальное значение, сообщаемое этим объектом, то этот объект должен сообщать свое максимальное значение (4 294 967 295), а ifHighSpeed должен использоваться для сообщения скорости интерфейса. Для подуровня, который не содержит понятие полосы пропускания, этот объект должен быть равен нулю.
Группа: IfGeneralInformationGroup **Trap-уведомление:** IfTableLastChange	**Функционал агента:** RC-IF-MIB-AC **Доступ:** Только для чтения **Синтаксическая структура:** Timeticks **Идентификатор объекта:** .1.3.6.1.2.1.31.1.5.0 **Определение:** Значение sysUpTime на момент последнего создания или удаления записи в ifTable. Если количество записей не изменилось с момента последней повторной инициализации подсистемы управления локальной сетью, то этот объект содержит нулевое значение.
Группа: IfGeneralInformationGroup **Trap-уведомление:** IfType	**Функционал агента:** RC-IP-MIB-AC **Доступ:** Только для чтения **Синтаксическая структура:** Integer **Идентификатор объекта:** .1.3.6.1.2.1.2.2.1.3.1 **Определение:** Тип интерфейса. Дополнительные значения для ifType присваиваются Администрацией адресного пространства Интернет (IANA) путем обновления синтаксиса текстового соглашения IANAifType.

IP-MIB

Группа/Объект	Описание
Группа: icmpGroup **Trap-уведомление:** icmpInAddrMaskReps	**Доступ:** Только для чтения **Синтаксическая структура:** Counter32 **Идентификатор объекта:** .1.3.6.1.2.1.5.13 **Определение:** Количество полученных ICMP-сообщений Address Mask Reply (ответ на запрос маски сети).
Группа: icmpGroup **Trap-уведомление:** icmpInAddrMasks	**Доступ:** Только для чтения **Синтаксическая структура:** Counter32 **Идентификатор объекта:** .1.3.6.1.2.1.5.12 **Определение:** Количество полученных ICMP-сообщений Address Mask Request (запрос маски сети).
Группа: icmpGroup **Trap-уведомление:** icmpInDestUnreachs	**Доступ:** Только для чтения **Синтаксическая структура:** Counter32 **Идентификатор объекта:** .1.3.6.1.2.1.5.3 **Определение:** Количество полученных ICMP-сообщений Destination Unreachable (цель недоступна).
Группа: icmpGroup **Trap-уведомление:** icmpInEchoReps	**Доступ:** Только для чтения **Синтаксическая структура:** Counter32 **Идентификатор объекта:** .1.3.6.1.2.1.5.9

Группа/Объект	Описание
	Определение: Количество полученных ICMP-сообщений Echo Reply (эхо-ответ).
Группа: icmpGroup **Trap-уведомление:** icmpInEchos	**Доступ:** Только для чтения **Синтаксическая структура:** Counter32 **Идентификатор объекта:** .1.3.6.1.2.1.5.8 **Определение:** Количество полученных ICMP-сообщений Echo (request) (эхо-запрос).
Группа: icmpGroup **Trap-уведомление:** icmpInErrors	**Доступ:** Только для чтения **Синтаксическая структура:** Counter32 **Идентификатор объекта:** .1.3.6.1.2.1.5.2 **Определение:** Количество ICMP-сообщений, которые объект получил, но определил как имеющие специфические для ICMP ошибки (неправильные контрольные суммы ICMP, неправильная длина и т. д.).
Группа: icmpGroup **Trap-уведомление:** icmpInMsgs	**Доступ:** Только для чтения **Синтаксическая структура:** Counter32 **Идентификатор объекта:** .1.3.6.1.2.1.5.1 **Определение:** Общее количество ICMP-сообщений, полученных объектом. Обратите внимание, что этот счетчик включает все подсчитанные icmpInErrors.
Группа: icmpGroup **Trap-уведомление:** icmpInParmProbs	**Доступ:** Только для чтения **Синтаксическая структура:** Counter32 **Идентификатор объекта:** .1.3.6.1.2.1.5.5 **Определение:** Количество полученных ICMP-сообщений Parameter Problem (проблема с параметром).
Группа: icmpGroup **Trap-уведомление:** icmpInRedirects	**Доступ:** Только для чтения **Синтаксическая структура:** Counter32 **Идентификатор объекта:** .1.3.6.1.2.1.5.7 **Определение:** Количество полученных ICMP-сообщений Redirect (перенаправление).
Группа: icmpGroup **Trap-уведомление:** icmpInSrcQuenchs	**Доступ:** Только для чтения **Синтаксическая структура:** Counter32 **Идентификатор объекта:** .1.3.6.1.2.1.5.6 **Определение:** Количество полученных ICMP-сообщений Time Exceeded (время истекло).
Группа: icmpGroup **Trap-уведомление:** icmpInTimeExcds	**Доступ:** Только для чтения **Синтаксическая структура:** Counter32 **Идентификатор объекта:** .1.3.6.1.2.1.5.4 **Определение:** Количество полученных ICMP-сообщений Timestamp Reply (ответ на запрос значения счетчика времени).
Группа: icmpGroup **Trap-уведомление:** icmpInTimestampReps	**Доступ:** Только для чтения **Синтаксическая структура:** Counter32 **Идентификатор объекта:** .1.3.6.1.2.1.5.11 **Определение:** Количество полученных ICMP-сообщений Timestamp Reply (ответ на запрос значения счетчика времени).
Группа: icmpGroup	**Доступ:** Только для чтения

Группа/Объект	Описание
Trap-уведомление: icmpInTimestamps	**Синтаксическая структура:** Counter32 **Идентификатор объекта:** .1.3.6.1.2.1.5.10 **Определение:** Количество полученных ICMP-сообщений Timestamp (request) (запрос значения счетчика времени).
Группа: icmpGroup **Trap-уведомление:** icmpOutAddrMaskReps	**Доступ:** Только для чтения **Синтаксическая структура:** Counter32 **Идентификатор объекта:** .1.3.6.1.2.1.5.26 **Определение:** Количество отправленных ICMP-сообщений Address Mask Reply (ответ на запрос маски сети).
Группа: icmpGroup **Trap-уведомление:** icmpOutDestUnreachs	**Доступ:** Только для чтения **Синтаксическая структура:** Counter32 **Идентификатор объекта:** .1.3.6.1.2.1.5.16 **Определение:** Количество отправленных ICMP-сообщений Destination Unreachable (цель недоступна).
Группа: icmpGroup **Trap-уведомление:** icmpOutEchoReps	**Доступ:** Только для чтения **Синтаксическая структура:** Counter32 **Идентификатор объекта:** .1.3.6.1.2.1.5.22 **Определение:** Количество отправленных ICMP-сообщений Echo Reply (эхо-ответ).
Группа: icmpGroup **Trap-уведомление:** icmpOutErrors	**Доступ:** Только для чтения **Синтаксическая структура:** Counter32 **Идентификатор объекта:** .1.3.6.1.2.1.5.15 **Определение:** Количество ICMP-сообщений, которые этот объект не отправил из-за проблем, обнаруженных в ICMP, таких как отсутствие буферов. Это значение не должно включать ошибки, обнаруженные за пределами уровня ICMP, такие как неспособность IP маршрутизировать результирующую датаграмму. В некоторых вариантах реализации могут отсутствовать типы ошибок, которые обеспечивают значение этого счетчика.
Группа: icmpGroup **Trap-уведомление:** icmpOutMsgs	**Доступ:** Только для чтения **Синтаксическая структура:** Counter32 **Идентификатор объекта:** .1.3.6.1.2.1.5.14 **Определение:** Общее количество ICMP-сообщений, которые этот объект пытался отправить. Обратите внимание, что этот счетчик включает все подсчитанные icmpOutErrors.
Группа: icmpGroup **Trap-уведомление:** icmpOutParmProbs	**Доступ:** Только для чтения **Синтаксическая структура:** Counter32 **Идентификатор объекта:** .1.3.6.1.2.1.5.18 **Определение:** Количество отправленных ICMP-сообщений Parameter Problem (проблема с параметром).
Группа: icmpGroup **Trap-уведомление:** icmpOutRedirects	**Доступ:** Только для чтения **Синтаксическая структура:** Counter32 **Идентификатор объекта:** .1.3.6.1.2.1.5.20 **Определение:** Количество отправленных ICMP-сообщений Redirect (перенаправление). Для хоста этот объект всегда будет равен нулю, так как хосты не отправляют сообщения о перенаправлении.

Группа/Объект	Описание
Группа: icmpGroup **Trap-уведомление:** icmpOutSrcQuenchs	**Доступ:** Только для чтения **Синтаксическая структура:** Counter32 **Идентификатор объекта:** .1.3.6.1.2.1.5.19 **Определение:** Количество отправленных ICMP-сообщений Source Quench (сдерживание источника).
Группа: icmpGroup **Trap-уведомление:** icmpOutTimeExcds	**Доступ:** Только для чтения **Синтаксическая структура:** Counter32 **Идентификатор объекта:** .1.3.6.1.2.1.5.17 **Определение:** Количество отправленных ICMP-сообщений Time Exceeded (время истекло).
Группа: icmpGroup **Trap-уведомление:** icmpOutTimestampReps	**Доступ:** Только для чтения **Синтаксическая структура:** Counter32 **Идентификатор объекта:** .1.3.6.1.2.1.5.24 **Определение:** Количество отправленных ICMP-сообщений Timestamp Reply (ответ на запрос значения счетчика времени).
Группа: icmpGroup **Trap-уведомление:** icmpOutTimestamps	**Доступ:** Только для чтения **Синтаксическая структура:** Counter32 **Идентификатор объекта:** .1.3.6.1.2.1.5.23 **Определение:** Количество отправленных ICMP-сообщений Timestamp (request) (запрос значения счетчика времени).
Группа: ipGroup **Trap-уведомление:** ipAdEntAddr	**Доступ:** Только для чтения **Синтаксическая структура:** IpAddress **Идентификатор объекта:** .1.3.6.1.2.1.4.20.1.1.192.168.0.180 **Определение:** IP-адрес, к которому относится адресная информация этой записи.
Группа: ipGroup **Trap-уведомление:** ipAdEntBcastAddr	**Доступ:** Только для чтения **Синтаксическая структура:** Integer **Идентификатор объекта:** .1.3.6.1.2.1.4.20.1.4.192.168.0.180 **Определение:** Значение наименее значимого бита в IP-адресе широковещательной передачи, используемое для отправки датаграмм на (логический) интерфейс, связанный с IP-адресом этой записи. Например, при использовании стандартного широковещательного адреса Интернета all-ones значение будет равно 1. Это значение относится как к подсети, так и к сетевым широковещательным адресам, используемым объектом в этом (логическом) интерфейсе.
Группа: ipGroup **Trap-уведомление:** ipAdEntIfIndex	**Доступ:** Только для чтения **Синтаксическая структура:** Integer **Идентификатор объекта:** .1.3.6.1.2.1.4.20.1.2.192.168.0.180 **Определение:** Значение индекса, которое однозначно идентифицирует интерфейс, к которому применима эта запись. Интерфейс, идентифицированный конкретным значением этого индекса, представляет собой тот же интерфейс, идентифицированный тем же значением индекса ifIndex RFC 1573.
Группа: ipGroup **Trap-уведомление:** ipAdEntNetMask	**Доступ:** Только для чтения **Синтаксическая структура:** IpAddress **Идентификатор объекта:** .1.3.6.1.2.1.4.20.1.3.192.168.0.180

Группа/Объект	Описание
	Определение: Маска подсети, связанная с IP-адресом этой записи. Маска представляет собой IP-адрес со значениями всех сетевых битов, установленными на 1, и значениями всех битов хостов, установленными на 0.
Группа: ipGroup **Trap-уведомление:** ipAdEntReasmMaxSize	**Доступ:** Только для чтения **Синтаксическая структура:** Integer **Идентификатор объекта:** .1.3.6.1.2.1.4.20.1.5.192.168.0.180 **Определение:** Размер самой большой IP-датаграммы, которую этот объект может повторно собрать из входящих IP-фрагментированных датаграмм, полученных на этом интерфейсе.
Группа: ipGroup **Trap-уведомление:** ipDefaultTTL	**Функционал агента:** RC-IP-MIB-AC **Доступ:** Только для чтения **Синтаксическая структура:** Integer **Идентификатор объекта:** .1.3.6.1.2.1.4.2.0 **Определение:** Значение по умолчанию, вставленное в поле Time-To-Live заголовка IP датаграмм, происходящих от этого объекта, когда значение TTL не указано протоколом транспортного уровня. **Примечание** Доступ для записи не поддерживается.
Группа: ipGroup **Trap-уведомление:** ipForwarding	**Функционал агента:** RC-IP-MIB-AC **Доступ:** Для чтения и записи **Синтаксическая структура:** Integer **Идентификатор объекта:** .1.3.6.1.2.1.4.1.0 **Определение:** Указание того, действует ли этот объект в качестве IP-маршрутизатора в отношении пересылки датаграмм, полученных этим объектом, но не адресованных ему. IP-маршрутизаторы пересылают датаграммы. IP-хосты — нет (кроме тех, которые направляются по источнику через хост). **Примечание** Поддержка значения "forwarding(1)" не реализована в соответствии с RFC 2011.
Группа: ipGroup **Trap-уведомление:** ipForwDatagrams	**Доступ:** Только для чтения **Синтаксическая структура:** Counter32 **Идентификатор объекта:** .1.3.6.1.2.1.4.6.0 **Определение:** Количество входных датаграмм, для которых данный объект не является конечным IP-получателем, в результате чего была предпринята попытка найти маршрут для их пересылки в конечный пункт назначения. В объектах, которые не выступают в качестве IP-маршрутизаторов, этот счетчик будет включать только те пакеты, которые были перенаправлены через этот объект, и обработка опции маршрутизации от источника выполнена успешно.
Группа: ipGroup **Trap-уведомление:** ipFragCreates	**Доступ:** Только для чтения **Синтаксическая структура:** Counter32 **Идентификатор объекта:** .1.3.6.1.2.1.4.19.0

Группа/Объект	Описание
	Определение: Количество фрагментов IP-датаграммы, сгенерированных в результате фрагментации на этом объекте.
Группа: ipGroup **Trap-уведомление:** ipFragFails	**Доступ:** Только для чтения **Синтаксическая структура:** Counter32 **Идентификатор объекта:** .1.3.6.1.2.1.4.18.0 **Определение:** Количество IP-датаграмм, которые были отброшены, поскольку они должны были быть фрагментированы в этом объекте, но не могли быть фрагментированы, например, потому, что был установлен флажок "Don 't Fragment" (не фрагментировать).
Группа: ipGroup **Trap-уведомление:** ipFragOKs	**Доступ:** Только для чтения **Синтаксическая структура:** Counter32 **Идентификатор объекта:** .1.3.6.1.2.1.4.17.0 **Определение:** Количество IP-датаграмм, которые были успешно фрагментированы на этом объекте.
Группа: ipGroup **Trap-уведомление:** ipInAddrErrors	**Функционал агента:** RC-LLDP-MIB-AC **Доступ:** Только для чтения **Синтаксическая структура:** Counter32 **Идентификатор объекта:** .1.3.6.1.2.1.4.5.0 **Определение:** Количество входных датаграмм, которые были отброшены, поскольку IP-адрес в поле назначения их IP-заголовка не является допустимым адресом для получения на этом объекте. Это число включает недопустимые адреса (например, 0.0.0.0) и адреса неподдерживаемых классов (например, класса E). Для объектов, которые не являются IP-маршрутизаторами и, следовательно, не пересылают датаграммы, этот счетчик включает датаграммы, которые были отброшены, поскольку адрес назначения не был локальным адресом.
Группа: ipGroup **Trap-уведомление:** ipInDelivers	**Доступ:** Только для чтения **Синтаксическая структура:** Counter32 **Идентификатор объекта:** .1.3.6.1.2.1.4.9.0 **Определение:** Общее количество входных датаграмм, успешно доставленных в пользовательские протоколы IP (включая ICMP).
Группа: ipGroup **Trap-уведомление:** ipInDiscards	**Доступ:** Только для чтения **Синтаксическая структура:** Counter32 **Идентификатор объекта:** .1.3.6.1.2.1.4.8.0 **Определение:** Количество входных IP-данных, в отношении которых не возникло проблем с предотвращением их дальнейшей обработки, но которые были отброшены (например, из-за отсутствия буферного пространства). Обратите внимание, что этот счетчик не содержит никаких датаграмм, отброшенных в ожидании повторной сборки.
Группа: ipGroup **Trap-уведомление:** ipInHdrErrors	**Доступ:** Только для чтения **Синтаксическая структура:** Counter32 **Идентификатор объекта:** .1.3.6.1.2.1.4.4.0 **Определение:** Количество входных датаграмм, отброшенных из-за ошибок в их IP-заголовках, включая неверные контрольные суммы, несоответствие номера версии, другие ошибки формата, превышение времени жизни, ошибки, обнаруженные при обработке их IP-адресов и т. д.

Группа/Объект	Описание
Группа: ipGroup **Trap-уведомление:** ipInReceives	**Доступ:** Только для чтения **Синтаксическая структура:** Counter32 **Идентификатор объекта:** .1.3.6.1.2.1.4.3.0 **Определение:** Общее количество входных датаграмм, полученных от интерфейсов, включая полученные по ошибке.
Группа: ipGroup **Trap-уведомление:** ipInUnknownProtos	**Доступ:** Только для чтения **Синтаксическая структура:** Counter32 **Идентификатор объекта:** .1.3.6.1.2.1.4.7.0 **Определение:** Количество локально адресованных датаграмм, успешно полученных, но отброшенных из-за неизвестного или неподдерживаемого протокола.
Группа: ipGroup **Trap-уведомление:** ipNetToMediaIfIndex	**Доступ:** Для чтения и создания **Синтаксическая структура:** Integer **Идентификатор объекта:** .1.3.6.1.2.1.4.22.1.1.1002.192.168.0.254 **Определение:** Интерфейс, для которого эквивалентность этой записи является действительной. Интерфейс, идентифицированный конкретным значением этого индекса, представляет собой тот же интерфейс, идентифицированный тем же значением индекса ifIndex RFC 1573.
Группа: ipGroup **Trap-уведомление:** ipNetToMediaNetAddress	**Доступ:** Для чтения и создания **Синтаксическая структура:** IpAddress **Идентификатор объекта:** .1.3.6.1.2.1.4.22.1.3.1002.192.168.0.254 **Определение:** IpAddress, соответствующий зависящему от среды передачи "физическому" адресу.
Группа: ipGroup **Trap-уведомление:** ipNetToMediaPhysAddress	**Доступ:** Для чтения и создания **Синтаксическая структура:** String **Идентификатор объекта:** .1.3.6.1.2.1.4.22.1.2.1002.192.168.0.254 **Определение:** Зависящий от среды передачи "физический" адрес.
Группа: ipGroup **Trap-уведомление:** ipNetToMediaType	**Доступ:** Для чтения и создания **Синтаксическая структура:** Integer **Идентификатор объекта:** .1.3.6.1.2.1.4.22.1.4.1002.192.168.0.254 **Определение:** Тип отображения. Установка этого объекта на значение invalid(2) приводит к аннулированию соответствующей записи в таблице ipNetToMediaTable. То есть он эффективно отделяет интерфейс, идентифицированный с указанной записью, от отображения, идентифицированного с указанной записью. Удаляет ли агент недействительную запись из таблицы, зависит от конкретной реализации. Соответственно, станции управления должны быть готовы к получению табличной информации от агентов, которая соответствует записям, не используемым в настоящее время. Правильная интерпретация таких записей требует изучения соответствующего объекта ipNetToMediaType.
Группа: ipGroup **Trap-уведомление:** ipOutDiscards	**Доступ:** Только для чтения **Синтаксическая структура:** Counter32 **Идентификатор объекта:** .1.3.6.1.2.1.4.11.0 **Определение:** Количество выходных IP-данных, в отношении которых не возникло проблем с их передачей по назначению, но

Группа/Объект	Описание
	которые были отброшены (например, из-за отсутствия буферного пространства). Обратите внимание, что этот счетчик будет включать датаграммы, подсчитанные в ipForwDatagrams, если любые такие пакеты удовлетворяют этому (дискреционному) критерию отбраковки.
Группа: ipGroup **Trap-уведомление:** ipOutNoRoutes	**Доступ:** Только для чтения **Синтаксическая структура:** Counter32 **Идентификатор объекта:** .1.3.6.1.2.1.4.12.0 **Определение:** Количество отброшенных IP-датаграмм, поскольку маршрут не может быть найден для их передачи в пункт назначения. Обратите внимание, что этот счетчик включает любые пакеты, подсчитанные в ipForwDatagrams, которые соответствуют критерию "без маршрута". Обратите внимание, что это включает в себя любые датаграммы, которые хост не может маршрутизировать, потому что все его маршрутизаторы по умолчанию отключены.
Группа: ipGroup **Trap-уведомление:** ipOutRequests	**Доступ:** Только для чтения **Синтаксическая структура:** Counter32 **Идентификатор объекта:** .1.3.6.1.2.1.4.10.0 **Определение:** Общее количество IP-датаграмм, которые локальные пользовательские IP-протоколы (включая ICMP) передают IP-адресу в запросах на передачу. Обратите внимание, что этот счетчик не включает датаграммы, подсчитанные в ipForwDatagrams.
Группа: ipGroup **Trap-уведомление:** ipReasmFails	**Доступ:** Только для чтения **Синтаксическая структура:** Counter32 **Идентификатор объекта:** .1.3.6.1.2.1.4.16.0 **Определение:** Количество отказов, обнаруженных IP-алгоритмом повторной сборки (по любой причине: истекло время ожидания, ошибки и т. п.). Обратите внимание, что это не обязательно является количеством отброшенных IP-фрагментов, поскольку некоторые алгоритмы (в частности, алгоритм в RFC 815) могут не выполнять отслеживание количества фрагментов, объединяя их по мере их получения.
Группа: ipGroup **Trap-уведомление:** ipReasmOKs	**Доступ:** Только для чтения **Синтаксическая структура:** Counter32 **Идентификатор объекта:** .1.3.6.1.2.1.4.15.0 **Определение:** Количество успешно собранных IP-датаграмм.
Группа: ipGroup **Trap-уведомление:** ipReasmReqds	**Доступ:** Только для чтения **Синтаксическая структура:** Counter32 **Идентификатор объекта:** .1.3.6.1.2.1.4.14.0 **Определение:** Количество полученных IP-фрагментов, которые необходимо было собрать заново на этом объекте.
Группа: ipGroup **Trap-уведомление:** ipReasmTimeout	**Доступ:** Только для чтения **Синтаксическая структура:** Integer **Идентификатор объекта:** .1.3.6.1.2.1.4.13.0 **Определение:** Максимальное количество секунд, в течение которых полученные фрагменты удерживаются в ожидании повторной сборки на этом объекте.
Группа: ipGroup **Trap-уведомление:** ipRoutingDiscards	**Доступ:** Только для чтения **Синтаксическая структура:** Counter32

Группа/Объект	Описание
	Идентификатор объекта: .1.3.6.1.2.1.4.23 **Определение:** Количество записей маршрутизации, которые были выбраны для удаления, даже если они действительны. Одна из возможных причин отказа от такой записи может заключаться в высвобождении буферного пространства для других записей маршрутизации.

LLDP-MIB

Группа/Объект	Описание
Группа: lldpConfigTxGroup **Trap-уведомление:** lldpConfigManAddrPortsTxEnable	**Функционал агента:** RC-LLDP-MIB-AC **Доступ:** Для чтения и записи **Синтаксическая структура:** Hex-String **Идентификатор объекта:** .1.0.8802.1.1.2.1.1.7.1.1.4 **Определение:** Набор портов, идентифицированных с помощью PortList, в котором каждый порт представлен как бит. Соответствующий экземпляр адреса для управления локальной системой будет передан на порты-члены lldpManAddrPortsTxEnable. Значение по умолчанию для объекта lldpConfigManAddrPortsTxEnable — пустая двоичная строка, что означает, что для указанного экземпляра управляющего адреса не указаны порты. Доступ для записи не реализован.
Группа: lldpLocSysGroup **Trap-уведомление:** lldpLocChassisId	**Доступ:** Только для чтения **Синтаксическая структура:** Hex-String **Идентификатор объекта:** .1.0.8802.1.1.2.1.3.2.0 **Определение:** Тип кодирования, используемый для идентификации блока, связанного с локальной системой.
Группа: lldpLocSysGroup **Trap-уведомление:** lldpLocChassisIdSubtype	**Доступ:** Только для чтения **Синтаксическая структура:** Integer **Идентификатор объекта:** .1.0.8802.1.1.2.1.3.1.0 **Определение:** Тип кодирования, используемый для идентификации блока, связанного с локальной системой.
Группа: lldpLocSysGroup **Trap-уведомление:** lldpLocManAddrIfId	**Доступ:** Только для чтения **Синтаксическая структура:** Integer **Идентификатор объекта:** .1.0.8802.1.1.2.1.3.8.1.5.192.168.0.180 **Определение:** Целое значение, используемое для идентификации номера интерфейса в отношении компонента адреса управления, связанного с локальной системой.
Группа: lldpLocSysGroup **Trap-уведомление:** lldpLocManAddrIfSubtype	**Доступ:** Только для чтения **Синтаксическая структура:** Integer **Идентификатор объекта:** .1.0.8802.1.1.2.1.3.8.1.4.192.168.0.180 **Определение:** Значение перечисления, которое идентифицирует метод нумерации интерфейса, используемый для определения номера интерфейса, связанного с локальной системой.
Группа: lldpLocSysGroup **Trap-уведомление:** lldpLocManAddrLen	**Доступ:** Только для чтения **Синтаксическая структура:** Integer

Группа/Объект	Описание
	Идентификатор объекта: .1.0.8802.1.1.2.1.3.8.1.3 **Определение:** Общая длина подтипа адреса управления и полей адреса управления в LLDPDU, передаваемых локальным агентом LLDP. Поле длины адреса управления необходимо для того, чтобы принимающие системы, которые не реализуют SNMP, не должны были реализовывать таблицу эквивалентности номеров/длины адреса семейства iana для декодирования адреса управления.
Группа: lldpLocSysGroup **Trap-уведомление:** lldpLocManAddrOID	**Доступ:** Только для чтения **Синтаксическая структура:** Идентификатор объекта **Идентификатор объекта:** .1.0.8802.1.1.2.1.3.8.1.6.192.168.0.180 **Определение:** Значение идентификатора объекта, используемое для идентификации типа аппаратного компонента или объекта протокола, связанного с адресом управления, выделенным локальным системным агентом.
Группа: lldpLocSysGroup **Trap-уведомление:** lldpLocPortDesc	**Доступ:** Только для чтения **Синтаксическая структура:** String **Идентификатор объекта:** .1.0.8802.1.1.2.1.3.7.1.4.1 **Определение:** Значение строки, используемое для идентификации описания порта станции 802 LAN, связанного с локальной системой. Если локальный агент поддерживает IETF RFC 2863, объект lldpLocPortDesc должен иметь то же значение объекта ifDescr.
Группа: lldpLocSysGroup **Trap-уведомление:** lldpLocPortId	**Доступ:** Только для чтения **Синтаксическая структура:** String **Идентификатор объекта:** .1.0.8802.1.1.2.1.3.7.1.3.1 **Определение:** Значение строки, используемое для идентификации компонента порта, связанного с данным портом в локальной системе.
Группа: lldpLocSysGroup **Trap-уведомление:** lldpLocPortIdSubtype	**Доступ:** Только для чтения **Синтаксическая структура:** Integer **Идентификатор объекта:** .1.0.8802.1.1.2.1.3.7.1.2.1 **Определение:** Тип кодировки идентификатора порта, используемой в связанном объекте lldpLocPortId.
Группа: lldpLocSysGroup **Trap-уведомление:** lldpLocSysCapEnabled	**Доступ:** Только для чтения **Синтаксическая структура:** Hex-String **Идентификатор объекта:** .1.0.8802.1.1.2.1.3.6.0 **Определение:** Точечное значение, используемое для определения того, какие возможности системы включены в локальной системе.
Группа: lldpLocSysGroup **Trap-уведомление:** lldpLocSysCapSupported	**Доступ:** Только для чтения **Синтаксическая структура:** Hex-String **Идентификатор объекта:** .1.0.8802.1.1.2.1.3.5.0 **Определение:** Точечное значение, используемое для определения того, какие возможности системы поддерживаются в локальной системе.
Группа: lldpLocSysGroup **Trap-уведомление:** lldpLocSysDesc	**Доступ:** Только для чтения **Синтаксическая структура:** String **Идентификатор объекта:** .1.0.8802.1.1.2.1.3.4.0 **Определение:** Значение строки, используемое для определения системного описания локальной системы. Если локальный агент

Группа/Объект	Описание
	поддерживает IETF RFC 3418, объект lldpLocSysDesc должен иметь то же значение объекта sysDesc.
Группа: lldpLocSysGroup **Trap-уведомление:** lldpLocSysName	**Доступ:** Только для чтения **Синтаксическая структура:** String **Идентификатор объекта:** .1.0.8802.1.1.2.1.3.3.0 **Определение:** Значение строки, используемое для определения системного имени локальной системы. Если локальный агент поддерживает IETF RFC 3418, объект lldpLocSysName должен иметь то же значение объекта sysName.
Группа: lldpConfigTxGroup **Trap-уведомление:** lldpMessageTxHoldMultiplier	**Доступ:** Для чтения и записи **Синтаксическая структура:** Integer **Идентификатор объекта:** .1.0.8802.1.1.2.1.1.2.0 **Определение:** Значение time-to-live, выраженное как кратное объекту lldpMessageTxInterval. Фактическое значение времени работы, используемое в кадрах LLDP, передаваемое от имени этого агента LLDP, может быть выражено следующей формулой: TTL = min(65535, (lldpMessageTxInterval * lldpMessageTxHoldMultiplier)) Например, если значение lldpMessageTxInterval равно 30, а значение lldpMessageTxHoldMultiplier равно 4, то значение 120 кодируется в поле TTL в заголовке LLDP. Значение по умолчанию для объекта lldpMessageTxHoldMultiplier — 4. Значение этого объекта необходимо восстанавливать из энергонезависимого запоминающего устройства после повторной инициализации системы управления.
Группа: lldpConfigTxGroup **Trap-уведомление:** lldpMessageTxInterval	**Доступ:** Для чтения и записи **Синтаксическая структура:** Integer **Идентификатор объекта:** .1.0.8802.1.1.2.1.1.1.0 **Определение:** Интервал, через который кадры LLDP передаются от имени этого агента LLDP. Значение по умолчанию для объекта lldpMessageTxInterval составляет 30 секунд. Значение этого объекта необходимо восстанавливать из энергонезависимого запоминающего устройства после повторной инициализации системы управления.
Группа: lldpConfigRxGroup **Trap-уведомление:** lldpNotificationInterval	**Функционал агента:** RC-LLDP-MIB-AC **Доступ:** Для чтения и записи **Синтаксическая структура:** Integer **Идентификатор объекта:** .1.0.8802.1.1.2.1.1.5.0 **Определение:** Этот объект управляет передачей уведомлений LLDP. Агент не должен генерировать более одного события уведомления lldpRemTablesChange в указанный период, где "событие уведомления" — передача одного типа PDU уведомлений списку получателей уведомлений. Если дополнительные изменения в группах объектов lldpRemoteSystemsData происходят в течение указанного периода регулирования скорости, агент должен подавить эти события ловушки. NMS должна периодически проверять значение lldpStatsRemTableLastChangeTime, чтобы обнаружить любые пропущенные события уведомления lldpRemTablesChange, например, из-за регулирования скорости или потери передачи. Если передача уведомления включена для конкретных портов, рекомендуемый период регулирования скорости по умолчанию составляет 5 секунд. Значение этого объекта необходимо восстанавливать из энергонезависимого запоминающего устройства после повторной инициализации системы управления.

Группа/Объект	Описание
	Примечание Доступ для записи не реализован.
Группа: lldpConfigGroup **Trap-уведомление:** lldpPortConfigAdminStatus	**Доступ:** Для чтения и записи **Синтаксическая структура:** Integer **Идентификатор объекта:** .1.0.8802.1.1.2.1.1.6.1.2.1 **Определение:** Требуемый для администрирования статус локального агента LLDP. Если связанный объект lldpPortConfigAdminStatus имеет значение "txOnly(1)", то агент LLDP будет передавать кадры LLDP на этом порту и не будет хранить никакой информации о подключенных удаленных системах. Если связанный объект lldpPortConfigAdminStatus имеет значение "rxOnly(2)", то агент LLDP будет получать, но не будет передавать кадры LLDP на этом порту. Если связанный объект lldpPortConfigAdminStatus имеет значение "txAndRx(3)", то агент LLDP будет передавать и принимать кадры LLDP на этом порту. Если связанный объект lldpPortConfigAdminStatus имеет значение "disabled(4)", агент LLDP не будет передавать или принимать кадры LLDP на этом порту. Если существует информация об удаленных системах, полученная на этом порту и сохраненная в других таблицах, до отключения lldpPortConfigAdminStatus порта, то информация естественно устареет.
Группа: lldpConfigRxGroup **Trap-уведомление:** lldpPortConfigNotificationEnable	**Доступ:** Для чтения и записи **Синтаксическая структура:** Integer **Идентификатор объекта:** .1.0.8802.1.1.2.1.1.6.1.3.1 **Определение:** Элементы управления lldpPortConfigNotificationEnable для каждого порта, независимо от того, включены ли уведомления от агента. Значение true(1) означает, что уведомления включены; значение false(2) означает, что они не включены.
Группа: lldpConfigTxGroup **Trap-уведомление:** lldpPortConfigTLVsTxEnable	**Функционал агента:** RC-LLDP-MIB-AC **Доступ:** Для чтения и записи **Синтаксическая структура:** Hex-String **Идентификатор объекта:** .1.0.8802.1.1.2.1.1.6.1.4.1 **Определение:** LldpPortConfigTLVsTxEnable, определяемый как растровый рисунок, включает базовый набор TLV LLDP, передача которых разрешена локальным агентом LLDP сетевым управлением. Каждый бит растрового изображения соответствует типу TLV, связанному с определенным необязательным TLV. Следует отметить, что специфические для организации TLV исключены из точечного рисунка lldpTLVsTxEnable. MIB расширения информации организации LLDP должны иметь аналогичный объект конфигурации для управления передачей своих организационно определенных TLV. Бит "portDesc(0)" указывает, что агент LLDP должен передавать "TLV описания порта". Бит "sysName(1)" указывает, что агент LLDP должен передавать "TLV системного имени". Бит "sysDesc(2)" указывает, что агент LLDP должен передавать "TLV описания системы". Бит "sysCap(3)" указывает, что агент LLDP должен передавать "TLV возможностей системы". Для типа TLV адреса управления не зарезервирован бит, так как передача TLV адреса управления контролируется другим объектом lldpConfigManAddrTable. Значение по умолчанию для объекта lldpPortConfigTLVsTxEnable пустое, что означает, что перечисляемые значения не заданы. Значение этого объекта необходимо восстанавливать из энергонезависимого

Группа/Объект	Описание
	запоминающего устройства после повторной инициализации системы управления. Доступ для записи не реализован.
Группа: lldpConfigTxGroup **Trap-уведомление:** lldpReinitDelay	**Доступ:** Для чтения и записи **Синтаксическая структура:** Integer **Идентификатор объекта:** .1.0.8802.1.1.2.1.1.3.0 **Определение:** LldpReinitDelay указывает на задержку (в секундах) с момента, когда статус объекта lldpPortConfigAdminStatus конкретного порта получает значение "disabled", до тех пор, пока не будет предпринята попытка повторной инициализации. Значение по умолчанию для объекта lldpReintDelay составляет две секунды. Значение этого объекта необходимо восстанавливать из энергонезависимого запоминающего устройства после повторной инициализации системы управления.
Группа: lldpRemSysGroup **Trap-уведомление:** lldpRemChassisId	**Доступ:** Только для чтения **Синтаксическая структура:** Hex-String **Идентификатор объекта:** .1.0.8802.1.1.2.1.4.1.1.5.3496.7.1 **Определение:** Значение строки, используемое для идентификации компонента блока, связанного с удаленной системой.
Группа: lldpRemSysGroup **Trap-уведомление:** lldpRemChassisIdSubtype	**Доступ:** Только для чтения **Синтаксическая структура:** Integer **Идентификатор объекта:** .1.0.8802.1.1.2.1.4.1.1.4.3496.7.1 **Определение:** Тип кодирования, используемый для идентификации блока, связанного с удаленной системой.
Группа: lldpRemSysGroup **Trap-уведомление:** lldpRemManAddrIfId	**Доступ:** Только для чтения **Синтаксическая структура:** Integer **Идентификатор объекта:** .1.0.8802.1.1.2.1.4.2.1.4.3496.7.1.1.4.192.168.0.20 **Определение:** Целое значение, используемое для идентификации номера интерфейса относительно компонента адреса управления, связанного с удаленной системой.
Группа: lldpRemSysGroup **Trap-уведомление:** lldpRemManAddrIfSubtype	**Доступ:** Только для чтения **Синтаксическая структура:** Integer **Идентификатор объекта:** .1.0.8802.1.1.2.1.4.2.1.3.3496.7.1.1.4.192.168.0.20 **Определение:** Значение перечисления, которое идентифицирует метод нумерации интерфейса, используемый для определения номера интерфейса, связанного с удаленной системой.
Группа: lldpRemSysGroup **Trap-уведомление:** lldpRemManAddrOID	**Доступ:** Только для чтения **Синтаксическая структура:** Идентификатор объекта **Идентификатор объекта:** .1.0.8802.1.1.2.1.4.2.1.5.6036.6.1.1.4.192.168.0.33 **Определение:** Значение идентификатора объекта, используемое для идентификации типа аппаратного компонента или объекта протокола, связанного с адресом управления, выделенным удаленным системным агентом.
Группа: lldpRemSysGroup	**Доступ:** Только для чтения

Группа/Объект	Описание
Trap-уведомление: lldpRemOrgDefInfo	**Синтаксическая структура:** String **Идентификатор объекта:** .1.0.8802.1.1.2.1.4.4.1.4 **Определение:** Эта таблица содержит одну или несколько строк на каждое физическое сетевое подключение, которое выделяет организационно определенную информацию. Обратите внимание, что эта таблица содержит одну или несколько строк организационно определенной информации, которая не распознается локальным агентом. Если локальная система способна распознавать любую организационно определенную информацию, для поиска информации следует использовать соответствующие расширения MIB от организации.
Группа: lldpRemSysGroup **Trap-уведомление:** lldpRemPortDesc	**Доступ:** Только для чтения **Синтаксическая структура:** String **Идентификатор объекта:** .1.0.8802.1.1.2.1.4.1.1.8 **Определение:** Значение строки, используемое для определения описания данного порта, связанного с удаленной системой.
Группа: lldpRemSysGroup **Trap-уведомление:** lldpRemPortId	**Доступ:** Только для чтения **Синтаксическая структура:** String **Идентификатор объекта:** .1.0.8802.1.1.2.1.4.1.1.7.3496.7.1 **Определение:** Значение строки, используемое для идентификации компонента порта, связанного с удаленной системой.
Группа: lldpRemSysGroup **Trap-уведомление:** lldpRemPortIdSubtype	**Доступ:** Только для чтения **Синтаксическая структура:** Integer **Идентификатор объекта:** .1.0.8802.1.1.2.1.4.1.1.6.3496.7.1 **Определение:** Тип кодировки идентификатора порта, используемой в связанном объекте lldpRemPortId.
Группа: lldpRemSysGroup **Trap-уведомление:** lldpRemSysCapEnabled	**Доступ:** Только для чтения **Синтаксическая структура:** Hex-String **Идентификатор объекта:** .1.0.8802.1.1.2.1.4.1.1.12.3496.7.1 **Определение:** Точечное значение, используемое для определения того, какие возможности системы включены в удаленной системе.
Группа: lldpRemSysGroup **Trap-уведомление:** lldpRemSysCapSupported	**Доступ:** Только для чтения **Синтаксическая структура:** Hex-String **Идентификатор объекта:** .1.0.8802.1.1.2.1.4.1.1.11.3496.7.1 **Определение:** Точечное значение, используемое для определения того, какие возможности системы поддерживаются в удаленной системе.
Группа: lldpRemSysGroup **Trap-уведомление:** lldpRemSysDesc	**Доступ:** Только для чтения **Синтаксическая структура:** String **Идентификатор объекта:** .1.0.8802.1.1.2.1.4.1.1.10.3496.7.1 **Определение:** Значение строки, используемое для определения системного описания удаленной системы.
Группа: lldpRemSysGroup **Trap-уведомление:** lldpRemSysName	**Доступ:** Только для чтения **Синтаксическая структура:** String **Идентификатор объекта:** .1.0.8802.1.1.2.1.4.1.1.9.3496.7.1

Группа/Объект	Описание
	Определение: Значение строки, используемое для определения системного имени удаленной системы.
Группа: lldpNotificationsGroup **Trap-уведомление:** lldpRemTablesChange	**Синтаксическая структура:** String **Идентификатор объекта:** 1.0.8802.1.1.2.0.0.1.0 **Определение:** Уведомление lldpRemTablesChange отправляется при изменении значения lldpStatsRemTableLastChangeTime. Оно может быть использовано NMS для запуска опросов технического обслуживания таблицы удаленных систем LLDP. Обратите внимание, что передача уведомлений lldpRemTablesChange ограничивается агентом, как указано объектом lldpNotificationInterval.
Группа: lldpRemSysGroup **Trap-уведомление:** lldpRemUnknownTLVInfo	**Доступ:** Только для чтения **Синтаксическая структура:** String **Идентификатор объекта:** 1.0.8802.1.1.2.1.4.3.1.2 **Определение:** Этот объект представляет значение, извлеченное из поля значения TLV.
Группа: lldpStatsRxGroup **Trap-уведомление:** lldpStatsRemTablesLastChangeTime	**Доступ:** Только для чтения **Синтаксическая структура:** Timeticks **Идентификатор объекта:** .1.0.8802.1.1.2.1.2.1.0 **Определение:** Значение объекта sysUpTime (определенное в IETF RFC 3418) на момент создания, изменения или удаления записи в таблицах, связанных с объектами lldpRemoteSystemsData и всеми объектами расширения LLDP, связанными с удаленными системами. NMS может использовать этот объект для уменьшения опроса объектов lldpRemoteSystemsData.
Группа: lldpStatsRxGroup **Trap-уведомление:** lldpStatsRxPortAgeoutsTotal	**Доступ:** Только для чтения **Синтаксическая структура:** Counter32 **Идентификатор объекта:** .1.0.8802.1.1.2.1.2.7.1.7.1 **Определение:** Счетчик, представляющий количество устареваний, произошедших на данном порту. Срок годности — это количество раз, когда полный набор информации, рекламируемой определенным MSAP, удалялся из таблиц, содержащихся в объектах lldpRemoteSystemsData и lldpExtensions, поскольку интервал своевременности информации истек. Этот счетчик аналогичен lldpStatsRemTablesAgeouts, за исключением того, что счетчик используется для каждого порта. Это позволяет NMS опросить таблицы, связанные с объектами lldpRemoteSystemsData и всеми объектами расширения LLDP, связанными с удаленными системами, только на указанном порту. Этот счетчик должен быть установлен на ноль во время инициализации агента, и его значение не должно сохраняться в энергонезависимом запоминающем устройстве. Когда статус администрирования порта меняется с "disabled" на "rxOnly", "txOnly" или "txAndRx", счетчик, связанный с тем же портом, должен быть сброшен на 0. Агент также должен сбросить всю удаленную системную информацию, связанную с одним и тем же портом. Этот счетчик следует увеличивать только один раз, когда полный набор информации недействителен (устарел) из всех связанных таблиц на конкретном порту. Частичное устаревание не допускается и, таким образом, не должно изменять значение этого счетчика.
Группа: lldpStatsRxGroup **Trap-уведомление:** lldpStatsRxPortFramesDiscardedTotal	**Доступ:** Только для чтения **Синтаксическая структура:** Counter32 **Идентификатор объекта:** .1.0.8802.1.1.2.1.2.7.1.2.1

Группа/Объект	Описание
	Определение: Количество кадров LLDP, полученных этим агентом LLDP на указанном порту, а затем отброшенных по любой причине. Этот счетчик может указывать на то, что проблемы с форматированием заголовка LLDP могут возникать с локальным агентом LLDP в системе отправки или что проблемы с валидацией LLDPDU могут возникать с локальным агентом LLDP в системе приема.
Группа: lldpStatsRxGroup **Trap-уведомление:** lldpStatsRxPortFramesErrors	**Доступ:** Только для чтения **Синтаксическая структура:** Counter32 **Идентификатор объекта:** .1.0.8802.1.1.2.1.2.7.1.3.1 **Определение:** Количество недопустимых кадров LLDP, полученных этим агентом LLDP на указанном порту, когда этот агент LLDP включен.
Группа: lldpStatsRxGroup **Trap-уведомление:** lldpStatsRxPortFramesTotal	**Доступ:** Только для чтения **Синтаксическая структура:** Counter32 **Идентификатор объекта:** .1.0.8802.1.1.2.1.2.7.1.4.1 **Определение:** Количество допустимых кадров LLDP, полученных этим агентом LLDP на указанном порту, когда этот агент LLDP включен.
Группа: lldpStatsRxGroup **Trap-уведомление:** lldpStatsRxPortTLVsDiscardedTotal	**Доступ:** Только для чтения **Синтаксическая структура:** Counter32 **Идентификатор объекта:** .1.0.8802.1.1.2.1.2.7.1.5.1 **Определение:** Количество TLV LLDP, отбракованных по любой причине данным агентом LLDP на указанном порту.
Группа: lldpStatsRxGroup **Trap-уведомление:** lldpStatsRxPortTLVsUnrecognizedTotal	**Доступ:** Только для чтения **Синтаксическая структура:** Counter32 **Идентификатор объекта:** .1.0.8802.1.1.2.1.2.7.1.6.1 **Определение:** Количество TLV LLDP, полученных на данном порту, которые не распознаются этим агентом LLDP на указанном порту. Нераспознанным TLV называется TLV, значение типа которого находится в диапазоне зарезервированных типов TLV (000 1001 — 111 1110) в таблице 9.1 стандарта IEEE 802.1AB-2005. Нераспознанным TLV может быть базовое TLV управления из более поздней версии LLDP.
Группа: lldpStatsTxGroup **Trap-уведомление:** lldpStatsTxPortFramesTotal	**Доступ:** Только для чтения **Синтаксическая структура:** Counter32 **Идентификатор объекта:** .1.0.8802.1.1.2.1.2.6.1.2.1 **Определение:** Количество кадров LLDP, передаваемых этим агентом LLDP на указанном порту.
Группа: lldpConfigTxGroup **Trap-уведомление:** lldpTxDelay	**Доступ:** Для чтения и записи **Синтаксическая структура:** Integer **Идентификатор объекта:** .1.0.8802.1.1.2.1.1.4.0 **Определение:** LldpTxDelay указывает задержку (в секундах) между последовательными передачами кадра LLDP, инициированными изменениями значений/состояния в MIB локальных систем LLDP. Рекомендуемое значение для lldpTxDelay задается по следующей формуле: 1 <= lldpTxDelay <= (0,25 * lldpMessageTxInterval) Значение по умолчанию для объекта lldpTxDelay составляет две секунды. Значение этого объекта необходимо восстанавливать из энергонезависимого запоминающего устройства после повторной инициализации системы управления.

Q-BRIDGE-MIB

Группа/Объект	Описание
Группа: qBridgeFdbUnicastGroup **Trap-уведомление:** dot1qFdbDynamicCount	**Доступ:** Только для чтения **Синтаксическая структура:** Counter32 **Идентификатор объекта:** .1.3.6.1.2.1.17.7.1.2.1.1.2.255.148.184.197.5.176.0 **Определение:** Текущее количество динамических записей в этой базе данных фильтрации.
Группа: qBridgeServiceRequirementsGroup **Trap-уведомление:** dot1qForwardAllForbiddenPorts	**Функционал агента:** RC-Q-BRIDGE-MIB-AC **Доступ:** Только для чтения **Синтаксическая структура:** Hex-String **Идентификатор объекта:** .1.3.6.1.2.1.17.7.1.2.4.1.3.22 **Определение:** Набор портов, заданных системой управления в этой VLAN, для которых атрибут Service Requirement со значением Forward All Multicast Groups не может динамически регистрироваться GMRP. Это значение будет восстановлено после перезапуска устройства. Порт не может быть добавлен в этот набор, если он уже является членом набора портов в dot1qForwardAllStaticPorts. Значение по умолчанию — строка нулей соответствующей длины. Значение этого объекта ДОЛЖНО сохраняться при повторной инициализации системы управления.
Группа: qBridgeServiceRequirementsGroup **Trap-уведомление:** dot1qForwardAllPorts	**Доступ:** Только для чтения **Синтаксическая структура:** Hex-String **Идентификатор объекта:** .1.3.6.1.2.1.17.7.1.2.4.1.1.22 **Определение:** Полный набор портов в этой VLAN, на которые должны быть перенаправлены все многоадресные групповые кадры. Сюда входят порты, для которых это требование было динамически определено GMRP или статически задано системой управления.
Группа: qBridgeServiceRequirementsGroup **Trap-уведомление:** dot1qForwardAllStaticPorts	**Функционал агента:** RC-Q-BRIDGE-MIB-AC **Доступ:** Только для чтения **Синтаксическая структура:** Hex-String **Идентификатор объекта:** .1.3.6.1.2.1.17.7.1.2.4.1.2.22 **Определение:** Набор портов, заданный системой управления в этой VLAN, на которые должны быть перенаправлены все многоадресные групповые кадры. Порты, внесенные в этот список, будут отображены в полном наборе, показанном dot1qForwardAllPorts. Это значение будет восстановлено после перезапуска устройства. Это относится только к портам, являющимся членами VLAN, определенным dot1qVlanCurrentEgressPorts. Порт не может быть добавлен в этот набор, если он уже является членом набора портов в dot1qForwardAllForbiddenPorts. Значение по умолчанию — это строка строк соответствующей длины, указывающая стандартное поведение при использовании базовых служб фильтрации, т.е. пересылке всех многоадресных рассылок на все порты. Значение этого объекта ДОЛЖНО сохраняться при повторной инициализации системы управления.
Группа: qBridgeServiceRequirementsGroup **Trap-уведомление:** dot1qForwardUnregisteredForbiddenPorts	**Доступ:** Для чтения и записи **Синтаксическая структура:** Hex-String **Идентификатор объекта:** .1.3.6.1.2.1.17.7.1.2.5.1.3.22

Группа/Объект	Описание
	Определение: Набор портов, заданный системой управления в этой VLAN, для которых атрибут Service Requirement со значением Forward Unregistered Multicast Groups может динамически не регистрироваться GMRP. Это значение будет восстановлено после перезапуска устройства. Порт не может быть добавлен в этот набор, если он уже является членом набора портов в dot1qForwardUnregisteredStaticPorts. Значение по умолчанию — строка нулей соответствующей длины. Значение этого объекта ДОЛЖНО сохраняться при повторной инициализации системы управления.
Группа: qBridgeServiceRequirementsGroup **Trap-уведомление:** dot1qForwardUnregisteredPorts	**Доступ:** Только для чтения **Синтаксическая структура:** Hex-String **Идентификатор объекта:** .1.3.6.1.2.1.17.7.1.2.5.1.1.22 **Определение:** Полный набор портов в этой VLAN, на которые будут пересылаться многоадресные групповые кадры, для которых нет более конкретной информации о переадресации. Сюда входят порты, для которых это требование было динамически определено GMRP или статически задано системой управления.
Группа: qBridgeServiceRequirementsGroup **Trap-уведомление:** dot1qForwardUnregisteredStaticPorts	**Доступ:** Для чтения и записи **Синтаксическая структура:** Hex-String **Идентификатор объекта:** .1.3.6.1.2.1.17.7.1.2.5.1.2.22 **Определение:** Набор портов, заданный системой управления в этой VLAN, на которые должны быть перенаправлены адресованные многоадресные групповые кадры, для которых нет более конкретной информации о переадресации. Порты, внесенные в этот список, также будут отображены в полном наборе, показанном dot1qForwardUnregisteredPorts. Это значение будет восстановлено после перезапуска устройства. Порт не может быть добавлен в этот набор, если он уже является членом набора портов в dot1qForwardUnregisteredForbiddenPorts. Значение по умолчанию — строка нулей соответствующей длины, хотя это не влияет на значение dot1qForwardAllStaticPorts по умолчанию. Значение этого объекта ДОЛЖНО сохраняться при повторной инициализации системы управления.
Группа: qBridgeBaseGroup **Trap-уведомление:** dot1qGvrpStatus	**Доступ:** Для чтения и записи **Синтаксическая структура:** Integer **Идентификатор объекта:** .1.3.6.1.2.1.17.7.1.1.5.0 **Определение:** Статус для администрирования, запрошенный системой управления для GVRP. Значение enabled(1) указывает на то, что GVRP должен быть включен на этом устройстве на всех портах, для которых он не был специально отключен. При значении disabled(2) GVRP отключается на всех портах, и все пакеты GVRP будут пересылаться без перекодировки. Этот объект влияет на все машины состояний Applicant and Registrar для GVRP. Переход от значения disabled(2) к enabled(1) приведет к сбросу всех машин состояний GVRP на всех портах. Значение этого объекта ДОЛЖНО сохраняться при повторной инициализации системы управления.
Группа: qBridgeBaseGroup **Trap-уведомление:** dot1qMaxSupportedVlans	**Доступ:** Только для чтения **Синтаксическая структура:** Gauge32 **Идентификатор объекта:** .1.3.6.1.2.1.17.7.1.1.3.0 **Определение:** Максимальное количество сетей VLAN IEEE 802.1Q, поддерживаемых этим устройством.
Группа: qBridgeBaseGroup	**Доступ:** Только для чтения

Группа/Объект	Описание
Trap-уведомление: dot1qMaxVlanId	**Синтаксическая структура:** Integer **Идентификатор объекта:** .1.3.6.1.2.1.17.7.1.1.2.0 **Определение:** Максимальный идентификатор VLAN IEEE 802.1Q, который поддерживает это устройство.
Группа: qBridgeVlanStaticGroup **Trap-уведомление:** dot1qNextFreeLocalVlanIndex	**Доступ:** Только для чтения **Синтаксическая структура:** Integer **Идентификатор объекта:** .1.3.6.1.2.1.17.7.1.4.4.0 **Определение:** Следующее доступное значение dot1qVlanIndex записи локальной VLAN в dot1qVlanStaticTable. Это приведет к сообщению значений >=4096, если может быть создана новая локальная сеть VLAN, или к значению 0, если это невозможно. Операция создания строки в этой таблице для записи с локальным значением VlanIndex может завершиться неудачей, если текущее значение этого объекта не используется в качестве индекса. Даже если используется считываемое значение, нет гарантии, что оно будет являться действительным индексом при попытке создать операцию; другой менеджер, возможно, уже включился в течение промежуточного интервала времени. В этом случае dot1qNextFreeLocalVlanIndex следует считать снова и повторить попытку создания с новым значением. Это значение автоматически изменится, когда текущее значение используется для создания новой строки.
Группа: qBridgeBaseGroup **Trap-уведомление:** dot1qNumVlans	**Доступ:** Только для чтения **Синтаксическая структура:** Gauge32 **Идентификатор объекта:** .1.3.6.1.2.1.17.7.1.1.4.0 **Определение:** Текущее количество сетей VLAN IEEE 802.1Q, сконфигурированных в этом устройстве.
Группа: qBridgePortGroup2 **Trap-уведомление:** dot1qPortAcceptableFrameTypes	**Функционал агента:** RC-Q-BRIDGE-MIB-AC **Доступ:** Для чтения и записи **Синтаксическая структура:** Integer **Идентификатор объекта:** .1.3.6.1.2.1.17.7.1.4.5.1.2.1 **Определение:** При admitOnlyVlanTagged(2) устройство будет отбрасывать кадры без меток или кадры с метками приоритета, полученные на этом порту. При admitAll(1) кадры без меток или кадры с метками приоритета, полученные на этом порту, будут приняты и назначены VID на основе PVID и VID Set для этого порта. Это управление не влияет на независимые от VLAN кадры блока протокольных данных моста (BPDU), такие как GVRP и протокол связующего дерева (STP). Это влияет на зависимые от VLAN кадры BPDU, такие как GMRP. Значение этого объекта ДОЛЖНО сохраняться при повторной инициализации системы управления. **Примечание** Значение «admitOnlyVlanTagged(2)» не поддерживается.
Группа: qBridgePortGroup2 **Trap-уведомление:** dot1qPortGvrpStatus	**Функционал агента:** RC-Q-BRIDGE-MIB-AC **Доступ:** Для чтения и записи **Синтаксическая структура:** Integer **Идентификатор объекта:** .1.3.6.1.2.1.17.7.1.4.5.1.4.1 **Определение:** Состояние работы GVRP на этом порту. Значение enabled(1) указывает на то, что GVRP включен на этом порту, при

Группа/Объект	Описание
	условии, что dot1qGvrpStatus также включен для этого устройства. Если установлено значение disabled(2), но dot1qGvrpStatus все еще включен для устройства, GVRP отключен на этом порту: любые полученные пакеты GVRP будут отброшены, и никакие регистрации GVRP не будут передаваться с других портов. Этот объект влияет на все машины состояний Applicant and Registrar для GVRP на этом порту. Переход от значения disabled(2) к enabled(1) приведет к сбросу всех машин состояний GVRP на этом порту. Значение этого объекта ДОЛЖНО сохраняться при повторной инициализации системы управления. **Примечание** Значение по умолчанию «disabled(2)».
Группа: qBridgePortGroup2 **Trap-уведомление:** dot1qPortIngressFiltering	**Функционал агента:** RC-Q-BRIDGE-MIB-AC **Доступ:** Для чтения и записи **Синтаксическая структура:** Integer **Идентификатор объекта:** .1.3.6.1.2.1.17.7.1.4.5.1.3.1 **Определение:** Если установлено значение true(1), устройство будет отбрасывать входящие кадры для виртуальных сетей VLAN, которые не включают этот порт в свой набор членов. Если установлено значение false(2), порт будет принимать все входящие кадры. Это управление не влияет на независимые от VLAN кадры блока протокольных данных моста (BPDU), такие как GVRP и протокол связующего дерева (STP). Это влияет на зависимые от VLAN кадры BPDU, такие как GMRP. Значение этого объекта ДОЛЖНО сохраняться при повторной инициализации системы управления. **Примечание** Значение «true(1)» не поддерживается.
Группа: qBridgePortGroup2 **Trap-уведомление:** dot1qPvid	**Доступ:** Для чтения и записи **Синтаксическая структура:** Gauge32 **Идентификатор объекта:** .1.3.6.1.2.1.17.7.1.4.5.1.1.1 **Определение:** PVID, VLAN-ID, присвоенные кадрам без меток или кадрам с метками приоритета, полученным на этом порту. Значение этого объекта ДОЛЖНО сохраняться при повторной инициализации системы управления.
Группа: qBridgeFdbUnicastGroup **Trap-уведомление:** dot1qTpFdbPort	**Доступ:** Только для чтения **Синтаксическая структура:** Integer **Идентификатор объекта:** .1.3.6.1.2.1.17.7.1.2.2.1.2.255.148.184.197.5.176.0 **Определение:** 0 или номер порта, на котором был обнаружен кадр с адресом отправителя, совпадающим со значением соответствующего экземпляра dot1qTpFdbAddress. 0 показывает, что номер порта не был определен, но у устройства имеется некая информация о пересылке/фильтрации для этого адреса (например, в dot1qStaticUnicastTable). Разработчикам рекомендуется назначать этому объекту номер порта, когда он определен, даже для адресов, у которых соответствующее значение dot1qTpFdbStatus не равно learned(3).
Группа: qBridgeFdbUnicastGroup **Trap-уведомление:** dot1qTpFdbStatus	**Доступ:** Только для чтения **Синтаксическая структура:** Integer

Группа/Объект	Описание
	Идентификатор объекта: .1.3.6.1.2.1.17.7.1.2.2.1.3.255.148.184.197.5.176.0 **Определение:** Статус этой записи. который может принимать значения: • other(1) — ни одно из перечисленных ниже. Это может включать ситуации, когда некий другой объект MIB (не соответствующий экземпляру dot1qTpFdbPort и не запись в dot1qStaticUnicastTable) используется для определения пересылки кадра, направленного по адресу из соответствующего dot1qTpFdbAddress. • invalid(2) — запись больше не пригодна (например, она уже устарела), но еще остается в таблице. • learned(3) — значение соответствующего экземпляра dot1qTpFdbPort определено и используется. • self(4) — значение соответствующего экземпляра dot1qTpFdbAddress представляет один из адресов устройства. Соответствующий экземпляр dot1qTpFdbPort показывает, какой из портов устройства имеет этот адрес. • mgmt(5) — значение соответствующего экземпляра dot1qTpFdbAddress является также значением имеющегося экземпляра dot1qStaticAddress.
Группа: qBridgeFdbMulticastGroup **Trap-уведомление:** dot1qTpGroupEgressPorts	**Доступ:** Только для чтения **Синтаксическая структура:** Integer **Идентификатор объекта:** .1.3.6.1.2.1.17.7.1.2.3.1.2 **Определение:** Полный набор портов в этой VLAN, на которые в настоящее время явно пересылаются кадры, предназначенные для этого MAC-адреса группы. Это не включает порты, для которых этот адрес пересылается только неявно, в список dot1qForwardAllPorts.
Группа: qBridgeFdbMulticastGroup **Trap-уведомление:** dot1qTpGroupLearnt	**Доступ:** Только для чтения **Синтаксическая структура:** Integer **Идентификатор объекта:** .1.3.6.1.2.1.17.7.1.2.3.1.3 **Определение:** Подмножество портов в dot1qTpGroupEgressPorts, которые были изучены GMRP или каким-либо другим динамическим механизмом в этой базе данных фильтрации.
Группа: qBridgeVlanGroup **Trap-уведомление:** dot1qVlanCreationTime	**Доступ:** Только для чтения **Синтаксическая структура:** Timeticks **Идентификатор объекта:** .1.3.6.1.2.1.17.7.1.4.2.1.7 **Определение:** Значение sysUpTime при создании этой виртуальной сети VLAN.
Группа: qBridgeVlanGroup **Trap-уведомление:** dot1qVlanCurrentEgressPorts	**Доступ:** Только для чтения **Синтаксическая структура:** Hex-String **Идентификатор объекта:** .1.3.6.1.2.1.17.7.1.4.2.1.4 **Определение:** Набор портов, которые передают трафик для этой виртуальной сети VLAN как кадры с метками или без меток.
Группа: qBridgeVlanGroup **Trap-уведомление:** dot1qVlanCurrentUntaggedPorts	**Доступ:** Только для чтения **Синтаксическая структура:** Hex-String **Идентификатор объекта:** .1.3.6.1.2.1.17.7.1.4.2.1.5 **Определение:** Набор портов, которые передают трафик для этой виртуальной сети VLAN как кадры без меток.

Группа/Объект	Описание
Группа: qBridgeVlanGroup **Trap-уведомление:** dot1qVlanFdbId	**Доступ:** Только для чтения **Синтаксическая структура:** Gauge32 **Идентификатор объекта:** .1.3.6.1.2.1.17.7.1.4.2.1.3 **Определение:** База данных фильтрации, используемая этой виртуальной сетью VLAN. Это одно из значений dot1qFdbId в таблице dot1qFdbTable. Это значение автоматически присваивается устройством при создании виртуальной сети VLAN: либо динамически с помощью GVRP, либо системой управления в dot1qVlanStaticTable. Распределение этого значения соответствует ограничениям обучения, определенным для этой VLAN в таблице dot1qLearningConstraintsTable.
Группа: qBridgeVlanStaticGroup **Trap-уведомление:** dot1qVlanForbiddenEgressPorts	**Доступ:** Для чтения и создания **Синтаксическая структура:** String **Идентификатор объекта:** .1.3.6.1.2.1.17.7.1.4.3.1.3.22 **Определение:** Набор портов, которые запрещены системой управления для включения в список выходных портов для этой сети VLAN. Изменения этого объекта, которые приводят к включению или исключению порта, на уровне порта и VLAN влияют на управление регистратором и запрет регистрации для соответствующей машины состояний GVRP на каждом порту. Порт не может быть добавлен в этот набор, если он уже является членом набора портов в dot1qVlanStaticEgressPorts. Значение по умолчанию для этого объекта — строка нулей соответствующей длины, исключающая все порты из набора запрещенных.
Группа: qBridgeVlanGroup **Trap-уведомление:** dot1qVlanNumDeletes	**Доступ:** Только для чтения **Синтаксическая структура:** Counter32 **Идентификатор объекта:** .1.3.6.1.2.1.17.7.1.4.1 **Определение:** Количество раз, когда запись VLAN удалялась из dot1qVlanCurrentTable (по любой причине). Если запись удалена, затем вставлена, а затем удалена, этот счетчик будет увеличен на 2.
Группа: qBridgeVlanStaticGroup **Trap-уведомление:** dot1qVlanStaticEgressPorts	**Доступ:** Для чтения и создания **Синтаксическая структура:** String **Идентификатор объекта:** .1.3.6.1.2.1.17.7.1.4.3.1.2.22 **Определение:** Набор портов, которые постоянно назначены системой управления для включения в список выходных портов для этой сети VLAN. Изменения битов этого объекта на уровне порта и VLAN влияют на управление регистратором и фиксацию регистрации для соответствующей машины состояний GVRP на каждом порту. Порт не может быть добавлен в этот набор, если он уже является членом набора портов в dot1qVlanForbiddenEgressPorts. Значение этого объекта по умолчанию — строка последовательности нулей соответствующей длины, указывающая на отсутствие фиксации.
Группа: qBridgeVlanStaticGroup **Trap-уведомление:** dot1qVlanStaticName	**Доступ:** Для чтения и создания **Синтаксическая структура:** String **Идентификатор объекта:** .1.3.6.1.2.1.17.7.1.4.3.1.1.22 **Определение:** Назначенная администратором строка, которая может использоваться для идентификации сети VLAN.
Группа: qBridgeVlanStaticGroup **Trap-уведомление:** dot1qVlanStaticRowStatus	**Доступ:** Для чтения и создания **Синтаксическая структура:** Integer **Идентификатор объекта:** .1.3.6.1.2.1.17.7.1.4.3.1.5.22

Группа/Объект	Описание
	Определение: Объект указывает статус этой записи.
Группа: qBridgeVlanStaticGroup **Trap-уведомление:** dot1qVlanStaticUntaggedPorts	**Доступ:** Для чтения и создания **Синтаксическая структура:** String **Идентификатор объекта:** .1.3.6.1.2.1.17.7.1.4.3.1.4.22 **Определение:** Набор портов, которые должны передавать выходные пакеты для этой VLAN как пакеты без меток. Значение этого объекта по умолчанию для VLAN по умолчанию (dot1qVlanIndex = 1) представляет собой строку соответствующей длины, включающую все порты. Для других VLAN значение по умолчанию не указано. Если агент устройства не может поддерживать набор портов, он отклонит операцию набора с ошибкой. Например, менеджер может попытаться установить несколько VLAN для присвоения меток на выходе, если устройство не поддерживает эту опцию IEEE 802.1Q.
Группа: qBridgeVlanGroup **Trap-уведомление:** dot1qVlanStatus	**Доступ:** Только для чтения **Синтаксическая структура:** Integer **Идентификатор объекта:** .1.3.6.1.2.1.17.7.1.4.2.1.6 **Определение:** Объект указывает статус этой записи. • other(1) — эта запись в настоящее время используется, но условия, при которых она останется такой, отличаются от следующих значений. • permanent(2) — эта запись, соответствующая записи в dot1qVlanStaticTable, в настоящее время используется и останется таковой после следующего перезапуска устройства. Списки портов для этой записи включают порты из эквивалентной записи dot1qVlanStaticTable и динамически изученные порты. • dynamicGvrp(3) — эта запись в настоящее время используется и будет использоваться до тех пор, пока GVRP не удалит ее. Статическая запись для этой VLAN отсутствует, и она будет удалена, после вывода последнего порта из VLAN.
Группа: qBridgeBaseGroup **Trap-уведомление:** dot1qVlanVersionNumber	**Доступ:** Только для чтения **Синтаксическая структура:** Integer **Идентификатор объекта:** .1.3.6.1.2.1.17.7.1.1.1.0 **Определение:** Номер версии IEEE 802.1Q, поддерживаемой этим устройством.

RMON-MIB

Группа/Объект	Описание
Группа: rmonAlarmGroup **Trap-уведомление:** AlarmFallingEventIndex	**Доступ:** Для чтения и создания **Синтаксическая структура:** Integer **Идентификатор объекта:** 1.3.6.1.2.1.16.3.1.1.10.1 **Определение:** Индекс eventEntry, который используется при пересечении порога снижения. Объект eventEntry, идентифицированный конкретным значением этого индекса, представляет собой тот же объект, идентифицированный тем же значением объекта eventIndex. Если в eventTable нет соответствующей записи, то связь не существует. В частности, если это значение равно нулю, связанное событие генерироваться не будет, так как нуль не

Группа/Объект	Описание
	является допустимым индексом события. Этот объект не может быть изменен, если связанный объект alarmStatus равен значению valid(1).
Группа: rmonAlarmGroup **Trap-уведомление:** AlarmFallingThreshold	**Доступ:** Для чтения и создания **Синтаксическая структура:** Integer **Идентификатор объекта:** 1.3.6.1.2.1.16.3.1.1.8.1 **Определение:** Порог для выборочной статистики. Когда текущее выборочное значение меньше или равно этому пороговому значению, а значение в последнем интервале выборки больше этого порогового значения, генерируется одно событие. Одно событие также будет генерироваться, если первый экземпляр после этой записи становится меньше или равен этому пороговому значению и связанный alarmStartupAlarm равен fallingAlarm(2) или risingOrFallingAlarm(3). После генерации события снижения другое такое событие не будет генерироваться до тех пор, пока выборочное значение не поднимется выше этого порога и не достигнет alarmRisingThreshold. Этот объект не может быть изменен, если связанный объект alarmStatus равен значению valid(1).
Группа: rmonAlarmGroup **Trap-уведомление:** AlarmIndex	**Функционал агента:** RC-RMON-MIB-AC **Доступ:** Только для чтения **Синтаксическая структура:** Integer **Идентификатор объекта:** 1.3.6.1.2.1.16.3.1.1.1.1 **Определение:** Индекс, который однозначно идентифицирует запись в таблице аварийных сигналов. Каждая такая запись определяет диагностический экземпляр с определенным интервалом для объекта на устройстве. **Определение:** В таблице alarmTable может быть создано в среднем четыре записи на порт.
Группа: rmonAlarmGroup **Trap-уведомление:** AlarmInterval	**Функционал агента:** RC-RMON-MIB-AC **Доступ:** Для чтения и создания **Синтаксическая структура:** Integer **Идентификатор объекта:** 1.3.6.1.2.1.16.3.1.1.2.1 **Определение:** Интервал в секундах, в течение которого отбираются данные и сравниваются с возрастающими и снижающимися пороговыми значениями. При установке этой переменной следует соблюдать осторожность при выборке deltaValue — установленный интервал должен быть достаточно коротким, чтобы выборочная переменная увеличивалась или уменьшалась не более чем на 2^31 — 1 в течение одного интервала выборки. Этот объект не может быть изменен, если связанный объект alarmStatus равен значению valid(1). **Определение:** Значение alarmInterval по умолчанию — 60 секунд.
Группа: rmonAlarmGroup **Trap-уведомление:** AlarmOwner	**Функционал агента:** RC-RMON-MIB-AC **Доступ:** Для чтения и создания **Синтаксическая структура:** String **Идентификатор объекта:** 1.3.6.1.2.1.16.3.1.1.11.1 **Определение:** Объект, который сконфигурировал эту запись и поэтому использует назначенные ей ресурсы. **Определение:** Значением по умолчанию для alarmOwner является строка 'Monitor'.
Группа: rmonAlarmGroup	**Доступ:** Для чтения и создания

Группа/Объект	Описание
Trap-уведомление: AlarmRisingEventIndex	**Синтаксическая структура:** Integer **Идентификатор объекта:** 1.3.6.1.2.1.16.3.1.1.9.1 **Определение:** Индекс eventEntry, который используется при пересечении порога повышения. Объект eventEntry, идентифицированный конкретным значением этого индекса, представляет собой тот же объект, идентифицированный тем же значением объекта eventIndex. Если в eventTable нет соответствующей записи, то связь не существует. В частности, если это значение равно нулю, связанное событие генерироваться не будет, так как нуль не является допустимым индексом события. Этот объект не может быть изменен, если связанный объект alarmStatus равен значению valid(1).
Группа: rmonAlarmGroup **Trap-уведомление:** AlarmRisingThreshold	**Доступ:** Для чтения и создания **Синтаксическая структура:** Integer **Идентификатор объекта:** 1.3.6.1.2.1.16.3.1.1.7.1 **Определение:** Порог для выборочной статистики. Когда текущее выборочное значение больше или равно этому пороговому значению, а значение в последнем интервале выборки меньше этого порогового значения, генерируется одно событие. Одно событие также будет генерироваться, если первый экземпляр после этой записи становится больше или равен этому пороговому значению и связанный alarmStartupAlarm равен risingAlarm(1) или risingOrFallingAlarm(3). После генерации события повышения другое такое событие не будет генерироваться до тех пор, пока выборочное значение не снизится ниже этого порога и не достигнет alarmFallingThreshold. Этот объект не может быть изменен, если связанный объект alarmStatus равен значению valid(1).
Группа: rmonAlarmGroup **Trap-уведомление:** AlarmSampleType	**Функционал агента:** RC-RMON-MIB-AC **Доступ:** Для чтения и создания **Синтаксическая структура:** Integer **Идентификатор объекта:** 1.3.6.1.2.1.16.3.1.1.4.1 **Определение:** Метод выборки выбранной переменной и вычисления значения для сравнения с пороговыми значениями. Если значение этого объекта равно absoluteValue(1), значение выбранной переменной будет сравниваться непосредственно с пороговыми значениями в конце интервала выборки. Если значением этого объекта является deltaValue(2), значение выбранной переменной на последнем образце будет вычтено из текущего значения, а разница сравнивается с пороговыми значениями. Этот объект не может быть изменен, если связанный объект alarmStatus равен значению valid(1). **Определение:** Значение alarmSampleType по умолчанию — deltaValue(2).
Группа: rmonAlarmGroup **Trap-уведомление:** AlarmStartupAlarm	**Функционал агента:** RC-RMON-MIB-AC **Доступ:** Для чтения и создания **Синтаксическая структура:** Integer **Идентификатор объекта:** 1.3.6.1.2.1.16.3.1.1.6.1 **Определение:** Аварийный сигнал, который может быть отправлен, когда эта запись впервые установлена на действительное значение. Если первый экземпляр после этого ввода становится больше или равен возрастающему пороговому значению, а alarmStartupAlarm равен risingAlarm(1) или risingOrFallingAlarm(3), то генерируется один возрастающий сигнал тревоги. Если первый экземпляр после этого ввода становится меньше или равен снижающемуся

Группа/Объект	Описание
	пороговому значению, а alarmStartupAlarm равен fallingAlarm(2) или risingOrFallingAlarm(3), то генерируется один снижающийся сигнал тревоги. Этот объект не может быть изменен, если связанный объект alarmStatus равен значению valid(1). **Определение:** Значение alarmStartupAlarm по умолчанию — risingOrFallingAlarm(3).
Группа: rmonAlarmGroup **Trap-уведомление:** AlarmStatus	**Доступ:** Для чтения и создания **Синтаксическая структура:** Integer **Идентификатор объекта:** 1.3.6.1.2.1.16.3.1.1.12.1 **Определение:** Статус записи этого аварийного сигнала.
Группа: rmonAlarmGroup **Trap-уведомление:** AlarmValue	**Доступ:** Только для чтения **Синтаксическая структура:** Integer **Идентификатор объекта:** 1.3.6.1.2.1.16.3.1.1.5.1 **Определение:** Значение статистики за последний период выборки. Например, если типом выборки является deltaValue, это значение будет разницей между выборками в начале и конце периода. Если типом выборки является absoluteValue, это значение будет выборочным значением в конце периода. Это значение сравнивается с возрастающим и снижающимся пороговыми значениями. Значение в течение текущего периода выборки не доступно до завершения периода и останется доступным до завершения следующего периода.
Группа: rmonAlarmGroup **Trap-уведомление:** AlarmVariable	**Доступ:** Для чтения и создания **Синтаксическая структура:** Идентификатор объекта **Идентификатор объекта:** 1.3.6.1.2.1.16.3.1.1.3.1 **Определение:** Идентификатор объекта конкретной переменной, подлежащей выборке. Only variables that resolve to an ASN.1 primitive type of Integer (Integer, Integer32, Counter32, Counter64, Gauge, or TimeTicks) may be sampled. Поскольку управление доступом SNMP сформулировано полностью с точки зрения содержимого представлений MIB, не существует механизма управления доступом, который может ограничить значение этого объекта для идентификации только тех объектов, которые существуют в конкретном представлении MIB. Поскольку, таким образом, нет приемлемых средств ограничения доступа на чтение, который может быть получен через механизм сигнализации, датчик должен предоставлять доступ на запись к этому объекту только в тех видах, которые имеют доступ на чтение ко всем объектам на датчике. Во время заданной операции, если указанное имя переменной недоступно в выбранном представлении MIB, возвращается ошибка badValue. Если в любой момент времени имя переменной установленного alarmEntry больше не доступно в выбранном представлении MIB, датчик должен изменить статус этого alarmEntry на invalid(4). Этот объект не может быть изменен, если связанный объект alarmStatus равен значению valid(1).
Группа: rmonEthernetHistoryGroup **Trap-уведомление:** etherHistoryBroadcastPkts	**Доступ:** Только для чтения **Синтаксическая структура:** Counter32 **Идентификатор объекта:** 1.3.6.1.2.1.16.2.2.1.7.1 **Определение:** Количество пригодных пакетов, полученных в течение этого интервала выборки, которые были направлены на широковещательный адрес.
Группа: rmonEthernetHistoryGroup **Trap-уведомление:** etherHistoryCollisions	**Доступ:** Только для чтения **Синтаксическая структура:** Counter32

Группа/Объект	Описание
	Идентификатор объекта: 1.3.6.1.2.1.16.2.2.1.14.1 **Определение:** Наилучшая оценка общего количества столкновений на этом сегменте Ethernet в течение этого интервала выборки. Возвращаемое значение будет зависеть от местоположения датчика RMON. В разделе 8.2.1.3 (10BASE-5) и разделе 10.3.1.3 (10BASE-2) стандарта IEEE 802.3 говорится, что станция должна обнаруживать столкновение в режиме приема, если три или более станций одновременно осуществляют передачу. Порт повторителя должен обнаруживать столкновение, когда две или несколько станций передают данные одновременно. Таким образом, датчик, размещенный на порту повторителя, может регистрировать больше столкновений, чем датчик, подключенный к станции на том же сегменте. Местоположение датчика играет гораздо меньшую роль при использовании 10BASE-T. 14.2.1.4 (10BASE-T) стандарта IEEE 802.3 определяет столкновение как одновременное присутствие сигналов в цепях DO и RD (передача и прием одновременно). Станция 10BASE-T может обнаруживать столкновения только при передаче. Таким образом, датчики, размещенные на станции и повторители, должны сообщать о одинаковом количестве столкновений. Следует также отметить, что датчик RMON внутри повторителя должен в идеале сообщать о столкновениях между повторителем и одним или несколькими другими хостами (передавать столкновения, как определено IEEE 802.3k), а также столкновениях приемника, наблюдаемых на любых коаксиальных сегментах, к которым подключен повторитель.
Группа: rmonEthernetHistoryGroup **Trap-уведомление:** etherHistoryCRCAlignErrors	**Доступ:** Только для чтения **Синтаксическая структура:** Counter32 **Идентификатор объекта:** 1.3.6.1.2.1.16.2.2.1.9.1 **Определение:** Количество пакетов, полученных в течение этого интервала выборки, которые имели длину (исключая биты кадрирования, но включая октеты FCS) от 64 до 1518 октетов включительно, но имели либо неудачную последовательность проверки кадра (FCS) с целым числом октетов (ошибка FCS), либо неудачную FCS с нецелым числом октетов (ошибка выравнивания).
Группа: rmonEthernetHistoryGroup **Trap-уведомление:** etherHistoryDropEvents	**Доступ:** Только для чтения **Синтаксическая структура:** Counter32 **Идентификатор объекта:** 1.3.6.1.2.1.16.2.2.1.4.1 **Определение:** Общее количество событий, в которых пакеты были удалены датчиком из-за нехватки ресурсов в течение этого интервала выборки. Обратите внимание, что это число не обязательно является количеством отброшенных пакетов, это просто количество раз, когда это условие было обнаружено.
Группа: rmonEthernetHistoryGroup **Trap-уведомление:** etherHistoryFragments	**Доступ:** Только для чтения **Синтаксическая структура:** Counter32 **Идентификатор объекта:** 1.3.6.1.2.1.16.2.2.1.12.1 **Определение:** Общее количество пакетов, полученных в течение этого интервала выборки, длина которых составляла менее 64 октетов (за исключением битов кадрирования, но включая октеты FCS), и которые имели либо неудачную последовательность проверки кадра (FCS) с целым числом октетов (ошибка FCS), либо неудачную FCS с нецелым числом октетов (ошибка выравнивания). Обратите внимание, что приращение количества фрагментов etherHistoryFragments абсолютно нормально. Это связано с тем, что учитываются как пакеты

Группа/Объект	Описание
	с недопустимо малой длиной (которые являются нормальными из-за столкновений), так и кратковременные помехи.
Группа: rmonEthernetHistoryGroup **Trap-уведомление:** etherHistoryIndex	**Доступ:** Только для чтения **Синтаксическая структура:** Integer **Идентификатор объекта:** 1.3.6.1.2.1.16.2.2.1.1.1 **Определение:** История, частью которой является эта запись. История, идентифицированная по конкретному значению этого индекса, является такой же историей, как идентифицированная по тому же значению historyControlIndex.
Группа: rmonEthernetHistoryGroup **Trap-уведомление:** etherHistoryIntervalStart	**Доступ:** Только для чтения **Синтаксическая структура:** Timeticks **Идентификатор объекта:** 1.3.6.1.2.1.16.2.2.1.3.1 **Определение:** Значение sysUpTime в начале интервала, в течение которого измерялся этот экземпляр. Если датчик отслеживает время суток, он должен выполнить запуск первого экземпляра истории в такой момент времени, чтобы при начале следующего часа дня, экземпляр запускался именно в этот момент. Обратите внимание, что соблюдение этого правила может потребовать от датчика задержки выполнения выборку данных первого экземпляра истории, поскольку интервалы для каждого экземпляра должны быть одинаковы. Также обратите внимание, что экземпляр, выборка данных которого выполняется в настоящее время, недоступен в этой таблице до конца его интервала измерений.
Группа: rmonEthernetHistoryGroup **Trap-уведомление:** etherHistoryJabbers	**Доступ:** Только для чтения **Синтаксическая структура:** Counter32 **Идентификатор объекта:** 1.3.6.1.2.1.16.2.2.1.13.1 **Определение:** Количество пакетов, полученных в течение этого интервала выборки, которые были длиннее 1518 октетов (за исключением битов кадрирования, но включая октеты FCS), и имели либо неудачную последовательность проверки кадра (FCS) с целым числом октетов (ошибка FCS), либо неудачную FCS с нецелым числом октетов (ошибка выравнивания). Обратите внимание, что это определение сбойного пакета (jabber) отличается от определения в разделе 8.2.1.5 (10BASE5) и разделе 10.3.1.4 (10BASE2) IEEE-802.3. В этих документах любой пакет определяется как сбойный пакет при условии, что его длина превышает 20 мс. Допустимый диапазон обнаружения сбойного пакета составляет от 20 мс до 150 мс.
Группа: rmonEthernetHistoryGroup **Trap-уведомление:** etherHistoryMulticastPkts	**Доступ:** Только для чтения **Синтаксическая структура:** Counter32 **Идентификатор объекта:** 1.3.6.1.2.1.16.2.2.1.8.1 **Определение:** Количество пригодных пакетов, полученных в течение этого интервала выборки, которые были направлены на групповой адрес. Обратите внимание, что это число не включает пакеты, адресованные на широковещательный адрес.
Группа: rmonEthernetHistoryGroup **Trap-уведомление:** etherHistoryOctets	**Доступ:** Только для чтения **Синтаксическая структура:** Counter32 **Идентификатор объекта:** 1.3.6.1.2.1.16.2.2.1.5.1 **Определение:** Общее количество октетов данных (в том числе в недопустимых пакетах), полученных в сети (исключая биты кадрирования, но включая октеты FCS).

Группа/Объект	Описание
Группа: rmonEthernetHistoryGroup **Trap-уведомление:** etherHistoryOversizePkts	**Доступ:** Только для чтения **Синтаксическая структура:** Counter32 **Идентификатор объекта:** 1.3.6.1.2.1.16.2.2.1.11.1 **Определение:** Количество пакетов, полученных в течение этого интервала выборки, которые были длиннее 1518 октетов (исключая биты кадрирования, но включая октеты FCS), но были иным образом правильно сформированы.
Группа: rmonEthernetHistoryGroup **Trap-уведомление:** etherHistoryPkts	**Доступ:** Только для чтения **Синтаксическая структура:** Counter32 **Идентификатор объекта:** 1.3.6.1.2.1.16.2.2.1.6.1 **Определение:** Количество пакетов (включая недопустимые пакеты), полученных в течение этого интервала выборки.
Группа: rmonEthernetHistoryGroup **Trap-уведомление:** etherHistorySampleIndex	**Доступ:** Только для чтения **Синтаксическая структура:** Integer **Идентификатор объекта:** 1.3.6.1.2.1.16.2.2.1.2.1 **Определение:** Индекс, однозначно идентифицирующий конкретный экземпляр, который эта запись представляет среди всех экземпляров, связанных с одной и той же historyControlEntry. Этот индекс начинается с 1 и увеличивается на единицу при каждой новой выборке.
Группа: rmonEthernetHistoryGroup **Trap-уведомление:** etherHistoryUndersizePkts	**Доступ:** Только для чтения **Синтаксическая структура:** Counter32 **Идентификатор объекта:** 1.3.6.1.2.1.16.2.2.1.10.1 **Определение:** Количество пакетов, полученных в течение этого интервала выборки, которые были длиной менее 64 октетов (исключая биты кадрирования, но включая октеты FCS) и были иным образом правильно сформированы.
Группа: rmonEthernetHistoryGroup **Trap-уведомление:** etherHistoryUtilization	**Доступ:** Только для чтения **Синтаксическая структура:** Integer **Идентификатор объекта:** 1.3.6.1.2.1.16.2.2.1.15.1 **Определение:** Наилучшая оценка среднего использования сети физического уровня на этом интерфейсе в течение этого интервала выборки, в сотых процентах.
Группа: rmonEtherStatsGroup **Trap-уведомление:** etherStatsBroadcastPkts	**Доступ:** Только для чтения **Синтаксическая структура:** Counter32 **Идентификатор объекта:** 1.3.6.1.2.1.16.1.1.1.6.1 **Определение:** Общее количество полученных пригодных пакетов, которые были направлены на широковещательный адрес. Обратите внимание, что это не включает многоадресные пакеты.
Группа: rmonEtherStatsGroup **Trap-уведомление:** etherStatsCollisions	**Доступ:** Только для чтения **Синтаксическая структура:** Counter32 **Идентификатор объекта:** 1.3.6.1.2.1.16.1.1.1.13.1 **Определение:** Наилучшая оценка общего количества столкновений на этом сегменте Ethernet. Возвращаемое значение будет зависеть от местоположения датчика RMON. В разделе 8.2.1.3 (10BASE-5) и разделе 10.3.1.3 (10BASE-2) стандарта IEEE 802.3 говорится, что станция должна обнаруживать столкновение в режиме приема, если три или более станций одновременно осуществляют передачу. Порт

Группа/Объект	Описание
	повторителя должен обнаруживать столкновение, когда две или несколько станций передают данные одновременно. Таким образом, датчик, размещенный на порту повторителя, может регистрировать больше столкновений, чем датчик, подключенный к станции на том же сегменте. Местоположение датчика играет гораздо меньшую роль при использовании 10BASE-T. 14.2.1.4 (10BASE-T) стандарта IEEE 802.3 определяет столкновение как одновременное присутствие сигналов в цепях DO и RD (передача и прием одновременно). Станция 10BASE-T может обнаруживать столкновения только при передаче. Таким образом, датчики, размещенные на станции и повторители, должны сообщать о одинаковом количестве столкновений. Следует также отметить, что датчик RMON внутри повторителя должен в идеале сообщать о столкновениях между повторителем и одним или несколькими другими хостами (передавать столкновения, как определено IEEE 802.3k), а также столкновениях приемника, наблюдаемых на любых коаксиальных сегментах, к которым подключен повторитель.
Группа: rmonEtherStatsGroup **Trap-уведомление:** etherStatsCRCAlignErrors	**Доступ:** Только для чтения **Синтаксическая структура:** Counter32 **Идентификатор объекта:** 1.3.6.1.2.1.16.1.1.1.8.1 **Определение:** Общее количество полученных пакетов, которые имели длину (исключая биты кадрирования, но включая октеты FCS) от 64 до 1518 октетов включительно, но имели либо неудачную последовательность проверки кадра (FCS) с целым числом октетов (ошибка FCS), либо неудачную FCS с нецелым числом октетов (ошибка выравнивания).
Группа: rmonEtherStatsGroup **Trap-уведомление:** etherStatsDataSource	**Доступ:** Для чтения и создания **Идентификатор объекта:** 1.3.6.1.2.1.16.1.1.1.2.1 **Определение:** Этот объект определяет источник данных, для анализа которых сконфигурирована эта запись etherStats. Этим источником может быть любой интерфейс Ethernet на этом устройстве. Чтобы идентифицировать конкретный интерфейс, этот объект должен идентифицировать экземпляр объекта ifIndex, определенного в RFC 2233 [17], для требуемого интерфейса. Например, если запись будет получать данные из интерфейса #1, этот объект будет установлен на ifIndex.1. Статистика в этой группе отражает все пакеты на сегменте локальной сети, подключенном к идентифицированному интерфейсу. Агент может или не может определить, произошли ли фундаментальные изменения в носителе интерфейса и требуют признания этой записи недействительной. Например, карту Ethernet с возможностью подключения в «горячем» режиме можно извлечь и заменить картой с поддержкой Token Ring. В таком случае, если агент имеет такую информацию об изменении, рекомендуется аннулировать эту запись. Этот объект не может быть изменен, если связанный объект etherStatsStatus равен значению valid(1).
Группа: rmonEtherStatsGroup **Trap-уведомление:** etherStatsDropEvents	**Доступ:** Только для чтения **Синтаксическая структура:** Counter32 **Идентификатор объекта:** 1.3.6.1.2.1.16.1.1.1.3.1 **Определение:** Общее количество событий, в которых пакеты были удалены датчиком из-за нехватки ресурсов. Обратите внимание, что это число не обязательно является количеством отброшенных пакетов, это просто количество раз, когда это условие было обнаружено.
Группа: rmonEtherStatsGroup	**Доступ:** Только для чтения

Группа/Объект	Описание
Trap-уведомление: etherStatsFragments	**Синтаксическая структура:** Counter32 **Идентификатор объекта:** 1.3.6.1.2.1.16.1.1.1.11.1 **Определение:** Общее количество полученных пакетов, длина которых составляла менее 64 октетов (за исключением битов кадрирования, но включая октеты FCS), и которые имели либо неудачную последовательность проверки кадра (FCS) с целым числом октетов (ошибка FCS), либо неудачную FCS с нецелым числом октетов (ошибка выравнивания). Обратите внимание, что приращение количества фрагментов etherStatsFragments абсолютно нормально. Это связано с тем, что учитываются как пакеты с недопустимо малой длиной (которые являются нормальными из-за столкновений), так и кратковременные помехи.
Группа: rmonEtherStatsGroup **Trap-уведомление:** etherStatsIndex	**Функционал агента:** RC-RMON-MIB-AC **Доступ:** Только для чтения **Синтаксическая структура:** Integer **Идентификатор объекта:** 1.3.6.1.2.1.16.1.1.1.1.1 **Определение:** Значение этого объекта однозначно идентифицирует эту запись etherStats. **Примечание** В таблице etherStatsTable создается по две записи на порт.
Группа: rmonEtherStatsGroup **Trap-уведомление:** etherStatsJabbers	**Доступ:** Только для чтения **Синтаксическая структура:** Counter32 **Идентификатор объекта:** 1.3.6.1.2.1.16.1.1.1.12.1 **Определение:** Общее количество полученных пакетов, которые были длиннее 1518 октетов (за исключением битов кадрирования, но включая октеты FCS), и имели либо неудачную последовательность проверки кадра (FCS) с целым числом октетов (ошибка FCS), либо неудачную FCS с нецелым числом октетов (ошибка выравнивания). Обратите внимание, что это определение сбойного пакета (jabber) отличается от определения в разделе 8.2.1.5 (10BASE5) и разделе 10.3.1.4 (10BASE2) IEEE-802.3. В этих документах любой пакет определяется как сбойный пакет при условии, что его длина превышает 20 мс. Допустимый диапазон обнаружения сбойного пакета составляет от 20 мс до 150 мс.
Группа: rmonEtherStatsGroup **Trap-уведомление:** etherStatsMulticastPkts	**Доступ:** Только для чтения **Синтаксическая структура:** Counter32 **Идентификатор объекта:** 1.3.6.1.2.1.16.1.1.1.7.1 **Определение:** Общее количество полученных пригодных пакетов, которые были направлены на групповой адрес. Обратите внимание, что это число не включает пакеты, направленные на широковещательный адрес.
Группа: rmonEtherStatsGroup **Trap-уведомление:** etherStatsOctets	**Доступ:** Только для чтения **Синтаксическая структура:** Counter32 **Идентификатор объекта:** 1.3.6.1.2.1.16.1.1.1.4.1 **Определение:** Общее количество октетов данных (в том числе в недопустимых пакетах), полученных в сети (исключая биты кадрирования, но включая октеты FCS). Этот объект может быть использован в качестве обоснованной оценки использования Ethernet 10-Megabit. Если требуется большая точность, экземпляры объектов

Группа/Объект	Описание

	etherStatsPkts и etherStatsOctets должны отбираться до и после общего интервала. Различия в выбранных значениях составляют Pkts и Octets, соответственно, а количество секунд в интервале — Interval. Эти значения используются для расчета использования следующим образом:
	
	`Pkts * (9.6 + 6.4) + (Octets * .8)`
	`Utilization = ----------------------------------`
	`Interval * 10,000`
	
	Результатом этого уравнения является значение использования, которое представляет собой процент использования сегмента Ethernet по шкале от 0 до 100 процентов.

Группа: rmonEtherStatsGroup **Trap-уведомление:** etherStatsOversizePkts	**Доступ:** Только для чтения **Синтаксическая структура:** Counter32 **Идентификатор объекта:** 1.3.6.1.2.1.16.1.1.1.10.1 **Определение:** Общее количество полученных пакетов, которые были длиннее 1518 октетов (исключая биты кадрирования, но включая октеты FCS) и были иным образом правильно сформированы.
Группа: rmonEtherStatsGroup **Trap-уведомление:** etherStatsOwner	**Функционал агента:** RC-RMON-MIB-AC **Доступ:** Для чтения и создания **Синтаксическая структура:** String **Идентификатор объекта:** 1.3.6.1.2.1.16.1.1.1.20.1 **Определение:** Объект, который сконфигурировал эту запись и поэтому использует назначенные ей ресурсы. **Определение:** Значение этой записи всегда устанавливается на 'Monitor', и не может быть изменено.
Группа: rmonEtherStatsGroup **Trap-уведомление:** etherStatsPkts	**Доступ:** Только для чтения **Синтаксическая структура:** Counter32 **Идентификатор объекта:** 1.3.6.1.2.1.16.1.1.1.5.1 **Определение:** Общее количество полученных пакетов (включая недопустимые пакеты, широковещательные пакеты и многоадресные пакеты).
Группа: rmonEtherStatsGroup **Trap-уведомление:** etherStatsPkts1024to1518Octets	**Доступ:** Только для чтения **Синтаксическая структура:** Counter32 **Идентификатор объекта:** 1.3.6.1.2.1.16.1.1.1.19.1 **Определение:** Общее количество полученных пакетов (включая недопустимые пакеты), которые имели длину от 1024 до 1518 октетов включительно (исключая биты кадрирования, но включая октеты FCS).
Группа: rmonEtherStatsGroup **Trap-уведомление:** etherStatsPkts128to255Octets	**Доступ:** Только для чтения **Синтаксическая структура:** Counter32 **Идентификатор объекта:** 1.3.6.1.2.1.16.1.1.1.16.1 **Определение:** Общее количество полученных пакетов (включая недопустимые пакеты), которые имели длину от 128 до 255 октетов включительно (исключая биты кадрирования, но включая октеты FCS).
Группа: rmonEtherStatsGroup **Trap-уведомление:** etherStatsPkts256to511Octets	**Доступ:** Только для чтения **Синтаксическая структура:** Counter32

Группа/Объект	Описание
	Идентификатор объекта: 1.3.6.1.2.1.16.1.1.1.17.1 **Определение:** Общее количество полученных пакетов (включая недопустимые пакеты), которые имели длину от 256 до 511 октетов включительно (исключая биты кадрирования, но включая октеты FCS).
Группа: rmonEtherStatsGroup **Trap-уведомление:** etherStatsPkts512to1023Octets	**Доступ:** Только для чтения **Синтаксическая структура:** Counter32 **Идентификатор объекта:** 1.3.6.1.2.1.16.1.1.1.18.1 **Определение:** Общее количество полученных пакетов (включая недопустимые пакеты), которые имели длину от 512 до 1023 октетов включительно (исключая биты кадрирования, но включая октеты FCS).
Группа: rmonEtherStatsGroup **Trap-уведомление:** etherStatsPkts64Octets	**Доступ:** Только для чтения **Синтаксическая структура:** Counter32 **Идентификатор объекта:** 1.3.6.1.2.1.16.1.1.1.14.1 **Определение:** Общее количество полученных пакетов (включая недопустимые пакеты), которые имели длину 64 октета (исключая биты кадрирования, но включая октеты FCS).
Группа: rmonEtherStatsGroup **Trap-уведомление:** etherStatsPkts65to127Octets	**Доступ:** Только для чтения **Синтаксическая структура:** Counter32 **Идентификатор объекта:** 1.3.6.1.2.1.16.1.1.1.15.1 **Определение:** Общее количество полученных пакетов (включая недопустимые пакеты), которые имели длину от 65 до 127 октетов включительно (исключая биты кадрирования, но включая октеты FCS).
Группа: rmonEtherStatsGroup **Trap-уведомление:** etherStatsStatus	**Функционал агента:** RC-RMON-MIB-AC **Доступ:** Для чтения и создания **Синтаксическая структура:** Integer **Идентификатор объекта:** 1.3.6.1.2.1.16.1.1.1.21.1 **Определение:** Статус этой записи etherStats. **Примечание** Одна запись на порт создается в таблице etherStatsTable при восходящей инициализации. Эти записи не могут быть изменены или удалены. Невозможно создать новые записи. Поэтому historyControlStatus всегда имеет значение valid(1).
Группа: rmonEtherStatsGroup **Trap-уведомление:** etherStatsUndersizePkts	**Доступ:** Только для чтения **Синтаксическая структура:** Counter32 **Идентификатор объекта:** 1.3.6.1.2.1.16.1.1.1.9.1 **Определение:** Общее количество полученных пакетов, которые были длиной менее 64 октетов (исключая биты кадрирования, но включая октеты FCS) и были иным образом правильно сформированы.
Группа: rmonEventGroup **Trap-уведомление:** eventCommunity	**Функционал агента:** RC-RMON-MIB-AC **Доступ:** Для чтения и создания **Синтаксическая структура:** String **Идентификатор объекта:** 1.3.6.1.2.1.16.9.1.1.4.1 **Определение:** Если должна быть отправлена SNMP-ловушка, она будет отправлена в SNMP-сообщество, указанное этой октетной строкой.

Группа/Объект	Описание
	Определение: Для этого объекта поддерживается строка длиной до 30 символов.
Группа: rmonEventGroup **Trap-уведомление:** eventDescription	**Функционал агента:** RC-RMON-MIB-AC **Доступ:** Для чтения и создания **Синтаксическая структура:** String **Идентификатор объекта:** 1.3.6.1.2.1.16.9.1.1.2.1 **Определение:** Комментарий, описывающий эту запись события.
Группа: rmonEventGroup **Trap-уведомление:** eventIndex	**Функционал агента:** RC-RMON-MIB-AC **Доступ:** Только для чтения **Синтаксическая структура:** Integer **Идентификатор объекта:** 1.3.6.1.2.1.16.9.1.1.1.1 **Определение:** Индекс, который однозначно идентифицирует запись в таблице событий. Каждая такая запись определяет одно событие, которое должно быть сгенерировано при возникновении соответствующих условий. **Определение:** В eventTable может быть создано в среднем по одной записи на alarmEntry.
Группа: rmonEventGroup **Trap-уведомление:** eventLastTimeSent	**Функционал агента:** RC-RMON-MIB-AC **Доступ:** Только для чтения **Синтаксическая структура:** Timeticks **Идентификатор объекта:** 1.3.6.1.2.1.16.9.1.1.5.1 **Определение:** Значение sysUpTime на момент последней генерации события записью события. Если эта запись не генерирует никаких событий, это значение будет равно нулю.
Группа: rmonEventGroup **Trap-уведомление:** eventOwner	**Функционал агента:** RC-RMON-MIB-AC **Доступ:** Для чтения и создания **Синтаксическая структура:** String **Идентификатор объекта:** 1.3.6.1.2.1.16.9.1.1.6.1 **Определение:** Объект, который сконфигурировал эту запись и поэтому использует назначенные ей ресурсы. Если этот объект содержит строку, начинающуюся с «monitor», и имеет связанные записи в таблице журнала, все подключенные станции управления должны получить эти записи журнала, поскольку они могут иметь значение для всех станций управления, подключенных к этому устройству. **Определение:** Значение eventOwner по умолчанию — строка Monitor.
Группа: rmonEventGroup **Trap-уведомление:** eventStatus	**Доступ:** Для чтения и создания **Синтаксическая структура:** Integer **Идентификатор объекта:** 1.3.6.1.2.1.16.9.1.1.7.1 **Определение:** Статус записи об этом событии. Если этот объект не равен valid(1), агент удаляет все связанные записи журнала.
Группа: rmonEventGroup **Trap-уведомление:** eventType	**Функционал агента:** RC-RMON-MIB-AC **Доступ:** Для чтения и создания **Синтаксическая структура:** Integer **Идентификатор объекта:** 1.3.6.1.2.1.16.9.1.1.3.1 **Определение:** Тип уведомления датчика об этом событии. В случае журнала для каждого события делается запись в таблице журнала.

Группа/Объект	Описание
	В случае snmp-ловушки SNMP-ловушка отправляется на одну или несколько станций управления. **Определение:** Значение eventType по умолчанию — logandtrap(4).
Группа: rmonHistoryControlGroup **Trap-уведомление:** historyControlBucketsGranted	**Доступ:** Только для чтения **Синтаксическая структура:** Integer **Идентификатор объекта:** 1.3.6.1.2.1.16.2.1.1.4.1 **Определение:** Количество интервалов дискретной выборки, в течение которых данные должны быть сохранены в части таблицы для конкретного носителя, связанной с этой записью historyControlEntry. При создании или изменении связанного объекта historyControlBucketsRequested датчик должен установить этот объект как можно ближе к запрашиваемому значению для конкретной реализации датчика и доступных ресурсов. Датчик не должен снижать это значение, кроме как в результате изменения связанного объекта historyControlBucketsRequested. Возможны случаи, когда фактическое количество блоков памяти, связанных с этой записью, будет меньше значения этого объекта. В этом случае в конце каждого интервала выборки в таблицу для конкретного носителя будет добавлен новый блок памяти. Когда количество блоков памяти достигает значения этого объекта и новый блок памяти должен быть добавлен в таблицу для конкретного носителя, самый старый блок памяти, связанный с этой historyControlEntry, должен быть удален агентом, чтобы можно было добавить новый. Когда значение этого объекта меняется на значение, меньшее текущего значения, записи удаляются из таблицы, относящейся к конкретному носителю, связанной с этой historyControlEntry. Достаточное количество старых записей должны быть удалены агентом, чтобы их количество оставалось меньше или равно новому значению этого объекта. Когда значение этого объекта изменяется на значение, превышающее текущее значение, количество связанных записей, специфичных для носителя, может увеличиваться.
Группа: rmonHistoryControlGroup **Trap-уведомление:** historyControlBucketsRequested	**Функционал агента:** RC-RMON-MIB-AC **Доступ:** Для чтения и создания **Синтаксическая структура:** Integer **Идентификатор объекта:** 1.3.6.1.2.1.16.2.1.1.3.1 **Определение:** Количество интервалов дискретной выборки, в течение которых данные должны быть сохранены в части таблицы для конкретного носителя, связанной с этой записью historyControlEntry. При создании или изменении этого объекта датчик должен установить historyControlBucketsGranted как можно ближе к этому объекту для конкретной реализации датчика и доступных ресурсов. **Определение:** Ограничение для значения historyControBucketRequested равно 4000.
Группа: rmonHistoryControlGroup **Trap-уведомление:** historyControlDataSource	**Доступ:** Для чтения и создания **Синтаксическая структура:** Идентификатор объекта **Идентификатор объекта:** 1.3.6.1.2.1.16.2.1.1.2.1 **Определение:** Этот объект определяет источник данных, для которого были собраны исторические данные и помещены в таблицу для конкретного носителя от имени этой historyControlEntry. Этим источником может быть любой интерфейс на этом устройстве. Чтобы идентифицировать конкретный интерфейс, этот объект должен идентифицировать экземпляр объекта ifIndex, определенного в RFC 2233 [17], для требуемого интерфейса. Например, если запись будет

Группа/Объект	Описание
	получать данные из интерфейса #1, этот объект будет установлен на ifIndex.1. Статистика в этой группе отражает все пакеты на сегменте локальной сети, подключенном к идентифицированному интерфейсу. Агент может или не может определить, произошли ли фундаментальные изменения в носителе интерфейса и требуют признания этой записи недействительной. Например, карту Ethernet с возможностью подключения в «горячем» режиме можно извлечь и заменить картой с поддержкой Token Ring. В таком случае, если агент имеет такую информацию об изменении, рекомендуется аннулировать эту запись. Этот объект не может быть изменен, если связанный объект historyControlStatus равен значению valid(1).
Группа: rmonHistoryControlGroup **Trap-уведомление:** historyControlIndex	**Функционал агента:** RC-RMON-MIB-AC **Доступ:** Только для чтения **Синтаксическая структура:** Integer **Идентификатор объекта:** 1.3.6.1.2.1.16.2.1.1.1.1 **Определение:** Индекс, который однозначно идентифицирует запись в таблице historyControl. Каждая такая запись определяет набор экземпляров с определенным интервалом для интерфейса на устройстве. **Определение:** В таблице historyControlTable может быть создано в среднем четыре записи на Ethernet-порт.
Группа: rmonHistoryControlGroup **Trap-уведомление:** historyControlInterval	**Доступ:** Для чтения и создания **Синтаксическая структура:** Integer **Идентификатор объекта:** 1.3.6.1.2.1.16.2.1.1.5.1 **Определение:** Интервал в секундах, в течение которого данные отбираются для каждого блока памяти в части таблицы, относящейся к конкретному носителю, связанной с этой historyControlEntry. Этот интервал может быть установлен на любое количество секунд от 1 до 3600 (1 час). Поскольку счетчики в блоке памяти могут переполняться при их максимальном значении без указания, предусмотрительный менеджер будет учитывать возможность переполнения в любом из связанных счетчиков. Важно учитывать минимальное время, в течение которого любой счетчик может переполниться на определенном типе носителя, и установить для объекта historyControlInterval значение меньше этого интервала. Это, как правило, наиболее важно для счетчика «октетов» в любой таблице для конкретного носителя. Например, в сети Ethernet счетчик etherHistoryOctets может переполниться примерно за час при максимальном использовании Ethernet. Этот объект не может быть изменен, если связанный объект historyControlStatus равен значению valid(1).
Группа: rmonHistoryControlGroup **Trap-уведомление:** historyControlOwner	**Функционал агента:** RC-RMON-MIB-AC **Доступ:** Для чтения и создания **Синтаксическая структура:** String **Идентификатор объекта:** 1.3.6.1.2.1.16.2.1.1.6.1 **Определение:** Объект, который сконфигурировал эту запись и поэтому использует назначенные ей ресурсы. **Определение:** Значением по умолчанию для historyControlOwner является строка 'Monitor'.
Группа: rmonHistoryControlGroup **Trap-уведомление:** historyControlStatus	**Доступ:** Для чтения и создания **Синтаксическая структура:** Integer **Идентификатор объекта:** 1.3.6.1.2.1.16.2.1.1.7.1

Группа/Объект	Описание
	Определение: Статус этой записи historyControl. Каждый экземпляр таблицы, связанной с этим элементом historyControlEntry, будет удален агентом, если этот элемент historyControlEntry не равен valid(1).
Группа: rmonEventGroup **Trap-уведомление:** logDescription	**Доступ:** Только для чтения **Синтаксическая структура:** String **Идентификатор объекта:** 1.3.6.1.2.1.16.9.2.1.4.1 **Определение:** Описание события, активировавшего эту запись журнала, зависящее от реализации.
Группа: rmonEventGroup **Trap-уведомление:** logEventIndex	**Доступ:** Только для чтения **Синтаксическая структура:** Integer **Идентификатор объекта:** 1.3.6.1.2.1.16.9.2.1.1.1 **Определение:** Запись события, которая сгенерировала эту запись журнала. Журнал, идентифицированный определенным значением этого индекса, связан с той же eventEntry, что и идентифицированный тем же значением eventIndex.
Группа: rmonEventGroup **Trap-уведомление:** logIndex	**Функционал агента:** RC-RMON-MIB-AC **Доступ:** Только для чтения **Синтаксическая структура:** Integer **Идентификатор объекта:** 1.3.6.1.2.1.16.9.2.1.2.1 **Определение:** Индекс, однозначно идентифицирующий запись в таблице журнала среди записей, сгенерированных одними и теми же eventEntries. Эти индексы назначаются начиная с 1 и увеличиваются на единицу с каждой новой записью журнала. Связь между значениями logIndex и logEntries фиксируется на протяжении всего срока службы каждой logEntry. Агент может удалить самые старые экземпляры logEntry по мере необходимости из-за нехватки памяти. Вопрос о том, когда может произойти это удаление, зависит от реализации. **Примечание** Для каждого значения eventEntry может быть создано сто записей в таблице logTable. Значение этого объекта будет увеличиваться для каждого нового журнала, сгенерированного для соответствующего события. Когда значение этого объекта становится больше 100, самые старые записи будут удалены.
Группа: rmonEventGroup **Trap-уведомление:** logTime	**Доступ:** Только для чтения **Синтаксическая структура:** Timeticks **Идентификатор объекта:** 1.3.6.1.2.1.16.9.2.1.3.1 **Определение:** Значение sysUpTime при создании этой записи журнала.

RS-232-MIB

Группа/Объект	Описание
Группа: rs232AsyncGroup **Trap-уведомление:** rs232AsyncPortAutobaud	**Доступ:** Для чтения и записи **Синтаксическая структура:** Integer **Идентификатор объекта:** 1.3.6.1.2.1.10.33.3.1.3.101 **Определение:** Управление способностью порта автоматически определять скорость ввода. Когда rs232PortAutoBaud включен, порт

Группа/Объект	Описание
	может автоматически передавать значения, отличные от заданных значений скорости, четности и размера символов. В результате система управления сетью может временно наблюдать значения, отличные от ранее установленных.
Группа: rs232AsyncGroup **Trap-уведомление:** rs232AsyncPortBits	**Доступ:** Для чтения и записи **Синтаксическая структура:** Integer **Идентификатор объекта:** 1.3.6.1.2.1.10.33.2.1.5.1.4 **Определение:** Количество битов порта в символе.
Группа: rs232AsyncGroup **Trap-уведомление:** rs232AsyncPortFramingErrs	**Доступ:** Только для чтения **Синтаксическая структура:** Counter32 **Идентификатор объекта:** 1.3.6.1.2.1.10.33.2.1.5.1.2 **Определение:** Общее количество символов с ошибкой кадрирования, введенных из порта с момента повторной инициализации системы и в то время как состояние порта было up или test.
Группа: rs232AsyncGroup **Trap-уведомление:** rs232AsyncPortIndex	**Доступ:** Только для чтения **Синтаксическая структура:** Integer **Идентификатор объекта:** 1.3.6.1.2.1.10.33.2.1.5.1.1 **Определение:** Уникальное значение для каждого порта. Его значение аналогично rs232PortIndex для порта.
Группа: rs232AsyncGroup **Trap-уведомление:** rs232AsyncPortOverrunErrs	**Доступ:** Только для чтения **Синтаксическая структура:** Counter32 **Идентификатор объекта:** 1.3.6.1.2.1.10.33.2.1.5.1.3 **Определение:** Общее количество символов с ошибкой переполнения, введенных из порта с момента повторной инициализации системы и в то время как состояние порта было up или test.
Группа: rs232AsyncGroup **Trap-уведомление:** rs232AsyncPortParity	**Доступ:** Для чтения и записи **Синтаксическая структура:** Integer **Идентификатор объекта:** 1.3.6.1.2.1.10.33.1.0 **Определение:** Опознавание портом бита четности символов.
Группа: rs232AsyncGroup **Trap-уведомление:** rs232AsyncPortParityErrs	**Доступ:** Только для чтения **Синтаксическая структура:** Counter32 **Идентификатор объекта:** 1.3.6.1.2.1.10.33.2.1.6.1.4 **Определение:** Общее количество символов с ошибкой четности, введенных из порта с момента повторной инициализации системы и в то время как состояние порта было up или test.
Группа: rs232AsyncGroup **Trap-уведомление:** rs232AsyncPortStopBits	**Доступ:** Для чтения и записи **Синтаксическая структура:** Integer **Идентификатор объекта:** 1.3.6.1.2.1.10.33.2.1.6.1.2 **Определение:** Номер порта стоповых битов.
Группа: rs232Group **Trap-уведомление:** rs232InSigChanges	**Доступ:** Только для чтения **Синтаксическая структура:** Counter32 **Идентификатор объекта:** 1.3.6.1.2.1.10.33.2.1.6.1.1 **Определение:** Количество раз, когда сигнал менялся с on на off или с off на on.
Группа: rs232Group	**Доступ:** Только для чтения

Группа/Объект	Описание
Trap-уведомление: rs232InSigName	**Синтаксическая структура:** Integer **Идентификатор объекта:** 1.3.6.1.2.1.10.33.2.1.6.1.3 **Определение:**>Идентификация аппаратного сигнала следующим образом: • rts: Запрос на передачу • cts: Готовность к передаче • dsr: Готовность канала связи • dtr: Готовность терминала • ri: Запрос на установку соединения от удаленного коммуникационного устройства • dcd: Обнаружение принимаемого сигнала • sq: Определение качества принимаемого сигнала • srs: Выбор скорости передачи данных • srts: Запрос на передачу по второму (резервному) каналу • scts: Готовность к передаче по второму (резервному) каналу • sdcd: Обнаружение принимаемого сигнала по второму (резервному) каналу
Группа: rs232Group **Trap-уведомление:** rs232InSigPortIndex	**Доступ:** Только для чтения **Синтаксическая структура:** Integer **Идентификатор объекта:** 1.3.6.1.2.1.10.33.2.1.1.101 **Определение:** Значение rs232PortIndex для порта, которому принадлежит эта запись.
Группа: rs232Group **Trap-уведомление:** rs232InSigState	**Доступ:** Только для чтения **Синтаксическая структура:** Integer **Идентификатор объекта:** 1.3.6.1.2.1.10.33.2.1.7.101 **Определение:** Текущее состояние сигнала.
Группа: rs232Group **Trap-уведомление:** rs232Number	**Доступ:** Только для чтения **Синтаксическая структура:** Integer **Идентификатор объекта:** 1.3.6.1.2.1.10.33.2.1.3.101 **Определение:** Количество портов (независимо от их текущего состояния) в общей таблице портов RS-232.
Группа: rs232Group **Trap-уведомление:** rs232OutSigChanges	**Доступ:** Только для чтения **Синтаксическая структура:** Integer **Идентификатор объекта:** 1.3.6.1.2.1.10.33.2.1.5.101 **Определение:** Количество раз, когда сигнал менялся с on на off или с off на on.
Группа: rs232Group **Trap-уведомление:** rs232OutSigName	**Доступ:** Только для чтения **Синтаксическая структура:** Integer **Идентификатор объекта:** 1.3.6.1.2.1.10.33.2.1.7.101 **Определение:** Идентификация аппаратного сигнала следующим образом: • rts: Запрос на передачу • cts: Готовность к передаче • dsr: Готовность канала связи • dtr: Готовность терминала

Группа/Объект	Описание
	• ri: Запрос на установку соединения от удаленного коммуникационного устройства • dcd: Обнаружение принимаемого сигнала • sq: Определение качества принимаемого сигнала • srs: Выбор скорости передачи данных • srts: Запрос на передачу по второму (резервному) каналу • scts: Готовность к передаче по второму (резервному) каналу • sdcd: Обнаружение принимаемого сигнала по второму (резервному) каналу
Группа: rs232Group **Trap-уведомление:** rs232OutSigPortIndex	**Доступ:** Только для чтения **Синтаксическая структура:** Integer **Идентификатор объекта:** 1.3.6.1.2.1.10.33.2.1.4.101 **Определение:** Значение rs232PortIndex для порта, которому принадлежит эта запись.
Группа: rs232Group **Trap-уведомление:** rs232OutSigState	**Доступ:** Только для чтения **Синтаксическая структура:** Integer **Идентификатор объекта:** 1.3.6.1.2.1.10.33.2.1.5.101 **Определение:** Текущее состояние сигнала.
Группа: rs232Group **Trap-уведомление:** rs232PortIndex	**Доступ:** Только для чтения **Синтаксическая структура:** Integer **Идентификатор объекта:** 1.3.6.1.2.1.10.33.2.1.2.101 **Определение:** Значение IfIndex для порта. По общему правилу и по возможности номера аппаратных портов привязываются непосредственно к внешним разъемам. Значение для каждого порта должно оставаться постоянным, по крайней мере, от одной повторной инициализации агента управления сетью до следующей.
Группа: rs232Group **Trap-уведомление:** rs232PortInFlowType	**Доступ:** Для чтения и записи **Синтаксическая структура:** Integer **Идентификатор объекта:** 1.3.6.1.6.3.10.2.1.2.0 **Определение:** Тип управления входным потоком порта; «none» указывает на отсутствие управления потоком на этом уровне. «ctsRts» и «dsrDtr» указывают на использование указанных аппаратных сигналов.
Группа: rs232Group **Trap-уведомление:** rs232PortInSigNumber	**Доступ:** Только для чтения **Синтаксическая структура:** Integer **Идентификатор объекта:** 1.3.6.1.6.3.10.2.1.1.0 **Определение:** Количество входных сигналов для порта в таблице входных сигналов (rs232PortInSigTable). Таблица содержит записи только для тех сигналов, которые могут быть обнаружены программным обеспечением и целесообразны для наблюдения.
Группа: rs232Group **Trap-уведомление:** rs232PortInSpeed	**Доступ:** Для чтения и записи **Синтаксическая структура:** Integer **Идентификатор объекта:** 1.3.6.1.6.3.10.2.1.4.0 **Определение:** Входная скорость порта в битах в секунду. Обратите внимание, что нестандартные значения, такие как 9612, вероятно, недопустимы в большинстве вариантов реализации.
Группа: rs232Group	**Доступ:** Для чтения и записи

Группа/Объект	Описание
Trap-уведомление: rs232PortOutFlowType	**Синтаксическая структура:** Integer **Идентификатор объекта:** 1.3.6.1.6.3.10.2.1.3.0 **Определение:** Тип управления выходным потоком порта; «none» указывает на отсутствие управления потоком на этом уровне. «ctsRts» и «dsrDtr» указывают на использование указанных аппаратных сигналов.
Группа: rs232Group **Trap-уведомление:** rs232PortOutSigNumber	**Доступ:** Только для чтения **Синтаксическая структура:** Integer **Идентификатор объекта:** 1.3.6.1.2.1.11.6.0 **Определение:** Количество выходных сигналов для порта в таблице выходных сигналов (rs232PortOutSigTable). Таблица содержит записи только для тех сигналов, которые могут быть подтверждены программным обеспечением и целесообразны для наблюдения.
Группа: rs232Group **Trap-уведомление:** rs232PortOutSpeed	**Доступ:** Для чтения и записи **Синтаксическая структура:** Integer **Идентификатор объекта:** 1.3.6.1.2.1.11.4.0 **Определение:** Выходная скорость порта в битах в секунду. Обратите внимание, что нестандартные значения, такие как 9612, вероятно, недопустимы в большинстве вариантов реализации.
Группа: rs232Group **Trap-уведомление:** rs232PortType	**Доступ:** Только для чтения **Синтаксическая структура:** Integer **Идентификатор объекта:** 1.3.6.1.2.1.11.5.0 **Определение:** Тип аппаратных средств порта.

RSTP-MIB

Группа/Объект	Описание
Группа: rstpPortGroup **Trap-уведомление:** dot1dStpPortAdminEdgePort	**Доступ:** Для чтения и записи **TruthValue** **Идентификатор объекта:** .1.3.6.1.2.1.17.2.19.1.2 **Определение:** Значение параметра Edge Port для администрирования. Значение true(1) указывает на то, что этот порт следует принимать в качестве граничного порта, а значение false(2) указывает на то, что этот порт следует принимать в качестве неграничного порта. Установка этого объекта также приведет к изменению соответствующего экземпляра dot1dStpPortOperEdgePort на то же значение. Обратите внимание, что даже если значение этого объекта равно true, значение соответствующего экземпляра dot1dStpPortOperEdgePort может быть false, если получен BPDU. Значение этого объекта ДОЛЖНО сохраняться при повторной инициализации системы управления.
Группа: rstpPortGroup **Trap-уведомление:** dot1dStpPortAdminPathCost	**Доступ:** Для чтения и записи **Синтаксическая структура:** Integer **Идентификатор объекта:** .1.3.6.1.2.1.17.2.19.1.6 **Определение:** Назначенное администратором значение вклада этого порта в стоимость путей к корню связующего дерева. Запись значения «0» присваивает порту автоматически рассчитанное значение стоимости пути по умолчанию. Если используется стоимость пути по умолчанию, этот объект возвращает «0» при чтении. Это дополняет объект dot1dStpPortPathCost или dot1dStpPortPathCost32, который

Группа/Объект	Описание
	возвращает операционное значение стоимости пути. Значение этого объекта ДОЛЖНО сохраняться при повторной инициализации системы управления.
Группа: rstpPortGroup **Trap-уведомление:** dot1dStpPortAdminPointToPoint	**Доступ:** Для чтения и записи **Синтаксическая структура:** Integer **Идентификатор объекта:** .1.3.6.1.2.1.17.2.19.1.4 **Определение:** Статус администрирования двухточечного канала связи для сегмента локальной сети, присоединенного к этому порту, с использованием значений из IEEE 802.1w. Значение forceTrue(0) указывает на то, что этот порт всегда следует рассматривать как подключенный к двухточечному каналу связи. Значение forceFalse(1) указывает на то, что этот порт следует рассматривать как имеющий общее медиа-соединение. Значение auto(2) указывает на то, что этот порт считается имеющим двухточечный канал связи, если он является Агрегатором и все его члены агрегируются, или если MAC-экземпляр настроен на работу в полнодуплексном режиме либо посредством автосогласования, либо средствами управления. Управление этим объектом изменяет базовый adminPortToPortMAC. Значение этого объекта ДОЛЖНО сохраняться при повторной инициализации системы управления.
Группа: rstpPortGroup **Trap-уведомление:** dot1dStpPortOperEdgePort	**Доступ:** Только для чтения **TruthValue** **Идентификатор объекта:** .1.3.6.1.2.1.17.2.19.1.3 **Определение:** Рабочее значение параметра Edge Port. Объект инициализируется до значения соответствующего экземпляра dot1dStpPortAdminEdgePort. При установке соответствующего экземпляра dot1dStpPortAdminEdgePort этот объект также будет изменен. Этот объект также будет изменен на false при получении BPDU.
Группа: rstpPortGroup **Trap-уведомление:** dot1dStpPortOperPointToPoint	**Доступ:** Только для чтения **TruthValue** **Идентификатор объекта:** .1.3.6.1.2.1.17.2.19.1.5 **Определение:** Рабочий статус двухточечного канала связи для сегмента локальной сети, подключенного к этому порту. Указывает, считается ли порт имеющим двухточечный канал связи. Если adminPointToPointMAC имеет значение auto(2), то значение operPointToPointMAC определяется в соответствии с конкретными процедурами, определенными для соответствующего MAC-объекта, как указано в пункте 6.5 IEEE 802.1w. Значение определяется динамически, то есть повторно оценивается всякий раз, когда изменяется значение adminPointToPointMAC, и всякий раз, когда конкретные процедуры, определенные для MAC-объекта, оценивают изменение статуса двухточечного канала связи.
Группа: rstpBridgeGroup **Trap-уведомление:** dot1dStpTxHoldCount	**Функционал агента:** RC-RSTP-MIB-AC **Доступ:** Для чтения и записи **Синтаксическая структура:** Integer **Идентификатор объекта:** .1.3.6.1.2.1.17.2.17.0 **Определение:** Значение, используемое конечным автоматом Port Transmit для ограничения максимальной скорости передачи. Значение этого объекта ДОЛЖНО сохраняться при повторной инициализации системы управления.

Группа/Объект	Описание
	Примечание RFC указывает диапазон 1...10. При реализации используется диапазон 0...100. Значение 0 используется для Unlimited (Без ограничений), а диапазон ROS фактически составляет 3...100.
Группа: rstpBridgeGroup **Trap-уведомление:** dot1dStpVersion	**Доступ:** Для чтения и записи **Синтаксическая структура:** Integer **Идентификатор объекта:** .1.3.6.1.2.1.17.2.16.0 **Определение:** Версия протокола связующего дерева, который в настоящее время запущен мостом. Значение stpCompatible(0) указывает протокол связующего дерева, определенный в IEEE 802.1D-1998, а rstp(2) указывает протокол быстрого связующего дерева, определенный в IEEE 802.1w и пункте 17 802.1D-2004. Значения получены непосредственно из стандарта IEEE. Новые значения могут быть определены по мере появления будущих версий протокола. Значение этого объекта ДОЛЖНО сохраняться при повторной инициализации системы управления.

SNMP-FRAMEWORK-MIB

Группа/Объект	Описание
Группа: snmpEngineGroup **Trap-уведомление:** snmpEngineBoots	**Доступ:** Только для чтения **Синтаксическая структура:** Integer **Идентификатор объекта:** 1.3.6.1.2.1.11.31.0 **Определение:** Количество раз, когда SNMP-движок был инициализирован (повторно инициализирован) с момента последней настройки snmpEngineID.
Группа: snmpEngineGroup **Trap-уведомление:** snmpEngineID	**Доступ:** Только для чтения **Синтаксическая структура:** Hex-String **Идентификатор объекта:** 1.3.6.1.2.1.1.4.0 **Определение:** Уникальный идентификатор SNMP-движка для администрирования. Эта информация ДОЛЖНА храниться в энергонезависимом запоминающем устройстве, чтобы она оставалась постоянной при повторной инициализации SNMP-движка.
Группа: snmpEngineGroup **Trap-уведомление:** snmpEngineMaxMessageSize	**Доступ:** Только для чтения **Синтаксическая структура:** Integer **Идентификатор объекта:** 1.3.6.1.2.1.1.1.0 **Определение:** Максимальная длина в октетах SNMP-сообщения, которое этот SNMP-движок может отправлять или принимать и обрабатывать, определяется как минимальное из максимальных значений размера сообщения, поддерживаемых всеми средствами передачи данных, доступными и поддерживаемыми движком.
Группа: snmpEngineGroup **Trap-уведомление:** snmpEngineTime	**Доступ:** Только для чтения **Синтаксическая структура:** Integer **Идентификатор объекта:** 1.3.6.1.2.1.1.6.0 **Определение:** Количество секунд с момента последнего изменения значения объекта snmpEngineBoots. При увеличении значения этого объекта, которое приведет к превышению его максимального

Группа/Объект	Описание
	значения, snmpEngineBoots увеличивается так, как если бы произошла повторная инициализация, и значение этого объекта, следовательно, возвращается к нулю.

SNMP-USER-BASED-SM-MIB

Группа/Объект	Описание
Группа: usmMIBBasicGroup **Trap-уведомление:** usmStatsDecryptionErrors	**Доступ:** Только для чтения **Синтаксическая структура:** Counter32 **Идентификатор объекта:** 1.3.6.1.6.3.15.1.2.2.1.9 **Определение:** Общее количество пакетов, полученных SNMP-движком, которые были удалены из-за невозможности расшифровки.
Группа: usmMIBBasicGroup **Trap-уведомление:** usmStatsNotInTimeWindows	**Доступ:** Только для чтения **Синтаксическая структура:** Counter32 **Идентификатор объекта:** 1.3.6.1.6.3.15.1.2.2.1.8.11.128.0.58.156.3.0.10.220.0.128.72.4.97.112.118.51 **Определение:** Общее количество пакетов, полученных SNMP-движком, которые были удалены, так как они появились за пределами достоверного интервала опроса SNMP-движка.
Группа: usmMIBBasicGroup **Trap-уведомление:** usmStatsUnknownEngineIDs	**Доступ:** Только для чтения **Синтаксическая структура:** Counter32 **Идентификатор объекта:** 1.3.6.1.6.3.15.1.2.2.1.11 **Определение:** Общее количество пакетов, полученных SNMP-движком, которые были удалены, поскольку они ссылались на snmpEngineID, который не был известен SNMP-движку.
Группа: usmMIBBasicGroup **Trap-уведомление:** usmStatsUnknownUserNames	**Доступ:** Только для чтения **Синтаксическая структура:** Counter32 **Идентификатор объекта:** 1.3.6.1.6.3.15.1.2.2.1.3 **Определение:** Общее количество пакетов, полученных SNMP-движком, которые были удалены, поскольку они ссылались на пользователя, который не был известен SNMP-движку.
Группа: usmMIBBasicGroup **Trap-уведомление:** usmStatsUnsupportedSecLevels	**Доступ:** Только для чтения **Синтаксическая структура:** Counter32 **Идентификатор объекта:** 1.3.6.1.6.3.15.1.2.1.0 **Определение:** Общее количество пакетов, полученных SNMP-движком, которые были удалены из-за запроса securityLevel, который был неизвестен SNMP-движку или недоступен по иной причине.
Группа: usmMIBBasicGroup **Trap-уведомление:** usmStatsWrongDigests	**Доступ:** Только для чтения **Синтаксическая структура:** Counter32 **Идентификатор объекта:** 1.3.6.1.6.3.15.1.2.2.1.13 **Определение:** Общее количество пакетов, полученных SNMP-движком, которые были удалены, поскольку они не содержали ожидаемого значения дайджеста.
Группа: usmMIBBasicGroup **Trap-уведомление:** usmUserAuthKeyChange	**Доступ:** Для чтения и создания **Синтаксическая структура:** String **Идентификатор объекта:** 1.3.6.1.6.3.15.1.2.2.1.12

Группа/Объект	Описание
	Определение: Объект, который при изменении приводит к изменению секретного ключа аутентификации, используемого для сообщений, отправляемых от имени этого пользователя, в/из SNMP-движка, идентифицированного usmUserEngineID, с помощью односторонней функции. Связанный протокол — usmUserAuthProtocol. Связанный секретный ключ — секретный ключ аутентификации пользователя (authKey). Связанный алгоритм хеширования — это алгоритм, используемый протоколом usmUserAuthProtocol пользователя. При создании нового пользователя ошибка inconsistentName для операции SET ссылается на этот объект, если он не инициализирован ранее или одновременно с помощью операции SET для соответствующего экземпляра usmUserCloneFrom. Если значение соответствующего usmUserAuthProtocol равно usmNoAuthProtocol, то набор является успешным, но фактически является no-op (пустой операцией). При чтении этого объекта возвращается строка нулевой длины (пустая). Рекомендуемый способ внесения ключевых изменений следующий: • 1) Выполните запрос GET(usmUserSpinLock.0) и сохраните в sValue. • 2) сгенерируйте значение keyChange на основе старого (существующего) секретного ключа и нового секретного ключа, назовем это значение kcValue. Если вы выполняете изменение ключа от имени другого пользователя: • 3) Выполните запрос SET(usmUserSpinLock.0=sValue, usmUserAuthKeyChange=kcValue usmUserPublic=randomValue) Если вы выполняете изменение ключа для себя: • 4) Выполните запрос SET(usmUserSpinLock.0=sValue, usmUserOwnAuthKeyChange=kcValue usmUserPublic=randomValue) Если вы получаете ответ со статусом ошибки noError, то запрос SET успешно выполнен и новый ключ активен. Если вы не получили ответа, вы можете выполнить запрос GET(usmUserPublic) и проверить, равно ли значение randomValue, отправленному в запросе SET. Если да, то изменение ключа прошло успешно и новый ключ активен (вероятно, ответ утерян). Если нет, то запрос SET, вероятно, так и не достиг цели, поэтому вы можете начать сначала согласно описанной выше процедуре.
Группа: usmMIBBasicGroup **Trap-уведомление:** usmUserAuthProtocol	**Доступ:** Для чтения и создания **Синтаксическая структура:** Идентификатор объекта **Идентификатор объекта:** 1.3.6.1.6.3.16.1.4.1.4.8.71.112.114.105.118.97.116.101.0.2.1 **Определение:** Указывает, могут ли сообщения, отправленные от имени этого пользователя в/из SNMP-движка, идентифицированного usmUserEngineID, быть аутентифицированы, и если да, то тип используемого протокола аутентификации. Экземпляр этого объекта создается одновременно с созданием любого другого экземпляра объекта для того же пользователя (т.е. в рамках обработки операции SET, которая создает первый экземпляр объекта в той же концептуальной строке). Если начальная операция SET (т.е. во время создания строки) пытается установить значение для неизвестного или неподдерживаемого протокола, возвращается ошибка wrongValue. Значение будет перезаписано/установлено при выполнении операции SET для соответствующего экземпляра usmUserCloneFrom. После создания экземпляра значение такого экземпляра этого объекта может быть изменено только с помощью операции SET на значение usmNoAuthProtocol. Если операция SET пытается изменить значение существующего экземпляра этого

Группа/Объект	Описание
	объекта на любое значение, отличное от usmNoAuthProtocol, возвращается ошибка inconsistentValue. Если операция SET пытается установить значение usmNoAuthProtocol, в то время как значение usmUserPrivProtocol в той же строке не равно usmNoPrivProtocol, возвращается ошибка inconsistentValue. Это означает, что приложение генератора команд SNMP должно сначала убедиться, что для usmUserPrivProtocol установлено значение usmNoPrivProtocol, прежде чем оно сможет установить значение usmUserAuthProtocol для usmNoAuthProtocol.
Группа: usmMIBBasicGroup **Trap-уведомление:** usmUserCloneFrom	**Доступ:** Для чтения и создания **Синтаксическая структура:** Идентификатор объекта **Идентификатор объекта:** 1.3.6.1.6.3.16.1.4.1.7.8.71.112.114.105.118.97.116.101.0.2.1 **Определение:** Указатель на другую концептуальную строку в этой таблице usmUserTable. Пользователь в этой другой концептуальной строке называется clone-from user (клон пользователя). При создании нового пользователя (т.е. в этой таблице создается новая концептуальная строка) параметры конфиденциальности и аутентификации нового пользователя должны быть клонированы у его клона пользователя. Этими параметрами являются: • - протокол аутентификации (usmUserAuthProtocol) • - протокол конфиденциальности (usmUserPrivProtocol) Они будут скопированы независимо от текущего значения. Клонирование также приводит к тому, что начальные значения секретного ключа аутентификации (authKey) и секретного ключа шифрования (privKey) нового пользователя устанавливаются на те же значения, что и соответствующие секретные ключи клона пользователя, чтобы процесс KeyChange происходил по мере необходимости во время создания пользователя. Первый раз, когда экземпляр этого объекта задается операцией управления (в момент или после его создания), запускается процесс клонирования. Последующие записи выполнены успешно, но не вызывают никаких действий, которые должны быть предприняты получателем. Процесс клонирования завершается ошибкой inconsistentName, если концептуальная строка, представляющая клон пользователя, не существует или не находится в активном состоянии при вызове процесса клонирования. При чтении этого объекта возвращается идентификатор объекта ZeroDotZero.
Группа: usmMIBBasicGroup **Trap-уведомление:** usmUserOwnAuthKeyChange	**Доступ:** Для чтения и создания **Синтаксическая структура:** String **Идентификатор объекта:** 1.3.6.1.6.3.16.1.4.1.5.8.71.112.114.105.118.97.116.101.0.2.1 **Определение:**Поведение соответствует поведению usmUserAuthKeyChange с одним заметным отличием: для успешного выполнения операции SET имя пользователя usmUserName инициатора запроса операции должно совпадать с именем пользователя usmUserName, индексирующего строку, являющуюся целевой для этой операции. Кроме того, для этой операции должна использоваться модель безопасности USM. Идея заключается в том, что доступ к этому столбцу может быть открытым, так как он позволит пользователю изменить только свой собственный секретный ключ аутентификации (authKey). Обратите внимание, что это можно сделать только в том случае, если строка активна. Если запрос SET получен, а usmUserName инициатора запроса не совпадает с umsUserName, для индексирующего

Группа/Объект	Описание
	строку, являющуюся целевой для этой операции, возвращается ошибка noAccess. Если запрос SET получен и используемая модель безопасности не является USM, возвращается ошибка noAccess.
Группа: usmMIBBasicGroup **Trap-уведомление:** usmUserOwnPrivKeyChange	**Доступ:** Для чтения и создания **Синтаксическая структура:** String **Идентификатор объекта:** 1.3.6.1.6.3.16.1.4.1.9.8.71.112.114.105.118.97.116.101.0.2.1 **Определение:**Поведение соответствует поведению usmUserPrivKeyChange с одним заметным отличием: для успешного выполнения операции SET имя пользователя usmUserName инициатора запроса операции должно совпадать с именем пользователя usmUserName, индексирующего строку, являющуюся целевой для этой операции. Кроме того, для этой операции должна использоваться модель безопасности USM. Идея заключается в том, что доступ к этому столбцу может быть открытым, так как он позволит пользователю изменить только свой собственный секретный ключ конфиденциальности (privKey). Обратите внимание, что это можно сделать только в том случае, если строка активна. Если запрос SET получен, а usmUserName инициатора запроса не совпадает с umsUserName, для индексирующего строку, являющуюся целевой для этой операции, возвращается ошибка noAccess. Если запрос SET получен и используемая модель безопасности не является USM, возвращается ошибка noAccess.
Группа: usmMIBBasicGroup **Trap-уведомление:** usmUserPrivKeyChange	**Доступ:** Для чтения и создания **Синтаксическая структура:** String **Идентификатор объекта:** 1.3.6.1.6.3.16.1.4.1.8.8.71.112.114.105.118.97.116.101.0.2.1 **Определение:** Объект, который при изменении приводит к изменению секретного ключа шифрования, используемого для сообщений, отправляемых от имени этого пользователя, в/из SNMP-движка, идентифицированного usmUserEngineID, с помощью односторонней функции. Связанный протокол — usmUserPrivProtocol. Связанный секретный ключ — секретный ключ конфиденциальности пользователя (privKey). Связанный алгоритм хеширования — это алгоритм, используемый протоколом usmUserAuthProtocol пользователя. При создании нового пользователя ошибка inconsistentName для операции SET ссылается на этот объект, если он не инициализирован ранее или одновременно с помощью операции SET для соответствующего экземпляра usmUserCloneFrom. Если значение соответствующего usmUserPrivProtocol равно usmNoPrivProtocol, то запрос SET выполнен успешно, но фактически является no-op (пустой операцией). При чтении этого объекта возвращается строка нулевой длины (пустая). Рекомендуемую процедуру изменения ключа см. в разделе описания usmUserAuthKeyChange.
Группа: usmMIBBasicGroup **Trap-уведомление:** usmUserPrivProtocol	**Доступ:** Для чтения и создания **Синтаксическая структура:** Идентификатор объекта **Идентификатор объекта:** 1.3.6.1.6.3.16.1.4.1.6.8.71.112.114.105.118.97.116.101.0.2.1 **Определение:** Указывает, могут ли сообщения, отправленные от имени этого пользователя в/из SNMP-движка, идентифицированного usmUserEngineID, быть защищены от разглашения, и если да, то тип используемого протокола конфиденциальности. Экземпляр этого объекта создается одновременно с созданием любого другого экземпляра объекта для того же пользователя (т.е. в рамках обработки

Группа/Объект	Описание
	операции SET, которая создает первый экземпляр объекта в той же концептуальной строке). Если начальная операция SET (т.е. во время создания строки) пытается установить значение для неизвестного или неподдерживаемого протокола, возвращается ошибка wrongValue. Значение будет перезаписано/установлено при выполнении операции SET для соответствующего экземпляра usmUserCloneFrom. После создания экземпляра значение такого экземпляра этого объекта может быть изменено только с помощью операции SET на значение usmNoPrivProtocol. Если операция SET пытается изменить значение существующего экземпляра этого объекта на любое значение, отличное от usmNoPrivProtocol, возвращается ошибка inconsistentValue. Обратите внимание, что если используется какой-либо протокол конфиденциальности, необходимо также использовать протокол аутентификации. Другими словами, если для usmUserPrivProtocol задано какое-либо иное значение, чем usmNoPrivProtocol, то соответствующий экземпляр usmUserAuthProtocol не может иметь значение usmNoAuthProtocol. Если он имеет такое значение, возвращается ошибка inconsistentValue.
Группа: usmMIBBasicGroup **Trap-уведомление:** usmUserPublic	**Доступ:** Для чтения и создания **Синтаксическая структура:** String **Идентификатор объекта:** 1.3.6.1.6.3.16.1.1.1.1 **Определение:** Общедоступное значение, которое может быть записано как часть процедуры изменения секретного ключа аутентификации и/или конфиденциальности пользователя, а затем прочитано, чтобы определить, было ли произведено изменение секретного ключа.
Группа: usmMIBBasicGroup **Trap-уведомление:** usmUserSecurityName	**Доступ:** Только для чтения **Синтаксическая структура:** String **Идентификатор объекта:** 1.3.6.1.6.3.16.1.2.1.3.2.7.112.114.105.118.97.116.101 **Определение:** Удобная для восприятия человеком строка, представляющая пользователя в независимом от модели безопасности формате. Преобразование по умолчанию идентификатора безопасности, зависящего от модели безопасности пользователя, в securityName и наоборот является функцией идентификации, так что securityName совпадает с userName.
Группа: usmMIBBasicGroup **Trap-уведомление:** usmUserSpinLock	**Доступ:** Для чтения и записи **Синтаксическая структура:** Integer **Идентификатор объекта:** 1.3.6.1.6.3.16.1.2.1.5.2.7.112.114.105.118.97.116.101 **Определение:** Рекомендованная блокировка, используемая для того, чтобы позволить нескольким взаимодействующим приложениям генератора команд координировать использование ими средств для изменения секретных ключей в таблице usmUserTable.
Группа: usmMIBBasicGroup **Trap-уведомление:** usmUserStatus	**Доступ:** Для чтения и создания **Синтаксическая структура:** Integer **Идентификатор объекта:** 1.3.6.1.6.3.16.1.2.1.4.2.7.112.114.105.118.97.116.101 **Определение:** Статус этого концептуального ряда. До тех пор, пока экземпляры всех соответствующих столбцов не будут настроены соответствующим образом, значение соответствующего экземпляра столбца usmUserStatus будет notReady. В частности, недавно созданная

Группа/Объект	Описание
	строка для пользователя, использующего аутентификацию, не может быть активирована до тех пор, пока не будут заданы соответствующие usmUserCloneFrom и usmUserAuthKeyChange. Кроме того, недавно созданная строка для пользователя, который также использует конфиденциальность, не может быть активирована до тех пор, пока не будет установлено usmUserPrivKeyChange. RowStatus [RFC2579 <rfc2579.html>] требует, чтобы в этом пункте ОПИСАНИЯ указывалось, при каких обстоятельствах другие объекты в этой строке могут быть изменены: Значение этого объекта не влияет на возможность изменения других объектов в этой концептуальной строке, за исключением usmUserOwnAuthKeyChange и usmUserOwnPrivKeyChange. Для этих 2 объектов значение usmUserStatus ДОЛЖНО быть активным.
Группа: usmMIBBasicGroup **Trap-уведомление:** usmUserStorageType	**Доступ:** Для чтения и создания **Синтаксическая структура:** Integer **Идентификатор объекта:** 1.3.6.1.6.3.16.1.5.1.0 **Определение:** Тип запоминающего устройства для этой концептуальной строки. Концептуальные строки, имеющие значение permanent, должны обеспечивать доступ к записи как минимум для: • - usmUserAuthKeyChange, usmUserOwnAuthKeyChange и usmUserPublic для пользователя, использующего аутентификацию, и • - usmUserPrivKeyChange, usmUserOwnPrivKeyChange и usmUserPublic для пользователя, использующего конфиденциальность. Обратите внимание, что любой пользователь, использующий аутентификацию или конфиденциальность, должен разрешить обновление своих секретных ключей и, следовательно, не может быть readOnly. Если начальная операция SET пытается установить значение readOnly для пользователя, использующего настройки аутентификации или конфиденциальности, возвращается ошибка inconsistentValue. Обратите внимание, что если в качестве значения ранее было установлено (неявно или явно) любое значение, то применяются правила, определенные в текстовом соглашении StorageType. Решение о том, принимается ли SET для строки со значением readOnly или permanent относится к способу реализации. В одних случаях это может иметь смысл, в других — нет. Если SET для строки со значением readOnly или permanent не принимается, возвращается ошибка wrongValue.

SNMPv2-MIB

Группа/Объект	Описание
Группа: snmpBasicNotificationsGroup **Trap-уведомление:** AuthenticationFailure	**Доступ:** 0 **Синтаксическая структура:** — **Идентификатор объекта:** 1.3.6.1.6.3.1.1.5.5 **Определение:** Ловушка authenticationFailure означает, что объект SNMPv2, действующий в роли агента, получил сообщение протокола, которое не прошло надлежащую аутентификацию. Хотя все реализации SNMPv2 должны быть способны генерировать эту ловушку, объект snmpEnableAuthenTraps указывает, будет ли эта ловушка генерироваться.
Группа: snmpGroup **Trap-уведомление:** snmpInASNParseErrs	**Доступ:** Только для чтения **Синтаксическая структура:** Counter32

Группа/Объект	Описание
	Идентификатор объекта: 1.3.6.1.2.1.1.5.0 **Определение:** Общее количество ошибок ASN.1 или BER, обнаруженных объектом SNMP при декодировании полученных SNMP-сообщений.
Группа: snmpCommunityGroup **Trap-уведомление:** snmpInBadCommunityNames	**Доступ:** Только для чтения **Синтаксическая структура:** Counter32 **Идентификатор объекта:** 1.3.6.1.2.1.1.2.0 **Определение:** Общее количество SNMP-сообщений, доставленных в объект SNMP, которая использовала имя SNMP-сообщества, неизвестное указанному объекту.
Группа: snmpCommunityGroup **Trap-уведомление:** snmpInBadCommunityUses	**Доступ:** Только для чтения **Синтаксическая структура:** Counter32 **Идентификатор объекта:** 1.3.6.1.2.1.1.9.1.3.0 **Определение:** Общее количество SNMP-сообщений, доставленных в объект SNMP, который представлял собой SNMP-операцию, запрещенную SNMP-сообществом, указанным в сообщении.
Группа: snmpGroup **Trap-уведомление:** snmpInBadVersions	**Доступ:** Только для чтения **Синтаксическая структура:** Counter32 **Идентификатор объекта:** 1.3.6.1.2.1.1.9.1.2.0 **Определение:** Общее количество SNMP-сообщений, доставленных в объект SNMP и предназначенных для неподдерживаемой версии SNMP.
Группа: snmpGroup **Trap-уведомление:** snmpInPkts	**Доступ:** Только для чтения **Синтаксическая структура:** Counter32 **Идентификатор объекта:** 1.3.6.1.2.1.1.8.0 **Определение:** Общее количество сообщений, доставленных объекту SNMP от транспортной службы.
Группа: snmpGroup **Trap-уведомление:** snmpProxyDrops	**Доступ:** Только для чтения **Синтаксическая структура:** Counter32 **Идентификатор объекта:** 1.3.6.1.2.1.1.9.1.4.0 **Определение:** Общее количество модулей GetRequest-PDU, GetNextRequest-PDU, GetBulkRequest-PDU, SetRequest-PDU и InformRequest-PDU, доставленных в объект SNMP, которые были отключены, поскольку передача (возможно, переведенного) сообщения на целевой прокси завершилась неудачно (кроме тайм-аута) таким образом, что не удалось вернуть модуль Response-PDU.
Группа: snmpSetGroup **Trap-уведомление:** snmpSetSerialNo	**Доступ:** Для чтения и записи **Синтаксическая структура:** Integer **Идентификатор объекта:** 1.3.6.1.2.1.1.7.0 **Определение:** Рекомендованная блокировка, используемая для того, чтобы позволить нескольким взаимодействующим объектам SNMPv2, каждый из которых выступает в роли менеджера, координировать использование ими операции SET для SNMPv2. Этот объект используется для координации крупномодульных структур. Для достижения координации мелкомодульных структур в каждой группе MIB может быть определен один или несколько аналогичных объектов, в зависимости от обстоятельств.
Группа: snmpGroup	**Доступ:** Только для чтения

Группа/Объект	Описание
Trap-уведомление: snmpSilentDrops	**Синтаксическая структура:** Counter32 **Идентификатор объекта:** 1.3.6.1.2.1.1.3.0 **Определение:** Общее количество модулей GetRequest-PDU, GetNextRequest-PDU, GetBulkRequest-PDU, SetRequest-PDU и InformRequest-PDU, доставленных в объект SNMP, было удалено, поскольку размер ответа, содержащего альтернативный модуль ответа с пустым полем привязки переменных, был больше, чем локальное ограничение или максимальный размер сообщения, связанный с инициатором запроса.
Группа: systemGroup **Trap-уведомление:** sysContact	**Функционал агента:** RC-SNMPv2-MIB-AC **Доступ:** Для чтения и записи **Синтаксическая структура:** String **Идентификатор объекта:** .1.3.6.1.2.1.6.5.0 **Определение:** Текстовая идентификация контактного лица для данного управляемого узла вместе с информацией о том, как связаться с этим лицом. Если контактная информация неизвестна, значение равно строке нулевой длины. **Определение:** Для этого объекта поддерживается строка до 49 символов.
Группа: systemGroup **Trap-уведомление:** sysDescr	**Доступ:** Только для чтения **Синтаксическая структура:** String **Идентификатор объекта:** .1.3.6.1.2.1.6.7.0 **Определение:** Текстовое описание объекта. Это значение должно включать полное название и идентификацию версии аппаратного типа системы, программно-оперативной системы и сетевого программного обеспечения.
Группа: systemGroup **Trap-уведомление:** sysLocation	**Функционал агента:** RC-SNMPv2-MIB-AC **Доступ:** Для чтения и записи **Синтаксическая структура:** String **Идентификатор объекта:** .1.3.6.1.2.1.6.13.1.2.0.0.0.0.22.0.0.0.0.0 **Определение:** Физическое расположение этого узла (например, "серверная, 3-й этаж"). Если местоположение неизвестно, значение равно строке нулевой длины. **Определение:** Для этого объекта поддерживается строка до 49 символов.
Группа: systemGroup **Trap-уведомление:** sysName	**Функционал агента:** RC-SNMPv2-MIB-AC **Доступ:** Для чтения и записи **Синтаксическая структура:** String **Идентификатор объекта:** .1.3.6.1.2.1.6.13.1.3.0.0.0.0.22.0.0.0.0.0 **Определение:** Назначенное администратором имя для этого управляемого узла. По общему правилу, это полное доменное имя узла. Если имя неизвестно, значение равно строке нулевой длины. **Определение:** Для этого объекта поддерживается строка до 24 символов.
Группа: systemGroup **Trap-уведомление:** sysObjectID	**Доступ:** Только для чтения **Синтаксическая структура:** String **Идентификатор объекта:** .1.3.6.1.2.1.6.13.1.4.0.0.0.0.22.0.0.0.0.0

Группа/Объект	Описание
	Определение: Авторитетная идентификация поставщиком подсистемы управления сетью, содержащейся в объекте. Это значение распределяется в рамках поддерева «Предприятия SMI» (1.3.6.1.4.1) и обеспечивает простое и однозначное средство для определения того, управление каким именно объектом осуществляется. Например, если поставщику «Flintstones, Inc.» было присвоено поддерево 1.3.6.1.4.1.4242, он мог присвоить идентификатор 1.3.6.1.4.1.4242.1.1 объекту «Fred Router».
Группа: systemGroup **Trap-уведомление:** sysORDescr	**Доступ:** Только для чтения **Синтаксическая структура:** String **Идентификатор объекта:** .1.3.6.1.2.1.6.13.1.5.0.0.0.0.22.0.0.0.0.0 **Определение:** Текстовое описание возможностей, идентифицированных соответствующим экземпляром sysORID.
Группа: systemGroup **Trap-уведомление:** sysORID	**Доступ:** Только для чтения **Синтаксическая структура:** Integer **Идентификатор объекта:** .1.3.6.1.2.1.6.13.1.1.0.0.0.0.22.0.0.0.0.0 **Определение:** Авторитетная идентификация заявления о возможностях в отношении различных модулей MIB, поддерживаемых локальным объектом SNMPv2, выступающим в роли агента.
Группа: systemGroup **Trap-уведомление:** sysORLastChange	**Доступ:** Только для чтения **Синтаксическая структура:** Timeticks **Идентификатор объекта:** .1.3.6.1.2.1.6.9.0 **Определение:** Значение sysUpTime на момент последнего изменения состояния или значения любого экземпляра sysORID.
Группа: systemGroup **Trap-уведомление:** sysORUpTime	**Доступ:** Только для чтения **Синтаксическая структура:** TimeStamp **Идентификатор объекта:** .1.3.6.1.2.1.6.8.0 **Определение:** Значение sysUpTime на момент последнего экземпляра этой концептуальной строки.
Группа: systemGroup **Trap-уведомление:** sysServices	**Доступ:** Только для чтения **Синтаксическая структура:** Integer **Идентификатор объекта:** .1.3.6.1.2.1.6.14.0 **Определение:** Значение, указывающее набор служб, которые этот объект может потенциально предоставить. Значением является сумма. Исходное значение этой суммы равно нулю. Затем, для каждого уровня L (в диапазоне от 1 до 7), для которого этот узел выполняет транзакции, используется повышающий коэффициент равный 2 (L — 1), который применяется к сумме. Например, узел, выполняющий только функции маршрутизации, будет иметь значение 4 (2^(3-1)). Напротив, узел, который является хостом, предоставляющим службы приложений, будет иметь значение 72 (2^(4-1) + 2^(7-1)). Обратите внимание, что в контексте набора протоколов Интернет значения следует рассчитывать соответственно: • Уровень 1: физический (например, повторители) • Уровень 2: канал передачи данных/подсеть (например, мосты) • Уровень 3: сетевой (например, поддержка IP) • Уровень 4: сквозной (например, поддержка TCP) • Уровень 7: приложения (например, поддержка SMTP)

Группа/Объект	Описание
	Для систем, включающих протоколы OSI, также могут быть засчитаны уровни 5 и 6.
Группа: systemGroup **Trap-уведомление:** sysUpTime	**Доступ:** Только для чтения **Синтаксическая структура:** Timeticks **Идентификатор объекта:** .1.3.6.1.2.1.6.17.0 **Определение:** Время (в сотых долях секунды) с момента последней повторной инициализации части системы управления сетью.

SNMP-VIEW-BASED-ACM-MIB

Группа/Объект	Описание
Группа: vacmBasicGroup **Trap-уведомление:** vacmAccessContextMatch	**Функционал агента:** RC-SNMP-VIEW-BASED-ACM-MIB-AC **Доступ:** Только для чтения **Синтаксическая структура:** Integer **Идентификатор объекта:** 1.3.6.1.6.3.16.1.5.2.1.3.5.86.49.77.105.98.1.1 **Определение:** Если значение этого объекта является exact(1), то выбираются все строки, в которых contextName точно соответствует vacmAccessContextPrefix. Если значение этого объекта является prefix(2), то выбираются все строки, в которых присутствует contextName с начальными октетами, точно совпадающими с vacmAccessContextPrefix. Это позволяет использовать простую форму подстановочных знаков.
Группа: vacmBasicGroup **Trap-уведомление:** vacmAccessNotifyViewName	**Доступ:** Для чтения и создания **Синтаксическая структура:** String **Идентификатор объекта:** 1.3.6.1.6.3.16.1.5.2.1.6.5.86.49.77.105.98.1.1 **Определение:** Значение экземпляра этого объекта определяет представление MIB для контекста SNMP, к которому эта концептуальная строка разрешает доступ для уведомлений. Идентифицированное представление MIB — это представление, для которого vacmViewTreeFamilyViewName имеет то же значение, что и экземпляр этого объекта; если значение является пустой строкой или если нет активного представления MIB, имеющего это значение vacmViewTreeFamilyViewName, то доступ не предоставляется.
Группа: vacmBasicGroup **Trap-уведомление:** vacmAccessReadViewName	**Доступ:** Для чтения и создания **Синтаксическая структура:** String **Идентификатор объекта:** 1.3.6.1.6.3.16.1.5.2.1.5.5.86.49.77.105.98.1.1 **Определение:** Значение экземпляра этого объекта идентифицирует представление MIB для контекста SNMP, к которому эта концептуальная строка разрешает доступ на чтение. Идентифицированное представление MIB — это представление, для которого vacmViewTreeFamilyViewName имеет то же значение, что и экземпляр этого объекта; если значение является пустой строкой или если нет активного представления MIB, имеющего это значение vacmViewTreeFamilyViewName, то доступ не предоставляется.
Группа: vacmBasicGroup **Trap-уведомление:** vacmAccessStatus	**Доступ:** Только для чтения **Синтаксическая структура:** Integer **Идентификатор объекта:** 1.3.6.1.6.3.16.1.5.2.1.4.5.86.49.77.105.98.1.1 **Определение:** Статус этого концептуального ряда. RowStatus [RFC2579 <rfc2579.html>] требует, чтобы в этом пункте ОПИСАНИЯ указывалось,

Группа/Объект	Описание
	при каких обстоятельствах другие объекты в этой строке могут быть изменены: Значение этого объекта не влияет на возможность изменения других объектов в этой концептуальной строке.
Группа: vacmBasicGroup **Trap-уведомление:** vacmAccessStorageType	**Доступ:** Только для чтения **Синтаксическая структура:** Integer **Определение:** Тип запоминающего устройства для этой концептуальной строки. Для концептуальных строк, имеющих значение permanent, не требуется предоставление доступа на запись для любых столбцовых объектов в строке.
Группа: vacmBasicGroup **Trap-уведомление:** vacmAccessWriteViewName	**Доступ:** Для чтения и создания **Синтаксическая структура:** String **Определение:** Значение экземпляра этого объекта идентифицирует представление MIB для контекста SNMP, к которому эта концептуальная строка разрешает доступ на запись. Идентифицированное представление MIB — это представление, для которого vacmViewTreeFamilyViewName имеет то же значение, что и экземпляр этого объекта; если значение является пустой строкой или если нет активного представления MIB, имеющего это значение vacmViewTreeFamilyViewName, то доступ не предоставляется.
Группа: vacmBasicGroup **Trap-уведомление:** vacmContextName	**Доступ:** Только для чтения **Синтаксическая структура:** String **Определение:** Удобное для восприятия человеком имя, идентифицирующее конкретный контекст в конкретном объекте SNMP. Пустое contextName (нулевая длина) представляет контекст по умолчанию.
Группа: vacmBasicGroup **Trap-уведомление:** vacmGroupName	**Доступ:** Для чтения и создания **Синтаксическая структура:** String **Определение:** Имя группы, к которой принадлежит эта запись (например, комбинация securityModel и securityName). Это groupName используется в качестве индекса в таблице vacmAccessTable для выбора политики управления доступом. Однако значение в этой таблице не означает, что экземпляр со значением существует в таблице vacmAccesTable.
Группа: vacmBasicGroup **Trap-уведомление:** vacmSecurityToGroupStatus	**Доступ:** Для чтения и создания **Синтаксическая структура:** Integer **Определение:** Статус этого концептуального ряда. До тех пор, пока экземпляры всех соответствующих столбцов не будут настроены соответствующим образом, значение соответствующего экземпляра столбца vacmSecurityToGroupStatus будет notReady. В частности, вновь созданная строка не может быть активирована, пока не будет установлено значение vacmGroupName. RowStatus [RFC2579 <rfc2579.html>] требует, чтобы в этом пункте ОПИСАНИЯ указывалось, при каких обстоятельствах другие объекты в этой строке могут быть изменены: Значение этого объекта не влияет на возможность изменения других объектов в этой концептуальной строке.
Группа: vacmBasicGroup **Trap-уведомление:** vacmSecurityToGroupStorageType	**Доступ:** Для чтения и создания **Синтаксическая структура:** Integer **Определение:** Тип запоминающего устройства для этой концептуальной строки. Для концептуальных строк, имеющих значение permanent, не требуется предоставление доступа на запись для любых столбцовых объектов в строке.

Группа/Объект	Описание
Группа: vacmBasicGroup **Trap-уведомление:** vacmViewSpinLock	**Доступ:** Для чтения и записи **Синтаксическая структура:** Integer **Определение:** Рекомендованная блокировка, используемая для того, чтобы приложения генератора команд SNMP могли координировать использование операции SET при создании или изменении представлений. При создании нового представления или изменении существующего представления важно понимать потенциальные взаимодействия с другими видами использования представления. Необходимо извлечь vacmViewSpinLock. Имя создаваемого представления должно быть определено как уникальное приложением генератора команд SNMP с помощью vacmViewTreeFamilyTable. Именованное представление может быть создано (операцией SET), включая рекомендуемую блокировку. Если за это время другое приложение генератора команд SNMP изменило представления, то значение спин-блокировки изменится, и поэтому это создание не будет выполнено, так как в нем будет указано неправильное значение спин-блокировки. Поскольку это рекомендованная блокировка, использование этой блокировки не обеспечивается.
Группа: vacmBasicGroup **Trap-уведомление:** vacmViewTreeFamilyMask	**Доступ:** Только для чтения **Синтаксическая структура:** String **Определение:** Битовая маска, которая в сочетании с соответствующим экземпляром vacmViewTreeFamilySubtree определяет семейство поддеревьев представлений. Каждый бит этой битовой маски соответствует субидентификатору vacmViewTreeFamilySubtree, причем наиболее значимый бит i-го октета этого значения октетной строки (при необходимости расширенного, см. ниже) соответствует (8*i — 7)-му субидентификатору, а наименее значимый бит i-го октета этой октетной строки соответствует (8*i)-му субидентификатору, где i находится в диапазоне от 1 до 16. Каждый бит этой битовой маски указывает, должны ли соответствующие субидентификаторы совпадать при определении, находится ли ИДЕНТИФИКАТОР ОБЪЕКТА в этом семействе поддеревьев представлений: "1" означает, что должно произойти точное совпадение: "0" означает "подстановочный знак", т.е. любое значение субидентификатора соответствует. Таким образом, ИДЕНТИФИКАТОР ОБЪЕКТА X экземпляра объекта содержится в семействе поддеревьев представлений, если для каждого субидентификатора значения vacmViewTreeFamilySubtree: • - i-й бит vacmViewTreeFamilyMask равен 0, или • - i-й субидентификатор X равен i-му субидентификатору значения vacmViewTreeFamilySubtree. >Если значение этой битовой маски имеет длину M бит и в соответствующем экземпляре vacmViewTreeFamilySubtree больше M субидентификаторов, то битовая маска расширяется на 1, чтобы иметь необходимую длину. Обратите внимание, что, когда значение этого объекта является строкой нулевой длины, это правило расширения приводит к использованию маски all-1 (т. е. без "подстановочного знака"), а семейство поддеревьев представлений является одним поддеревом представлений, уникальным образом идентифицированным соответствующим экземпляром vacmViewTreeFamilySubtree. Обратите внимание, что маски длиной более нуля не должны поддерживаться. В этом случае этот объект доступен только для чтения.
Группа: vacmBasicGroup	**Доступ:** Только для чтения **Синтаксическая структура:** Integer

Группа/Объект	Описание
Trap-уведомление: vacmViewTreeFamilyStatus	**Определение:** Статус этого концептуального ряда. RowStatus [RFC2579 <rfc2579.html>] требует, чтобы в этом пункте ОПИСАНИЯ указывалось, при каких обстоятельствах другие объекты в этой строке могут быть изменены: Значение этого объекта не влияет на возможность изменения других объектов в этой концептуальной строке.
Группа: vacmBasicGroup **Trap-уведомление:** vacmViewTreeFamilyStorageType	**Доступ:** Только для чтения **Синтаксическая структура:** Integer **Определение:** Тип запоминающего устройства для этой концептуальной строки. Для концептуальных строк, имеющих значение permanent, не требуется предоставление доступа на запись для любых столбцовых объектов в строке.
Группа: vacmBasicGroup **Trap-уведомление:** vacmViewTreeFamilyType	**Доступ:** Только для чтения **Синтаксическая структура:** Integer **Определение:** Указывает, определяют ли соответствующие экземпляры vacmViewTreeFamilySubtree и vacmViewTreeFamilyMask семейство поддеревьев представлений, которые включены в представление MIB или исключены из него.

TCP-MIB

Группа/Объект	Описание
Группа: tcpGroup **Trap-уведомление:** tcpActiveOpens	**Доступ:** Только для чтения **Синтаксическая структура:** Counter32 **Идентификатор объекта:** .1.3.6.1.2.1.6.4.0 **Определение:** Количество прямых переходов TCP-соединений в состояние SYN-SENT из состояния CLOSED.
Группа: tcpGroup **Trap-уведомление:** tcpAttemptFails	**Доступ:** Только для чтения **Синтаксическая структура:** Counter32 **Идентификатор объекта:** .1.3.6.1.2.1.6.15.0 **Определение:** Количество прямых переходов TCP-соединений в состояние CLOSED из состояния SYN-SENT или состояния SYN-RCVD, а также количество прямых переходов TCP-соединений в состояние LISTEN из состояния SYN-RCVD.
Группа: tcpGroup **Trap-уведомление:** tcpConnLocalAddress	**Доступ:** Только для чтения **Синтаксическая структура:** IpAddress **Идентификатор объекта:** .1.3.6.1.2.1.6.11.0 **Определение:** Локальный IP-адрес для этого TCP-соединения. В случае соединения в состоянии прослушивания, которое готово принять соединения для любого IP-интерфейса, связанного с узлом, используется значение 0.0.0.0.
Группа: tcpGroup **Trap-уведомление:** tcpConnLocalPort	**Доступ:** Только для чтения **Синтаксическая структура:** Integer **Идентификатор объекта:** .1.3.6.1.2.1.6.6.0 **Определение:** Локальный номер порта для этого TCP-соединения.
Группа: tcpGroup **Trap-уведомление:** tcpConnRemAddress	**Доступ:** Только для чтения **Синтаксическая структура:** IpAddress **Идентификатор объекта:** .1.3.6.1.2.1.6.12.0

Группа/Объект	Описание
	Определение: Удаленный IP-адрес для этого TCP-соединения.
Группа: tcpGroup **Trap-уведомление:** tcpConnRemPort	**Доступ:** Только для чтения **Синтаксическая структура:** Integer **Идентификатор объекта:** .1.3.6.1.2.1.6.1.0 **Определение:** Удаленный номер порта для этого TCP-соединения.
Группа: tcpGroup **Trap-уведомление:** tcpConnState	**Доступ:** Для чтения и записи **Синтаксическая структура:** Integer **Идентификатор объекта:** .1.3.6.1.2.1.6.3.0 **Определение:** Статус этого TCP-соединения. Единственное значение, которое может быть задано станцией управления, — deleteTCB(12). Соответственно, для агента допустимо возвращать ответ badValue, если станция управления пытается задать для этого объекта любое другое значение. Если станция управления устанавливает для этого объекта значение deleteTCB(12), то это приводит к удалению TCB (как определено в RFC 793) соответствующего соединения на управляемом узле, что приводит к немедленному прекращению соединения. В качестве варианта, зависящего от реализации, сегмент RST может быть отправлен из управляемого узла в другую конечную точку TCP (обратите внимание, на то, что сегменты RST не отправляются безошибочно).
Группа: tcpGroup **Trap-уведомление:** tcpCurrEstab	**Доступ:** Только для чтения **Синтаксическая структура:** Gauge32 **Идентификатор объекта:** .1.3.6.1.2.1.6.2.0 **Определение:** Количество TCP-соединений, для которых текущим состоянием является ESTABLISHED или CLOSE- WAIT.
Группа: tcpGroup **Trap-уведомление:** tcpEstabResets	**Доступ:** Только для чтения **Синтаксическая структура:** Counter32 **Идентификатор объекта:** .1.3.6.1.2.1.7.1.0 **Определение:** Количество прямых переходов TCP-соединений в состояние CLOSED либо из состояния ESTABLISHED, либо из состояния CLOSE-WAIT.
Группа: tcpGroup **Trap-уведомление:** tcpInErrs	**Доступ:** Только для чтения **Синтаксическая структура:** Counter32 **Идентификатор объекта:** .1.3.6.1.2.1.7.3.0 **Определение:** Общее количество сегментов, полученных по ошибке (например, неверные контрольные суммы TCP).
Группа: tcpGroup **Trap-уведомление:** tcpInSegs	**Доступ:** Только для чтения **Синтаксическая структура:** Counter32 **Идентификатор объекта:** .1.3.6.1.2.1.7.5.1.1.0.0.0.0.69 **Определение:** Общее количество полученных сегментов, включая полученные по ошибке. Это количество включает сегменты, полученные на текущих установленных соединениях.
Группа: tcpGroup **Trap-уведомление:** tcpMaxConn	**Доступ:** Только для чтения **Синтаксическая структура:** Integer **Идентификатор объекта:** .1.3.6.1.2.1.7.5.1.2.0.0.0.0.69 **Определение:** Ограничение общего количества TCP-соединений, которые может поддерживать объект. В объектах, где максимальное

Группа/Объект	Описание
	число соединений является динамическим, этот объект должен содержать значение -1.
Группа: tcpGroup **Trap-уведомление:** tcpOutRsts	**Доступ:** Только для чтения **Синтаксическая структура:** Counter32 **Идентификатор объекта:** .1.3.6.1.2.1.7.2.0 **Определение:** Количество отправленных TCP-сегментов, содержащих RST-флажок.
Группа: tcpGroup **Trap-уведомление:** tcpOutSegs	**Доступ:** Только для чтения **Синтаксическая структура:** Counter32 **Идентификатор объекта:** .1.3.6.1.2.1.7.4.0 **Определение:** Общее количество отправленных сегментов, включая сегменты с текущими соединениями, за исключением сегментов, содержащих только ретранслируемые октеты.
Группа: tcpGroup **Trap-уведомление:** tcpPassiveOpens	**Доступ:** Только для чтения **Синтаксическая структура:** Counter32 **Идентификатор объекта:** 1.3.6.1.6.3.15.1.1.6.0 **Определение:** Количество прямых переходов TCP-соединений в состояние SYN-RCVD из состояния LISTEN.
Группа: tcpGroup **Trap-уведомление:** tcpRetransSegs	**Доступ:** Только для чтения **Синтаксическая структура:** Counter32 **Идентификатор объекта:** 1.3.6.1.6.3.15.1.1.2.0 **Определение:** Количество прямых переходов TCP-соединений в состояние SYN-RCVD из состояния LISTEN.
Группа: tcpGroup **Trap-уведомление:** tcpRtoAlgorithm	**Доступ:** Только для чтения **Синтаксическая структура:** Integer **Идентификатор объекта:** 1.3.6.1.6.3.15.1.1.4.0 **Определение:** Алгоритм, используемый для определения значения тайм-аута, используемого для повторной передачи неподтвержденных октетов.
Группа: tcpGroup **Trap-уведомление:** tcpRtoMax	**Доступ:** Только для чтения **Синтаксическая структура:** Integer **Идентификатор объекта:** 1.3.6.1.6.3.15.1.1.3.0 **Определение:** Максимальное значение, допустимое реализацией TCP для тайм-аута повторной передачи, измеренное в миллисекундах. Более точная семантика для объектов этого типа зависит от алгоритма, используемого для определения тайм-аута повторной передачи. В частности, когда алгоритмом тайм-аута — rsre(3), объект этого типа семантически соответствует количеству UBOUND, описанному в RFC 793.
Группа: tcpGroup **Trap-уведомление:** tcpRtoMin	**Доступ:** Только для чтения **Синтаксическая структура:** Integer **Идентификатор объекта:** 1.3.6.1.6.3.15.1.1.1.0 **Определение:** Минимальное значение, допустимое реализацией TCP для тайм-аута повторной передачи, измеренное в миллисекундах. Более точная семантика для объектов этого типа зависит от алгоритма, используемого для определения тайм-аута повторной передачи. В частности, когда алгоритмом тайм-аута является rsre(3), объект этого

Группа/Объект	Описание
	типа семантически соответствует количеству LBOUND, описанному в RFC 793.

UDP-MIB

Группа/Объект	Описание
Группа: udpGroup **Trap-уведомление:** udpInDatagrams	**Доступ:** Только для чтения **Синтаксическая структура:** Counter32 **Идентификатор объекта:** 1.3.6.1.6.3.15.1.1.5.0 **Определение:** Общее количество доставленных пользователям UDP датаграмм.
Группа: udpGroup **Trap-уведомление:** udpInErrors	**Доступ:** Только для чтения **Синтаксическая структура:** Counter32 **Идентификатор объекта:** 1.3.6.1.6.3.15.1.2.2.1.6 **Определение:** Количество полученных UDP датаграмм, которые не удалось доставить по причинам, отличным от отсутствия приложения в порту назначения.
Группа: udpGroup **Trap-уведомление:** udpLocalAddress	**Доступ:** Только для чтения **Синтаксическая структура:** IpAddress **Идентификатор объекта:** 1.3.6.1.6.3.15.1.2.2.1.5.11.128.0.58.156.3.0.10.220.0.128.72.4.97.112.118.51 **Определение:** Локальный IP-адрес для этого блока прослушивания UDP. В случае блока прослушивания UDP, который готов принять датаграммы для любого IP-интерфейса, связанного с узлом, используется значение 0.0.0.0.
Группа: udpGroup **Trap-уведомление:** udpLocalPort	**Доступ:** Только для чтения **Синтаксическая структура:** Integer **Идентификатор объекта:** 1.3.6.1.6.3.15.1.2.2.1.4.11.128.0.58.156.3.0.10.220.0.128.72.4.97.112.118.51 **Определение:** Локальный номер порта для этого блока прослушивания UDP.
Группа: udpGroup **Trap-уведомление:** udpNoPorts	**Доступ:** Только для чтения **Синтаксическая структура:** Counter32 **Идентификатор объекта:** 1.3.6.1.6.3.15.1.2.2.1.7 **Определение:** Общее количество полученных датаграмм UDP, для которых отсутствует приложение в порту-адресате.
Группа: udpGroup **Trap-уведомление:** udpOutDatagrams	**Доступ:** Только для чтения **Синтаксическая структура:** Counter32 **Идентификатор объекта:** 1.3.6.1.6.3.15.1.2.2.1.10 **Определение:** Общее количество датаграмм UDP, отправленных от этого объекта.

12.3.1.2 Поддерживаемые проприетарные базы RUGGEDCOM MIB

RUGGEDCOM ROS поддерживает следующие проприетарные базы RUGGEDCOM MIB:

⚠ ЗАМЕТКА

В этом разделе перечислены все базы MIB, поддерживаемые RUGGEDCOM ROS, и он приводится исключительно в качестве справочной информации. Поддержка отдельных устройств может отличаться.

- **RUGGEDCOM-AAA-SERVER-MIB**

  Для получения дополнительной информации см. "RUGGEDCOM-AAA-SERVER-MIB".
- **RUGGEDCOM-DIGITAL-INPUTS-MIB**

  Для получения дополнительной информации см. "RUGGEDCOM-DIGITAL-INPUTS-MIB".
- **RUGGEDCOM-GPS-MIB**

  Для получения дополнительной информации см. "RUGGEDCOM-GPS-MIB".
- **RUGGEDCOM-IP-MIB**

  Для получения дополнительной информации см. "RUGGEDCOM-IP-MIB".
- **RUGGEDCOM-IRIGB-MIB**

  Для получения дополнительной информации см. "RUGGEDCOM-IRIGB-MIB".
- **RUGGEDCOM-MC30-MIB**

  Для получения дополнительной информации см. "RUGGEDCOM-MC30-MIB".
- **RUGGEDCOM-NTP-MIB**

  Для получения дополнительной информации см. "RUGGEDCOM-NTP-MIB".
- **RUGGEDCOM-POE-MIB**

  Для получения дополнительной информации см. "RUGGEDCOM-POE-MIB".
- **RUGGEDCOM-PTP1588-MIB**

  Для получения дополнительной информации см. "RUGGEDCOM-PTP1588-MIB".
- **RUGGEDCOM-SERIAL-MIB**

  Для получения дополнительной информации см. "RUGGEDCOM-SERIAL-MIB".
- **RUGGEDCOM-STP-MIB**

  Для получения дополнительной информации см. "RUGGEDCOM-STP-MIB".
- **RUGGEDCOM-SYS-INFO-MIB**

  Для получения дополнительной информации см. "RUGGEDCOM-SYS-INFO-MIB".
- **RUGGEDCOM-TIMECONFIG-MIB**

  Для получения дополнительной информации см. "RUGGEDCOM-TIMECONFIG-MIB".

RUGGEDCOM-AAA-SERVER-MIB

Группа(ы)	Объект	Описание
rcRadiusNotifyGroup	radiusServiceAvailableChange	**Идентификатор объекта:** 1.3.6.1.4.1.15004.4.14.1.2.1.3 **Определение:** Уведомление, которое генерируется при изменении статуса службы RADIUS.
rcRadiusBaseGroup	rcRadiusServerAutUdpPort	**Доступ:** Для чтения и записи **Синтаксическая структура:** Integer32 **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.14.1.1.1.1.3 **Определение:** Порт UDP сервера RADIUS.
rcRadiusBaseGroup	rcRadiusServerId	**Доступ:** Только для чтения **Синтаксическая структура:** Integer32 **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.14.1.1.1.1.1 **Определение:** Значение индекса, используемое для идентификации сервера RADIUS. 1. Первичный сервер 2. Резервный сервер
rcRadiusBaseGroup	rcRadiusServerIP	**Доступ:** Для чтения и записи **Синтаксическая структура:** IpAddress **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.14.1.1.1.1.2 **Определение:** IP-адрес сервера RADIUS.
rcRadiusBaseGroup	rcRadiusServerMaxRetry	**Доступ:** Для чтения и записи **Синтаксическая структура:** Integer32 **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.14.1.1.1.1.4 **Определение:** Максимальное количество попыток аутентификатора связаться с сервером RADIUS, чтобы аутентифицировать пользователя в случае какой-либо ошибки.
rcRadiusBaseGroup rcRadiusServiceStatusGroup	rcRadiusServerReachable	**Доступ:** Только для чтения **Синтаксическая структура:** TruthValue **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.14.1.1.1.1.6 **Определение:** Статус первичного сервера RADIUS.
rcRadiusBaseGroup	rcRadiusServerTimeOut	**Доступ:** Для чтения и записи **Синтаксическая структура:** Integer32 **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.14.1.1.1.1.5 **Определение:** Время ожидания аутентификатора при получении ответа от сервера RADIUS (в миллисекундах).
rcRadiusBaseGroup	rcTacacsServerAutTcpPort	**Доступ:** Для чтения и записи **Синтаксическая структура:** Integer32 **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.14.2.1.1.1.3

Группа(ы)	Объект	Описание
		Определение: TCP-порт сервера TACACS.
rcRadiusBaseGroup	rcTacacsServerId	**Доступ:** Только для чтения **Синтаксическая структура:** Integer32 **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.14.2.1.1.1.1 **Определение:** Значение индекса, используемое для идентификации сервера TACACS. 1. Первичный сервер 2. Резервный сервер
rcRadiusBaseGroup	rcTacacsServerIP	**Доступ:** Для чтения и записи **Синтаксическая структура:** IpAddress **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.14.2.1.1.1.2 **Определение:** IP-адрес сервера TACACS.
rcRadiusBaseGroup	rcTacacsServerMaxRetry	**Доступ:** Для чтения и записи **Синтаксическая структура:** Integer32 **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.14.2.1.1.1.4 **Определение:** Максимальное количество попыток аутентификатора связаться с сервером TACACS, чтобы аутентифицировать пользователя в случае какой-либо ошибки.
rcTacacsBaseGroup rcTacacsServiceStatusGroup	rcTacacsServerReachable	**Доступ:** Только для чтения **Синтаксическая структура:** TruthValue **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.14.2.1.1.1.6 **Определение:** Статус сервера TACACS.
rcTacacsBaseGroup	rcTacacsServerTimeOut	**Доступ:** Для чтения и записи **Синтаксическая структура:** Integer32 **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.14.2.1.1.1.5 **Определение:** Время ожидания аутентификатора при получении ответа от сервера TACACS (в миллисекундах).
rcTacacsNotifyGroup	tacacsServiceAvailableChange	**Идентификатор объекта:** 1.3.6.1.4.1.15004.5.23 **Определение:** Уведомление, которое генерируется при изменении статуса службы TACACS.

RUGGEDCOM-DIGITAL-INPUTS-MIB

Группа(ы)	Объект	Описание
rcDigitalInputsTableGroup	rcDiActiveState	**Доступ:** Для чтения и записи **Синтаксическая структура:** RcLowOrHigh **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.8.1.1.1.3.1 **Определение:** Состояние, которое активирует оповещение для этого цифрового входа.

Группа(ы)	Объект	Описание
rcDigitalInputsTableGroup	rcDiAlarm	**Доступ:** Для чтения и записи **Синтаксическая структура:** EnabledStatus **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.8.1.1.1.2.1 **Определение:** Текущее состояние оповещения для этого цифрового входа. Изменение значения этого объекта приведет к отправке уведомления (Trap-уведомления) digitalInputTrap.
rcDigitalInputsTableGroup	rcDiAlarmStatus	**Доступ:** Только для чтения **Синтаксическая структура:** RcActiveOrInactive **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.8.1.1.1.8.1 **Определение:** Текущее состояние оповещения для этого цифрового входа. Изменение значения этого объекта приведет к отправке уведомления (Trap-уведомления) digitalInputTrap.
rcDigitalInputsTableGroup	rcDiDelayOff	**Доступ:** Для чтения и записи **Синтаксическая структура:** Integer32 **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.8.1.1.1.5.1 **Определение:** Время, в течение которого вход должен быть неактивен, прежде чем оповещение будет отключено.
rcDigitalInputsTableGroup	rcDiDelayOn	**Доступ:** Для чтения и записи **Синтаксическая структура:** Integer32 **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.8.1.1.1.4.1 **Определение:** Время, в течение которого вход должен быть неактивен, прежде чем оповещение будет отключено.
rcDigitalInputsTableGroup	rcDiDescription	**Доступ:** Для чтения и записи **Синтаксическая структура:** DisplayString **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.8.1.1.1.6.1 **Определение:** Текущее состояние цифрового входа считывается с аппаратного обеспечения.
rcDigitalInputsTableGroup	rcDiID	**Доступ:** Недоступно **Синтаксическая структура:** Integer32 **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.8.1.1.1.1 **Определение:** Идентификатор физического цифрового входа устройства, для которого эта запись содержит параметры конфигурации.
rcDigitalInputsTableGroup	rcDiInputState	**Доступ:** Только для чтения **Синтаксическая структура:** RcLowOrHigh **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.8.1.1.1.7.1 **Определение:** Текущее состояние цифрового входа считывается с аппаратного обеспечения.

RUGGEDCOM-GPS-MIB

Группа(ы)	Объект	Описание
rcGpsBaseGroup01	rcFreqAdj	**Доступ:** Только для чтения **Синтаксическая структура:** Integer32 **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.9.1.9.0 **Определение:** Показывает текущий уровень дисциплины, применяемый к локальной эталонной частоте (TCXO).
rcGpsBaseGroup01	rcGpsAntPower	**Доступ:** Для чтения и записи **Синтаксическая структура:** TruthValue **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.9.1.4.0 **Определение:** Для GPS-приемника необходима активная антенна. Активная антенна включает в себя предварительный усилитель, который фильтрует и усиливает сигналы GPS до передачи их на приемник. Эта опция позволяет пользователю включать или выключать электропитание антенны GPS. Если антенна GPS используется совместно несколькими устройствами, то питание антенны GPS должно обеспечиваться только одним из всех устройств.
rcGpsBaseGroup01	rcGpsCableCompensate	**Доступ:** Для чтения и записи **Синтаксическая структура:** Integer32 **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.9.1.3.0 **Определение:** В случае использования длинного кабеля может потребоваться настройка величины компенсации задержки (в наносекундах), чтобы минимизировать погрешность синхронизации.
rcGpsBaseGroup01	rcGpsLatitude	**Доступ:** Только для чтения **Синтаксическая структура:** DisplayString **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.9.1.6.0 **Определение:** Широта GPS.
rcGpsBaseGroup01	rcGpsLocInt	**Доступ:** Для чтения и записи **Синтаксическая структура:** Integer32 **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.9.1.2.0 **Определение:** Интервал времени, который отводится приемнику GPS для завершения синхронизации с источником времени. Обычно для GPS-приемника требуется интервал времени порядка нескольких минут, чтобы захватить сигнал. Пользователь должен установить приемлемое значение интервала времени. Если этот интервал времени истечет без установления синхронизации, то система начнет раздавать точное время, используя значения локальных часов.
rcGpsBaseGroup01	rcGpsLongtitude	**Доступ:** Только для чтения **Синтаксическая структура:** DisplayString **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.9.1.7.0 **Определение:** Долгота GPS.

Группа(ы)	Объект	Описание
rcGpsNotifyGroup rcGpsBaseGroup rcGpsBaseGroup01	rcGpsStatus	**Доступ:** Только для чтения **Синтаксическая структура:** RcTimeSyncStatus **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.9.1.1.0 **Определение:** Статус синхронизации системы, когда GPS является первичным источником времени. При изменении значения этого объекта генерируется уведомление rcGpsStatusChange.
rcGpsNotifyGroup	rcGpsStatusChange	**Идентификатор объекта:** 1.3.6.1.4.1.15004.5.19 **Определение:** Уведомление, которое генерируется при изменении статуса модуля GPS.
rcGpsBaseGroup01	rcOFM	**Доступ:** Только для чтения **Синтаксическая структура:** Integer32 **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.9.1.8.0 **Определение:** Текущее смещение времени между системными и эталонными часами.
rcGpsBaseGroup01	rcSatelliteInView	**Доступ:** Только для чтения **Синтаксическая структура:** Integer32 **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.9.1.5.0 **Определение:** Количество спутников, отслеживаемых в настоящее время модулем GPS.

RUGGEDCOM-IP-MIB

Группа(ы)	Объект	Описание
rcIpObjectsGroup	rcIpConfigDefaultGateway	**Доступ:** Для чтения и записи **Синтаксическая структура:** IpAddress **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.3.1.3.0 **Определение:** IP-шлюз устройства по умолчанию.
rcIpObjectsGroupDflt	rcIpConfigDfltMgmtIpAddress	**Доступ:** Для чтения и записи **Синтаксическая структура:** IpAddress **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.3.1.4.0 **Определение:** Административный IP-адрес устройства.
rcIpObjectsGroupDflt	rcIpConfigDfltMgmtIpSubnet	**Доступ:** Для чтения и записи **Синтаксическая структура:** IpAddress **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.3.1.5.0 **Определение:** Маска подсети, связанная с записью административного IP-адреса. Маска представляет собой IP-адрес со значениями всех сетевых битов, установленными на 1, и значениями всех битов хостов, установленными на 0.
rcIpObjectsGroup	rcIpConfigMgmtIpAddress	**Доступ:** Для чтения и записи **Синтаксическая структура:** IpAddress **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.3.1.1.0 **Определение:** Административный IP-адрес устройства.
rcIpObjectsGroup	rcIpConfigMgmtIpSubnet	**Доступ:** Для чтения и записи

Группа(ы)	Объект	Описание
		Синтаксическая структура: IpAddress **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.3.1.2.0 **Определение:** Маска подсети, связанная с записью административного IP-адреса. Маска представляет собой IP-адрес со значениями всех сетевых битов, установленными на 1, и значениями всех битов хостов, установленными на 0.

RUGGEDCOM-IRIGB-MIB

Группа(ы)	Объект	Описание
rcIrigbAMOutGroup	rcIrigbAMOutput	**Доступ:** Для чтения и записи **Синтаксическая структура:** Integer **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.10.1.2.0 **Определение:** Выбор режима AM (амплитудная модуляция) для порта IRIGB.
rcIrigbCommonGroup	rcIrigbCableComp	**Доступ:** Для чтения и записи **Синтаксическая структура:** Integer32 **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.10.1.7.0 **Определение:** В случае использования длинного кабеля может потребоваться настройка величины компенсации задержки (в наносекундах), чтобы минимизировать погрешность синхронизации.
rcIrigbCommonGroup	rcIrigbExt	**Доступ:** Для чтения и записи **Синтаксическая структура:** Integer **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.10.1.4.0 **Определение:** В расширениях стандарта IRIGB, добавленных в IEEE1344, используются дополнительные биты в секции управляющих функций (CF) таймкода IRIGB. В пределах этой части таймкода биты предназначены для дополнительных функций, в том числе: календарный год, секунды координации, ожидающееся прибавление секунд координации, декретное летнее время (DST), ожидающееся применение DST, сдвиг местного времени и качество отсчета времени. Обратите внимание, что только временные коды Bxx0, Bxx1, Bxx4 и Bxx5 поддерживают расширения IRIGB.
rcIrigbCommonGroup	rcIrigbFreqAdj	**Доступ:** Для чтения и записи **Синтаксическая структура:** Integer32 **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.10.1.9.0 **Определение:** Показывает текущий уровень дисциплины, применяемый к локальной эталонной частоте (TCXO).
rcIrigbInputGroup	rcIrigbInput	**Доступ:** Для чтения и записи **Синтаксическая структура:** Integer **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.10.1.5.0

Группа(ы)	Объект	Описание
		Определение: Этот параметр относится как к входам с режимом AM (амплитудная модуляция), так и к входам с режимом PWM (широтно-импульсная модуляция).
rcIrigbCommonGroup	rcIrigbLockInt	**Доступ:** Для чтения и записи **Синтаксическая структура:** Integer32 **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.10.1.6.0 **Определение:** Интервал времени, который отводится приемнику IRIGB для завершения синхронизации с источником времени. Обычно для IRIGB-приемника требуется интервал времени порядка нескольких минут, чтобы захватить сигнал. Пользователь должен установить приемлемое значение интервала времени. Если этот интервал времени истечет без установления синхронизации, то система начнет раздавать точное время, используя значения локальных часов.
rcIrigbCommonGroup	rcIrigbOFM	**Доступ:** Только для чтения **Синтаксическая структура:** Integer32 **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.10.1.8.0 **Определение:** Текущее смещение времени между системными и эталонными часами.
rcIrigbTTLOutput01Group	rcIrigbOutputPWM1	**Доступ:** Для чтения и записи **Синтаксическая структура:** Integer **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.10.1.10.0 **Определение:** Выбирает режим работы порта TTL-выхода. Режим PWM (ШИМ) соответствует стандарту IRIG 200-04. PPx обеспечивает универсальный интерфейс передачи сигналов "импульс в секунду" для синхронизации внешних устройств.
rcIrigbTTLOutput02Group	rcIrigbOutputPWM2	**Доступ:** Для чтения и записи **Синтаксическая структура:** Integer **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.10.1.14.0 **Определение:** Выбирает режим работы порта2 TTL-выхода. Режим PWM (ШИМ) соответствует стандарту IRIG 200-04. PPx обеспечивает универсальный интерфейс передачи сигналов "импульс в секунду" для синхронизации внешних устройств.
rcIrigbTTLOutput01Group	rcIrigbPulseInterval1	**Доступ:** Для чтения и записи **Синтаксическая структура:** Integer32 **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.10.1.11.0 **Определение:** Выбор интервала импульсов для порта TTL-выхода (в секундах). Этот параметр используется совместно с PPx для обеспечения универсального интерфейса передачи сигналов "импульс в секунду" для синхронизации внешних устройств.
rcIrigbTTLOutput02Group	rcIrigbPulseInterval2	**Доступ:** Для чтения и записи **Синтаксическая структура:** Integer32 **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.10.1.15.0 **Определение:** Выбор интервала импульсов для порта2 TTL-выхода (в секундах). Этот параметр используется

Группа(ы)	Объект	Описание
		совместно с PPx для обеспечения универсального интерфейса передачи сигналов "импульс в секунду" для синхронизации внешних устройств.
rcIrigbTTLOutput01Group	rcIrigbPulseWidth1	**Доступ:** Для чтения и записи **Синтаксическая структура:** Integer32 **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.10.1.12.0 **Определение:** Выбирает значение ширины импульса для порта TTL-выхода (в миллисекундах). Этот параметр используется вместе с PPx для управления шириной импульса.
rcIrigbTTLOutput02Group	rcIrigbPulseWidth2	**Доступ:** Для чтения и записи **Синтаксическая структура:** Integer32 **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.10.1.16.0 **Определение:** Выбирает значение ширины импульса для порта2 TTL-выхода (в миллисекундах). Этот параметр используется вместе с PPx для управления шириной импульса.
rcIrigbTTLOutput01Group	rcIrigbStartTime1	**Доступ:** Для чтения и записи **Синтаксическая структура:** RcTimeStamp **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.10.1.13.0 **Определение:** Этот параметр используется вместе с PPx для установки времени начала первого события PPx. Для этого параметра должно быть задано значение времени не позже 15-ти секунд до начала требуемого события PPx, в противном случае первое событие PPx может быть потеряно.
rcIrigbTTLOutput02Group	rcIrigbStartTime2	**Доступ:** Для чтения и записи **Синтаксическая структура:** RcTimeStamp **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.10.1.17.0 **Определение:** Этот параметр используется вместе с PPx для установки времени начала первого события PPx. Для этого параметра должно быть задано значение времени не позже 15-ти секунд до начала требуемого события PPx, в противном случае первое событие PPx может быть потеряно.
rcIrigbCommonGroup rcIrigbBaseGroup	rcIrigbStatus	**Доступ:** Только для чтения **Синтаксическая структура:** RcTimeSyncStatus **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.10.1.1.0 **Определение:** Статус синхронизации системы, когда IRIGB является первичным источником времени. При изменении значения этого объекта будет отправлено уведомление rcIrigbStatusChange.
rcIrigbNotifyGroup	rcIrigbStatusChange	**Идентификатор объекта:** 1.3.6.1.4.1.15004.5.20 **Определение:** Уведомление, которое генерируется при изменении статуса модуля IRIGB.
rcIrigbCommonGroup	rcIrigbTimeCode	**Доступ:** Для чтения и записи **Синтаксическая структура:** Integer **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.10.1.3.0

Группа(ы)	Объект	Описание
		Определение: Данное устройство использует следующие условные обозначения для декодирования таймкода IRIGB: буква [B] представляет формат IRIG-B, [xx] представляет [00] для режима работы ШИМ/TTL и [12] для режима работы AM. Например, Bxx7 представляет B007 для режима работы ШИМ/TTL и B127 для режима работы AM. Только таймкоды Bxx0, Bxx1, Bxx4 и Bxx5 поддерживают расширения IRIGB.

RUGGEDCOM-MC30-MIB

Группа(ы)	Объект	Описание
rcPoeNotifyGroup	rcPoeOverheat	**Доступ:** Только для чтения **Синтаксическая структура:** Integer **Идентификатор объекта:** 1.3.6.1.4.1.15004.5.12.1 **Определение:** При перегреве PoE для этого объекта будет установлено значение "true(1)". При каждом изменении значения этого объекта с false (2) на true(1) устройство генерирует уведомление rcPoeOverheat.

RUGGEDCOM-NTP-MIB

Группа(ы)	Объект	Описание
rcNTPNotifyGroup	ntpServiceAvailableChange	**Идентификатор объекта:** 1.3.6.1.4.1.15004.5.21 **Определение:** Уведомление, которое генерируется при изменении статуса службы NTP.
rcNTPBaseGroup	rcNTPBackUpServerIP	**Доступ:** Для чтения и записи **Синтаксическая структура:** IpAddress **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.13.1.4.0 **Определение:** IP-адрес резервного сервера.
rcNTPServiceStatusGroup	rcNTPBackUpServerReachable	**Доступ:** Только для чтения **Синтаксическая структура:** TruthValue **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.13.1.9.0 **Определение:** Статус резервного сервера NTP.
rcNTPBaseGroup	rcNTPBackUpServerUpdatePeriod	**Доступ:** Для чтения и записи **Синтаксическая структура:** Integer32 **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.13.1.5.0 **Определение:** Частота опроса (S)NTP-сервера для обновления времени (в минутах).
rcNTPBaseGroup	rcNTPFRQADJ	**Доступ:** Только для чтения **Синтаксическая структура:** Integer32

Группа(ы)	Объект	Описание
		Идентификатор объекта: 1.3.6.1.4.1.15004.4.13.1.7.0 **Определение:** Показывает текущий уровень дисциплины, применяемый к локальной эталонной частоте (TCXO), т. е. объем корректировки в данной системе, необходимый для синхронизации с текущим эталонным значением.
rcNTPBaseGroup	rcNTPOFM	**Доступ:** Только для чтения **Синтаксическая структура:** Integer32 **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.13.1.6.0 **Определение:** Текущее смещение времени между часами (S)NTP-сервера и часами на стороне клиента рассчитывается как <время часов на стороне клиента> – <время часов на стороне сервера>.
rcNTPBaseGroup	rcNTPPriServerIP	**Доступ:** Для чтения и записи **Синтаксическая структура:** IpAddress **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.13.1.2.0 **Определение:** IP-адрес первичного сервера.
rcNTPServiceStatusGroup	rcNTPPriServerReachable	**Доступ:** Только для чтения **Синтаксическая структура:** TruthValue **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.13.1.8.0 **Определение:** IP-адрес первичного сервера NTP.
rcNTPBaseGroup	rcNTPPriServerUpdatePeriod	**Доступ:** Для чтения и записи **Синтаксическая структура:** Integer32 **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.13.1.3.0 **Определение:** Частота опроса (S)NTP-сервера для обновления времени (в минутах).
rcNTPBaseGroup	rcSNTPEnabled	**Доступ:** Для чтения и записи **Синтаксическая структура:** TruthValue **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.13.1.1.0 **Определение:** Включение/отключение функций SNTP-сервера.

RUGGEDCOM-POE-MIB

Группа(ы)	Объект	Описание
rcBasePoeGroup	rcPoeCapacity	**Доступ:** Для чтения и записи **Синтаксическая структура:** Integer32

Группа(ы)	Объект	Описание
		Идентификатор объекта: 1.3.6.1.4.1.15004.4.7.1.1.0 **Определение:** Максимальная общая выходная мощность, которая может быть обеспечена портами PoE. При установке для этого объекта значения "0" емкость будет не ограничена. Когда общее энергопотребление достигнет этого предела, порты PoE с низким приоритетом будут отключены.
rcBasePoeGroup	rcPoeConsumption	**Доступ:** Только для чтения **Синтаксическая структура:** Integer32 **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.7.1.4.0 **Определение:** Текущее общее энергопотребление для всех устройств PoE.
rcBasePoeGroup	rcPoeMinimumVoltage	**Доступ:** Для чтения и записи **Синтаксическая структура:** Integer32 **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.7.1.2.0 **Определение:** Минимальное требуемое напряжение, выдаваемое портами PoE. Минимальное необходимое напряжение для портов PoE. Если напряжение PoE падает ниже этого порога, порты PoE с низким приоритетом будут отключены.
rcBasePoeStatusGroup	rcPoeOverheatStatus	**Доступ:** Только для чтения **Синтаксическая структура:** TruthValue **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.7.1.5.0 **Определение:** При перегреве PoE для этого объекта будет установлено значение "true(1)". При каждом изменении значения этого объекта с false (2) на true(1) устройство генерирует уведомление *rcPoeOverheat*.
rcPoeNotifyGroup	rcPoeOverload	**Доступ:** Только для чтения **Синтаксическая структура:** Integer **Идентификатор объекта:** 1.3.6.1.4.1.15004.5.12.2 **Определение:** При перегрузке PoE для этого объекта будет установлено значение "true(1)". При каждом изменении значения этого объекта с false(2) на true(1) устройство генерирует уведомление *rcPoeOverload*.
rcBasePoeStatusGroup	rcPoeOverloadStatus	**Доступ:** Только для чтения **Синтаксическая структура:** TruthValue **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.7.1.6.0 **Определение:** При перегрузке PoE для этого объекта будет установлено значение "true(1)". При каждом изменении значения этого объекта с false(2) на true(1) устройство генерирует уведомление *rcPoeOverload*.
rcPoeTableGroup	rcPoePort	**Доступ:** Недоступно **Синтаксическая структура:** Integer32 **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.7.2.1.1.1 **Определение:** Порт PoE, для которого эта запись содержит данные. Значение ограничено количеством портов в устройстве.
rcPoeTableGroup	rcPoePortAdmin	**Доступ:** Для чтения и записи

Группа(ы)	Объект	Описание
		Синтаксическая структура: TruthValue **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.7.2.1.1.2.13 **Определение:** Порт PoE, для которого эта запись содержит данные. Значение ограничено количеством портов в устройстве.
rcPoeTableGroup	rcPoePortClass	**Доступ:** Только для чтения **Синтаксическая структура:** Integer32 **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.7.2.1.1.5.13 **Определение:** Значение класса PoE, которое определяет уровень мощности.
rcPoeTableGroup	rcPoePortCurrent	**Доступ:** Только для чтения **Синтаксическая структура:** Integer32 **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.7.2.1.1.7.13 **Определение:** Значение класса PoE, которое определяет уровень мощности.
rcPoeTableGroup	rcPoePortPowered	**Доступ:** Только для чтения **Синтаксическая структура:** TruthValue **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.7.2.1.1.4.13 **Определение:** Независимо от того, подается ли питание через порт в настоящий момент.
rcPoeTablePriorityGroup	rcPoePortPriority	**Доступ:** Для чтения и записи **Синтаксическая структура:** Integer **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.7.2.1.1.3.13 **Определение:** Приоритет порта. Порты с низким приоритетом будут отключены при перегрузке источника питания.
rcPoeTableGroup	rcPoePortVoltage	**Доступ:** Только для чтения **Синтаксическая структура:** Integer32 **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.7.2.1.1.6.13 **Определение:** Значение класса PoE, которое определяет уровень мощности.
rcBasePoeGroup	rcPoeReenableTime	**Доступ:** Для чтения и записи **Синтаксическая структура:** Unsigned32 **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.7.1.3.0 **Определение:** Время ожидания повторного включения портов PoE с низким приоритетом после их отключения из-за перегрузки.
rcPoeNotifyGroup	rcPoeUndervoltage	**Идентификатор объекта:** 1.3.6.1.4.1.15004.5.12.3 **Определение:** Низкое напряжение на PoE.
rcBasePoeStatusGroup	rcPoeUndervoltageStatus	**Доступ:** Только для чтения

Группа(ы)	Объект	Описание
		Синтаксическая структура: TruthValue **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.7.1.7.0 **Определение:** Символ, который можно использовать для принудительного перенаправления накопленных данных в сеть для подключения к ведущему устройству с динамическим адресом. Если символ определения пакета не указан, накопленные данные будут перенаправляться на основе значения параметра времени ожидания обработки пакета *rcPreemptRSDynPackTimer*.

RUGGEDCOM-PTP1588-MIB

Группа(ы)	Объект	Описание
rcPTP1588BaseGroup	rcPTP1588ClkType	**Доступ:** Для чтения и записи **Синтаксическая структура:** Integer **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.12.1.1.0 **Определение:** Тип часов PTP1588.
rcPTP1588BaseGroup	rcPTP1588E2EDelay	**Доступ:** Только для чтения **Синтаксическая структура:** Integer32 **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.12.1.12.0 **Определение:** Измеренная задержка E2E (т.е. запрос-ответ) между ведущим и ведомым часами.
rcPTP1588BaseGroup	rcPTP1588EthPorts	**Доступ:** Для чтения и записи **Синтаксическая структура:** PortList **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.12.1.2.0 **Определение:** Выбор портов Ethernet, которые будут участвовать в обмене сообщениями по протоколу PTP (Протокол точного времени).
rcPTP1588BaseGroup	rcPTP1588NetClass	**Доступ:** Для чтения и записи **Синтаксическая структура:** Integer **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.12.1.4.0 **Определение:** Указывает, все ли синхронизируемые устройства соответствуют требованиям IEEE 1588 (сеть с поддержкой IEEE 1588) или включены также устройства, не поддерживающие IEEE 1588 (для сетей без поддержки IEEE 1588).
rcPTP1588BaseGroup	rcPTP1588ServoStatus	**Доступ:** Только для чтения **Синтаксическая структура:** DisplayString **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.12.1.10.0 **Определение:** Показывает статус сервосистемы часов. Сервосистема часов используется для регулирования системных часов. Статус часов представляет значение точности часов, указываемое в желаемых пределах.
rcPTP1588BaseGroup	rcPTP1588SlaveAutoReg	**Доступ:** Для чтения и записи **Синтаксическая структура:** TruthValue **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.12.1.7.0

Группа(ы)	Объект	Описание
		Определение: Этот параметр является специфичным для одноадресной передачи. Позволяет пользователю автоматически регистрировать ведомые часы в одноадресном ведущем устройстве, согласно значению атрибута "Master IP Address".
rcPTP1588BaseGroup	rcPTP1588SlaveBackUpIP	**Доступ:** Для чтения и записи **Синтаксическая структура:** IpAddress **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.12.1.9.0 **Определение:** Этот параметр является специфичным для одноадресной передачи и представляет собой IP-адрес ведущих часов для резервирования при одноадресной передаче сигнала по протоколу PTP (Протокол точного времени).
rcPTP1588BaseGroup	rcPTP1588SlaveDomain	**Доступ:** Для чтения и записи **Синтаксическая структура:** Integer32 **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.12.1.6.0 **Определение:** Выбор номера домена PTP (Протокол точного времени) для ведомых часов. PTP-домен – это логическая группа PTP-часов, которые синхронизируются друг с другом по протоколу PTP.
rcPTP1588BaseGroup	rcPTP1588SlaveEthPort	**Доступ:** Для чтения и записи **Синтаксическая структура:** PortList **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.12.1.5.0 **Определение:** Выбирает порт Ethernet, который будет работать как ведомый при конфигурации устройства в качестве граничных часов.
rcPTP1588BaseGroup	rcPTP1588SlaveFeqAdj	**Доступ:** Только для чтения **Синтаксическая структура:** Integer32 **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.12.1.11.0 **Определение:** Этот параметр показывает текущий уровень дисциплины, применяемый к локальной эталонной частоте (TCXO), т. е. объем корректировки в данной системе, необходимый для синхронизации с текущим эталонным значением.
rcPTP1588BaseGroup	rcPTP1588SlaveMasteIP	**Доступ:** Для чтения и записи **Синтаксическая структура:** IpAddress **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.12.1.8.0 **Определение:** Этот параметр является специфичным для одноадресной передачи и представляет собой IP-адрес ведущих часов при одноадресной передаче сигнала по протоколу PTP (Протокол точного времени).
rcPTP1588BaseGroup	rcPTP1588StartUpWait	**Доступ:** Для чтения и записи **Синтаксическая структура:** Integer32 **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.12.1.3.0 **Определение:** Время в секундах для начальной загрузки PTP-сети более упорядоченным образом.

RUGGEDCOM-SERIAL-MIB

Группа(ы)	Объект	Описание
rcSerialConnStatsGroup	rcConnStatsRxPkts	**Доступ:** Только для чтения **Синтаксическая структура:** Integer32 **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.6.15.1.1.4 **Определение:** Количество полученных пакетов.
rcSerialConnStatsGroup	rcConnStatsTxPkts	**Доступ:** Только для чтения **Синтаксическая структура:** Integer32 **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.6.15.1.1.5 **Определение:** Количество переданных пакетов.
rcSerialDnpGroup	rcDnpAgingTimer	**Доступ:** Для чтения и записи **Синтаксическая структура:** Integer32 **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.6.8.4.0 **Определение:** Время бездействия связи, после которого полученный при обучении DNP-адрес удаляется из таблицы адресов устройства. Записи в таблице "Статистика по ссылкам" с устаревшими адресами будут храниться до момента очистки статистики.
rcSerialDnpGroup	rcDnpDscp	**Доступ:** Для чтения и записи **Синтаксическая структура:** Integer32 **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.6.8.6.0 **Определение:** Значение байта DS, которое должно быть указано в заголовке IP. Настройка значения байта DS поддерживается только для исходящего трафика.
rcSerialDnpGroup	rcDnpIpPort	**Доступ:** Для чтения и записи **Синтаксическая структура:** Integer32 **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.6.8.2.0 **Определение:** Номер локального порта, на котором прослушиваются соединения или датаграммы UDP с использованием протокола DNP.
rcSerialDnpGroup	rcDnpLearning	**Доступ:** Для чтения и записи **Синтаксическая структура:** IpAddress **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.6.8.3.0 **Определение:** Разрешение или запрет определения адресов. Определение может быть отключено или включено с помощью административного IP-интерфейса, или включено для интерфейса с определенным IP-адресом. Если обучение включено и удаленный адрес неизвестен, будет отправлено широковещательное сообщение UDP и адреса источников для устройств, использующих протокол DNP, будут изучены. Если локальный адрес неизвестен, то на все последовательные порты, работающие по протоколу DNP, будет отправлено сообщение. Обучение для локальных адресов будет выполнено по данным локальных ответов. Если передача по TCP настроена, будет установлено соединение с устройствами с соответствующим IP-адресом.
rcSerialDnpGroup	rcDnpLinkStats	**Доступ:** Для чтения и записи

Группа(ы)	Объект	Описание
		Синтаксическая структура: Integer32 **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.6.8.5.0 **Определение:** Включение сбора статистики по ссылкам.
rcSerialDnpRsGroup	rcDnpRsCalllDir	**Доступ:** Для чтения и записи **Синтаксическая структура:** RcCallDir **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.6.9.1.1.2.1 **Определение:** Определяет следующее: • входящее(0): Принять входящее соединение • исходящее(1): Установить исходящее соединение • оба(2): Установить исходящее соединение и ожидать входящего соединения **Примечание** Этот параметр применим только для передачи по TCP.
rcSerialDnpRsGroup	rcDnpRsIpAdd	**Доступ:** Для чтения и записи **Синтаксическая структура:** IpAddress **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.6.9.1.1.7.1 **Определение:** Определяет IpAddress на основе следующего: • Для исходящего TCP-соединения (клиент), rcRawSockCallDir имеет значение "out(2)". Это удаленный IP-адрес для связи. • Для входящего TCP-соединения (сервер) rcRawSockCallDir имеет значение "out (2)" или "both(3)". Это IP-адрес локального интерфейса при прослушивании локального порта для запроса на подключение. • Если разрешены как исходящие, так и входящие соединения (клиент или сервер), rcRawSockCallDir имеет значение "both (3)". Это удаленный IP-адрес для запроса на установку исходящего TCP-соединения или для приема вызовов. • Для UDP-транспорта – адрес интерфейса для прослушивания датаграмм UDP.
rcSerialDnpRsGroup	rcDnpRsLinkStats	**Доступ:** Для чтения и записи **Синтаксическая структура:** EnabledStatus **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.6.9.1.1.8.1 **Определение:** Включение сбора статистики по ссылкам.
rcSerialDnpRsGroup	rcDnpRsLocPort	**Доступ:** Для чтения и записи **Синтаксическая структура:** Integer32 **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.6.9.1.1.5.1 **Определение:** Локальный IP-порт для прослушивания входящего TCP-соединения или датаграмм UDP.
rcSerialDnpRsGroup	rcDnpRsMaxConns	**Доступ:** Для чтения и записи **Синтаксическая структура:** Integer32 **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.6.9.1.1.4.1

Группа(ы)	Объект	Описание
		Определение: Максимальное количество разрешенных входящих TCP-соединений.
rcSerialDnpRsGroup	rcDnpRsRemPort	**Доступ:** Для чтения и записи **Синтаксическая структура:** Integer32 **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.6.9.1.1.6.1 **Определение:** Удаленный TCP-порт, используемый при установке исходящего соединения.
rcSerialDnpRsGroup	rcDnpRsTransport	**Доступ:** Для чтения и записи **Синтаксическая структура:** RcTransport **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.6.9.1.1.3.1 **Определение:** Транспортный протокол, используемый для IP-трафика с использованием протокола DNPRS на этом порту.
rcSerialDnpGroup	rcDnpTransport	**Доступ:** Для чтения и записи **Синтаксическая структура:** RcTransport **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.6.8.1.0 **Определение:** Транспортный протокол, используемый для IP-трафика с использованием протокола DNP.
	rcMbClient	**Идентификатор объекта:** 1.3.6.1.4.1.15004.4.6.3 **Определение:** Главное поддерево для управления параметрами клиента протокола Modbus на последовательных устройствах RUGGEDCOM.
	rcMbClientDscp	**Доступ:** Для чтения и записи **Синтаксическая структура:** Integer32 **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.6.3.4.0 **Определение:** Значение байта DS, которое должно быть указано в заголовке IP. Настройка значения байта DS поддерживается только для исходящего трафика.
	rcMbClientFwdExcp	**Доступ:** Для чтения и записи **Синтаксическая структура:** Integer32 **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.6.3.2.0 **Определение:** Включает перенаправление сообщений об исключениях на ведущее устройство в виде кодов исключений 10 (без пути) или 11 (без ответа). Когда ведущее устройство опрашивает RTU без конфигурации или удаленный сервер Modbus получает опрос для RTU, конфигурация для которого отсутствует или время ожидания для которого превышает допустимое значение, возвращается сообщение об исключении. Для этого объекта следует задать значение "disabled(2)", если ведущее устройство не поддерживает исключения, но распознает сбои превышения время ожидания для ответа.
	rcMbClientIPPort	**Доступ:** Для чтения и записи **Синтаксическая структура:** Integer32 **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.6.3.1.0

Группа(ы)	Объект	Описание
		Определение: Номер удаленного порта, на который диспетчер соединений протокола отправляет запросы для TCP-соединения.
	rcMbClientLinkStats	**Доступ:** Для чтения и записи **Синтаксическая структура:** Integer32 **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.6.3.3.0 **Определение:** Включение сбора статистики по ссылкам.
rcSerialMbServerGroup	rcMbServerAuxTcpPort	**Доступ:** Для чтения и записи **Синтаксическая структура:** Integer32 **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.6.2.1.1.3.1 **Определение:** Альтернативный номер TCP-порта, на котором rcMbServerPort может прослушивать входящие TCP-соединения. Поскольку сервер TCP Modbus всегда прослушивает TCP-порт 502, этот параметр позволяет последовательному устройству RUGGEDCOM принимать запрос на подключение по протоколу TCP Modbus на обоих TCP-портах.
rcSerialMbServerGroup	rcMbServerLinkStats	**Доступ:** Для чтения и записи **Синтаксическая структура:** EnabledStatus **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.6.2.1.1.5.1 **Определение:** Включение сбора статистики по ссылкам.
	rcMbServerPort	**Доступ:** Недоступно **Синтаксическая структура:** Integer **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.6.2.1.1.1 **Определение:** Физический номер последовательного порта, для которого эта запись содержит настройки конфигурации протокола сервера Modbus.
rcSerialMbServerGroup	rcMbServerRespTimer	**Доступ:** Для чтения и записи **Синтаксическая структура:** Integer32 **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.6.2.1.1.2.1 **Определение:** Допустимое время ожидания начала ответа RTU.
rcSerialMbServerGroup	rcMbServerSendExcep	**Доступ:** Для чтения и записи **Синтаксическая структура:** EnabledStatus **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.6.2.1.1.4.1 **Определение:** Позволяет RUGGEDCOM последовательным устройствам включать или отключать отправку исключения TCP Modbus обратно ведущему устройству, если ответ от RTU не был получен в течение ожидаемого времени.
rcSerialMicrolokGroup	rcMicrolokDscp	**Доступ:** Для чтения и записи **Синтаксическая структура:** Integer32 **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.6.7.4.0 **Определение:** Значение байта DS, которое должно быть указано в заголовке IP. Настройка значения байта DS поддерживается только для исходящего трафика.
rcSerialMicrolokGroup	rcMicrolokIpPort	**Доступ:** Для чтения и записи

Группа(ы)	Объект	Описание
		Синтаксическая структура: Integer32 **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.6.7.2.0 **Определение:** Номер локального порта, на котором прослушиваются соединения или датаграммы UDP с использованием протокола Microlok.
rcSerialMicrolokGroup	rcMicrolokLinkStats	**Доступ:** Для чтения и записи **Синтаксическая структура:** EnabledStatus **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.6.7.3.0 **Определение:** Включение сбора статистики по ссылкам.
rcSerialMicrolokGroup	rcMicrolokTransport	**Доступ:** Для чтения и записи **Синтаксическая структура:** RcTransport **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.6.7.1.0 **Определение:** Транспортный протокол, используемый для IP-трафика с использованием протокола Microlok.
rcSerialMirrBitsGroup	rcMirrBitsIpAdd	**Доступ:** Для чтения и записи **Синтаксическая структура:** IpAddress **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.6.10.1.1.5.1 **Определение:** IP-адрес интерфейса для прослушивания датаграмм UDP.
rcSerialMirrBitsGroup	rcMirrBitsLinkStats	**Доступ:** Для чтения и записи **Синтаксическая структура:** EnabledStatus **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.6.10.1.1.6.1 **Определение:** Включение сбора статистики по ссылкам.
rcSerialMirrBitsGroup	rcMirrBitsLocPort	**Доступ:** Для чтения и записи **Синтаксическая структура:** Integer32 **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.6.10.1.1.3.1 **Определение:** Локальный IP-порт для прослушивания UDP датаграмм.
rcSerialMirrBitsGroup	rcMirrBitsRemPort	**Доступ:** Для чтения и записи **Синтаксическая структура:** Integer32 **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.6.10.1.1.4.1 **Определение:** Удаленный порт, с которым протоколы на этом порту могут обмениваться датаграммами UDP.
rcSerialMirrBitsGroup	rcMirrBitsTransport	**Доступ:** Для чтения и записи **Синтаксическая структура:** RcTransport **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.6.10.1.1.2.1 **Определение:** Транспортный протокол, используемый для IP-трафика с использованием Mirrored Bits (зеркалируемых битов) на этом порту. Этот объект всегда имеет значение udp(2).
rcSerialPreEmpRawSockGroup	rcPreemptRSDynPackChar	**Доступ:** Для чтения и записи

Группа(ы)	Объект	Описание
		Синтаксическая структура: Integer32 **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.6.5.1.1.10.1 **Определение:** Символ, который можно использовать для принудительного перенаправления накопленных данных в сеть для подключения к ведущему устройству с динамическим адресом. Если символ определения пакета не указан, накопленные данные будут перенаправляться на основе значения параметра времени ожидания обработки пакета *rcPreemptRSDynPackTimer*.
rcSerialPreEmpRawSockGroup	rcPreemptRSDynPackTimer	**Доступ:** Для чтения и записи **Синтаксическая структура:** Integer32 **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.6.5.1.1.11.1 **Определение:** Задержка с момента получения последнего символа до момента перенаправления данных на ведущее устройство с динамическим адресом (в миллисекундах).
rcSerialPreEmpRawSockGroup	rcPreemptRSDynTimeout	**Доступ:** Для чтения и записи **Синтаксическая структура:** Integer32 **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.6.5.1.1.12.1 **Определение:** Время простоя ведущего устройства с динамическим адресом до того, как его соединение будет закрыто (в секундах). Протокол прослушивает сокет, открытый для ведущего устройства с динамическим адресом, и, если в течение этого времени данные не будут получены, соединение будет закрыто.
rcSerialPreEmpRawSockGroup	rcPreemptRSFlowControl	**Доступ:** Для чтения и записи **Синтаксическая структура:** RcFlowControl **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.6.5.1.1.5.1 **Определение:** Тип FlowControl, который будет использоваться для порта.
rcSerialPreEmpRawSockGroup	rcPreemptRSIpAdd	**Доступ:** Для чтения и записи **Синтаксическая структура:** IpAddress **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.6.5.1.1.8.1 **Определение:** Определяет IpAddress на основе следующего: • Для исходящих TCP-соединений (клиент), rcRawSockCallDir имеет значение "out(2)" и является удаленным IP-адрес для установки соединения. • Для входящего TCP-соединения (сервер) rcRawSockCallDir имеет значение "out (2)" или "both(3)"; это IP-адрес локального интерфейса при прослушивании локального порта для запроса на подключение. • Если разрешены как исходящие, так и входящие соединения (клиент или сервер), rcRawSockCallDir имеет значение "both (3)"; это удаленный IP-

Группа(ы)	Объект	Описание
		адрес для запроса на установку исходящего TCP-соединения или для приема вызовов.
rcSerialPreEmpRawSockGroup	rcPreemptRSLinkStats	**Доступ:** Для чтения и записи **Синтаксическая структура:** EnabledStatus **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.6.5.1.1.9.1 **Определение:** Включение сбора статистики по ссылкам.
rcSerialPreEmpRawSockGroup	rcPreemptRSLocPort	**Доступ:** Для чтения и записи **Синтаксическая структура:** Integer32 **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.6.5.1.1.6.1 **Определение:** Локальный IP-порт для прослушивания входящего TCP-соединения или датаграммы UDP.
rcSerialPreEmpRawSockGroup	rcPreemptRSPackChar	**Доступ:** Для чтения и записи **Синтаксическая структура:** Integer32 **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.6.5.1.1.2.1 **Определение:** Символ, который можно использовать для принудительного перенаправления накопленных данных в сеть. Если символ определения пакета не указан, для объекта устанавливается значение "256", и накопленные данные будут перенаправляться на основе значения параметра времени ожидания обработки пакета – значения, указанного для объекта *rcPreemptRSPackTimer*.
rcSerialPreEmpRawSockGroup	rcPreemptRSPackSize	**Доступ:** Для чтения и записи **Синтаксическая структура:** Integer32 **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.6.5.1.1.4.1 **Определение:** Максимальное количество байт, полученных от последовательного порта, которые должны быть упакованы в один IP-пакет.
rcSerialPreEmpRawSockGroup	rcPreemptRSPackTimer	**Доступ:** Для чтения и записи **Синтаксическая структура:** Integer32 **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.6.5.1.1.3.1 **Определение:** Задержка с момента получения последнего символа до момента перенаправления данных (в миллисекундах).
rcSerialPreEmpRawSockGroup	rcPreemptRSRemPort	**Доступ:** Для чтения и записи **Синтаксическая структура:** Integer32 **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.6.5.1.1.7.1 **Определение:** Удаленный TCP-порт, используемый при установке исходящего соединения.
rcSerialRawSocketGroup	rcRawSockCallDir	**Доступ:** Для чтения и записи **Синтаксическая структура:** RcCallDir **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.6.4.1.1.7.1 **Определение:** Определяет следующее: **Примечание** Этот параметр применим только для передачи по TCP.

Группа(ы)	Объект	Описание
		• входящее(0): Принять входящее соединение • исходящее(1): Установить исходящее соединение • оба(2): Установить исходящее соединение и ожидать входящего соединения
rcSerialRawSocketGroup	rcRawSockFlowControl	**Доступ:** Для чтения и записи **Синтаксическая структура:** RcFlowControl **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.6.4.1.1.5.1 **Определение:** Тип FlowControl, который будет использоваться для порта.
rcSerialRawSocketGroup	rcRawSockIpAdd	**Доступ:** Для чтения и записи **Синтаксическая структура:** IpAddress **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.6.4.1.1.11.1 **Определение:** >Определяет IpAddress на основе следующего: • Для исходящих TCP-соединений (клиент), rcRawSockCallDir имеет значение "out(2)" и является удаленным IP-адрес для установки соединения. • Для входящего TCP-соединения (сервер) rcRawSockCallDir имеет значение "out (2)" или "both(3)"; это IP-адрес локального интерфейса при прослушивании локального порта для запроса на подключение. • Если разрешены как исходящие, так и входящие соединения (клиент или сервер), rcRawSockCallDir имеет значение "both (3)"; это удаленный IP-адрес для запроса на установку исходящего TCP-соединения или для приема вызовов. • Для UDP-транспорта – адрес интерфейса для прослушивания датаграмм UDP.
rcSerialRawSocketGroup	rcRawSockLinkStats	**Доступ:** Для чтения и записи **Синтаксическая структура:** EnabledStatus **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.6.4.1.1.12.1 **Определение:** Включение сбора статистики по ссылкам для RawSocket на этом порту.
rcSerialRawSocketGroup	rcRawSockLocPort	**Доступ:** Для чтения и записи **Синтаксическая структура:** Integer32 **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.6.4.1.1.9.1 **Определение:** Локальный IP-порт для прослушивания входящего TCP-соединения или датаграмм UDP.
rcSerialRawSocketGroup	rcRawSockMaxConn	**Доступ:** Для чтения и записи **Синтаксическая структура:** Integer32 **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.6.4.1.1.8.1 **Определение:** Максимальное количество разрешенных входящих TCP-соединений.
rcSerialMbClientGroup	rcRawSockPackChar	**Доступ:** Для чтения и записи **Синтаксическая структура:** Integer32

Группа(ы)	Объект	Описание
		Идентификатор объекта: 1.3.6.1.4.1.15004.4.6.4.1.1.2.1 **Определение:** Символ, который можно использовать для принудительного перенаправления накопленных данных в сеть. Если символ определения пакета не указан, для объекта устанавливается значение "256", и накопленные данные будут перенаправляться на основе значения параметра времени ожидания обработки пакета – значения, указанного для объекта *rcRawSockPackTimer*.
rcSerialRawSocketGroup	rcRawSockPackSize	**Доступ:** Для чтения и записи **Синтаксическая структура:** Integer32 **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.6.4.1.1.4.1 **Определение:** Максимальное количество байт, полученных от последовательного порта, которые должны быть перенаправлены.
rcSerialRawSocketGroup	rcRawSockPackTimer	**Доступ:** Для чтения и записи **Синтаксическая структура:** Integer32 **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.6.4.1.1.3.1 **Определение:** Задержка с момента получения последнего символа до момента перенаправления данных (в миллисекундах).
rcSerialRawSocketGroup	rcRawSockRemPort	**Доступ:** Для чтения и записи **Синтаксическая структура:** Integer32 **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.6.4.1.1.10.1 **Определение:** Удаленный IP-порт, используемый при установке исходящего соединения.
rcSerialRawSocketGroup	rcRawSockTransport	**Доступ:** Для чтения и записи **Синтаксическая структура:** RcTransport **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.6.4.1.1.6.1 **Определение:** Транспортный протокол, используемый для IP-трафика с использованием протоколов на этом порту.
rcSerialCommandsGroup	rcSerDeviceCmndClearStats	**Доступ:** Для чтения и записи **Синтаксическая структура:** PortList **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.6.16.2.0 **Определение:** Список портов, для которых должна выполняться команда "Очистка статистики" на последовательных устройствах RUGGEDCOM. При попытке чтения этого объекта всегда возвращается пустой список портов.
rcSerialCommandsGroup	rcSerDeviceCmndResetPort	**Доступ:** Для чтения и записи **Синтаксическая структура:** PortList **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.6.16.1.0 **Определение:** Список портов, для которых должна выполняться команда "Сброс" на последовательных устройствах RUGGEDCOM. При попытке чтения этого объекта всегда возвращается пустой список портов.

Группа(ы)	Объект	Описание
rcSerialPortParamsGroup	rcSerialDscp	**Доступ:** Для чтения и записи **Синтаксическая структура:** Integer32 **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.6.1.1.1.9.1 **Определение:** Значение байта DS, которое должно быть указано в заголовке IP. Настройка значения байта DS поддерживается только для исходящего трафика.
rcSerialPortParamsGroup	rcSerialForceHD	**Доступ:** Для чтения и записи **Синтаксическая структура:** Integer **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.6.1.1.1.5.1 **Определение:** Включает принудительное выполнение полудуплексного режима работы на последовательном порту. При отправке данных через последовательный порт все полученные данные игнорируются. Этот режим работы доступен только на портах, которые работают в полнодуплексном режиме.
rcSerialPortParamsGroup	rcSerialHoldTime	**Доступ:** Для чтения и записи **Синтаксическая структура:** Integer32 **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.6.1.1.1.8.1 **Определение:** Максимальное время, в течение которого пакет последовательной передачи может храниться в очереди перед отправкой в канал связи с последовательной передачей (в миллисекундах). Время измеряется с момента получения пакета с IP-уровня.
rcSerialPortParamsGroup	rcSerialPortIfIndex	**Доступ:** Для чтения и записи **Синтаксическая структура:** InerfaceIndex **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.6.1.1.1.2.1 **Определение:** Значение IfIndex для порта. Это значение совпадает со значением "rs232PortIndex", являющимся индексом, используемым для "rs232PortTable" в RS-232-MIB.
rcSerialPortParamsGroup	rcSerialPortType	**Доступ:** Для чтения и записи **Синтаксическая структура:** RcSerPortType **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.6.1.1.1.4.1 **Определение:** Тип последовательного порта, который поддерживается последовательным портом, представленным этой записью.
rcSerialPortParamsGroup	rcSerialPostTxDelay	**Доступ:** Для чтения и записи **Синтаксическая структура:** Integer32 **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.6.1.1.1.7.1 **Определение:** Количество битов, необходимое для генерации требуемой задержки с настроенной скоростью передачи данных ('rs232PortOutSpeed') после отправки последнего бита пакета до того, как последовательный порт UART начинает прослушивать канал связи RX. Это значение актуально только для интерфейса RS485 со значением "rs232PortType" равным other(1).
rcSerialPortParamsGroup	rcSerialProtocol	**Доступ:** Для чтения и записи

Группа(ы)	Объект	Описание
		Синтаксическая структура: RcSerProtocol **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.6.1.1.1.3.1 **Определение:** Последовательный протокол, который поддерживается последовательным портом, представленным этой записью.
rcSerialPortParamsGroup	rcSerialRxtoTxDelay	**Доступ:** Для чтения и записи **Синтаксическая структура:** Integer32 **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.6.1.1.1.10.1 **Определение:** Минимальное время задержки передачи нового сообщения после получения последнего сообщения через порт AI (в миллисекундах). Этот параметр используется для полудуплексного режима передачи, например по двухпроводной линии связи с использованием протокола последовательной передачи RS485. Это обеспечивает достаточное время подключенному устройству для отключения передатчика и включения приемника, чтобы получить следующее сообщение с побитовой точностью.
rcSerialPortParamsGroup	rcSerialTurnAround	**Доступ:** Для чтения и записи **Синтаксическая структура:** Integer32 **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.6.1.1.1.6.1 **Определение:** Величина задержки между передачей отдельных сообщений от последовательного порта. Значение modbusServer(3) для объекта "rcSerialProtocol" должно быть ненулевым. Представляет значение задержки между отправкой широковещательного сообщения и следующим опросом последовательного порта. Поскольку ответ устройств RTU на широковещательные сообщения не предусмотрен, необходимо обеспечить достаточное время для их обработки.
rcSerialTelnetComportGroup	rcTelnetComportCallDir	**Доступ:** Для чтения и записи **Синтаксическая структура:** RcCallDir **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.6.11.1.1.6.1 **Определение:** Определяет следующее: **Примечание** Этот параметр применим только для передачи по TCP. • входящее(0): Принять входящее соединение • исходящее(1): Установить исходящее соединение • оба(2): Установить исходящее соединение и ожидать входящего соединения
rcSerialTelnetComportGroup	rcTelnetComportFlowControl	**Доступ:** Для чтения и записи **Синтаксическая структура:** RcFlowControl **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.6.11.1.1.5.1

Группа(ы)	Объект	Описание
		Определение: Тип FlowControl, который будет использоваться для порта.
rcSerialTelnetComportGroup	rcTelnetComportIpAdd	**Доступ:** Для чтения и записи **Синтаксическая структура:** IpAddress **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.6.11.1.1.9.1 **Определение:** Определяет IpAddress на основе следующего: • Для исходящих TCP-соединений (клиент), rcRawSockCallDir имеет значение "out(2)" и является удаленным IP-адрес для установки соединения. • Для входящего TCP-соединения (сервер) rcRawSockCallDir имеет значение "out (2)" или "both(3)"; это IP-адрес локального интерфейса при прослушивании локального порта для запроса на подключение. • Если разрешены как исходящие, так и входящие соединения (клиент или сервер), rcRawSockCallDir имеет значение "both (3)"; это удаленный IP-адрес для запроса на установку исходящего TCP-соединения или для приема вызовов.
rcSerialTelnetComportGroup	rcTelnetComportLinkStats	**Доступ:** Для чтения и записи **Синтаксическая структура:** EnabledStatus **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.6.11.1.1.10.1 **Определение:** Определяет IpAddress на основе следующего: • Для исходящих TCP-соединений (клиент), rcRawSockCallDir имеет значение "out(2)" и является удаленным IP-адрес для установки соединения. • Для входящего TCP-соединения (сервер) rcRawSockCallDir имеет значение "out (2)" или "both(3)"; это IP-адрес локального интерфейса при прослушивании локального порта для запроса на подключение. • Если разрешены как исходящие, так и входящие соединения (клиент или сервер), rcRawSockCallDir имеет значение "both (3)"; это удаленный IP-адрес для запроса на установку исходящего TCP-соединения или для приема вызовов.
rcSerialTelnetComportGroup	rcTelnetComportLocPort	**Доступ:** Для чтения и записи **Синтаксическая структура:** Integer32 **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.6.11.1.1.7.1 **Определение:** Локальный IP-порт для прослушивания входящего TCP-соединения.
rcSerialTelnetComportGroup	rcTelnetComportPackChar	**Доступ:** Для чтения и записи **Синтаксическая структура:** Integer32 **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.6.11.1.1.2.1

Группа(ы)	Объект	Описание
		Определение: Символ, который можно использовать для принудительного перенаправления накопленных данных в сеть. Если символ определения пакета не указан, для объекта устанавливается значение "256", и накопленные данные будут перенаправляться на основе значения параметра времени ожидания обработки пакета – значения, указанного для объекта *rcTelnetComportPackTimer*.
rcSerialTelnetComportGroup	rcTelnetComportPackSize	**Доступ:** Для чтения и записи **Синтаксическая структура:** Integer32 **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.6.11.1.1.4.1 **Определение:** Максимальное количество байт, полученных от последовательного порта, которые должны быть упакованы в один IP-пакет.
rcSerialTelnetComportGroup	rcTelnetComportPackTimer	**Доступ:** Для чтения и записи **Синтаксическая структура:** Integer32 **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.6.11.1.1.3.1 **Определение:** Задержка с момента получения последнего символа до момента перенаправления данных.
rcSerialTelnetComportGroup	rcTelnetComportRemPort	**Доступ:** Для чтения и записи **Синтаксическая структура:** Integer32 **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.6.11.1.1.8.1 **Определение:** Удаленный TCP-порт, используемый при установке исходящего соединения.
rcTimeConfigBaseGroup	rcTimeAndDate	**Доступ:** Для чтения и записи **Синтаксическая структура:** DateandTime **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.11.1.2.0 **Определение:** Этот параметр позволяет просматривать и настраивать локальное время и дату в формате *DateAndTime*. DateAndTime — стандартное текстовое соглашение, определенное в SNMPv2-TC.

RUGGEDCOM-STP-MIB

Группа(ы)	Объект	Описание
rcRstpBaseGroup	rcRstpDot1dRstpAlternatePorts	**Доступ:** Только для чтения **Синтаксическая структура:** PortList **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.5.1.5.0 **Определение:** Подмножество портов с ролью "Альтернативный".
rcRstpBaseGroup	rcRstpDot1dRstpBackupPorts	**Доступ:** Только для чтения **Синтаксическая структура:** PortList

Группа(ы)	Объект	Описание
		Идентификатор объекта: 1.3.6.1.4.1.15004.4.5.1.6.0 **Определение:** Подмножество портов с ролью "Резервный".
rcRstpBaseGroup	rcRstpDot1dStpBlockedPorts	**Доступ:** Только для чтения **Синтаксическая структура:** PortList **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.5.1.3.0 **Определение:** Подмножество портов с ролью "Заблокированный".
rcRstpBaseGroup	rcRstpDot1dStpBrokenPorts	**Доступ:** Только для чтения **Синтаксическая структура:** PortList **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.5.1.4.0 **Определение:** Подмножество портов в таблице *в dot1dStpPortTable*, которые находятся в состоянии "broken" (объект *dot1dStpPortState* имеет значение "broken").
rcRstpBaseGroup	rcRstpDot1dStpForwardingPorts	**Доступ:** Только для чтения **Синтаксическая структура:** PortList **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.5.1.2.0 **Определение:** Подмножество портов в таблице *в dot1dStpPortTable*, которые находятся в состоянии "forwarding" (объект *dot1dStpPortState* имеет значение "forwarding").
rcRstpBaseStpTxHoldCountGroup	rcRstpDot1dStpTxHoldCount	**Доступ:** Для чтения и записи **Синтаксическая структура:** Integer32 **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.5.1.1.0 **Определение:** Значение, используемое конечным автоматом Port Transmit для ограничения максимальной скорости передачи. Более высокие значения позволяют сети быстрее восстанавливаться после сбоев линий связи/мостов. Значение "0" указывает неограниченную скорость передачи. Если значение объекта *dot1dStpTxHoldCount* находится в диапазоне 3–10, то оно должно соответствовать значению объекта *dot1dStpTxHoldCount* (RSTP-MIB). Если значение объекта *dot1dStpTxHoldCount* равно 10, то значение этого объекта представляет фактический настроенный предел скорости передачи.

RUGGEDCOM-SYS-INFO-MIB

Группа(ы)	Объект	Описание
rcSysDeviceCommGroup	rcDeviceCommClearAlarms	**Доступ:** Для чтения и записи **Синтаксическая структура:** TruthValue **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.2.4.3.0 **Определение:** Установка для этого объекта значения "true(1)" приведет к сбросу всех оповещений для устройства. После выполнения запроса на чтение агент возвращает значение "false (2)".
rcSysDeviceCommGroup	rcDeviceCommClearLogs	**Доступ:** Для чтения и записи **Синтаксическая структура:** TruthValue **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.2.4.5.0 **Определение:** Установка для этого объекта значения "true(1)" приведет к очистке файлов syslog.txt и crashlog.txt для устройства. После выполнения запроса на чтение агент возвращает значение "false (2)".
rcSysDeviceCommGroup	rcDeviceCommClearSyslog	**Доступ:** Для чтения и записи **Синтаксическая структура:** TruthValue **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.2.4.4.0 **Определение:** Установка для этого объекта значения "true(1)" приведет к очистке файла syslog.txt для устройства. После выполнения запроса на чтение агент возвращает значение "false (2)".
rcSysDeviceCommGroup	rcDeviceCommLoadDefaultCfg	**Доступ:** Для чтения и записи **Синтаксическая структура:** TruthValue **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.2.4.2.0 **Определение:** Установка для этого объекта значения "true(1)" приведет принудительной загрузке конфигурации по умолчанию во все таблицы для устройства. После выполнения запроса на чтение агент возвращает значение "false (2)".
rcSysDeviceCommGroup	rcDeviceCommReset	**Доступ:** Для чтения и записи **Синтаксическая структура:** TruthValue **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.2.4.1.0 **Определение:** Установка для этого объекта значения "true(1)" приведет к перезагрузке устройства. После выполнения запроса на чтение агент возвращает значение "false (2)".
rcSysErrObjectsGroup	rcDeviceErrBootPTftpTrFailed	**Доступ:** Только для чтения **Синтаксическая структура:** TruthValue

Группа(ы)	Объект	Описание
		Идентификатор объекта: 1.3.6.1.4.1.15004.4.2.1.9.0 **Определение:** Указывает, был ли файл передан правильно после получения IP-адреса с сервера BootP. При каждом изменении значения этого объекта с false(2) на true(1) устройство генерирует уведомление genericTrap.
rcSysErrObjectsGroup	rcDeviceErrBootupError	**Доступ:** Только для чтения **Синтаксическая структура:** DisplayString **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.2.1.1.0 **Определение:** Обнаружена ошибка в процессе загрузки. Если ошибки в процессе загрузки отсутствуют, возвращается объект DisplayString нулевой длины.
rcSysErrObjectsGroup	rcDeviceErrConfigurationFailure	**Доступ:** Только для чтения **Синтаксическая структура:** TruthValue **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.2.1.3.0 **Определение:** Указывает, были ли обнаружены ошибки при применении параметров конфигурации из файла конфигурации. Конфигурация обновляется из файла конфигурации в процессе загрузки, когда файл загружается из энергонезависимой памяти или когда новый файл загружается на устройство. При каждом изменении значения этого объекта с false (2) на true(1) устройство генерирует уведомление genericTrap.
rcSysErrObjectsGroup	rcDeviceErrCrashLogCreated	**Доступ:** Только для чтения **Синтаксическая структура:** TruthValue **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.2.1.4.0 **Определение:** Указывает, была ли обнаружена ошибка устройства, вызвавшая создание записи в файле crashlog.txt. При каждом изменении значения этого объекта с false (2) на true(1) устройство генерирует уведомление genericTrap.
rcSysErrObjectsGroup	rcDeviceErrDateAndTimeSetFailed	**Доступ:** Только для чтения **Синтаксическая структура:** TruthValue **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.2.1.7.0 **Определение:** Указывает на ошибки настройки даты и времени для устройства. При каждом изменении значения этого объекта с false (2) на true(1) устройство генерирует уведомление genericTrap.
rcSysErrObjectsGroup	rcDeviceErrHeapError	**Доступ:** Только для чтения

Группа(ы)	Объект	Описание
		Синтаксическая структура: TruthValue **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.2.1.6.0 **Определение:** Указывает, обнаружено ли повреждение системной памяти. При каждом изменении значения этого объекта с false (2) на true(1) устройство генерирует уведомление genericTrap.
rcSysErrObjectsGroup	rcDeviceErrNtpServerUnreachable	**Доступ:** Только для чтения **Синтаксическая структура:** TruthValue **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.2.1.8.0 **Определение:** Указывает, можно ли получить доступ к какому-либо из серверов NTP (если требуется). Этот объект будет иметь значение "false", если оба сервера недоступны. При изменении значения этого объекта устройство генерирует уведомление *ntpServiceAvailableChange*.
rcSysErrObjectsGroup	rcDeviceErrRadiusServerUnreachable	**Доступ:** Только для чтения **Синтаксическая структура:** TruthValue **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.2.1.10.0 **Определение:** Указывает, можно ли получить доступ к серверу RADIUS (если требуется). При изменении значения этого объекта устройство генерирует уведомление *radiusServiceAvailableChange*.
rcSysErrObjectsGroup	rcDeviceErrStackOverflow	**Доступ:** Только для чтения **Синтаксическая структура:** TruthValue **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.2.1.5.0 **Определение:** Указывает, превышает ли объем стека для выполнения какой-либо из системных задач системное пороговое значение. При каждом изменении значения этого объекта с false (2) на true(1) устройство генерирует уведомление *genericTrap*.
rcSysErrObjectsGroup	rcDeviceErrTacacsServerUnreachable	**Доступ:** Только для чтения **Синтаксическая структура:** TruthValue **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.2.1.11.0 **Определение:** Указывает, можно ли получить доступ к серверу TACACS+ (если требуется). При изменении значения этого объекта устройство генерирует уведомление *tacacsServiceAvailableChange*.
rcSysErrObjectsGroup	rcDeviceErrWatchdogReset	**Доступ:** Только для чтения **Синтаксическая структура:** TruthValue

Группа(ы)	Объект	Описание
		Идентификатор объекта: 1.3.6.1.4.1.15004.4.2.1.2.0 **Определение:** Указывает, была ли последняя перезагрузка устройства вызвана схемой обеспечения безопасности.
rcSysInfoDeviceInfoGroup	rcDeviceInfoBootSwVersion	**Доступ:** Только для чтения **Синтаксическая структура:** DisplayString **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.2.3.2.0 **Определение:** Версия и дата сборки программного обеспечения загрузчика операционной системы.
rcSysInfoDeviceInfoGroup	rcDeviceInfoCfgRevision	**Доступ:** Только для чтения **Синтаксическая структура:** Integer32 **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.2.3.8.0 **Определение:** Версия файла конфигурации. Номер редакции будет обновляться при каждом сохранении файла во флеш-память. Этот номер записывается в файл config.csv при загрузке файла с устройства. При изменении значения этого объекта устройство генерирует уведомление *cfgChangeTrap*.
rcSysInfoDeviceInfoGroup	rcDeviceInfoMainBoardType	**Доступ:** Только для чтения **Синтаксическая структура:** RcMainBoard **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.2.3.4.0 **Определение:** Идентификационный код главной платы устройства.
rcSysInfoDeviceInfoGroup	rcDeviceInfoMainSwVersion	**Доступ:** Только для чтения **Синтаксическая структура:** DisplayString **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.2.3.3.0 **Определение:** Версия и дата сборки основного программного обеспечения операционной системы.
rcSysInfoDeviceInfoGroup	rcDeviceInfoPendingBootSwVersion	**Доступ:** Только для чтения **Синтаксическая структура:** DisplayString **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.2.3.6.0 **Определение:** Версия и дата сборки программного обеспечения загрузчика операционной системы, загруженного на устройство и ожидающего перезагрузки. При каждом изменении значения этого объекта с DisplayString нулевой длины на DisplayString ненулевой длины устройство генерирует уведомление *swUpgradeTrap*.
rcSysInfoDeviceInfoGroup	rcDeviceInfoPendingMainSwVersion	**Доступ:** Только для чтения

Группа(ы)	Объект	Описание
		Синтаксическая структура: DisplayString **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.2.3.7.0 **Определение:** Версия и дата сборки основного программного обеспечения операционной системы, загруженного на устройство и ожидающего перезагрузки. При каждом изменении значения этого объекта с DisplayString нулевой длины на DisplayString ненулевой длины устройство генерирует уведомление *swUpgradeTrap*.
rcSysInfoDeviceInfoGroup	rcDeviceInfoSerialNumber	**Доступ:** Только для чтения **Синтаксическая структура:** DisplayString **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.2.3.1.0 **Определение:** Серийный номер производителя для устройства.
rcSysInfoDeviceInfoGroup	rcDeviceInfoTotalRam	**Доступ:** Только для чтения **Синтаксическая структура:** Integer32 **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.2.3.5.0 **Определение:** Общее количество байт ОЗУ для ЦП управления системой.
rcSysStsPowerSupplyGroup	rcDeviceStsPowerSupply1	**Доступ:** Только для чтения **Синтаксическая структура:** RcHardwareStatus **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.2.2.4.0 **Определение:** Указывает статус модуля питания 1. При каждом изменении значения этого объекта с functional(2) на notFunctional(3) или с notFunctionl(3) на functional(2) устройство генерирует уведомление *powerSupplyTrap*.
rcSysStsPowerSupplyGroup	rcDeviceStsPowerSupply2	**Доступ:** Только для чтения **Синтаксическая структура:** RcHardwareStatus **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.2.2.5.0 **Определение:** Указывает статус модуля питания 2. При каждом изменении значения этого объекта с functional(2) на notFunctional(3) или с notFunctionl(3) на functional(2) устройство генерирует уведомление *powerSupplyTrap*.
rcSysStsObjectsTemperatureGroup	rcDeviceStsTemperature	**Доступ:** Только для чтения **Синтаксическая структура:** Integer32 **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.2.2.3.0

Группа(ы)	Объект	Описание
		Определение: Измеренная температура устройства.

RUGGEDCOM-TIMECONFIG-MIB

Группа(ы)	Объект	Описание
rcTimeConfigBaseGroup	rcCurrentUTCOfst	**Доступ:** Для чтения и записи **Синтаксическая структура:** Unsigned32 **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.11.1.4.0 **Определение:** Позволяет пользователю настраивать разницу между UTC и TAI.
rcTimeConfigBaseGroup	rcDSTOfst	**Доступ:** Для чтения и записи **Синтаксическая структура:** Unsigned32 **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.11.1.3.0 **Определение:** Этот параметр определяет время, на которое необходимо выполнить сдвиг вперед/назад при переходе на летнее время и обратно. Например, для большинства регионов США и Канады при переходе на летнее время выполняется сдвиг на 1 час (01:00:00) вперед, когда начинается действие летнего времени, или на 1 час назад, когда действие летнего времени заканчивается.
rcTimeConfigBaseGroup	rcDSTRule	**Доступ:** Для чтения и записи **Синтаксическая структура:** DisplayString **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.11.1.6.0 **Определение:** Этот параметр определяет правило для времени и даты при переходе со стандартного на летнее время. Формат: mm.n.d/HH:MM:SS mm.n.d/HH:MM:SS • mm — месяц года (01 — январь, 12 — декабрь) • n — n-й день месяца (1 — 1-й день, 5 — 5-й/последний день) • d — день недели (0 — воскресенье, 6 — суббота) • HH — час дня (0–24) • MM — минута часа (0–59) • SS — секунда минуты (0–59) Пример: В большинстве регионов США и Канады действует следующее правило: 03.2.0/02:00:00 11.1.0/02:00:00 Действие летнего времени начинается во второе воскресенье марта в 2:00. Действие летнего времени заканчивается в первое воскресенье ноября в 2:00.
rcTimeConfigBaseGroup	rcLeapSecPending	**Доступ:** Для чтения и записи **Синтаксическая структура:** TruthValue **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.11.1.5.0

Группа(ы)	Объект	Описание
		Определение: Этот параметр позволяет пользователям управлять событием секунд координации. Секунда координации представляет собой одну секунду, которая прибавляется к всемирному координированному времени (UTC).
rcTimeConfigBaseGroup	rcTimeSource	**Доступ:** Для чтения и записи **Синтаксическая структура:** Integer **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.11.1.1.0 **Определение:** Источник времени, который управляет локальными часами.
rcSerialTinAndWinGroup	rcTinAndWinAddrAgingTime	**Доступ:** Для чтения и записи **Синтаксическая структура:** Integer32 **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.6.6.7.0 **Определение:** Время бездействия связи, по истечении которого полученный при обучении TIN-адрес удаляется из таблицы динамических адресов устройств (в миллисекундах). Записи в таблице "Статистика по ссылкам" с устаревшими адресами будут храниться до момента очистки статистики.
rcSerialTinAndWinGroup	rcTinAndWinBroadCastAddr	**Доступ:** Для чтения и записи **Синтаксическая структура:** Integer **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.6.6.8.0 **Определение:** Таблица адресов устройств для поиска адресов для широковещательных сообщений.
rcSerialTinAndWinGroup	rcTinAndWinLinkStats	**Доступ:** Для чтения и записи **Синтаксическая структура:** EnabledStatus **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.6.6.10.0 **Определение:** Включение сбора статистики по ссылкам для протоколов TIN и WIN.
rcSerialTinAndWinGroup	rcTinAndWinMsgAgingTime	**Доступ:** Для чтения и записи **Синтаксическая структура:** Integer32 **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.6.6.6.0 **Определение:** Время устаревания для сообщений TIN mode2. При установке для этого объекта значения "0" эта функция будет отключена. Если эта функция включена, то все принимаемые сообщения TIN mode2 будут сохраняться во внутренней таблице. Если это же сообщение принимается в пределах интервала времени, заданного этим параметром, то новое сообщение рассматривается как дублирующее и, таким образом, отбрасывается.
rcSerialTinAndWinGroup	rcTinAndWinTinDscp	**Доступ:** Для чтения и записи **Синтаксическая структура:** Integer32 **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.6.6.12.0 **Определение:** Значение байта DS, которое должно быть указано в заголовке IP. Настройка значения байта DS поддерживается только для исходящего трафика.
rcSerialTinAndWinGroup	rcTinAndWinTinIpPort	**Доступ:** Для чтения и записи

Группа(ы)	Объект	Описание
		Синтаксическая структура: Integer32 **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.6.6.4.0 **Определение:** Номер локального порта, на котором прослушиваются соединения или датаграммы UDP с использованием протокола TIN.
rcSerialTinAndWinGroup	rcTinAndWinTinMode	**Доступ:** Для чтения и записи **Синтаксическая структура:** Integer **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.6.6.1.0 **Определение:** Режим работы протокола TIN.
rcSerialTinAndWinGroup	rcTinAndWinTinTrans	**Доступ:** Для чтения и записи **Синтаксическая структура:** RcTransport **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.6.6.2.0 **Определение:** Транспортный протокол, используемый для IP-трафика с использованием протокола TIN.
rcSerialTinAndWinGroup	rcTinAndWinUniAddr	**Доступ:** Для чтения и записи **Синтаксическая структура:** Integer **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.6.6.9.0 **Определение:** Таблица адресов устройств для поиска адресов для одноадресных сообщений.
rcSerialTinAndWinGroup	rcTinAndWinWinDscp	**Доступ:** Для чтения и записи **Синтаксическая структура:** Integer32 **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.6.6.11.0 **Определение:** Значение байта DS, которое должно быть указано в заголовке IP. Настройка значения байта DS поддерживается только для исходящего трафика.
rcSerialTinAndWinGroup	rcTinAndWinWinIpPort	**Доступ:** Для чтения и записи **Синтаксическая структура:** Integer32 **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.6.6.5.0 **Определение:** Номер локального порта, на котором прослушиваются соединения или датаграммы UDP с использованием протокола WIN.
rcSerialTinAndWinGroup	rcTinAndWinWinTrans	**Доступ:** Для чтения и записи **Синтаксическая структура:** RcTransport **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.6.6.3.0 **Определение:** Транспортный протокол, используемый для IP-трафика с использованием протокола WIN.

12.3.1.3 Поддерживаемые возможности агента

RUGGEDCOM ROS поддерживает следующие возможности агента SNMP:

⚠ ЗАМЕТКА

В этом разделе перечислены все базы MIB, поддерживаемые RUGGEDCOM ROS, и он приводится исключительно в качестве справочной информации. Поддержка отдельных устройств может отличаться.

Примечание

Для получения информации о возможностях агента SNMPv2 см. RFC 2580 [http://tools.ietf.org/html/rfc2580].

Имя файла	Возможности агента	Поддерживаемая база MIB
RC-SNMPv2-MIB-AC.mib	RC-SNMPv2-MIB-AC	SNMPv2-MIB
RC-UDP-MIB-AC.mib	RC-UDP-MIB-AC	UDP-MIB
RC-TCP-MIB-AC.mib	RC-TCP-MIB-AC	TCP-MIB
RC-SNMP-USER-BASED-SM-MIB-AC.mib	RC-SNMP-USER-BASED-SM-MIB-AC	SNMP-USER-BASED-SM-MIB-AC
RC-SNMP-VIEW-BASED-ACM-MIB-AC.mib	RC-SNMP-VIEW-BASED-ACM-MIB-AC	SNMP-VIEW-BASED-ACM-MIB-AC
RC-IF-MIB-AC.mib	RC-IF-MIB-AC	IF-MIB
RC-BRIDGE-MIB-AC.mib	RC-BRIDGE-MIB-AC	BRIDGE-MIB
RC-RMON-MIB-AC.mib	RC-RMON-MIB-AC	RMON-MIB
RC-Q-BRIDGE-MIB-AC.mib	RC-Q-BRIDGE-MIB-AC	Q-BRIDGE-MIB
RC-IP-MIB-AC.mib	RC-IP-MIB-AC	IP-MIB
RC-LLDP-MIB-AC.mib	RC-LLDP-MIB-AC	LLDP-MIB
RC-LAG-MIB-AC.mib	RC-LAG-MIB-AC	IEEE8023-LAG-MIB
RC_RSTP-MIB-AC.mib	RC_RSTP-MIB-AC	RSTP-MIB
RC-RUGGEDCOM-DOT11-MIB-AC.mib	RC-RUGGEDCOM-DOT11-MIB-AC	RUGGEDCOM-DOT11- MIB
RC-RUGGEDCOM-POE-MIB-AC.mib	RC-RUGGEDCOM-POE-MIB-AC	RUGGEDCOM-POE-MIB
RC-RUGGEDCOM-STP-AC-MIB.mib	RC-RUGGEDCOM-STP-AC-MIB	RUGGEDCOM-STP-MIB
RC-RUGGEDCOM-SYS-INFO-MIB-AC.mib	RC-RUGGEDCOM-SYS-INFO-MIB-AC	RUGGEDCOM-SYS-INFO-MIB
RC-RUGGEDCOM-TRAPS-MIB-AC.mib	RC-RUGGEDCOM-TRAPS-MIB-AC	RUGGEDCOM-TRAPS-MIB
RUGGEDCOM_RS-232-MIB-AC.mib	RUGGEDCOM_RS-232-MIB-AC	RS-232-MIB
RC-RUGGEDCOM-SERIAL-MIB-AC.mib	RC-RUGGEDCOM-SERIAL-MIB-AC	RUGGEDCOM-SERIAL-MIB
RC-GPS-MIB-AC.mib	RC-GPS-MIB-AC	GPS-MIB
RC-IRIGB-MIB-AC.mib	RC-IRIGB-MIB-AC	IRIGB-MIB
RC-NTP-MIB-AC.mib	RC-NTP-MIB-AC	NTP-MIB
RC-PTP1588-MIB-AC.mib	RC-PTP1588-MIB-AC	PTP1588-MIB
RC-TIMECONFIG-MIB-AC.mib	RC-TIMECONFIG-MIB-AC	TIMECONFIG-MIB
RC-SNMP-FRAMEWORK-MIB-AC.MIB	RC-SNMP-FRAMEWORK-MIB-AC	SNMP-FRAMEWORK-MIB.MIB
RC-RUGGEDCOM-AAA-SERVER-MIB-AC.MIB	RC-RUGGEDCOM-AAA-SERVER-MIB-AC	RUGGEDCOM-AAA-SERVER-MIB.MIB

12.3.2 Trap-уведомления SNMP

Устройство генерирует следующие trap-уведомления:

Стандартные trap-уведомления

Переменная	Описание
coldStart	**Группа объектов:** snmpBasicNotificationsGroup **MIB:** SNMPv2-MIB **Доступ:** только для чтения **Идентификатор объекта:** 1.3.6.1.6.3.1.1.5.1.0 **Стандарт:** RFC-1907 **Определение:** Trap-уведомление coldStart означает, что объект SNMPv2, действующий в роли агента, повторно инициализируется и что его конфигурация могла быть изменена.
ieeeC37238EventChangeOfMaster	**Группа объектов:** ieeeC37238EventsPropertiesGroup **MIB:** IEEEC37-238-MIB **Доступ:** только для чтения **Идентификатор объекта:** 1.3.111.3.37.238.9999.0.0.1.0 **Стандарт:** PC37.238/D5.5 **Определение:** Указывает, что выбраны новые гроссмейстерские часы.
ieeeC37238EventMasterStepChange	**Группа объектов:** ieeeC37238EventsPropertiesGroup **MIB:** IEEEC37-238-MIB **Доступ:** только для чтения **Идентификатор объекта:** 1.3.111.3.37.238.9999.0.0.2.0 **Стандарт:** Указывает на изменение шага для текущего времени гроссмейстерских часов. **Определение:** PC37.238/D5.5
ieeeC37238EventOfstExceedsLimit	**Группа объектов:** ieeeC37238EventsPropertiesGroup **MIB:** IEEEC37-238-MIB **Доступ:** только для чтения **Идентификатор объекта:** 1.3.111.3.37.238.9999.0.0.5.0 **Стандарт:** PC37.238/D5.5 **Определение:** Указывает, что для часов, находящихся в ведомом состоянии, смещение от ведущего устройства превышает настраиваемый предел.
ieeeC37238EventPTPServiceStarted	**Группа объектов:** ieeeC37238EventsPropertiesGroup **MIB:** IEEEC37-238-MIB **Доступ:** только для чтения **Идентификатор объекта:** 1.3.111.3.37.238.9999.0.0.8.0 **Стандарт:** PC37.238/D5.5 **Определение:** Указывает, что служба PTP запущена.
ieeeC37238EventPTPServiceStopped	**Группа объектов:** ieeeC37238EventsPropertiesGroup

Переменная	Описание
	MIB: IEEEC37-238-MIB **Доступ:** только для чтения **Идентификатор объекта:** 1.3.111.3.37.238.9999.0.0.9.0 **Стандарт:** PC37.238/D5.5 **Определение:** Указывает, что служба PTP запущена.
linkDown	**Группа объектов:** linkUpDownNotificationsGroup **MIB:** IF-MIB **Доступ:** только для чтения **Синтаксическая структура:** Counter32 **Идентификатор объекта:** .1.3.6.1.6.3.1.1.5.3 **Стандарт:** RFC-2863 **Определение:** Trap-уведомление linkDown означает, что объектом SNMP, действующим в роли агента, обнаружена готовность перехода объекта ifOperStatus для одного из каналов связи в состояние down из другого состояния (кроме состояния notPresent). Это другое состояние обозначается включенным значением ifOperStatus.
linkUp	**Группа объектов:** linkUpDownNotificationsGroup **MIB:** IF-MIB **Функционал агента:** RC-IF-MIB-AC **Доступ:** только для чтения **Идентификатор объекта:** .1.3.6.1.6.3.1.1.5.4 **Определение:** Trap-уведомление linkDown означает, что объектом SNMP, действующим в роли агента, обнаружен переход объекта ifOperStatus для одного из каналов связи из состояния down в другое состояние (кроме состояния notPresent). Это другое состояние обозначается включенным значением ifOperStatus.
lldpRemTablesChange	**Группа объектов:** lldpNotificationsGroup **MIB:** LLDP-MIB **Функционал агента:** RC-LLDP-MIB-AC **Доступ:** только для чтения **Синтаксическая структура:** STRING **Идентификатор объекта:** 1.0.8802.1.1.2.0.0.1.0 **Стандарт:** ISO8802-LLDP-MIB **Определение:** Уведомление lldpRemTablesChange отправляется при изменении значения lldpStatsRemTableLastChangeTime. Оно может быть использовано NMS для запуска опросов технического обслуживания таблицы удаленных систем LLDP. Обратите внимание, что передача уведомлений lldpRemTablesChange ограничивается агентом, как указано объектом lldpNotificationInterval.
lldpStatsRemTablesAgeouts	**Группа объектов:** lldpStatsRxGroup **MIB:** LLDP-MIB **Функционал агента:** RC-LLDP-MIB-AC **Доступ:** только для чтения

Переменная	Описание
	Синтаксическая структура: Gauge32 **Идентификатор объекта:** .1.0.8802.1.1.2.1.2.5.0 **Стандарт:** ISO8802-LLDP-MIB **Определение:** Количество раз, когда набор информации, объявленный определенным MSAP, полностью удалялся из таблиц, содержащихся в объектах lldpRemoteSystemsData и lldpExtensions, поскольку интервал актуальности информации истек. Этот счетчик следует увеличивать только один раз, когда весь набор информации полностью недействителен (устарел) для всех связанных таблиц. Частичное устаревание (аналогично случаю удаления) не допускается и, таким образом, не должно изменять значение этого счетчика.
lldpStatsRemTablesDeletes	**Группа объектов:** lldpStatsRxGroup **MIB:** LLDP-MIB **Функционал агента:** RC-LLDP-MIB-AC **Доступ:** только для чтения **Синтаксическая структура:** Gauge32 **Идентификатор объекта:** .1.0.8802.1.1.2.1.2.3.0 **Стандарт:** ISO8802-LLDP-MIB **Определение:** Обратите внимание, что передача уведомлений lldpRemTablesChange ограничивается агентом, как указано объектом lldpNotificationInterval.
lldpStatsRemTablesDrops	**Группа объектов:** lldpStatsRxGroup **MIB:** LLDP-MIB **Функционал агента:** RC-LLDP-MIB-AC **Доступ:** только для чтения **Синтаксическая структура:** Gauge32 **Идентификатор объекта:** .1.0.8802.1.1.2.1.2.4.0 **Стандарт:** Количество раз, когда набор информации, объявленный определенным MSAP, не может быть полностью введен в таблицы, содержащиеся в объектах lldpRemoteSystemsData и lldpExtensions из-за нехватки ресурсов. **Определение:** ISO8802-LLDP-MIB
lldpStatsRemTablesInserts	**Группа объектов:** lldpStatsRxGroup **MIB:** LLDP-MIB **Функционал агента:** RC-LLDP-MIB-AC **Доступ:** только для чтения **Синтаксическая структура:** Gauge32 **Идентификатор объекта:** .1.0.8802.1.1.2.1.2.2.0 **Стандарт:** ISO8802-LLDP-MIB **Определение:** Количество раз, когда набор информации, объявленный определенным MSAP, полностью был вставлен в таблицы, содержащиеся в объектах lldpRemoteSystemsData и lldpExtensions. Полный набор информации, полученной из конкретного MSAP,

Переменная	Описание
	должен быть вставлен в соответствующие таблицы. Если часть информации не может быть вставлена по причине нехватки ресурсов, то весь набор информации должен быть удален. Этот счетчик следует увеличивать только один раз, когда весь набор информации будет успешно записан во все соответствующие таблицы. Любые сбои во время вставки набора информации, которые приводят к удалению ранее вставленной информации, не должны вызывать никаких изменений в lldpStatsRemTablesInserts, поскольку вставка еще не завершена, или в lldpStatsRemTablesDeletes, поскольку удаление будет только частичным. Если сбой произошел из-за нехватки ресурсов, счетчик lldpStatsRemTablesDrops следует увеличить однократно.
RMON_alarmIndex	**Доступ:** только для чтения **Синтаксическая структура:** 1.3.6.1.2.1.16.3.1.1.1.0 **Идентификатор объекта:** 1.3.6.1.2.1.16.3.1.1.1.0 **Стандарт:** RFC-2819
RMON_alarmSampleType	**Доступ:** только для чтения **Синтаксическая структура:** 1.3.6.1.2.1.16.3.1.1.4.0 **Идентификатор объекта:** 1.3.6.1.2.1.16.3.1.1.4.0 **Стандарт:** RFC-2819
RMON_alarmThreshold	**Доступ:** только для чтения **Синтаксическая структура:** 1.3.6.1.2.1.16.3.1.1.0.0 **Идентификатор объекта:** 1.3.6.1.2.1.16.3.1.1.0.0 **Стандарт:** RFC-2819
RMON_alarmValue	**Доступ:** только для чтения **Синтаксическая структура:** 1.3.6.1.2.1.16.3.1.1.5.0 **Идентификатор объекта:** 1.3.6.1.2.1.16.3.1.1.5.0 **Стандарт:** RFC-2819
RMON_alarmVariable	**Доступ:** только для чтения **Синтаксическая структура:** 1.3.6.1.2.1.16.3.1.1.3.0 **Идентификатор объекта:** 1.3.6.1.2.1.16.3.1.1.3.0 **Стандарт:** RFC-2819
RMON_fallingAlarm	**Доступ:** только для чтения **Синтаксическая структура:** 1.3.6.1.2.1.16.0.2.0 **Идентификатор объекта:** 1.3.6.1.2.1.16.0.2.0 **Стандарт:** RFC-2819
RMON_risingAlarm	**Доступ:** только для чтения **Синтаксическая структура:** 1.3.6.1.2.1.16.0.1.0 **Идентификатор объекта:** 1.3.6.1.2.1.16.0.1.0 **Стандарт:** RFC-2819
RstpNewRoot	**Доступ:** только для чтения **Синтаксическая структура:** 1.3.6.1.2.1.17.0.1.0 **Идентификатор объекта:** 1.3.6.1.2.1.17.0.1.0

Переменная	Описание
	Стандарт: RFC-4188
RstpTopolgyChange	**Доступ:** только для чтения **Синтаксическая структура:** 1.3.6.1.2.1.17.0.2.0 **Идентификатор объекта:** 1.3.6.1.2.1.17.0.2.0 **Стандарт:** RFC-4188
SnmpAuthenticationFailure	**Доступ:** только для чтения **Синтаксическая структура:** 1.3.6.1.6.3.1.1.5.5.0 **Идентификатор объекта:** 1.3.6.1.6.3.1.1.5.5.0 **Стандарт:** RFC-1907
snmpEnableAuthenTraps	**Группа объектов:** snmpGroup **MIB:** SNMPv2-MIB **Доступ:** для чтения и записи **Синтаксическая структура:** INTEGER **Идентификатор объекта:** 1.3.6.1.2.1.11.30.0 **Определение:** Указывает на наличие разрешения для объекта SNMP генерировать trap-уведомления authenticationFailure. Значение этого объекта переопределяет любую конфигурационную информацию; таким образом, он предоставляет средство для отключения всех trap-уведомлений authenticationFailure. Обратите внимание, что настоятельно рекомендуется хранить этот объект в энергонезависимой памяти, чтобы предотвратить его изменения при повторной инициализации системы управления сетью.
warmStart	**Группа объектов:** ROS-Standard-Trap **MIB:** SNMPv2-MIB **Доступ:** только для чтения **Синтаксическая структура:** 1.3.6.1.6.3.1.1.5.2.0 **Идентификатор объекта:** 1.3.6.1.6.3.1.1.5.2.0 **Определение:** Trap-уведомление warmStart означает, что объект SNMPv2, действующий в роли агента, повторно инициализируется без изменения конфигурации.

Особые проприетарные trap-уведомления

Переменная	Описание
bootVersionMismatchTrap	**Группа объектов:** ruggedcomSecurityGroup01 **MIB:** RUGGEDCOM-TRAPS-MIB **Идентификатор объекта:** 1.3.6.1.4.1.15004.5.14 **Определение:** Trap-уведомление индикации версии загрузочного программного обеспечения, генерируемое устройствами RUGGEDCOM.
cfgChangeTrap	**Группа объектов:** ruggedcomNotificationsGroup **MIB:** RUGGEDCOM-TRAPS-MIB **Идентификатор объекта:** 1.3.6.1.4.1.15004.5.4

Переменная	Описание
	Определение: Общее trap-уведомление, генерируемое при изменении конфигурации. Скорость выдачи этого уведомления составляет 60 секунд.
defaultKeysTrap	**Группа объектов:** ruggedcomSecurityGroup01 **MIB:** RUGGEDCOM-TRAPS-MIB **Идентификатор объекта:** 1.3.6.1.4.1.15004.5.13 **Определение:** Использование ключей по умолчанию для trap-уведомления индикации защищенных протоколов (SSH и SSL), генерируемое устройствами RUGGEDCOM.
genericTrap	**Группа объектов:** ruggedcomNotificationsGroup **MIB:** RUGGEDCOM-TRAPS-MIB **Идентификатор объекта:** 1.3.6.1.4.1.15004.5.1 **Определение:** Использование ключей по умолчанию для trap-уведомления индикации защищенных протоколов (SSH и SSL), генерируемое устройствами RUGGEDCOM.
genericTrapDescription	**Группа объектов:** ruggedcomGenericTrapGroup **MIB:** RUGGEDCOM-TRAPS-MIB **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.1.1.1.2 **Определение:** Описание общего trap-уведомления.
genericTrapSeverity	**Группа объектов:** ruggedcomGenericTrapGroup **MIB:** RUGGEDCOM-TRAPS-MIB **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.1.1.1.1 **Определение:** Уровень серьезности общего trap-уведомления:
powerSupplyDescription	**Группа объектов:** ruggedcomPowerSupplyGroup **MIB:** RUGGEDCOM-TRAPS-MIB **Идентификатор объекта:** 1.3.6.1.4.1.15004.4.1.1.2.1 **Определение:** Описание неисправного источника питания.
powerSupplyTrap	**Группа объектов:** ruggedcomNotificationsGroup **MIB:** RUGGEDCOM-TRAPS-MIB **Идентификатор объекта:** 1.3.6.1.4.1.15004.5.2 **Определение:** Trap-уведомление, генерируемое при выходе из строя источника питания. Первое trap-уведомление генерируется при первом выходе из строя источника питания. Состояние источника питания (сбой или восстановление) извлекается с помощью объекта powerSupplyDescription в момент генерирования trap-уведомления. Сведения о состоянии источника питания устройства можно получить с помощью объектов rcDeviceStsPowerSupply1 и rcDeviceStsPowerSupply2, объект powerSupplyIdentifier рекомендуется добавить в качестве дополнительного параметра в список объектов.
rcRstpNewTopology	**Группы объектов:** rcRstpNotifyGroup, rcDigitalInputsNotifyGroup **MIB:** RUGGEDCOM-STP-MIB **Идентификатор объекта:** 1.3.6.1.4.1.15004.5.11.1

Переменная	Описание
	Определение: Trap-уведомление rcRstpNewTopology отправляется мостом после возникновения trap-уведомления об изменении топологии на одном или нескольких портах (отправляются trap-уведомления topologyChange) и стабилизации топологии. Топология стабильна, если значение таймера tcWhile для всех портов на этом мосту равно нулю. Это trap-уведомление отключено, если trap-уведомление topologyChange trap отключено в конфигурации устройства.
swUpgradeTrap	**Группа объектов:** ruggedcomNotificationsGroup **MIB:** RUGGEDCOM-SYS-INFO-MIB **Идентификатор объекта:** 1.3.6.1.4.1.15004.5.3 **Определение:** Общее trap-уведомление, генерируемое при обновлении программного обеспечения. Скорость выдачи этого уведомления составляет 60 секунд.
weakPasswordTrap	**Группа объектов:** ruggedcomSecurityGroup01 **MIB:** RUGGEDCOM-SYS-INFO-MIB **Идентификатор объекта:** 1.3.6.1.4.1.15004.5.8 **Определение:** Trap-уведомление индикации ненадежного пароля, генерируемое устройствами RUGGEDCOM.

12.3.3 Управление пользователями SNMP

В данном разделе рассматривается управление пользователями SNMP.

12.3.3.1 Просмотр списка пользователей SNMP

Чтобы просмотреть список пользователей SNMP, сконфигурированных на устройстве, перейдите в ***Administration » Configure SNMP » Configure SNMP Users***. Появится таблица **SNMP Users**.

Если пользователи не были сконфигурированы, добавьте необходимых пользователей. Для получения дополнительной информации см. "Добавление пользователя SNMP (Страница 438)".

12.3.3.2 Добавление пользователя SNMP

Для локального ядра SNMPv3 и для сообществ SNMPv1 и SNMPv2c можно сконфигурировать несколько пользователей (до 32).

Примечание
Обратите внимание, что при использовании уровня безопасности SNMPv1 или SNMPv2c параметр **User Name** связывает имя строки-ключа с группой безопасности и уровнем доступа.

CLI-команды, относящиеся к добавлению пользователя SNMP, см в "Доступные CLI-команды (Страница 27)".

Чтобы добавить нового пользователя SNMP, сделайте следующее:

1. Перейдите в ***Administration » Configure SNMP » Configure SNMP Users***. Появится **SNMP Users Table**.
2. Нажмите **InsertRecord**. Появится форма **SNMP Users**.

Примечание
Все пароли пользователей в RUGGEDCOM ROS должны соответствовать установленным требованиям, чтобы не допустить использования ненадежных паролей. При создании нового пароля убедитесь в том, что он соответствует следующим требованиям:

- Длина должна быть не менее 6 символов.
- Не должен содержать в себе имя пользователя или любые 4 буквенно-цифровых символа, которые присутствуют в имени пользователя и идут один за другим. Например, в случае имени пользователя *Subnet25* нельзя использовать пароль *subnet25admin* или *subnetadmin*. Однако допускаются пароли *net25admin* или *Sub25admin*.
- Должен содержать хотя бы один буквенный символ и одну цифру. Допускаются специальные символы.
- Не должен содержать более 3 последовательно возрастающих или убывающих цифр. Например, пароли *Sub123* и *Sub19826* допускаются, а *Sub12345* не допускается.

Если сконфигурирован ненадежный пароль, то будет генерироваться оповещение. Оповещение в связи с ненадежным паролем может быть отключено пользователем. Для получения дополнительной информации об отключении оповещений см. "Управление оповещениями (Страница 112)".

3. Необходимо сконфигурировать следующие параметры:

Параметр	Описание
`Name`	**Краткий обзор:** Строка длиной 32 символа(ов) **Значение по умолчанию:** initial Имя пользователя. Это имя пользователя также представляет собой имя режима безопасности, которое сопоставляет этого пользователя группе безопасности.
`IP Address`	**Краткий обзор:** Any valid IP address IP-адрес пользовательской станции администрирования SNMP. Если IP-адрес задан, то SNMP-запрос от данного пользователя будет также проверяться по IP-адресу. Для приемников trap-уведомлений будет генерироваться trap-уведомление о SNMP-аутентификации, если запрос получен от этого пользователя, но с любого другого IP-адреса. Если поле IP-адреса пустое, то trap-уведомления не могут генерироваться для этого пользователя, но SNMP-

Параметр	Описание
	запросы будут обслуживаться для этого пользователя с любого IP-адреса.
`v1/v2c Community`	**Краткий обзор:** Строка длиной 32 символа(ов) Строка Community, которая отображается с помощью имени этого пользователя/режима безопасности на группу безопасности в случае модели защиты SNMPv1 или SNMPv2c. Если эта строка оставлена пустой, то будет предполагаться, что она совпадает с именем пользователя.
`Auth Protocol`	**Краткий обзор:** [noAuth | HMACMD5 | HMACSHA] **Значение по умолчанию:** noAuth Указывает, должны ли подвергаться аутентификации сообщения, посылаемые от имени этого пользователя к SNMP-движку и обратно, а если должны, то какой тип протокола аутентификации применяется.
`Priv Protocol`	**Краткий обзор:** [noPriv | CBC-DES] **Значение по умолчанию:** noPriv Указывает, могут ли быть защищены от разглашения сообщения, посылаемые от имени этого пользователя к SNMP-движку и обратно, а если могут, то какой тип протокола шифрования применяется.
`Auth Key`	**Краткий обзор:** Строка длиной 31 символа(ов) Секретный ключ аутентификации (пароль), который должен использоваться совместно с SNMP-клиентом. Если этот ключ не представляет собой пустую строку, то его длина должна быть не менее 6 символов.
`Confirm Auth Key`	**Краткий обзор:** Строка длиной 31 символа(ов) Секретный ключ аутентификации (пароль), который должен использоваться совместно с SNMP-клиентом. Если этот ключ не представляет собой пустую строку, то его длина должна быть не менее 6 символов.
`Priv Key`	**Краткий обзор:** Строка длиной 31 символа(ов) Секретный ключ аутентификации (пароль), который должен использоваться совместно с SNMP-клиентом. Если этот ключ не представляет собой пустую строку, то его длина должна быть не менее 6 символов.
`Confirm Priv Key`	**Краткий обзор:** Строка длиной 31 символа(ов) Секретный ключ аутентификации (пароль), который должен использоваться совместно с SNMP-клиентом. Если этот ключ не представляет собой пустую строку, то его длина должна быть не менее 6 символов.

4. Нажмите **Apply**.

12.3.3.3 Удаление пользователя SNMP

CLI-команды, относящиеся к удалению пользователя SNMP, см. в "Доступные CLI-команды (Страница 27)".

Чтобы удалить пользователя SNMP, сделайте следующее:

1. Перейдите в ***Administration » Configure SNMP » Configure SNMP Users***. Появится **SNMP Users Table**.
2. Выберите пользователя из таблицы. Появится форма **SNMP Users**.
3. Нажмите **Delete**.

12.3.4 Управление соответствиями групп пользователей моделям и уровням безопасности

В данном разделе описывается процесс конфигурирования соответствий групп пользователей моделям и уровням безопасности и управления ими.

12.3.4.1 Просмотр соответствий групп пользователей моделям и уровням безопасности

Чтобы просмотреть список соответствий групп пользователей моделям и уровням безопасности, сконфигурированных на устройстве, перейдите в ***Administration » Configure SNMP » Configure SNMP Security to Group Maps***. Появится таблица **SNMP Security to Group Maps**.

Добавьте необходимые соответствия групп пользователей моделям и уровням безопасности, если они не были сконфигурированы. Для получения дополнительной информации см. "Добавление соответствия группы пользователей модели и уровню безопасности (Страница 441)".

12.3.4.2 Добавление соответствия группы пользователей модели и уровню безопасности

Для протокола SNMP можно определить несколько (до 32) комбинаций соответствия группы пользователей модели и уровню безопасности.

CLI-команды, относящиеся к добавлению соответствий групп пользователей моделям и уровням безопасности SNMP, см. "Доступные CLI-команды (Страница 27)".

Чтобы добавить соответствие группы пользователей модели и уровню безопасности, сделайте следующее:

1. Перейдите в ***Administration » Configure SNMP » Configure SNMP Security to Group Maps***. Появится **SNMP Security to Group Maps Table**.
2. Нажмите **InsertRecord**. Появится форма **SNMP Security to Group Maps**.

3. Необходимо сконфигурировать следующие параметры:

Параметр	Описание
`SecurityModel`	**Краткий обзор:** [snmpV1 | snmpV2c | snmpV3] **Значение по умолчанию:** snmpV3 Модель защиты, которая предусматривает имя, упоминаемое в этой таблице.
`Name`	**Краткий обзор:** Строка длиной 32 символа(ов) Имя пользователя, которое сопоставлено с помощью этой записи определенному имени группы.
`Group`	**Краткий обзор:** Строка длиной 32 символа(ов) Имя группы, которой принадлежат модель защиты и имя. Это имя используется в качестве указателя на таблицу доступа SNMPv3 VACM.

4. Нажмите **Apply**.

12.3.4.3 Удаление соответствия группы пользователей модели и уровню безопасности

CLI-команды, относящиеся к удалению соответствий групп пользователей моделям и уровням безопасности, см. "Доступные CLI-команды (Страница 27)".

Чтобы удалить соответствие группы пользователей модели и уровню безопасности, сделайте следующее:

1. Перейдите в ***Administration » Configure SNMP » Configure SNMP Security to Group Maps***. Появится **SNMP Security to Group Maps Table**.
2. Выберите привязку из таблицы. Появится форма **SNMP Security to Group Maps**.
3. Нажмите **Delete**.

12.3.5 Управление группами SNMP

На доступ к SNMP можно сконфигурировать несколько (до 32) групп SNMP.

12.3.5.1 Просмотр списка групп SNMP

Чтобы просмотреть список групп SNMP, сконфигурированных на устройстве, перейдите в ***Administration » Configure SNMP » Configure SNMP Access***. Появится таблица **SNMP Access**.

Добавьте необходимые группы SNMP, если они не были сконфигурированы. Для получения дополнительной информации см. "Добавление группы SNMP (Страница 443)".

12.3.5.2 Добавление группы SNMP

CLI-команды, относящиеся к добавлению группы SNMP, см. в "Доступные CLI-команды (Страница 27)".

Чтобы добавить группу SNMP, сделайте следующее:

1. Перейдите в ***Administration » Configure SNMP » Configure SNMP Access***. Появится **SNMP Access Table**.
2. Нажмите **InsertRecord**. Появится форма **SNMP Access**.
3. Необходимо сконфигурировать следующие параметры:

Параметр	Описание
`Group`	**Краткий обзор:** Строка длиной 32 символа(ов) Имя группы, которой принадлежат модель защиты и имя. Это имя используется в качестве указателя на таблицу доступа SNMPv3 VACM.
`SecurityModel`	**Краткий обзор:** [snmpV1 | snmpV2c | snmpV3] **Значение по умолчанию:** snmpV3 Чтобы получить права доступа, разрешенные этой записью, должна использоваться сконфигурированная модель защиты.
`SecurityLevel`	**Краткий обзор:** [noAuthNoPriv | authNoPriv | authPriv] **Значение по умолчанию:** noAuthNoPriv Минимальный необходимый уровень безопасности, чтобы получить права доступа, разрешенные этой записью. Уровень безопасности noAuthNoPriv ниже, чем authNoPriv, который в свою очередь ниже, чем authPriv.
`ReadViewName`	**Краткий обзор:** [noView | V1Mib | allOfMib] **Значение по умолчанию:** noView Этот параметр идентифицирует подраздел (подразделы) информационной базы данных управления (MIB), к которым эта запись разрешает доступ для чтения. В случае значения noView доступ для чтения не будет предоставляться.
`WriteViewName`	**Краткий обзор:** [noView | V1Mib | allOfMib] **Значение по умолчанию:** noView Этот параметр идентифицирует подраздел (подразделы) информационной базы данных управления (MIB), к которым эта запись разрешает доступ для записи. В случае значения noView доступ для записи не будет предоставляться.
`NotifyViewName`	**Краткий обзор:** [noView | V1Mib | allOfMib] **Значение по умолчанию:** noView Этот параметр идентифицирует подраздел (подразделы) информационной базы данных управления (MIB), к которым эта запись разрешает доступ для оповещений. В случае значения noView доступ для оповещений не будет предоставляться.

4. Нажмите **Apply**.

12.3.5.3 Удаление группы SNMP

CLI-команды, относящиеся к удалению группы SNMP, см. в "Доступные CLI-команды (Страница 27)".

Чтобы удалить группу SNMP, сделайте следующее:

1. Перейдите в ***Administration » Configure SNMP » Configure SNMP Access***. Появится **SNMP Access Table**.
2. Выберите группу из таблицы. Появится форма **SNMP Access**.
3. Нажмите **Delete**.

12.4 Поддержка управления ModBus

Поддержка администрирования ModBus в устройствах RUGGEDCOM обеспечивает простой интерфейс для извлечения базовой информации о состоянии. Поддержка ModBus упрощает работу интеграторов системы SCADA (диспетчерское управление и сбор данных), предусматривая привычный протокол для извлечения информации об устройстве под управлением RUGGEDCOM. ModBus обеспечивает главным образом информацию о состоянии только для чтения, однако существует также небольшое число регистров с возможностью записи для команд оператора.

Блок данных протокола (PDU) ModBus следующий:

Код функции	Данные

12.4.1 Функциональные коды ModBus

Устройства RUGGEDCOM поддерживают следующие коды функций ModBus для администрирования устройств через ModBus:

Примечание
Устройства RUGGEDCOM имеют различное количество портов, поэтому не все регистры и биты применимы к любому изделию.

Регистры, не применимые к конкретному устройству, возвращают нулевое (0) значение. Например, к коммутационным аппаратам RUGGEDCOM, не имеющим последовательных портов, не применимы относящиеся к таким портам регистры.

Чтение входных регистров или чтение регистров временного хранения данных — 0x04 или 0x03

Пример запроса PDU

Код функции	1 байт	0x04(0x03)
Начальный адрес	2 байта	0x0000 — 0xFFFF (шестнадцатеричный) 128 — 65535 (десятичный)
Количество входных регистров	2 байта	Байты 0x0001 — 0x007D

Пример ответа PDU

Код функции	1 байт	0x04(0x03)
Количество байтов	1 байт	2 x *N* [a]
Количество входных регистров	*N*[a] x 2 байта	

[a] Количество входных регистров

Запись в несколько регистров — 0x10

Пример запроса PDU

Код функции	1 байт	0x10
Начальный адрес	2 байта	0x0000 — 0xFFFF
Количество входных регистров	2 байта	Байты 0x0001 — 0x0079
Количество байтов	1 байт	2 x *N* [a]
Значение регистров	*N*[a] x 2 байта	Значение регистра

[a] Количество входных регистров

Пример ответа PDU

Код функции	1 байт	0x10
Начальный адрес	2 байта	0x0000 — 0xFFFF
Количество регистров	2 байта	1 — 121 (0x79)

12.4.2 Распределение адресного пространства ModBus

Ниже приведены сведения об отображении переменных данных процесса ModBus.

Информация об изделии

Приведенные ниже данные отображаются в таблице *Productinfo*:

Адрес	Число регистров	Описание (справочная таблица в UI)	R/W (чтение/ запись)	Формат
0000	16	Идентификация изделия	R	Текстовый
0010	32	Идентификация микропрограммного обеспечения	R	Текстовый
0040	1	Количество Ethernet-портов	R	Uint16
0042	1	Количество оповещений	R	Uint16
0043	1	Состояние блока питания	R	PSStatusCmd
0044	1	Статус FailSafe Relay (отказоустойчивое реле)	R	TruthValue
0045	1	Статус ErrorAlarm (оповещение при ошибке)	R	TruthValue

Регистры изделия, допускающие запись

Приведенные ниже данные отображаются в различных таблицах:

Адрес	Число регистров	Описание (справочная таблица в UI)	R/W (чтение/ запись)	Формат
0080	1	Удаление оповещений	W	Cmd
0081	2	Сброс Ethernet-портов	W	PortCmd
0083	2	Удаление статистики Ethernet	W	PortCmd

Оповещения

Приведенные ниже данные отображаются в таблице *alarms*:

Адрес	Число регистров	Описание (справочная таблица в UI)	R/W (чтение/ запись)	Формат
0100	64	Оповещение 1	R	Оповещение
0140	64	Оповещение 2	R	Оповещение
0180	64	Оповещение 3	R	Оповещение
01C0	64	Оповещение 4	R	Оповещение
0200	64	Оповещение 5	R	Оповещение
0240	64	Оповещение 6	R	Оповещение
0280	64	Оповещение 7	R	Оповещение
02C0	64	Оповещение 8	R	Оповещение

Статус Ethernet-порта

Приведенные ниже данные отображаются в таблице *ethPortStats*:

Адрес	Число регистров	Описание (справочная таблица в UI)	R/W (чтение/запись)	Формат
03FE	2	Коммуникационный статус порта	R	PortCmd

Статистика Ethernet

Приведенные ниже данные отображаются в таблице *rmonStats*:

Адрес	Число регистров	Описание (справочная таблица в UI)	R/W (чтение/запись)	Формат
0400	2	Статистика порта 1 — входящие Ethernet-пакеты	R	Uint32
0402	2	Статистика порта 2 — входящие Ethernet-пакеты	R	Uint32
0404	2	Статистика порта 3 — входящие Ethernet-пакеты	R	Uint32
0406	2	Статистика порта 4 — входящие Ethernet-пакеты	R	Uint32
0408	2	Статистика порта 5 — входящие Ethernet-пакеты	R	Uint32
040A	2	Статистика порта 6 — входящие Ethernet-пакеты	R	Uint32
040C	2	Статистика порта 7 — входящие Ethernet-пакеты	R	Uint32
040E	2	Статистика порта 8 — входящие Ethernet-пакеты	R	Uint32
0410	2	Статистика порта 9 — входящие Ethernet-пакеты	R	Uint32
0412	2	Статистика порта 10 — входящие Ethernet-пакеты	R	Uint32
0414	2	Статистика порта 11 — входящие Ethernet-пакеты	R	Uint32
0416	2	Статистика порта 12 — входящие Ethernet-пакеты	R	Uint32
0418	2	Статистика порта 13 — входящие Ethernet-пакеты	R	Uint32
041A	2	Статистика порта 14 — входящие Ethernet-пакеты	R	Uint32
041C	2	Статистика порта 15 — входящие Ethernet-пакеты	R	Uint32
041E	2	Статистика порта 16 — входящие Ethernet-пакеты	R	Uint32
0420	2	Статистика порта 17 — входящие Ethernet-пакеты	R	Uint32

Адрес	Число регистров	Описание (справочная таблица в UI)	R/W (чтение/ запись)	Формат
0422	2	Статистика порта 18 — входящие Ethernet-пакеты	R	Uint32
0424	2	Статистика порта 19 — входящие Ethernet-пакеты	R	Uint32
0426	2	Статистика порта 20 — входящие Ethernet-пакеты	R	Uint32
0440	2	Статистика порта 1 — исходящие Ethernet-пакеты	R	Uint32
0442	2	Статистика порта 2 — исходящие Ethernet-пакеты	R	Uint32
0444	2	Статистика порта 3 — исходящие Ethernet-пакеты	R	Uint32
0446	2	Статистика порта 4 — исходящие Ethernet-пакеты	R	Uint32
0448	2	Статистика порта 5 — исходящие Ethernet-пакеты	R	Uint32
044A	2	Статистика порта 6 — исходящие Ethernet-пакеты	R	Uint32
044C	2	Статистика порта 7 — исходящие Ethernet-пакеты	R	Uint32
044E	2	Статистика порта 8 — исходящие Ethernet-пакеты	R	Uint32
0450	2	Статистика порта 9 — исходящие Ethernet-пакеты	R	Uint32
0452	2	Статистика порта 10 — исходящие Ethernet-пакеты	R	Uint32
0454	2	Статистика порта 11 — исходящие Ethernet-пакеты	R	Uint32
0456	2	Статистика порта 12 — исходящие Ethernet-пакеты	R	Uint32
0458	2	Статистика порта 13 — исходящие Ethernet-пакеты	R	Uint32
045A	2	Статистика порта 14 — исходящие Ethernet-пакеты	R	Uint32
045C	2	Статистика порта 15 — исходящие Ethernet-пакеты	R	Uint32
045E	2	Статистика порта 16 — исходящие Ethernet-пакеты	R	Uint32
0460	2	Статистика порта 17 — исходящие Ethernet-пакеты	R	Uint32
0462	2	Статистика порта 18 — исходящие Ethernet-пакеты	R	Uint32
0464	2	Статистика порта 19 — исходящие Ethernet-пакеты	R	Uint32
0466	2	Статистика порта 20 — исходящие Ethernet-пакеты	R	Uint32

Адрес	Число регистров	Описание (справочная таблица в UI)	R/W (чтение/ запись)	Формат
0480	2	Статистика порта 1 — входящие Ethernet-октеты	R	Uint32
0482	2	Статистика порта 2 — входящие Ethernet-октеты	R	Uint32
0484	2	Статистика порта 3 — входящие Ethernet-октеты	R	Uint32
0486	2	Статистика порта 4 — входящие Ethernet-октеты	R	Uint32
0488	2	Статистика порта 5 — входящие Ethernet-октеты	R	Uint32
048A	2	Статистика порта 6 — входящие Ethernet-октеты	R	Uint32
048C	2	Статистика порта 7 — входящие Ethernet-октеты	R	Uint32
048E	2	Статистика порта 8 — входящие Ethernet-октеты	R	Uint32
0490	2	Статистика порта 9 — входящие Ethernet-октеты	R	Uint32
0492	2	Статистика порта 10 — входящие Ethernet-октеты	R	Uint32
0494	2	Статистика порта 11 — входящие Ethernet-октеты	R	Uint32
0496	2	Статистика порта 12 — входящие Ethernet-октеты	R	Uint32
0498	2	Статистика порта 13 — входящие Ethernet-октеты	R	Uint32
049A	2	Статистика порта 14 — входящие Ethernet-октеты	R	Uint32
049C	2	Статистика порта 15 — входящие Ethernet-октеты	R	Uint32
049E	2	Статистика порта 16 — входящие Ethernet-октеты	R	Uint32
04A0	2	Статистика порта 17 — входящие Ethernet-октеты	R	Uint32
04A2	2	Статистика порта 18 — входящие Ethernet-октеты	R	Uint32
04A4	2	Статистика порта 19 — входящие Ethernet-октеты	R	Uint32
04A6	2	Статистика порта 20 — входящие Ethernet-октеты	R	Uint32
04C0	2	Статистика порта 1 — исходящие Ethernet-октеты	R	Uint32
04C2	2	Статистика порта 2 — исходящие Ethernet-октеты	R	Uint32
04C4	2	Статистика порта 3 — исходящие Ethernet-октеты	R	Uint32

Адрес	Число регистров	Описание (справочная таблица в UI)	R/W (чтение/ запись)	Формат
04C6	2	Статистика порта 4 — исходящие Ethernet-октеты	R	Uint32
04C8	2	Статистика порта 5 — исходящие Ethernet-октеты	R	Uint32
04CA	2	Статистика порта 6 — исходящие Ethernet-октеты	R	Uint32
04CC	2	Статистика порта 7 — исходящие Ethernet-октеты	R	Uint32
04CE	2	Статистика порта 8 — исходящие Ethernet-октеты	R	Uint32
04D0	2	Статистика порта 9 — исходящие Ethernet-октеты	R	Uint32
04D2	2	Статистика порта 10 — исходящие Ethernet-октеты	R	Uint32
04D4	2	Статистика порта 11 — исходящие Ethernet-октеты	R	Uint32
04D6	2	Статистика порта 12 — исходящие Ethernet-октеты	R	Uint32
04D8	2	Статистика порта 13 — исходящие Ethernet-октеты	R	Uint32
04DA	2	Статистика порта 14 — исходящие Ethernet-октеты	R	Uint32
04DC	2	Статистика порта 15 — исходящие Ethernet-октеты	R	Uint32
04DE	2	Статистика порта 16 — исходящие Ethernet-октеты	R	Uint32
04E0	2	Статистика порта 17 — исходящие Ethernet-октеты	R	Uint32
04E2	2	Статистика порта 18 — исходящие Ethernet-октеты	R	Uint32
04E4	2	Статистика порта 19 — исходящие Ethernet-октеты	R	Uint32
04E6	2	Статистика порта 20 — исходящие Ethernet-октеты	R	Uint32

12.4.3 Форматы памяти ModBus

В данном разделе указаны форматы памяти Modbus, поддерживаемые RUGGEDCOM ROS.

12.4.3.1 Текстовый

Текстовый формат обеспечивает простое ASCII-представление информации, относящейся к изделию. Старший байт регистра символов ASCII идет первым.

Например, рассмотрим запрос *Чтение из нескольких регистров* для считывания идентификационных данных изделия начиная с адреса 0x0000.

0x04	0x00	0x00	0x00	0x08

Ответ может иметь следующий вид:

0x04	0x10	0x53	0x59	0x53	0x54	0x45	0x4D	0x20	0x4E	0x41	0x4D	0x45
0x00	0x00	0x00	0x00	0x00								

В этом примере, начиная с байта 3 и до конца, ответ является ASCII-представлением символов для идентификации изделия, со следующим текстом: *НАИМЕНОВАНИЕ СИСТЕМЫ*. Длина этого поля меньше восьми регистров, поэтому остаток поля заполняется нулями (0).

12.4.3.2 Cmd

Этот формат дает устройству команду устанавливать на выходе состояние *true (истинно)* или *false (ложно)*. Первым идет старший байт.

- Шестнадцатеричное значение FF 00 требует установить выход в состояние True (истинно).
- Шестнадцатеричное значение 00 00 требует установить выход в состояние False (ложно).
- Любое другое значение, помимо указанных значений, не влияет на запрошенную операцию.

Например, рассмотрим запрос *Запись в несколько регистров* для удаления оповещений на устройстве.

0x10	0x00	0x80	0x00	0x01	2	0xFF	0x00

- FF 00 для регистра 00 80 удаляет оповещения тревоги.
- 00 00 не удаляет оповещения тревоги.

Ответ может иметь следующий вид:

0x10	0x00	0x80	0x00	0x01

12.4.3.3 Uint16

Формат Uint16 описывает стандартный 16-разрядный регистр Modbus.

12.4.3.4 Uint32

Формат Uint32 описывает 2 стандартных 16-разрядных регистра Modbus. В первом регистре временно хранятся старшие 16 битов 32-разрядного значения. Во втором регистре временно хранятся младшие 16 битов 32-разрядного значения.

12.4.3.5 PortCmd

Формат PortCmd описывает конфигурацию битов на портах, причем 1 указывает, что запрошенная операция имеет статус "истинно", а 0 указывает, что запрошенная операция имеет статус "ложно".

PortCmd предусматривает конфигурацию битов максимум для 32 портов. Таким образом, используется два регистра Modbus:

- первый регистр Modbus соответствует портам 1–16;
- второй регистр Modbus соответствует портам 17–32 для конкретной операции.

Для разрядов, которые не применимы к соответствующему изделию, всегда установлено нулевое значение (0).

Значение бита, равное 1, указывает, что запрошенная операция имеет статус "истинно". Например, соответствующий порт *соединен*.

Значение бита, равное 0, указывает, что запрошенная операция имеет статус "ложно". Например, соответствующий порт *разъединен*.

Считывание данных с использованием PortCmd

Чтобы понять как осуществляется считывание данных с использованием PortCmd, рассмотрим запрос Modbus произвести чтение из нескольких регистров начиная с адреса 0x03FE.

0x04	0x03	0xFE	0x00	0x02

Ответ зависит от числа доступных портов на данном устройстве. Например, если максимальное число портов на подключенном устройстве RUGGEDCOM равно 20, то мог бы выглядеть следующим образом.

0x04	0x04	0xF2	0x76	0x00	0x05

В этом примере байты 3 и 4 относятся к регистру 1 по адресу 0x03FE и представляют состояние портов 1–16. Байты 5 и 6 относятся к регистру 2 по адресу 0x03FF и представляют состояние портов 17–32. Устройство имеет только 20 портов, так что байт 6 содержит индикацию состояния для портов 17–20, начиная справа налево. Остальные биты в регистре 2, которые соответствуют несуществующим портам 21–31, обнулены (0).

Выполнение операций записи с использованием PortCmd

Чтобы понять, как осуществляется запись с использованием PortCmd, рассмотрим запрос "Запись в несколько регистров" для удаления статистики Ethernet-порта:

0x10	0x00	0x83	0x00	0x01	2	0x55	0x76	0x00	0x50

Значение бита, равное 1, является командой удалить статистику Ethernet для соответствующего порта. При значении бита, равном 0, статистика Ethernet для соответствующего порта не удаляется.

0x10	0x00	0x81	0x00	0x02

12.4.3.6 Оповещение

Формат "Оповещение" представляет собой другую форму текстового описания. Текст сигнала тревоги соответствует описанию оповещения из таблицы, в которой временно хранятся все оповещения. Подобно формату "Текст" этот формат возвращает ASCII-представление оповещений.

Примечание
Оповещения помещаются в стек на устройстве в порядке их возникновения (т. е. Оповещение 1, Оповещение 2, Оповещение 3 и т. д.).

Вы можете вызвать первые восемь оповещений из стека, если они существуют. Если соответствующее оповещение не существует, то возвращается нулевое значение (0).

12.4.3.7 PSStatusCmd

Формат PSStatusCmd описывает конфигурацию битов для представления состояния имеющихся блоков питания. Для этой цели используются биты 0–4 младшего байта регистра.

- Биты 0–1: Состояние блока питания 1.
- Биты 2–3: Состояние блока питания 2.

Остальные биты этого регистра не несут какой-либо информации о состоянии системы.

Значения битов	Описание
01	Блок питания отсутствует (01 = 1).
10	Блок питания работоспособен (10 = 2).
11	Блок питания неработоспособен (11 = 3).

Значения, используемые для представления статуса блока питания, происходят из специальной базы SNMP MIB для устройств под управлением RUGGEDCOM.

Считывание состояния блока питания из устройства с использованием PSStatusCmd

Чтобы понять, как осуществляется считывание состояния блока питания из устройства с использованием PSStatusCmd, рассмотрим запрос Modbus произвести чтение из нескольких регистров начиная с адреса 0x0043.

0x04	0x00	0x43	0x00	0x01

Ответ может иметь следующий вид:

0x04	0x02	0x00	0x0A

Младший байт регистра показывает состояние блоков питания. В этом примере оба источника питания данного устройства являются работоспособными.

12.4.3.8 TruthValues

Формат Truthvalues представляет состояние "истинно" или "ложно" в конкретном устройстве.

- 1 — указывает, что соответствующее состояние для данного устройства должно быть true (истинно)
- 2 — указывает, что соответствующее состояние для данного устройства должно быть false (ложно)

Считывание состояния реле аварийной сигнализации с использованием TruthValue

Чтобы понять, как осуществляется считывание состояния "реле аварийной сигнализации" с использованием TruthValue, рассмотрим запрос Modbus произвести чтение из нескольких регистров начиная с адреса 0x0044.

0x04	0x00	0x44	0x00	0x01

Ответ может иметь следующий вид:

0x04	0x02	0x00	0x01

Младший байт регистра показывает статус "реле аварийной сигнализации". В этом примере на обмотку реле аварийной сигнализации подано напряжение.

Считывание статуса "Оповещение при ошибке" с использованием TruthValue

Чтобы понять, как осуществляется считывание статуса "Оповещение при ошибке" с использованием TruthValue, рассмотрим запрос Modbus произвести чтение из нескольких регистров начиная с адреса 0x0045.

0x04	0x00	0x45	0x00	0x01

Ответ может иметь следующий вид:

0x04	0x02	0x00	0x01

Младший байт регистра показывает статус "Оповещение при ошибке". В этом примере на устройстве отсутствуют активные оповещения из категорий "ОШИБКА", "ТРЕВОГА" или "КРИТИЧЕСКАЯ ОШИБКА".

13 Назначение IP-адреса

В данном разделе рассматриваются функции, связанные с назначением IP-адресов.

13.1 Управление DHCP

Протокол динамического конфигурирования хоста (DHCP) — это протокол связи, позволяющий сетевым администраторам централизованно осуществлять управление и автоматизацию сетевой конфигурации устройств, присоединенных к IP-сети.

13.1.1 Концепция DHCP

В следующем разделе описываются принципы, имеющие значение для конфигурирования и применения протокола DHCP.

13.1.1.1 Отслеживание DHCP

Отслеживание DHCP — функция сетевой безопасности, которая защищает сеть от ненадежных серверов DHCP и ненадежных клиентов путем отслеживания портов, где располагаются клиенты и серверы DHCP. Эта информация отслеживается путем построения таблицы привязки DHCP, содержащей все связи MAC–IP, запомненные коммутатором путем отслеживания обмена данными клиента и сервера DHCP. Таблица привязок содержит информацию по связям MAC–IP, которая может в дальнейшем использоваться приложениями отслеживания DHCP. RUGGEDCOM ROS будет регистрировать сообщения в системном журнале и/или выдавать оповещение при обнаружении нарушений DHCP.

Примечание
Отслеживание DHCP включается на устройстве для каждой сети VLAN в отдельности. Для получения дополнительной информации о включении отслеживания DHCP в отдельных сетях VLAN см. "Управление статическими сетями VLAN (Страница 173)".

13.1.1.2 Надежные и ненадежные порты

Отслеживание DHCP классифицирует порты как надежные и ненадежные. Эта классификация портов определяет, как сообщение DHCP обрабатывается коммутатором. Сообщения DHCP, получаемые на надежных портах, пересылаются без дальнейшей проверки, а сообщения, полученные на ненадежных портах, проверяются на предмет легитимности. Предполагается, что пользователь сконфигурирует порты как надежные или ненадежные.

Что касается использования, то предполагается, что пользователь сконфигурирует порты как надежные. Сетевые порты обычно подключаются к другому коммутатору или маршрутизатору. Это необходимо, поскольку сервер DHCP может быть подключен к порту коммутатора не напрямую.

Для получения дополнительной информации о конфигурировании портов в качестве надежных или ненадежных см. "Конфигурирование доверенных/недоверенных портов (Страница 463)".

13.1.1.3 Агент ретрансляции DHCP (Опция 82)

Агент ретрансляции DHCP представляет собой устройство, которое пересылает DHCP-пакеты между клиентами и серверами, если они находятся в разных физических сегментах локальной сети или в разных IP-подсетях. Эта функция активна, если указаны IP-адрес DHCP-сервера и группа ethernet-портов для доступа.

Опциональное поле номер 82 протокола DHCP обеспечивает механизм для выбора выдаваемого клиентскому устройству IP-адреса, исходя из расположения клиентского устройства в сети. Информация о местонахождении клиента может передаваться на сервер вместе с DHCP-запросом. На основании этой информации DHCP-сервер принимает решение о назначаемом IP-адресе.

Агент ретрансляции DHCP перехватывает широковещательные DHCP-запросы от клиентов, принимаемые на сконфигурированный порт доступа, и вставляет в пакет дополнительные данные агента ретрансляции (опция 82). Опция 82 содержит идентификатор виртуальной локальной сети VLAN ID (2 байта) и номер порта клиента (2 байта – подопция идентификатора канала), а также MAC-адрес агента реле (подопция идентификатора удаленного устройства). Эта информация однозначно определяет местонахождение в сети клиента.

Например, идентификатором канала для клиента, подключенного к сети VLAN 1 на порте 1, является `00:01:00:01`.

DHCP-сервер, поддерживающий DHCP-опцию 82, посылает направленный ответ и эхо-сообщения с полем данных "опция 82". Агент ретрансляции DHCP удаляет поле данных "опция 82" и ретранслирует пакет на порт, с которого был получен исходный запрос.

Эти параметры обеспечивают возможность сконфигурировать информацию на основании агента ретрансляции DHCP (Опция 82).

Для получения дополнительной информации о конфигурировании агента ретрансляции DHCP см. "Конфигурирование агента ретрансляции DHCP (Страница 461)".

13.1.1.4 Динамический контроль ARP

Динамический контроль ARP (DAI) — это приложение отслеживания DHCP, которое проверяет пакеты протокола преобразования адресов (ARP) в сети. DAI фильтрует пакеты ARP с недействительными привязками IP- и MAC-адреса. Это защищает сеть от некоторых атак "противник в середине". Динамическая проверка ARP обеспечивает перенаправление только действительных запросов и ответов ARP.

Примечание
Динамический контроль ARP можно включить только при включенном на устройстве отслеживании DHCP.

Пакеты запросов и ответов ARP, поступающие через ненадежные порты, перехватываются устройством и подлежат проверке. Пакеты ARP не перехватываются на портах, которые сконфгурированы как надежные. Пользователь должен сконфигурировать сетевые порты как *надежные*, чтобы трафик ARP между устройствами не подвергался проверке.

Поля MAC-адрес отправителя и IP-адрес отправителя в пакетах запроса/ответа ARP проверяются по наличию записи привязки MAC–IP в таблице привязок отслеживания DHCP. Если запись привязки отсутствует в таблице или информация в записи отличается, пакет запроса/ответа ARP отбрасывается.

Для получения дополнительной информации о статистике контроля ARP см. "Вывод диагностики контроля ARP (Страница 464)".

13.1.1.5 Таблица привязки DHCP

Отслеживание DHCP динамически оставляет и ведет таблицу привязок, используя информацию, извлекаемую из перехваченных сообщений DHCP. Таблица содержит запись для каждого ненадежного хоста с арендованным IP-адресом от сервера DHCP. Таблица не содержит записи для хостов, подключенных через надежные интерфейсы. Функция отслеживания DHCP обновляет таблицу, когда коммутатор получает специальные сообщения DHCP.

Когда устройство сбрасывается, вся запомненная коммутатором информация о привязках MAC–IP теряется, если запомненные привязки не сохранить в файле конфигурации коммутатора.

Если канал связи порта коммутатора отключается, все динамически запомненные записи, относящиеся к этому порту, удаляются из таблицы.

Вводимые вручную записи можно конфигурировать с использованием статической таблицы привязок. Для получения дополнительной информации

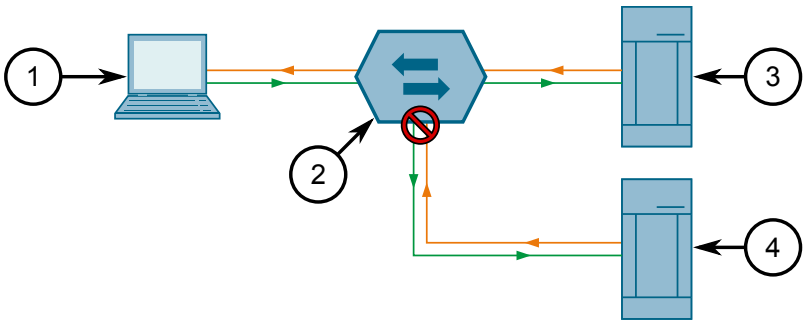
о конфигурировании таблицы привязки статического DHCP см. "Добавление записей в таблицу привязки DHCP (Страница 465)".

13.1.1.6 Предотвращаемые сетевые атаки

Следующие сетевые атаки можно предотвратить путем включения на коммутаторе отслеживания DHCP и динамического контроля ARP. Для получения дополнительной информации см. "Конфигурирование отслеживания DHCP (Страница 462)".

- **Неправильная конфигурация хоста неавторизованным DHCP-сервером**

  Неавторизованный DHCP-сервер может назначить клиенту неправильные IP-адрес, шлюз по умолчанию и/или параметры DNS-сервера. Неправильно сконфигурированный клиент подвержен потенциальным сетевым атакам. Коммутаторы, поддерживающие отслеживание DHCP, могут идентифицировать сообщения DHCP от неавторизованного DHCP-сервера и блокировать эти сообщения на самом коммутаторе.



① Клиент DHCP
② Коммутатор
③ DHCP-сервер
④ Неавторизованный DHCP-сервер

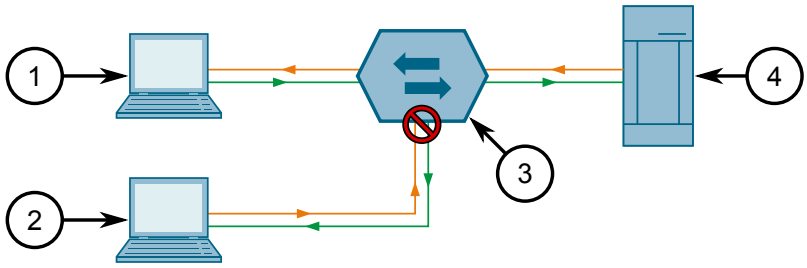
Рисунок 13.1 Неправильная конфигурация неавторизованным DHCP-сервером

- **Атака DHCP-клиента**

  Неавторизованный DHCP-клиент или хост злоумышленника может отменить аренду IP-адреса, назначенного другому клиенту, путем отправки

сообщения DHCPRELEASE DHCP-серверу. Он также может отклонить IP-адрес для другого клиента путем отправки сообщения DHCPDECLINE.

Отслеживание DHCP составляет таблицу привязок DHCP для проверки легитимности сообщений DHCPRELEASE и DHCPDECLINE. Если эти сообщения не проходят проверку, устройство отбрасывает их.



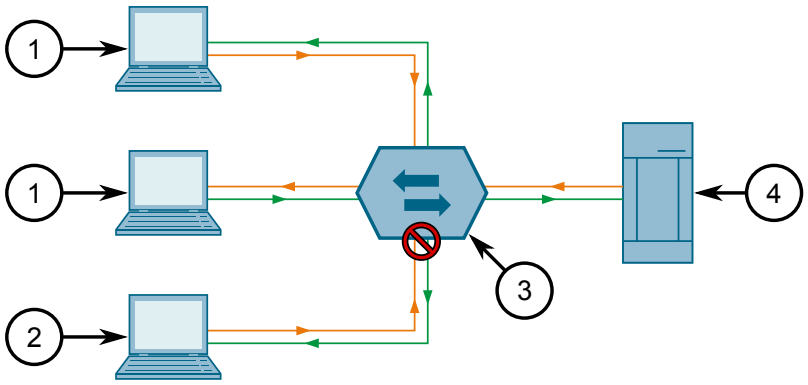
① Клиент DHCP
② Хост злоумышленника
③ Коммутатор
④ DHCP-сервер

Рисунок 13.2 Атака DHCP-клиента

- **Атака истощения DHCP**

  Перегрузка DHCP происходит, когда DHCP-сервер переполняется DHCP-запросами от одного неавторизованного DHCP-клиента, который подделал аппаратные адреса других клиентов. Это перегружает пул IP-адресов DHCP-сервера, после чего сервер становится неспособен отвечать и обеспечивать аренду легитимным DHCP-клиентам. Отслеживание DHCP

обеспечивает пользователей опцией проверки аппаратного адреса клиента в сообщении DHCPREQUEST, позволяя предотвратить атаку истощения.



① Клиент DHCP
② Злоумышленник
③ Коммутатор
④ DHCP-сервер

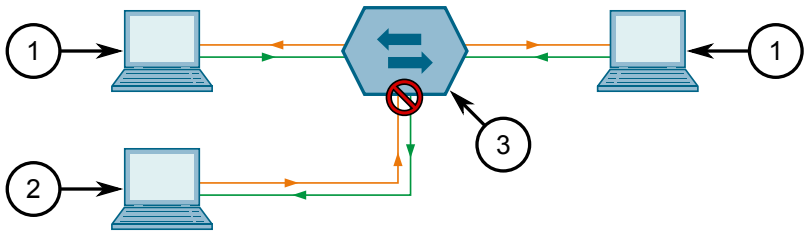
Рисунок 13.3 Атака истощения DHCP

- **Атака фальсификации (спуфинг) ARP/порча кэша**

  Атаки фальсификации ARP и порча кэша могут произойти, если ARP разрешает неоправданный ответ от хоста, даже если запрос ARP не был получен. После атаки весь трафик от атакованного устройства перетекает в компьютер злоумышленника. Атака фальсификации ARP может быть направлена на хосты, коммутаторы и маршрутизаторы, подключенные к сети 2-го уровня, путем порчи ARP-кэша систем, подключенных к подсети, и путем перехвата трафика, предназначенного для других хостов подсети.

  Атаку фальсификации ARP можно предотвратить путем включения динамического контроля ARP на коммутаторе. Для получения

дополнительной информации о включении динамического контроля ARP см. "Конфигурирование отслеживания DHCP (Страница 462)".



① Хост
② Злоумышленник
③ Коммутатор

Рисунок 13.4 Порча ARP-кэша

13.1.2 Конфигурирование агента ретрансляции DHCP

Чтобы сконфигурировать устройство в качестве агента ретрансляции DHCP (Опция 82), сделайте следующее:

1. Перейдите в ***Network Access Control » DHCP Snooping » Configure DHCP Parameters***. Появится форма **DHCP Parameters**.
2. Необходимо сконфигурировать следующие параметры:

Параметр	Описание
`DHCP Server Address`	**Краткий обзор:** Any valid IP address IP-адрес DHCP-сервера, на который будут пересылаться DHCP-запросы. Для работы агента ретрансляции необходимо сконфигурировать IP DHCP-сервера.

3. Нажмите **Apply**.
4. Включите агент ретрансляции DHCP (Опция 82) на портах, подключенных к DHCP-клиенту. Для получения дополнительной информации см. "Включение информации агента ретрансляции DHCP (Опция 82) для конкретных портов (Страница 461)".

13.1.3 Включение информации агента ретрансляции DHCP (Опция 82) для конкретных портов

Агент ретрансляции DHCP (Опция 82) можно включить для любого Ethernet-порта, подключенного к DHCP-клиенту.

Чтобы включить агент ретрансляции DHCP (Опция 82) для конкретного порта, сделайте следующее:

1. Перейдите в ***Network Access Control » DHCP Snooping » Configure DHCP Port Parameters***. Появится таблица **DHCP Port Parameters**.
2. Выберите порт. Появится форма **DHCP Port Parameters**.

   Примечание
   Параметр `Trusted` конфигурируется как часть функции агента ретрансляции DHCP. Для получения дополнительной информации см. "Конфигурирование доверенных/недоверенных портов (Страница 463)".

3. Необходимо сконфигурировать следующие параметры:

Параметр	Описание
`Port`	**Краткий обзор:** 1 to maximum port number Номер порта.
`Option-82`	**Краткий обзор:** [Disabled | Enabled] **Значение по умолчанию:** Disabled Вставка DHCP, Опция 82.

4. Нажмите **Apply**.

13.1.4 Конфигурирование отслеживания DHCP

Чтобы сконфигурировать отслеживание DHCP, сделайте следующее:

Примечание
Отслеживание DHCP включается на устройстве для каждой сети VLAN в отдельности. Для получения дополнительной информации о включении отслеживания DHCP в отдельных сетях VLAN см. "Управление статическими сетями VLAN (Страница 173)".

1. Перейдите в ***Network Access Control » DHCP Snooping » Configure DHCP Parameters***. Появится форма **DHCP Parameters**.
2. Необходимо сконфигурировать следующие параметры:

Параметр	Описание
`DHCP Server Address`	**Краткий обзор:** Any valid IP address IP-адрес DHCP-сервера, на который будут пересылаться DHCP-запросы. Для работы агента ретрансляции необходимо сконфигурировать IP DHCP-сервера.

Параметр	Описание
`Verify Hardware Address`	**Краткий обзор:** [No | Yes] **Значение по умолчанию:** Yes Проверьте, совпадает ли аппаратный адрес клиента, присутствующий в сообщении DHCP, полученном от ненадежного порта, с MAC-адресом источника.

3. Нажмите **Apply**.
4. Сконфигурируйте отдельные порты как *доверенные* или *недоверенные*. Для получения дополнительной информации см. "Конфигурирование доверенных/недоверенных портов (Страница 463)".

13.1.5 Конфигурирование доверенных/недоверенных портов

После включения отслеживания DHCP отдельные порты должны быть помечены как *доверенные* или *недоверенные*. Порты, подключенные к DHCP-серверу, должны быть *доверенными*, тогда как порты, подключенные к клиенту или ненадежному DHCP-серверу, должны считаться *недоверенными*.

Чтобы сконфигурировать порт как *доверенный* или *недоверенный*, сделайте следующее:

1. Перейдите в ***Network Access Control » DHCP Snooping » Configure DHCP Port Parameters***. Появится таблица **DHCP Port Parameters**.
2. Выберите Ethernet-порт. Появится форма **DHCP Port Parameters**.

Примечание
Параметр `Option-82` конфигурируется как часть функции агента ретрансляции DHCP. Для получения дополнительной информации см. "Включение информации агента ретрансляции DHCP (Опция 82) для конкретных портов (Страница 461)".

3. Необходимо сконфигурировать следующие параметры:

Параметр	Описание
`Trusted`	**Краткий обзор:** [No | Yes] **Значение по умолчанию:** No Настройка надежности DHCP для порта.

4. Нажмите **Apply**.

13.1.6 Управление динамическим контролем ARP

В данном разделе описывается процесс конфигурирования и управления для проверки протокола преобразования адресов (ARP).

13.1.6.1 Включение/отключение динамического контроля ARP

Чтобы включить или выключить динамический контроль ARP, сделайте следующее:

1. Перейдите в ***Network Access Control » DHCP Snooping » Configure DHCP Parameters***. Появится форма **DHCP Parameters**.
2. Необходимо сконфигурировать следующие параметры:

Параметр	Описание
`ARP Inspection`	**Краткий обзор:** [Disabled | Enabled] **Значение по умолчанию:** Disabled Включение или выключение динамического контроля ARP.

3. Нажмите **Apply**.

13.1.6.2 Вывод диагностики контроля ARP

Чтобы просмотреть статистику контроля ARP, сделайте следующее:

1. Перейдите в ***Network Access Control » DHCP Snooping » View ARP Inspection Statistics***. Появится таблица **ARP Inspection Statistics**.
2. Выберите Ethernet-порт. Появится форма **ARP Inspection Statistics**.
3. Необходимо сконфигурировать следующие параметры:

Параметр	Описание
`Port`	Номер порта.
`In Packets`	**Краткий обзор:** Целое число от 0 до 4294967295 Общее количество входящих пакетов ARP, которые были обработаны динамическим контролем ARP на этом порте.
`Dropped Packets`	**Краткий обзор:** Целое число от 0 до 4294967295 Общее количество входящих пакетов ARP, которые были отброшены динамическим контролем ARP на этом порте.

4. Нажмите **Apply**.

13.1.6.3 Очистка статистики контроля ARP

Чтобы очистить статистику контроля ARP, сделайте следующее:

1. Перейдите в ***Network Access Control » DHCP Snooping » Clear ARP Inspection Statistics***. Появится форма **Clear ARP Inspection Statistics**.
2. Нажмите **Confirm**.

13.1.7 Управление таблицей привязки DHCP

В данном разделе описывается процесс конфигурирования таблицы привязки DHCP и управления ею.

13.1.7.1 Добавление записей в таблицу привязки DHCP

Таблица привязки DHCP автоматически заполняется информацией, которую RUGGEDCOM ROS определяет о ненадежных портах. В таблицу также можно добавить конкретные хосты. Срок действия статических записей не истекает и не будет удаляться при отключении отслеживания DHCP или сбросе устройства.

Чтобы добавить статическую запись в таблицу DHCP, сделайте следующее:

1. Перейдите в ***Network Access Control » DHCP Snooping » Configure Static DHCP Binding Table***. Появится **Configure Static DHCP Binding Table**.
2. Нажмите **InsertRecord**. Появится форма **Static DHCP Binding Table**.
3. Необходимо сконфигурировать следующие параметры:

Параметр	Описание
`MAC Address`	**Краткий обзор:** ##-##-##-##-##-## where ## ranges 0 to FF **Значение по умолчанию:** 00-00-00-00-00-00 MAC-адрес DHCP-хоста.
`IP Address`	**Краткий обзор:** ##-##-##-##-##-## where ## ranges 0 to 255 IP-адрес, назначенный DHCP-хосту.
`VID`	**Краткий обзор:** Целое число от 0 до 65535 **Значение по умолчанию:** 1 Сеть VLAN, в которой была зарегистрирована запись привязки IP-MAC.
`Port`	**Краткий обзор:** 1 to maximum port number **Значение по умолчанию:** 1 Порт, на котором была зарегистрирована запись привязки IP-MAC.

4. Нажмите **Apply**.

13.1.7.2 Просмотр таблицы привязки DHCP

Чтобы просмотреть статическую запись в таблице DHCP, сделайте следующее:

1. Перейдите в ***Network Access Control » DHCP Snooping » View DHCP Binding Table***. Появится **View DHCP Binding Table**.
2. Выберите Ethernet-порт. Появится форма **DHCP Binding Table**.

В таблице привязки DHCP отображается следующая информация:

Параметр	Описание
`MAC Address`	**Краткий обзор:** ##-##-##-##-##-## where ## ranges 0 to FF MAC-адрес DHCP-хоста.
`IP Address`	**Краткий обзор:** ##-##-##-##-##-## where ## ranges 0 to 255 IP-адрес, назначенный DHCP-хосту.
`VID`	**Краткий обзор:** Целое число от 0 до 65535 Сеть VLAN, в которой была зарегистрирована запись привязки IP-MAC.
`Port`	**Краткий обзор:** 1 to maximum port number **Значение по умолчанию:** 1 Порт, на котором была зарегистрирована запись привязки IP-MAC.
`Type`	**Краткий обзор:** [Static | Dynamic] Записи динамической привязки IP-MAC для DHCP.
`Lease (secs)`	**Краткий обзор:** Целое число от 0 до 4294967295 или [–] Время аренды, назначенное для записи динамической привязки в секундах. Если запись относится к статической привязке, то время аренды бесконечно и обозначается как "–".

Чтобы обновить таблицу, нажмите **Reload**.

13.1.7.3 Сохранение таблицы привязки DHCP

Информация, динамически определяемая и добавляемая в таблицу привязки DHCP, автоматически удаляется в следующих случаях:

- Истекает срок аренды.
- Отключение отслеживания DHCP.
- Перезапуск устройства.

Однако эту информацию можно сохранить в файл конфигурации для ссылок/использования в будущем.

Чтобы сохранить статическую запись в таблице DHCP, сделайте следующее:

1. Перейдите в ***Network Access Control » DHCP Snooping » Save DHCP Binding Table***. Появится таблица **Save DHCP Binding Table**.
2. Нажмите **Confirm**.

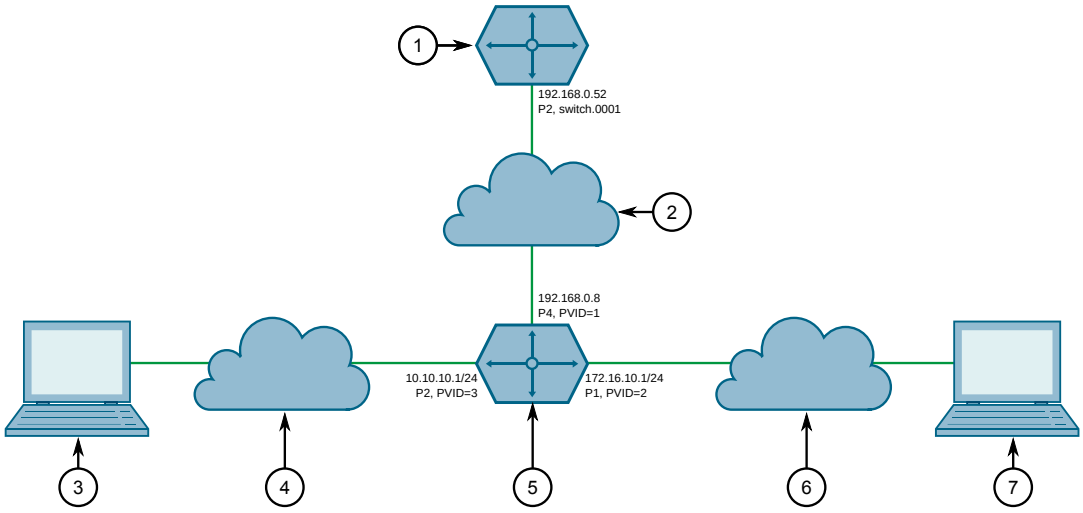
13.1.7.4 Пример: Конфигурирование устройства в качестве агента ретрансляции

В данном примере рассматривается, как сконфигурировать устройство в качестве агента ретрансляции DHCP.

Следующая топология описывает сценарий, при котором двум клиентам на отдельных сетях LAN требуются IP-адреса на разных подсетях от DHCP-сервера. Каждый клиент подключается к агенту ретрансляции DHCP с использованием различных сетей VLAN. Агент ретрансляции DHCP управляет запросами и ответами между клиентами и DHCP-сервером.

⚠ ЗАМЕТКА

Указанные значения характерны для представленной топологии. Фактические значения могут отличаться, в зависимости от конфигурации пользователя.



① DHCP-сервер
② Сеть LAN A
③ Клиент 2
④ Сеть LAN B
⑤ Агент ретрансляции DHCP (устройство под управлением RUGGEDCOM ROS)
⑥ Сеть LAN C
⑦ Клиент 1

Рисунок 13.5 Топология — устройство как агент ретрансляции

Чтобы сконфигурировать устройство в качестве агента ретрансляции DHCP в соответствии с топологией, сделайте следующее:

1. Сконфигурируйте отдельное устройство в качестве DHCP-сервера. Если в качестве сервера DHCP используется устройство RUGGEDCOM ROX II, дополнительную информацию см. в руководстве пользователя для соответствующего устройства.

2. Сконфигурируйте устройство под управлением RUGGEDCOM ROS в качестве агента ретрансляции DHCP:
   a. Добавьте сети VLAN 2 и VLAN 3. Для получения дополнительной информации см. "Добавление статической сети VLAN (Страница 174)".
   b. Назначьте IP-адрес *192.168.0.8* сети VLAN 1. Для получения дополнительной информации см. "Добавление IP-интерфейса (Страница 92)".
   c. Измените PVID порта 1 на PVID 2, а PVID порта 2 на PVID 3. Для получения дополнительной информации см. "Конфигурирование сетей VLAN для конкретных Ethernet-портов (Страница 171)".
   d. Сконфигурируйте *192.168.0.52* в качестве адреса DHCP-сервера. Для получения дополнительной информации см. "Конфигурирование агента ретрансляции DHCP (Страница 461)".
   e. Сконфигурируйте порты клиента и сервера DHCP следующим образом:

Порт	Опция 82
1	Включено
2	Включено
4	Отключено

   Для получения дополнительной информации о конфигурировании агента ретрансляции DHCP (Опция 82) для конкретного порта см. "Включение информации агента ретрансляции DHCP (Опция 82) для конкретных портов (Страница 461)".
   f. Для проверки конфигурации необходимо убедиться, что IP-адрес Клиента 1 — 172.16.10.1/24, а Клиента 2 — 10.10.10.1/24.
3. [Дополнительно] Сконфигурируйте отслеживание DHCP:
   a. Включите отслеживание DHCP на DHCP-сервере. Если в качестве сервера DHCP используется устройство RUGGEDCOM ROX II, дополнительную информацию см. в руководстве пользователя для соответствующего устройства.
   b. Убедитесь, что опция DHCP включена в сетях VLAN 1, 2, и 3. Для получения дополнительной информации о включении DHCP для конкретной сети VLAN см. "Добавление статической сети VLAN (Страница 174)".
   c. Сконфигурируйте порты клиента и сервера DHCP:

      Для получения дополнительной информации о конфигурировании параметров порта DHCP см. "Конфигурирование доверенных/недоверенных портов (Страница 463)".

Порт	Надежный
1	Нет
2	Нет

Порт	Надежный
4	Да

Для проверки конфигурации необходимо убедиться, что IP-адрес Клиента 1 — 172.16.10.1/24, а Клиента 2 — 10.10.10.1/24.

Убедитесь, что в таблицу привязки агента ретрансляции были добавлены записи для портов 1 и 2, а также в отсутствии в ней записей для порта 4. Для получения дополнительной информации см. "Просмотр таблицы привязки DHCP (Страница 465)".

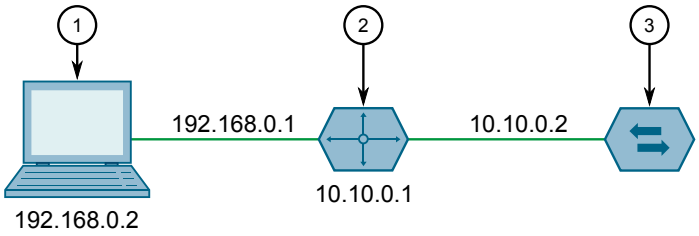
14 Выявление и устранение проблем

В данном разделе приведены шаги для решения распространенных проблем, которые могут возникать при использовании операционной системы RUGGEDCOM ROS или при проектировании сети.

⚠ ЗАМЕТКА
Для получения дополнительной помощи обратитесь в Службу поддержки клиентов.

14.1 Общее

Ниже приведено описание распространенных проблем.

Проблема	Решение
IP-адрес и шлюз сконфигурированы, но коммутатор не реагирует на ping-запросы. Коммутатор получает ping-запросы, поскольку статистика устройства регистрирует их, а светодиодные индикаторы мигают. Что происходит в данном случае?	Не производится ли проверка коммутатора с помощью команды ping через маршрутизатор? Если это так, то следует также сконфигурировать адрес шлюза коммутатора. Данную проблему иллюстрирует следующий рисунок.  ① Рабочая станция ② Маршрутизатор ③ Коммутатор Рисунок 14.1 Использование маршрутизатора в качестве шлюза Маршрутизатор сконфигурирован с соответствующими IP-подсетями и будет пересылать ping-запрос от рабочей станции коммутатору. Однако, когда коммутатор отвечает, ему неизвестно, какой из своих интерфейсов он должен использовать для доступа к рабочей станции, так что он будет отбрасывать ответ. Программирование адреса шлюза 10.0.0.1 приведет к тому, что коммутатор будет пересылать на маршрутизатор кадры, проблему которых он не может разрешить.

Проблема	Решение
	Подобная проблема также будет возникать в том случае, если адрес шлюза не сконфигурирован, а коммутатор пытается послать SNMP-уведомление (SNMP trap) на хост, который не находится в локальной подсети.

14.2 Ethernet-порты

Ниже приведено описание распространенных проблем, относящихся к Ethernet-портам.

Проблема	Решение
Канал связи кажется исправным при низком уровне трафика, но отказывает при увеличении скорости трафика; ИЛИ канал получает ping-запросы, но имеют место проблемы с FTP, SQL, HTTP и т. д.	Другая возможная причина нестабильной работы при отключенном автосогласовании — несоответствие дуплексного режима. Если на одной стороне канала связи установлен фиксированный полнодуплексный режим, а партнер по связи производит автоматическое согласование, то сторона с автосогласованием переключится в полудуплексный режим. При небольшом объеме трафика канал связи может демонстрировать меньше ошибок или даже их отсутствие. По мере роста объема трафика на стороне с фиксированным согласованием параметров связи начнут теряться пакеты, тогда как на стороне с автоматическим согласованием будут иметь место коллизии. И наконец, по мере приближения интенсивности трафика к 100 % канал связи станет полностью непригодным для использования. Команда ping с опциями, порождающими большой объем трафика, служит полезным инструментом для тестирования линий связи, которые вводятся в эксплуатацию. Для ping-проверки следующего коммутатора путем отправки указанного количества эхо-запросов с указанным интервалом в миллисекундах можно использовать команду **`ping`** `{destination} {count} {timeout}`. Например, **`ping`** `192.168.0.1 500 2` отправляет 500 ping-запросов на следующий коммутатор с интервалом между запросами две миллисекунды. Если используемый канал обеспечивает высокое качество связи, то ping-запросы не должны теряться, а среднее продолжительность пребывания в коммутаторе в прямом и обратном направлениях должно быть небольшим.
Каналы недоступны даже при использовании функции Link Fault Indication (LFI — индикация отказа канала связи).	Проверьте, не включена ли функция LFI также на устройстве партнере. Если на обеих сторонах линии связи включена функция LFI, то обе стороны будут воздерживаться от передачи сигнала наличия связи друг другу.
В работе ранее стабильного порта могут наблюдаться перебои при подключении новой среды передачи.	Это нормальное явление при подключении волоконно-оптических устройств. Во время загрузки нового подключенного волоконно-оптического устройства волоконно-оптические порты находятся в переходном состоянии, поэтому на смежных работающих системах (функционирующих и стабильных) могут происходить перебои в работе портов до завершения последовательности начальной загрузки. Это вызвано тем, что уровни питания оптоволоконного трансивера меняются

Проблема	Решение
	во время загрузки, что приводит к перебоям в работе подключенного канала связи. Установка волоконно-оптических кабелей в работающей сети также приведет к таким эффектам, особенно для несимметричных и фиксируемых коннекторов, например, коннекторов ST.
Удаленный системный журнал пропускает события или регистрирует их в неправильной последовательности.	Это нормальное явление при подключении Ethernet-коммутатора к сети. BRUGGEDCOM ROS стабильность системы и сети имеет высший приоритет. При подключении нового Ethernet коммутатора к сети происходит ее реконфигурирование для предотвращения формирования петель и возникновения широковещательных штормов. Когда происходит такая реконфигурация, высший приоритет назначается RSTP-сообщениям и действиям по реконфигурированию, а не регистрации событий.

14.3 Связующее дерево

Ниже приведено описание распространенных проблем, относящихся к Spanning Tree Protocol (STP — протокол связующего дерева).

Проблема	Решение
Сеть блокируется при подключении нового порта, а светодиодные индикаторы статуса порта быстро мигают.	Возможно, что на одном из коммутаторов в сети или на одном из портов коммутатора, находящегося в сети, отключен протокол STP, и он случайно соединен с другим коммутатором. Если это произошло, то возникла петля трафика.
Периодически происходит кратковременная значительная перегрузка портов пакетами.	Если проблема имеет временный характер, то возможно, что порты, являющиеся частью связующего дерева, были сконфигурированы как граничные порты. После того как на граничных портах активизируются канальные уровни, STP сразу переведет эти порты (не исключено, что некорректно) в состояние пересылки данных. Если затем будет получено конфигурационное сообщение RSTP, то порт вернется в состояние блокировки. Петля трафика могла возникнуть на время, пока порт находился в состоянии пересылки данных.
Один из коммутаторов демонстрирует странное поведение, когда роль корневого безостановочно переходит то к одному, то к другому порту.	Если на одном из коммутаторов корневой порт перебрасывается с одного порта на другой, то может иметь место одна из проблем приоритезации трафика. Для получения дополнительной информации см. "The network becomes unstable when a specific application is started." (Страница 475). Другая возможная причина нестабильной работы состоит в несовпадении при автоматическом согласовании. Если на одной стороне канала связи установлен фиксированный полнодуплексный режим, а партнер по связи производит автоматическое согласование, то сторона с автосогласованием переключится в полудуплексный режим. При меньшем трафике канал связи может демонстрировать меньше ошибок или даже их отсутствие. По мере роста объема трафика на стороне с фиксированным согласованием параметров связи начнут теряться пакеты, тогда как на стороне с автоматическим согласованием будут иметь место коллизии. И наконец, по мере приближения интенсивности

Проблема	Решение
	трафика к 100 % канал связи станет полностью непригодным для использования. С этого момента RSTP больше не сможет передавать конфигурационные сообщения по каналу связи и топология связующего дерева распадется. Если существует альтернативный порт в транковой группе, то RSTP активизирует его вместо перегруженного порта. Поскольку активизация альтернативного порта нередко освобождает перегруженный порт от его трафика, то перегруженный порт снова становится работоспособным. RSTP снова оперативно введет его в эксплуатацию, повторно начиная тот же цикл. Корневой порт будет перебрасываться назад и вперед между двумя портами коммутатора.
Компьютер или устройство подключается к коммутатору. После сброса коммутатора на его загрузку уходит много времени.	Возможно ли, что для параметра Edge (граничный) в настройках RSTP для этого порта задано значение false (ложно)? Если для параметра Edge (граничный) задано значение false (ложно), то мост обеспечит для этого порта две задержки пересылки данных, прежде чем порт сможет посылать или принимать кадры. Если для параметра Edge (граничный) задано значение true (истинно), то порт сразу переходит в состояние пересылки данных после установления соединения. Другое возможное объяснение состоит в том, что некоторые каналы связи в сети работают в полудуплексном режиме. В RSTP используется одноранговый протокол под названием Proposing-Agreeing (предложение-соглашение), чтобы обеспечить переход к другой топологии в случае отказа какого-либо канала связи. Этот протокол требует функционирования в полнодуплексном режиме. Когда RSTP обнаруживает порт, который не находится в полнодуплексном режиме, то полагаться на протокол "предложение–соглашение" нельзя, так что переход между состояниями порта приходится производить медленным (т. е. принятым в STP) способом. Сконфигурируйте порт для работы в полнодуплексном режиме, если это возможно. В противном случае задайте для параметра настройки порта point-to-point (соединение точка-точка) значение true (истинно). Любая из этих мер позволит использовать протокол "предложение-соглашение".
При тестировании коммутатора разрывом канала связи проходит много времени до того, как можно будет опрашивать устройства, расположенные за коммутатором.	Возможно, что некоторые участвующие в топологии порты были сконфигурированы в режиме STP, либо для параметра порта point-to-point (соединение точка-точка) задано значение false (ложно)? STP и порты с множественным доступом имеют медленную сходимость после возникновения отказа. Возможно, что порт мигрировал к STP? Если порт подключен к сегменту локальной сети через совместно используемую среду передачи данных, а STP-мосты также подключены к этой среде передачи данных, то сходимость после отказа канала связи будет медленная. В результате могут иметь место задержки порядка десятков или сотен миллисекунд в обстоятельствах, когда разорванный канал связи является единственным каналом связи с корневым мостом, а вторичный корневой мост выбран неудачно. Худшая из всех возможных топологий получается, когда вторичный корневой мост находится на самой дальней от корневого моста границе сети. В этом случае

Проблема	Решение
	конфигурирующее сообщение должно будет распространиться от границы, а затем обратно, чтобы восстановить топологию.
Сеть состоит из кольца мостов, два из которых (подключены друг к другу) управляемые, а остальные неуправляемые. Почему протокол RSTP работает быстро, когда линия связи разрывается между управляемыми мостами, но не в остальной части кольца с неуправляемыми мостами?	Правильно функционирующий неуправляемый мост прозрачен для конфигурационных сообщений STP. Управляемые мосты будут обмениваться конфигурационными сообщениями через остальную часть кольца с неуправляемыми мостами так, словно ее не существует. Однако при отказе канала связи в неуправляемой части кольца управляемые мосты смогут обнаружить отказ только через тайм-аут hello-сообщений (конфигурационных сообщений, подтверждающих работоспособность устройств). Для восстановления полной связности потребуется трехкратный интервал времени выдачи hello-сообщений плюс двукратный интервал задержки перехода в режим пересылки.
Сеть становится нестабильной, когда запущено конкретное приложение. Сеть возвращается в нормальное состояние после остановки приложения.	RSTP посылает свои конфигурационные сообщения, используя самый высокий уровень приоритета из возможных. Если CoS (класс сервиса) настроен таким образом, что для передачи трафика также используется самый высокий приоритет, а объем трафика возрастает до 100% пропускной способности канала, то работа протокола STP может быть нарушена. Таким образом, не рекомендуется использовать самый высокий CoS.
При введении нового порта он становится корневым, вместо порта, который должен был стать/остаться корневым.	Возможно ли, что неправильно задана стоимость порта, либо при автоматическом согласовании вычисляется неверное значение? Проверьте стоимость порта и пути для каждого порта, который активен в качестве корневого порта.
Интеллектуальное электронное устройство (ИЭУ) или контроллер не работает с устройством.	Было обнаружено, что на некоторых контроллерах с низкой производительностью процессора наблюдаются проблемы при получении Ethernet-кадров с неизвестным им содержимым. Попытайтесь отключить STP для данного порта. Если контроллер отказывает приблизительно во время перебоя в работе канала связи, то существует незначительная вероятность, что причиной проблемы может быть нарушение порядка передачи кадров или их дублирование. Попробуйте настроить параметры STP для корневого порта моста, к которому подключен контроллер.
Опросы, отправляемые на другие устройства, периодически теряются.	Проконтролируйте сетевую статистику, чтобы определить, принимает ли корневой мост Topology Change Notifications (TCN — оповещения об изменении топологии) приблизительно во время наблюдаемой потери кадров. Могут иметь место проблемы с промежуточными каналами в сети.
Корневое устройство получает множество сообщений TCN. Откуда они поступают?	Проанализируйте статистику порта RSTP, чтобы определить порт, с которого приходят сообщения TCN. Подключитесь и просмотрите диагностику на коммутаторе на другом конце канала связи, подключенного к данному порту. Повторяйте этот шаг, пока не будет найден коммутатор, генерирующий сообщения TCN (то есть коммутатор, который сам не принимает большого числа сообщений TCN). Определите причину проблемы на этом коммутаторе.

14.4 Сети VLAN

Ниже приведено описание распространенных проблем, относящихся к сетям VLAN.

Проблема	Решение
Сети VLAN не нужны в сети. Можно ли их выключить?	Да. Просто оставьте для настроек всех портов тип *edge (граничный)* и оставьте для настройки native VLAN значение 1. Это конфигурация коммутатора по умолчанию.
Было создано две сети VLAN и несколько портов были сделаны участниками этих сетей. Теперь необходимо, чтобы некоторые устройства в одной сети VLAN посылали сообщения на некоторые устройства в другой сети VLAN.	Если устройства должны взаимодействовать на уровне физических адресов, то они должны быть участниками одной и той же сети VLAN. Если они могут взаимодействовать одним из способов уровня 3 (например, используя протокол IP или IPX), то можно использовать маршрутизатор. Маршрутизатор будет рассматривать каждую сеть VLAN как отдельный интерфейс, с которым связано собственное пространство IP-адресов.
В сети, содержащей 30 коммутаторов, управляющий трафик необходимо ограничить до отдельного домена. Как выполнить эту перенастройку, чтобы в ее процессе не потерять доступ к коммутаторам для управления ими?	Сконфигурируйте порт коммутатора, при котором находится станция администратора, чтобы использовать новую сеть VLAN с передачей трафика управления коммутаторами в качестве его native VLAN (VLAN, в которой кадры не тегируются). Сконфигурируйте сервер таким образом, чтобы он действовал в качестве временной станции администратора. В конфигурации каждого коммутатора укажите новое значение для сети VLAN с передачей трафика управления коммутаторами. Контакт с каждым отдельным коммутатором будет мгновенно утерян по мере их конфигурирования, но обмен данными должно получиться восстановить с временной станции управления. После того как все коммутаторы будут привязаны к новой сети VLAN с передачей трафика управления коммутаторами, сконфигурируйте порты всех присоединенных управляющих устройств, чтобы использовалась новая сеть VLAN. **Примечание** Формирование домена управления часто сопровождается созданием IP-подсети специально для управляемых устройств.

Дополнительная информация

Siemens RUGGEDCOM
https://www.siemens.com/ruggedcom

Сайт технической поддержки продуктов для Промышленности (поддержка и сервис)
https://support.industry.siemens.com

Торговая площадка продуктов для Промышленности
https://mall.industry.siemens.com

Siemens Canada Ltd.
Digital Industries
Process Automation
300 Applewood Crescent
Concord, Ontario, L4K 4E5
Canada

© 2021 Siemens Canada Ltd.
Возможны изменения