

SIMATIC NET

Промышленные Ethernet- коммутаторы SCALANCE XB-200/XC-200/ XF-200BA/XP-200/XR-300WG Web

Руководство по проектированию

Введение

1

Описание

2

Рекомендации по сетевой
безопасности

3

Присвоение IP-адреса

4

Технические основы

5

Конфигурирование с
помощью функции Web
Based Management

6

Устранение неполадок /
FAQ

7

Приложение А

А

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:



ОПАСНО

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.



ОСТОРОЖНО

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

ВНИМАНИЕ

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

Оглавление

1	Введение	9
2	Описание	15
2.1	Свойства изделия.....	15
2.2	Системные функции и оборудование	17
2.3	Количественная структура	21
2.4	Требования к установке и эксплуатации	25
3	Рекомендации по сетевой безопасности	27
4	Присвоение IP-адреса	33
4.1	Структура IP-адреса	33
4.2	Первоначальное присвоение IP-адреса	34
4.3	Присвоение адреса через DHCP	36
5	Технические основы	37
5.1	PROFINET.....	37
5.2	EtherNet/IP	37
5.3	Режим резервирования.....	38
5.3.1	Spanning Tree.....	38
5.3.1.1	RSTP, MSTP, CIST	40
5.3.2	RSTP+	41
5.3.2.1	Свойства и функции RSTP+	41
5.3.2.2	Топология для RSTP+	41
5.3.2.3	Конфигурирование протокола RSTP+	44
5.3.2.4	Конфигурирование Spanning Tree для протокола RSTP+	45
5.3.2.5	Конфигурирование кольцевого резервирования для протокола RSTP+	46
5.3.2.6	Включение протокола RSTP+ и подсоединение проводов	47
5.3.3	HRP	47
5.3.4	MRP	49
5.3.4.1	MRP - Media Redundancy Protocol (протокол резервирования среды передачи данных)	49
5.3.4.2	Проектирование в системе WBM.....	51
5.3.4.3	Проектирование в ПО STEP 7	52
5.3.5	MRP Interconnection	58
5.3.5.1	Топология и принцип работы	58
5.3.5.2	Устройства для MRP Interconnection.....	60
5.3.5.3	Конфигурирование соединения MRP Interconnection	61
5.3.5.4	Соединение устройств и основная конфигурация.....	62
5.3.5.5	Конфигурация кольцевого резервирования	63
5.3.5.6	Конфигурация MRP Interconnection	65
5.3.6	Standby	70
5.3.7	Link Check	72

5.3.8	Parallel Redundancy Protocol (протокол параллельного резервирования)	74
5.3.9	Dual Network Access (DNA).....	74
5.3.10	Dual Network Access-Redundanz (DNA-Redundanz)	76
5.4	VLAN	81
5.4.1	Основы.....	81
5.4.2	Маркировка VLAN	82
5.4.3	Частная сеть VLAN.....	84
5.4.4	Tunnelling	86
5.5	Mirroring	87
5.6	SNMP	88
5.7	Quality of Service.....	90
5.8	NAT/NAPT	90
5.9	Single Hop Inter-VLAN Routing	93
6	Конфигурирование с помощью функции Web Based Management	95
6.1	Web Based Management.....	95
6.2	Авторизация.....	97
6.3	Меню «Information»	100
6.3.1	Стартовая страница.....	100
6.3.2	Версии	106
6.3.3	I&M	108
6.3.4	Таблица ARP.....	109
6.3.5	Log Table	110
6.3.6	Ошибки	112
6.3.7	Резервирование.....	113
6.3.7.1	Spanning Tree.....	113
6.3.7.2	Кольцевое резервирование	117
6.3.7.3	Standby	119
6.3.7.4	Link Check	121
6.3.7.5	MRP Interconnection.....	122
6.3.8	Ethernet Statistics	124
6.3.8.1	Interface Statistics.....	124
6.3.8.2	Packet Size.....	125
6.3.8.3	Frame Type	126
6.3.8.4	Packet Error	127
6.3.8.5	History.....	129
6.3.9	Unicast	130
6.3.10	Multicast	132
6.3.11	LLDP	133
6.3.12	Fiber Monitoring Protocol.....	135
6.3.13	Routing	137
6.3.13.1	Routing Table.....	137
6.3.13.2	NAT Translations	138
6.3.14	DHCP Server	139
6.3.15	Diagnostics	140
6.3.16	SNMP	143
6.3.17	Security	143
6.3.17.1	Overview	143

6.3.17.2	Supported Function Rights	146
6.3.17.3	Roles	147
6.3.17.4	Groups	148
6.3.17.5	802.1X Port Status	149
6.3.17.6	MAC-Auth. Address Table	150
6.4	Меню «System»	151
6.4.1	Configuration.....	151
6.4.2	General	157
6.4.2.1	Device	157
6.4.2.2	Coordinates	158
6.4.3	Agent IP.....	159
6.4.4	Restart.....	162
6.4.5	Load&Save.....	165
6.4.5.1	HTTP	166
6.4.5.2	TFTP	170
6.4.5.3	SFTP	174
6.4.5.4	Passwords.....	178
6.4.6	Events	179
6.4.6.1	Configuration.....	179
6.4.6.2	Severity Filter	183
6.4.7	SMTP Client	185
6.4.7.1	General	185
6.4.7.2	Receiver.....	188
6.4.8	DHCP	189
6.4.8.1	DHCP Client	189
6.4.8.2	DHCP Server	191
6.4.8.3	Port-IP Address Mapping	196
6.4.8.4	Port Range	198
6.4.8.5	DHCP Options	199
6.4.8.6	Relay Agent Information	202
6.4.8.7	Static Leases	203
6.4.8.8	Опции хоста	205
6.4.9	SNMP	206
6.4.9.1	Общая информация	207
6.4.9.2	SNMPv3 Users.....	210
6.4.9.3	SNMPv3 User to Group mapping	212
6.4.9.4	SNMPv3 Access.....	213
6.4.9.5	SNMPv3 Views	215
6.4.9.6	Notifications	217
6.4.10	System Time	219
6.4.10.1	Manual Setting	219
6.4.10.2	DST Overview	220
6.4.10.3	DST Configuration	222
6.4.10.4	SNTP Client.....	225
6.4.10.5	NTP Client.....	229
6.4.10.6	SIMATIC Time Client	232
6.4.10.7	PTP-Client	234
6.4.11	Automatic Logout	235
6.4.12	Конфигурация кнопки SELECT/SET	236
6.4.13	Syslog Client.....	237
6.4.14	Ports.....	239
6.4.14.1	Overview	239

6.4.14.2	Configuration.....	243
6.4.15	Fault Monitoring	252
6.4.15.1	Power Supply.....	252
6.4.15.2	Link Change.....	253
6.4.15.3	Redundancy.....	254
6.4.16	PROFINET.....	255
6.4.17	EtherNet/IP	257
6.4.17.1	EtherNet/IP	257
6.4.17.2	DLR Status	258
6.4.18	Модуль PLUG	260
6.4.18.1	Configuration.....	260
6.4.19	Ping.....	263
6.4.20	DCP Discovery.....	264
6.4.21	Power over Ethernet (PoE).....	266
6.4.21.1	General	266
6.4.21.2	Port	267
6.4.21.3	Schedule	270
6.4.22	Port Diagnostics.....	272
6.4.22.1	Cable Tester	272
6.4.22.2	SFP Diagnostics.....	273
6.5	Меню «Layer 2»	276
6.5.1	Configuration.....	276
6.5.2	Quality of Service (QoS)	280
6.5.2.1	General	281
6.5.2.2	CoS Map	282
6.5.2.3	DSCP Mapping	283
6.5.2.4	QoS Trust.....	285
6.5.2.5	CoS Port Remap	287
6.5.3	Rate Control.....	288
6.5.4	VLAN	290
6.5.4.1	Общая информация	290
6.5.4.2	GVRP	296
6.5.4.3	VLAN на базе портов	297
6.5.5	Private VLAN.....	300
6.5.5.1	General	300
6.5.5.2	IP Interface Mapping	301
6.5.6	Provider Bridge	303
6.5.6.1	Туннельные порты	303
6.5.7	Mirroring	305
6.5.7.1	General	305
6.5.7.2	Порт.....	308
6.5.8	Dynamic MAC Aging	309
6.5.9	Ring Redundancy	311
6.5.9.1	Ring.....	311
6.5.9.2	Standby	318
6.5.9.3	Link Check	321
6.5.9.4	MRP-Interconnection.....	324
6.5.10	Spanning Tree.....	327
6.5.10.1	Общая информация	327
6.5.10.2	CIST General	329
6.5.10.3	Порт CIST	331
6.5.10.4	MST General	336

6.5.10.5	MST Port.....	338
6.5.10.6	Enhanced Passive Listening Compatibility.....	340
6.5.11	Loop Detection	340
6.5.12	Link Aggregation	343
6.5.12.1	General	343
6.5.12.2	Время ожидания LACP	346
6.5.13	DCP Forwarding	347
6.5.14	LLDP.....	349
6.5.15	Fiber Monitoring Protocol.....	350
6.5.16	Unicast	353
6.5.16.1	Фильтрация	353
6.5.16.2	Locked Ports	355
6.5.16.3	Обучение	357
6.5.16.4	Blocking	358
6.5.17	Multicast	360
6.5.17.1	Groups	360
6.5.17.2	IGMP	363
6.5.17.3	GMRP	366
6.5.17.4	Блокировка многоадресной рассылки.....	368
6.5.18	Broadcast.....	369
6.5.19	PTP.....	371
6.5.19.1	General	371
6.5.19.2	TC основное	371
6.5.19.3	TC Port.....	372
6.5.20	RMON.....	374
6.5.20.1	Statistics	374
6.5.20.2	История	376
6.6	Меню «Layer 3»	378
6.6.1	Subnets	378
6.6.1.1	Overview	378
6.6.1.2	Configuration.....	381
6.6.1.3	Default Gateway	382
6.6.2	DHCP Relay Agent	383
6.6.2.1	General	383
6.6.2.2	Option	384
6.6.3	NAT	387
6.6.3.1	NAT	387
6.6.3.2	Static	389
6.6.3.3	Pool.....	391
6.6.3.4	NAPT	392
6.7	Меню «Security»	394
6.7.1	Управление пользователями.....	394
6.7.2	User.....	396
6.7.2.1	Local Users	396
6.7.2.2	Roles	399
6.7.2.3	Groups	400
6.7.3	Пароли	402
6.7.3.1	Пароли	402
6.7.3.2	Options	404
6.7.4	AAA.....	405
6.7.4.1	General	405

6.7.4.2	RADIUS Client	406
6.7.4.3	Аутентификация пользователей 802.1X	410
6.7.5	Management ACL	415
6.7.6	Brute Force Prevention	418
7	Устранение неполадок / FAQ	423
7.1	Загрузка новой прошивки через протокол TFTP без WBM и CLI.....	423
7.2	Сообщения: SINEMA Configuration not accepted yet	424
7.3	Обмен данными конфигурации через файл с ПО STEP7 Basic/Professional.....	425
A	Приложение А	427
	Указатель	443

Введение

Область применения этого руководства по проектированию

Это руководство по проектированию касается следующих изделий:

- SCALANCE XB-200
- SCALANCE XC-200
- SCALANCE XF-200BA
- SCALANCE XP-200
- SCALANCE XR-300WG

Далее эти изделия обозначаются также как промышленный Ethernet-коммутатор, устройство или сетевые компоненты.

Некоторые устройства имеют два варианта с разными артикулами. Оба варианта различаются только своими заводскими настройками. Все другие свойства одинаковые.

Руководство по проектированию действует для следующих версий ПО:

- SCALANCE XB-200 Микропрограммное обеспечение начиная с версии 4.3.1
- SCALANCE XC-200 Микропрограммное обеспечение начиная с версии 4.3.1
- SCALANCE XF-200BA Микропрограммное обеспечение начиная с версии 4.3.1
- SCALANCE XP-200 Микропрограммное обеспечение начиная с версии 4.3.1
- SCALANCE XR-300WG Микропрограммное обеспечение начиная с версии 4.3.1

Заводские настройки

Варианты PROFINET

- Протокол Industrial Ethernet: PROFINET
- Базовый режим моста: 802.1D Transparent Bridge
- Процедура резервирования: Кольцевое резервирование
- Режим определения приоритетов: Trust COS
- IGMP Snooping/IGMP Querier: Выкл.
- Распознавание конфликтов IPv4-адресов: Never give up

Варианты EtherNet/IP

- Протокол Industrial Ethernet: EtherNet/IP
- Базовый режим моста: 802.1Q VLAN Bridge
- Процедура резервирования: RSTP

- Режим определения приоритетов: Trust COS-DSCP
- IGMP Snooping/IGMP Querier: Вкл.
- Распознавание конфликтов IPv4-адресов: Attempt to defend

Профиль промышленного Industrial Ethernet

- Протокол Industrial Ethernet: PROFINET
- Базовый режим моста: 802.1Q VLAN Bridge
- Процедура резервирования: RSTP
- Режим определения приоритетов: Trust COS-DSCP
- IGMP Snooping/IGMP Querier: Выкл.
- Распознавание конфликтов IPv4-адресов: Never give up

Используемые обозначения

Классификация	Описание	Используемые обозначения
Группа изделий	Если информация касается всех устройств и вариантов одной группы изделий, используется название группы изделий.	Например, SCALANCE XC-200
Устройство	Если информация касается какого-либо специфического устройства, используется название этого устройства.	Например, SCALANCE XC206-2SFP
Группа устройств	Если информация касается какой-либо специфичной группы устройств, используется соответствующее сокращение.	-
	Если информация касается всех гигабитных вариантов устройства SCALANCE XC-200, используется следующее понятие.	SCALANCE XC-200G

Назначение данного руководства по проектированию

Настоящее руководство по проектированию предназначено для того, чтобы помочь пользователю ввести промышленный Ethernet-коммутатор в эксплуатацию и управлять им. Он даёт необходимые значения для конфигурации промышленного Ethernet-коммутатора.

Включение в комплект документации

Для изделий кроме настоящего руководства по проектированию имеются ещё следующие документы:

- Руководство по проектированию «SCALANCE XB-200/XC-200/XF-200BA/XP-200/XR-300WG Command Line Interface»
Данный документ содержит CLI-команды, поддерживаемые промышленным Ethernet-коммутатором.
- Инструкция «SCALANCE XB-200», «SCALANCE XC-200», «SCALANCE XF-200BA», «SCALANCE XP-200» и «SCALANCE XR-300WG»
Эти документы содержат информацию о монтаже, подключении и допусках изделий.

Документацию можно найти:

- На носителе данных, прилагаемом к некоторым изделиям:
 - CD/DVD для изделия
 - Сборник руководств SIMATIC NET
- На интернет-страницах онлайн-сервиса Siemens Industry Online Support под пунктами:
 - SCALANCE XB-200 (<https://support.industry.siemens.com/cs/ww/en/ps/15291/man>)
 - SCALANCE XC-200 (<https://support.industry.siemens.com/cs/ww/en/ps/24185/man>)
 - SCALANCE XF-200BA (<https://support.industry.siemens.com/cs/ww/en/ps/15287/man>)
 - SCALANCE XP-200 (<https://support.industry.siemens.com/cs/ww/en/ps/21869/man>)
 - SCALANCE XR-300WG (<https://support.industry.siemens.com/cs/ww/en/ps/15296/man>)

Дополнительная документация

В системных руководствах «Industrial Ethernet / PROFINET Industrial Ethernet» и «Industrial Ethernet / PROFINET, пассивные сетевые компоненты» приводятся указания по другим изделиям SIMATIC NET, которые можно использовать вместе с устройствами данной линейки изделий в сети Industrial Ethernet.

В них можно также найти оптические характеристики партнёров связи, необходимых для установки.

Системные руководства можно найти:

- На носителе данных, прилагаемом к некоторым изделиям:
 - CD/DVD для изделия
 - Сборник руководств SIMATIC NET
- На интернет-страницах онлайн-сервиса Siemens Industry Online Support.
 - Системное руководство Industrial Ethernet / PROFINET Industrial Ethernet (<https://support.industry.siemens.com/cs/ww/en/view/27069465>)
 - Системное руководство Industrial Ethernet / PROFINET, пассивные сетевые компоненты (<https://support.industry.siemens.com/cs/ww/en/view/84922825>)

Руководства SIMATIC NET

Руководства SIMATIC NET можно найти:

- На носителе данных, прилагаемом к некоторым изделиям:
 - CD/DVD для изделия
 - Сборник руководств SIMATIC NET
- На интернет-страницах онлайн-сервиса Siemens Industry Online Support (<https://support.industry.siemens.com/cs/ww/en/ps/15247>).

Что нового в устройствах с версии 4.3?

Далее приводится обзор важных функциональных расширений.

- Два соединения режима MRP Interconnection на каждое устройство в некоторых вариантах устройств
- Конфигурирование максимального числа абонентов на каждый порт (Страница 243)
- Поддержка индивидуального пользовательского ключа SSH (Страница 178)
- Временное ограничение для PoE (Страница 270)
- Расширенная конфигурация SNMP (Страница 206)
- Множественные кольца MRP (Страница 311)
- Конфигурируемые правила назначения паролей (Страница 404)
- Brute Force Prevention (Страница 418)

См. также

Diagnostics (Страница 140)

Глоссарий SIMATIC NET

Глоссарий SIMATIC NET описывает технические термины, которые могут использоваться в этом документе.

Глоссарий SIMATIC NET можно найти в службе поддержки Siemens Industry Online по следующему адресу:

50305045 (<https://support.industry.siemens.com/cs/ww/en/view/50305045>)

Указания по безопасности

Siemens предоставляет продукты и решения для обеспечения промышленной безопасности при эксплуатации производственных комплексов, систем, рабочих станций и сетей.

Для защиты производственных комплексов, систем, машинного оборудования и сетей от киберугроз необходимо внедрение и поддержка комплексной высокотехнологичной модели промышленной безопасности. Продукты и решения Siemens являются одним из компонентов такой модели.

За предотвращение несанкционированного доступа к производственным комплексам, системам, рабочим станциям и сетям клиента несет ответственность клиент. Доступ систем, рабочих станций и их компонентов к корпоративной сети или сети Интернет должен быть организован только в необходимой степени и с применением соответствующих локальных мер безопасности (например, использование брандмауэров и/или деление сети на подсети).

Для получения дополнительных сведений о возможных мерах промышленной безопасности см.

<https://www.siemens.com/industrialsecurity> (<https://www.siemens.com/industrialsecurity>)

Продукты и решения Siemens постоянно совершенствуются для обеспечения максимальной степени безопасности. Siemens настоятельно рекомендует выполнять обновления сразу после их выпуска и всегда использовать самые последние версии продуктов. Использование неподдерживаемых версий продуктов и неприменение последних обновлений повышает риск киберугроз для клиента.

Для получения сведений об обновлениях продуктов, подпишитесь на RSS-канал Siemens по промышленной безопасности:

<https://www.siemens.com/industrialsecurity> (<https://www.siemens.com/industrialsecurity>)

Примечание о поддержке микропрограммного /программного обеспечения

Компания Siemens предоставляет исправления ошибок безопасности только для последней обновлённой версии микропрограммного /программного обеспечения. Это означает, что компания Siemens обеспечивает проверку только текущую версию микропрограммного /программного обеспечения на предмет уязвимостей.

Условия лицензирования

Примечание

Программное обеспечение с открытым исходным кодом

Прежде чем начать использовать устройство, внимательно прочтите условия лицензирования программного обеспечения с открытым исходным кодом.

Условия лицензирования можно загрузить в WBM на странице «System > Load&Save > Copyright».

Марка

Следующие обозначения, в том числе те, которые не отмечены символом зарегистрированного товарного знака ®, являются зарегистрированными товарными знаками компании Siemens AG:

SCALANCE, C-PLUG, OLM

Микропрограммное обеспечение

Микропрограммное обеспечение зашифровано и закодировано. Предусмотрены меры для того, чтобы разрешить загрузку в устройство только микропрограммного обеспечения, созданного компанией Siemens.

Описание

2.1 Свойства изделия

Промышленные Ethernet-коммутаторы имеют следующие свойства:

- Интерфейсы Ethernet поддерживают следующие режимы работы и состояния.
 - 10 Мбит/с и 100 Мбит/с каждый в дуплексном и полудуплексном режиме
 - 1000 Мбит/с в дуплексном режиме (SCALANCE XC206-2SFP с соответствующими вставными трансиверами, SCALANCE XC-200G, SCALANCE XP216 и SCALANCE XR-300WG)
 - 10 Гбит/с в дуплексном режиме (SCALANCE XC-200G PoE, SCALANCE XC-200G EEC und SCALANCE XR-300PoE WG с соответствующими вставными трансиверами)
 - Автоматическое определение сети
 - Автокроссинг (Auto-Crossing)
 - Автоматическое определение полярности (Auto-Polarity)
- EtherNet/IP
EtherNet/IP (Ethernet/Industrial Protocol) — открытый промышленный стандарт для промышленной сети Ethernet реального времени, основанный на TCP/IP и UDP/IP.
- PROFINET
PROFINET (Process Field Network) — открытый промышленный стандарт для промышленной сети Ethernet реального времени, основанный на TCP/IP и стандартах ИТ. С помощью сети PROFINET можно подсоединять децентрализованные периферийные устройства к контроллеру.
- Процедура резервирования Spanning Tree Protocol
Процедура резервирования Spanning Tree задаёт в сети несколько путей соединения между абонентами сети, из которых активен только один. В результате этого подавляются петли и оптимизируются пути.
- Виртуальные сети (VLAN)
Для структурирования промышленных сетей Ethernet с существенным ростом числа абонентов имеющуюся физическую сеть можно подразделять на несколько виртуальных подсетей.
- Ограничение нагрузки протоколов при использовании многоадресных протоколов и протоколов широковещательной передачи, например передачи видеосигналов
Путём настройки многоадресных источников и целей (IGMP-Snooping, IGMP-Querier) промышленные Ethernet-коммутаторы могут фильтровать многоадресный обмен данными и тем самым ограничивать нагрузку в сети. Возможно ограничение многоадресного и широковещательного обмена данными.

2.1 Свойства изделия

- Синхронизация времени
Диагностические сообщения, как например записи в таблицах журналов или электронных письмах, отмечаются временными отметками. Локальное время путём синхронизации с передатчиком времени SICLOCK или сервером SNTP/NTP едино во всей сети, что облегчает координацию диагностических сообщений нескольких устройств. Кроме этого, синхронизация времени поддерживается через протокол точного времени (PTP, IEEE 1588).
- Устройства с питанием через сеть Ethernet (PoE)
с обозначением «PoE» в обозначении типа поддерживают питание через сеть Ethernet.
- Качество и класс предоставляемых услуг передачи данных (Quality of Service) для классификации обмена данными согласно CoS (класс сервиса (Class of Service) - IEEE 802.11Q) и DSCP (кодированная точка дифференцированного обслуживания (Differentiated Services Code Point) - RFC 2474)
- Зеркалирование портов (Port Mirroring)
Зеркалирование портов позволяет трафик одного порта отображать на другой порт (порт мониторинга). На порте мониторинга затем можно анализировать трафик без обратного влияния.
- Защита доступа к сети согласно стандарту IEEE 802.1X
Порты можно конфигурировать для конечных устройств, поддерживающие аутентификацию согласно IEEE 802.1X. Аутентификация выполняется через RADIUS-сервер, который должен быть доступен по сети.
- Таблица журнала
В таблице журнала протоколируются события, возникающие во время работы устройства. Пользователь может установить, какие события приводят к их записи в таблице журнала.
- Агрегирование каналов (Link Aggregation) (IEEE 802.1AX) для объединения портов (SCALANCE XC-200/SCALANCE XP-200)
- Поддержка H-Sync
Дополнительную информацию см. главу «Ring (Страница 311)»

- Устройства S2 (конфигурация сети PROFINET с простым резервированием системы)
Устройства S2 могут устанавливать два соединения с автоматизированной системой, по одной взаимосвязи приложений (AR) с обоими контроллерам ввода-вывода данных. Когда прерывается одно коммуникационное соединение, все данные и диагностические функции доступны по-прежнему через второе соединение. Какие промышленные Ethernet-коммутаторы можно использовать в качестве устройства S2 см. главу «Системные функции и аппаратное обеспечение». Конфигурирование устройств S2 выполняется только с помощью ПО STEP 7 Basic или Professional.
Дополнительную информацию см. также: PROFINET в устройствах SIMATIC PCS 7 (<https://support.industry.siemens.com/cs/ww/en/view/72887082>)
- Поддержка функций CiR/H-CiR (конфигурирование в рабочем режиме)
Configuration in Run (CiR) — функция для конфигурирования оборудования и изменения конфигураций в рабочем режиме. Эта функция доступна в различном объеме как для стандартных автоматизированных систем, так и для H-систем (H-CiR). Какие промышленные Ethernet-коммутаторы поддерживают CiR, см. главу «Системные функции и аппаратное обеспечение». Конфигурирование CiR выполняется только с помощью ПО STEP 7 Basic или Professional.
Дополнительную информацию см. также: PROFINET в устройствах SIMATIC PCS 7 (<https://support.industry.siemens.com/cs/ww/en/view/72887082>)

2.2 Системные функции и оборудование

Доступность системных функций

В следующей таблице показана доступность системных функций на промышленных Ethernet-коммутаторах. Обратите внимание, что в этом руководстве по проектированию и онлайн-справке приводится описание всех функций. В зависимости от вашего промышленного Ethernet-коммутатора некоторые функции могут быть недоступны.

Мы оставляем за собой право на технические изменения.

		SCALANCE XB-200	SCALANCE XR-300WG	SCALANCE XC-200	SCALANCE XP-200	SCALANCE XF-200BA
Информация	Таблица ARP	✓	✓	✓	✓	✓
	Таблица журнала	✓	✓	✓	✓	✓
	Статистика Ethernet	✓	✓	✓	✓	✓
	Диагностика (температура)	-	✓	✓	✓	✓

2.2 Системные функции и оборудование

		SCALANCE XB-200	SCALANCE XR-300WG	SCALANCE XC-200	SCALANCE XP-200	SCALANCE XF-200BA
Система	SMTP-клиент	✓	✓	✓	✓	✓
	DHCP-клиент	✓	✓	✓	✓	✓
	DHCP-сервер	✓ ¹⁾	✓ ¹⁾	✓	✓	✓
	SNMP	✓	✓	✓	✓	✓
	Ручная настройка времени	✓	✓	✓	✓	✓
	DST	✓	✓	✓	✓	✓
	SNTP	✓	✓	✓	✓	✓
	NTP	✓	✓	✓	✓	✓
	SIMATIC Time Client	✓	✓	✓	✓	✓
	Автом. выход из системы	✓	✓	✓	✓	✓
	Syslog Client	✓	✓	✓	✓	✓
	Функции NOA-коммутатора	-	-	✓ ⁴⁾	-	-
	Контроль ошибок	✓	✓	✓	✓	✓
	PROFINET	✓	✓	✓	✓	✓
	EtherNet/IP	✓	✓	✓	✓	✓ ²⁾
	Тестер кабеля	✓	✓	✓	✓	✓
	Диагностика SFP	-	✓	✓	-	-

		SCALANCE XB-200	SCALANCE XR-300WG	SCALANCE XC-200	SCALANCE XP-200	SCALANCE XF-200BA
Уро- вень 2	Приоритеты отправки	-	-	✓	✓	✓
	Присвоение CoS	✓	✓	✓	✓	✓
	Присвоение DSCP	✓	✓	✓	✓	✓
	Определение приоритетов QoS	✓	✓	✓	✓	✓
	Новое присвоение портов CoS	-	-	✓	✓	✓
	Контроль скорости	✓	✓	✓	✓	✓
	GVRP	-	-	✓	✓	✓
	VLAN на базе портов	✓	✓	✓	✓	✓ ²⁾
	Частная сеть VLAN	-	-	✓	✓	-
	Provider Bridge	-	-	✓	✓	-
	Switch-Port VLAN Trunk	-	-	✓	✓	✓ ²⁾
	Зеркалирование на ба- зе порта	✓	✓	✓	✓	✓
	Dynamic MAC Aging	✓	✓	✓	✓	✓
	Кольцевое резервиро- вание	✓	✓	✓	✓	✓
	Поддержка H-Sync	-	-	✓	✓	✓
	Устройства S2	-	-	✓	✓	✓
	Поддержка CiR/H-CiR	-	-	✓	✓	✓
	Кольцевая сеть с RSTP	✓	✓	✓	✓	✓
	Standby (HRP)	✓	✓	✓	✓	✓
	Наблюдатель (HRP)	-	-	✓	✓	✓
	Link Check	✓	✓	✓	-	✓
	Множественные кольца MRP	✓	✓	✓	✓	-
	MRP Interconnection	✓	✓	✓	✓	✓
	Spanning Tree	✓	✓	✓	✓	✓
	RSTP	✓	✓	✓	✓	✓
	RSTP+	✓	✓	✓	✓	✓
	MSTP	-	-	✓	✓	-
	Enhanced Passive Listening Compatibility	✓	✓	✓	✓	✓
	Loop Detection	✓	✓	✓	✓	✓
	Link Aggregation	-	-	✓	✓	✓
	Переадресация DCP	✓	✓	✓	✓	✓
	LLDP	✓	✓	✓	✓	✓
	Мониторинг волокна	-	-	✓	-	-
	Одноадресный фильтр (Unicast-Filter)	✓	✓	✓	✓	✓
	Заблокированные порты	✓	✓	✓	✓	✓

2.2 Системные функции и оборудование

		SCALANCE XB-200	SCALANCE XR-300WG	SCALANCE XC-200	SCALANCE XP-200	SCALANCE XF-200BA
	Одноадресное программирование	✓	✓	✓	✓	✓
	Одноадресная блокировка	✓	✓	✓	✓	✓
	Многоадресные группы	✓	✓	✓	✓	✓
	IGMP	✓	✓	✓	✓	✓
	GMRP	-	-	✓	✓	✓
	Многоадресная блокировка	✓	✓	✓	✓	✓
	Широковещательная блокировка	✓	✓	✓	✓	✓
	PTP	-	-	✓ ³⁾	-	-
	RMON	✓	✓	✓	✓	✓
	История RMON	✓	✓	✓	✓	✓
Уровень 3	Single Hop Inter-VLAN Routing	-	-	✓	✓	-
	DHCP Relay Agent	✓	✓	✓	✓	✓
	Общий адрес агента	-	-	✓	✓	-
	NAT/NAPT	-	-	✓	✓	-
Security	Пользователь	✓	✓	✓	✓	✓
	Пароли	✓	✓	✓	✓	✓
	RADIUS-аутентификация	✓	✓	✓	✓	✓
	MAC-аутентификация	-	✓	✓	✓	✓
	Guest VLAN	-	-	✓	✓	✓
	Повторная аутентификация 802.1X	✓	✓	✓	✓	✓
	Management ACL	✓	✓	✓	✓	✓
	Brute Force Prevention	✓	✓	✓	✓	✓

¹⁾ Ограниченный

²⁾ Не для устройств DNA

³⁾ Только SCALANCE XC-200G

⁴⁾ Только SCALANCE XC-200G EEC

Доступность аппаратного обеспечения

В следующей таблице показано аппаратное обеспечение промышленных Ethernet-коммутаторов.

Мы оставляем за собой право на технические изменения.

	SCALANCE XB-200	SCALANCE XR-300WG	SCALANCE XC-200	SCALANCE XP-200	SCALANCE XF-200BA
Поддержка карты памяти C-PLUG	-	-	✓	✓	✓
Кнопка SELECT/SET	-	-	✓ ²⁾ ³⁾	✓ ³⁾	-
Кнопка RESET	✓ ²⁾	✓ ²⁾	-	✓ ²⁾	-
Кнопка SET	-	-	-	-	✓ ²⁾
Сигнальный контакт	-	-	✓	✓	✓
Последовательный интерфейс	✓	✓	✓	✓	-
Режимы индикации	-	-	✓	✓	-
Гнёзда вставного трансивера	-	-	✓	-	-
Порты Combo	-	✓	✓	-	-
Гнёзда шинного адаптера	-	-	-	-	✓
Питание через сеть Ethernet	-	✓ ¹⁾	✓ ¹⁾	✓ ¹⁾	-

¹⁾ Обозначение «PoE» в имени устройства

Функция кнопок

²⁾ Сброс на заводские настройки

³⁾ Активация сигнальной маски

2.3 Количественная структура

Количественная структура устройства

В следующей таблице приведена количественная структура для системы управления на базе Web (Web Based Management) и интерфейса с командной строкой (Command Line Interface) устройства.

2.3 Количественная структура

В зависимости от вашего промышленного Ethernet-коммутатора некоторые функции могут быть недоступны.

	Конфигурируемая функция	Максимальное количество				
		SCALANCE XB-200	SCALANCE XR-300WG	SCALANCE XC-200	SCALANCE XP-200	SCALANCE XF-200BA
Система	Максимальный размер кадра (Ingress)	1632 байта	10 кбайт	1632 байта / 2048 байтов / 10 кбайт ⁷⁾	1632 байта / 10 кбайт ⁸⁾	1632 байта
	Syslog-сервер	3				
	Сервер эл. почты	3				
	Группы DHCP	16 ¹⁾	28 ¹⁾	24		
	IPv4-адреса на каждую группу DHCP	1		24		
	IPv4-адреса, которые управляют DHCP-сервером (динамический + статический)	16 ¹⁾	28 ¹⁾	576		
	DHCP статические присвоения на каждую группу DHCP	-		24		
	SNMPv1 получатель ловушки	10				
	Пользователи SNMPv3	48				
	SNMPv3 группы	41				
	Виды SNMPv3 (вкл. 2 вида по умолчанию)	46				
	SNTP-сервер	1				
	NTP-сервер	-		1 ⁹⁾		
	Интерфейсы агента/TIA ²⁾	1				
	Показанные устройства через DCP Discovery	100				

	Конфигурируемая функция	Максимальное количество				
		SCALANCE XB-200	SCALANCE XR-300WG	SCALANCE XC-200	SCALANCE XP-200	SCALANCE XF-200BA
Уровень 2	Очередь по приоритету QoS	4		4/8 ⁶⁾	4	
	Виртуальные сети LAN (на базе портов, включая VLAN 1)	257 ^{3) 10)}				
	Частная сеть VLAN	-		1		-
	Первичные сети PVLAN	-		1		-
	Вторичные изолированные сети PVLAN	-		24		-
	Вторичные общественные сети PVLAN	-		256		-
	Сеансы зеркалирования	1				
	Порты Standby	1				
	Кольцевые сети MRP	4				1
	Сконфигурированные соединения MRP Interconnection	64				
	Активированные соединения MRP Interconnection	1		2		
	Максимальное количество устройств с активированным соединением MRP Interconnection в одной кольцевой сети	10				
	Множественные экземпляры Spanning Tree	-		4		-
	Агрегирования каналов	-		4/8 ⁵⁾		
	Порты в агрегировании каналов	-		8		4
	Статические индивидуальные адреса	128				
	Статические групповые адреса без активированного GMRP	256				
	Статические групповые адреса с активированным GMRP	-		50		
	Адреса, запрограммированные через IGMP-отслеживание	512				
Уровень 3	VLAN-IP-интерфейсы	1		24		1
	Интерфейсы агента ретрансляции DHCP	1		24		1
	Сервер агента ретрансляции DHCP	4				
	NAT-интерфейсы	-		1		-
	Динамические конфигурации NAT (группы)			100		
	Статические конфигурации NAT	-		100		-

2.3 Количественная структура

	Конфигурируемая функция	Максимальное количество				
		SCALANCE XB-200	SCALANCE XR-300WG	SCALANCE XC-200	SCALANCE XP-200	SCALANCE XF-200BA
Security	Пользователь	30 (вкл. настроенного заводом-изготовителем пользователя «admin»)				
	Роли	29				
	Группы	32				
	IP-адреса RADIUS-серверов	6				
	Одновременные MAC-аутентификации (аутентификация и блокировка) на каждое устройство ⁴⁾	-		2000		
	Одновременные MAC-аутентификации (аутентификация и блокировка) на каждый порт (конфигурируемый) ⁴⁾	-	200			
	Управление ACLs (правила доступа для управления)	10				

- ¹⁾ В устройствах SCALANCE XB-200 и SCALANCE XR-300WG количество групп DHCP и управляемых IPv4-адресов зависит от количества портов. Количество портов соответствует максимальному числу групп DHCP и управляемых IPv4-адресов.
- ²⁾ Здесь речь идёт об IP-интерфейсе.
- ³⁾ Устройства с Y-функциональностью не поддерживают сети VLAN.
- ⁴⁾ Если превышаете максимальное число MAC-аутентификаций на каждое устройство, сбрасываются все MAC-аутентификации порта, на котором было превышено значение.
Если превышаете максимальное число MAC-аутентификаций на каждый порт, сбрасываются все MAC-аутентификации этого порта.
- ⁵⁾ Для устройств группы изделий SCALANCE XC-200 и SCALANCE XP-200 действует следующее условие.
Так как одно агрегирование каналов состоит по меньшей мере из 2 портов, то максимальное количество агрегирования каналов зависит от количества портов. В устройствах до 8 портов возможно создание не более 4 агрегирований каналов, в устройствах, имеющих более 8 портов, возможно создание не более 8 агрегирований каналов.
- ⁶⁾ Устройства группы изделий SCALANCE XC-200G поддерживают 8 очередей. Все другие устройства XC-200 поддерживают 4 очереди.
- ⁷⁾ В следующих устройствах максимальный размер кадра (Ingress) составляет 2048 байт:
- устройства с портами Combo (добавление «С» в обозначении типа);
- варианты PoE (добавление «PoE» в обозначении типа).
Следующие устройства поддерживают кадры Jumbo размером 10 кбайт:
- все гигабитные варианты (дополнение «G» в обозначении типа), в том числе такие с портами Combo.
- все устройства, поддерживающие питание через сеть Ethernet (добавление «PoE» в обозначении типа);
- SCALANCE XC216-4C
Во всех других устройствах XC-200 максимальный размер кадра (Ingress) составляет 1632 байта.
- ⁸⁾ Гигабитные порты устройства SCALANCE XP-200 поддерживают кадры Jumbo размером 10 кбайт. Во всех других портах максимальный размер кадра составляет 1632 байт.
- ⁹⁾ Максимальное количество NTP/SNTP-серверов, которые можно сконфигурировать для устройств SCALANCE XB-200/XR-300WG/XC-200/XP-200/XF-200BA.
- ¹⁰⁾ Чтобы избежать возможных сбоев в работе сети, настройте в качестве участников кольца максимум до 35 VLAN (MRP-кольцо, HRP-кольцо, резервное соединение). Обратите внимание, что это рекомендация. При конфигурировании нет автоматического ограничения.

2.4 Требования к установке и эксплуатации

Требования к установке и эксплуатации промышленных Ethernet-коммутаторов

Для конфигурирования промышленного Ethernet-коммутатора необходимо наличие программатора/ПК с подключением к сети. Если DHCP-сервер недоступен, для первоначального присвоения IP-адреса промышленному Ethernet-коммутатору требуется программатор/ПК (PG/PC), на котором установлено ПО SINEC PNI. Для дальнейшего конфигурирования необходим программатор/ПК с Telnet или интернет-браузером.

См. также

Первоначальное присвоение IP-адреса (Страница 34)

2.4 Требования к установке и эксплуатации

Рекомендации по сетевой безопасности

Программное обеспечение (функции безопасности)

- Своевременно устанавливайте обновления прошивки. Регулярно проверяйте информацию о наличии обновлений устройства, касающихся безопасности. Информацию об этом можно найти на интернет-страницах по промышленной безопасности Industrial Security (<https://www.siemens.com/industrialsecurity>).
- Регулярно проверяйте информацию о наличии рекомендаций по безопасности, которые публикуются Siemens ProductCERT (<https://www.siemens.com/cert/en/cert-security-advisories.htm>).
- Активируйте только те протоколы, которые необходимы для эксплуатации устройства.
- Ограничьте доступ к управлению устройством с помощью правил в списке управления доступом (Management ACL - Access Control List).
- Возможность структурирования сети VLAN позволяет защищать от DoS-атак и несанкционированного доступа. Проверьте, целесообразно ли это для вашей среды.
- Пользуйтесь центральным сервером регистрации для протоколирования изменений и доступа. Используйте сервер регистрации только в пределах защищённой сетевой зоны и регулярно проверяйте информацию регистрации.

Аутентификация

Примечание

Риск доступности — риск потери данных

Не теряйте пароли к устройству. Доступ к устройству можно восстановить только путем сброса устройства до заводских настроек, при котором будут удалены имеющиеся данные конфигурации.

- Перед использованием устройства замените пароли по умолчанию для всех учетных записей пользователей, режимов доступа и приложений (если возможно).
- Установите правила для создания паролей.
- Используйте сложные пароли. Не используйте слабые пароли (например, password1, 123456789, abcdefgh) или повторяющиеся комбинации символов (например, abcabc).
Данная рекомендация также применима для симметричных паролей/ключей, сконфигурированных на устройстве.
- Убедитесь, что пароли защищены и доступны только уполномоченному персоналу.
- Не используйте одни и те же пароли для нескольких имен пользователей и систем.
- Храните пароли в надежном месте (не в сети), чтобы они были под рукой при потере.

- Регулярно обновляйте пароли, чтобы повысить уровень безопасности.
- Пароль следует изменять, как только он становится известен неуполномоченным лицам, или при наличии подозрения на это.
- Если аутентификация пользователя выполняется через протокол RADIUS, убедитесь, что все коммуникации проходят в безопасной среде или осуществляются через безопасный канал.
- Обратите внимание на протоколы канального уровня, которые не предлагают собственной аутентификации между конечными точками, такие как протоколы ARP или IPv4. Злоумышленник может использовать уязвимости в этих протоколах для атаки на узлы, коммутаторы и маршрутизаторы, подключенные к вашей сети уровня 2, например, используя манипуляции («отравляя») кэши ARP систем в подсети, а затем перехватывая трафик данных. Должны быть приняты надлежащие меры безопасности для незащищенных протоколов уровня 2, чтобы предотвратить несанкционированный доступ к сети. Кроме того, можно ограничить физический доступ к локальной сети или использовать безопасные протоколы более высокого уровня.

Ключи и сертификаты

- Устройство имеет предустановленный сертификат X.509 с ключом. Замените данный сертификат на самостоятельно созданный сертификат с ключом. Используйте сертификат, подписанный надежным внешним или внутренним центром сертификации. Вы сможете установить сертификат, используя веб-интерфейс (System > Load and Save).
- Воспользуйтесь органом сертификации, включая возможности отзыва ключа и управления им, для подписания сертификатов.
- Убедитесь, что все установленные пользователями пароли хранятся в безопасном месте и недоступны для неуполномоченных лиц.
- Если есть подозрение на нарушение безопасности, немедленно замените все сертификаты и ключи.
- Используйте защищенные паролем сертификаты в формате «PKCS # 12».
- Мы рекомендуем использовать сертификаты с длиной ключа 4096 бит.
- Выполните верификацию сертификатов на основании отпечатков пальцев на стороне сервера и клиента, чтобы предотвратить атаки через посредников. Используйте для этого второй безопасный путь передачи.
- Прежде чем отправить устройство обратно в компанию Siemens для ремонта, замените текущие сертификаты и ключи временными одноразовыми сертификатами и ключами, которые могут быть удалены при возврате устройства.

Безопасные/небезопасные протоколы и службы

- Не пользуйтесь или деактивируйте небезопасные протоколы и службы, например HTTP, Telnet и TFTP. Такие протоколы доступны по причине эксплуатации давно выпущенного оборудования, однако не предусмотрены для безопасного применения. Используйте небезопасные протоколы на устройстве в исключительных случаях и осторожно.
- Проверьте необходимость применения следующих протоколов и служб:
 - Порты без аутентификации и без кодировки
 - MRP, HRP
 - IGMP Snooping
 - LLDP
 - Syslog
 - RADIUS
 - Опции DHCP 66/67
 - TFTP
 - GMRP и GVRP
- Для следующих протоколов есть безопасные альтернативы:
 - HTTP → HTTPS
 - Telnet → SSH
 - SNMPv1/v2c → SNMPv3
 Проверьте необходимость применения протокола SNMPv1/v2c. Протокол SNMPv1/v2c классифицируется как небезопасный. Воспользуйтесь возможностью запрета доступа с правом на запись. Устройство предлагает соответствующие возможности настройки.
 Если протокол SNMP активирован, измените имена сообщества. Если неограниченный доступ не требуется, ограничьте доступ через протокол SNMP. Воспользуйтесь механизмами аутентификации и кодировки протокола SNMPv3.
- Используйте безопасные протоколы, когда доступ к устройству не предохранён физическими устройствами защиты.
- Если требуется применение небезопасных протоколов и служб, пользуйтесь ими только в пределах защищённой сетевой зоны.
- Ограничьте использование служб и протоколов, адресованных внешним потребителям, до минимума.
- После ввода в эксплуатацию активируйте для функции DCP режим «Read-Only».
- Если для доступа системы управления к устройству используется порт RADIUS, активируйте безопасные протоколы и службы.

Доступные протоколы

В следующем списке представлен обзор открытых портов протокола.

Таблица содержит следующие столбцы.

- **Протокол**
- **Порт**
- **Заданное состояние порта**
 - Открытый
Заводская настройка порта «Открытый».
 - Закрытый
Заводская настройка порта «Закрытый».
- **Конфигурируемый порт**
 - ✓
Состояние порта можно изменить.
 - --
Состояние порта невозможно изменить.
- **Аутентификация**
Указывает, выполняется ли аутентификация партнёра связи.
- **Кодировка**
Указывает, закодирована ли передаваемая информация.

Список доступных служб (локальный доступ по локальной сети)

Далее перечисляются все доступные протоколы и их порты, через которые можно получить доступ к устройству.

Службы	Протокол/ номер порта	Заданное со- стояние порта	Конфигури- руемый порт	Аутентифика- ция	Кодировка
DHCPv4 Server	UDP/67	Закрытый	✓	Нет	Нет
DHCPv4 Client	UDP/68	Открытый	✓	Нет	Нет
EtherNet/IP	TCP/44818 UDP/2222 UDP/44818	Закрытый (открытый для вариантов EtherNet/IP)	✓	Нет	Нет
HTTP	TCP/80	Открытый	✓	Да	Нет
HTTPS	TCP/443	Открытый	✓	Да	Да
NTP SNTP	UDP/123	Закрытый	✓	Нет	Нет
NTP (secure)	UDP/123	Закрытый	✓	Да	Нет
PROFINET	UDP/34964 UDP/49151 ... 49159 ¹⁾	Открытый	✓	Нет	Нет
RADIUS	UDP/1812,1813	Закрытый	✓	Да	Да
SMTP	TCP/25 TCP/465	Закрытый	✓	Да	Да
SNMP	UDP/161	Открытый	✓	Да	Да (если скон- фигурировано)

Службы	Протокол/ номер порта	Заданное со- стояние порта	Конфигури- руемый порт	Аутентифика- ция	Кодировка
SSH	TCP/22	Открытый	✓	Да	Да
Syslog	UDP/514 TCP/6514	Закрытый	✓	Да	Да
TELNET	TCP/23	Открытый	✓	Да	Нет
TFTP	UDP/69	Открытый	✓	Нет	Нет

¹⁾ Номер порта настраивается с помощью WBM.

Присвоение IP-адреса

4.1 Структура IP-адреса

Классы адресов

Диапазон IP-адресов	Макс. число сетей	Макс. число хостов/сети	Класс	CIDR
От 1.х.х.х до 126.х.х.х	126	16777214	A	/8
От 128.0.х.х до 191.255.х.х	16383	65534	B	/16
От 192.0.0.х до 223.255.255.х	2097151	254	C	/24
224.0.0.0 - 239.255.255.255	Применения многоадресной рассылки		D	
240.0.0.0 - 255.255.255.255	Зарезервировано для будущих случаев применения		E	

Один IP-адрес состоит из 4 байт. Каждый байт представляется в десятичном формате и отделён точкой от предыдущего. В результате образуется следующая структура, где для XXX задаётся число от 0 до 255:

XXX.XXX.XXX.XXX

IP-адрес состоит из двух частей: адреса сети и адреса конечного абонента. Благодаря этому можно образовывать различные подсети. В зависимости от того, какие используются байты IP-адреса в качестве адреса сети и какие в качестве адреса конечного абонента, IP-адрес можно отнести к определенному классу адресов.

Маска подсети

Биты адреса конечного абонента могут использоваться для создания подсетей. При этом ведущие биты представляют собой адрес подсети, а остальные биты интерпретируются как адрес компьютера в подсети.

Подсеть определяется маской подсети. Структура маски подсети соответствует структуре IP-адреса. Если в маске подсети в какой-либо позиции бита задаётся «1», этот бит относится в определённом месте в IP-адресе к адресу подсети, в противном случае к адресу компьютера.

Пример для класса сети B.

Стандартным адресом подсети для класса сетей B является 255.255.0.0, таким образом последние два байта предоставляются для задания подсети. Если следует задать 16 подсетей, необходимо установить третий байт адреса подсети на 11110000 (двоичное представление). В этом случае получаем маску подсети 255.255.240.0.

Чтобы определить, относятся ли два IP-адреса к одной и той же подсети, на обоих IP-адресах и маске подсети применяется по битам логическая операция И. Если обе логические операции имеют одинаковый результат, оба IP-адреса относятся к одинаковой подсети, как например 141.120.246.210 и 141.120.252.108.

4.2 Первоначальное присвоение IP-адреса

Вне локальной сети описанный способ задания адреса конечного абонента не имеет значения, там для коммутации пакетов значение в целом имеет только IP-адрес.

Примечание

В битовом представлении маски подсети «единицы» должны устанавливаться ближе к левому краю, т. е. между «нулями» не допускается установка «единиц».

4.2 Первоначальное присвоение IP-адреса

Возможности конфигурации

Первоначальное присвоение IP-адреса для промышленного Ethernet-коммутатора невозможно выполнять с помощью системы Web Based Management (WBM), так как данный инструмент конфигурирования уже предполагает наличие IP-адреса.

Имеются следующие возможности присвоения IP-адреса неконфигурированному устройству.

- **DHCP** (заводская настройка)
- **SINEC PNI** (SINEC Primary Network Initialization (инициализация первичной сети))
Эта программа для первоначального ввода в эксплуатацию сетевых устройств использует протокол DCP, чтобы распознавать устройства в сети и присваивать IP-адрес.

Дополнительную информацию см. PNI (<https://support.industry.siemens.com/cs/products?mfn=ps&pnid=26672&lc=en-US>)

- **STEP 7**

В ПО STEP 7 можно проектировать топологию, название устройств и IP-адрес. Когда неконфигурированный промышленный Ethernet-коммутатор подсоединяется к контроллеру, контроллер автоматически присваивает промышленному Ethernet-коммутатору запроецированное название устройства и IP-адрес.

- **STEP 7**

- SCALANCE XB-200: с версии V5.5.4

- SCALANCE XP-200: с версии V5.5.4 HF9

- SCALANCE XC-200: с версии V5.5.4 HF11

- SCALANCE XR-300WG: с версии V5.6

- SCALANCE XF-200BA: с версии V5.6 HF3

- SCALANCE XC-200G: с версии V5.6 HSP11

- В отношении дополнительной информации по присвоению IP-адреса с помощью STEP 7 обратите внимание на документацию «Конфигурирование аппаратного обеспечения и соединений с помощью STEP 7», раздел «Этапы конфигурирования системы ввода-вывода данных сети PROFINET».

- **STEP 7 Basic или Professional**

- SCALANCE XB-200: с версии V13 SP1

- SCALANCE XC-200: с версии V14

- SCALANCE XP-200: с версии V14

- SCALANCE XR-300WG: с версии V15

- SCALANCE XF-200BA: с версии V15

- SCALANCE XC-200G, устройства с 8 портами: с версии V15

- SCALANCE XC-200G, устройства с более 8 портами: с версии V16

- В отношении дополнительной информации по присвоению IP-адреса с помощью STEP 7 обратите внимание на онлайн-справку «Информационная система», раздел «Адресация устройств PROFINET».

- **CLI через последовательный интерфейс**

В отношении дополнительной информации по присвоению IP-адреса с помощью последовательного интерфейса обратите внимание на инструкцию соответствующего устройства, см. также главу «Введение», раздел «Включение в комплект документации».

- **NCM PC**

В отношении дополнительной информации по присвоению IP-адреса с помощью NCM PC обратите внимание на документацию «Ввод в эксплуатацию станций ПК, инструкция и быстрый запуск», раздел «Создание системы ввода-вывода данных сети PROFINET».

Примечание

DHCP находится в состоянии при поставке и включается после восстановления заводских настроек. Если DHCP-сервер доступен в локальной сети и он отвечает на DHCP-запрос промышленного Ethernet-коммутатора, то при первом запуске автоматически присваиваются IP-адрес, маска подсети и шлюз.

4.3 Присвоение адреса через DHCP

Свойства DHCP

Протокол DHCP (Dynamic Host Configuration Protocol) представляет собой процедуру для автоматического присвоения IP-адресов. Он имеет следующие свойства.

- Протокол DHCP можно использовать как во время запуска устройства, так и в его рабочем режиме.
- Присвоенный IP-адрес остаётся действительным только в течение ограниченного времени (Lease Time). По истечении половины времени срока действия DHCP-клиент может продлить действие присвоенного IPv4-адреса. По истечении всего периода действия DHCP-клиент должен запросить новый IPv4-адрес.
- Если запрос нового IP-адреса после истечения времени Lease Time выполнить не удаётся, IP-конфигурация зависит от функции «Keep Alive». Если функция Keep Alive активирована, IP-адрес при обрыве соединения сохраняется и на 0.0.0.0 не сбрасывается. Функция Keep Alive активирована по умолчанию. Если функция Keep Alive деактивирована, то IP-адрес при разрыве соединения сбрасывается на 0.0.0.0.
- Если IP-адрес конфигурировался через протокол DHCP и протокол DHCP отключается, IP-конфигурация зависит от функции «Keep Alive». Если функция Keep Alive деактивирована, IP-конфигурация сбрасывается на 0.0.0.0 («Не конфигурировано»). Если функция Keep Alive активирована, IP-адрес сохраняется и на 0.0.0.0 не сбрасывается.
- Если IP-адрес конфигурировался через протокол DHCP и соединение с сетью временно прерывается (состояние интерфейса «Up» (включено), «Down» (выключено) и снова «Up»), IP-конфигурацию необходимо сначала подтвердить DHCP-сервером. Если подтверждение невозможно, IP-конфигурация сбрасывается на 0.0.0.0 («Не конфигурировано»), и DHCP-сервером запрашивается новая IP-конфигурация.
- Если у какого-либо устройства протокол DHCP был активен, то после перезапуска необходимо запрашивать только новый IP-адрес на сервере DHCP-сервере.
- Обычно статические адреса не присваиваются, т. е. когда клиент заново запрашивает IP-адрес, он получает, как правило, другой адрес, чем в предыдущем запросе. Имеется возможность сконфигурировать DHCP-сервер таким образом, чтобы DHCP-клиент на свой запрос получал один и тот же присвоенный статический адрес. Через какой параметр DHCP-клиент идентифицируется для присвоения статического адреса, устанавливается в настройках DHCP-клиента и DHCP-сервера. Этот адрес может присваиваться через MAC-адрес, идентификатор DHCP-клиента, имя сети PROFINET или системное имя. Параметр можно сконфигурировать в меню «System > DHCP > DHCP-Client».
- Если конфигурировался статический IP-адрес, и активируется протокол DHCP, IP-конфигурация зависит от функции «Keep Alive». Если функция Keep Alive деактивирована, то при включении DHCP IP-адрес устанавливается на 0.0.0.0 и ожидается новый IP-адрес от DHCP-сервера. При отсутствии адреса, присвоенного через DHCP-сервер, коммутатор перестаёт быть доступным через IP.

Технические основы

5.1 PROFINET

PROFINET

PROFINET — открытый стандарт Ethernet (МЭК 61158/61784) для промышленной автоматизации на базе промышленной сети Ethernet. PROFINET использует существующие стандарты ИТ и позволяет создавать непрерывную связь между полевым уровнем и уровнем управления, а также проектировать всю систему. Дополнительные свойства PROFINET:

- Применение набора протоколов TCP/IP
- Автоматизация процессов с требованием работы в режиме реального времени
 - Связь реального времени (RT)
 - Связь изохронного реального времени (IRT)
- Беспроблемная интеграция систем полевых шин

Конфигурацию сети PROFINET можно выполнить под пунктом «Система > PROFINET (Страница 255)».

PROFINET IO

В рамках сети PROFINET сеть PROFINET IO представляют собой концепцию связи для реализации модульных, децентрализованных решений. Реализация сети PROFINET IO осуществляется через стандарт PROFINET для устройств автоматизации (МЭК 61158-х-10).

5.2 EtherNet/IP

EtherNet/IP

EtherNet/IP (Ethernet/Industrial Protocol) — открытый промышленный стандарт для промышленной сети Ethernet реального времени, основанный на TCP/IP и UDP/IP. С помощью EtherNet/IP сеть Ethernet дополняется протоколом Common Industrial Protocol (CIP) на прикладном уровне. В EtherNet/IP нижние уровни базовой модели OSI сети Ethernet принимаются вместе с функциями передачи, коммутации, сетевыми функциями и функциями транспортировки.

Конфигурацию EtherNet/IP можно выполнить под пунктом «Система > EtherNet/IP».

Common Industrial Protocol (общий промышленный протокол)

Common Industrial Protocol (CIP) — протокол приложения процессов автоматизации, поддерживающий переход полевых шин в промышленную сеть Ethernet и в сети IP. Этим протоколом пользуются полевые шины / промышленные сети как например, DeviceNet, ControlNet и EtherNet/IP на прикладном уровне в качестве интерфейса между детерминированным окружением полевых шин и устройством автоматизации (контроллер, E/A, HMI, OPC, ...). Протокол CIP находится выше уровня транспортировки и расширяет исключительные службы транспортировки на службы коммуникации для техники автоматизации. К ним относятся службы для циклического, критичного по времени и управляемого событиями обмена данными. Протокол CIP различает между критичными по времени входящими/исходящими сообщениями (implicit messages (неявные сообщения)) и индивидуальными пакетами вопрос/ответ для конфигурирования и сбора данных (explicit messages (явные сообщения)). Протокол CIP является объектно-ориентированным протоколом; все «видимые» снаружи данные доступны в форме объектов. Протокол CIP имеет общую базу конфигурирования: EDS (Electronic Data Sheet (электронные технические данные)).

Electronic Data Sheet

Electronic Data Sheet (EDS) — электронный технический паспорт для описания устройств.

Необходимый для работы EtherNet/IP электронный технический паспорт можно найти под пунктом «Система > Загрузка и сохранение (Страница 165)».

5.3 Режим резервирования

5.3.1 Spanning Tree

Предотвращение образования петель в избыточных соединениях

Процедура Spanning Tree позволяет создавать сетевые структуры, в которых существует множество соединений между двумя промышленными Ethernet-коммутаторами / мостами. Алгоритм Spanning Tree предотвращает образование петель в сети, допуская в ней работу только одного канала и деактивируя другие (избыточные) порты для обмена данными. При обрыве связи данные могут посылаются через альтернативный канал. Процедура Spanning Tree основана на обмене пакетами изменения конфигурации и топологии.

Определение топологии сети посредством конфигурационных пакетов

Для расчёта топологии устройства обмениваются между собой конфигурационными пакетами, так называемыми BPDU (Bridge Protocol Data Units (блоки протокольных данных моста)). С помощью этих пакетов выбирается корневой мост Root Bridge и создаётся топология сети. Кроме этого, пакеты BPDU влияют на смену статуса корневых портов.

Корневой мост представляет собой мост, который управляет процедурой Spanning Tree для всех задействованных компонентов.

После задания корневого моста каждое устройство определяет корневой порт. Корневой порт — порт с наименьшей стоимостью пути к корневому мосту.

Характеристики при изменении топологии сети

Подсоединение или отключение абонентов в сети может повлиять на выбор оптимальных каналов прохождения пакетов данных. Для учёта таких изменений корневой мост с регулярными интервалами пересылает конфигурационные сообщения. Временной интервал между двумя конфигурационными сообщениями можно настроить с помощью параметра «Hello Time» (время, через которое устройство посылает подтверждение своей работоспособности).

Актуальность конфигурационной информации

С помощью параметра «Max Age» (макс. возраст информации) можно установить максимальный срок действия конфигурационной информации. Когда какой-либо мост получает конфигурационную информацию, возраст которой старше значения параметра «Max Age», он отклоняет это сообщение и запрашивает новый расчёт канала передачи данных.

Новая конфигурационная информация применяется мостом всё же не сразу, а лишь через заданный в параметре «Forward Delay» (задержка отправления) период времени. Таким образом, гарантируется, что рабочий режим в соответствии с новой топологией запускается только тогда, когда все мосты получают необходимую информацию.

5.3.1.1 RSTP, MSTP, CIST

Rapid Spanning Tree Protocol (ускоренный протокол связующих деревьев) (RSTP)

Недостатком протокола STP является то, что при сбое в работе или отказе устройства сеть необходимо конфигурировать повторно: Устройства начинают создавать новые каналы только в момент прерывания работы. Этот процесс длится до 30 секунд. По этой причине протокол STP был расширен протоколом Rapid Spanning Tree Protocol (ускоренный протокол связующих деревьев) (RSTP, IEEE 802.1w). Он отличается от протокола STP в основном тем, что устройства собирают информацию об альтернативных каналах уже в момент их бесперебойной работы, которые не потребуются до момента возникновения сбоя в работе. В результате этого время повторного конфигурирования для сети, управляемой протоколом RSTP, уменьшается до нескольких секунд. Это достигается благодаря следующим функциям.

- **Edge-Ports (порт конечного пользователя)**
Edge-Ports — порты, соединённые с конечным устройством.
Порт, определяемый как Edge-Port, активируется непосредственно после установления соединения. Когда на каком-либо порте Edge-Port принимается пакет Spanning Tree-BPDU, порт теряет роль порта Edge-Port и снова работает с протоколом (R)STP. Если по истечении интервала времени (3x Hello-Time) никакой пакет BPDU не принимается, порт снова переходит в статус порта Edge-Port.
- **Узел–узел (прямая связь двух соседних устройств)**
Благодаря прямому соединению устройств возможно изменение состояния (переконфигурация портов) без задержки.
- **Альтернативный порт (замена для корневого порта)**
Он сконфигурирован в качестве замены для корневого порта. При потере соединения с корневым мостом устройство сможет без задержки благодаря новой конфигурации установить соединение через альтернативный порт.
- **Реакция на события**
Rapid Spanning Tree (высокоскоростное связующее дерево) реагирует на события, например обрыв соединения, без задержки. Следовательно, нет необходимости в ожидании срабатывания таймера как в случае с Spanning Tree.
- **Счётчики максимального количества мостовых переходов**
Количество мостовых переходов, максимально которое допускается выполнить пакету, перед тем как он автоматически станет недействительным.

Как правило, при использовании Rapid Spanning Tree для нескольких параметров предварительно конфигурируются варианты и учитываются определённые свойства сетевой структуры, чтобы уменьшить время реконфигурации.

Multiple Spanning Tree Protocol (протокол множественных связующих деревьев) (MSTP)

Multiple Spanning Tree Protocol (MSTP) усовершенствованный вариант протокола Rapid Spanning Tree Protocol. Среди прочего он предлагает возможность работы нескольких экземпляров RSTP внутри различных сетей VLAN или групп сетей VLAN, делая таким образом доступными, например, каналы, которые заблокировали бы глобально простой протокол Rapid Spanning Tree Protocol для обмена данными, внутри отдельных сетей VLAN.

Common and Internal Spanning Tree (общее и внутреннее связующее дерево) (CIST)

CIST обозначает используемые внутри коммутатором экземпляры, которые аналогичны внутреннему экземпляру RSTP.

5.3.2 RSTP+

5.3.2.1 Свойства и функции RSTP+

Основным случаем применения протокола RSTP+ является избыточная интеграция кольцевых сетей MRP в сеть RSTP. В основном было бы возможно управление такой сетью исключительно с помощью протокола RSTP. В кольцевой топологии MRP является всё же более эффективной и быстрой процедурой. Процедура кольцевого резервирования MRP не зависит от RSTP+, так как обе процедуры работают независимо друг от друга.

Другим случаем применения является избыточное соединение кольцевых сетей MRP. Кроме этого, с помощью RSTP+ возможно соединение двух сетей RSTP через кольцевую сеть MRP. Без RSTP+ это выполнить невозможно, так как алгоритм Spanning Tree отключён на портах кольцевой сети.

Совместимость устройств без RSTP+

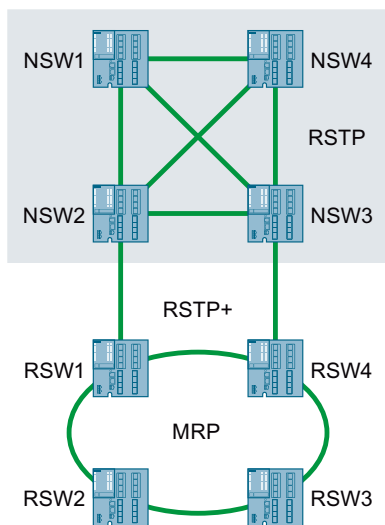
В основном действует условие, что все устройства в местах соединения между сетью RSTP и кольцевой сетью MRP должны поддерживать процедуру RSTP+. Все остальные устройства в кольцевой сети MRP должны перенаправлять пакеты BPDU (Bridge Protocol Data Unit).

5.3.2.2 Топология для RSTP+

Сеть RSTP и кольцевая сеть MRP

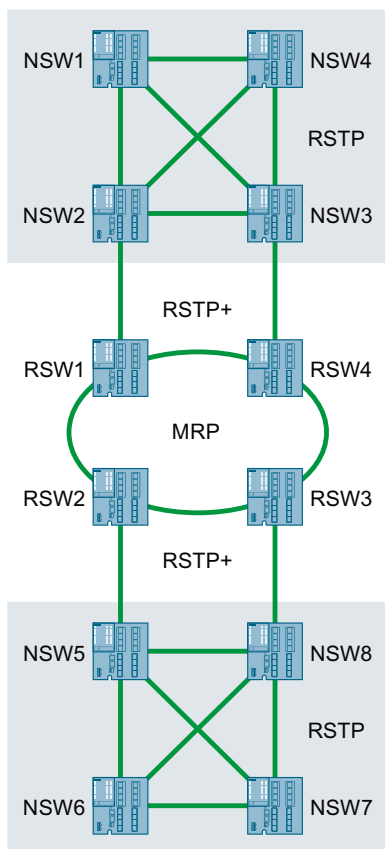
Избыточная интеграция кольцевых сетей MRP в сеть RSTP без протокола RSTP+ невозможна, так как не допускается параллельная работа RSTP и MRP на одном порте. Только устройства кольцевой сети MRP, имеющие соединение с сетью RSTP, должны поддерживать протокол RSTP+. В представленной топологии в качестве примера этими устройствами являются оба устройства RSW1 и RSW4. Другие устройства должны перенаправлять пакеты BPDU.

Обозначение устройств на рисунках относится к соответствующей функции устройства. «NSW» — аббревиатура для коммутатора сети, «RSW» — аббревиатура для коммутатора кольцевой сети.



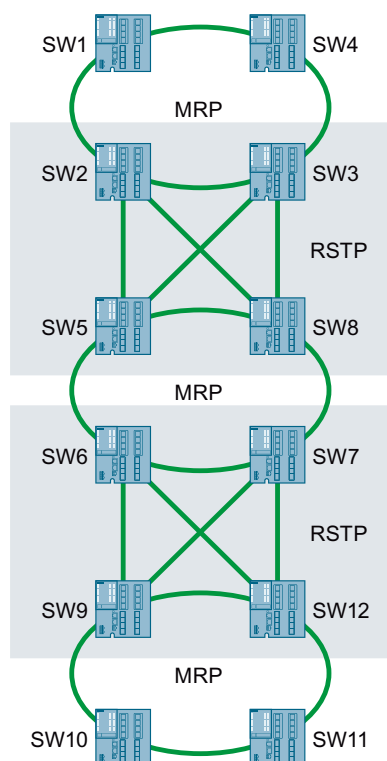
Несколько зон сети RSTP и кольцевая сеть MRP

Другим случаем применения протокола RSTP+ является соединение двух или более зон сети RSTP через кольцевую сеть MRP. Протокол RSTP+ должен быть активирован для всех устройств в кольцевой сети MRP, имеющих соединение с сетями RSTP. В приведённом примере такими устройствами являются устройства RSW1, RSW2, RSW3 и RSW4.



Несколько кольцевых сетей MRP

Протокол RSTP+ можно использовать также для того, чтобы соединить между собой несколько кольцевых сетей MRP через RSTP. Протокол RSTP+ в этом случае гарантирует, что MRP по-прежнему управляет кольцевым резервированием без нарушений со стороны протокола RSTP.

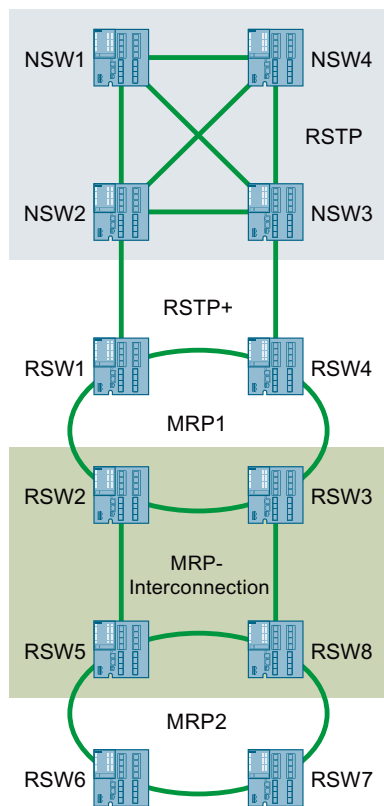


Сеть RSTP и две кольцевые сети MRP с MRP Interconnection

Протокол RSTP+ может соединять также сеть RSTP с помощью двух кольцевых сетей MRP, соединённых через MRP Interconnection. Оба устройства RSW1 и RSW4 в представленной в качестве примера топологии должны поддерживать протокол RSTP+. Задействованные в соединении обеих кольцевых сетей MRP устройства (RSW2, RSW3, RSW5 и RSW8) должны поддерживать MRP Interconnection. Дополнительно устройства RSW2 и RSW3 должны перенаправлять пакеты BPDU (Bridge Protocol Data Unit).

Для идентификатора домена RSTP+ MRP Interconnection действуют в представленном примере следующие правила.

- Для устройств RSW1 и RSW4 должен быть сконфигурирован одинаковый идентификатор домена RSTP+ MRP Interconnection.
- Для устройств RSW2, RSW3, RSW5 и RSW8 должен быть сконфигурирован одинаковый идентификатор домена RSTP+ MRP Interconnection.
- Идентификатор домена RSTP+ MRP Interconnection устройств RSW1 и RSW4 должен отличаться от идентификатора домена RSTP+ MRP Interconnection устройств RSW2, RSW3, RSW5 и RSW8.



5.3.2.3 Конфигурирование протокола RSTP+

В данной главе приводится подробное описание процесса конфигурирования протокола RSTP+. Выполните этапы конфигурирования для всех устройств, в которых следует активировать протокол RSTP+. Номера позиций на скриншотах соответствуют номерам последовательности этапов. Данное описание касается устройств, которые ещё не были сконфигурированы (заводские настройки).

Описание подразделяется на три раздела.

- Конфигурирование Spanning Tree (этапы с 1 по 4)
- Конфигурирование кольцевого резервирования (этапы с 5 по 7)
- Активация протокола RSTP+ и подсоединение проводов (этапы с 8 по 9)

Общие правила конфигурирования

Во время процесса конфигурирования придерживайтесь следующих правил, действующих в зависимости от определённой топологии сети.

- Функция управления резервированием не должна переноситься на одно из двух устройств соединения RSTP/MRP.
- Между обоими портами кольцевой сети устройств соединения должно существовать прямое LAN-соединение.

5.3.2.4 Конфигурирование Spanning Tree для протокола RSTP+

В WBM для конфигурирования Spanning Tree имеется меню «Уровень 2 > Spanning Tree». Выполните этапы с 1 по 4 для каждого устройства, в котором следует активировать протокол RSTP+.

Этап 1: конфигурирование портов кольцевой сети

Конфигурирование кольцевых портов можно выполнить на вкладке «CIST-порт» или на вкладке «ST-порт».

- Деактивируйте флажки опций обоих портов кольцевой сети в столбце таблицы «Spanning Tree-Status».

Port	Spanning Tree Status	Priority
P0.1	☐	128
P0.2	☐	128
P0.3	☒	128

- Деактивируйте флажки опций обоих портов кольцевой сети в столбце таблицы «Ограниченная роль». Это необходимо сделать для того, чтобы характеристики портов кольцевой сети управлялась исключительно с MRP, т. е. устройства управления резервированием. На работу MRP протокол RSTP+ никакого влияния не оказывает.

Hello Time	Restr. Role	Restr. TCN
2	☐	☐
2	☐	☐
2	☐	☐

Этап 2: конфигурирование совместимости протоколов

Выберите в раскрывающемся списке «Protocol Compatibility» запись «RSTP».

Этап 3: включение режима Spanning Tree

Имеются устройства, в которых режим Spanning Tree уже активирован на заводе-изготовителе. Если режим Spanning Tree ещё не включён, активируйте флажок опции «Spanning Tree».

Таблица на вкладке «CIST-порт» предлагает возможность конфигурации режима Spanning Tree для отдельных портов. Флажки опций портов для соединения с сетью RSTP должны быть активированы.

Этап 4: задание идентификатора домена RSTP+ MRP Interconnection

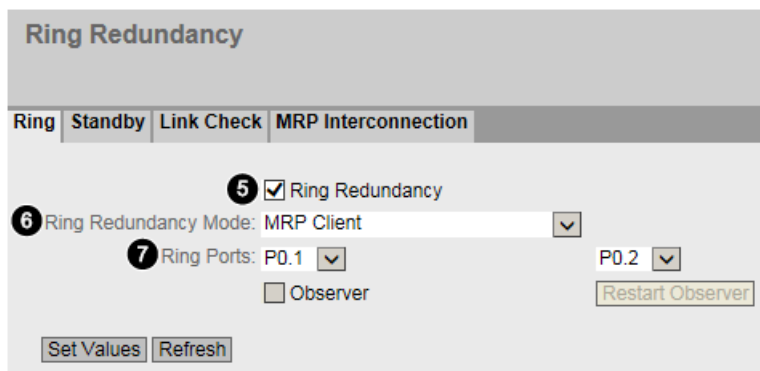
RSTP+ MRP Interconnection Domain ID должен быть уникальным во всей сети и отличаться от настраиваемого MRP Interconnection Domain ID. Разные идентификаторы нужны, чтобы различать TCN (Topology Change Notifications) сети RSTP от TCN кольцевой сети MRP. Это присвоение позволяет удалить только те записи FDB (записи Forwarding Database), на которые влияет изменение топологии.

Каждое устройство проверяет, были ли для этих обоих параметров сконфигурированы различные значения. Если идентификаторы совпадают, устройство выдаёт сообщение об ошибке. Администратор сети несёт ответственность за уникальность этих идентификаторов во всей сети. Такая проверка не может быть проведена одним устройством.

Затем щёлкните кнопку «Set Values», чтобы сохранить конфигурацию.

5.3.2.5 Конфигурирование кольцевого резервирования для протокола RSTP+

В WBM для конфигурирования кольцевого резервирования имеется меню «Layer 2 > Ring Redundancy». На вкладке «Ring» выполните этапы с 5 по 7 для каждого устройства, в котором следует активировать протокол RSTP+.

**Этап 5: включение кольцевого резервирования**

Активируйте флажок опции «Ring Redundancy» для включения MRP.

Этап 6: присвоение роли MRP

Выберите в раскрывающемся списке «Ring Redundancy Mode» запись «MRP Client» или «MRP Auto Manager». Функция управления резервированием не должна переноситься на одно из двух устройств соединения RSTP-MRP.

Этап 7: задание портов кольцевой сети

В раскрывающихся списках выберите подходящие записи для кольцевых портов.

Затем щёлкните кнопку «Set Values», чтобы сохранить конфигурацию.

5.3.2.6 Включение протокола RSTP+ и подсоединение проводов

Spanning Tree Protocol (STP) General

General CIST General CIST Port MST General MST Port Enhanced Passive Listening Compatibility

☒ Spanning Tree Protocol Compatibility: RSTP

8 ☒ RSTP+

RSTP+ MRP Interconnection Domain ID: 2

Set Values Refresh

Этап 8: включение протокола RSTP+

Активируйте флажок опции «RSTP+». Появляется диалоговое окно с сообщением «Spanning Tree is enabled on ring ports due to enabled RSTP+». Это сообщение отображается, так как обычно невозможна параллельная работа кольцевого резервирования (MRP) и протокола RSTP на одном порте. Щёлкните кнопку «ОК» для закрытия диалогового окна.

После включения протокола RSTP+ невозможно будет изменить предварительно сконфигурированные параметры. Затем щёлкните кнопку «Set Values», чтобы сохранить конфигурацию.

Этап 9: соединение проводов

После конфигурирования всех устройств подсоедините провода в соответствии с запланированной топологией. Процедура RSTP+ теперь активирована.

5.3.3 HRP

HRP - High Speed Redundancy Protocol (высокоскоростной протокол резервирования)

HRP обозначает процедуру резервирования для сетей кольцевой топологии. Коммутаторы соединены между собой через порты кольцевой сети. Один из коммутаторов конфигурируется как устройство управления резервированием (RM). Другие коммутаторы являются клиентами резервирования. С помощью тестовых пакетов устройство управления резервированием проверяет кольцевую сеть на предмет отсутствия обрывов. Устройство управления резервированием передаёт тестовые пакеты через порты кольцевой сети и проверяет их получение каждым соответствующим портом кольцевой сети. Клиенты резервирования перенаправляют эти тестовые пакеты.

Когда тестовые пакеты устройства RM перестают поступать на другой порт при обрыве кольцевой сети, устройство RM подключает оба своих порта и немедленно информирует клиентов резервирования о смене. Время реконфигурации при обрыве кольцевой сети составляет не более 300 мс.

Резервирование Standby

Резервирование замещением — процедура, при которой кольцевые сети, защищённые высокоскоростным резервированием, имеют резервное соединение. В кольцевой сети конфигурируется пара из ведущего и ведомого устройств, которые контролируют друг друга через свои порты кольцевой сети. Трафик в случае ошибки Ethernet-соединения (Standby-порт ведущего устройства или Standby-сервер) перенаправляется на другое Ethernet-соединение (Standby-порт ведомого устройства).

Требования

HRP

- Процедура HRP в кольцевой топологии поддерживает работу до 50 устройств. Превышение количества устройств может привести к сбою обмена данными.
- Для HRP в кольцевой сети разрешается использовать только те устройства, которые поддерживают и эту функцию.
- Устройства, которые не поддерживают HRP, должны подсоединяться к соответствующей кольцевой сети с помощью специальных устройств, способных работать с HRP. Данное соединение до кольцевой сети не является избыточным.
- Все устройства должны быть соединены между собой через свои порты кольцевой сети. При этом между двумя промышленными Ethernet-коммутаторами возможно создание многорежимных соединений до 3 км и однорежимных соединений до 26 км. При большей удалённости может увеличиться указанное время реконфигурации.
- Устройство в кольцевой сети должно конфигурироваться путём выбора настройки «HRP-Manager» как устройство управления резервированием. Во всех других устройствах в кольцевой сети должен активироваться либо рабочий режим «HRP-Client» или рабочий режим "Automatic Redundancy Detection" (обнаружение автоматического резервирования).
- Standby-порты должны быть деактивированы в режиме Spanning Tree.
- Конфигурирование HRP можно выполнять с помощью системы Web Based Management, интерфейса Command Line Interface или SNMP.

Резервирование Standby

- Для участников соединения режима Standby процедура HRP должна иметь фиксированную настройку.
- Порты участников соединения режима Standby в Spanning Tree должны быть деактивированы.
- Конфигурирование резервирования замещением можно выполнять с помощью системы Web Based Management, интерфейса Command Line Interface или SNMP.

5.3.4 MRP

5.3.4.1 MRP - Media Redundancy Protocol (протокол резервирования среды передачи данных)

Процедура «MRP» работает в соответствии с протоколом резервирования среды передачи данных (MRP), который описывается в следующем стандарте:

IEC 62439-2:2016 Industrial communication networks - High availability automation networks Part 2: Media Redundancy Protocol (MRP)

Время реконфигурации при обрыве кольцевой сети составляет не более 200 мс.

Топология

На следующем рисунке показана возможная топология для устройств в кольцевой сети с MRP.

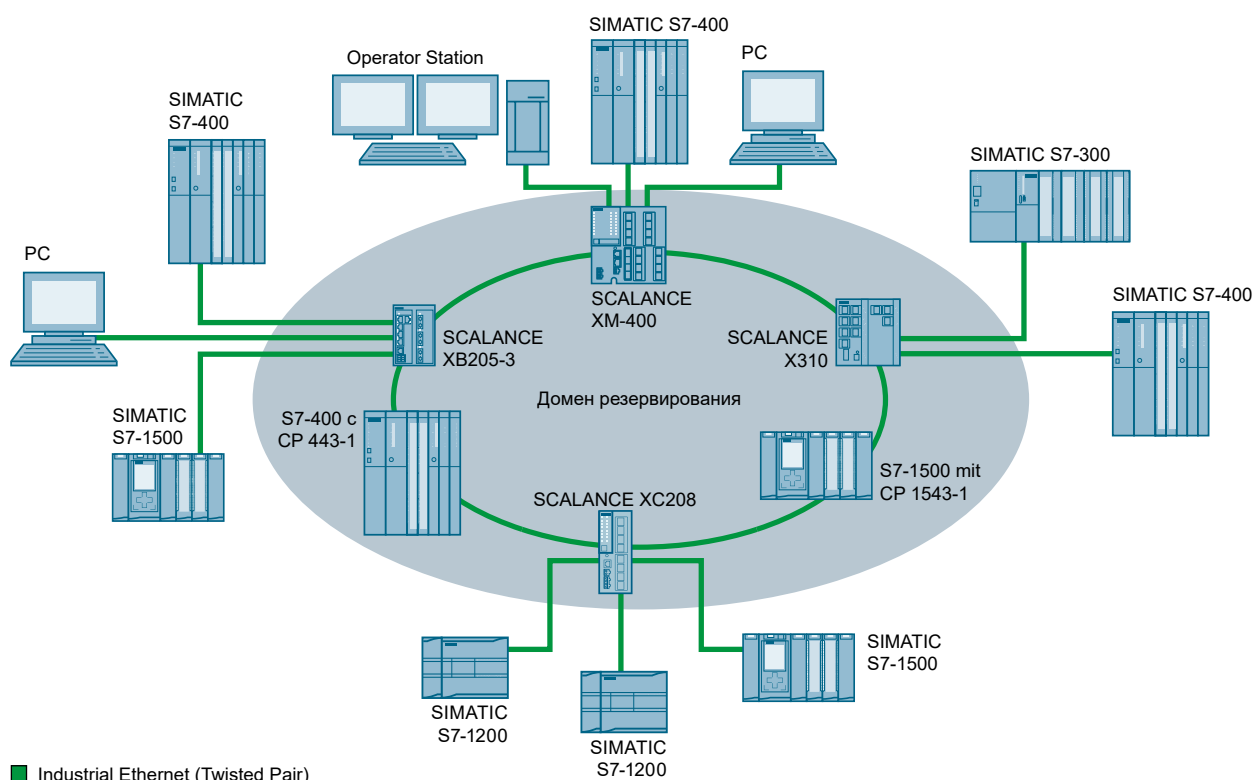


Рисунок 5-1 Пример кольцевой топологии с процедурой резервирования среды передачи данных MRP

Для кольцевой топологии с резервированием среды передачи данных в соответствии с процедурой MRP действуют следующие правила.

- Все соединённые внутри кольцевой топологии устройства являются участниками одного и того же домена резервирования.
- Устройство в кольцевой сети является устройством управления резервированием.
- Все другие устройства в кольцевой топологии являются клиентами резервирования.

Не поддерживающие MRP устройства могут подсоединяться к кольцевой сети через коммутатор SCALANCE X или ПК с коммуникационным процессором, поддерживающим MRP.

Требования

Требования для бесперебойной работы с использованием процедуры резервирования среды передачи данных MRP следующие.

- MRP в кольцевой топологии поддерживает работу до 50 устройств. Превышение количества устройств может привести к сбою обмена данными.
- Кольцевая сеть, в которой вы хотите использовать MRP, должна состоять только из устройств, поддерживающих эту функцию. К ним относятся, например, некоторые промышленные Ethernet-коммутаторы SCALANCE X, некоторые коммуникационные процессоры (CP) для устройства SIMATIC S7 и программаторы/ПК или не изготовленные Siemens устройства, поддерживающие эту функцию.
- Все устройства должны быть соединены между собой через свои порты кольцевой сети. При этом между двумя промышленными Ethernet-коммутаторами SCALANCE X возможно создание многорежимных соединений до 3 км и одnoreжимных соединений до 26 км. При большей удалённости может увеличиться указанное время реконфигурации.
- Во всех устройствах в кольцевой сети должна быть активирована функция «MRP».
- Настройки соединения (средство передачи / дуплексный режим) должны быть установлены для всех портов кольцевой сети на дуплексный режим и скорость не менее 100 Мбит/с. В противном случае может возникнуть сбой обмена данными.
 - STEP 7: в диалоговом окне свойств всех задействованных в кольцевой сети портов на вкладке «Options» установите соединение на значение «Auto».
 - WBM: при проектировании через систему Web Based Management порты кольцевой сети автоматически настраиваются на автоматическое определение сети.

5.3.4.2 Проектирование в системе WBM

Роль

Выбор роли зависит от следующих случаев применения.

- Вы хотите в кольцевой топологии использовать MRP только с устройствами Siemens.
 - Выберите по меньшей мере в одном устройстве в кольцевой сети роль «Automatic Redundancy Detection» или «MRP Auto-Manager».
 - Выберите для всех остальных устройств в кольцевой сети роль «MRP-Client» или «Automatic Redundancy Detection».
- Вы хотите в кольцевой топологии использовать MRP также с не изготовленными Siemens устройствами.
 - Выберите только в одном устройстве в кольцевой сети роль «MRP Auto-Manager».
 - Выберите для всех остальных устройств кольцевой топологии роль «MRP-Client».

Примечание

Применение роли «Automatic Redundancy Detection» с не изготовленными Siemens устройствами невозможно.

- Вы проектируете устройства с кольцевой топологией частично с помощью системы WBM и частично с помощью ПО STEP 7:
 - Выберите на всех устройствах, которые проектируются с помощью системы WBM, роль «MRP-Client».
 - Выберите на всех устройствах, которые проектируются с помощью ПО STEP 7, по меньшей мере для одного устройства роль «Manager» или «Manager (Auto)», а всех остальных устройств роль «MRP-Client».

Примечание

Если одному устройству через ПО STEP 7 присваивается роль «Manager», то необходимо всем другим устройствам в кольцевой сети назначить роль «MRP-Client». Если в одной кольцевой сети присутствует устройство с ролью «Manager» и устройство с ролью «Manager (Auto)»/«MRP Auto-Manager», могут возникать циркулирующие кадры, что приведёт к сбою работы сети.

Проектирование

В системе WBM можно выполнять проектирование MRP на следующих страницах.

- Configuration (Страница 276)
- Ring (Страница 311)

5.3.4.3 Проектирование в ПО STEP 7

Проектирование в ПО STEP 7

Для проектирования в ПО STEP 7 выберите группу параметров «Резервирование среды передачи» на интерфейсе PROFINET.

Настройте следующие параметры для конфигурации MRP устройства.

- Домены
- Роль
- Порт кольцевой сети
- Сигналы диагностики

Описание этих настроек приводится далее.

Примечание

Действительное проектирование MRP

При проведении проектирования MRP в ПО STEP 7 убедитесь в том, что все устройства в кольцевой сети имеют действительное проектирование MRP перед замыканием кольцевой сети. В противном случае могут возникать циркулирующие кадры, что приведёт к сбою работы сети.

Одно устройство в кольцевой сети нужно конфигурировать как «Устройство управления резервированием», а все другие устройства в кольцевой сети — как «Клиент».

Примечание

Обращайте внимание на заводские настройки

В следующих новых и установленных на заводские настройки промышленных Ethernet-коммутаторах режим MRP деактивирован, а режим Spanning Tree активирован.

- SCALANCE XB-200 (варианты EtherNet/IP)
- SCALANCE XC-200 (варианты EtherNet/IP)
- SCALANCE XP-200 (варианты EtherNet/IP)
- SCALANCE XR-300WG
- SCALANCE XM-400
- SCALANCE XR-500

Чтобы загрузить конфигурацию PROFINET с MRP в одно из указанных устройств, деактивируйте сначала на устройстве режим Spanning Tree. Деактивация режима Spanning Tree возможна только для портов кольцевой сети.

Примечание

Переконфигурация только при разомкнутой кольцевой сети

Сначала разомкните кольцевую сеть перед

- изменением роли MRP или
- переконфигурированием портов кольцевой сети.

Примечание**Перезапуск и повторный пуск**

Настройки MRP остаются действительными также после перезапуска устройства или после исчезновения напряжения и повторного пуска, если только исчезновение напряжения не возникает в течение 90 секунд после изменения конфигурации.

Примечание**Приоритетный запуск**

Если MRP проектируется в кольцевой сети, то в задействованных устройствах сети PROFINET невозможно использовать функцию «Приоритетный запуск».

Если вы хотите использовать функцию «Приоритетный запуск», то в проектировании MRP нужно деактивировать.

Установите в проектировании через ПО STEP 7 соответствующего устройства роль «Не участник кольцевой сети».

Домены

Простые кольцевые сети MRP

Если конфигурируется отдельная кольцевая сеть MRP, оставьте в раскрывающемся списке «Domain» заводскую настройку «mrpdomain-1».

Все устройства, проектируемые в одной кольцевой сети с MRP, должны принадлежать одному и тому же домену резервирования. Одно устройство не может принадлежать нескольким доменам резервирования в простой кольцевой сети.

Несколько кольцевых сетей MRP

С помощью функции многократных кольцевых сетей MRP можно управлять несколькими кольцевыми сетями MRP с помощью центрального устройства управления резервированием. Если конфигурируются несколько отдельных кольцевых сетей MRP, участники кольцевой сети присваиваются через параметр «Domain» отдельным кольцевым сетям. Внутри одной кольцевой сети устанавливайте для всех устройств одинаковые домены. Для различных кольцевых сетей устанавливайте различные домены. Устройства, которые не принадлежат одной кольцевой сети, должны иметь разные домены.

При проектировании многократных кольцевых сетей MRP выбирайте в качестве центрального устройства управления резервированием устройство, поддерживающее работу с многократными кольцевыми сетями. Установите для всех экземпляров кольцевой сети различные домены и присвойте их соответствующим портам кольцевой сети устройства управления резервированием. Спроектируйте остальные устройства

в качестве клиентов. При этом внутри одной кольцевой сети для всех устройств должны быть установлены одинаковые домены.

Примечание

Подходящие устройства для многократных кольцевых сетей MRP

В качестве устройства управления резервированием, соединяющего несколько кольцевых сетей, можно использовать все устройства следующих линеек изделий.

- SCALANCE X-300 с версии прошивки V4.0
- SCALANCE X408-2 с версии прошивки V4.0
- SCALANCE X414-3E с версии прошивки V3.10
- SCALANCE XB-200 с версии прошивки V4.3
- SCALANCE XC-200 с версии прошивки V4.3
- SCALANCE XP-200 с версии прошивки V4.3
- SCALANCE XR-300WG с версии прошивки V4.3
- SCALANCE XM-400 с версии прошивки V6.4
- SCALANCE XR-500 с версии прошивки V6.4

Примечание

Подходящие устройства для MRP Interconnection

В качестве устройства управления взаимосвязями при резервировании среды передачи и клиента взаимосвязей при резервировании среды передачи можно использовать все устройства следующих линеек изделий.

- SCALANCE XB-200 с версии прошивки V4.3
- SCALANCE XC-200 с версии прошивки V4.2
- SCALANCE XF-200BA с версии прошивки V4.2
- SCALANCE XP-200 с версии прошивки V4.2
- SCALANCE XR-300WG с версии прошивки V4.3
- SCALANCE XM-400 с версии прошивки V6.3 или V6.2 для однородных сетей
- SCALANCE XR-500 с версии прошивки V6.3 или V6.2 для однородных сетей

Роль

Примечание

Переконфигурация только при разомкнутой кольцевой сети!

Выбор роли зависит от следующих случаев применения.

- Вы хотите в топологии **с кольцевой сетью** использовать MRP только с устройствами Siemens, и никакие сигналы диагностики не контролировать.
Присвойте всем устройствам домены «mrpdomain-1» и роль «Manager (Auto)». Устройство, которое в рабочем режиме фактически принимает на себя роль устройства управления резервированием, автоматически согласуется среди устройств Siemens.
- Вы хотите в топологии **с несколькими кольцевыми сетями** использовать MRP только с устройствами Siemens, и никакие сигналы диагностики не контролировать.
 - Присвойте всем экземплярам устройства, соединяющего кольцевые сети, роль «Manager». Устройство с наименьшим MAC-адресом становится устройством управления.
 - Выберите для всех остальных устройств кольцевой топологии роль «Client».

5.3 Режим резервирования

- Вы хотите в кольцевой топологии использовать MRP также с не изготовленными Siemens устройствами, или получать с устройства сигналы диагностики о состоянии MRP (см. «Сигналы диагностики»).
 - Выберите только в одном устройстве в кольцевой сети роль «Manager (Auto)».
 - Выберите для всех остальных устройств кольцевой топологии роль «Client».
- Вы хотите деактивировать MRP.
Выберите опцию «Non Ring Member», если вы хотите использовать устройство не внутри кольцевой топологии с MRP.

Примечание

Роль при сбросе до заводских настроек

Разомкните кольцевую сеть перед сбросом устройства в этой сети до заводских настроек.

В новых и установленных на заводские настройки устройствах Siemens настроена следующая роль MRP.

- «Manager (Auto)»
 - CP
- «Automatic Redundancy Detection»
 - SCALANCE X-200
 - SCALANCE XB-200 (варианты PROFINET)
 - SCALANCE XC-200 (варианты PROFINET)
 - SCALANCE XF-200BA
 - SCALANCE XP-200 (варианты PROFINET)
 - SCALANCE X-300
 - SCALANCE X-400

В следующих новых и установленных на заводские настройки промышленных Ethernet-коммутаторах режим MRP деактивирован, а режим Spanning Tree активирован.

- SCALANCE XB-200 (варианты EtherNet/IP)
 - SCALANCE XC-200 (варианты EtherNet/IP)
 - SCALANCE XP-200 (варианты EtherNet/IP)
 - SCALANCE XR-300WG
 - SCALANCE XM-400
 - SCALANCE XR-500
-

Порт кольцевой сети 1 / порт кольцевой сети 2

Выберите здесь соответственно порт, который вы хотите спроектировать как порт кольцевой сети 1 или порт кольцевой сети 2.

В устройствах с более 8 портами в определённых случаях не все порты можно выбирать в качестве порта кольцевой сети.

Раскрывающийся список показывает для каждого типа устройства выбор возможных портов. Если эти порты настроены заводом-изготовителем, поля выделены серым цветом.

ВНИМАНИЕ
Порты кольцевой сети при сбросе до заводских настроек
При сбросе до заводских настроек выполняется сброс настроек портов кольцевой сети.

Примечание

Переконфигурация только при разомкнутой кольцевой сети

Сначала разомкните кольцевую сеть перед переконфигурацией портов кольцевой сети устройства управления кольцевой сетью.

Сигналы диагностики

Активируйте опцию «Diagnostics Alarms», если следует выдавать сигналы диагностики о состоянии MRP в локальный ЦП.

Могут выдаваться следующие сигналы диагностики.

- Ошибки кабельной проводки и ошибки порта
При возникновении следующих ошибок на портах кольцевой сети генерируются сигналы диагностики.
 - Обрыв соединения на каком-либо порте
 - Соседний элемент порта кольцевой сети не поддерживает MRP.
 - Порт кольцевой сети соединён с портом не кольцевой сети.
 - Порт кольцевой сети соединён с портом кольцевой сети другого домена MRP.
- Смена статуса активная/пассивная (только устройство управления резервированием)
Если в кольцевой сети меняется статус (активная/пассивная), генерируется сигнал диагностики.

Параметрирование резервирования не задано в ПО STEP7 (альтернативное резервирование)

Эта опция касается всех коммутаторов SCALANCE X. Выберите эту опцию при проектировании в ПО STEP7, если следует параметризовать свойства для резервирования средств передачи путём альтернативных механизмов, как например системы WBM, CLI или SNMP.

5.3 Режим резервирования

Когда активируется данная опция, имеющиеся настройки резервирования сохраняются и не перезаписываются. Параметры в поле «MRP Configuration» затем сбрасываются и отображаются серым цветом. Эти записи затем не имеют значения.

Примечание

Если для какого-либо устройства в кольцевой цепи активирована опция «Alternate Redundancy» и топология контролируется посредством ПО STEP7 (контроллер), в остальных устройствах в кольцевой сети также необходимо активировать опцию «Alternate Redundancy».

5.3.5 MRP Interconnection

5.3.5.1 Топология и принцип работы

Процедура MRP Interconnection является расширением процедуры MRP, которая позволяет выполнять резервное соединение двух или более кольцевых сетей MRP. Исключением являются сети изохронного реального времени (IRT). MRP Interconnection как и MRP описывается в стандарте МЭК 62439-2. С помощью MRP Interconnection возможно проведение очень быстрой реконфигурации. Время реконфигурации составляет обычно менее 200 миллисекунд.

Топология

На следующем рисунке показано резервное соединение двух кольцевых сетей MRP. Для резервного соединения в каждой сети необходимо наличие соединительной пары. На каждую кольцевую сеть MRP допускается наличие не более 5 соединительных пар.

Информацию о максимальном количестве активных соединений MRP Interconnection на каждое устройство можно найти в главе «Количественная структура».

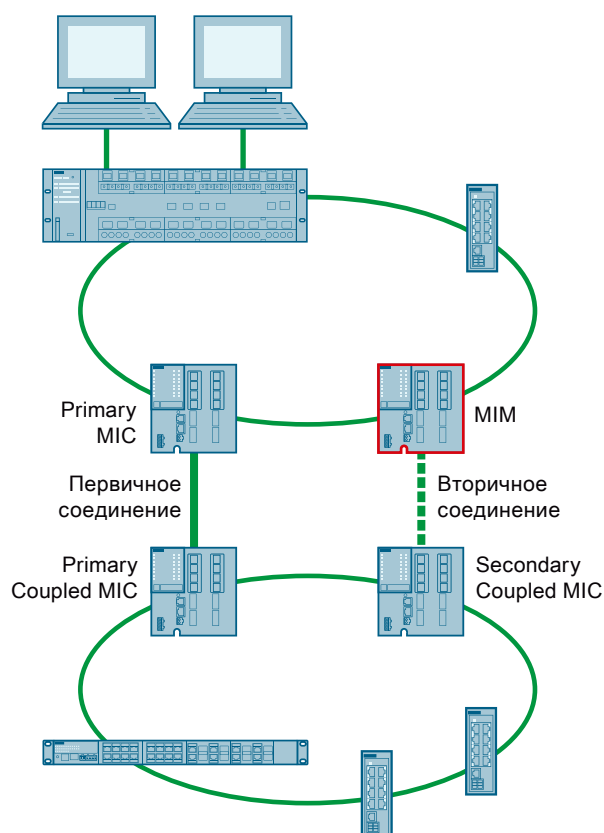


Рисунок 5-2 Резервное соединение двух кольцевых сетей с помощью MRP Interconnection

Принцип работы

Требованием для MRP Interconnection является применение MRP во всех задействованных кольцевых сетях. Для обоих соединений MRP Interconnection требуются четыре устройства.

- Устройство управления взаимосвязями при резервировании среды передачи (MIM, на рисунке показано красным контуром)
- Три клиента взаимосвязей при резервировании среды передачи (Primary MIC, Primary Coupled MIC и Secondary Coupled MIC)

Так как каждое устройство является частью кольцевой сети MRP, каждое устройство принимает заданную для MRP роль, следовательно MRP-Client или MRP-Manager.

В зависимости от статуса соединения порты Interconnection пересылают сообщения о статусе Primary MIC и Primary Coupled MIC (Link-Up или Link-Down) в MIM. Порты Interconnection представляют собой порты, между которыми имеется первичное или вторичное соединение. Благодаря этому MIM всегда получает информацию о статусе соединения между Primary MIC и Primary Coupled MIC («Первичное соединение»), а также своего собственного соединения с Secondary Coupled MIC («Вторичное соединение»). В обычном режиме работы обмен данными выполняется между обеими кольцевыми сетями через первичное соединение и MIM блокирует свой порт Interconnection. Если в устройство MIM поступает сигнал об отключении канала Link-Down первичного соединения, он переключает свой порт Interconnection в статус перенаправления

«Forwarding» и обмен данными между обеими кольцевыми сетями выполняется через вторичное соединение между MIM и Secondary Coupled MIC.

5.3.5.2 Устройства для MRP Interconnection

Подходящие устройства для MRP Interconnection

Устройство управления Interconnection, клиенты Interconnection, а также все устройства управления кольцевых сетей должны поддерживать MRP Interconnection. Это возможно в следующих устройствах.

- SCALANCE XB-200 с версии прошивки V4.3
- SCALANCE XC-200 с версии прошивки V4.2
- SCALANCE XF-200BA с версии прошивки V4.2
- SCALANCE XP-200 с версии прошивки V4.2
- SCALANCE XR-300WG с версии прошивки V4.3
- SCALANCE XM-400 с версии прошивки V6.3 или V6.2 для однородных сетей
- SCALANCE XR-500 с версии прошивки V6.3 или V6.2 для однородных сетей

IEC62439-2 ред.2 и IEC62439-2 ред.3

Некоторые определения MRP Interconnection при переходе с МЭК62439-2 редакции 2 на МЭК62439-2 редакции 3 были расширены или адаптированы. По причине межоперационной совместимости среди всего прочего был введён дополнительный MAC-адрес для MRP Interconnection. Результатом этого стало изменение используемых MAC-адресов для MRP Interconnection по сравнению с требованиями предыдущего стандарта. В данной главе приводится описание последствий на работу устройств SCALANCE.

Прошивка версии V6.2 для устройств SCALANCE XM-400 и XR-500

Технология MRP Interconnection, основанная на прошивке версии V6.2, работает только тогда в однородных сетях из устройств SCALANCE XM-400 и SCALANCE XR-500, когда все устройства имеют прошивку версии V6.2.

ВНИМАНИЕ

Отсутствие MRP Interconnection в неоднородных сетях с прошивкой версии V6.2

Активация MRP Interconnection в неоднородных сетях с устройствами SCALANCE XM-400/SCALANCE XR-500 и прошивкой версии V6.2 может привести к сбою в работе сети. MRP Interconnection в таких сетях, как правило, не следует активировать.

Прошивка версии V6.3 для устройств SCALANCE XM-400 и XR-500

С версии прошивки V6.3 MRP Interconnection для устройств SCALANCE XM-400 и SCALANCE XR-500 разрешена к применению и может использоваться без ограничений.

ВНИМАНИЕ
Обновление прошивки для MRP Interconnection
Для уже имеющихся в сети устройств SCALANCE XM-400 и SCALANCE XR-500 обновление прошивки до версии V6.3 обязательно для бесперебойной работы MRP Interconnection.

Работа MRP Interconnection с устройствами SCALANCE в неоднородных сетях возможна при следующих условиях.

- Все устройства SCALANCE XM-400 и SCALANCE XR-500 имеют прошивку версии V6.3 и выше.
- Все устройства SCALANCE XC-200, XF-200BA и XP-200 имеют прошивку версии V4.2 и выше.
- Все устройства SCALANCE XB-200 и SCALANCE XR300WG имеют прошивку версии V4.3 и выше.
- Все прочие сетевые компоненты отвечают требованиям стандарта МЭК 62439-2 редакции 3.

Прошивка версии V4.2 для устройств SCALANCE XC-200, XF-200BA и XP-200

С версии прошивки V4.2 MRP Interconnection для устройств SCALANCE XC-200, XF-200BA и XP-200 разрешена к применению и может использоваться без ограничений. Названные устройства могут соединяться с устройствами SCALANCE XM-400 и SCALANCE XR-500 с версии прошивки V6.3 с помощью MRP Interconnection.

Прошивка версии V4.3 для устройств SCALANCE XB-200 и SCALANCE XR300WG

С версии прошивки V4.3 MRP Interconnection для устройств SCALANCE XB-200 и SCALANCE XR300WG разрешена к применению и может использоваться без ограничений. Названные устройства могут соединяться с устройствами SCALANCE XM-400 и SCALANCE XR-500 с версии прошивки V6.3 с помощью MRP Interconnection.

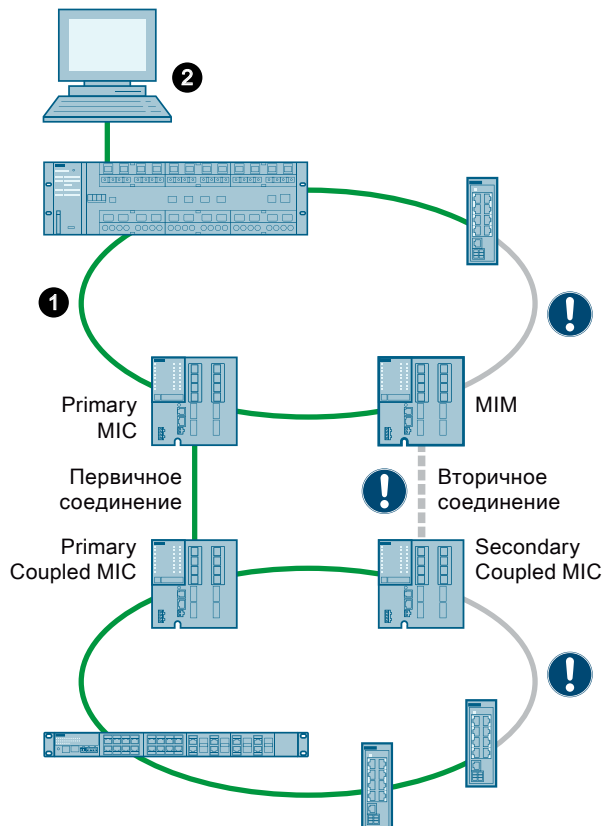
5.3.5.3 Конфигурирование соединения MRP Interconnection

В следующей главе приводится подробное описание процесса конфигурирования соединения MRP Interconnection. Выполняйте этапы конфигурации в указанной последовательности, чтобы не допустить образования петель сети. В процессе конфигурирования не всегда могут быть доступны все устройства для конфигурационного ПК. Указанная последовательность конфигурации гарантирует, что остаются доступными по меньшей мере неконфигурированные устройства. Номера позиций на рисунках соответствуют номерам последовательности этапов.

Описание подразделяется на три раздела.

- Соединение устройств и основная конфигурация (этап с 1 по 3)
- Конфигурирование кольцевого резервирования (этап с 4 по 7)
- Конфигурирование MRP Interconnection (этап с 8 по 16)

5.3.5.4 Соединение устройств и основная конфигурация



Этап 1: подсоединение проводов

В каждой кольцевой сети подсоедините устройства в соответствии с запланированной топологией, выполнив не более одного участка соединения в каждом случае. Также не допускается пока соединять оба предусмотренные для вторичного соединения устройства (MIM и Secondary Coupled MIC).

Этап 2: присвоение IP-адреса

Для доступа к устройствам используйте подключённый к сети ПК. Присвойте каждому устройству IP-адрес, например, с помощью SINEC PNI. Затем сконфигурируйте устройства с помощью WBM или CLI.

Этап 3: конфигурирование Spanning Tree

Выполните следующие оба этапа для каждого устройства, если для вашей топологии сети требуется Spanning Tree. Деактивируйте режим Spanning Tree для каждого устройства, если он не требуется.

- Установите для совместимости протоколов параметр «RSTP». (Команда меню WBM «Layer 2 > Spanning Tree», вкладка «General», раскрывающийся список «Protocol Compatibility»)
- Деактивируйте режим Spanning Tree для кольцевых портов и портов MRP Interconnection. (Команда меню WBM «Уровень 2 > Spanning Tree», вкладка «Порт CIST», столбец таблицы «Spanning Tree Status»)

5.3.5.5 Конфигурация кольцевого резервирования

В WBM для конфигурирования кольцевого резервирования имеется меню «Layer 2 > Ring Redundancy». На вкладке «Ring» выполните этапы с 4 по 6 для каждого устройства.

The screenshot shows the 'Ring Redundancy' configuration interface. The 'Ring' tab is selected. The 'Ring Redundancy' checkbox is checked. The 'Ring Redundancy Mode' is set to 'MRP Auto-Manager'. The 'Ring Ports' are set to 'P0.1' and 'P0.2'. There is an 'Observer' checkbox and a 'Restart Observer' button. At the bottom are 'Set Values' and 'Refresh' buttons.

Этап 4: задание портов кольцевой сети

В раскрывающихся списках выберите подходящие записи для кольцевых портов.

Примечание

Если выбранные порты имеют различные свойства аппаратного обеспечения, появляется сообщение «Port Configuration of the Ring Ports is different». Сообщение может появляться по следующим причинам.

- Различная скорость передачи данных (порт гигабитной сети Ethernet / порт ускоренной сети Ethernet)
- Различный режим передачи данных (дуплексный режим / полудуплексный режим)
- Различные среды передачи данных (медный провод / волоконно-оптический кабель)

Проверьте в этом случае, предполагалась ли конфигурация фактически в этой форме. Как правило, различные свойства портов кольцевой сети приводят к функциональным ограничениям, даже если принципиально возможна передача данных.

Подробную информацию о свойствах портов можно найти в меню «System > Ports».

Этап 5: активация режима MRP

Активируйте флажок опции «Ring Redundancy» для включения MRP.

Этап 6: присвоение роли MRP

Для процедуры MRP в раскрывающемся списке «Ring Redundancy Mode» имеются следующие записи:

- MRP Auto-Manager
- MRP Client

Сконфигурируйте для двух устройств в каждой кольцевой сети процедуру кольцевого резервирования «MRP Auto-Manager», чтобы также при выходе из строя какого-либо устройства могла следовать незамедлительная реконфигурация кольцевой сети MRP.

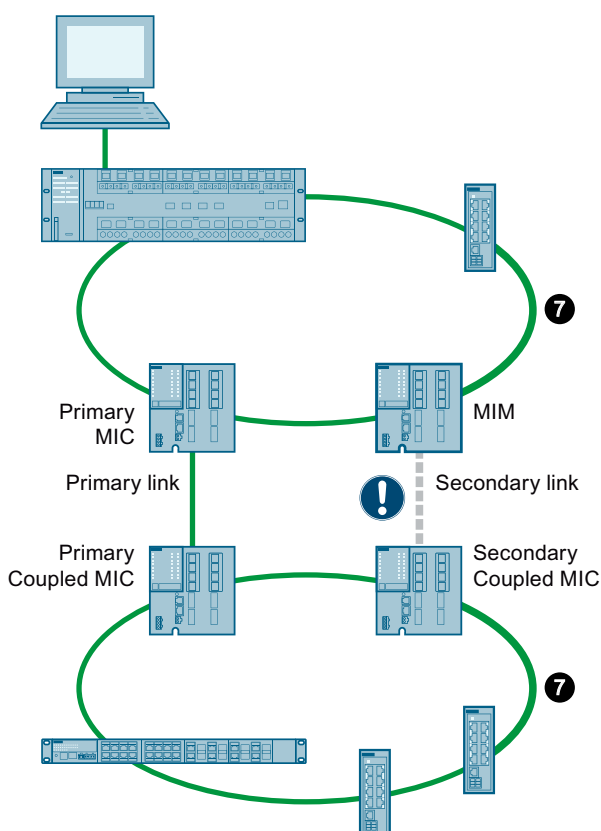
Примечание

Когда больше чем одному устройству присваивается процедура кольцевого резервирования «MRP Auto-Manager», устройство с наименьшим MAC-адресом становится устройством управления. Остальные устройства автоматически настраиваются на рабочий режим «MRP-Client».

Затем щёлкните кнопку «Set Values», чтобы сохранить конфигурацию.

Этап 7: подключение кольцевых сетей

После конфигурирования всех устройств в обеих кольцевых сетях для MRP замкните обе кольцевые сети MRP, подключив кабели между устройствами, которые ещё не были соединены. Провод между MIM и Secondary Coupled MIC пока не подсоединять.



Информация о кольцевом резервировании

Информацию и текущем состоянии кольцевого резервирования можно найти в системе WBM и CLI.

- **WBM**
Меню «Information > Redundancy», вкладка «Ring Redundancy»
- **CLI**
Команда `show ring-redundancy` в режиме User EXEC или в Privileged EXEC

5.3.5.6 Конфигурация MRP Interconnection

В резервированном соединении двух кольцевых сетей с MRP Interconnection участвуют четыре устройства. При конфигурировании этих устройств необходимо соблюдать определённую последовательность, чтобы были доступны ещё не сконфигурированные устройства для конфигурационного ПК. Учитывайте следующее правило.

5.3 Режим резервирования

Сначала сконфигурируйте устройства с соединением MRP Interconnection в кольце MRP, к которому не подключён ПК для настройки. Начните с устройства, для соединения MRP Interconnection которого пока никакой провод не подсоединён, в представленном примере с устройством «Secondary Coupled MIC».

В результате получается следующая последовательность конфигурирования.

1. Secondary Coupled MIC
2. Primary Coupled MIC
3. Primary MIC
4. MIM

Примечание**Доступность устройств и сообщение об ошибке из-за отсутствия провода**

- После конфигурирования устройств Secondary Coupled MIC и Primary Coupled MIC обе кольцевые сети разомкнуты и оба названных устройства больше недоступны.
- После конфигурирования устройства Primary MIC снова доступны устройства Secondary Coupled MIC и Primary Coupled MIC, а также все другие устройства второй кольцевой сети.
- После конфигурирования устройства MIM выдаётся сообщение об ошибке. Причиной ошибки является ещё неподсоединённый провод между устройствами MIM и Secondary Coupled MIC. Когда этот провод подсоединяется после завершения конфигурирования (этап 16), ошибка исчезает.

В WBM для конфигурирования кольцевого резервирования имеется меню «Layer 2 > Ring Redundancy». На вкладке «MRP Interconnection» выполните этапы с 8 по 15 для каждого устройства.

MRP Interconnection

Ring Standby Link Check **MRP Interconnection**

15 ☒ MRP Interconnection

Select	Interconnection Domain ID	Interconnection Domain Name	Interconnection Port	Wait (Manager)	Role/Position	Status
☐	1	MrpIntCon	P0.1	☒	Manager	☒

1 entry.

8

Этап 8: создание записи таблицы для нового соединения

Щёлкните кнопку «Create», чтобы создать в таблице с соединениями MRP Interconnection новую строку.

Этап 9: присвоение идентификатора домена Interconnection

Введите идентификатор домена Interconnection. При присвоении ID соблюдайте следующие правила:

- ID домена Interconnection не должен иметь значение «0».
- Для всех четырёх устройств, используемых для соединения кольцевых сетей, необходимо конфигурировать одинаковый Interconnection Domain ID.

Этап 10: присвоение имени домена Interconnection

Введите любое имя для соединения Interconnection. Необходимо задать имя, хотя это имя не влияет на параметры конфигурации. В качестве допустимых символов для имени можно использовать буквы от A до Z и от a до z, а также цифры от 0 до 9 и символ «-». В качестве первого и последнего символа имени нельзя использовать дефис. В имени нельзя использовать пробелы. Имя домена Interconnection должно состоять по меньшей мере из одного символа и содержать не более 240 символов.

Этап 11: задание порта Interconnection

В раскрывающемся списке выберите порт, который используется для соединения MRP Interconnection. Обратите внимание на следующие ограничения:

- Порт не должен быть отключён или заблокирован. Нельзя активировать функцию «Unicast Blocking» для порта.
- Порт не должен использоваться для функции Link Aggregation.
- Порт не должен быть портом мониторинга функции «Mirroring».
- Порт не должен быть портом Spanning Tree.
- Порт не должен быть кольцевым портом.
- Порт не должен быть портом 802.1X Authenticator.
- Порт не должен быть портом 802.1X Supplicant.
- Дополнительно для устройств SCALANCE XM-400 и SCALANCE XR-500: Порт не должен быть портом маршрутизатора.

Этап 12: выбор роли и положения устройства

Каждому устройству, которое задействовано в соединении MRP Interconnection, необходимо назначить роль. Имеется две роли «Manager» (устройство управления) и «Client» (клиент). Для клиентов также задаётся состояние («Primary» или «Secondary»). Выберите в раскрывающемся списке столбца таблицы «Role/Position». В представленном примере устройствам назначены следующие роли.

Устройство	Роль
Secondary Coupled MIC	Secondary Client
Primary Coupled MIC	Primary Client
Primary MIC	Primary Client
MIM	Manager

Этап 13: активация опции «Ожидание» для устройства управления

В устройствах с ролью «Client» флажки опций в этом столбце деактивированы. На устройстве с ролью «Manager» активируйте флажок опции «Wait (Manager)», чтобы передача данных запускалась лишь тогда, когда первичный клиент (Primary Client) будет готов к работе для MRP Interconnection.

Этап 14: активация соединения MRP Interconnection

Активируйте флажок опции «Status», чтобы активировать соединение MRP Interconnection. Обратите внимание на следующие правила:

- Если не активировано по меньшей мере одно соединение MRP Interconnection, для устройства невозможно включение MRP Interconnection.
- Для количества активных соединений MRP Interconnection действуют следующие максимальные значения:
 - SCALANCE XM-400 и XR-500 с версии прошивки V6.3 и SCALANCE XC-200, SCALANCE XP-200, SCALANCE XF-200BA с версии прошивки V4.3
Два соединения
 - SCALANCE XB-200 и SCALANCE XR-300WG с версии прошивки V4.3
Одно соединение

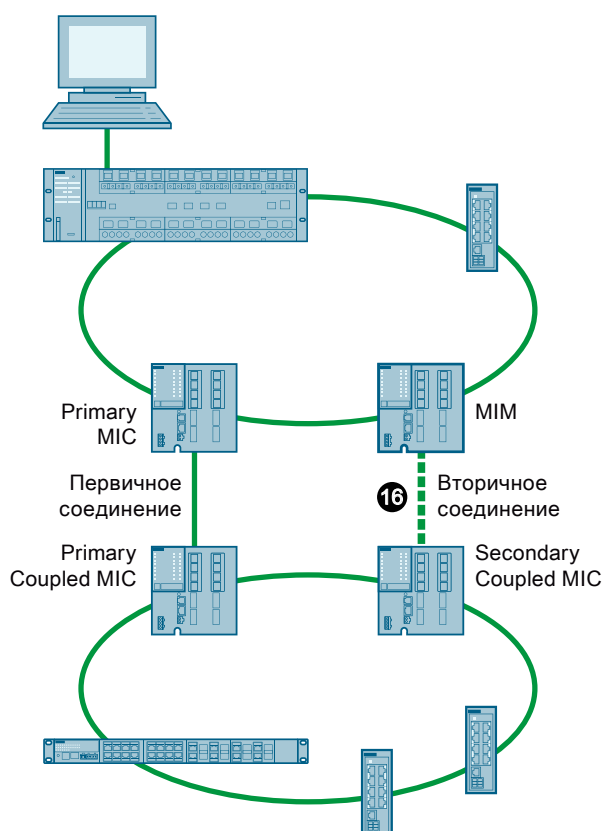
Щёлкните кнопку «Set Values».

Этап 15: активация MRP Interconnection для устройства

Установите флажок «MRP Interconnection» для включения MRP Interconnection. Затем щёлкните кнопку «Set Values», чтобы сохранить конфигурацию.

Этап 16: подсоединение провода для вторичного соединения

После выполнения конфигурирования всех устройств в обеих кольцевых сетях для MRP Interconnection, подсоедините провод для вторичного соединения между устройствами MIM и Secondary Coupled MIC. После этого светодиод ошибок перестает гореть. После этого соединение MRP Interconnection функционирует.



Информация о MRP Interconnection

Актуальную информацию о MRP Interconnection можно найти в системе WBM и CLI.

- **WBM**
Меню «Information > Redundancy», вкладка «MRP Interconnection»
- **CLI**
Команда `show ring-redundancy` в режиме User EXEC или в Privileged EXEC

5.3.6 Standby

Общая информация

Коммутаторы SCALANCE X помимо кольцевого резервирования внутри кольцевой сети поддерживают также резервное соединение кольцевых сетей или открытых сетевых сегментов (линий). При резервном соединении кольцевые сети соединяются между собой через два Ethernet-соединения. Для этого в кольцевой сети конфигурируется пара ведущего/ведомого устройств с взаимным контролем, которая перенаправляет трафик в случае ошибки с используемого обычным образом Ethernet-соединения ведущего (Master) устройства на резервное Ethernet-соединения ведомого (Slave) устройства.

Резервирование Standby

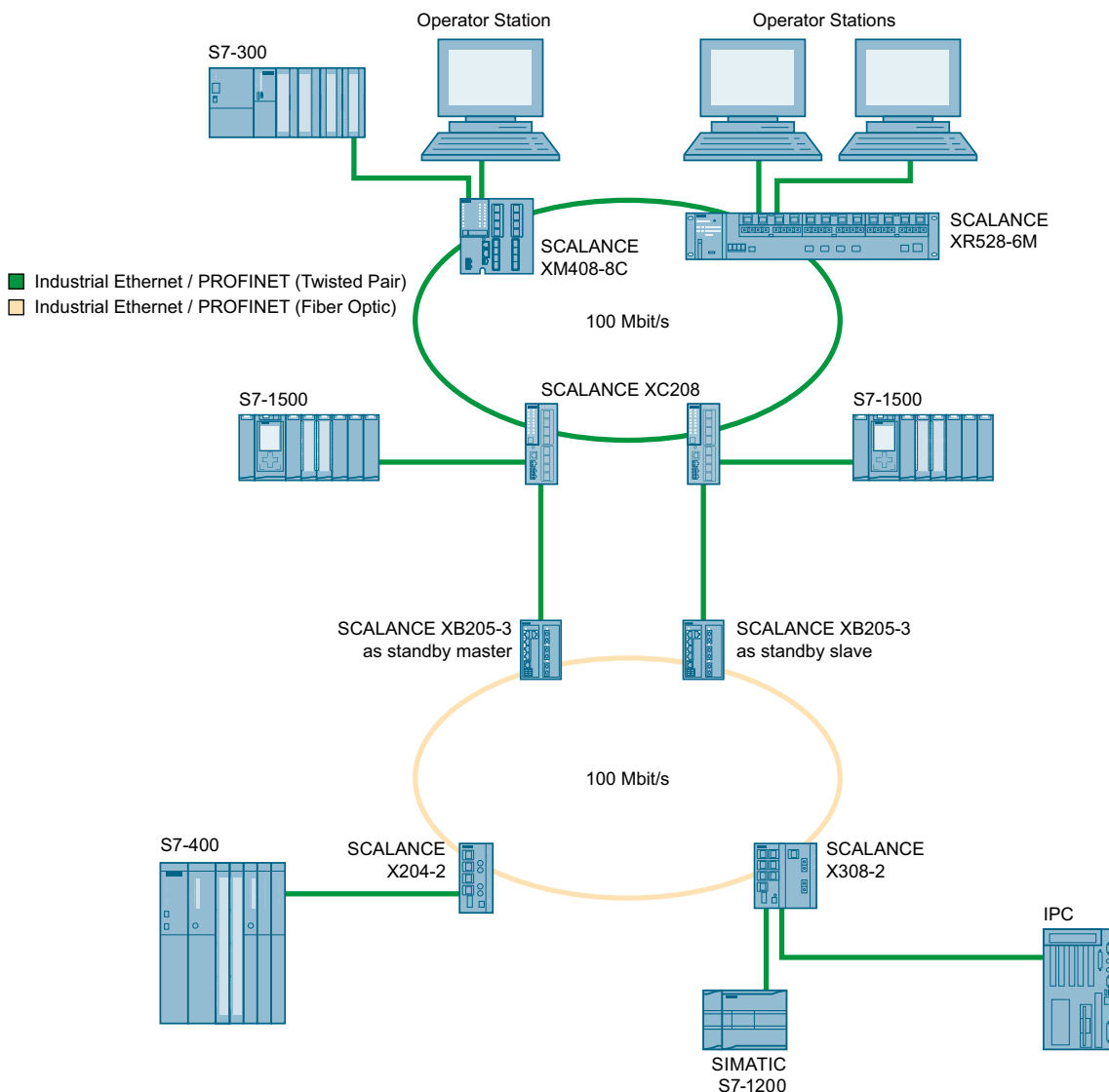


Рисунок 5-3 Пример резервного соединения двух кольцевых сетей

Для резервного соединения, как показано на рисунке, два устройства внутри одного сетевого сегмента должны проектироваться как коммутаторы резервирования замещением. Сетевыми сегментами здесь являются кольцевые сети с устройством управления резервированием. На месте кольцевых сетей могут при этом выступать также сетевые сегменты в линейной форме.

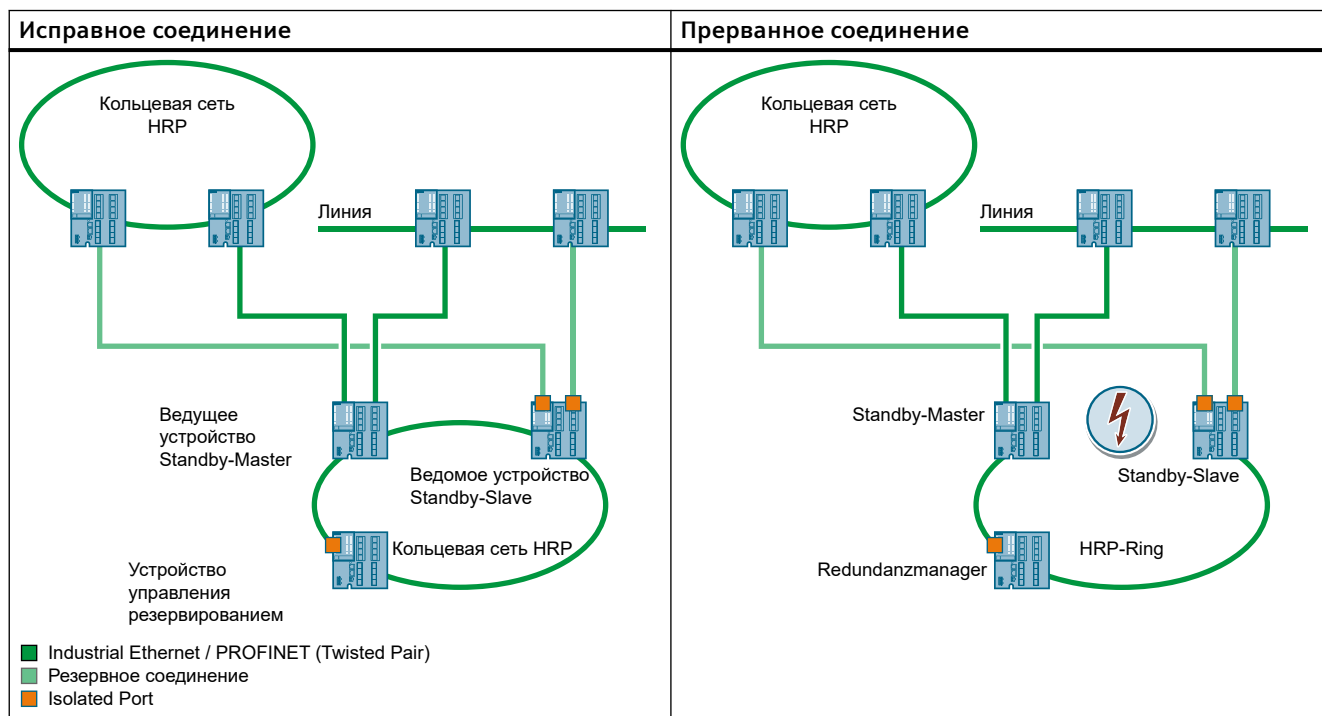
Оба коммутатора резервирования замещением, соединённые путём проектирования, обмениваются между собой датаграммами и синхронизирует таким образом своё рабочее состояние (одно устройство становится ведущим устройством, а другое — ведомым). В исправном состоянии только на ведущем устройстве активен участок соединения с другим сетевым сегментом. При выходе такого участка соединения из строя (например, вследствие Link-Down или сбоя устройства) ведомое устройство активирует свой участок соединения, пока присутствует ошибка.

Соединение нескольких сетевых сегментов HRP

Если несколько кольцевых сетей HRP или линий соединяются через резервирование замещением, устройства Standby-Master и Standby-Slave должны находиться в замкнутом сетевом сегменте. Данный сегмент ни в коем случае не должен быть разомкнутым, т. е. какой-либо линией.

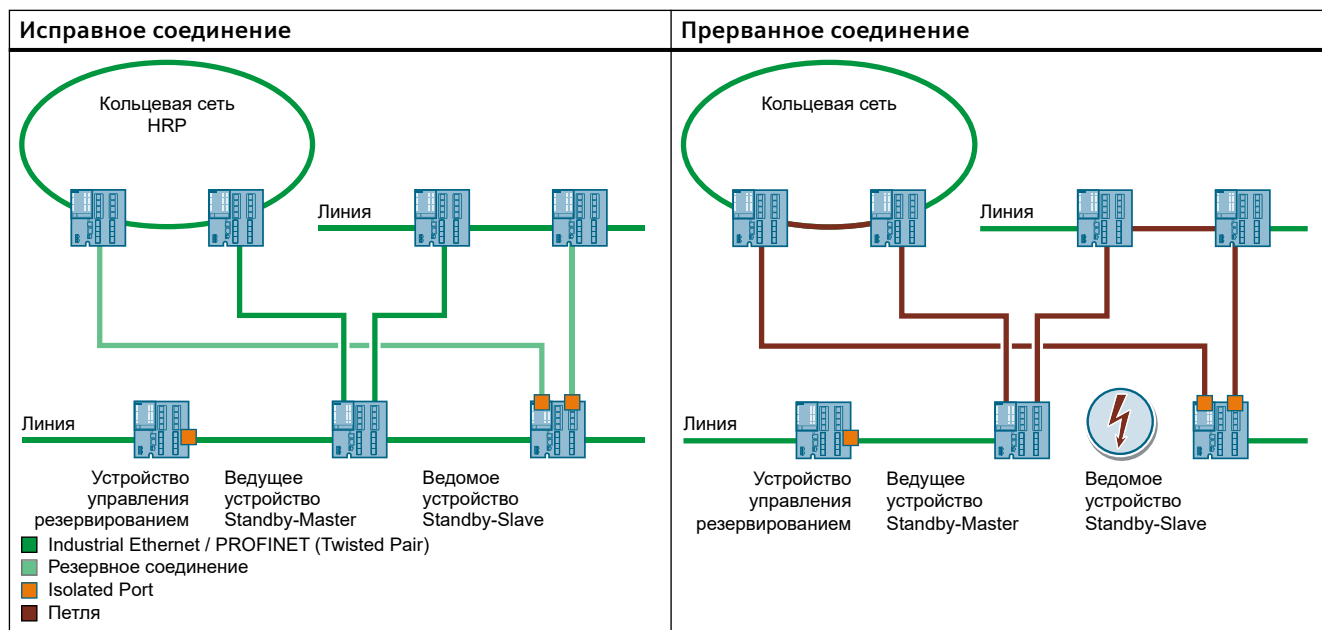
Устройства Standby-Master и Standby-Slave в замкнутом сетевом сегменте

Если прерывается соединением между устройствами Standby-Master и Standby-Slave, оба устройства могут по-прежнему обмениваться данными через резервный участок устройства управления резервированием HRP.



Устройства Standby-Master и Standby-Slave в разомкнутом сетевом сегменте

Если прерывается соединением между устройствами Standby-Master и Standby-Slave, оба устройства не смогут по-прежнему обмениваться данными. Это приводит к образованию петли на соединённых сетевых сегментах.



5.3.7 Link Check

Контроль оптических соединений в кольце

В оптических участках передачи данных возможны неисправности, при которых оптическое соединение прерывается не полностью, но лишь периодически теряются пакеты. Такие неисправности могут быть вызваны, например, дефектными оптическими кабелями, загрязнёнными штекерными разъёмами или повреждениями устройств.

Устройство управления резервированием кольцевой сети HRP или MRP с оптическими соединениями распознаёт при такой неисправности неустранимую ошибку кольцевой сети «Non-Recoverable Ring Error». Устройство управления резервированием не может устранять неисправности, замыкая кольцевую сеть. Замыкание кольцевой сети в этом случае привело бы к циркулирующим пакетам.

С помощью функции Link Check можно контролировать качество передачи данных на оптических участках внутри кольцевой сети HRP или MRP, идентифицировать неисправные участки передачи данных и отключать их при определённых условиях. Когда неисправный участок отключён, устройство управления резервированием может замкнуть кольцевую сеть и восстановить связь.

Принцип действия функции Link Check

Характеристики при бесперебойном соединении

Если функция Link Check активируется на двух соединённых портах кольцевой сети, оба партнёра соединения обмениваются через эти порты циклично тестовыми пакетами функции Link Check. Пакеты, которые получает один партнёр связи, этот партнёр пересылается другому.

Когда устройства от партнёров соединения получают обратно свои отправленные пакеты, соединение подготовлено для функции Link Check. Затем партнёры связи увеличивают частоту передачи тестовых пакетов функции Link Check и собственно процесс контроля соединения становится активным.

Характеристики при сбое в работе

При активном контроле соединения можно увидеть количество отправленных и полученных тестовых пакетов функции Link Check на странице Information > Redundancy > Link Check. На основании этой статистики можно распознавать даже незначительные сбои в работе, при которых неисправность не ведёт пока к отключению участка передачи данных посредством функции Link Check.

Функция Link Check распознаёт соединение как неисправное и отключает его, если в течение определённых периодов времени теряется слишком большое количество тестовых пакетов. Функция Link Check использует при этом несколько временных интервалов, чтобы распознавать как внезапное появление ошибок, так и непрерывную, низкую интенсивность ошибок.

Порт, который отключался функцией Link Check, должен сбрасываться, чтобы снова обмениваться данными. При этом есть 2 возможности.

- Извлеките соединительный кабель и снова подсоедините его.
- Сбросьте функцию на обоих партнёрах связи нажатием кнопки «Reset». Это необходимо выполнять на обоих устройствах в течение 30 с.

Примечание

Когда используется кнопка «Reset», могут образоваться кратковременные коммутационные петли и, следовательно, сбой обмена данными. Петля автоматически исчезает.

Если в вашем случае применения это неприемлемо, сбросьте функцию Link Check, отсоединив соединительный кабель и вновь подсоединив его.

После сброса Link Check функция перезапускается на порте, а статистика сбрасывается.

Проектирование через контроллер ввода-вывода данных PROFINET

Если MRP проектируется через контроллер ввода-вывода данных PROFINET, функцию Link Check можно подключить с помощью WBM или CLI для оптических портов кольцевой сети 1-го экземпляра кольцевой сети MRP.

5.3 Режим резервирования

Когда передаётся новое проектирование, функция Link Check автоматически деактивируется на всех портах, которые не были сконфигурированы в качестве портов кольцевой сети 1-го экземпляра кольцевой сети MRP.

Примечание

События, которые касаются функции Link Check, сигнализируются только косвенно посредством ввода-вывода данных PROFINET. Если активированы сигналы диагностики MRP и деактивируется порт кольцевой сети посредством функции LinkCheck, системой ввода-вывода Profinet создаётся сообщение об ошибке, что это соединение перестало существовать.

5.3.8 Parallel Redundancy Protocol (протокол параллельного резервирования)

Parallel Redundancy Protocol (протокол параллельного резервирования)

Протокол Parallel Redundancy Protocol (PRP) представляет собой резервный протокол для сетей Ethernet. Его определение приводится в части 3 стандарта МЭК 62439. Данная процедура резервирования позволяет при обрывах сети сохранять обмен данными без прерывания / времени реконфигурации.

Процедура PRP поддерживается, например, устройствами линейки изделий SCALANCE X-200RNA.

Кадры чрезмерной длины

При передаче кадров PRP промышленный Ethernet-коммутатор расширяет кадр на метку конца PRP. В кадрах с максимальной длиной образуется вследствие добавленной метки конца PRP кадр чрезмерной длины, который превышает допустимую длину кадра (согласно стандарту IEEE 802.3).

Чтобы исключить потери данных при кадрах чрезмерной длины, все сетевые компоненты, которые находятся в сети PRP, должны поддерживать длину кадра не менее 1528 байтов.

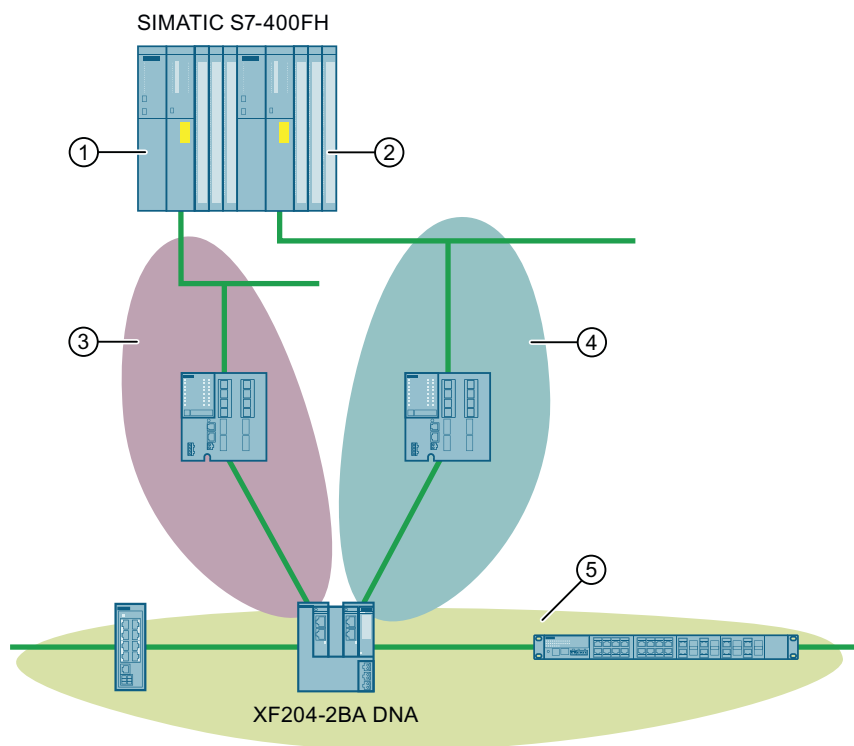
Устройства, описание которых приводится в данной инструкции, могут использоваться в сетях PRP, см. также главу «Количественная структура (Страница 21)».

5.3.9 Dual Network Access (DNA)

Принцип работы и топология

Dual Network Access (DNA) — технология для соединения сети с двумя разделёнными друг от друга сетями. Коммутатор, который предоставляет данную функцию, обозначается также как «Y-коммутатор». Такое обозначение касается соединений коммутатора с обеими другими сетями. Порты Y-коммутатора для соединения с обеими разделёнными сетями являются DNA-портами.

Типичный случай применения — интеграция резервного контроллера в кольцевую сеть MRP. Возможна также интеграция линейной топологии, как представлено на следующем рисунке.



- ① Первый контроллер резервной системы управления
- ② Второй контроллер резервной системы управления
- ③ Сеть первого контроллера
- ④ Сеть второго контроллера
- ⑤ Общая сеть (в этом примере: линейная топология), оба контроллера имеют доступ к этой сети.

Первый DNA-порт Y-коммутатора соединён с сетью ③, второй DNA-порт — с сетью ④. Y-коммутатор гарантирует, что обе сети ③ и ④ разделены друг от друга. С устройств в сети ③ невозможно доступ к устройствам в сети ④ и наоборот.

Другие порты Y-коммутатора, которые не являются DNA-портами, соединяют обе сети ③ и ④ с сетью ⑤. Устройства в сети ⑤ могут быть доступны как с сети ③, так и с сети ④. В сети ⑤ используются устройства, работающие как устройства S2 и как таковые устанавливают связь с обоими контроллерами.

Примечание

В качестве Y-коммутатора можно использовать следующие устройства.

- SCALANCE XF204-2BA DNA
-

5.3.10 Dual Network Access-Redundanz (DNA-Redundanz)

Принцип работы и топология

Под DNA-резервированием понимается применение резервного двойного сетевого доступа для соединения сети с двумя разделёнными друг от друга сетями. Для этого используются два Y-коммутатора, устройство управления DNA и DNA-клиент. DNA-резервирование возможно только с кольцевой сетью MRP. Y-коммутатор принимает роли устройства управления MRP и устройства управления DNA, а второй Y-коммутатор — роли MRP-клиента и DNA-клиента. Соединение с обеими разделёнными сетями установлено, когда работает по меньшей мере один Y-коммутатор.

В обычном режиме работы DNA-порты DNA-клиента заблокированы, DNA-порты устройства управления DNA находятся в состоянии «Forwarding». Если DNA-клиент перестаёт получать пакеты MRP с устройства управления, так как он, например, отключён, он переключает оба свои DNA-порта в состояние «Forwarding».

Примечание

В качестве устройства управления DNA или DNA-клиента можно использовать следующие устройства.

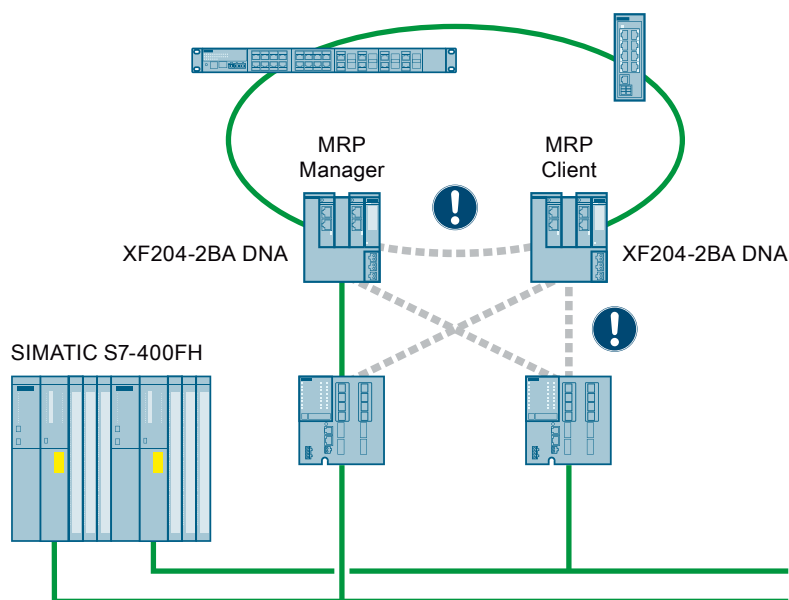
- SCALANCE XF204-2BA DNA
-

Конфигурирование DNA-резервирования

В следующем разделе приводится описание процесса конфигурирования DNA-резервирования. Соблюдайте указанную последовательность этапов конфигурирования, чтобы предотвратить образование шлейфов в сети.

Этап 1: соединение устройств

Подсоедините все устройства кольцевой сети MRP до соединения между устройством управления MRP и MRP-клиентом. Соедините только DNA-порт устройства управления MRP с одним из контроллеров или с коммутатором, к которому подсоединен контроллер.



Этап 2: Конфигурация

Если устройствам не нужно использовать функции PROFINET, то DNA-резервирование можно создавать без ПО STEP7 Classic. Сконфигурируйте MRP и DNA-резервирование, используя прямой доступ к устройствам с помощью WBM или CLI. Оба устройства доступны через кольцевую сеть MRP. Так как кольцевая сеть MRP ещё разомкнута, циркулирующие пакеты исключаются, даже если сначала ещё никакая MRP-конфигурация не была активна.

Этап 2 без функций PROFINET в системе Web Based Management

1. Откройте систему WBM Y-коммутатора, который должен принять функцию устройства управления DNA.
2. Откройте страницу WBM «Layer 2 > Ring Redundancy > Ring»:

3. Установите флажок «Ring Redundancy».
4. Выберите в раскрывающемся списке «Ring Redundancy Mode» запись «MRP Manager».
5. Выберите в обоих раскрывающихся списках «Ring Ports» кольцевые порты MRP Manager.
6. Активируйте флажок опции «DNA Redundancy». Оба порта, которые не являются портами кольцевой сети, являются DNA-портами.
7. Щёлкните кнопку «Set values».
8. Откройте систему WBM Y-коммутатора, который должен принять функцию DNA-клиента.
9. Откройте страницу WBM «Layer 2 > Ring Redundancy > Ring».
10. Установите флажок «Ring Redundancy».
11. Выберите в раскрывающемся списке «Ring Redundancy Mode» запись «MRP Client».
12. Выберите в обоих раскрывающихся списках «Ring Ports» кольцевые порты MRP Client.
13. Активируйте флажок опции «DNA Redundancy». Оба порта, которые не являются портами кольцевой сети, являются DNA-портами.
14. Щёлкните кнопку «Set values».
15. Сконфигурируйте остальные устройства в кольцевой сети в качестве MRP-клиентов.

Этап 2 без функций PROFINET с Command Line Interface

1. Откройте систему CLI Y-коммутатора, который должен принять функцию устройства управления DNA, в консоли Windows.
2. В глобальном режиме конфигурирования выполните следующую команду:
ring-redundancy mode mrpmanager

3. Сконфигурируйте порты кольцевой сети в режиме конфигурирования резервирования с помощью следующей команды:

```
ring ports <interface-type> <interface-id> <interface-type> <interface-id>
```

Параметры — тип интерфейса и обозначение интерфейса для обоих портов кольцевой сети.
Пример:
Чтобы сконфигурировать одинаковые порты кольцевой сети как в предыдущем скриншоте, требуется следующая команда:

```
ring ports fa 1/1 fa 2/1
```

Оба порта, которые не являются портами кольцевой сети, являются DNA-портами. В примере это порты 1/2 и 2/2.
4. Сконфигурируйте DNA-резервирование в глобальном режиме конфигурирования с помощью следующей команды:

```
ring-redundancy dna-redundancy
```
5. Откройте систему CLI Y-коммутатора, который должен принять функцию DNA-клиента, в консоли Windows.
6. В глобальном режиме конфигурирования выполните следующую команду:

```
ring-redundancy mode mrpclient
```
7. Сконфигурируйте порты кольцевой сети в режиме конфигурирования резервирования с помощью следующей команды:

```
ring ports <interface-type> <interface-id> <interface-type> <interface-id>
```

Параметры — тип интерфейса и обозначение интерфейса для обоих портов кольцевой сети. Оба порта, которые не являются портами кольцевой сети, являются DNA-портами.
8. Сконфигурируйте DNA-резервирование в глобальном режиме конфигурирования с помощью следующей команды:

```
ring-redundancy dna-redundancy
```
9. Сконфигурируйте остальные устройства в кольцевой сети в качестве MRP-клиентов.

Примечание

Деактивируйте DNA-резервирование в глобальном режиме конфигурирования с помощью следующей команды:

```
no ring-redundancy dna-redundancy
```

Этап 2 с функциями PROFINET

Если устройствам нужно использовать функции PROFINET, то DNA-резервирование нужно конфигурировать в ПО STEP7 Classic. Для этого выполните следующие этапы.

Примечание**Загрузка файла GSDML в ПО STEP7 Classic**

DNA-резервирование доступно с версии прошивки V4.2. В определённых случаях файл GSDML Y-коммутатора сначала необходимо загрузить в ПО STEP7 Classic, перед тем как конфигурировать DNA-резервирование с функциями PROFINET в ПО STEP7 Classic. Файл GSDML устройства можно найти в следующем меню WBM: System > Load&Save > GSDML.

1. Откройте программу HW Config.
2. Отметьте Y-коммутатор, который должен принять роль устройства управления DNA, и откройте диалоговое окно «PNIO Properties».
3. Щёлкните вкладку «Media Redundancy» и сконфигурируйте следующие параметры.
 - Role
Выберите настройку «Manager».
 - Ring Ports
Порты кольцевой сети устройства управления MRP.
 - Domains
Оба Y-коммутатора должны находиться в одинаковом домене.
4. Щёлкните вкладку «Parameters» и активируйте флажок опции «DNA Redundancy». Устройство управления MRP будет также устройством управления DNA.
5. Щёлкните кнопку «ОК» для завершения конфигурирования DNA Manager.
6. Отметьте Y-коммутатор, который должен принять роль DNA-клиента, и откройте диалоговое окно «PNIO Properties».
7. Щёлкните вкладку «Media Redundancy» и сконфигурируйте следующие параметры.
 - Role
Выберите настройку «Client».
 - Ring Ports
Порты кольцевой сети MRP-клиента.
 - Domains
Оба Y-коммутатора должны находиться в одинаковом домене.
8. Щёлкните вкладку «Parameters» и активируйте флажок опции «DNA Redundancy». MRP-клиент будет также DNA-клиентом.
9. Щёлкните кнопку «ОК» для завершения конфигурирования DNA Client.
10. Сконфигурируйте остальные устройства в кольцевой сети в качестве MRP-клиентов. Все MRP-клиенты должны принадлежать к домену устройства управления MRP.
11. Загрузите конфигурацию в контроллер.

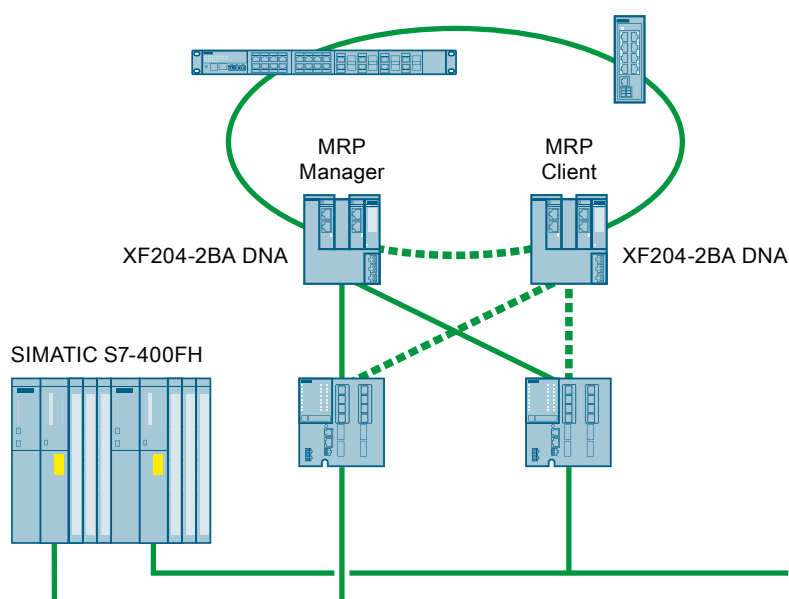
Примечание

Выполняйте проектирование топологии в ПО STEP7 Classic.

Состояние DNA-портов невозможно контролировать с помощью функции «MRP Diagnostics Alarm» контроллера. Для контроля соединений между Y-коммутатором и контроллером необходимо спроектировать топологию в ПО STEP7 Classic.

Этап 3: подсоединение проводов

Подсоедините кольцевую сеть MRP. Подсоедините оставшиеся порты DNA к контроллерам или коммутаторам, к которым подсоединены контроллеры.

**5.4 VLAN****5.4.1 Основы****Определение сети вне зависимости от пространственного положения участников**

VLAN (виртуальная локальная сеть или Virtual Local Area Network) делит физическую сеть на множество логических сетей, которые экранированы друг от друга. При этом устройства скомпонованы в логические группы. Только узлы одной сети VLAN могут обращаться друг к другу. Поскольку многоадресные и широковещательные пакеты также передаются только в пределах соответствующей сети VLAN, мы говорим о широковещательных доменах.

5.4 VLAN

Отсюда в качестве особого преимущества сети VLAN возникает уменьшенная сетевая нагрузка для участников или сегментов других сетей VLAN.

Для обозначения того, какой пакет к какой сети VLAN относится, пакет расширяется на 4 байта (Маркировка VLAN (Страница 82)). Это расширение наряду с идентификатором VLAN содержит также информацию о приоритетности.

Возможности присвоения VLAN

Каждому порту устройства присваивается идентификатор VLAN (идентификатор VLAN на основе порта). Идентификатор VLAN на основе порта конфигурируется в разделе «Layer 2 > VLAN > Port Based VLAN (Страница 297)».

5.4.2 Маркировка VLAN

Расширение Ethernet-пакетов на четыре байта

Для CoS (Class of Service, определение приоритетов пакетов) и для VLAN в стандарте IEEE 802.1Q было установлено расширение Ethernet-пакетов на размер тега VLAN.

Примечание

Из-за тега VLAN допустимая общая длина пакета увеличивается с 1518 до 1522 байт. Требуется проверка того, способны ли конечные участники сети обрабатывать такую длину/такой тип пакета. Если это не так, то таким участникам разрешается отправлять пакеты только со стандартной длиной.

Дополнительные 4 байта находятся в заголовке Ethernet-пакета между адресом источника и полем типа/длины Ethernet:

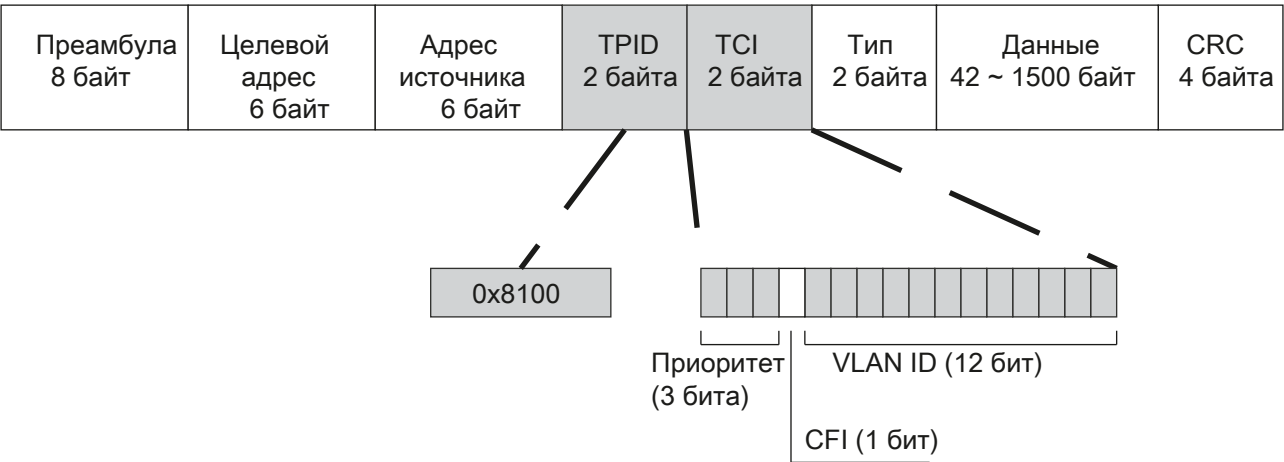


Рисунок 5-4 Структура расширенного Ethernet-пакета

Дополнительные байты содержат идентификатор протокола тега, Tag Protocol Identifier (TPID), и контрольную информацию тега, Tag Control Information (TCI).

Идентификатор протокола тега, Tag Protocol Identifier (TPID)

Первые 2 байта формируют идентификатор протокола тега, Tag Protocol Identifier (TPID), и фиксированно заняты 0x8100. Это значение указывает, что пакет данных содержит сведения VLAN или данные о приоритетности.

Контрольная информация тега, Tag Control Information (TCI)

Два байта контрольной информации тега, Tag Control Information (TCI), содержат следующие сведения:

Определение приоритета CoS

В пакете с тегом имеется 3 бита для приоритета, которые также обозначаются как Class of Service (CoS), см. также IEEE 802.1Q.

Биты CoS	Приоритет	Вид трафика
000	0 (минимальный)	Background (фон)
001	1	Best Effort
010	2	Excellent Effort
011	3	Critical Applications (критичные задачи)
100	4	Video, задержка менее < 100 мс (время ожидания и дрожание)
101	5	Voice (язык), задержка менее < 10 мс (время ожидания и дрожание)
110	6	Internet Control
111	7 (максимальный)	Network Control

Приоритетность пакетов данных требует наличия очереди в компонентах, в которой они могут буферизировать пакеты данных с более низким приоритетом.

Устройство имеет несколько параллельных очередей, в которых обрабатываются пакеты с различными приоритетами. По умолчанию сначала обрабатываются пакеты с наиболее высоким приоритетом. Этот способ гарантирует, что пакеты с наиболее высоким приоритетом будут отправлены в любом случае даже в условиях большого объема данных.

Canonical Format Identifier (CFI)

CFI требуется для совместимости Ethernet с кольцом токена (Token Ring). Значения можно интерпретировать следующим образом:

Значение	Интерпретация
0	Формат MAC-адреса является каноническим. При каноническом представлении MAC-адреса сначала передаётся бит с самым низким значением. Настройка Ethernet-коммутатора по умолчанию.
1	Формат MAC-адреса не является каноническим.

VLAN ID

5.4 VLAN

В 12-битовом поле данных могут отражаться до 4096 идентификаторов VLAN. При этом действуют следующие положения:

VLAN ID	Интерпретация
0	Пакет содержит только информацию о приоритете (кадры с тегами приоритетов, Priority Tagged Frames) и не содержит действительного идентификатора VLAN.
1 — 4094	Действительный идентификатор VLAN, пакет присвоен VLAN, также может содержать информацию о приоритете.
4095	Резерв

5.4.3 Частная сеть VLAN

С помощью Private VLAN (PVLAN) можно разделить широковещательный домен 2-го уровня для одной сети VLAN.

Private VLAN состоит из следующих блоков:

- Primary Private VLAN (Primary PVLAN)
Разделяемая сеть VLAN называется Primary Private VLAN.
- Secondary Private VLANs (Secondary PVLAN)
Сети Secondary PVLAN существуют только внутри одной сети Primary PVLAN. Каждая сеть Secondary PVLAN имеет конкретный VLAN ID и связана с Primary PVLAN. Сети Secondary PVLAN подразделяются на следующие типы:
 - Isolated Secondary PVLAN
Устройства внутри Isolated Secondary PVLAN не могут обмениваться данными друг с другом через уровень 2.
 - Community Secondary PVLAN
Устройства внутри Community Secondary PVLAN могут обмениваться данными друг с другом напрямую через уровень 2. Устройства не могут обмениваться данными через уровень 2 с устройствами других сообществ PVLAN.

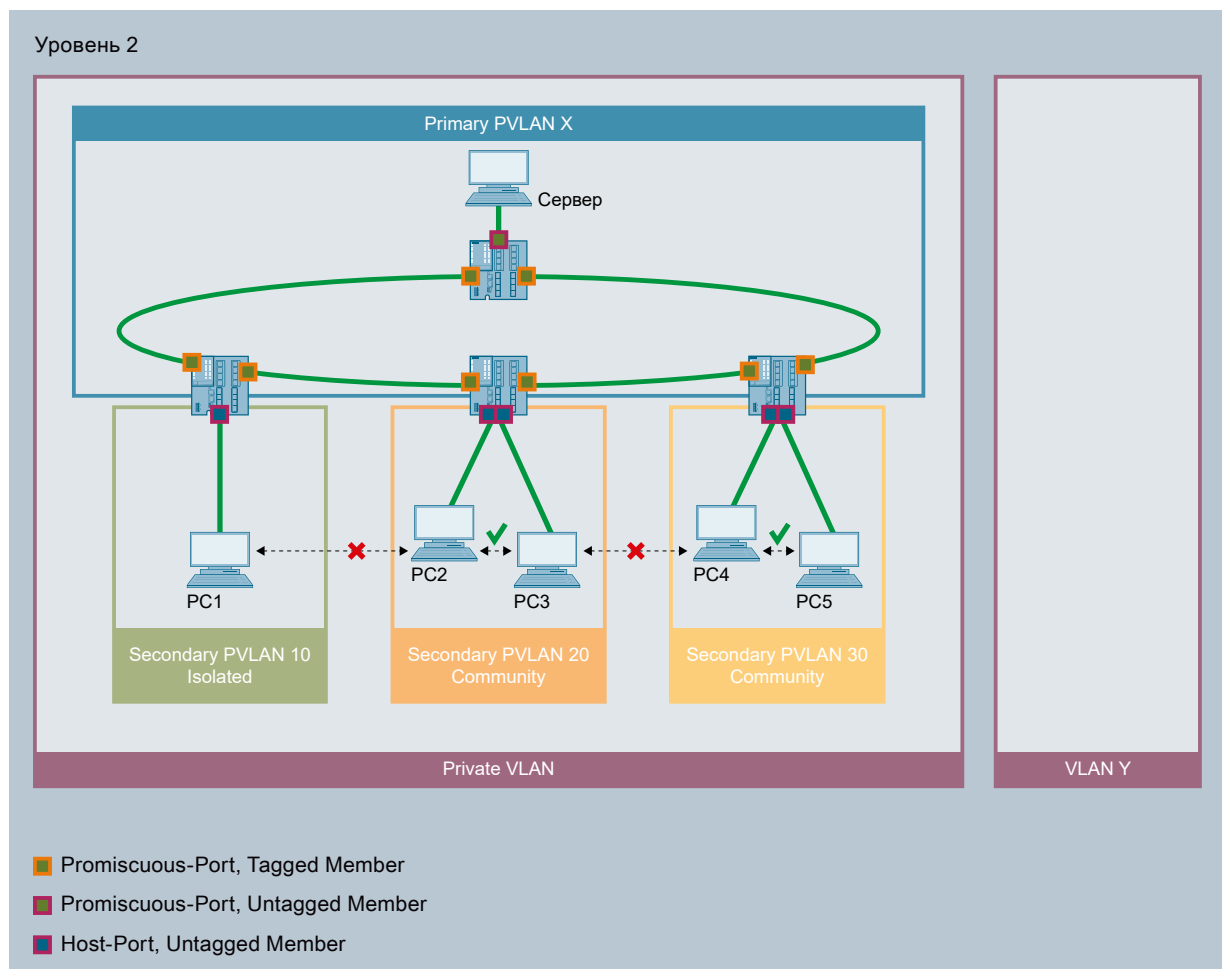
Примечание**VLAN ID в Secondary PVLAN**

Если вы используете один и тот же VLAN ID для Secondary PVLAN на различных IE-коммутаторах, то оконечные устройства в такой Secondary PVLAN могут обмениваться данными друг с другом по Layer 2 вне зависимости от коммутатора. Условием является конфигурация портов, соединяющих различные IE-коммутаторы, как Promiscuous Port. Если эти порты сконфигурированы как Trunk Port, а для Isolated Secondary PVLAN используется один и тот же VLAN-ID, то оконечные устройства останутся изолированными.

Примечание**Функции Private VLAN и аутентификация RADIUS**

Если активировано присвоение VLAN через аутентификацию RADIUS для одного или нескольких портов сети VLAN, то эту сеть VLAN не потребуется дополнительно конфигурировать как Private VLAN.

Спектр функций Private VLAN в связи с присвоением VLAN через аутентификацию RADIUS может привести к не единообразному состоянию системы.



В этом примере порты IE-коммутатора, которые связывают его с другими IE-коммутаторами, сконфигурированы как случайные порты. Эти порты являются Tagged Member во всех PVLAN: Primary PVLAN и всех Secondary PVLAN.

Порты, к которым подключены ПК, являются Host Port. Порты Host Port являются соответственно Untagged Member в Primary PVLAN и в своей соответствующей Secondary PVLAN.

Порт, к которому подключён сервер, является Promiscuous Port. Этот Promiscuous Port является Untagged Member во всех PVLAN: Primary PVLAN и всех Secondary PVLAN.

В этом примере все ПК могут обмениваться данными с сервером. Сервер может обмениваться данными со всеми ПК. ПК1 не может обмениваться данными ни с одним другим ПК. ПК внутри Community Secondary PVLAN могут обмениваться данными друг с другом, но не с ПК в другой Secondary PVLAN.

5.4.4 Tunnelling

С помощью функции туннеля VLAN Q-in-Q можно перенаправлять трафик из различных клиентских сетей через сеть провайдера, используя туннель VLAN. При этом каждая клиентская сеть может иметь полный спектр возможных VLAN.

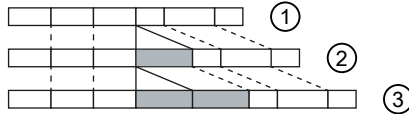
Туннель VLAN устанавливается между коммутаторами провайдера, которые сконфигурированы на границах сети провайдера. Коммутатор провайдера имеет следующие типы портов:

- Access Port

Через Access Port коммутатор провайдера соединяется с клиентской сетью.

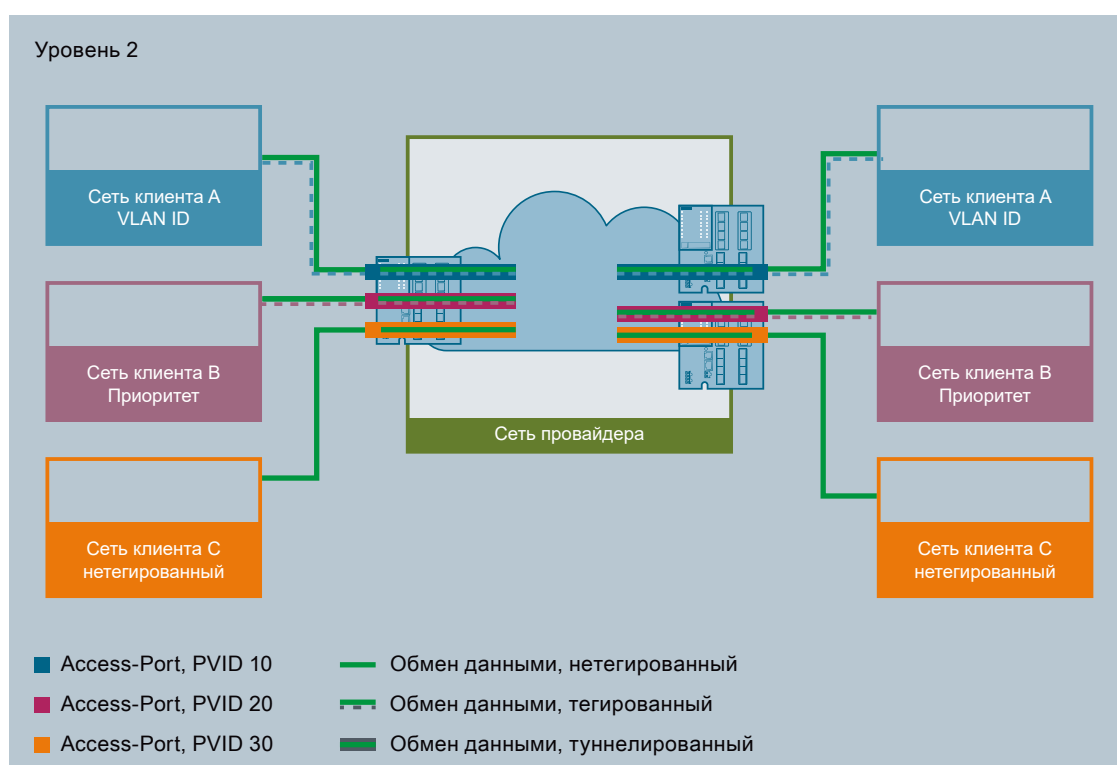
 - Входящий трафик

Входящий трафик на Access Port обрабатывается так, как если бы он не имел тегов ①. Все входящие пакеты расширяются одним тегом с Access Port VID ②. Для уже тегированных пакетов это означает, что они расширяются вторым тегом 802.1Q ③, тегом внешней VLAN.


 - Исходящий трафик

При исходящем трафике на порте Access тег внешней VLAN вновь удаляется.
- Core Port

Через Core Port коммутатор провайдера соединяется с сетью провайдера. Порты Core Port являются участниками в сети VLAN для Access Port или имеют конфигурацию «Switch Port VLAN Trunk».



В этом примере трафик перенаправляется из клиентских сетей А, В и С через VLAN-туннель по сети провайдера. Пакеты из клиентской сети А получают тег идентификатора VLAN. Пакеты из клиентской сети В получают тег приоритета. Пакеты из клиентской сети С не получают тег.

Когда пакеты достигают соответствующего порта Access, то они расширяются на величину тега с VID порта доступа и туннелируются по сети провайдера. Как только пакеты покидают сеть провайдера, внешний тег VLAN (PVID) вновь удаляется. Пакеты пересылаются в своём первоначальном виде. Приоритет пакета при этом сохраняется.

5.5 Mirroring

Устройство предлагает возможность параллельно выводить входящие или исходящие потоки данных на другие интерфейсы для анализа или мониторинга. При этом обратное влияние на контролируемые потоки данных отсутствует. Этот процесс называется зеркалированием (Mirroring). В этом разделе меню можно включить или выключить зеркалирование и настроить его параметры.

Зеркалирование портов

Зеркалирование порта означает, что трафик на одном порте (зеркалируемый порт) IE-коммутатора копируется на другой порт (порт мониторинга). На один порт мониторинга можно зеркалировать один или несколько портов.

Если к порту мониторинга подключается анализатор протоколов, можно регистрировать трафик на зеркалируемом порту, не прерывая соответствующее соединение. В результате можно исследовать трафик без обратного воздействия на него. Условием для

этого является наличие на устройстве свободного порта, который можно использовать как порт мониторинга.

Примечание

Пересылка потока RSPAN

Если устройству требуется пересылать потоки RSPAN, то должны быть выполнены два требования:

- Входящий и исходящий порт должны принадлежать к одной группе портов.
 - Функция «Обучение» должна быть отключена для входящего порта. Это возможно только с помощью интерфейса командной строки CLI **нет одноадресного обучения Мас.**
-

5.6 SNMP

Введение

С помощью протокола Simple Network Management Protocol (SNMP) осуществляется контроль и управление сетевыми компонентами, например, маршрутизаторами или коммутаторами, с центральной станции. SNMP при этом регулирует обмен данными между контролируемыми устройствами и контролирующей станцией.

Задачи SNMP:

- Контроль сетевых компонентов
- Удалённое управление и параметрирование сетевых компонентов
- Распознавание ошибок и уведомление об ошибках

В версиях v1 и v2c протокол SNMP не обладает механизмами безопасности. Любой пользователь сети с помощью соответствующего программного обеспечения может получать доступ к данным и изменять параметры.

Для простого управления правами доступа без аспектов безопасности используются строки сообщества.

Строка сообщества передаётся вместе с запросом. Если строка сообщества верна, то SNMP-агент отвечает и направляет требуемые данные. Если строка сообщества неверна, то SNMP-агент отклоняет запрос. Для прав чтения и записи следует определить различные строки сообщества. Строки сообщества передаются открытым текстом.

Значения строк сообщества по умолчанию:

- public
обладает только правами чтения
- private
обладает правами чтения и записи

Примечание

Так как в случае строк сообщества SNMP речь идёт о защите прав доступа, не следует использовать значения по умолчанию «public» или «private». Измените эти значения после первого ввода в эксплуатацию.

Прочие простые механизмы защиты на уровне устройств:

- Allowed Host
Контролируемой системе известны IP-адреса контролирующих систем.
- Read Only
Если присвоить контролируемому устройству статус «Read Only», то контролирующие станции смогут только считывать данные, но не смогут их изменять.

Пакеты данных SNMP не зашифрованы и могут быть с лёгкостью прочитаны.

Центральная станция также обозначается как станция управления. На подлежащих контролю устройствах установлен SNMP-агент, с которым станция управления обменивается данными.

Станция управления отправляет пакеты данных следующих типов:

- GET
Запрос блока данных от SNMP-агента
- GETNEXT
Вызывает следующий блок данных.
- GETBULK (доступно, начиная с SNMPv2c)
Запрашивает сразу несколько блоков данных, например, несколько строк одной таблицы.
- SET
Содержит данные для параметрирования соответствующего устройства.

SNMP-агент отправляет пакеты данных следующих типов:

- RESPONSE
SNMP-агент отправляет данные, запрошенные станцией управления.
- TRAP
Если наступает определенное событие, то SNMP-агент самостоятельно отправляет прерывания.

SNMPv1/v2c/v3 используют протокол UDP (User Datagram Protocol) и пользуются UDP-портами 161 и 162. Описание данных выполняется в базе данных управления, Management Information Base (MIB).

SNMPv3

SNMPv3, в отличие от предшественников SNMPv1 и SNMPv2c, вводит комплексную концепцию безопасности.

SNMPv3 поддерживает следующие функции:

- Полностью зашифрованная аутентификация пользователей
- Шифрование всего трафика
- Контроль доступа MIB-объектов на уровне пользователя/группы

5.7 Quality of Service

Quality of Service (QoS) представляет собой метод эффективного использования имеющейся ширины полосы пропускания сети.

QoS реализуется путём распределения приоритетов в трафике. Входящие кадры в соответствии с определённым приоритетом сортируются в очередь (Queue) и обрабатываются. Благодаря этому определённым кадрам отдаётся преимущество.

Различные методы QoS влияют друг на друга, поэтому рассматриваются в следующем порядке:

1. Сначала коммутатор проверяет, представляет ли собой входящий кадр широковещательный кадр или агентский кадр.
→ Если условие 1 выполнено, то коммутатор учитывает установленный приоритет на странице «General (Страница 281)». Коммутатор распределяет кадр в очередь в соответствии с распределением на странице «CoS Map (Страница 282)».
2. Если условие 1 не выполнено, то коммутатор проверяет, содержит ли кадр тег VLAN.
→ Если условие 2 выполнено, то коммутатор проверяет настройки приоритета на странице «Общая информация (Страница 290)». Коммутатор проверяет, установлено ли для приоритета значение, отличающееся от «Do not force». Если приоритет установлен, то коммутатор распределяет кадр в очередь в соответствии с распределением на странице «CoS Map (Страница 282)».
3. Если условие 2 также не выполнено, то кадры обрабатываются дальше в соответствии с Trust Mode. Конфигурирование Trust Mode выполняется на странице «QoS Trust (Страница 285)».

5.8 NAT/NAPT

Примечание

Функция NAT/NAPT возможна только на Layer 3 эталонной модели ISO/OSI. Для использования функции NAT сети должны использовать протокол IP.

При использовании протокола ISO, который работает на Layer 2, использовать функцию NAT невозможно.

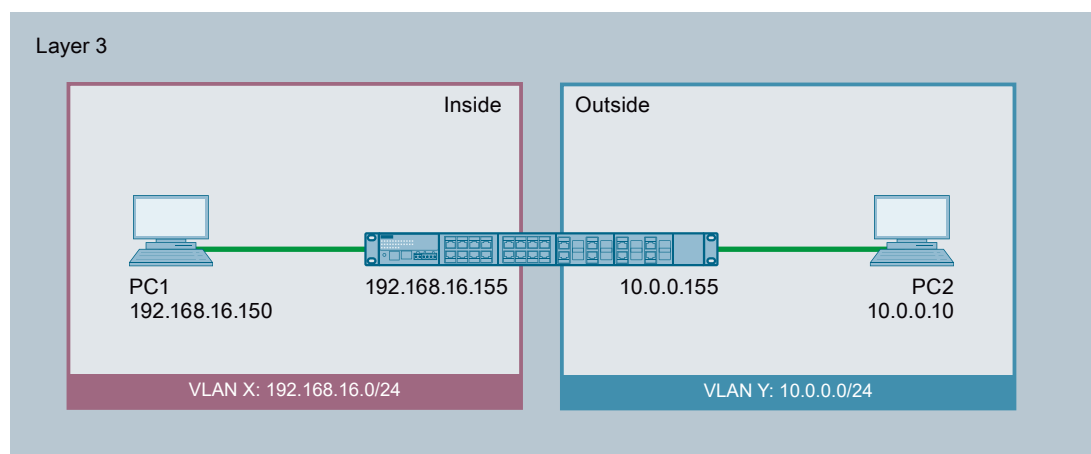
В функции преобразования сетевого адреса, или Network Address Translation (NAT), подсети IP разделяются на «Inside» и «Outside». Разделение происходит с позиции NAT-интерфейса. Все сети, которые сами по себе доступны через NAT-интерфейс, считаются для этого интерфейса как «Outside». Все сети, которые доступны через другие IP-интерфейсы того же устройства, считаются для NAT-интерфейса как «Inside».

Если маршрутизация выполняется через NAT-интерфейс, то IP-адреса источника и цели в передаваемых пакетах данных изменяются при переходе между «Inside» и «Outside». Изменение IP-адреса источника или цели зависит от направления обмена данными. Всегда адаптируется IP-адрес того участника процесса обмена данными, который находится «Inside». В зависимости от перспективы IP-адрес участника процесса обмена данными обозначается как «Local» или «Global».

		Перспектива	
		Local	Global
Положение	Inside	Фактический IP-адрес, который присвоен устройству во внутренней сети. Этот адрес недоступен из внешней сети.	IP-адрес, под которым внутреннее устройство доступно из внешней сети.
	Outside	Фактический IP-адрес, который присвоен устройству во внешней сети. Так как преобразуются только адреса «Inside», то различие между Outside Local и Outside Global не проводится.	

Пример

В примере две подсети IP связаны друг с другом через IE-коммутатор. Разделение происходит с позиции NAT-интерфейса 10.0.0.155. Обмен данными между ПК2 и ПК1 преобразуется через NAT/NAPT.



Фактический IP-адрес ПК1 (Inside Local) статически преобразуется с помощью NAT. ПК1 доступен для ПК2 по адресу Inside Global.

		Перспектива	
		Local	Global
Положение	Inside	192.168.16.150	10.0.0.7
	Outside	10.0.0.10	

Фактический IP-адрес ПК1 (Inside Local) преобразуется с помощью NAPT (Network Address and Port Translation). ПК1 доступен для ПК2 по адресу Inside Global.

		Перспектива	
		Local	Global
Положение	Inside	192.168.16.150:80	10.0.0.7:80
	Outside	10.0.0.10:1660	

Вычислительная мощность

Приём пакетов устройством ограничен до 300 пакетов в секунду в виду ограничения нагрузки ЦП. Это соответствует максимальной пропускной способности данных 1,7 Мбит/с. Это ограничение нагрузки действует не для каждого интерфейса, а в целом для всех пакетов, которые направляются к ЦП.

Весь обмен данными NAT происходит через ЦП и тем самым конкурирует с обменом данными IP, которые отправляются на ЦП, например, WBM и Telnet.

Следует учитывать, что при использовании NAT занимается значительная часть вычислительной мощности. Из-за этого доступ через Telnet или WBM может быть замедлен.

NAT

С помощью функции преобразования сетевого адреса (Network Address Translation, или NAT) IP-адрес в пакете данных заменяется на другой. Функция NAT, как правило, используется в шлюзе между внутренней сетью и внешней сетью.

В варианте Source NAT адрес источника Inside Local IP-пакета устройства во внутренней сети преобразуется NAT-устройством в шлюзе в адрес Inside Global.

В варианте Destination NAT адрес цели Inside Global IP-пакета устройства во внешней сети преобразуется NAT-устройством в шлюзе в адрес Inside Local.

Для преобразования внутреннего IP-адреса во внешний и обратно NAT-устройство содержит список преобразований. Присвоение адресов может быть динамическим или статическим. Конфигурирование NAT выполняется через «Layer 3 (IPv4) > NAT (Страница 387)».

NAPT

С помощью функции Network Address Port Translation, или NAPT, множество внутренних IP-адресов преобразуются в один и тот же внешний IP-адрес. Для идентификации отдельных участников в списке преобразований NAT-устройства также сохраняется порт внутреннего устройства, который преобразуется для внешнего адреса.

Если несколько внутренних устройств направляют запрос на один и тот же Destination IP через NAT-устройство, то NAT-устройство вносит собственный внешний Source IP в заголовок этих перенаправляемых пакетов. Так как перенаправляемые пакеты имеют один и тот же Source IP, то NAT-устройство присваивает пакеты устройствам с помощью различных номеров портов.

Если устройство из внешней сети захочет использовать службу во внутренней сети, то потребуется сконфигурировать список преобразований для статического присвоения адресов. Конфигурирование NAPT выполняется в пункте меню Layer 3 (IPv4) > NAT > NAPT (Страница 392).

NAT/NAPT и IP Routing

Функцию NAT/NAPT и IP Routing можно активировать одновременно. В этом случае потребуется регулировать доступность внутренних адресов из внешних сетей с помощью правил ACL.

5.9 Single Hop Inter-VLAN Routing

Введение

Физическая сеть подразделяется с помощью VLAN на широковещательные домены и подсети.

Устройства (хосты) внутри VLAN могут обмениваться данными друг с другом напрямую по Layer 2. Пакеты перенаправляются на соответствующее устройство на основании MAC-адреса.

Устройства из различных сетей VLAN не могут обмениваться данными друг с другом напрямую по Layer 2. Требуется маршрутизация трафика на основании IP-адреса.

С помощью функции Single-Hop Inter-VLAN-Routing для устройств из разных сетей VLAN возникает возможность обмена данными друг с другом без использования маршрутизатора.

Требования

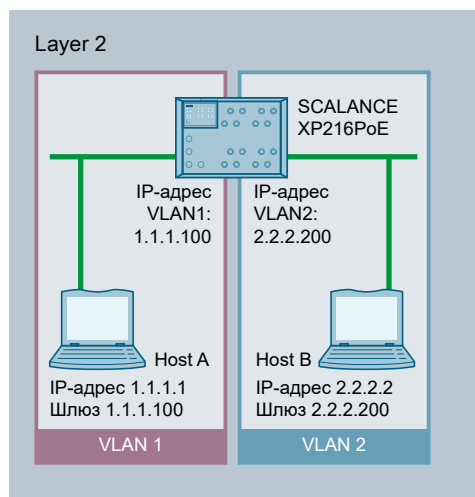
- IE-коммутатор может управлять несколькими IP-интерфейсами.
- IE-коммутатор является участником сетей VLAN, между которыми требуется маршрутизация.
- В хост-компьютерах IP-адрес VLAN установлен как Default Gateway.

Single Hop Inter-VLAN Routing

IE-коммутатор получает пакет и распознает, что он адресован устройству в другой сети VLAN. Он перенаправляет пакет на соответствующий порт в VLAN.

IE-коммутатор знает только те сети VLAN, с которыми он напрямую соединен (Connected). Поэтому при Single-Hop Inter-VLAN-Routing маршрутизация возможна только между двумя локальными IP-интерфейсами.

Пример



В этом примере хост А соединён с IE-коммутатором через VLAN 1. Хост-компьютер В соединён с IE-коммутатором через VLAN 2. В хост-компьютере А IP-адрес VLAN 1 зарегистрирован как шлюз по умолчанию. В хост-компьютере В IP-адрес VLAN 2 зарегистрирован как шлюз по умолчанию.

Если на SCALANCE XP216PoE активирована функция Single-Hop Inter-VLAN-Routing, то хост-компьютеры А и В могут обмениваться данными друг с другом.

Конфигурирование с помощью функции Web Based Management

6

6.1 Web Based Management

Принцип работы

Устройство имеет интегрированный HTTP-сервер для Web Based Management (WBM). Если обращение к устройству выполняется через интернет-браузер, то он в зависимости от введённых пользователем данных отправляет клиентскому ПК HTML-страницы.

Пользователь вносит данные конфигурации в отправленные устройством HTML-страницы. Устройство анализирует эту информацию и динамически генерирует страницы с ответами.

Преимуществом этого принципа работы является то, что на стороне клиента требуется только наличие интернет-браузера.

Примечание

Безопасное соединение

WBM также предлагает возможность установления защищённого соединения по протоколу HTTPS.

Используйте протокол HTTPS для защищённой передачи ваших данных. При желании получать доступ к WBM исключительно через безопасное соединение в пункте меню System > Configuration необходимо активировать опцию «HTTPS Server only».

Требования

Отображение WBM

- Устройство имеет IP-адрес.
- Между устройством и клиентским ПК имеется соединение. Доступность устройства можно проверить с помощью команды пинга.
- Доступ через HTTP(S) активирован.
- В браузере активирован JavaScript.

6.1 Web Based Management

- Интернет-браузер нельзя настраивать таким образом, чтобы при каждом доступе к странице ее требовалось загружать с сервера заново. Актуальность динамического содержимого страниц обеспечивается другими механизмами. Соответствующую возможность настройки для Internet Explorer можно найти в меню «Дополнительно > Опции Интернет > Общие» в разделе «Работа браузера», щёлкнув кнопку «Настройки». В пункте «Искать новые версии сохранённых страниц» следует выбрать вариант «Автоматически».
- Если используется брандмауэр, то должны быть разблокированы соответствующие порты.
 - Для доступа через HTTP: TCP-порт 80
 - Для доступа через HTTPS: TCP-порт 443

Отображение WBM было протестировано в следующих стационарных версиях интернет-браузеров:

- Microsoft Edge 83
- Mozilla Firefox ESR 78
- Google Chrome V83

Примечание

Просмотр в режиме совместимости

Деактивируйте в Microsoft Internet Explorer просмотр в режиме совместимости для того, чтобы гарантировать правильность отображения и безупречность конфигурирования через WBM.

Отображение WBM

Для мобильных устройств применяются следующие минимальные условия:

Разрешение	Операционная система
960 x 640 пикселей	Android, начиная с версии 4.2.1 iOS, начиная с версии 6.0.2

Тестирование проводилось в следующих интернет-браузерах для мобильных устройств:

- Apple Safari, начиная с версии 8, на iOS, начиная с версии 8.1.3 (iPad Mini модели A1432)
- Google Chrome, начиная с версии 40, на Android, начиная с версии 5.0.2 (Nexus 7C Asus)
- Mozilla Firefox, начиная с версии 35, на Android, начиная с версии 5.0.2 (Nexus 7C Asus)

Примечание

Отображение страниц и управление WBM на мобильных устройствах

Отображение страниц WBM и управление ими на мобильных устройствах может отличаться от отображения тех же страниц и управления ими на стационарных устройствах. Некоторые страницы также имеются в виде, оптимизированном для отображения на мобильных устройствах.

6.2 Авторизация

Соединение с устройством

Чтобы с помощью интернет-браузера установить соединение с устройством, выполните следующие действия:

1. Между устройством и клиентским ПК имеется соединение. Доступность устройства можно проверить с помощью команды пинга.
2. Введите в адресную строку интернет-браузера IP-адрес или URL устройства. Когда с устройством будет установлено соединение, то появится страница авторизации системы Web Based Management (WBM).

Авторизация с помощью интернет-браузера

Выбор языка WBM

1. В раскрывающемся списке в правой верхней части выберите версию языка, на котором будут отображаться страницы WBM.
2. Щёлкните кнопку «Go», чтобы переключиться на выбранный язык.

Примечание

Доступные языки

В этой версии доступны немецкий и английский язык.

SIEMENS

English [Go](#)

Name

Password

[Login](#)

?

LOGIN

Name:

Password:

[Login](#)

For information about browser compatibility please refer to the manual

Персонализация страницы авторизации

На странице авторизации можно показывать дополнительный текст.

1. Создайте файл, который содержит нужный текст или арт в формате ASCII. Под артом в формате ASCII подразумеваются пиктограммы, например, фирменный логотип Siemens на основе доступных символов. Поддерживаются до 50 строк текста, каждая из которых может содержать до 255 символов, включая пробелы.

Примечание

Не поддерживается использование специальных символов:

- Обратная косая черта (\)
 - Знак вопроса (?)
 - Табуляторы: вместо табуляторов следует использовать пробелы
-

2. Загрузите текстовый файл в устройство, выбрав «System > Load&Save». Для этого вне зависимости от используемого протокола воспользуйтесь кнопкой «Upload» в ячейке таблицы «LoginWelcomeMessage».
3. После этого выйдите из системы. На странице авторизации под данными авторизации отобразится сконфигурированный текст.

Авторизация через HTTP

У вас есть следующие возможности для авторизации через HTTP. Можно воспользоваться либо возможностью авторизации в центре окна браузера, либо возможностью авторизации в верхней левой части окна браузера. Для обеих возможностей действуют следующие этапы.

Авторизация в устройстве с заводскими настройками

При первой авторизации или авторизации после восстановления заводских настроек выполните следующие действия:

1. Введите в поле ввода «Name» предустановленное на заводе имя пользователя «admin».
С помощью этой учётной записи можно изменять настройки устройства (доступ к данным конфигурации для чтения и записи).

Примечание

Заводская предварительная настройка пользователя «user»

Начиная с версии прошивки 2.1 заводская настройка пользователя «user» в состоянии поставки более недоступна.

Если обновить устройство до прошивки V2.1, сначала ещё будет доступна заводская предварительная настройка пользователя «user». Однако при последующем сбросе устройства на заводские настройки («Restore Factory Defaults and Restart») предустановленный на заводе пользователь «user» удаляется.

Можно создавать пользователей с ролью «user».

2. Введите в поле ввода «Password» пароль предустановленного на заводе пользователя «admin»: «admin».

3. Щёлкните кнопку «Login» или подтвердите ввод кнопкой ввода.
Появится следующая страница. Появится запрос на изменение пароля.

4. Вновь введите в поле ввода «Current User Password» пароль предустановленного на заводе пользователя «admin».
5. При необходимости введите в поле «New Admin Account Name» новое имя пользователя.
При первой авторизации или авторизации после выполнения функции «Restore Factory Defaults and Restart» появляется однократная возможность переименовать предустановленного на заводе пользователя «admin». Затем переименование «admin» будет невозможно.
6. Введите в поле «New Password» новый пароль для пользователя.
Новый пароль должен соответствовать следующим требованиям к нему:
 - Длина пароля: минимум 8 символов, максимум 32 символа
 - Минимум 1 прописная буква
 - Минимум 1 специальный символ
 - Минимум 1 цифра
7. Введите новый пароль ещё раз в поле «Password Confirmation». Оба введенных пароля должны совпадать.
Щёлкните кнопку «Set Values», чтобы завершить процесс и активировать новый пароль.

Если вы успешно авторизовались, появляется стартовая страница.

Авторизация в сконфигурированном устройстве

При авторизации в сконфигурированном устройстве порядок действий следующий:

1. В поле ввода «Name» вводится имя пользователя существующей учётной записи. Локальные учётные записи пользователей конфигурируются в пункте «Security > Users».
2. Введите в поле ввода «Password» пароль соответствующей учётной записи.
3. Щёлкните кнопку «Login» или подтвердите ввод кнопкой ввода.

Если вы успешно авторизовались, появляется стартовая страница.

Авторизация через HTTPS

Система Web Based Management также предлагает возможность установления защищённого соединения с устройством по протоколу HTTPS.

При соединении с устройством по протоколу HTTPS порядок действий следующий:

1. Щёлкните ссылку «Switch to secure HTTP» на странице авторизации или введите в адресную строку интернет-браузера «https://» и IP-адрес устройства.
2. Проверьте отображающееся предупреждение о сертификате и подтвердите его при необходимости.
Появится страница авторизации системы Web Based Management.
3. Далее следуйте инструкциям из пункта «Login via HTTP».

Защита от атак Brute Force

Для защиты от атак Brute Force авторизация на устройстве отключается для IP-адреса пользователя или пользователя после 11 неудачных попыток.

6.3 Меню «Information»

6.3.1 Стартовая страница

Вид стартовой страницы

При вводе IP-адреса устройства после успешной авторизации отображается стартовая страница. Выполнение конфигурации на этой странице невозможно.

Общая структура страниц WBM

На каждой странице WBM в ваше распоряжение предоставляются следующие общие области:

- Область выбора (1): верхняя область
- Область выбора (2): верхняя область
- Область навигации (3): левая область
- Область содержания (4): центральная область



Область выбора (1)

В области выбора имеются следующие элементы:

- Логотип Siemens AG
При щелчке логотипа открывается веб-страница соответствующего базового устройства на портале Siemens Industry Online Support.
- Отображение следующих параметров: «Device location / System name»
 - «Device location» содержит информацию о местонахождении устройства.
В состоянии поставки здесь отображается IP-адрес.
 - «System name» — это название устройства.
В состоянии поставки здесь отображается тип устройства.

Содержание этой индикации можно изменять, выбрав пункт меню System > General > Device.

- Раскрывающийся список для выбора языка
- Системные дата и время с индикацией состояния
Содержание этой индикации можно изменять, выбрав пункт меню System > System time.
Если системное время не настроено, то состояние будет отображаться как . Если системное время сконфигурировано, однако его синхронизация невозможна, то будет отображаться жёлтый предупреждающий треугольник . Проверьте, доступен ли сервер времени. При необходимости скорректируйте конфигурацию. Если системное время настроено и/или может синхронизироваться, то состояние будет отображаться как .

Область выбора (2)

В верхней части области отображения находится имя текущего авторизованного пользователя, а также полный заголовок текущего выбранного пункта меню.

В нижней части области отображения находятся следующие элементы:

- **Logout**
Можно выйти из системы на любой странице WBM, щёлкнув ссылку «Logout».
- **LED Simulation** 
Каждое устройство имеет множество светодиодов, которые передают информацию о рабочем состоянии устройства. Тем не менее, в зависимости от места установки непосредственный доступ к устройству возможен не всегда. По этой причине система Web Based Management предлагает возможность просмотра симуляции светодиодов. Не распределённые подключения отображаются как серые светодиоды. Объяснение светодиодной индикации описано в руководстве по эксплуатации.
При щелчке этой кнопки открывается окно светодиодной симуляции. Это окно можно отобразить во время смены меню и передвигать в соответствии с потребностями. Для закрытия светодиодной симуляции щёлкните кнопку закрытия внутри окна светодиодной симуляции.

- **Help ?**
При щелчке этой кнопки открывается страница справки к текущему выбранному пункту меню в новом окне браузера. На странице справки находится описание области содержимого. При определённых обстоятельствах здесь также может приводиться описание опций, которые не представлены на устройстве. В верхней части каждой страницы справки имеется поле ввода для функции поиска. Введите здесь понятие, по которому требуется дополнительная информация, и запустите поиск, подтвердив кнопкой ввода. В диалоговом окне отобразится список страниц WBM, которые содержат искомое понятие. При выборе элемента списка соответствующая страница WBM откроется в новой вкладке браузера.
- **Print **
При щелчке этой кнопки открывается всплывающее окно. Всплывающее окно содержит представление содержимого страницы, оптимизированное для вывода на печать.

Примечание

Печать больших таблиц

При необходимости распечатать большую таблицу следует использовать функцию «Предварительный просмотр для печати» интернет-браузера.

- **Favorites**
В состоянии поставки кнопка деактивирована на всех страницах .
При щелчке этой кнопки символ  меняется, и текущая открытая страница или текущая открытая вкладка помечается как избранное. После первой активации этой кнопки область навигации делится на две вкладки. Первая вкладка «Menu» содержит все доступные меню, как и ранее. Вторая вкладка «Favorites» содержит все страницы/вкладки, помеченные как избранное. Страницы/вкладки располагаются на вкладке «Favorites» в соответствии со структурой на вкладке «Menu».
Если деактивировать всё сохранённое ранее избранное, то вкладка «Favorites» также вновь исчезнет. Для этого на соответствующих страницах/вкладках щёлкните кнопку .
Конфигурацию избранного в устройстве можно сохранять по HTTP и TFTP, выгружать и удалять на странице System > Load&Save.

Область навигации (3)

В области навигации доступны различные меню. Щелкайте по отдельным меню, чтобы просматривать подменю. Подменю содержат страницы, на которых можно найти информацию или с помощью которых можно выполнять конфигурацию. Эти страницы всегда отображаются в области содержимого.

При наличии элементов в избранном область навигации делится на две вкладки: «Menu» и «Favorites».

Область содержимого (4)

Область содержимого содержит изображение устройства. Изображение всегда показывает устройство, интерфейс WBM которого активен.

Под изображением устройства отображается следующая информация:

- **PROFINET Name of Station**
Отображает имя устройства PROFINET.
- **Diagnostics Mode**
Отображает, активированы ли EtherNet/IP или PROFINET IO.
- **System Name**
Отображает название устройства.
- **Device Type**
Отображает типовое обозначение устройства.
- **PROFINET AR Status**
Отображает статус отношения приложения PROFINET.
 - Online
Установлено соединение с контроллером PROFINET. Контроллер PROFINET загрузил свои данные конфигурации в устройство. Устройство может отправить данные статуса контроллеру PROFINET.
В этом состоянии параметры, настраиваемые с помощью контроллера PROFINET, невозможно конфигурировать на устройстве.
 - Offline
Соединение с контроллером PROFINET не установлено.
- **Power Line 1 / Power Line 2**
 - Up
Напряжение питания 1 или 2 имеется
 - Down
Напряжение питания 1 или 2 отсутствует, либо допустимое напряжение недостаточно высокое.
- **PLUG Configuration**
Отображает статус данных конфигурации на PLUG, см. главу «System > PLUG > Configuration».
- **Fault Status**
Отображает статус ошибки устройства.

Часто используемые кнопки

Страницы WBM по умолчанию содержат следующие кнопки:

- **Обновление отображения с помощью кнопки «Refresh»**

Страницы системы Web Based Management, отображающие актуальные параметры, содержат внизу кнопку «Refresh». Щёлкните эту кнопку, если вы хотите запросить актуальные данные от устройства для текущей страницы.

Примечание

Если щёлкнуть кнопку «Refresh» до того, как сохранить изменения конфигурации с помощью кнопки «Set values» на устройстве, то внесённые изменения будут удалены, из устройства будет загружена предыдущая конфигурация, которая отобразится здесь.

- **Сохранение записей с помощью кнопки «Set values»**

Страницы, на которых можно выполнять настройки конфигурации, внизу содержат кнопку «Set values». Эта кнопка становится активной только после того, как на странице будет изменено хотя бы одно значение. Щёлкните кнопку, чтобы сохранить введённые данные конфигурации в устройстве. После сохранения кнопка вновь становится неактивной.

Примечание

Изменение данных конфигурации возможно только в роли «admin».

- **Создание записей с помощью кнопки «Create»**

Страницы, на которых можно создавать новые записи, содержат внизу кнопку «Create». Для того, чтобы создать новую запись, щёлкните эту кнопку. При создании записи страница обновится.

- **Удаление записей с помощью кнопки «Delete»**

Страницы, на которых можно удалять записи, содержат кнопку «Delete». Щёлкните эту кнопку, чтобы удалить предварительно выделенные записи из памяти устройства. При удалении записи страница обновится.

- **Перелистывание вперёд с помощью кнопки «Next»**

На страницах с множеством блоков данных количество отображаемых на одной странице блоков данных ограничено. Щёлкните кнопку «Next», чтобы выполнить перелистывание вперёд между блоками данных.

- **Перелистывание назад с помощью кнопки «Previous»**

На страницах с множеством блоков данных количество отображаемых на одной странице блоков данных ограничено. Щёлкните кнопку «Previous», чтобы выполнить перелистывание назад между блоками данных.

Сообщения

Если активирован режим работы «Automatic Save» и внесены изменения в параметры, то в области индикации появляется следующее сообщение «Changes will be saved automatically in %u seconds. Press 'Write Startup Config' to save immediately.».

Примечание

Прерывание процесса сохранения

Процесс сохранения запускается только после того, как истечёт показанный в сообщении таймер. После этого появится следующее сообщение «Saving configuration data in progress. Please do not switch off the device.». Длительность процесса сохранения зависит от устройства.

- Не выключайте устройство сразу же по истечении таймера.

6.3.2 Версии

Версии аппаратного и программного обеспечения

На этой странице приведены сведения о версиях аппаратного и программного обеспечения устройства. Выполнение конфигурации на этой странице невозможно.

Version Information			
Hardware	Name	Revision	Order ID
Basic Device	SCALANCE XB208	1	6GK5 208-0BA00-2AB2
Software	Description	Version	Date
Firmware	SCALANCE XB200 Firmware	V02.00.00	06/10/2014 19:35:41
Bootloader	SCALANCE XB200 Bootloader	V02.00.00	06/04/2014 19:30:00
Firmware_Running	Current running Firmware	V02.00.00	06/10/2014 19:35:41
Refresh			

Описание отображаемых значений

Таблица 1 состоит из следующих столбцов:

- **Hardware**
 - Basic Device
Отображает базовое устройство.
 - Px.x
x.x обозначает порт, в который вставлен модуль SFP.
- **Name**
Отображает название устройства или модуля.

- **Revision**
Отображает версию аппаратного обеспечения устройства.
- **Order ID**
Отображает артикул устройства или описанного модуля.

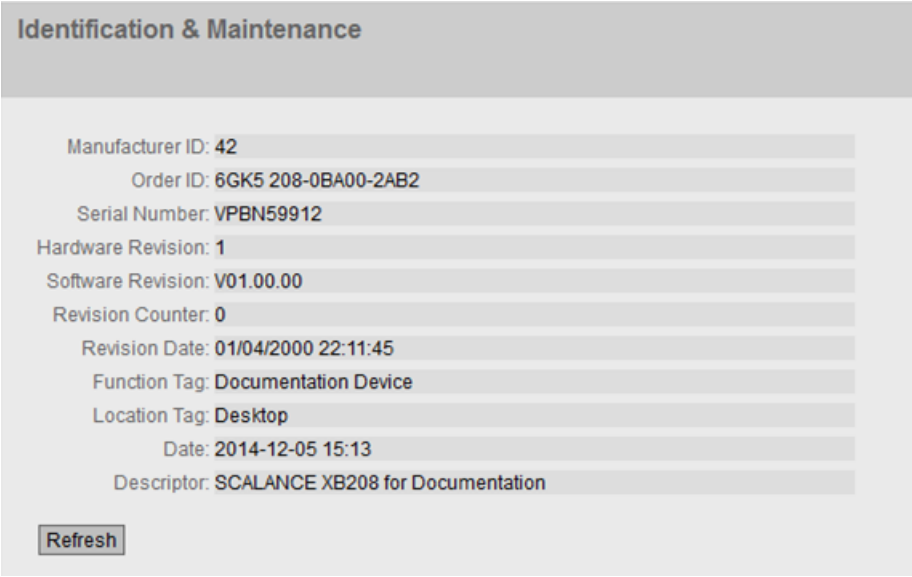
Таблица 2 состоит из следующих столбцов:

- **Software**
 - Firmware
Отображает текущую версию прошивки. Если загружен новый файл прошивки, а устройство ещё не перезапущено, то здесь отобразится версия загруженной прошивки из файла. После повторного пуска загруженная прошивка активируется и будет использоваться.
 - Bootloader
Отображает версию загрузочного программного обеспечения, которое сохранено в устройстве.
 - Firmware_Running
Отображает версию прошивки, которая в настоящий момент используется в устройстве.
- **Description**
Отображает краткое описание программного обеспечения.
- **Version**
Отображает номер версии программного обеспечения.
- **Date**
Отображает дату создания версии программного обеспечения.

6.3.3 I&M

Данные производителя и технического обслуживания

Эта страница содержит специфические данные о производителе и техническом обслуживании устройства, серийный номер, номера версий и т. д. Выполнение конфигурации на этой странице невозможно.



Identification & Maintenance

Manufacturer ID:	42
Order ID:	6GK5 208-0BA00-2AB2
Serial Number:	VPBN59912
Hardware Revision:	1
Software Revision:	V01.00.00
Revision Counter:	0
Revision Date:	01/04/2000 22:11:45
Function Tag:	Documentation Device
Location Tag:	Desktop
Date:	2014-12-05 15:13
Descriptor:	SCALANCE XB208 for Documentation

Описание отображаемых значений

Таблица состоит из следующих строк:

- **Manufacturer ID**
Отображает код производителя.
- **Order ID**
Отображает номер для заказа.
- **Serial Number**
Отображает серийный номер.
- **Hardware Revision**
Отображает версию аппаратного обеспечения.
- **Software Revision**
Отображает версию программного обеспечения.
- **Revision Counter**
Вне зависимости от изменения версии, это поле всегда отображает значение «0».
- **Revision Date**
Отображает дату и время последнего изменения версии.
- **Function Tag**
Отображает шифр функции (шифр установки) устройства. Шифр установки (AKZ) закладывается при конфигурировании устройства с помощью HWKonfig в STEP7.

- **Location Tag**
Отображает шифр местоположения устройства. Шифр местоположения (OKZ) закладывается при конфигурировании устройства с помощью HWKonfig в STEP7.
- **Date**
Отображает дату, заложенную при конфигурировании устройства с помощью HWKonfig в STEP7.
- **Descriptor**
Отображает описание, заложенное при конфигурировании устройства с помощью HWKonfig в STEP7.

6.3.4 Таблица ARP

Сопоставление MAC-адресов и IPv4-адресов

С помощью протокола разрешения адресов (Address Resolution Protocol, или ARP) выполняется однозначное сопоставление MAC-адреса с IPv4-адресом. Каждый участник сети поддерживает это сопоставление в собственной таблице ARP. Страница WBM отображает таблицу ARP устройства.

Address Resolution Protocol (ARP) Table			
Interface	MAC Address	IP Address	Media Type
vlan1	68-05-ca-19-40-bb	192.168.16.1	Dynamic
1 entry.			
Refresh			

Описание отображаемых значений

Таблица состоит из следующих столбцов:

- **Interface**
Отображает интерфейс, через который было выполнено программирование записи в строке.
- **MAC Address**
Отображает MAC-адрес целевого устройства и устройства-источника.

6.3 Меню «Information»

- **IP Address**
Отображает IPv4-адрес целевого устройства.
- **Media Type**
Отображает вид соединения.
 - Dynamic
Устройство автоматически распознало данные адреса.
 - Static
Адреса были внесены как статические.

6.3.5 Log Table

Протоколирование событий

Устройство предлагает возможность протоколировать возникающие события, которые можно частично задавать на странице меню «System > Events». Так, можно, например, задавать параметры неудачной попытки аутентификации или изменения статуса соединения для порта.

Содержание таблицы протокола событий сохраняется даже после выключения устройства.

Log Table

Severity Filters

☐ Info

☐ Warning

☐ Critical

Restart	System Up Time	System Time	Severity	Log Message
41	08:25:24	Date/time not set	6 - Info	Spanning Tree: topology change detected.
41	08:24:48	Date/time not set	6 - Info	Link up on P0.15.
41	08:24:18	Date/time not set	6 - Info	Link down on P0.15.
41	07:29:01	Date/time not set	6 - Info	IP communication is possible. Remote logging activated.

1 - 10 of 517 entries [Show all](#)

1 [Next](#)

Описание отображаемых значений

Severity Filter

Записи в таблице можно фильтровать по степени сложности. Выберите нужные записи в таблице, проставив галочки в полях сверху таблицы.

- **Info**
Если этот параметр активирован, то отображаются все записи категории «Info».
- **Warning**
Если этот параметр активирован, то отображаются все записи категории «Warning».
- **Critical**
Если этот параметр активирован, то отображаются все записи категории «Critical».

Для того, чтобы отобразить все записи, либо выберите все поля, либо оставьте все поля с галочками пустыми.

Таблица состоит из следующих столбцов:

- **Restart**
Подсчитывает количество повторных пусков с последнего сброса заводских настроек и указывает, после какого повторного пуска устройства возникло соответствующее событие.
- **System Up Time**
Отображает время работы устройства после последнего повторного пуска, при котором возникло описанное событие.
- **System Time**
Если системное время установлено, то отображаются дата и время возникновения события.
- **Severity**
Распределение записи в вышеуказанные категории.
- **Log Message**
Отображает краткое описание возникшего события.

Описание кнопок и полей ввода

Кнопка «Clear»

Щёлкните эту кнопку, чтобы очистить содержимое файла протокола событий. Будут удалены все записи вне зависимости от того, что было выбрано в пункте «Severity Filter».

Индикация также будет очищена. Счётчик повторных пусков будет сброшен только после восстановления заводских настроек и последующего повторного пуска устройства.

Примечание

Количество записей в этой таблице ограничивается 1200. Для каждой степени сложности таблица может содержать 400 записей. Если это число достигнуто, то все наиболее старые записи соответствующей степени серьёзности будут удалены. Таблица постоянно сохраняется в памяти устройства.

Кнопка «Show all»

Для того, чтобы просмотреть все записи на странице WBM, щёлкните эту кнопку. Помните, что отображение всех сообщений может занять некоторое время.

Кнопка «Next»

Для того, чтобы перейти к следующей странице, щёлкните эту кнопку.

Кнопка «Previous»

Для того, чтобы перейти к предыдущей странице, щёлкните эту кнопку.

Раскрывающийся список для смены страницы

Выберите в раскрывающемся списке нужную страницу, чтобы перейти к ней.

Кнопка «Refresh»

Обновляет индикацию значений в таблице.

6.3.6 Ошибки

Состояние ошибки

Если возникает ошибка, она отображается на этой странице. Устройство сигнализирует об ошибках миганием красного светодиода.

Передаются сообщения об ошибках устройства, а также ошибки, сконфигурированные на следующих страницах:

- «System > Events»
- «System > Fault Monitoring»

Расчёт момента ошибки начинается с последнего пуска системы. При отсутствии ошибок светодиод ошибок гаснет.

Faults		
No. of Signaled Faults: 1		
Reset Counters		
Fault Time	Fault Description	Clear Fault State
16s	Link down on P0.1.	Clear Fault State
17s	Warm start performed.	Clear Fault State
Refresh		

Описание

- **No. of Signaled Faults**
Отображает, как часто включался светодиод ошибок, а не количество возникших ошибок.
- **Кнопка Reset Counter**
С помощью этой кнопки количество сбрасывается. Счётчик сбрасывается при повторном пуске устройства.

Таблица содержит следующие столбцы:

- **Fault Time**
Отображает время работы устройства после последнего повторного пуска, при котором возникла описанная ошибка.
- **Fault Description**
Отображает краткое описание возникшей ошибки.
- **Clear Fault State**
Некоторые ошибки можно квитировать и тем самым удалить из списка ошибок, например, ошибку при событии «Cold/Warm Start». Если активна кнопка «Clear Fault State», то ошибку можно удалить.

6.3.7 Резервирование

6.3.7.1 Spanning Tree

Введение

Страница отображает текущую информацию в отношении основного дерева (Spanning Tree) и настройки корневого моста (Root Bridge).

Spanning Tree

Spanning Tree
Ring Redundancy
Standby
Link Check
MRP Interconnection

Spanning Tree Mode: MSTP

Instance ID: 0

Bridge Priority: 32768

Bridge Address: 08-00-07-70-84-b0

Root Priority: 32768

Root Address: 08-00-06-70-56-00

Root Cost: 20000

Regional Root Priority: 32768

Regional Root Address: 08-00-07-70-84-b0

Regional Root Cost: 0

Port	Role	State	Oper. Version	Priority	Path Cost	Edge Type	P.t.P. Type
P0.2	Root	Forwarding	MSTP	128	20000	No Edge Port	P.t.P

Refresh

Описание отображаемых значений

Отображаются следующие поля:

- **Spanning Tree Mode**
Отображает настроенный режим. Режим задаётся в пункте «Layer 2 > Configuration» и в «Layer 2 > Spanning Tree > General».
Допускаются следующие значения:
 - «-»
 - STP
 - RSTP
 - MSTP
- **Instance ID**
Отображает номер экземпляра. Этот параметр зависит от сконфигурированного режима.
- **Bridge Priority / Root Priority**
На основании параметра Bridge Priority определяется, какое устройство будет Root Bridge. Мост с наибольшим приоритетом (то есть с минимальным значением этого параметра) будет Root Bridge. Если в сети несколько устройств имеют одинаковый приоритет, то корневым мостом становится устройство, MAC-адрес которого имеет наименьшее числовое значение. Оба параметра, Bridge Priority и MAC Address, вместе образуют идентификатор моста. Так как Root Bridge управляет изменениями путей, то он из-за времени прохождения пакетов должен иметь как можно более близкое к центру расположение. Значение Bridge Priority является целым числом, кратным 4096, с диапазоном значений от 0 до 32768.
- **Bridge Address / Root Address**
Адрес моста отображает MAC-адрес устройства, а адрес корня отображает MAC-адрес корневого коммутатора.
- **Root Costs**
Отображает стоимость пути от устройства к Root Bridge.
- **Bridge Status**
Отображает статус моста, например, является ли устройство Root Bridge.
- **Regional Root Priority** (доступно только для MSTP)
Описание см. в пункте Bridge Priority / Root Priority
- **Regional Root Address** (доступно только для MSTP)
Отображает MAC-адрес устройства.
- **Regional Root Costs** (доступно только для MSTP)
Отображает стоимость пути от регионального Root Bridge к Root Bridge.

Таблица состоит из следующих столбцов:

- **Port**
Отображает порт, через который устройство обменивается данными. Порт складывается из номера модуля и номера порта, например, порт 0.1 означает модуль 0, порт 1.
- **Role**
Отображает статус порта. Возможны следующие значения:
 - Disabled
Порт был вручную удалён из Spanning Tree и более не учитывается в Spanning Tree.
 - Designated
Порты, которые ведут от Root Bridge.
 - Alternate
Порт с альтернативным путём к сегменту сети.
 - Backup
Если коммутатор имеет несколько портов для одного и того же сегмента сети, то «наихудший» порт становится резервным, или Backup Port.
 - Root
Порт, который предлагает наилучший путь к Root Bridge.
 - Master
Этот порт ведёт к Root Bridge, расположенному за пределами региона MST.
 - RSTP+
Кольцевые порты устройств, в которых активирована функция RSTP+.
- **Status**
Отображает текущий статус, в котором находится порт. Значения только отображаются. Этот параметр зависит от сконфигурированного протокола. Возможны следующие значения:
 - Discarding
Порт принимает пакеты BPDU. Другие исходящие или входящие пакеты отклоняются.
 - Listening
Порт принимает и отправляет пакеты BPDU. Порт задействован в алгоритме Spanning Tree. Другие исходящие и входящие пакеты отклоняются.
 - Learning
Порт активно изучает топологию, то есть адреса участников. Другие исходящие и входящие пакеты отклоняются.
 - Forwarding
Порт активен в сети по истечении времени изменения конфигурации. Порт принимает и отправляет пакеты данных.
- **Oper. Version**
Отображает режим совместимости Spanning Tree, который используется портом.

- **Priority**

Если определённый алгоритмом Spanning путь может вести через несколько альтернативных портов одного устройства, то выбирается порт с наивысшим приоритетом (то есть с минимальным значением для этого параметра). Для приоритета можно вводить значения от 0 до 240 с шагом в 16. Если ввести значение, которое не делится на 16, то значение будет автоматически адаптировано. Значение по умолчанию равняется 128.

- **Path Cost**

Этот параметр предназначен для расчёта выбираемого пути. В качестве пути выбирается маршрут с наименьшим значением. Если несколько портов устройства имеют одинаковое значение, то выбирается порт с самым низким номером. Если значение в поле «Cost Calc.» равно «0», то отображается автоматически рассчитанное значение. В противном случае отображается значение поля «Cost Calc.». Определение стоимости пути в основном ориентируется на скорость передачи данных. Чем выше достижимая скорость передачи, тем меньше значение стоимости пути.

Типовые значения стоимости пути в алгоритме Rapid Spanning Tree:

- 10000 Мбит/с = 2000
- 1000 Мбит/с = 20000
- 100 Мбит/с = 200000
- 10 Мбит/с = 2000000

Конфигурация параметра «Cost Calc.» выполняется на страницах «Layer 2 > Spanning Tree > CIST Port» и «Layer 2 > Spanning Tree > MST Port».

- **Edge Type**

Отображает тип соединения. Возможны следующие значения:

- Edge Port
На этом порте находится оконечное устройство.
- No Edge Port
На этом порте находится устройство Spanning Tree.

- **P.t.P. Type**

Отображает вид соединения point-to-point. Возможны следующие значения:

- P.t.P.
При полудуплексе за основу берётся соединение point-to-point.
- Shared Media
При полнодуплексном соединении за основу не берётся соединение point-to-point.

6.3.7.2 Кольцевое резервирование

Информация о кольцевом резервировании

На этой вкладке можно найти сведения о статусе устройства в отношении кольцевого резервирования. Текстовые поля этой страницы доступны только для чтения.

Ring Redundancy											
Spanning Tree	Ring Redundancy	Standby	Link Check	MRP Interconnection							
Ring ID	Domain Name	Admin Role	Oper Role	RM Status	Admin Ring Port 1	Admin Ring Port 2	Oper Ring Port 1	Oper Ring Port 2	No. of Changes to RM Active State	Max. Delay of RM Test Packets[ms]	
1	default-mrpdome	Automatic Redur	MRP Auto-Mana	Active	P0.7	P0.8	P0.7	P0.8	1	0	

Observer Status: -

[Reset Counters](#)

[Refresh](#)

Описание отображаемых значений

Таблица состоит из следующих столбцов:

- **Ring ID**
Идентификатор кольца.
- **Domain Name**
Имя, которое однозначно присваивается каждому кольцу.
- **Admin Role**
Способ кольцевого резервирования.
- **Oper. Role**
Роль устройства внутри кольца:
 - No Ring Redundancy
IE-коммутатор работает без использования функции кольцевого резервирования.
 - HRP Client
IE-коммутатор работает как HRP Client.
 - HRP Manager
IE-коммутатор работает как HRP Manager.
 - MRP Client
IE-коммутатор работает как MRP Client.
 - MRP Manager
IE-коммутатор работает как MRP Manager. Для устройства настроена роль «MRP Manager» через WBM или роль «Manager» через STEP 7.
 - MRP Auto Manager
IE-коммутатор работает как MRP Manager. Для устройства настроена роль «MRP Auto Manager» через WBM или CLI, либо роль «Manager (Auto)» через STEP 7.

- **RM Status**

Столбец «RM Status» показывает, работает ли IE-коммутатор как менеджер резервирования и размыкает или переключает ли он кольцо в этой роли.

- **Passive**

IE-коммутатор работает в роли менеджера резервирования и разомкнул кольцо, то есть линия коммутаторов, подключённая к портам кольца, работает без ошибок. Состояние «Passive» также отображается, если IE-коммутатор не работает как менеджер резервирования (Redundancy Manager Disabled).

- **Active**

IE-коммутатор работает в роли менеджера резервирования и замкнул кольцо, то есть линия коммутаторов, подключённая к портам кольца, разорвана (случай ошибки). Менеджер резервирования переключает соединение между своими кольцевыми портами и тем самым вновь обеспечивает сквозную линейную топологию.

- «-»

Функция резервирования активирована.

- **Admin Ring Port 1 и Admin Ring Port 2**

Эти столбцы демонстрируют порты, которые сконфигурированы как кольцевые порты.

- **Oper. Ring Port 1 и Oper. Ring Port 2**

Эти столбцы демонстрируют порты, которые используются как кольцевые порты. Если резервирование носителей в кольцевой топологии полностью отключено, то отображаются последние сконфигурированные кольцевые порты.

- **No. of Changes to RM Active State**

Отображает, как часто устройство переключалось в активное состояние в качестве менеджера резервирования, то есть как часто замыкалось кольцо.

Если функция резервирования деактивирована, или если для устройства выбрана роль «HRP/MRP Client», появляется текст «Redundancy Manager Disabled».

- **Max. Delay of RM Test Packets [ms]**

Отображает максимальное время задержки тестовых пакетов Redundancy Manager.

Если функция резервирования деактивирована, или если для устройства выбрана роль «HRP/MRP Client», появляется текст «Redundancy Manager Disabled».

Отображаются следующие поля:

- **Observer Status**

Отображает текущий статус наблюдателя.

- **Кнопка «Reset Counter»**

Примечание

Эта кнопка становится активной только в том случае, если активен способ кольцевого резервирования «HRP Manager».

Щёлкните «Reset Counter», чтобы сбросить все счётчики. Счётчики сбрасываются при повторном пуске устройства.

6.3.7.3 Standby

Информация о Standby Redundancy

На этой вкладке можно найти сведения о статусе устройства в отношении резервирования в режиме ожидания. Текстовые поля этой страницы доступны только для чтения.

Примечание

Устройство с более высоким MAC-адресом получает статус Master

Для соединения HRP-колец с резервированием всегда конфигурируются два устройства как пара Master/Slave. Это также относится к разорванным HRP-кольцам = линиям. В состоянии без ошибок функцию Master всегда принимает на себя устройство с более высоким MAC-адресом.

Этот вид распределения важен, в частности, при замене устройств. В зависимости от MAC-адреса предыдущее устройство с функцией Slave может принимать на себя роль Master в режиме ожидания.

На вкладке Standby находится информация о статусе функции ожидания:

Standby

Spanning Tree | Ring Redundancy | **Standby** | Link Check | MRP Interconnection

Standby Ports: P0.6

Standby Name: STB1

Standby Function: Waiting for connection

Standby Status: Passive

No. of Changes to Standby Active State: 0

Reset Counters

Refresh

Описание отображаемых значений

Отображаются следующие поля:

- **Standby Ports**
Показывает порт режима ожидания.
- **Standby Name**
Имя соединения в режиме ожидания

- **Standby Function**

- Master
Устройство установило соединение с партнёрским устройством и работает как Master. В безупречном состоянии на этом устройстве активирован порт режима ожидания.
- Slave
Устройство установило соединение с партнёрским устройством и работает как Slave. В безупречном состоянии на этом устройстве деактивирован порт режима ожидания.
- Disabled
Соединение в режиме ожидания деактивировано. Устройство не работает ни как Master, ни как Slave. Порт, сконфигурированный в качестве порта режима ожидания, работает как нормальный порт без функции ожидания.
- Waiting for connection
Соединение с партнёрским устройством пока не установлено. Порт режима ожидания неактивен. В этом случае либо конфигурация партнёрского устройства не единообразна (например, неверное имя соединения, соединение в режиме ожидания деактивировано), либо имеется физическая ошибка (например, отказ устройства или падение канала).
- Connection Lost
Установленное соединение с партнёрским устройством потеряно. В этом случае либо конфигурация партнёрского устройства изменилась (например, другое имя соединения, соединение в режиме ожидания деактивировано), либо имеется физическая ошибка (например, отказ устройства или падение канала).

- **Standby Status**

Поле индикации «Standby Status» отображает статус порта режима ожидания:

- Active
Порт режима ожидания этого устройства активен, то есть разблокирован для обмена пакетами.
- Passive
Порт режима ожидания этого устройства неактивен, то есть заблокирован для обмена пакетами.
- «-»:
функция режима ожидания деактивирована.

- **No. of Changes to Standby Active State**

Показывает, как часто IE-коммутатор менял статус с состояния «Passive» на состояние «Active». Если происходит отказ соединения в режиме ожидания у устройства Master для режима ожидания, то IE-коммутатор переключается в состояние «Active». Если функция режима ожидания деактивирована, то в этом поле появляется текст «Standby Disabled».

Описание кнопки

Кнопка «Reset Counter»

Щёлкните «Reset Counter», чтобы сбросить счётчик. Счётчик сбрасывается при повторном пуске устройства.

6.3.7.4 Link Check

Контроль оптических соединений в кольце

Страница отображает следующие данные для Link Check:

- Порты кольца
- Текущий статус (активировано или не активировано)
- Статистика отправленных и полученных пакетов Link Check контролируемых соединений

Примечание

При использовании Link Check вместе с протоколом резервирования (например, HRP) значения для отправленных и полученных пакетов Link Check могут быть различны.

Link Check				
Spanning Tree	Ring Redundancy	Standby	Link Check	MRP-Interconnection
Port	Link Check	Operating Status	Frames In	Frames Out
P0.11	disabled	disabled	0	0
P0.12	disabled	disabled	0	0
Refresh				

Описание отображаемых значений

Отображаются следующие поля:

- **Port**
Отображает порт, к которому относятся различные данные. Порт складывается из номера модуля и номера порта, например, порт 0.1 означает модуль 0, порт 1.
- **Link Check**
Отображает, активирована ли функция Link Check или нет. Функцию Link Check можно активировать только для оптических портов.

- **Operational State**
Отображает статус функции Link Check. Существуют следующие состояния:
 - Disabled
Функция деактивирована.
 - Enabled
Функция активирована. Партнёр по соединению ещё не подтвердил контроль.
 - Running
Функция активирована. Контроль соединения активен. Исходящие и входящие пакеты подсчитываются и сравниваются.
 - Faults
Функция активирована. Функция Link Check зафиксировала ошибку на контролируемом участке и отключила порт.
- **Frames In**
Отображает, сколько тестовых пакетов Link Check принято.
- **Frames Out**
Отображает, сколько тестовых пакетов Link Check отправлено.

6.3.7.5 MRP Interconnection

Резервное соединение кольцевых сетей

MRP Interconnection							
Spanning Tree	Ring Redundancy	Standby	Link Check	MRP Interconnection			
Interconnection Domain ID	Interconnection Domain Name	Interconnection Port	Port State	Oper. Role/Position	Connection State	Open Count	Open Time
1	MrpIntCon1	P0.5	Not connected	Disabled	-	0	-
Reset Counters							
Refresh							

Описание

Отображаются следующие поля:

- **Interconnection Domain ID**
Идентификатор соединения MRP Interconnection.
- **Interconnection Domain Name**
Название соединения MRP Interconnection.
- **Interconnection Port**
Порт, который используется для соединения MRP Interconnection.

- **Port Status**
Отображает, включён порт или выключен. Обмен данными возможен только через включённый порт. Имеются следующие возможности:
 - Forwarding
Порт используется.
 - Blocked
Порт заблокирован.
 - Disabled
Порт деактивирован.
 - Not connected
Порт не подключён.
- **Oper. Role/Position**
Отображает роль устройства. В роли Client дополнительно отображается позиция клиента. Имеются следующие возможности:
 - Disabled
 - Manager
 - Primary Client
 - Secondary Client
- **Connection Status**
Статус домена MRP Interconnection. Имеются следующие возможности:
 - Disabled
 - Undefined
 - Open
Резервное соединение недоступно.
 - Closed
Резервное соединение доступно.
- **Open Count**
Отображает, как часто после последнего сброса счётчиков в MIM наступало состояние Open. В MIC это значение всегда равно «0».
- **Open Time**
Время, прошедшее с последнего наступления состояния Open. В MIC значение здесь не отображается.
- **Reset Counter**
Щёлкните Reset Counter, чтобы сбросить счётчик. Счётчик сбрасывается при повторном пуске устройства.

6.3.8 Ethernet Statistics

6.3.8.1 Interface Statistics

Interface Statistics

Страница отображает статистику из таблицы интерфейсов Management Information Base (MIB).

Примечание

Статистика интерфейсов приводит общее число полученных или отправленных байтов для каждого порта. В отличие от этого, данные для интерфейсов VLAN основываются только на трафике Layer 3 соответствующего интерфейса.

Ethernet Statistics: Interface Statistics									
Interface Statistics	Packet Size	Packet Type	Packet Error	History					
	In Octet	Out Octet	In Unicast	In Non-Unicast	Out Unicast	Out Non-Unicast	In Discard	Out Discard	In Errors
P0.1	0	0	0	0	0	0	0	0	0
P0.2	1024384	2631069	3810	5991	4627	269	0	0	0
P0.3	0	0	0	0	0	0	0	0	0
P0.4	0	0	0	0	0	0	0	0	0
P0.5	0	0	0	0	0	0	0	0	0
P0.6	0	0	0	0	0	0	0	0	0
P0.7	0	0	0	0	0	0	0	0	0
P0.8	0	0	0	0	0	0	0	0	0
AG1	0	0	0	0	0	0	0	0	0
vlan1	455383	2542767	4903	0	4647	12	0	0	0
loopback0	0	0	0	0	0	0	0	0	0
Reset Counter									
Refresh									

Описание отображаемых значений

Таблица состоит из следующих столбцов:

- **In Octet**
Отображает количество полученных байтов.
- **Out Octet**
Отображает количество отправленных байтов.
- **In Unicast**
Отображает количество полученных пакетов Unicast.
- **In Non-Unicast**
Отображает количество полученных пакетов, которые не относятся к типу Unicast.
- **Out Unicast**
Отображает количество отправленных пакетов Unicast.
- **Out Non-Unicast**
Отображает количество отправленных пакетов, которые не относятся к типу Unicast.

- **In Discard**
Отображает количество входящих кадров, которые были отбракованы.
- **Out Discard**
Отображает количество исходящих кадров, которые были отбракованы.
- **In Errors**
Отображает количество всех возможных ошибок RX, см. вкладку Packet Error.

Описание кнопки

Кнопка «Reset Counter»

Щёлкните «Reset Counter», чтобы сбросить все счётчики. Счётчики сбрасываются при повторном пуске устройства.

6.3.8.2 Packet Size

Пакеты, отсортированные по длине

Эта страница показывает количество, длину и порт отправленных и полученных пакетов. Выполнение конфигурации на этой странице невозможно.

Отображаемые значения передаются через RMON.

На странице «Layer 2 > RMON > Statistics» можно настроить, для каких портов должны отображаться значения.

Ethernet Statistics: Packet Size						
Interface Statistics	Packet Size	Packet Type	Packet Error	History		
Port	64	65-127	128-255	256-511	512-1023	1024-max
P0.1	0	0	0	0	0	0
P0.2	0	0	0	0	0	0
P0.3	0	0	0	0	0	0
P0.4	0	0	0	0	0	0
Reset Counter						
Refresh						

Описание отображаемых значений

Таблица состоит из следующих столбцов:

- **Port**

Отображает доступные порты и агрегации каналов. Порт складывается из номера модуля и номера порта, например, порт 0.1 означает модуль 0, порт 1.

Примечание

Отображение статистики пакетов

В отношении статистики длины пакетов следует учитывать, что подсчитываются, как входящие, так и исходящие пакеты.

- **Packet Size**

Дополнительные столбцы после соответствующего номера порта содержат абсолютные значения для пакетов в соответствии с их длиной.

При этом различают следующую длину пакетов:

- 64 байта
- 65—127 байтов
- 128—255 байтов
- 256—511 байтов
- 512—1023 байтов
- 1024—макс.

Примечание

Трафик на заблокированных портах

По техническим причинам на заблокированных портах могут отображаться пакеты данных.

Описание кнопки

Кнопка «Reset Counter»

Щёлкните «Reset Counter», чтобы сбросить все счётчики. Счётчики сбрасываются при повторном пуске устройства.

6.3.8.3 Frame Type

Полученные пакеты, отсортированные по параметру Frame Type

Эта страница показывает количество полученных пакетов типов Unicast, Multicast и Broadcast на каждом порте. Выполнение конфигурации на этой странице невозможно.

Отображаемые значения передаются через RMON.

На странице «Layer 2 > RMON > Statistics» можно настроить, для каких портов должны отображаться значения.

Ethernet Statistics: Packet Type

Interface Statistics	Packet Size	Packet Type	Packet Error	History
Port	Unicast	Multicast	Broadcast	
P0.1	0	0	0	
P0.2	0	0	0	
P0.3	0	0	0	
P0.4	0	0	0	

Reset Counter

Refresh

Описание отображаемых значений

Таблица состоит из следующих столбцов:

- **Port**
Отображает доступные порты и агрегации каналов. Порт складывается из номера модуля и номера порта, например, порт 0.1 означает модуль 0, порт 1.
- **Unicast / Multicast / Broadcast**
Дополнительные столбцы после соответствующего номера порта содержат абсолютные значения в соответствии с параметром типа пакета Frame Type: Unicast, Multicast и Broadcast.

Описание кнопки

Кнопка «Reset Counter»

Щёлкните «Reset Counter», чтобы сбросить все счётчики. Счётчики сбрасываются при повторном пуске устройства.

6.3.8.4 Packet Error

Ошибочные полученные пакеты

Эта страница отображает количество ошибочных полученных пакетов для каждого порта. Выполнение конфигурации на этой странице невозможно.

Отображаемые значения передаются через RMON.

На странице «Layer 2 > RMON > Statistics» можно настроить, для каких портов должны отображаться значения.

Ethernet Statistics: Packet Error						
Interface Statistics	Packet Size	Packet Type	Packet Error	History		
Port	CRC	Undersize	Oversize	Fragments	Jabbers	Collisions
P0.1	0	0	0	0	0	0
P0.2	0	0	0	0	0	0
P0.3	0	0	0	0	0	0
P0.4	0	0	0	0	0	0
Reset Counter						
Refresh						

Описание отображаемых значений

Таблица поделена на следующие столбцы:

- **Port**
Отображает доступные порты и агрегации каналов. Порт складывается из номера модуля и номера порта, например, порт 0.1 означает модуль 0, порт 1.
- **Типы ошибок**
Дополнительные столбцы после соответствующего номера порта содержат абсолютные значения входящих пакетов в соответствии с их типом ошибок. При этом в столбцах таблицы различают следующие типы ошибок:
 - CRC
Пакеты, содержимое которых не совпадает с соответствующей контрольной суммой CRC.
 - Undersize
Пакеты с длиной менее 64 байтов.
 - Oversize
Пакеты, отбракованные из-за слишком большой длины.
 - Fragments
Пакеты с длиной менее 64 байтов и неверной контрольной суммой CRC.
 - Jabbers
Пакеты с тегом VLAN и неверной контрольной суммой CRC, отбракованные из-за слишком большой длины.
 - Collisions
Распознанные коллизии.

Описание кнопки

Кнопка «Reset Counter»

Щёлкните «Reset Counter», чтобы сбросить все счётчики. Счётчики сбрасываются при повторном пуске устройства.

6.3.8.5 History

Образцы статистики

Страница отображает выборочные пробы с данными из статистики RMON для каждого порта.

На странице «Layer 2 > RMON > History» можно настроить, для каких портов должны выполняться выборочные пробы.

Ethernet History

Interface Statistics

Packet Size

Packet Type

Packet Error

History

Port: P0.1

Buckets: 24

Interval[s]: 3600

Sample	Sample Time	Unicast	Multicast	Broadcast	CRC	Undersize	Oversize	Fragments	Jabbers	Collisions	Utilization[%]
67	2d 18h 14m 13s	0	0	0	0	0	0	0	0	0	0
68	2d 19h 14m 25s	0	0	0	0	0	0	0	0	0	0
69	2d 20h 14m 37s	0	0	0	0	0	0	0	0	0	0
70	2d 21h 14m 49s	0	0	0	0	0	0	0	0	0	0
71	2d 22h 15m 1s	0	0	0	0	0	0	0	0	0	0

Refresh

Настройки

- **Порт**
Выберите порт, для которого должна отображаться история History.

Описание отображаемых значений

- **Buckets**
Максимальное количество выборочных проб, которые сохраняются одновременно.
- **Interval[s]**
Интервал, в соответствии с которым текущий уровень статистики будет сохраняться как выборочная проба.

Таблица состоит из следующих столбцов:

- **Sample**
Номер выборочной пробы
- **Sample Time**
Время работы системы (System Up Time), в которое была взята выборочная проба.
- **Unicast**
Количество полученных пакетов Unicast.
- **Multicast**
Количество полученных пакетов Multicast.

6.3 Меню «Information»

- **Broadcast**
Количество полученных пакетов Broadcast.
- **CRC**
Количество полученных пакетов с неверной контрольной суммой CRC.
- **Undersize**
Количество пакетов с длиной менее 64 байтов.
- **Oversize**
Количество пакетов, забракованных из-за превышения размера.
- **Fragments**
Количество пакетов с длиной менее 64 байтов и имеющих неверную контрольную сумму CRC.
- **Jabbers**
Количество пакетов с тегом VLAN, имеющих неверную контрольную сумму CRC и забракованных из-за превышения размера.
- **Collisions**
Количество коллизий полученных пакетов.
- **Utilization[%]**
Использование портов во время выборочной пробы.

6.3.9 Unicast

Статус таблицы фильтров Unicast

Эта страница отображает актуальное содержимое таблицы фильтров Unicast. В этой таблице приводятся адреса источников адресных пакетов Unicast. Записи могут выполняться либо динамически, когда участник отправляет пакет порту, либо статически путём параметрирования со стороны пользователя.

Зависимость от режима «Base Bridge Mode»

Отображаемые столбцы зависят от настроенного режима базового моста (Base Bridge Mode). При изменении режима «Base Bridge Mode» существующие записи будут потеряны.

Страница WBM для режима базового моста «802.1D Transparent Bridge»:

Unicast		
MAC Address	Status	Port
08-00-06-70-2f-41	Learnt	P0.1
68-05-ca-19-40-bb	Learnt	P0.1
2 entries.		
Refresh		

Страница WBM для режима базового моста «802.1Q VLAN Bridge»:

Unicast			
VLAN ID	MAC Address	Status	Port
1	00-1b-1b-a5-5d-98	Learnt	P0.1
1	08-00-06-70-2f-41	Learnt	P0.1
1	68-05-ca-19-40-bb	Learnt	P0.1
3 entries.			
Refresh			

Описание

Таблица может содержать следующие столбцы:

- **VLAN ID**
Отображает идентификатор VLAN, присвоенный этому MAC-адресу.
- **MAC Address**
Отображает MAC-адрес участника, который был запомнен устройством или сконфигурирован пользователем.

- **Status**

Отображает статус каждой записи адреса:

- **Learnt**

Введённый адрес запомнен благодаря приёму пакета этого участника и по истечении параметра Aging Time будет вновь удалён, если от участника не поступят следующие пакеты.

Примечание

При падении канала запомненные MAC-адреса удаляются.

- **Static**

Запрограммирован пользователем. Статические адреса хранятся постоянно, то есть они не будут удалены по истечении параметра времени старения (Aging Time) или повторном пуске коммутатора.

- **Other**

Введённый адрес был запомнен не напрямую с помощью Private VLAN.

- **Port**

Отображает, через какой порт доступен участник с указанным адресом. Полученные устройством пакеты, целевой адрес которых совпадает с этим адресом, будут переданы далее на этот порт.

6.3.10 Multicast

Статус таблицы фильтров Multicast

Эта таблица отображает пакеты Multicast с их целевыми портами, зарегистрированные в текущий момент в таблице фильтров. Эти записи могут выполняться как динамическим (устройство их запомнило), так и динамическим способом (пользователь запрограммировал их).

Зависимость от режима «Base Bridge Mode»

При изменении режима «Base Bridge Mode» существующие записи будут потеряны.

Multicast						
VLAN ID	MAC Address	Status	P0.1	P0.2	P0.3	P0.4
1	01-00-5a-00-00-00	Static	-	-	-	-
1 entry.						
Refresh						

Описание

Таблица может содержать следующие столбцы:

- **VLAN ID**
Отображает идентификатор VLAN, который присвоен MAC-адресу Multicast.
- **MAC Address**
Отображает MAC-адрес Multicast, который запомнило устройство или сконфигурировал пользователь.
- **Status**
Отображает статус каждой записи адреса. При этом допускаются следующие данные:
 - Static
Адрес запрограммирован пользователем статическим способом. Статические адреса хранятся постоянно, то есть они не будут удалены по истечении параметра времени старения (Aging Time) или повторном пуске устройства. Пользователь может самостоятельно удалить их.
 - IGMP
Целевой порт для этого адреса определен через IGMP.
 - GMRP
Целевой порт для этого адреса зарегистрирован через полученную пакет GMRP.
- **Список портов**
Для каждого гнезда существует столбец. Внутри столбца для каждого порта отображается принадлежность к группе Multicast:
 - M
(Member) Через этот порт отправляются пакеты Multicast.
 - R
(Registered) Участник группы Multicast, регистрация выполнена с помощью пакета GMRP.
 - I
(IGMP) Участник группы Multicast, регистрация выполнена с помощью пакета IGMP.
 - –
Не является участником группы Multicast. Через этот порт не отправляются пакеты Multicast с определенным MAC-адресом Multicast.
 - F
(Forbidden) Не является участником группы Multicast. Кроме того, запрещено динамическое обучение этого порта через IGMP.

6.3.11 LLDP

Статус таблицы соседства

Эта страница отображает актуальное содержимое таблицы соседства. В этой таблице сохраняются данные, которые LLDP-агент получил от подключённых устройств.

6.3 Меню «Information»

Интерфейсы, через которые LLDP-агент принимает или передаёт данные, задаются в следующем разделе: Layer 2 > LLDP.

Link Layer Discovery Protocol (LLDP) Neighbors					
System Name	Device ID	Local Interface	Hold Time	Capability	Port ID
	00:5e:1d:d2:76:00	P1.2	20	Bridge,Router	port-002-00002
MD15UYDC	md15uydc	P1.3	20	Station	port-001
Refresh					

Описание отображаемых значений

Таблица содержит следующие столбцы:

- **System Name**
Системное имя подключённого устройства
- **Device ID**
Кодовое обозначение подключённого устройства. Идентификатор устройства соответствует имени устройства, которое задаётся, например, через SINEC PNI. Если имя устройства не задано, отображается MAC-адрес устройства.
- **Local Interface**
Порт, на котором IE-коммутатор получил данные
- **Hold Time**
Время сохранения в секундах
Запись сохраняется в устройстве в течение указанного здесь времени. Если IE-коммутатор в течение этого времени не получает новые данные от подключённого устройства, запись удаляется.
- **Capability**
Отображает характеристики подключённого устройства:
 - Маршрутизатор
 - Мост
 - Телефон
 - Кабельное устройство DOCSIS
 - Точка доступа WLAN
 - Повторитель
 - Станция
 - Другое
- **Port ID**
Порт устройства, с которым соединён IE-коммутатор.

6.3.12 Fiber Monitoring Protocol

Контроль оптических участков

С помощью функции Fiber Monitoring можно контролировать оптические участки. Отображает текущее состояние порта.

Контролируемые значения можно настроить на следующей странице: Layer 2 > FMP.

Fiber Monitoring Protocol (FMP) Diagnosis				
Port	Rx Power State	Rx Power[dBm]	Power Loss State	Power Loss[dB]
P0.1	link down	-	idle	-
P0.2	ok	-21.1	ok	-5.9
P0.4	link down	-	idle	-
Refresh				

Описание отображаемых значений

Порт

Отображает оптические порты, которые поддерживают функцию Fiber Monitoring. Это зависит от трансиверов.

Rx Power State

- **disabled**
Функция Fiber Monitoring деактивирована.
- **ok**
Значение для мощности приёма оптического участка находится в установленных пределах.
- **maint. req.**
Участок желательно проверить.
Сообщается предупреждение.
- **maint. dem.**
Участок необходимо проверить.
Сообщается сигнал тревоги и загорается светодиод ошибки.
- **link down**
Соединение с партнёром по обмену данными прервано. Канал не обнаружен.

Rx Power[dBm]

Отображает текущее значение мощности приёма. Значение может иметь погрешность +/- 3 дБ.

При отсутствии соединения (Link down) или деактивированной функции Fiber Monitoring отображается «-». Если на порте партнёра не активирована функция Fiber Monitoring, то отображается значение 0.0.

Power Loss State

6.3 Меню «Information»

Для контроля падения мощности соединения необходимо активировать функцию Fiber Monitoring для оптического порта партнёра по соединению.

- **disabled**
Функция Fiber Monitoring деактивирована.
- **ok**
Значение для падения мощности оптического участка находится в установленных пределах.
- **maint. req.**
Участок желательно проверить.
Сообщается предупреждение.
- **maint. dem.**
Участок необходимо проверить.
Сообщается сигнал тревоги и загорается светодиод ошибки.
- **idle**
Порт не имеет соединения с другим портом с активированной функцией Fiber Monitoring.
Если в течение 5 циклов не будут получены диагностические данные от оптического порта партнёра по соединению, то соединение Fiber Monitoring будет считаться разорванным. Один цикл длится 5 секунд.

Power Loss[dB]

Отображает текущее значение падения мощности. Значение может иметь погрешность +/- 3 дБ.

При отсутствии соединения (Link down), деактивированной функции Fiber Monitoring или в том случае, если порт партнёра не поддерживает функцию Fiber Monitoring, отображается «-».

6.3.13 Routing

6.3.13.1 Routing Table

Введение

Эта страница отображает текущие использованные маршруты.

Layer 3: IPv4 Routing Table					
Routing Table		NAT Translations			
Destination Network	Subnet Mask	Gateway	Interface	Metric	Routing Protocol
0.0.0.0	0.0.0.0	192.168.178.1	vlan1	1	static
192.168.178.0	255.255.255.0	0.0.0.0	vlan1	0	connected

2 entries.

[Refresh](#)

Описание отображаемых значений

Таблица состоит из следующих столбцов:

- **Destination Network**
Показывает адрес цели этого маршрута.
- **Subnet Mask**
Показывает маску подсети этого маршрута.
- **Gateway**
Показывает шлюз для этого маршрута. В маршрутах Sink вместо IP-адреса отображается указание «Sink».
- **Interface**
Показывает интерфейс для этого маршрута.
- **Metric**
Показывает метрику маршрута. Чем больше значение, тем больше потребуется времени пакетам для достижения цели.
- **Routing Protocol**
Показывает, какой протокол маршрутизации является источником записи в таблице маршрутизации. Допускаются следующие записи:
 - Connected: связанные маршруты
 - Static: статические маршруты
 - RIP: маршруты через RIP
 - OSPF: маршруты через OSPF
 - Other: прочие маршруты

6.3.13.2 NAT Translations

Обзор

Эта страница отображает активные соединения NAT.

Описание отображаемых значений

Network Address Translation (NAT) Translations							
Routing Table NAT Translations							
Interface	Inside Local Address	Inside Local Port	Inside Global Address	Inside Global Port	Outside Local/Global Address	Outside Local/Global Port	Last Use Time[s]
vlan1	10.0.0.2	161	140.80.100.1	161	140.80.58.23	59269	11
vlan1	10.0.0.2	49156	140.80.100.1	49156	140.80.57.72	123	46
vlan1	10.0.0.9	80	140.80.103.1	80	140.80.57.73	49620	49
vlan1	10.0.0.9	80	140.80.103.1	80	140.80.57.73	49621	49
vlan1	10.0.0.9	80	140.80.103.1	80	140.80.57.73	49623	47
vlan1	10.0.0.9	80	140.80.103.1	80	140.80.57.73	49624	46
vlan1	10.0.0.9	80	140.80.103.1	80	140.80.57.73	49625	46
vlan1	10.0.0.9	80	140.80.103.1	80	140.80.57.73	49626	46
vlan1	10.0.0.9	80	140.80.103.1	80	140.80.57.73	49627	46
vlan1	10.0.0.9	80	140.80.103.1	80	140.80.57.73	49628	46

[Refresh](#)

Таблица состоит из следующих столбцов:

- **Interface**
отображает IP-интерфейс.
- **Inside Local Address**
Отображает фактический адрес устройства, которое должно быть доступно извне.
- **Inside Local Port**
Отображает порт, присвоенный адресу Inside Local Address.
- **Inside Global Address**
Отображает адрес, по которому устройство должно быть доступно для внешних источников.
- **Inside Global Port**
Отображает порт, присвоенный адресу Inside Global Address.
- **Outside Local/Global Address**
Отображает адрес партнёра по коммуникации.
- **Outside Local/Global Port**
Отображает порт внешнего партнёра по коммуникации.
- **Last Use Time[s]**
Показывает момент времени передачи последнего пакета.

6.3.14 DHCP Server

Эта страница отображает, какие адреса IPv4 присвоены устройствам сервером DHCP.

DHCP Server Bindings						
IP Address	Pool ID	Identification Method	Identification Value	Allocation Method	Binding State	Expire Time
192.168.16.90	1	Client ID	OS-EC74BA03FED2	dynamic	assigned	01/01/2000 05:21:03
1 entry.						
Refresh						

Описание

- **IP Address**
Отображает адрес IPv4, присвоенный клиенту DHCP.
- **Pool ID**
Отображает номер диапазона IPv4-адресов.
- **Identification Method**
Отображает метод идентификации клиента DHCP.
- **Identification Value**
Отображает MAC-адрес или идентификатор клиента DHCP.
- **Allocation Method**
Отображает, был ли адрес IPv4 присвоен статически или динамически. Статические записи конфигурируются в пункте меню System > DHCP > Static Leases.
- **Binding State**
Отображает статус присвоения.
 - assigned
Присвоение используется.
 - not used
Присвоение не используется.
 - probing
Присвоение проверяется.
 - unknown
Статус присвоения неизвестен.
- **Expire Time**
Отображает срок действия присвоенного адреса IPv4. До этого момента клиент DHCP либо должен запросить новый адрес IPv4, либо продлить срок действия присвоенного адреса IPv4.

6.3.15 Diagnostics

Эта страница отображает значения производительности и температуры внутренних и внешних узлов устройства. Узлы отображаются только в том случае, если они предоставляют соответствующие данные. При добавлении или удалении узла индикация автоматически адаптируется. Если показатель производительности превышает установленное пороговое значение, то статус изменяется соответствующим образом. В случае значения температуры статус также изменяется, если не достигается нижнее пороговое значение.

Пороговые значения задаются устройством, и изменить их невозможно. Если пороговые значения не заданы, то отображается «-». На странице System > Events > Configuration можно настроить, как устройство будет сообщать об изменении статуса.

Diagnostics

Usage Table

Name	Status	Usage [%]	High Warning Threshold [%]	High Critical Threshold [%]
CPU	OK	3	-	-
RAM	OK	63	90	98

Temperature Table

Name	Status	Temperature [°C]	Low Critical Threshold [°C]	Low Warning Threshold [°C]	High Warning Threshold [°C]	High Critical Threshold [°C]
Chassis	OK	34	-25	-17	87	95

Refresh

Описание

Таблица **Usage Table** состоит из следующих столбцов:

- **Name**
Отображает имя узла.
- **Status**
В зависимости от соотношения между пороговыми значениями и текущей мощностью отображаются следующие значения статуса с возрастающим приоритетом:
 - **OK**
Мощность находится ниже заданного порогового значения.
 - **WARNING**
Верхнее пороговое значение степени сложности Warning превышено. Мощность ещё находится в нормальном диапазоне. Условия эксплуатации устройства желательно проверить.
 - **CRITICAL**
Верхнее пороговое значение степени сложности Critical превышено. Устройство необходимо проверить. Перегрузка устройства может привести к его неправильной работе.
 - **INVALID**
Мощность не удалось определить, либо она недействительна. В поле «Usage [%]» отображается «-».
 - **INITIAL**
Данные ещё не считаны. Во всех полях отображается «-».
- **Usage [%]**
Отображает текущее значение мощности устройства. Индикация регулярно обновляется.
- **High Warning Threshold [%]**
При превышении этого порогового значения статус меняется на WARNING. Можно сконфигурировать вывод этого сообщения.
- **High Critical Threshold [%]**
При превышении этого порогового значения статус меняется на CRITICAL. Можно сконфигурировать вывод этого сообщения.

Таблица **Temperature Table** состоит из следующих столбцов:

- **Name**
Отображает имя узла.
Данные в строке **Chassis** относятся ко внутренней температуре корпуса.
В случае вставных трансиверов отображаются порт и тип.
- **Status**
В зависимости от соотношения между пороговыми значениями и текущей температурой отображаются следующие значения статуса с возрастающим приоритетом:
 - **OK**
Значение температуры находится в рамках установленных пороговых значений.
 - **WARNING**
Нижнее или верхнее пороговое значение степени сложности **Warning** не достигнуто или превышено. Температура ещё находится в нормальном диапазоне. Устройство распознало падение или рост температуры, например, из-за изменения охлаждения электрошкафа. Температуру желательно проверить.
 - **CRITICAL**
Нижнее или верхнее пороговое значение степени сложности **Critical** не достигнуто или превышено. Устройство необходимо проверить. Слишком низкая или высокая температура может привести к ограничению мощности или повреждениям устройства.
 - **INVALID**
Значение не удалось считать, либо оно недействительно. В поле **Temperature [°C]** отображается «-».
 - **INITIAL**
Данные ещё не считаны. Во всех полях отображается «-».
- **Temperature [°C]**
Отображает текущее значение температуры. Индикация регулярно обновляется. Значение может иметь погрешность +/- 3°C. Из-за этого значение для одинаковых устройств с аналогичными условиями окружающей среды может различаться.
- **Low Critical Threshold [°C]**
При недостижении этого порогового значения статус меняется на **CRITICAL**. Можно сконфигурировать вывод этого сообщения.
- **Low Warning Threshold [°C]**
При недостижении этого порогового значения статус меняется на **WARNING**. Можно сконфигурировать вывод этого сообщения.
- **High Warning Threshold [°C]**
При превышении этого порогового значения статус меняется на **WARNING**. Можно сконфигурировать вывод этого сообщения.
- **High Critical Threshold [°C]**
При превышении этого порогового значения статус меняется на **CRITICAL**. Можно сконфигурировать вывод этого сообщения.

6.3.16 SNMP

Эта страница отображает созданные группы SNMPv3. Группы SNMPv3 конфигурируются в пункте меню System > SNMP.

Simple Network Management Protocol v3 (SNMPv3) Groups Overview	
Group Name	User Name
Service	Mueller
Wartung	Peterson
Refresh	

Описание

Таблица состоит из следующих столбцов:

- **Group Name**
Отображает имя группы.
- **Username**
Отображает пользователя, который присвоен группе.

6.3.17 Security

6.3.17.1 Overview

Примечание

От прав авторизованного пользователя зависит, какие значения будут отображаться.

Страница отображает настройки безопасности, а также локальные и внешние учётные записи пользователей.

Security Overview

OverviewSupported Function RightsRolesGroups802.1X Port StatusMAC Authentication

Services

Telnet Server: enabled
SSH Server: enabled
SSH Fingerprint: MD5: 6c:bf:66:d6:d2:e0:ae:cc:21:c2:13:46:70:2e:75:06
SHA256: GQL5H5lev5IZK/iwWA491LnmXNMKpDJHms8s7TJJEe8
Web Server: HTTP/HTTPS
SNMP: SNMPv1/v2c/v3
Management ACL: disabled: no access restriction
Login Authentication: Local
Password Policy: low

Local User Accounts

User Account	Role
admin	admin
Service	user

External User Accounts

User Account	Role
admin	admin
Service	user

Refresh

Описание

Services

Список Services отображает настройки безопасности.

- Telnet Server**
Настройки выполняются в пункте меню System > Configuration.
 - Enabled: доступ к CLI без шифрования
 - Disabled: доступ к CLI без шифрования отсутствует
- SSH Server**
Настройки выполняются в пункте меню System > Configuration.
 - Enabled: доступ к CLI с шифрованием
 - Disabled: доступ к CLI с шифрованием отсутствует
- SSH Fingerprint**
Поле отображает SSH Fingerprint.

- **Web Server**

Настройки выполняются в пункте меню System > Configuration.

- HTTP/HTTPS: доступ к WBM возможен через HTTP и HTTPS.
- HTTPS: доступ к WBM возможен только через HTTPS.

- **SNMP**

Настройки выполняются в пункте меню System > SNMP > General.

- «-» (SNMP деактивирован)
Доступ к параметрам устройства по SNMP невозможен.
- SNMPv1/v2c/v3
Доступ к параметрам устройства возможен через SNMP версий 1, 2с или 3.
- SNMPv3
Доступ к параметрам устройства возможен только через SNMP версии 3.

- **Management ACL**

Настройки выполняются в пункте Security > Management ACL

- Enabled: restricted access only: Доступ ограничивается списком Access Control List (ACL).
- Disabled: no access restriction: функция Management ACL не активирована.

- **Login Authentication**

Настройки выполняются в пункте меню Security > AAA > General.

- Local
Аутентификация должна выполняться локально на устройстве.
- RADIUS
Аутентификация должна выполняться через сервер RADIUS.
- Local and RADIUS
Аутентификация может выполняться как через учётные записи пользователей, имеющих на устройстве (имя пользователя и пароль), так и через сервер RADIUS. Сначала выполняется поиск пользователя в локальной базе данных. Если пользователь отсутствует, то отправляется запрос RADIUS.
- RADIUS and fallback Local
Аутентификация должна выполняться через сервер RADIUS. Локальная аутентификация выполняется только в том случае, если сервер RADIUS недоступен в сети.

- **Password Policy**

Отображает, какая политика паролей используется в настоящий момент.

Локальные и внешние учётные записи пользователей

Локальные учётные записи пользователей и роли конфигурируются в пункте Security > Users.

При создании локальной учётной записи пользователя автоматически генерируется и внешняя учётная запись пользователя.

В случае локальных учётных записей речь идёт о пользователях с паролем для авторизации на устройстве.

6.3 Меню «Information»

В таблице External User Accounts пользователь связывается с ролью. В этом примере пользователь Service связывается с ролью user. Пользователь определяется на сервере RADIUS. Роль определяется локально на устройстве. Когда сервер RADIUS аутентифицирует пользователя, однако сопутствующая группа неизвестна или ещё не создана, то устройство проверяет, имеется ли для пользователя запись в таблице External User Accounts. Если соответствующая запись существует, то пользователь авторизуется с правами, имеющимися у связанной роли. Если соответствующая группа известна устройству, то выполняется анализ обеих таблиц. Пользователю присваивается роль с более обширными правами.

Примечание

Анализ таблицы External User Accounts выполняется только в том случае, если в пункте RADIUS Authorization Mode выбрана настройка Vendor Specific.

С помощью CLI можно получать доступ к внешним учётным записям пользователей. Таблицы Local User Accounts и External User Accounts состоят из следующих столбцов:

- **User Account**
Отображает имя локального пользователя.
- **Role**
Отображает роль пользователя. Дополнительные сведения о функциональных правах роли см. в пункте Information > Security > Roles.

6.3.17.2 Supported Function Rights

Примечание

От роли авторизованного пользователя зависит, какие значения будут отображаться.

Страница отображает функциональные права (Function Rights), которые находятся в локальном доступе на устройстве.

Supported Function Rights	
Overview	Supported Function Rights
Roles	Groups
802.1X Port Status	MAC Authentication
Function Right	Description
1	Read-only access to configuration data.
15	Read/write access to configuration data.
Refresh	

Описание отображаемых значений

- **Function Right**
Отображает номер функционального права (Function Right). Номеру присвоены различные права в отношении параметров устройства.
- **Description**
Отображает описание функционального права (Function Right).

6.3.17.3 Roles

Примечание

От роли авторизованного пользователя зависит, какие значения будут отображаться.

Страница отображает роли, которые локально действительны на устройстве.

User Roles

Overview	Supported Function Rights	Roles	Groups	802.1X Port Status	MAC Authentication	
Role	Function Right	Description				
user	1	System defined role, with readonly access to configuration data of this component.				
admin	15	System defined role, with read/write access to configuration data of this component.				
default	1	Internal role, for authenticated users without group/role mapping in this component.				
everybody	0	Internal role, assigned to users when authentication failes. Access will be denied.				
Refresh						

Описание

Таблица содержит следующие столбцы:

- **Role**
Отображает имя роли.
- **Function Right**
Отображает функциональное право роли:
 - 1
Пользователи с этой ролью могут читать параметры устройства, но не могут их изменять.
 - 15
Пользователи с этой ролью могут как читать, так и изменять параметры устройства.
 - 0
При этом речь идёт о роли, которую присваивает само устройство, если пользователя не удастся идентифицировать. Пользователю запрещается доступ к устройству.
- **Description**
Отображает описание роли.

6.3.17.4 Groups

Примечание

От роли авторизованного пользователя зависит, какие значения будут отображаться.

Эта страница отображает связь группы с определённой ролью. Группа определяется на сервере RADIUS. Роль определяется локально на устройстве.

User Groups

OverviewSupported Function RightsRolesGroups802.1X Port StatusMAC Authentication

GroupRoleDescription

Grp1userAdmin Group

Refresh

Описание отображаемых значений

Таблица состоит из следующих столбцов:

- **Group**
Отображает имя группы. Имя соответствует группе на сервере RADIUS.
- **Role**
Отображает имя роли. Пользователи, прошедшие аутентификацию в связанной группе через сервер RADIUS, получают права этой роли локально на устройстве.
- **Description**
Отображает описание для привязки.

6.3.17.5 802.1X Port Status

Эта страница отображает статус аутентификации 802.1X для отдельных портов.

802.1X Port Status

Overview	Supported Function Rights	Roles	Groups	802.1X Port Status	MAC Authentication
----------	---------------------------	-------	--------	--------------------	--------------------

Port	802.1X Auth. Status	MAC Auth. Actual Allowed Addresses	MAC Auth. Actual Blocked Addresses	Guest VLAN Actual Allowed Addresses
P0.1	Authorized	0	0	0
P0.2	Authorized	0	0	0
P0.3	Authorized	0	0	0
P0.4	Authorized	0	0	0

Refresh

Описание

Таблица состоит из следующих столбцов:

- **Port**
В этом столбце приводятся все порты устройства.
- **802.1X Auth. Status**
Статус аутентификации участника. Имеются следующие возможности:
 - Authorized
Возможен обмен данными через этот порт после успешной аутентификации по методу «802.1X».
 - Unauthorized
Обмен данными через этот порт невозможен, так как ещё не выполнена аутентификация по методу «802.1X», либо попытка аутентификации была неудачной.
- **MAC Auth. Actual Allowed Addresses**
Отображает количество участников, которым разрешён доступ после успешной MAC-аутентификации.

- **MAC Auth. Actual Blocked Addresses**
Отображает количество участников, которым не разрешён доступ после неудачной MAC-аутентификации.
- **Guest VLAN Actual Allowed Addresses**
Отображает количество участников, которым разрешён доступ посредством функции «Guest VLAN».

6.3.17.6 MAC-Auth. Address Table

Эта страница отображает, для каких MAC-адресов выполнена MAC-аутентификация.

MAC-Auth. Address Table

Overview	Supported Function Rights	Roles	Groups	802.1X Port Status	MAC Authentication
VLAN ID	MAC Address	Status	Port		
1	00-10-94-13-00-01	Authenticated	P1.6		
1	00-10-94-13-00-02	Authenticated	P1.6		
1	00-10-94-ff-00-00	Authenticated	P1.6		
1	00-10-94-ff-00-01	Authenticated	P1.6		

Refresh

Описание

Таблица состоит из следующих столбцов:

- **VLAN ID**
Отображает идентификатор VLAN, присвоенный этому MAC-адресу.
- **MAC Address**
Отображает MAC-адрес участника, для которого отображается статус аутентификации.
- **Status**
Статус аутентификации участника. Имеются следующие возможности:
 - **Authorized**
Обмен данными возможен через порт после успешной аутентификации по методу MAC-аутентификации.
 - **Unauthorized**
Обмен данными через порт невозможен, так как ещё не выполнена аутентификация по методу MAC-аутентификации, либо попытка аутентификации была неудачной.
- **Port**
Отображает порт, через который можно осуществлять обмен данными с участником с заданным адресом.

6.4 Меню «System»

6.4.1 Configuration

System Configuration

Страница WBM содержит обзор конфигурации возможностей доступа для устройства.

Устанавливайте, с помощью каких служб к устройству будет осуществляться доступ. Для некоторых служб имеются дополнительные страницы конфигурации, на которых возможны дополнительные настройки.

System Configuration

☒ Telnet Server
Telnet Port: 23

☒ SSH Server
SSH Port: 22
SSH Key Exchange Algorithm Level: Low

☒ HTTP Server
HTTP Port: 80

☒ HTTPS Server
HTTPS Port: 443
Minimum TLS Version: TLSv1.1

☐ SMTP Client
☐ Syslog Client

DCP Server: Read/Write
Time: Manual

SNMP: SNMPv1/v2c/v3
☐ SNMPv1/v2 Read-Only
☒ SINEMA Configuration Interface
☒ ARP Keep Alive
ARP Keep Alive Interval: 30

Configuration Mode: Automatic Save
Write Startup Config

Set Values Refresh

Описание отображаемых полей

Страница содержит следующие поля:

- **Telnet Server**
Для доступа к CLI без шифрования можно активировать или деактивировать службу Telnet Server.
- **Telnet Port**
По умолчанию установлен порт 23. В качестве опции можно задать номер порта в диапазоне 1024 ... 49151 или 49500 ... 65535.
- **SSH Server**
Для доступа к CLI с шифрованием можно активировать или деактивировать службу SSH Server.
- **SSH Port**
По умолчанию установлен порт 22. В качестве опции можно задать номер порта в диапазоне 1024 ... 49151 или 49500 ... 65535.

- **SSH Key Exchange Algorithm Level**

Выберите в раскрывающемся списке ступень алгоритма обмена для ключа SSH. Имеются возможности настройки Low и High. Обе ступени содержат следующие алгоритмы шифрования:

- **Low**
Curve25519-sha256
Curve25519-sha256@libssh.org
Ecdh-sha2-nistp256
Ecdh-sha2-nistp384
Ecdh-sha2-nistp521
Diffie-hellman-group16-sha512
Diffie-hellman-group18-sha512
Diffie-hellman-group14-sha256
Diffie-hellman-group14-sha1
- **High**
Curve25519-sha256
Curve25519-sha256@libssh.org
Ecdh-sha2-nistp256
Ecdh-sha2-nistp384
Ecdh-sha2-nistp521
Diffie-hellman-group16-sha512
Diffie-hellman-group18-sha512

При обновлении прошивки до версии 4.3 алгоритм обмена для ключа SSH по причинам совместимости устанавливается на значение «Low». При настройке «Low» невозможно установить соединение со следующими SSH-клиентами, так как эти программы не поддерживают соответствующие алгоритмы:

- **TeraTerm**
- **PuTTY**
- **STS**

После сброса на заводские настройки в случае прошивки версии 4.3 алгоритм обмена для ключа SSH устанавливается на значение по умолчанию «High». При выборе настройки «High» следующие алгоритмы больше не предлагаются:

- **diffie-hellman-group14-sha256**
- **diffie-hellman-group14-sha1**

- **HTTP Server**

Для доступа к WBM без шифрования можно активировать или деактивировать службу HTTP Server.

- **HTTP Port**

По умолчанию установлен порт 80. В качестве опции можно задать номер порта в диапазоне 1024 ... 49151 или 49500 ... 65535.

- **HTTPS Server**

Для доступа к WBM с шифрованием можно активировать или деактивировать службу HTTPS Server.

- **HTTPS Port**

По умолчанию установлен порт 443. В качестве опции можно задать номер порта в диапазоне 1024 ... 49151 или 49500 ... 65535.

6.4 Меню «System»

- **Min. TLS Version**
Выберите в раскрывающемся списке минимальную версию TLS, которая должна использоваться для шифрования. Обмен данными с устройствами, не поддерживающими требуемую версию TLS, невозможен.
- **SMTP Client**
Активируйте или деактивируйте SMTP-клиент. Дополнительные настройки выполняются в пункте меню System > SMTP Client.
- **Syslog Client**
Активируйте или деактивируйте клиент Syslog. Дополнительные настройки выполняются в пункте меню System > Syslog Client.
- **DCP Server**
Определите возможность доступа к устройству по протоколу DCP (Discovery and Configuration Protocol):
 - «-» (деактивировано)
DCP деактивирован. Чтение и изменение параметров устройства невозможно.
 - Read/Write
DCP позволяет считывать и изменять параметры устройства.
 - Read-Only
DCP позволяет считывать, но не позволяет изменять параметры устройства.
- **Time Method**
Выберите в раскрывающемся списке настройку. Возможны следующие настройки:
 - Manual
Системное время настраивается вручную. Дополнительные настройки выполняются в пункте меню System > System Time > Manual Setting.
 - SIMATIC Time
Системное время настраивается датчиком времени SIMATIC. Дополнительные настройки выполняются в пункте меню System > System Time > SIMATIC Time Client.
 - SNTP Client
Системное время настраивается сервером SNTP. Дополнительные настройки выполняются в пункте меню System > System Time > SNTP Client.
 - NTP Client
Системное время настраивается сервером NTP. Дополнительные настройки выполняются в пункте меню System > System Time > NTP Client.
 - PTP Client(только для устройств, поддерживающих PTP)
Системное время настраивается через PTP. Дополнительные настройки выполняются в пункте меню System > System Time > PTP Client.

- **SNMP**

Выберите в раскрывающемся списке протокол. Возможны следующие настройки:

- «-» (SNMP деактивирован)
Доступ к параметрам устройства по SNMP невозможен.
- SNMPv1/v2c/v3
Доступ к параметрам устройства возможен через SNMP версий 1, 2с или 3.
Дополнительные настройки выполняются в пункте меню System > SNMP > General.
- SNMPv3
Доступ к параметрам устройства возможен только через SNMP версии 3.
Дополнительные настройки выполняются в пункте меню System > SNMP > General.

- **SNMPv1/v2 Read-Only**

Активируйте или деактивируйте доступ к переменным SNMP для записи в версии SNMPv1/v2c.

- **SINEMA Configuration Interface**

Если интерфейс конфигурации SINEMA активирован, то конфигурации можно загружать на IE-коммутатор через STEP 7 Basic / Professional.

- **ARP Keep Alive**

Активируйте или деактивируйте функцию ARP Keep Alive. При активированной функции ARP Keep Alive устройство проверяет все записи в таблице маршрутизации на предмет того, имеется ли для указанного шлюза (Next Hop) запись в таблице ARP.

- **ARP Keep Alive Interval**

Интервал в секундах, после которого выполняется циклическая проверка. При внесении сюда значения автоматически активируется поле-флажок опции ARP Keep Alive.

Диапазон значений: 30 ... 86400 секунд

По умолчанию: 30 секунд

- **Configuration Mode**

Выберите в раскрывающемся списке режим работы. Допустимы следующие режимы работы:

- Automatic Save

Работа с автоматическим сохранением. Спустя примерно 1 минуту после последнего изменения параметров или перед повторным пуском устройства конфигурация автоматически сохраняется.

Дополнительно в области индикации появляется следующее сообщение «Changes will be saved automatically in %u seconds. Press 'Write Startup Config' to save immediately.».

Примечание

Прерывание процесса сохранения

Процесс сохранения запускается только после того, как истечёт показанный в сообщении таймер. Длительность процесса сохранения зависит от устройства.

- Не выключайте устройство сразу же по истечении таймера.
-

- Trial

Пробный режим. В пробном режиме изменения записываются, однако не сохраняются в файле конфигурации (Startup Configuration).

Для сохранения изменений в файле конфигурации используйте кнопку «Write Startup Config». Дополнительно в области индикации отображается сообщение «Trial Mode Active - Press 'Write Startup Config' button to make your settings persistent», если имеются несохранённые изменения. Это сообщение будет отображаться на каждой странице WBM до тех пор, пока либо не будут сохранены выполненные изменения, либо устройство не будет перезапущено.

Примечание

В режиме конфигурации «Trial» спектр функций PROFINET IO отключён. После этого устройство больше не реагирует на запросы PROFINET, и, следовательно, контроллер не получает от устройства информацию о PROFINET.

Серверы SINEC NMS или SINEMA не могут контролировать устройство по протоколу PROFINET в режиме конфигурации Trial.

Порядок действий при конфигурации

1. Для использования желаемой функции активируйте соответствующее поле-флажок опции.
2. Выберите в раскрывающихся списках нужные опции.
3. Щёлкните кнопку «Set values».

6.4.2 General

6.4.2.1 Device

Общие сведения об устройстве

Эта страница содержит общие сведения об устройстве.

Device

Device Coordinates

Current System Time: 07/21/2015 13:06:01

System Up Time: 4h 56m 25s

Device Type: SCALANCE

System Name: sysName Not Set

System Contact: sysContact Not Set

System Location: sysLocation Not Set

Set Values Refresh

Поля Current System Time, System Up Time и Device Type изменять невозможно.

Описание

Страница содержит следующие поля:

- **Current System Time**
Отображает текущее время системы. Системное время либо настраивается пользователем, либо синхронизируется пакетом точного времени: пакет времени SINEC H1, NTP или SNTP. (доступно только для чтения)
- **System Up Time**
Отображает время работы устройства после последнего повторного пуска. (доступно только для чтения)
- **Device Type**
Отображает типовое обозначение устройства. (доступно только для чтения)
- **System Name**
Сюда можно внести название устройства. Внесённое название будет отображаться в области выбора. Максимум 255 символов.
Системное имя также отображается в запросе на ввод CLI (Prompt). В запросе на ввод CLI количество символов ограничено. Системное имя обрезается после 16 символов.

- **System Contact**
Можно указать имя контактного лица, которое несёт ответственность за управление устройством. Максимум 255 символов.
- **Device location**
Сюда можно внести место монтажа устройства. Внесённое место монтажа будет отображаться в области выбора. Максимум 255 символов.

Примечание

В полях ввода используются коды ASCII с 0x20 по 0x7e.

Порядок действий

1. Введите в поле ввода System Contact контактное лицо, несущее ответственность за устройство.
2. Введите в поле ввода Device location обозначение места монтажа устройства.
3. Введите в поле ввода System Name название устройства.
4. Щёлкните кнопку «Set values».

6.4.2.2 Coordinates

Информация о географических координатах

В окне Geographic Coordinates можно внести сведения о географических координатах. Параметры географических координат (широта и долгота в градусах, а также высота над эллипсоидом согласно WGS84) вводятся непосредственно в поля ввода в окне Geographic Coordinates.

Определение координат

Для определения географических координат устройства используйте соответствующие карты.

Географические координаты можно также определить с помощью GPS-приёмника. В большинстве своём подобные устройства сразу же демонстрируют географические координаты, их затем лишь требуется перенести в поля ввода на этой странице.

Geographic Coordinates

Device	Coordinates
Latitude: e.g. DD°MM'SS" Longitude: e.g. DDD°MM'SS" Height: e.g. dddd m	
Set Values Refresh	

Описание

Страница содержит следующие поля ввода с максимальной длиной 32 символа:

- **Поле ввода Latitude**
 Географическая широта: здесь вводится значение северной или южной широты для местоположения устройства.
 Значение +49° 1 '31,67" означает, что устройство находится на 49 градусах, 1 угловой минуте и 31,67 угловых секундах северной широты.
 При указании южной широты перед значением ставится знак минуса.
 Также к цифровому значению можно добавить буквы N (северная широта) или S (южная широта), например, 49° 1 '31,67" N.
- **Поле ввода Longitude**
 Географическая долгота: Здесь указывается значение для восточной или западной долготы местоположения устройства.
 Значение +8° 20 '58,73" означает, что устройство находится на 8 градусах, 20 угловых минутах и 58,73 угловых секундах восточной долготы.
 При указании западной широты перед значением ставится знак минуса.
 Также к цифровому значению можно добавить буквы O, E (восточная долгота) или W (западная долгота), например, 8° 20 '58,73" E.
- **Поле ввода: Height**
 Географическая высота: Здесь указывается значение для географической высоты выше или ниже стандартного нуля (уровня моря) в метрах.
 Например, 158 m означает, что устройство находится на высоте 158 м выше стандартного нуля.
 При указании значений ниже стандартного нуля (например, на Мёртвом Море) перед ними ставится знак минуса.

Порядок действий

1. Введите в поле ввода Latitude определённую широту в градусах.
2. Введите в поле ввода Longitude определённую долготу в градусах.
3. Введите в поле ввода Height определённую высоту над уровнем моря.
4. Щёлкните кнопку «Set values».

6.4.3 Agent IP

Примечание

В устройствах с несколькими IP-интерфейсами обращение к этому пункту ведёт в пункт меню Subnets > Configuration в меню Layer 3 и имеющуюся там конфигурацию интерфейса TIA.

IP Address Configuration

На этой странице WBM выполняется конфигурация IP-адреса устройства.

Описание

Страница содержит следующие поля:

- **IP Assgn. Method**
Отображает, каким образом присваивается IP-адрес.
 - Static
IP-адрес является статическим. Настройки IP вносятся в поля ввода IP Address и Subnet Mask.
 - Dynamic (DHCP)
Устройство получает динамический IP-адрес от сервера DHCP.
- **IP Address**
Введите IP-адрес устройства.
После щелчка кнопки «Set values» происходит следующее:
 - Клиент DHCP деактивируется. Активировать клиент DHCP можно на странице System > DHCP > DHCP Client.
 - IP-адрес также отображается в адресной строке интернет-браузера. Если это не происходит автоматически, потребуется вручную ввести IP-адрес в адресную строку браузера.
- **Subnet Mask**
Введите маску подсети устройства.
- **Default Gateway**
Введите IP-адрес шлюза по умолчанию, чтобы обмениваться данными с устройствами в другой подсети, например, со станциями диагностики или сервером электронной почты.

- **Agent VLAN ID**

Выберите в раскрывающемся списке VLAN ID. Можно выбирать только из уже сконфигурированных VLAN.

Примечание

Agent VLAN ID для портов кольца

Для кольцевых портов необходимо настроить Agent VLAN ID.

В режиме «802.1D Transparent Bridge» этот раскрывающийся список неактивен, см. также «Layer 2 > VLAN > General».

Примечание

Изменение Agent VLAN ID

Если ПК для конфигурирования подключён к устройству напрямую через Ethernet, то после изменения Agent VLAN-ID устройство становится более недоступно по Ethernet.

- **MAC Address**

Отображает MAC-адрес устройства. MAC-имеет привязку к аппаратному обеспечению, и изменить его невозможно.

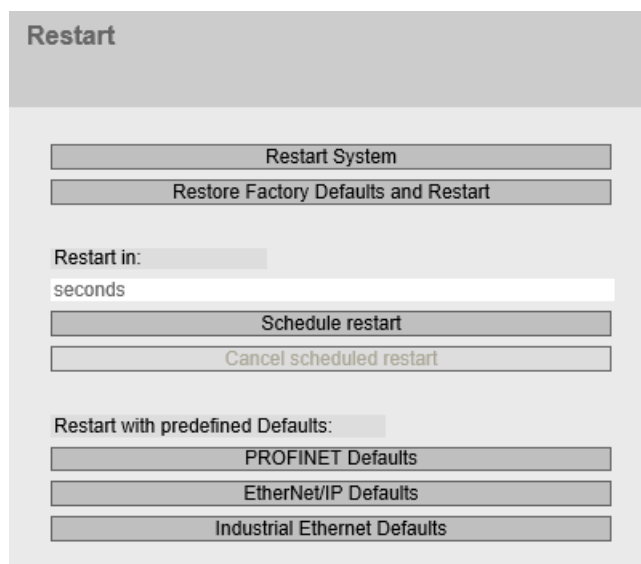
Порядок действий

1. Введите в поля ввода IP-адрес, маску подсети и шлюз по умолчанию.
2. Выберите в раскрывающемся списке «Agent VLAN ID» нужный VLAN ID.
3. Щёлкните кнопку «Set values».

6.4.4 Restart

Сброс настроек по умолчанию

В этом меню находится кнопка для повторного пуска (Restart) устройства, а также возможность сбросить устройство на заводские настройки или настройки по умолчанию различных профилей.



Restart

Restart System

Restore Factory Defaults and Restart

Restart in:
seconds

Schedule restart

Cancel scheduled restart

Restart with predefined Defaults:

PROFINET Defaults

EtherNet/IP Defaults

Industrial Ethernet Defaults

Restart

При повторном пуске устройства необходимо учитывать следующие пункты:

- Повторный пуск устройства можно выполнить только с правами администратора.
- Повторный пуск устройства разрешается выполнять только с помощью имеющихся в этом меню кнопок, а не путём выключения и включения напряжения питания устройства.
- Если устройство находится в режиме Trial, то изменения конфигурации необходимо вручную сохранить перед повторным пуском устройства. Внесённые изменения становятся активными только после щелчка кнопки «Set values» на соответствующей странице WBM устройства.
- Если устройство находится в режиме Automatic Save, то последние изменения автоматически сохраняются перед повторным пуском устройства.

Сброс на заводские настройки

При сбросе всех настроек на заводские значения также сбрасываются IP-адрес и пароли. После этого устройство доступно только через последовательный интерфейс, SINEC PNI или DHCP.

ВНИМАНИЕ

При соответствующем подключении предварительно сконфигурированное устройство может стать причиной круговых пакетов и, соответственно, отказа обмена данными.

Сброс на настройки по умолчанию (профили)

Профили содержат предварительную конфигурацию для различных вариантов применения устройства.

Если выполнить повторный пуск устройства с настройками профиля по умолчанию, то настройки сбросятся на заводские и значения некоторых параметров установятся таким образом, что они будут пригодны для определённого варианта применения. В отличие от сброса на заводские настройки, пользователи и пароли сохраняются после повторного пуска. Сконфигурированный IP-адрес утрачивается, в результате устройство становится доступным только через последовательный интерфейс, SINEC PNI или DHCP.

ВНИМАНИЕ

При соответствующем подключении предварительно сконфигурированное устройство может стать причиной круговых пакетов и, соответственно, отказа обмена данными.

То, какие настройки будут специально установлены для профиля, отображается перед повторным пуском.

Профили можно использовать независимо от заводской настройки устройства.

Описание отображаемых полей

Примечание

Учитывайте влияние отдельных функций, которые описываются в приведённых ранее разделах.

Для повторного пуска устройства предлагаются следующие возможности благодаря имеющимся на этой странице кнопкам:

- **Restart**
Для того, чтобы выполнить повторный пуск системы, щёлкните эту кнопку. Потребуется подтвердить повторный пуск в диалоговом окне. При повторном пуске устройства выполняется его повторная инициализация, внутренняя прошивка загружается заново, и устройство выполняет самодиагностику. Настройки стартовой конфигурации, например, IP-адрес устройства, сохраняются. Запрограммированные записи в таблице адресов удаляются. При повторном пуске устройства можно оставить окно браузера открытым. После повторного пуска потребуется заново авторизоваться.
- **Restore Factory Defaults and Restart**
Для того, чтобы восстановить заводские настройки устройства и выполнить его повторный пуск, щёлкните эту кнопку. Потребуется подтвердить повторный пуск в диалоговом окне.
Заводские настройки зависят от устройства.
- **Restart in:**
Введите время в секундах, по истечении которого будет выполнен повторный пуск устройства. Если активен режим конфигурации «Automatic Save», то отобразится дополнительное диалоговое окно. В этом диалоговом окне можно указать, должно ли устройство сохранить текущую конфигурацию и переключиться в режим конфигурации «Trial». В любом случае устройство перезапускается по истечении указанного времени.
- **Schedule restart**
При щелчке этой кнопки запустится таймер, который начнёт обратный отсчёт от заданного времени. Когда это время истечёт, устройство выполнит повторный пуск.
- **Cancel scheduled restart**
При щелчке этой кнопки таймер для запланированного повторного пуска (Restart) деактивируется.

Для повторного пуска устройства с предварительно заданным профилем предлагаются следующие возможности благодаря имеющимся на этой странице кнопкам:

- **PROFINET Defaults**
Чтобы восстановить заводские настройки профиля PROFINET и выполнить повторный пуск устройства, щёлкните эту кнопку. Потребуется подтвердить повторный пуск в диалоговом окне. В диалоговом окне отобразятся настройки, которые специально адаптированы для работы с протоколом PROFINET.
- **EtherNet/IP Defaults**
Для того, чтобы восстановить заводские настройки профиля EtherNet/IP и выполнить его повторный пуск, щёлкните эту кнопку. Потребуется подтвердить повторный пуск в диалоговом окне. В диалоговом окне отобразятся настройки, которые специально адаптированы для работы с протоколом EtherNet/IP.
- **Industrial Ethernet Defaults**
Для того, чтобы восстановить заводские настройки профиля Industrial Ethernet и выполнить его повторный пуск, щёлкните эту кнопку. Потребуется подтвердить повторный пуск в диалоговом окне. В диалоговом окне отобразятся настройки, которые специально адаптированы для работы с протоколом Industrial Ethernet.

6.4.5 Load&Save

Обзор типов файлов

Тип файла	Описание
Config	Этот файл содержит стартовую конфигурацию. Помимо прочего, этот файл содержит определения пользователей. Пароли сохранены в файле «Users».
ConfigPack	Подробные сведения о конфигурации, например, стартовая конфигурация, пользователи, сертификаты и избранные элементы WBM.
Debug	Этот файл содержит сведения для службы поддержки Siemens. Они зашифрованы, и их можно без риска для безопасности отправлять в службу поддержки Siemens по электронной почте.
DebugExt	Этот файл содержит более подробные сведения для службы поддержки Siemens. Они зашифрованы, и их можно без риска для безопасности отправлять в службу поддержки Siemens по электронной почте. Сохранение этих файлов может занять некоторое время.
EDS	Electronic Data Sheet (EDS) Электронный лист данных для описания устройств в режиме EtherNet/IP
Firmware	Прошивка зашифрована и закодирована. Благодаря этому гарантируется, что в устройство можно загрузить только прошивку, созданную компанией Siemens.
GSDML	Сведения PROFINET о характеристиках устройства
HTTPSCert	Предварительно настроенные сертификаты HTTPS с ключом Предварительно настроенные и автоматически созданные сертификаты HTTPS являются самоподписанными. Настоятельно рекомендуется создать и подготовить собственные сертификаты HTTPS. Рекомендуется использовать сертификаты HTTPS, подписанные надёжными сторонними или внутренними органами сертификации. Сертификат HTTPS проверяет подлинность устройства и управляет обменом зашифрованными данными. В устройство можно загружать файлы следующих типов: • .pem Для успешной загрузки сертификата HTTPS с таким типом файла в устройство сертификат должен иметь собственный незашифрованный приватный ключ. • .p12 Сертификаты HTTPS с этим типом файла имеют зашифрованный приватный ключ, который защищён паролем. Для успешной загрузки сертификата с таким типом файла в устройство необходимо сконфигурировать заданный для сертификата пароль на странице WBM System > Load&Save > Passwords. Использовать сертификаты другого формата невозможно. Рекомендуется использовать защищённые паролем сертификаты в формате PKCS#12 с длиной ключа не менее 2048 бит.
LogFile	Файл с записями из таблицы протокола событий

Тип файла	Описание
LoginWelcomeMessage	Файл с текстом для страницы авторизации. Файл может содержать не более 50 строк и 255 символов ASCII.
MIB	Файл Private MSPS MIB
RunningCLI	Текстовый файл с командами CLI Этот файл содержит обзор текущей конфигурации в форме команд CLI. Текстовый файл можно загрузить. Файл не предназначен для его повторной выгрузки без изменений.
RunningSINEMAConfig	В этом типе файла сохраняется текущая конфигурация устройства для передачи в STEP7 Basic/Professional. Файл можно импортировать в STEP7 Basic/Professional и загрузить на устройство с аналогичным артикулом и версией прошивки. Перед сохранением файла необходимо задать пароль для «RunningSINEMAConfig» в WBM в пункте меню System > Load&Save > Passwords. Этот пароль также потребуется для того, чтобы импортировать файл в STEP7 Basic/Professional. см. также «SINEMAConfig»
Script	Текстовый файл с командами CLI Файл сценария можно загрузить в устройство. Содержащиеся в файле команды CLI будут соответственно выполнены.
SINEMAConfig	С помощью файла этого типа загружаются данные конфигурации, которые были экспортированы через STEP7 Basic/Professional для передачи в WBM. Для загрузки файла потребуется задать пароль для «SINEMAConfig» в пункте меню System > Load&Save > Passwords. Этот пароль также потребуется для того, чтобы экспортировать файл из STEP7 Basic/Professional. см. также «RunningSINEMAConfig»
SSHPrivateKey	Приватный ключ SSH с максимальной длиной 4096 бит в кодировке PEM.
StartupInfo	Файл журнала пуска Этот файл содержит сообщения, зарегистрированные во время последнего пуска в журнале.
Users	Этот файл содержит сопоставление имён пользователей с соответствующими паролями.
WBMFav	Избранное WBM Этот файл содержит элементы избранного, сохранённые в WBM. Файл можно загрузить и затем выгрузить в другие устройства.

6.4.5.1 HTTP

Загрузка и сохранение данных через HTTP

WBM предлагает возможность сохранить данные устройства во внешний файл на клиентском ПК или загрузить такие данные из внешнего файла на клиентском ПК. Так, например, можно загрузить новую прошивку из файла на клиентском ПК.

Примечание

Эта страница доступна для соединений как по HTTP, так и по HTTPS.

Прошивка

Прошивка зашифрована и закодирована. Гарантируется, что в устройство можно загрузить только прошивку, созданную компанией Siemens.

Примечание

Несовместимость с предыдущими версиями прошивки со вставленным модулем PLUG или без него

Установка предыдущей версии может привести к потере данных конфигурации. В этом случае устройство выполнит повторный пуск с заводскими настройками после установки прошивки.

В этом случае, если в устройство вставлен модуль PLUG, то он после повторного пуска будет иметь статус «Not Accepted», так как на модуле PLUG будут продолжаться находиться данные конфигурации предыдущей, более актуальной версии прошивки. Благодаря этому можно будет вернуться к предыдущей, более актуальной версии прошивки без потери данных конфигурации. Если предыдущая конфигурация на PLUG более не требуется, то PLUG можно вручную удалить или заново описать на странице WBM System > PLUG.

Файлы конфигурации

Примечание

Файлы конфигурации и режим Trial/Automatic Save

В режиме «Automatic Save» выполняется автоматическое сохранение до передачи файлов конфигурации (ConfigPack и Config).

В режиме «Trial» изменения принимаются, однако не сохраняются в файлах конфигурации (ConfigPack и Config). Используйте кнопку «Write Startup Config» на странице WBM System > Configuration для сохранения изменений в файлах конфигурации.

Файл сценариев CLI

Можно загрузить существующие конфигурации CLI (RunningCLI) и выгрузить собственные сценарии CLI (Script).

Примечание

Загружаемый сценарий CLI не предназначен для его повторной выгрузки без изменений.

Обмен данными конфигурации через файл с ПО STEP7 Basic/Professional

С помощью файлов обоих типов «RunningSINEMAConfig» и «SINEMAConfig» можно обмениваться файлами конфигурации между устройством (WBM) и STEP7 Basic/Professional посредством файла.

6.4 Меню «System»

Обязательные условия:

- Одинаковый артикул
- Одинаковая версия прошивки
- Пароль
Пароль задаётся в WBM в пункте меню System > Load&Save > Passwords.

Типы файлов можно использовать следующим образом:

- Для офлайн-диагностики
Неверную конфигурацию устройства можно сохранить как «RunningSINEMAConfig» через WBM и импортировать в STEP7 Basic/Professional. Диагностика в STEP7 Basic/Professional выполняется без установления соединения с настоящим устройством. Исправленную конфигурацию можно экспортировать и вновь загрузить через WBM как «SINEMAConfig».
- Для конфигурации
Можно выполнять конфигурацию в STEP7 Basic/Professional без установления соединения с настоящим устройством. Конфигурацию можно экспортировать и вновь загрузить через WBM как «SINEMAConfig» в настоящее устройство.

Load and Save via HTTP

HTTPTFTPSFTPPasswords

Type	Description	Load	Save	Delete
Config	Startup Configuration	Load	Save	
ConfigPack	Startup Config, Users, Certificates and WBM favourites	Load	Save	
Debug	Debug Information for Siemens Support		Save	Delete
DebugExt	Extended Debug Information for Siemens Support		Save	
EDS	EtherNet/IP Device Description		Save	
Firmware	Firmware Update	Load	Save	
GSDML	PROFINET Device Description		Save	
HTTPSCert	HTTPS Certificate	Load	Save	Delete
LogFile	Event Log (ASCII)		Save	
LoginWelcomeMessage	Login Welcome Message	Load	Save	Delete
MIB	SCALANCE X200 MSPS MIB		Save	
RunningCLI	'show running-config all' CLI settings		Save	
RunningSINEMAConfig	SINEMA Running Configuration		Save	
Script	Script	Load		
SINEMAConfig	SINEMA Offline Configuration	Load		
SSHPrivateKey	SSH Private Key	Load	Save	Delete
StartupInfo	Startup Information		Save	
Users	Users and Passwords	Load	Save	
WBMFav	WBM favourite pages	Load	Save	Delete

Refresh

Описание отображаемых полей

Таблица состоит из следующих столбцов:

- **Type**
Отображает тип файла.
- **Description**
Отображает краткое описание типа файла.
- **Load**
С помощью этой кнопки можно выгрузить файлы на устройство. Кнопка активируется, если эта функция поддерживается для типа файла.
- **Save**
С помощью этой кнопки можно загрузить файлы с устройства. Кнопка активируется, если эта функция поддерживается для типа файла и файл имеется на устройстве.
- **Delete**
С помощью этой кнопки можно удалить файлы с устройства. Кнопка активируется, если эта функция поддерживается для типа файла и файл имеется на устройстве.

Примечание

После обновления прошивки очистите кэш вашего интернет-браузера.

Порядок действий при конфигурации

Выгрузка данных через HTTP

1. Запустите выгрузку данных, щёлкнув одну из кнопок «Load».
Откроется диалоговое окно для выгрузки файла.
2. Выберите нужный файл и подтвердите его выгрузку.
Файл выгружается.
3. Если требуется повторный пуск, то выдаётся соответствующее сообщение. Щёлкните кнопку «ОК», чтобы выполнить повторный пуск. При щелчке кнопки «Cancel» повторный пуск устройства выполнен не будет. Изменения вступают в силу только после повторного пуска устройства.

Загрузка данных через HTTP

1. Запустите загрузку данных, щёлкнув одну из кнопок «Save».
2. Укажите место сохранения и название файла.
3. Сохраните файл.
Файл загружается и сохраняется.

Удаление данных через HTTP

1. Запустите удаление данных, щёлкнув одну из кнопок «Delete».
Файл удаляется.

Повторное использование файлов конфигурации

Если несколько идентичных устройств должны иметь одинаковую конфигурацию, а присвоение IP-адресов выполняется через DHCP, то можно сократить затраты на новое конфигурирование с помощью сохранения и считывания данных конфигурации.

6.4 Меню «System»

Порядок действий для повторного использования файлов конфигурации:

1. Сохраните данные конфигурации сконфигурированного устройства на ПК.
2. Загрузите эти файлы конфигурации на все остальные устройства, которые требуется сконфигурировать аналогичным образом.
3. Если для отдельных устройств требуются индивидуальные настройки, то их следует выполнять в режиме онлайн на соответствующем устройстве.

Примечание

Данные конфигурации содержат контрольную сумму. При изменении этих данных их более нельзя будет выгрузить на IE-коммутатор.

6.4.5.2 TFTP

Загрузка и сохранение данных с помощью сервера TFTP

На этой странице можно сконфигурировать сервер TFTP и имена файлов. WBM предлагает возможность сохранить данные устройства во внешний файл на сервере TFTP или загрузить такие данные на устройства из внешнего файла на сервере TFTP. Так, например, можно загрузить новую прошивку из файла на сервере TFTP.

Прошивка

Прошивка зашифрована и закодирована. Гарантируется, что в устройство можно загрузить только прошивку, созданную компанией Siemens.

Примечание

Несовместимость с предыдущими версиями прошивки со вставленным модулем PLUG или без него

Установка предыдущей версии может привести к потере данных конфигурации. В этом случае устройство выполнит повторный пуск с заводскими настройками после установки прошивки.

В этом случае, если в устройство вставлен модуль PLUG, то он после повторного пуска будет иметь статус «Not Accepted», так как на модуле PLUG будут продолжаться находиться данные конфигурации предыдущей, более актуальной версии прошивки. Благодаря этому можно будет вернуться к предыдущей, более актуальной версии прошивки без потери данных конфигурации. Если предыдущая конфигурация на PLUG более не требуется, то PLUG можно вручную удалить или заново описать на странице WBM System > PLUG.

Файлы конфигурации

Примечание

Файлы конфигурации и режим Trial/Automatic Save

В режиме «Automatic Save» выполняется автоматическое сохранение до передачи файлов конфигурации (ConfigPack и Config).

В режиме «Trial» изменения принимаются, однако не сохраняются в файлах конфигурации (ConfigPack и Config). Используйте кнопку «Write Startup Config» на странице WBM System > Configuration для сохранения изменений в файлах конфигурации.

Файл сценариев CLI

Можно загрузить существующие конфигурации CLI (RunningCLI) и выгрузить собственные сценарии CLI (Script).

Примечание

Загружаемый сценарий CLI не предназначен для его повторной выгрузки без изменений.

Обмен данными конфигурации через файл с ПО STEP7 Basic/Professional

С помощью файлов обоих типов «RunningSINEMAConfig» и «SINEMAConfig» можно обмениваться файлами конфигурации между устройством (WBM) и STEP7 Basic/Professional посредством файла.

Обязательные условия:

- Одинаковый артикул
- Одинаковая версия прошивки
- Пароль
Пароль задаётся в WBM в пункте меню System > Load&Save > Passwords.

Типы файлов можно использовать следующим образом:

- Для офлайн-диагностики
Неверную конфигурацию устройства можно сохранить как «RunningSINEMAConfig» через WBM и импортировать в STEP7 Basic/Professional. Диагностика в STEP7 Basic/Professional выполняется без установления соединения с настоящим устройством. Исправленную конфигурацию можно экспортировать и вновь загрузить через WBM как «SINEMAConfig».
- Для конфигурации
Можно выполнять конфигурацию в STEP7 Basic/Professional без установления соединения с настоящим устройством. Конфигурацию можно экспортировать и вновь загрузить через WBM как «SINEMAConfig» в настоящее устройство.

6.4 Меню «System»

Load and Save via TFTP

HTTP

TFTP

SFTP

Passwords

TFTP Server Address: 0.0.0.0

TFTP Server Port: 69

Type	Description	Filename	Actions
Config	Startup Configuration	config_SCALANCE_XC200.conf	Select action ▼
ConfigPack	Startup Config, Users, Certificates and WBM favourites	configpack_SCALANCE_XC200.zip	Select action ▼
Debug	Debug Information for Siemens Support	debug_SCALANCE_XC200.bin	Select action ▼
DebugExt	Extended Debug Information for Siemens Support	DebugExt.bin	Select action ▼
EDS	EtherNet/IP Device Description	EDS_SCALANCE_X200_MSPS.zip	Select action ▼
Firmware	Firmware Update	firmware_SCALANCE_XC200.sfw	Select action ▼
GSDML	PROFINET Device Description	gsdml_SCALANCE_XC200.zip	Select action ▼
HTTPSCert	HTTPS Certificate	https_cert	Select action ▼
LogFile	Event Log (ASCII)	logfile_SCALANCE_XC200.csv	Select action ▼
LoginWelcomeMessage	Login Welcome Message	login_welcome_message.txt	Select action ▼
MIB	SCALANCE X200 MSPS MIB	scalance_x200_msp.mib	Select action ▼
RunningCLI	'show running-config all' CLI settings	RunningCLI.txt	Select action ▼
RunningSINEMAConfig	SINEMA Running Configuration	sinema_config_running.zip	Select action ▼
Script	Script	Script.txt	Select action ▼
SINEMAConfig	SINEMA Offline Configuration	sinema_config.zip	Select action ▼
SSHPrivateKey	SSH Private Key	sshprivatekey	Select action ▼
StartupInfo	Startup Information	startup_SCALANCE_XC200.log	Select action ▼
Users	Users and Passwords	users.enc	Select action ▼
WBMFav	WBM favourite pages	wbmfav.txt	Select action ▼

Set Values

Refresh

Описание отображаемых полей

Страница содержит следующие поля:

- TFTP Server Address**
Введите здесь IP-адрес сервера TFTP, с которым требуется обмен данными.
- TFTP Server Port**
Введите здесь порт сервера TFTP, через который должен осуществляться обмен данными. При необходимости можно изменить значение по умолчанию 69 в соответствии с конкретными требованиями.

Таблица состоит из следующих столбцов:

- Type**
Отображает тип файла.
- Description**
Отображает краткое описание типа файла.

- **Filename**

Для каждого типа файла здесь задаётся имя.

Примечание

Изменение имени файла

В этом столбце можно изменить предварительно заданное имя файла. После щелчка кнопки «Set values» изменённое имя файла сохраняется в устройстве, и его можно использовать в том числе и с интерфейсом командной строки.

- **Actions**

Выберите в раскрывающемся списке действие. Выбор зависит от ранее выбранного типа файла, например, файл журнала можно только сохранить.

Возможны следующие действия:

- **Save File**

При выборе этого пункта выполняется сохранение файла на сервере TFTP.

- **Load file**

При выборе этого пункта выполняется загрузка файла с сервера TFTP.

Порядок действий при конфигурации

Загрузка или сохранение данных через TFTP

1. Введите в поле ввода «TFTP Server Address» IP-адрес сервера TFTP.
2. Введите в поле ввода «TFTP Server Port» используемый порт сервера TFTP.
3. При необходимости введите в поле «Filename» имя файла, который требуется сохранить, либо данные из которого требуется принять.
4. В раскрывающемся списке «Actions» выберите действие, которое требуется выполнить.
5. Щёлкните кнопку «Set Values», чтобы запустить выбранное действие.
6. Если требуется повторный пуск, то выдаётся соответствующее сообщение. Щёлкните кнопку «OK», чтобы выполнить повторный пуск. При щелчке кнопки «Cancel» повторный пуск устройства выполнен не будет. Изменения вступают в силу только после повторного пуска устройства.

Повторное использование файлов конфигурации

Если несколько идентичных устройств должны иметь одинаковую конфигурацию, а присвоение IP-адресов выполняется через DHCP, то можно сократить затраты на новое конфигурирование с помощью сохранения и считывания данных конфигурации.

Порядок действий для повторного использования файлов конфигурации:

1. Сохраните данные конфигурации сконфигурированного устройства на ПК.
2. Загрузите эти файлы конфигурации на все остальные устройства, которые требуется сконфигурировать аналогичным образом.
3. Если для отдельных устройств требуются индивидуальные настройки, то их следует выполнять в режиме онлайн на соответствующем устройстве.

Примечание

Данные конфигурации содержат контрольную сумму. При изменении этих данных их более нельзя будет выгрузить на IE-коммутатор.

6.4.5.3 SFTP

Загрузка и сохранение данных с помощью сервера SFTP

SFTP (SSH File Transfer Protocol) передаёт файлы в зашифрованном виде. На этой странице конфигурируются реквизиты доступа для сервера SFTP.

Кроме того, WBM предлагает возможность сохранить данные устройства во внешний файл на клиентском ПК или загрузить такие данные в устройства из внешнего файла на ПК. Так, например, можно загрузить новую прошивку из файла на ПК администратора.

Кроме того, на этой странице также можно загрузить сертификаты, которые требуются для установления защищённого VPN-соединения.

Прошивка

Прошивка зашифрована и закодирована. Гарантируется, что в устройство можно загрузить только прошивку, созданную компанией Siemens.

Файлы конфигурации

Примечание

Файлы конфигурации и режим Trial/Automatic Save

В режиме «Automatic Save» выполняется автоматическое сохранение до передачи файлов конфигурации (ConfigPack и Config).

В режиме «Trial» изменения принимаются, однако не сохраняются в файлах конфигурации (ConfigPack и Config). Используйте кнопку «Write Startup Config» на странице WBM System > Configuration для сохранения изменений в файлах конфигурации.

Файл сценариев CLI

Можно загрузить существующие конфигурации CLI (RunningCLI) и выгрузить собственные сценарии CLI (Script).

Примечание

Загружаемый сценарий CLI не предназначен для его повторной выгрузки без изменений.

Команды CLI для сохранения и загрузки файлов невозможно выполнить с помощью файла сценариев CLI (Script).

Обмен данными конфигурации через файл с ПО STEP7 Basic/Professional

С помощью файлов обоих типов «RunningSINEMAConfig» и «SINEMAConfig» можно обмениваться файлами конфигурации между устройством (WBM) и STEP7 Basic/Professional посредством файла.

Обязательные условия:

- Одинаковый артикул
- Одинаковая версия прошивки
- Пароль
Пароль задаётся в WBM в пункте меню System > Load&Save > Passwords.

Типы файлов можно использовать следующим образом:

- Для офлайн-диагностики
Неверную конфигурацию устройства можно сохранить как «RunningSINEMAConfig» через WBM и импортировать в STEP7 Basic/Professional. Диагностика в STEP7 Basic/Professional выполняется без установления соединения с настоящим устройством. Исправленную конфигурацию можно экспортировать и вновь загрузить через WBM как «SINEMAConfig».
- Для конфигурации
Можно выполнять конфигурацию в STEP7 Basic/Professional без установления соединения с настоящим устройством. Конфигурацию можно экспортировать и вновь загрузить через WBM как «SINEMAConfig» в настоящее устройство.

Load and Save via SFTP

HTTP

TFTP

SFTP

Passwords

SFTP Server Address: 0.0.0.0

SFTP Server Port: 22

SFTP User:

SFTP Password:

SFTP Password Confirmation:

Type	Description	Filename	Actions
Config	Startup Configuration	config_SCALANCE_XC200.conf	Select action ▼
ConfigPack	Startup Config, Users, Certificates and WBM favourites	configpack_SCALANCE_XC200.zip	Select action ▼
Debug	Debug Information for Siemens Support	debug_SCALANCE_XC200.bin	Select action ▼
DebugExt	Extended Debug Information for Siemens Support	DebugExt.bin	Select action ▼
EDS	EtherNet/IP Device Description	EDS_SCALANCE_X200_MSPS.zip	Select action ▼
Firmware	Firmware Update	firmware_SCALANCE_XC200.sfw	Select action ▼
GSDML	PROFINET Device Description	gsdml_SCALANCE_XC200.zip	Select action ▼
HTTPSCert	HTTPS Certificate	https_cert	Select action ▼
LogFile	Event Log (ASCII)	logfile_SCALANCE_XC200.csv	Select action ▼
LoginWelcomeMessage	Login Welcome Message	login_welcome_message.txt	Select action ▼
MIB	SCALANCE X200 MSPS MIB	scalance_x200_msp.mib	Select action ▼
RunningCLI	'show running-config all' CLI settings	RunningCLI.txt	Select action ▼
RunningSINEMAConfig	SINEMA Running Configuration	sinema_config_running.zip	Select action ▼
Script	Script	Script.txt	Select action ▼
SINEMAConfig	SINEMA Offline Configuration	sinema_config.zip	Select action ▼
SSHPrivateKey	SSH Private Key	sshprivatekey	Select action ▼
StartupInfo	Startup Information	startup_SCALANCE_XC200.log	Select action ▼
Users	Users and Passwords	users.enc	Select action ▼
WBM Fav	WBM favourite pages	wbmfav.txt	Select action ▼

Set Values

Refresh

Описание

Страница содержит следующие поля:

- **SFTP Server Address**
Введите здесь IP-адрес сервера SFTP, с которым требуется обмен данными.
- **SFTP Server Port**
Введите здесь порт сервера SFTP, через который должен осуществляться обмен данными. При необходимости можно изменить значение по умолчанию 22 в соответствии с конкретными требованиями.
- **SFTP User**
Введите пользователя для доступа к серверу SFTP. Условием является наличие на SFTP-сервере пользователя с соответствующими правами.
- **SFTP Password**
Введите пароль для пользователя
- **SFTP Password Confirmation**
Подтвердите введенный пароль.

Таблица состоит из следующих столбцов:

- **Type**
Отображает тип файла.
- **Description**
Отображает краткое описание типа файла.
- **Filename**
Для каждого типа файла здесь задаётся имя.

Примечание

Изменение имени файла

В этом столбце можно изменить предварительно заданное имя файла. После щелчка кнопки «Set values» изменённое имя файла сохраняется в устройстве, и его можно использовать в том числе и с интерфейсом командной строки.

- **Actions**
Выберите в раскрывающемся списке действие. Выбор зависит от ранее выбранного типа файла, например, файл журнала можно только сохранить.
Возможны следующие действия:
 - **Save file**
При выборе этого пункта выполняется сохранение файла на SFTP-сервере.
 - **Load file**
При выборе этого пункта выполняется загрузка файла с SFTP-сервера.

Порядок действий

Загрузка или сохранение файлов через SFTP

1. Введите адрес SFTP-сервера в пункте «SFTP Server Address».
2. Введите используемый порт SFTP-сервера в пункте «SFTP Server Port».

3. Введите реквизиты пользователя (имя пользователя и пароль), которые требуются для доступа к SFTP-серверу
4. При необходимости введите в пункте «Filename» имя файла, в который вы хотите выполнить сохранение или из которого требуется скопировать данные.

Примечание

Файлы, доступ к которым защищён паролем

Для успешной загрузки этих файлов в устройство потребуется ввести заданный для файла пароль в пункте меню System > Load&Save > Passwords.

5. В раскрывающемся списке «Actions» выберите действие, которое требуется выполнить.
6. Для запуска выбранного действия щёлкните «Set values».
7. Если требуется повторный пуск, то выдаётся соответствующее сообщение. Щёлкните кнопку «ОК», чтобы выполнить повторный пуск. При щелчке кнопки «Cancel» повторный пуск устройства выполнен не будет. Изменения вступают в силу только после повторного пуска устройства.

Повторное использование файлов конфигурации

Если несколько идентичных устройств должны иметь одинаковую конфигурацию, а присвоение IP-адресов выполняется через DHCP, то можно сократить затраты на новое конфигурирование с помощью сохранения и считывания данных конфигурации.

Порядок действий для повторного использования файлов конфигурации:

1. Сохраните данные конфигурации сконфигурированного устройства на ПК.
2. Загрузите эти файлы конфигурации на все остальные устройства, которые требуется сконфигурировать аналогичным образом.
3. Если для отдельных устройств требуются индивидуальные настройки, то их следует выполнять в режиме онлайн на соответствующем устройстве.

Примечание

Данные конфигурации содержат контрольную сумму. При изменении этих данных их более нельзя будет выгрузить на IE-коммутатор.

6.4.5.4 Passwords

Имеются файлы, доступ к которым защищён паролем. Например, для возможности использования сертификата HTTPS потребуется ввести на этой странице WBM соответствующий пароль.

HTTP

TFTP

SFTP

Passwords

Type	Description	Setting	Password	Password Confirmation	Status
HTTPSCert	HTTPS Certificate	☐			-
RunningSINEMAConfig	SINEMA Running Configuration	☐			Required
SINEMAConfig	SINEMA Offline Configuration	☐			Required
SSHPrivateKey	SSH Private Key	☐			-

Set Values

Refresh

Описание

Таблица состоит из следующих столбцов:

- **Type**
Отображает тип файла.
- **Description**
Отображает краткое описание типа файла.
- **Setting**
Если этот пункт активирован, то файл используется. Можно активировать только при сконфигурированном пароле.
- **Password**
Введите здесь пароль для файла.
- **Password Confirmation**
Подтвердите введённый пароль.
- **Status**
Отображает, соответствует ли пароль файлу на устройстве.
 - valid
Поле для опции «Setting» активировано, и пароль соответствует файлу.
 - invalid
Поле для опции «Setting» активировано, однако пароль не соответствует файлу или файл ещё не загружен.
 - «-»
Пароль невозможно проанализировать, либо он ещё не используется. Поле для опции «Setting» ещё не активировано.
 - Required
Для использования указанного типа файла требуется пароль. Поле для опции «Setting» ещё не активировано.

Порядок действий

1. Введите пароль в поле «Password».
2. Для подтверждения пароля повторно введите его в поле «Password confirmation».
3. Активируйте опцию «Setting».
4. Щёлкните кнопку «Set values».

6.4.6 Events

6.4.6.1 Configuration

Выбор системных событий

На этой странице задаётся реакция устройства на системные события. Для активации или деактивации опций щёлкните соответствующие поля опций определённого столбца.

Event Configuration

Configuration

Severity Filters

Signaling Contact Method:

conventional

Signaling Contact Status:

open

	E-mail	Trap	Log Table	Syslog	Fault	Copy To Table
All Events	No Change	No Change	No Change	No Change	No Change	Copy To Table

Event	E-mail	Trap	Log Table	Syslog	Fault
Cold/Warm Start	☒	☒	☒	☒	☐
Link Change	☒	☒	☒	☒	
Authentication Failure	☒	☒	☒	☒	
RMON Alarm	☒	☒	☒	☒	
Power Change	☒	☒	☒	☒	
RM State Change	☒	☒	☒	☒	
Spanning Tree Change	☒	☒	☒	☒	
Fault State Change	☒	☒	☒	☒	
Standby State Change	☒	☒	☒	☒	
Loop Detection	☒	☒	☒	☒	
Diagnostics Alarms	☒	☒	☒	☒	
802.1X Port Authentication State Change	☒	☒	☒	☒	
PoE State Change	☒	☒	☒	☒	
FMP Status Change	☒	☒	☒	☒	
Link Check	☒	☒	☒	☒	
Secure NTP	☒	☒	☒	☒	
Configuration Change	☒	☒	☒	☒	
MRP Interconnection State Change	☒	☒	☒	☒	
Service Information	☒	☒		☒	

Set Values

Refresh

Описание отображаемых полей

Страница содержит следующие поля:

- **Signaling Contact Method**

Выберите в раскрывающемся списке реакцию сигнального контакта. Возможны следующие варианты реакции:

- Standard

Стандартная настройка для сигнального контакта. О возникшей ошибке сигнализирует светодиод ошибки, и сигнальный контакт размыкается. Если состояния ошибки больше нет, то светодиод ошибки гаснет, а сигнальный контакт замыкается.

- User Defined

Функция сигнального контакта не зависит от возникающей ошибки. Сигнальный контакт может размыкаться или замыкаться вследствие действий пользователя.

- **Signaling Contact Status**

Для изменения состояния сигнального контакта выберите в раскрывающемся списке «Signaling Contact Method» вариант реакции «User Defined».

Выберите в раскрывающемся списке состояние сигнального контакта. Доступны следующие варианты состояния:

- Closed

Сигнальный контакт замкнут.

- Open

Сигнальный контакт разомкнут.

С помощью таблицы 1 можно сразу же активировать или деактивировать все поля опций столбца таблицы 2. Таблица 1 состоит из следующих столбцов:

- **All Events**

Отображает, что настройки для всех событий таблицы 2 действительны.

- **E-Mail / Trap / Log Table / Syslog / Error**

Активируйте или деактивируйте нужный вид уведомления для всех событий. При выборе варианта «No Change» все записи соответствующего столбца в таблице 2 остаются без изменений.

- **Copy to Table**

При щелчке этой кнопки копируется настройка для всех событий таблицы 2.

Таблица 2 состоит из следующих столбцов:

- **Event**

Столбец содержит следующие значения:

- Cold/Warm Start
Устройство было включено, либо пользователь выполнил его повторный пуск. В памяти ошибок устройства сохраняется новая запись с видом выполненного повторного пуска.
- Link Change
Это событие возникает только в том случае, если статус порта контролируется и изменяется соответствующим образом, см. System > Fault Monitoring > Link Change.
- Authentication Failure
Это событие возникает при попытке доступа с неправильным паролем.
- RMON Alarm
Сигнал тревоги или событие возникло в связи с дистанционным контролем системы.
- Power Change
Это событие возникает только в том случае, если контролируются источники питания 1 и 2. Оно отображает, что произошло переключение на линию 1 или на линию 2. См. System > Fault Monitoring > Power Supply.
- RM State Change
Менеджер резервирования распознал прерывание или восстановление кольца и переключил/включил обратно участок.
- Spanning Tree Change
Топология Spanning Tree изменилась.
- Fault State Change
Статус ошибки изменился. Статус ошибки может относиться к активированному мониторингу портов, к реакции сигнального контакта или к контролю напряжения.
- Standby State Change
Устройство с установленным соединением Standby (Master или Slave) активировало или деактивировало участок сопряжения с другим кольцом (портом режима ожидания). Трафик был перенаправлен от одного соединения Ethernet (порт Standby устройства Master) к другому соединению Ethernet (порт Standby устройства Slave).
- Loop Detection
В сегменте сети обнаружена петля.
- Diagnostics Alarms
Диагностическое значение превысило определённый порог или не достигло его.
- 802.1X Port Authentication State Change
Это событие возникает при аутентификации 802.1X.
- PoE State Change
Состояние PoE изменилось.

Примечание

Это событие можно сконфигурировать только в устройствах с поддержкой PoE.

6.4 Меню «System»

- FMP State Change
Значением мощности приёма или доля падения мощности превысило определённый порог или не достигло его.

Примечание

Это событие можно сконфигурировать только в устройствах с поддержкой FMP.

- Link Check
На участке оптической передачи распознана неисправность.

Примечание

Это событие можно сконфигурировать только в устройствах с оптическими интерфейсами.

- NTP (secure)
При использовании Secure NTP возникла ошибка, например, был указан ключ с неверной длиной.
- Configuration Change
В конфигурации сохранены долговременные изменения.
- MRP Interconnection State Change
Это событие активируется, если соединение с резервированием более недоступно. При этом причиной может быть потеря как первичного, так и вторичного соединения MRP Interconnection.
- Service Information
Для определённых событий, например, сообщений о времени синхронизации времени, изменения пароля, изменения общей конфигурации, создаются записи в таблице журнала даже без конфигурации. Для этих событий можно настроить здесь последующие действия (E-Mail, Trap, Syslog).
- **E-Mail**
Устройство отправляет сообщение по электронной почте. Обязательным условием является настройка сервера SMTP и активация функции «SMTP Client».
- **Trap**
Устройство активирует ловушку SNMP. Обязательным условием является активация ловушек SNMPv1 Trap в пункте меню System > Configuration.
- **Log Table**
Устройство создаёт запись в таблице протокола событий, см. Information > Log Table
- **Syslog**
Устройство создаёт запись на сервере системного протокола. Обязательным условием является настройка сервера системного протокола и активация функции «Syslog Client».
- **Error**
Устройство активирует ошибку. Загорается светодиод ошибки.

Порядок действий при конфигурации

1. Активируйте поле опции в строке нужного события. При этом выберите событие из столбца под следующими действиями:
 - E-Mail
 - Trap
 - Log Table
 - Syslog
 - Faults
2. Щёлкните кнопку «Set values».

6.4.6.2 Severity Filter

Настройка функции Severity Filter

Настройте на этой странице ступени пороговых значений для отправки уведомлений о системных событиях.

Event Severity Filters	
Configuration Severity Filters	
Client Type	Severity
E-mail	Info
Log Table	Info
Syslog	Info

Set Values Refresh

Описание

Таблица состоит из следующих столбцов:

- **Client Type**
Выберите тип клиента, для которого выполняются настройки:
 - E-Mail
Отправка сообщений о системных событиях по электронной почте
 - Log Table
Регистрация системных событий в таблице журнала
 - Syslog
Отправка сообщений о системных событиях на сервер Syslog
- **Severity**
Выберите нужную ступень. Возможны следующие настройки:
 - Critical
Системные события обрабатываются, начиная с уровня сложности Critical.
 - Warning
Системные события обрабатываются, начиная с уровня сложности Warning.
 - Info
Системные события обрабатываются, начиная с уровня сложности Info.

Порядок действий

Для конфигурации нужной ступени выполните следующие действия:

1. Выберите нужные значения в раскрывающихся списках во втором столбце таблицы после типов клиентов.
2. Щёлкните кнопку «Set values».

6.4.7 SMTP Client

6.4.7.1 General

Контроль сети по электронной почте

При возникновении событий устройство может автоматически отправлять сообщение по электронной почте, например, технику сервисной службы. Электронное письмо содержит идентификатор устройства-отправителя, описание причины открытым текстом, а также отметку времени. Благодаря этому для сетей с небольшим количеством абонентов можно организовать простой централизованный контроль сети на основе системы электронной почты.

Simple Mail Transfer Protocol (SMTP) Client General

General Receiver

☒ SMTP Client

SMTP Server Address:

Select	Status	SMTP Server Address	Sender Address	Username	Password	Password Confirmation	Port	Security	Test	Test Result
☐	☒	192.168.16.10	Device1@auto.de				465	SSL/TLS	Test	Connection with server failed
☐	☒	192.168.16.200	Device1@auto.de				25	None	Test	
☐	☒	192.168.16.220					25	None	Test	

3 entries.

Обязательное условие для отправки сообщений электронной почты

- В пункте System > Events > Configuration для соответствующего события активирована опция «E-Mail».
- В пункте System > Events > Severity Level сконфигурирована соответствующая сложность.
- В пункте System > SMTP Client > Receiver имеется как минимум одна запись и активирована настройка «Send».

Описание

Страница содержит следующие поля:

- **SMTP Client**
Активируйте или деактивируйте SMTP-клиент.
- **SMTP Server Address**
Введите IP-адрес SMTP-сервера.

Таблица содержит следующие столбцы:

- **Select**
Активируйте поле опций в подлежащей удалению строке.
- **Status**
Задайте, используется ли этот SMTP-сервер.

6.4 Меню «System»

- **SMTP Server Address**
Отображает IP-адрес SMTP-сервера.
- **Sender Email Address**
Введите адрес электронной почты отправителя, который указывается в письме.
- **Username**
При необходимости введите имя пользователя, который используется для идентификации на SMTP-сервере.
- **Password**
При необходимости введите пароль, который используется для идентификации на SMTP-сервере.
- **Password Confirmation**
Повторите пароль.
- **Port**
Введите порт, через который доступен SMTP-сервер.
Заводская настройка:
 - 25 (нет)
 - 465 (SSL/TLS и StartTLS)
- **Security**
Определите, будет ли передача сообщения электронной почты с устройства на SMTP-сервер зашифрована. Это значит, что обязательным условием является поддержка выбранной настройки SMTP-сервером.

Примечание

Двухфакторная аутентификация (2FA)

Двухфакторная аутентификация не поддерживается.

- SSL/TLS
- StartTLS
- None: передача сообщений электронной почты не зашифровывается.
- **Test**
Сконфигурированному получателю отправляется тестовое сообщение электронной почты.
- **Test Result**
Отображает, успешно ли отправлено сообщение электронной почты или нет. Если отправка не была успешной, то сообщение содержит возможные причины.

Порядок действий

Конфигурация SMTP-сервера

1. Активируйте функцию «SMTP Client».
2. Введите IP-адрес SMTP-сервера в поле «SMTP Server Address».
3. Щёлкните кнопку «Create». В таблице создаётся новая запись.

4. Введите адрес отправителя, который указывается в письме, в поле «Sender Email Address».
5. Если SMTP-сервер требует авторизации, введите имя пользователя и пароль.
6. Определите в пункте «Security», будет ли передача сообщения электронной почты с устройства на SMTP-сервер зашифрована.
7. Активируйте запись SMTP-сервера.
8. Щёлкните кнопку «Set values».

Примечание

В зависимости от характеристик и конфигурации SMTP-сервера может потребоваться адаптировать данные, введённые в поле «Sender Email Address». Обратитесь за консультацией к администратору SMTP-сервера.

Тестирование конфигурации SMTP-сервера

1. Конфигурирование получателя
 - Щёлкните вкладку «Receiver».
 - В пункте «SMTP Server» выберите нужный SMTP-сервер.
 - В поле «SMTP Receiver Email Address» введите нужный адрес.
 - Щёлкните кнопку «Create». В таблице создаётся новая запись. По умолчанию активирована настройка «Send».
2. Отправка тестового письма электронной почты
 - Щёлкните вкладку «General».
 - Щёлкните кнопку «Test» в записи SMTP-сервера. Устройство отправляет каждому сконфигурированному получателю тестовое сообщение электронной почты.
 - Проверьте результат теста. Если отправка не была успешной, то сообщение содержит возможные причины.

6.4.7.2 Receiver

На этой странице определяется, кто получает сообщение электронной почты при наступлении события.

Simple Mail Transfer Protocol (SMTP) Client Receiver

General **Receiver**

SMTP Server: 192.168.16.10

SMTP Receiver Email Address:

Select	SMTP Server	Send	SMTP Receiver Email Address
☐	192.168.16.10	☒	service@device.de

1 entry.

Create Delete Set Values Refresh

Описание

Страница содержит следующие поля:

- **SMTP Server**
Определите, через какой SMTP-сервер будет отправляться сообщение электронной почты.
- **SMTP Receiver Email Address**
Введите адрес электронной почты, на который устройство будет отправлять сообщение электронной почты.

Таблица содержит следующие столбцы:

- **Select**
Активируйте поле опций в подлежащей удалению строке.
- **SMTP Server**
Отображает IP-адрес SMTP-сервера, к которому относится запись.
- **Send**
Если этот пункт активирован, то устройство отправляет сообщение электронной почты этому получателю.
- **SMTP Receiver Email Address**
Отображает адрес электронной почты, на который устройство отправляет сообщение электронной почты в случае ошибки.

Порядок действий

Конфигурирование получателя SMTP

1. Выберите нужный «SMTP Server».
2. Введите адрес электронной почты получателя SMTP.

3. Щёлкните кнопку «Create». В таблице создаётся новая запись.
4. Активируйте опцию «Send» для записи.
5. Щёлкните кнопку «Set values».

6.4.8 DHCP

6.4.8.1 DHCP Client

Настройка режима DHCP

Если устройство сконфигурировано как DHCP-клиент, то оно запускает запрос DHCP. В качестве ответа от DHCP-сервера устройство получает присвоенный адрес IPv4. Сервер управляет диапазоном адресов, из которого он выдаёт адреса IPv4. Также можно сконфигурировать сервер таким образом, чтобы клиент в ответ на свой запрос всегда получал один и тот же адрес IPv4.

Dynamic Host Configuration Protocol (DHCP) Client

DHCP Client	DHCP Server	Port-IP Address Mapping	Port Range	DHCP Options	Relay Agent Information	Static Leases	Host Options
-------------	-------------	-------------------------	------------	--------------	-------------------------	---------------	--------------

☐ Keep Alive
☒ DHCP Client Configuration Request (Opt.66, 67)
DHCP Mode: via MAC Address

Interface	DHCP
vlan1	☐

Set Values Refresh

Описание

Страница содержит следующие поля:

- **Keep Alive**
Если эта опция активирована, то IP-адрес сохраняется при разрыве соединения и не сбрасывается на 0.0.0.0. Функция Keep Alive активирована по умолчанию. Если функция Keep Alive деактивирована, то IP-адрес при разрыве соединения сбрасывается на 0.0.0.0.
- **DHCP Client Configuration Request (Opt. 66, 67)**
При активации этой функции DHCP-клиент использует опции для загрузки файла конфигурации (опция 67) с TFTP-сервера (опция 66). После повторного пуска устройство использует данные из файла конфигурации.
- **DHCP Mode**
Определите, с помощью какого вида идентификации DHCP-клиент авторизуется на своём DHCP-сервере:
 - via MAC Address
Идентификация выполняется по MAC-адресу.
 - via DHCP Client ID
Идентификация выполняется с помощью свободно определяемого идентификатора DHCP-клиента.
 - via System Name
Идентификация выполняется по системному имени. Если длина имени системы составляет 255 символов, то последний символ не используется для идентификации.
 - via PROFINET Name of Station
Идентификация выполняется по имени устройства PROFINET.

Таблица состоит из следующих столбцов:

- **Interface**
Интерфейс, к которому относится настройка.
- **DHCP**
Активируйте или деактивируйте DHCP-клиент для соответствующего интерфейса.

Порядок действий

Для конфигурации IP-адреса с помощью идентификатора DHCP-клиента выполните следующие действия:

1. Активируйте опцию «DHCP Client».
2. Выберите в раскрывающемся списке «DHCP Mode» режим работы DHCP «via DHCP Client ID».
3. В активированное поле ввода «DHCP Client ID» введите цепочку символов для идентификации устройства. Затем DHCP-сервер выполняет её анализ.

4. Выберите опцию «Client Configuration Request (Opt.66, 67)», если DHCP-клиент должен использовать опции 66 и 67 для того, чтобы загружать файл конфигурации и активировать его.
5. Щёлкните кнопку «Set Values».

Примечание

Если загружается файл конфигурации, то это вызывает повторный пуск системы. Помните о том, что в этом файле конфигурации опция «Client Configuration Request (Opt.66, 67)» более не активирована.

6.4.8.2 DHCP Server

Устройство можно использовать в качестве DHCP-сервера. Благодаря этому возможно автоматически присваивать IP-адреса подключённым устройствам. IP-адреса либо динамически распределяются из заданного диапазона адресов (Pool), либо определённому устройству присваивается определённый IP-адрес.

Примечание

Удаление присвоений DHCP-сервера

Если вы деактивируете или удаляете диапазон адресов IPv4, либо выключаете и вновь включаете DHCP-сервер, то присвоения DHCP-сервера удаляются, см. Information > DHCP Server.

Структура этой страницы зависит от количества интерфейсов VLAN-IP, которыми обладает устройство.

Требование

Подключённые устройства сконфигурированы таким образом, что они получают IP-адрес от DHCP-сервера.

Устройства с интерфейсом VLAN-IP

На этой странице задаются адреса IPv4, которые присваиваются через определённые порты.

Dynamic Host Configuration Protocol (DHCP) Server

DHCP Client

DHCP Server

☐ DHCP Server
☐ Probe address with ICMP Echo before offer

Select	Pool ID	Port	Enable	IP Address	Subnet Mask	Lease Time [sec]
☐	1	-	☐	0.0.0.0	0.0.0.0	3600

1 entry.

Create

Delete

Set Values

Refresh

Описание

Страница содержит следующие поля:

- DHCP Server**

Активируйте или деактивируйте DHCP-сервер на устройстве.

Примечание

Во избежание возникновения конфликтов с адресами IPv4 в сети разрешается конфигурировать лишь одно устройство в качестве DHCP-сервера.

- Probe address with ICMP Echo before offer**

Если этот пункт активирован, то DHCP-сервер проверяет, присвоен ли уже IP-адрес. Для этого DHCP-сервер отправляет сообщения ICMP Echo (Ping) на этот IPv4-адрес. Если ответ не приходит, то адрес IPv4 присваивается.

Примечание

При статических присвоениях эта проверка не выполняется.

Примечание

Если в вашей сети имеются устройства, в которых служба Echo по умолчанию деактивирована, то могут возникнуть конфликты адресов IPv4. Во избежание этого присваивайте таким устройствам адрес IPv4, который находится за пределами диапазона адресов IPv4, используемого DHCP-сервером.

Таблица состоит из следующих столбцов:

- **Select**
Установите флажок в строке, которую необходимо удалить.
- **Pool ID**
Отображает номер диапазона IPv4-адресов. При щелчке кнопки «Create» создаётся новая строка с однозначным номером (Pool ID).
- **Port**
Определите, через какой порт должны присваиваться адреса IPv4 этого диапазона DHCP.
- **Enable**
Задайте, используется ли этот адрес IPv4.

Примечание

Если вы активируете адрес IPv4, то его настройки становятся неактивными в этой вкладке DHCP, и редактировать их более невозможно.

- **IP Address**
Введите адрес IPv4, который должен присваиваться через указанный порт.
- **Subnet**
Введите маску подсети, соответствующую адресу IPv4. Используйте кодировку CIDR.
- **Lease Time [sec]**
Установите количество секунд, в течение которого адрес IPv4 остаётся действительным. По истечении половины времени срока действия DHCP-клиент может продлить действие присвоенного IPv4-адреса. По истечении всего периода действия DHCP-клиент должен запросить новый IPv4-адрес.

Устройства с несколькими интерфейсами VLAN-IP

На этой странице определяется диапазон адресов, из которого подключённое устройство получает определённый IP-адрес. Статическое присвоение IP-адресов конфигурируется в пункте «Static Leases».

Dynamic Host Configuration Protocol (DHCP) Server

DHCP Client
DHCP Server
Port-IP Address Mapping
Port Range
DHCP Options
Relay Agent Information
Static Leases
Host Options

☒ DHCP Server
☐ Probe address with ICMP Echo before offer

Select	Pool ID	Interface	Enable	Subnet	Lower IP Address	Upper IP Address	Lease Time [sec]
☐	1	vlan1	☒	192.168.16.175/32	192.168.16.175	192.168.16.175	3600

1 entry.

Create
Delete
Set Values
Refresh

Описание

Страница содержит следующие поля:

- **DHCP Server**

Активируйте или деактивируйте DHCP-сервер на устройстве.

Примечание

Во избежание возникновения конфликтов с адресами IPv4 в сети разрешается конфигурировать лишь одно устройство в качестве DHCP-сервера.

- **Probe address with ICMP Echo before offer**

Если этот пункт активирован, то DHCP-сервер проверяет, присвоен ли уже IP-адрес. Для этого DHCP-сервер отправляет сообщения ICMP Echo (Ping) на этот IPv4-адрес. Если ответ не приходит, то адрес IPv4 присваивается.

Примечание

Если в вашей сети имеются устройства, в которых служба Echo по умолчанию деактивирована, то могут возникнуть конфликты адресов IPv4. Во избежание этого присваивайте таким устройствам адрес IPv4, который находится за пределами диапазона адресов IPv4, используемого DHCP-сервером.

Таблица состоит из следующих столбцов:

- **Select**

Установите флажок в строке, которую необходимо удалить.

- **Pool ID**

Отображает номер диапазона IPv4-адресов. При щелчке кнопки «Create» создаётся новая строка с однозначным номером (Pool ID).

- **Interface**

Выберите интерфейс VLAN-IP. С помощью этого интерфейса выполняется динамическое присвоение адресов IPv4.

Обязательным условием для присвоения является нахождение адреса IPv4 интерфейса в подсети диапазона адресов IPv4. Если это не так, то интерфейс не присваивает IPv4-адреса.

- **Enable**

Задайте, используется ли этот диапазон адресов IPv4.

Примечание

Если вы активируете диапазон адресов IPv4, то его настройки становятся неактивными в этой вкладке и других вкладках DHCP, и редактировать их более невозможно.

- **Subnet**

Введите диапазон сетевых адресов, который присваивается устройствам. Используйте кодировку CIDR.

Примечание

Влияние на другие вкладки

Если сконфигурированы поля «Subnet», «Lower IP Address» и «Upper IP Address», то строка соответствующего пула DHCP на вкладке «Port-IP Address Mapping» удаляется. При удалении конфигурации строка на вкладке «Port-IP Address Mapping» становится вновь доступной.

- **Lower IP Address**

Введите адрес IPv4, который определяет начало динамического диапазона адресов IPv4. Адрес IPv4 должен находиться в пределах диапазона сетевых адресов, который сконфигурирован в пункте «Subnet».

- **Upper IP Address**

Введите адрес IPv4, который определяет окончание динамического диапазона адресов IPv4. Адрес IPv4 должен находиться в пределах диапазона сетевых адресов, который сконфигурирован в пункте «Subnet».

- **Lease Time [sec]**

Установите количество секунд, в течение которого адрес IPv4 остаётся действительным. По истечении половины времени срока действия DHCP-клиент может продлить действие присвоенного IPv4-адреса. По истечении всего периода действия DHCP-клиент должен запросить новый IPv4-адрес.

Порядок действий

Глобальная активация DHCP-сервера

1. Активируйте поле для опции «DHCP Server».
2. Щёлкните кнопку «Set values».

Конфигурация для устройств с одним интерфейсом VLAN-IP

1. Щёлкните кнопку «Create».
Создаётся новая строка с однозначным номером (Pool ID).
2. Выберите необходимый порт.
3. Введите адрес IPv4 и маску подсети.
4. Настройте время действия.
5. Щёлкните кнопку «Set values».
6. Выберите в этой вкладке поле для опции «Enable».
7. Щёлкните кнопку «Set values».

Конфигурация для устройств с несколькими интерфейсами VLAN-IP

1. Щёлкните кнопку «Create».
Создаётся новая строка с однозначным номером (Pool ID).
2. Выберите интерфейс VLAN-IP.

3. Щёлкните кнопку «Set values».

Во вкладке «Port-IP Address Mapping» создаётся новая строка для идентификатора диапазона. В столбце «Port» на выбор предлагаются все порты, которые на текущий момент относятся к выбранной VLAN.

Во вкладке «Port Range» создаётся новая строка для идентификатора диапазона. В строке активируются все порты, которые на текущий момент относятся к выбранной VLAN.

Во вкладке «DHCP Options» указываются все стандартные опции для пула.
4. Предлагаются следующие возможности конфигурирования диапазона:

Конфигурирование пула DHCP для диапазона адресов IPv4

 - Введите подсеть, верхний и нижний адреса IPv4.
 - Настройте время действия.
 - Щёлкните кнопку «Set values».

Конфигурирование пула DHCP для одного адреса IPv4

 - Переключитесь на вкладку «Port-IP Address Mapping».
 - Выберите необходимый порт.
 - Во вкладке «Port Range» теперь доступен выбранный порт.
 - Введите адрес IPv4 и маску подсети.
 - Щёлкните кнопку «Set values».
 - Во вкладке «DHCP Server» соответствующим образом заполнены поля «Subnet», «Lower IP Address» и «Upper IP Address».
 - Сконфигурируйте на вкладке «DHCP Server» время действия.
5. Выполните нужные настройки пула в остальных вкладках DHCP.

Активация пула DHCP

1. Активируйте на вкладке «DHCP Server» поле для опции «Enable».
2. Щёлкните кнопку «Set values».

Удаление пула DHCP

Примечание

Можно удалять только те записи, которые не активированы.

1. Активируйте поле для опции «Select» в подлежащей удалению строке. Повторите процедуру для всех записей, которые необходимо удалить.
 2. Щёлкните кнопку «Delete».
- Запись удаляется.

6.4.8.3 Port-IP Address Mapping

На этой странице выполняется точное присвоение определённому порту IP-адреса.

После создания пула на вкладке «DHCP Server» в таблице на этой странице создаётся новая строка. Теперь в соответствующем раскрывающемся списке выберите, какой порт присвоен этому пулу.

Конфигурация на этой странице влияет на вкладки «DHCP Server» и «Port Range».

DHCP Server Port-IP Address Mapping

DHCP Client	DHCP Client Options	DHCP Server	Port-IP Address Mapping	Port Range	DHCP Options	Relay Agent Information	Static Leases	Host Options								
			<table border="1"> <thead> <tr> <th>Pool ID</th> <th>Port</th> <th>IP Address</th> <th>Subnet Mask</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>P9.2</td> <td>192.168.16.175</td> <td>255.255.255.255</td> </tr> </tbody> </table>	Pool ID	Port	IP Address	Subnet Mask	1	P9.2	192.168.16.175	255.255.255.255					
Pool ID	Port	IP Address	Subnet Mask													
1	P9.2	192.168.16.175	255.255.255.255													

Описание

Таблица содержит следующие столбцы:

- **Pool ID**
Отображает номер диапазона IPv4-адресов. Для каждого диапазона адресов закладывается строка.
- **Port**
Выберите в раскрывающемся списке настройку. Предлагаются следующие возможности настройки:
 - Rx.y
Определите, через какой порт должны присваиваться адреса IPv4. Можно выбрать только те порты, которые находятся в соответствующей VLAN.
Если выбрать один порт, то только этот порт будет активирован на вкладке «Port Range».
 - Not selected
При этой настройке на вкладке «Port Range» не выбраны порты или выбрано более одного порта.
Если выбрать настройку «Not selected», то все порты на вкладке «Port Range» деактивируются.
- **IP Address**
Введите адрес IPv4.
Во вкладке «DHCP Server» соответствующим образом заполняются поля «Lower IP Address» и «Upper IP Address».
- **Subnet Mask**
Введите соответствующую маску подсети.
Во вкладке «DHCP Server» соответствующим образом заполняется поле «Subnet».

Порядок действий

Присвоение порта IP-адресу

1. Выберите необходимый порт.
2. Введите адрес IPv4 и маску подсети.
3. Щёлкните кнопку «Set values».
Во вкладке «Port Range» теперь для соответствующего пула DHCP активирован выбранный порт.
Во вкладке «DHCP Server» для соответствующего пула DHCP соответствующим образом заполнены поля «Subnet», «Lower IP Address» и «Upper IP Address».

6.4.8.4 Port Range

На этой странице задаются порты, через которые присваиваются адреса IPv4 выбранного диапазона адресов.

После указания диапазона адресов IPv4 на вкладке «DHCP Server» на этой вкладке создаётся новая строка и выбираются все порты, которые находятся в соответствующей VLAN на текущий момент. При последующем добавлении портов в VLAN порты в этой вкладке не активируются автоматически.

DHCP Server Port Range

DHCP Client		DHCP Client Options		DHCP Server		Port-IP Address Mapping		Port Range		DHCP Options		Relay Agent Information		Static Leases		Host Options		
Pool ID	Interface	All ports	P0.1	P0.2	P0.3	P0.4	P1.1	P1.2	P1.3	P1.4	P2.1	P2.2	P2.3	P2.4	P3.1	P3.2	P3.3	P3.4
1	vlan1	No Change	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒

Описание

Таблица содержит следующие столбцы:

- **Pool ID**
Отображает номер диапазона IPv4-адресов. Для каждого диапазона адресов закладывается строка.
- **Interface**
Отображает присвоенный IP-интерфейс.

- **All Ports**
Выберите в раскрывающемся списке настройку. Предлагаются следующие возможности настройки:
 - Enabled
Поле для опции активируется у всех портов соответствующей VLAN.
 - Disabled
Поле для опции деактивируется у всех портов соответствующей VLAN.
 - No Change
Таблица остаётся без изменений.
- **Px.y**
Определите, через какие порты должны присваиваться адреса IPv4 диапазона адресов.
Можно выбрать только те порты, которые находятся в соответствующей VLAN.

Примечание

Влияние на другие вкладки

Если вы активируете всего один порт, то этот порт выбран на вкладке «Port-IP Address Mapping».

Если вы не активируете ни один порт или более одного порта, то на вкладке «Port-IP Address Mapping» выбирается настройка «Not selected».

Порядок действий

Конфигурирование портов по отдельности

1. Активируйте поле для опций соответствующего порта.
2. Щёлкните кнопку «Set values».

Конфигурирование всех портов

1. Выберите в раскрывающемся списке «All Ports» нужную запись.
2. Щёлкните кнопку «Set values».

6.4.8.5 DHCP Options

На этой странице задаётся то, какие опции DHCP поддерживает DHCP Server. Различные опции DHCP Options определены в RFC 2132.

Опции DHCP Options 1, 3, 6, 66 и 67 задаются автоматически при создании диапазона адресов IPv4. Опции можно удалять, за исключением DHCP Option 1. В опции DHCP Option 1 автоматически настраивается маска подсети, указанной в пункте «DHCP Server» для диапазона адресов. В опции DHCP Option 3 можно с помощью поля опции настроить внутренний адрес IPv4 сервера DHCP Server как параметр DHCP.

Dynamic Host Configuration Protocol (DHCP) Options

DHCP Client | **DHCP Client Options** | **DHCP Server** | **Port-IP Address Mapping** | **Port Range** | **DHCP Options** | **Relay Agent Information** | **Static Leases** | **Host Options**

Pool ID:

Option Code:

Select	Pool ID	Option Code	Description	Use Interface IP	Value
☐	1	1	Subnet Mask	☐	255.255.255.255
☐	1	3	Router	☐	0.0.0.0
☐	1	6	Domain Name Server		0.0.0.0
☐	1	66	TFTP Server Name		
☐	1	67	Bootfile Name		Bootfile name not set

5 entries.

Описание

Страница содержит следующие поля:

- **Pool ID**
Выберите нужный диапазон IPv4-адресов.
- **Option Value**
Выберите номер нужной опции DHCP Option. Различные опции DHCP Options определены в RFC 2132. Поддерживаемые опции DHCP Options приведены в следующем абзаце.

Таблица состоит из следующих столбцов:

- **Select**
Установите флажок в строке, которую необходимо удалить.
- **Pool ID**
Отображает номер диапазона IPv4-адресов.
- **Option Value**
Отображает номер опции DHCP Option.
- **Description**
Отображает описание опции DHCP Option.

- **Use Interface IP**
При активации поля опции адрес IPv4 используется в качестве шлюза по умолчанию, который присвоен IP-интерфейсу диапазона адресов. Если поле опций деактивировано, то адрес IPv4 можно ввести.
- **Value**
Введите параметр DHCP, который передаётся DHCP-клиенту. Содержимое зависит от опции DHCP Option.
 - DHCP Option 3 (шлюз по умолчанию)
Введите параметр DHCP в качестве адреса IPv4, например, 192.168.100.2.
 - DHCP Option 6 (DNS-сервер)
Введите параметр DHCP в качестве адреса IPv4, например, 192.168.100.2. Можно ввести до трёх адресов IPv4, разделённых запятой.
 - DHCP Option 12 (имя хост-компьютера)
Введите имя хост-компьютера в формате строки.
 - DHCP Option 15 (имя домена)
Укажите имя домена, в котором находится клиент.
 - DHCP Option 66 (TFTP-сервер)
Введите параметр DHCP в качестве адреса IPv4, например, 192.168.100.2.
 - DHCP Option 67 (имя файла загрузки)
Введите имя файла загрузки в формате строки.

Поддерживаемые опции DHCP Options

Поддерживаются следующие опции DHCP:

- Опция 1
- Опция 3
- Опция 6
- Опция 12
- Опция 15
- Опция 66
- Опция 67

Порядок действий

Задание опции DHCP Option

1. Выберите Pool ID.
2. Введите значение опции.
3. Щёлкните кнопку «Create».
4. Введите значение.
5. При необходимости активируйте для опции 3 поле опции «Use Interface IP».
6. Щёлкните кнопку «Set values».

6.4 Меню «System»

Удаление опции DHCP Option

1. Активируйте поле для опции «Select» в подлежащей удалению строке. Повторите процедуру для всех записей, которые необходимо удалить.
2. Щёлкните кнопку «Delete». Запись удаляется.

6.4.8.6 Relay Agent Information

На этой странице определяется, что устройства с определённым Remote ID и Circuit ID получают IPv4-адреса из определённого диапазона адресов.

При создании такой записи для диапазона адресов порты диапазона адресов будут реагировать только на запросы DHCP через DHCP Relay Agent (опция 82). Можно создать дополнительные диапазоны адресов для одних и тех же IP-интерфейсов для того, чтобы порты реагировали на различные запросы.

Relay Agent Information

DHCP Client
DHCP Client Options
DHCP Server
Port-IP Address Mapping
Port Range
DHCP Options
Relay Agent Information
Static Leases
Host Options

Pool ID: 1
Remote ID:
Circuit ID:

Select	Pool ID	Remote ID	Circuit ID
☐	1	Switch	7

1 entry.

Create
Delete
Refresh

Описание

Страница содержит следующие поля:

- **Pool ID**
Выберите нужный диапазон IPv4-адресов.
- **Remote ID**
Введите Remote ID.
- **Circuit ID**
Введите Circuit ID.

Таблица состоит из следующих столбцов:

- **Select**
Установите флажок в строке, которую необходимо удалить.
- **Pool ID**
Отображает номер диапазона IPv4-адресов.

- **Remote ID**
Отображает Remote ID.
- **Circuit ID**
Отображает Circuit ID.

Порядок действий

Создание записи

1. Выберите Pool ID.
2. Введите Remote ID.
3. Введите Circuit ID.
4. Щёлкните кнопку «Create».

Удаление записи

1. Активируйте поле для опции «Select» в подлежащей удалению строке. Повторите процедуру для всех записей, которые необходимо удалить.
2. Щёлкните кнопку «Delete».
Запись удаляется.

6.4.8.7 Static Leases

На этой странице определяется, что DHCP-клиенту в зависимости от его идентификатора клиента или MAC-адреса присваивается заданный IPv4-адрес.

Static Leases

DHCP Client	DHCP Client Options	DHCP Server	Port-IP Address Mapping	Port Range	DHCP Options	Relay Agent Information	Static Leases	Host Options
-------------	---------------------	-------------	-------------------------	------------	--------------	-------------------------	---------------	--------------

Pool ID:

Client Identification Method:

Value:

Select	Pool ID	Identification Method	Value	IP Address	Comment
☐	1	Client ID	65756767	0.0.0.0	

1 entry.

Описание

Страница содержит следующие поля:

- **Pool ID**
Выберите нужный диапазон IPv4-адресов.
- **Client Identification Method**
Выберите метод, по которому идентифицируется клиент.
 - Ethernet MAC
Клиент идентифицируется по своему MAC-адресу.
 - Client ID
Клиент идентифицируется по свободно определяемому идентификатору DHCP-клиента.
- **Value**
Введите MAC-адрес (Ethernet MAC), идентификатор клиента (Client ID) или DUID клиента.

Таблица состоит из следующих столбцов:

- **Select**
Установите флажок в строке, которую необходимо удалить.
- **Pool ID**
Отображает номер диапазона IPv4-адресов.
- **Identification Method**
Отображает, выполняется ли идентификация клиента по MAC-адресу, идентификатору клиента или DUID.
- **Value**
Отображает MAC-адрес или идентификатор клиента.
- **IP Address**
Задайте IPv4-адрес, который будет присваиваться клиенту. IPv4-адрес должен находиться в пределах диапазона IPv4-адресов.
- **Comment**
При необходимости введите комментарий.

Порядок действий

Создание статического присвоения

1. Выберите Pool ID.
2. Выберите метод идентификации клиента (Client Identification Method).
3. Введите значение Value.
4. Щёлкните кнопку «Create».
5. Задайте IPv4-адрес, который будет присваиваться клиенту.
6. Щёлкните кнопку «Set values».

Удаление статического присвоения

1. Активируйте поле для опции «Select» в подлежащей удалению строке. Повторите процедуру для всех записей, которые необходимо удалить.
2. Щёлкните кнопку «Delete».
Запись удаляется.

6.4.8.8 Опции хоста

Для устройства, которому присвоен статический IP-адрес, на этой странице можно задать опции DHCP. С помощью опций DHCP DHCP-сервер предоставляет клиентам дополнительные параметры конфигурации.

Dynamic Host Configuration Protocol (DHCP) Host Options

DHCP Client	DHCP Client Options	DHCP Server	Port-IP Address Mapping	Port Range	DHCP Options	Relay Agent Information	Static Leases	Host Options												
Pool ID: 1 Client: Client ID: 65756767 Option Code: Host Name (12) <table border="1"> <thead> <tr> <th>Select</th> <th>Pool ID</th> <th>Identification Method</th> <th>Value</th> <th>Option Code</th> <th>Option Value</th> </tr> </thead> <tbody> <tr> <td>☐</td> <td>1</td> <td>Client ID</td> <td>65756767</td> <td>Host Name (12)</td> <td> </td> </tr> </tbody> </table> 1 entry. Create Delete Set Values Refresh									Select	Pool ID	Identification Method	Value	Option Code	Option Value	☐	1	Client ID	65756767	Host Name (12)	
Select	Pool ID	Identification Method	Value	Option Code	Option Value															
☐	1	Client ID	65756767	Host Name (12)																

Описание

Страница содержит следующие поля:

- **Pool ID**
Выберите нужный диапазон IPv4-адресов.
- **Client**
Выберите устройство, для которого требуется задать опцию DHCP.
- **Option Code**
Выберите в этом раскрывающемся списке опцию DHCP. Доступны следующие опции:
 - Host Name (12)
 - TFTP Server Name (66)
 - Bootfile Name (67)

Таблица состоит из следующих столбцов:

- **Select**
Активируйте это поле для опций, чтобы отметить строку, которую хотите удалить.
- **Pool ID**
Отображает номер диапазона IPv4-адресов.

6.4 Меню «System»

- **Identification Method**
Отображает, каким образом идентифицируется клиент. Имеются следующие возможности:
 - MAC
 - Client ID
- **Value**
Отображает значение параметра Identification Method, заданное в пункте «Static Leases».
- **Option Code**
Отображает опцию DHCP.
- **Option Value**
В зависимости от выбранного кода опции введите имя хост-компьютера, имя TFTP-сервера или загрузочного файла.

Порядок действий

Задание опции

1. Выберите Pool ID.
2. Выберите клиента.
3. Выберите параметр Option Code.
4. Щёлкните кнопку «Create». В таблице создаётся дополнительная строка.
5. В новой созданной строке введите параметр Option Value для опции DHCP.
6. Щёлкните кнопку «Set values».

Удаление опции

1. Активируйте поле для опции той строки, которую хотите удалить.
2. Щёлкните кнопку «Delete».

6.4.9 SNMP

Для этого см. также главу «Технические основы», раздел «SNMP (Страница 88)».

6.4.9.1 Общая информация

Конфигурация SNMP

Примечание

Конфигурация SNMPv3 при обновлении прошивки

Начиная с версии прошивки 6.4 (для SCALANCE XM-400 / XR-500) или начиная с версии прошивки 4.3 (для SCALANCE XB-200 / XR-300WG / XC-200 / XP-200 / XF-200BA) конфигурация SNMP распределена по нескольким страницам WBM.

Для удаления конфигурации SNMPv3 необходимо выполнить следующие действия:

1. Удалите все виды SNMPv3, за исключением предварительно заданных видов **SIMATICNETRD** и **SIMATICNETWR**.
2. Удалите все доступы SNMPv3 Access.
3. Удалите все записи в таблице «SNMPv3 User to Group mapping».
4. Удалите всех SNMPv3 User.

На этой странице можно найти все основные настройки SNMP. Активируйте опции в зависимости от функций, которые хотите использовать.

Simple Network Management Protocol (SNMP) General

General	SNMPv3 Users	SNMPv3 User to Group mapping	SNMPv3 Access	SNMPv3 Views	Notifications
----------------	--------------	------------------------------	---------------	--------------	---------------

SNMP: SNMPv1/v2c/v3 ▼

☐ SNMPv1/v2c Read Only

SNMPv1/v2c Read Community String: public

SNMPv1/v2c Read/Write Community String: private

☒ SNMPv3 User Migration

SNMP Engine ID: 80.00.10.e9.05.00.1b.1b.af.a2.00

SNMP Agent Listen Port: 161

Set Values
Refresh

Описание

Страница содержит следующие поля:

- **SNMP**
Выберите в раскрывающемся списке протокол SNMP. Возможны следующие настройки:
 - «-» (деактивировано)
SNMP деактивирован.
 - SNMPv1/v2c/v3
SNMPv1/v2c/v3 поддерживается.
-
- Примечание**
- Следует помнить о том, что SNMP версий 1 и 2с не имеет механизмов безопасности.
-
- SNMPv3
Поддерживается только SNMPv3.
- **SNMPv1/v2c Read Only**
При активации этой опции SNMPv1/v2c может получать доступ к переменным SNMP только для чтения.

Примечание

Community String

По соображениям безопасности не следует использовать значения по умолчанию «public» или «private». Измените параметры Community Strings после первой установки.

Рекомендованная минимальная длина для параметров Community String составляет 6 символов.

По соображениям безопасности при использовании SNMPv1/v2c Read Community String возможен только ограниченный доступ к объектам SNMPCommunityMIB. При использовании SNMPv1/v2c Read/Write Community String вы получите полный доступ к SNMPCommunityMIB.

- **SNMPv1/v2c Read Community String**
Введите Community String для доступа протокола SNMP только для чтения.
- **SNMPv1/v2c Read/Write Community String**
Введите Community String для доступа протокола SNMP для чтения и записи.

- **SNMPv3 User Migration**
 - **Активировано**
Если функция активирована, то генерируется идентификатор SNMP Engine, который можно использовать для миграции. Сконфигурированных пользователей SNMPv3 можно переносить на другое устройство.
Если активировать эту функцию и загрузить конфигурацию устройства на другое устройство, сконфигурированные пользователи SNMPv3 сохранятся.
 - **Disabled**
Если функция деактивирована, генерируется идентификатор SNMP Engine ID для конкретного устройства. Для генерации идентификатора используется агентский MAC-адрес устройства. Эту конфигурацию пользователей SNMP нельзя перенести на другие устройства.
Если загрузить конфигурацию устройства на другое устройство, то все сконфигурированные пользователи SNMPv3 удаляются.
- **SNMP Engine ID**
Отображает идентификатор SNMP Engine.
- **SNMP Agent Listen Port**
Задайте, на каком порте агент SNMP будет ожидать запросы SNMP. По умолчанию установлен стандартный порт 161. В качестве опции можно ввести стандартный порт 162 или номер порта в диапазоне 1024 ... 49151 или 49500 ... 65535.

Порядок действий

1. Выберите в раскрывающемся списке «SNMP» нужную опцию:
 - «-» (деактивировано)
 - SNMPv1/v2c/v3
 - SNMPv3
2. Активируйте поле для опций «SNMPv1/v2c Read Only», если доступ к переменным SNMP с использованием SNMPv1/v2c требуется только для чтения.
3. Введите в поле ввода «SNMPv1/v2c Read Community String» нужную цепочку символов.
4. Введите в поле ввода «SNMPv1/v2c Read/Write Community String» нужную цепочку символов.
5. При необходимости активируйте параметр «SNMPv3 User Migration».
6. Щёлкните кнопку «Set values».

6.4.9.2 SNMPv3 Users

Пользовательские настройки безопасности

На странице WBM можно создавать новых пользователей SNMPv3 User, изменять или удалять их. Модель безопасности на основе пользователей использует в работе концепцию имени пользователя, то есть каждому пакету присваивается код пользователя. Это имя пользователя и соответствующие настройки безопасности проверяют как отправитель, так и получатель.

Simple Network Management Protocol (SNMP) v3 Users

General | **SNMPv3 Users** | SNMPv3 User to Group mapping | SNMPv3 Access | SNMPv3 Views | Notifications

User Name:

Select	User Name	Authentication Protocol	Privacy Protocol	Authentication Password	Authentication Password Confirmation	Privacy Password	Privacy Password Confirmation
☐	Miller	MD5	DES	*****	*****	*****	*****

1 entry.

[Create](#) [Delete](#) [Set Values](#) [Refresh](#)

Описание

Страница содержит следующие поля:

- **Username**
Введите желаемое имя пользователя. После сохранения данных изменить имя более невозможно.

Таблица состоит из следующих столбцов:

- **Select**
Выберите строку, которую необходимо удалить.
- **Username**
Отображает созданного пользователя.
- **Authentication Protocol**
Задайте протокол аутентификации, для которого требуется установить пароль. Доступны следующие настройки:
 - None
 - MD5
 - SHA

- **Privacy Protocol**
Задайте протокол шифрования, для которого требуется установить пароль. Этот раскрывающийся список активируется только в том случае, если выбран протокол аутентификации.

Доступны следующие настройки:

- None
- DES
- AES

- **Authentication Password**

Введите пароль для аутентификации в первое поле ввода. Длина пароля должна составлять не менее 1 символа, но не более 32 символов.

Примечание

Длина пароля

В качестве важной меры по повышению безопасности рекомендуется задавать пароль не менее 6 символов и использовать специальные символы, прописные и строчные буквы, а также цифры.

- **Authentication Password Confirmation**

Подтвердите пароль, повторно введя его.

- **Privacy Password**

Введите пароль для шифрования. Длина пароля должна составлять не менее 1 символа, но не более 32 символов.

Примечание

Длина пароля

В качестве важной меры по повышению безопасности рекомендуется задавать пароль не менее 6 символов и использовать специальные символы, прописные и строчные буквы, а также цифры.

- **Privacy Password Confirmation**

Подтвердите пароль шифрования, повторно введя его.

Порядок действий

Создание нового пользователя

1. В поле ввода «Username» введите имя нового пользователя.
2. Щёлкните кнопку «Create». В таблице создаётся новая запись.
3. Выберите алгоритм аутентификации в пункте «Authentication Protocol». Введите пароль для аутентификации и его подтверждение в соответствующие поля ввода.
4. Выберите алгоритм в пункте «Privacy Protocol». Введите пароль для шифрования и его подтверждение в соответствующие поля ввода.
5. Щёлкните кнопку «Set values».

Удаление пользователя

1. Активируйте опцию «Select» в подлежащей удалению строке.
Повторите процедуру для всех пользователей, которых хотите удалить.
2. Щёлкните кнопку «Delete». Запись удаляется.

6.4.9.3 SNMPv3 User to Group mapping

Конфигурация участников групп

На этой странице WBM пользователи распределяются по определённым группам SNMPv3 Group. Каждый пользователь может быть участником только одной группы.

Simple Network Management Protocol (SNMP) v3 Groups

General | **SNMPv3 Users** | **SNMPv3 User to Group mapping** | SNMPv3 Access | SNMPv3 Views | Notifications

Group Name:

User Name:

Select	Group Name	User Name
☐	Service	Miller

1 entry.

Описание

Страница содержит следующие поля:

- **Group Name**
Введите группу, которая будет присвоена пользователю.
- **Username**
Выберите пользователя, который должен быть участником указанной группы.
Раскрывающийся список содержит только пользователей, которые ещё не присвоены ни одной группе.

Таблица состоит из следующих столбцов:

- **Select**
Выберите строку, которую необходимо удалить.
- **Group Name**
Отображает группу SNMPv3 Group. Имя группы впоследствии можно изменить, если для группы ещё не заданы права доступа.
- **Username**
Отображает пользователя, который является участником этой группы.

6.4.9.4 SNMPv3 Access

Настройки безопасности и выдача прав

SNMP версии 3 предлагает возможности выдачи прав, аутентификации и шифрования на уровне протокола. Уровень безопасности и права чтения/доступа задаются в зависимости от конкретных групп. Для каждого участника группы автоматически применяются соответствующие настройки.

Примечание

Группе могут быть присвоены различные полномочия доступа для различных уровней безопасности. Если для уровня безопасности не задано полномочие доступа, то участникам группы не предоставляется доступ к устройству при использовании этого уровня безопасности.

Simple Network Management Protocol (SNMP) v3 Access

General	SNMPv3 Users	SNMPv3 User to Group mapping	SNMPv3 Access	SNMPv3 Views	Notifications
---------	--------------	------------------------------	---------------	--------------	---------------

Group Name:
Security Level:

Select	Group Name	Security Level	Read View Name	Write View Name	Notify View Name
☐	Service	no Auth/no Priv	SIMATICNETRD	SIMATICNETWR	SIMATICNETRD

1 entry.

Описание

Страница содержит следующие поля:

- **Group Name**
Выберите имя для группы.
- **Security Level**
Выберите уровень безопасности (аутентификация, шифрование), для которого требуется задать полномочия для доступа:
 - **no Auth/no Priv**
Аутентификация не активирована/шифрование не активировано.
 - **Auth/no Priv**
Аутентификация активирована/шифрование не активировано.
 - **Auth/Priv**
Аутентификация активирована / шифрование активировано.

Таблица состоит из следующих столбцов:

- **Select**
Выберите строку, которую необходимо удалить.
- **Group Name**
Отображает имя группы SNMPv3 Group.
- **Security Level**
Отображает уровень безопасности, для которого действует полномочие доступа.
- **Read View Name**
Введите SNMPv3 View, который должен использоваться для доступа SNMP Access с правом чтения участниками группы с определённым уровнем безопасности.
- **Write View Name**
Введите SNMPv3 View, который должен использоваться для доступа SNMP Access с правом записи участниками группы с определённым уровнем безопасности.

Примечание

Для того, чтобы был активен доступ для записи, потребуется также активировать доступ для чтения.

- **Write View Name**
Введите SNMPv3 View, который должен использоваться для уведомления SNMP для участников группы с определённым уровнем безопасности.

Порядок действий

Создание новой группы

1. Выберите имя группы, для которой конфигурируется доступ SNMP Access.
2. Выберите в раскрывающемся списке «Security Level» нужный уровень безопасности:
3. Чтобы создать новую запись, щёлкните кнопку «Create».
4. Введите в поле «Read View Name» вид SNMPv3 View для доступа с правом чтения.
5. Введите в поле «Write View Name» вид SNMPv3 View для доступа с правом записи.
6. Введите в поле «Notification View Name» вид SNMPv3 View для уведомлений.
7. Щёлкните кнопку «Set values».

Изменение группы

Изначально присвоенное имя группы и уровень безопасности впоследствии невозможно изменить. При желании изменить имя группы или уровень безопасности потребуется удалить группу, создать её с новым именем и сконфигурировать её.

Удаление группы

1. Активируйте поле опций «Select» в подлежащей удалению строке.
Повторите процесс для всех групп, которые хотите удалить.
2. Щёлкните кнопку «Delete». Записи удаляются.

6.4.9.5 SNMPv3 Views

Конфигурация видов SNMPv3

На этой странице WBM конфигурируются параметры видов SNMP View.

Simple Network Management Protocol (SNMP) v3 Views

General
SNMPv3 Users
SNMPv3 User to Group mapping
SNMPv3 Access
SNMPv3 Views
Notifications

View Name:
MIB Tree:

Select	View Name	MIB Tree	View Type
☐	MY_RD	org	Included
☐	MY_RD	private	Included
☐	MY_WR	1.3.6.1.3.6.18.1.1.1.83.73.77	Included
☐	SIMATICNETRD	iso	Included
☐	SIMATICNETRD	1.3.6.1.6.3.18.1.1	Excluded
☐	SIMATICNETRD	1.3.6.1.6.3.18.1.1.1.1.83.73.77.65.84.73.67.78.69.84.82.68	Included
☐	SIMATICNETWR	iso	Included

7 entries.

Create
Delete
Set Values
Refresh

Примечание

Управление доступами SNMPv1 и SNMPv2c

Предварительно сконфигурированные виды **SIMATICNETRD** и **SIMATICNETWR** используются внутри системы для управления доступом SNMPv1 и SNMPv2c. Удаление или изменение этих видов напрямую влияет на доступы SNMPv1 и SNMPv2c.

Описание

Страница содержит следующие поля:

- **View Name**
Выберите имя вида, который требуется сконфигурировать. Вид SNMPv3 View должен быть всегда присвоен определённому доступу SNMPv3 Access. Поэтому потребуется внести новый вид SNMPv3 View в таблице на вкладке «SNMPv3 Access».
- **MIB Tree**
Выберите Object Identifier (OID) области MIB, который требуется использовать для вида SNMPv3 View. Имеются следующие возможности:
 - iso
 - std
 - member-body
 - org
 - mgmt
 - private
 - snmpV2

В раскрывающемся списке содержатся только OID, которые используются чаще всего. Если требуется конфигурация определённого OID, не приведённого в списке, то его можно сконфигурировать через CLI командой `snmp view`. Этот OID затем также отображается в WBM в обзорной таблице.

Таблица состоит из следующих столбцов:

- **Select**
Выберите строку, которую необходимо удалить.
- **View Name**
Имя вида SNMPv3 View.
- **MIB Tree**
OID области MIB для вида SNMPv3 View.
- **View Type**
Имеются следующие возможности:
 - **Included**
MIB-OID и его подчинённые узлы являются частью SNMPv3 View. Возможен доступ к соответствующим объектам MIB.
 - **Excluded**
MIB-OID и его подчинённые узлы не являются частью SNMPv3 View. Доступ к соответствующим объектам MIB невозможен.

6.4.9.6 Notifications

Ловушки SNMP и SNMPv3-уведомления

При наступлении события устройство может одновременно направлять SNMP-уведомления (ловушки и информационные уведомления) до десяти различных станций управления. Уведомления отправляются только для тех событий, которые заданы в пункте «Events».

Simple Network Management Protocol (SNMP) Notifications

General | **SNMPv3 Users** | SNMPv3 User to Group mapping | SNMPv3 Access | SNMPv3 Views | Notifications

☐ SNMPv1 Traps

SNMPv1/v2c Trap Community String: public

SNMPv3 Notify User: -

SNMPv3 Notify Security Level: no Auth/no Priv

Notification Receiver Type: SNMPv1 Trap

Notification Receiver Address:

Select	Notification Receiver Address	Notification Receiver Type	SNMP Engine ID	Notification
☐	192.168.178.107	SNMPv1 Trap	-	☐

1 entry.

Create Delete Set Values Refresh

Описание

Страница содержит следующие поля:

- **SNMPv1 Traps**
Активируйте или деактивируйте отправку ловушек SNMPv1. Эта настройка относится ко всем получателям ловушек SNMPv1 и не влияет на получателей уведомлений SNMPv2c или SNMPv3.
- **SNMPv1/v2c Trap Community String**
Введите Community String для отправки уведомлений SNMPv1/v2c.
- **SNMPv3 Notify User**
Выберите, каким пользователям должны направляться уведомления SNMPv3.
- **SNMPv3 Notify Security Level**
Выберите уровень безопасности (аутентификация, уведомление), которое требуется использовать для уведомления SNMPv3. Имеются следующие возможности:
 - No Auth/No Priv
Аутентификация не активирована / шифрование не активировано.
 - Auth/No Priv
Аутентификация активирована / шифрование не активировано.
 - Auth/Priv
Аутентификация активирована / шифрование активировано.

- **Notification Receiver Type**
Тип получателя определяет версию SNMP и вид уведомления. Информационные уведомления SNMP требуют квитирования получателем, а SNMP-ловушки нет. Имеются следующие возможности:
 - SNMPv1 Trap
 - SNMPv2c Trap
 - SNMPv2c Inform
 - SNMPv3 Trap
 - SNMPv3 Inform
- **Notification Receiver Address**
Введите IP-адрес станции-получателя, на который устройство будет отправлять уведомления SNMP. Можно указать до десяти получателей.

Таблица состоит из следующих столбцов:

- **Select**
Выберите строку, которую необходимо удалить.
- **Notification Receiver Address**
При необходимости измените IP-адрес станций.
- **Notification Receiver Type**
Отображает указанный тип получателя.
- **SNMP Engine ID**
Идентификатор SNMP-Engine, которому направляются информационные уведомления SNMPv3. Этот параметр можно сконфигурировать только для типа получателя «SNMPv3 Inform».
- **Notification**
Активируйте или деактивируйте отправку уведомлений SNMP. Указанные, но не выбранные станции не получают уведомлений SNMP.

Примечание

Если строка таблицы отмечена серым, то соответствующее уведомление было сконфигурировано через CLI, и удалить его можно также через CLI.

Порядок действий

Конфигурирование уведомления

1. В раскрывающемся списке «SNMPv3 Notify User» выберите получателя уведомлений SNMPv3.
2. В раскрывающемся списке «SNMPv3 Notify Security Level» выберите уровень безопасности для уведомлений SNMPv3.
3. В раскрывающемся списке «Notification Receiver Type» выберите тип получателя.
4. В пункте Notification Receiver Address введите IP-адрес станции-получателя, на который устройство будет отправлять ловушки или уведомления.
5. Чтобы создать новую запись ловушки, щёлкните кнопку «Create».

6. Активируйте в нужной строке «Notification».
7. Щёлкните кнопку «Set values».

Удаление записи ловушки

1. Активируйте «Select» в подлежащей удалению строке.
2. Щёлкните кнопку «Delete». Запись удаляется.

6.4.10 System Time

Для настройки системного времени имеются следующее время. Единоновременно может быть активен только один метод.

При активации того или иного метода автоматически деактивируется последний выбранный метод.

6.4.10.1 Manual Setting

Ручная настройка системного времени

На этой странице можно самостоятельно настроить дату и время системы. Для использования этой настройки потребуется активировать опцию «Time Manually».

Описание

Страница содержит следующие поля:

- **Time Manually**
Активируйте настройку времени ручную. При активации этой опции поле ввода «System Time» становится редактируемым.
- **System Time**
Введите дату и время в формате «ММ/ДД/ГГГГ ЧЧ:ММ:СС». После повторного пуска отсчёт времени начинается с 01/01/2000 00:00:00.

6.4 Меню «System»

- **Use PC Time**
Щёлкните кнопку, чтобы использовать настройку времени компьютера.
- **Last Synchronization Time**
Отображает, когда выполнялась последняя синхронизация времени. Если синхронизация времени невозможна, то в поле будет указано «Date/time not set».
- **Last Synchronization Mechanism**
Отображает, каким образом была выполнена последняя синхронизация времени.
 - Not set
Время не настроено.
 - Manual
Ручная настройка времени
 - SNTP
Автоматическая синхронизация времени по SNTP
 - NTP
Автоматическая синхронизация времени по NTP
 - SIMATIC
Автоматическая синхронизация времени с помощью пакета времени SIMATIC
 - PTP (только в устройствах, которые поддерживают PTP)
Автоматическая синхронизация времени по PTP
- **Daylight Saving Time**
Отображает, активирована ли перенастройка на летнее время.
 - active (offset +1 h)
Система была перенастроена на летнее время, то есть добавляется один час. Текущее системное время можно увидеть справа вверху в области выбора WBM. В поле «System Time» отображается текущее время, включая летнее время.
 - inactive (offset +0 h)
Текущее системное время не изменяется.

Порядок действий

1. Активируйте опцию «Time Manually».
2. Введите в поле ввода «System Time» дату и время в формате «ММ/ДД/ГГГГ ЧЧ:ММ:СС».
3. Щёлкните кнопку «Set values». Дата и время сохраняются, а в поле «Last Synchronization Mechanism» появится надпись «Manual».

6.4.10.2 DST Overview

На этой странице можно создавать новые записи для перенастройки летнего времени. В таблице приводится обзор существующих записей.

Настройки

Daylight Saving Time (DST) Overview

Manual Setting	DST Overview	DST Configuration	SNTP Client	NTP Client	SIMATIC Time Client	PTP Client			
Select	DST No▲	Name	Year	Start Date	End Date	Recurring Date		State	Type
☐	1	CEST	-	03/31 02:00	10/27 03:00	Last Sunday March 02 Last Sunday October 03		enabled	Recurring
☐	2	DST 2017	2017	03/30 02:00	11/15 03:00	-		enabled	Date

2 entries.

Create

Delete

Refresh

- **Select**
Выберите строку, которую необходимо удалить.
- **DST No**
Отображает номер записи.
Если создать новую запись, то создаётся новая строка с однозначным номером.
- **Name**
Отображает имя записи.
- **Year**
Отображает год, для которого создана запись.
- **Start Date**
Отображает месяц, день и время суток для начала зимнего времени.
- **End Date**
Отображает месяц, день и время суток для окончания зимнего времени.
- **Recurring Date**
В случае записи типа «Recurring» отображается период времени, состоящий из недели, дня, месяца и времени суток, в течение которого активно значение летнего времени.
В случае записи типа «Date» отображается «-».
- **Status**
Отображает статус записи:
 - Enabled
Запись создана правильно.
 - Invalid
Запись создана заново, и даты начала и окончания идентичны.
- **Type**
Отображает, каким образом выполняется переход на летнее время:
 - Date
Для перехода на летнее время указана фиксированная дата.
 - Recurring
Для перехода на летнее время задано правило.

Порядок действий

Создание записи

1. Щёлкните кнопку «Create».
В таблице создаётся новая запись.
2. В столбце «DST No» щёлкните нужную запись.
Вы перейдёте на страницу «DST Configuration».
3. Выберите в раскрывающемся списке «Type» нужный тип.
В зависимости от выбранного типа вам предлагаются различные настройки.
4. Введите имя в поле «Name».
5. При выборе типа «Date» потребуется заполнить следующие поля:
 - Год
 - День (для даты начала и окончания)
 - Час (для даты начала и окончания)
 - Месяц (для даты начала и окончания)
6. При выборе типа «Recurring» потребуется заполнить следующие поля:
 - Час (для даты начала и окончания)
 - Месяц (для даты начала и окончания)
 - Неделя (для даты начала и окончания)
 - День (для даты начала и окончания)
7. Щёлкните кнопку «Set values».

Удаление записи

1. Активируйте «Select» в подлежащей удалению строке.
2. Щёлкните кнопку «Delete». Запись удаляется.

6.4.10.3 DST Configuration

На этой странице можно конфигурировать записи для перехода на летнее время. Благодаря переходу на летнее или зимнее время системное время будет правильно настроено на местный часовой пояс.

Для перехода на летнее время можно задать правило или установить фиксированную дату.

Настройки

Примечание

Содержимое этой страницы зависит от того, что выбрано в поле «Type».

Поля «DST No», «Type» и «Name» отображаются всегда.

- **DST No**
Выберите номер записи.
- **Type**
Выберите, каким образом должен выполняться переход на летнее время:
 - Date
Можно указать фиксированную дату для перехода на летнее время.
Эта настройка подходит для регионов, в которых переход на летнее время не следует правилам.
 - Recurring
Можно задать правило для перехода на летнее время.
Эта настройка подходит для регионов, в которых летнее время всегда начинается или заканчивается в определенный день недели.
- **Name**
Введите имя для записи.
Длина имени может составлять не более 16 символов.

Настройки при выборе «Date»

DST Configuration

Manual Setting	DST Overview	DST Configuration	SNTP Client	NTP Client	SIMATIC Time Client	PTP Client
----------------	--------------	-------------------	-------------	------------	---------------------	------------

DST No: 2

Type: Date

Name: DST 2017

Year: 2017

Start Date	End Date
Day: 30 v	Day: 15 v
Hour: 02:00 v	Hour: 03:00 v
Month: March v	Month: November v

Для начала и окончания летнего времени можно указать фиксированные даты.

- **Year**
Введите год для перехода на летнее время.
- **Start Date**
Введите следующие значения для начала летнего времени:
 - Day
Укажите день.
 - Hour
Укажите час.
 - Month
Укажите месяц.
- **End Date**
Введите следующие значения для окончания летнего времени:
 - Day
Укажите день.
 - Hour
Укажите час.
 - Month
Укажите месяц.

Настройки при выборе «Recurring»

DST Configuration

Manual Setting	DST Overview	DST Configuration	SNTP Client	NTP Client	SIMATIC Time Client	PTP Client
----------------	--------------	-------------------	-------------	------------	---------------------	------------

DST No: 1 ▼

Type: Recurring ▼

Name: CEST

Start Date

Hour: 02:00 ▼

Month: March ▼

Week: Last ▼

Day: Sunday ▼

End Date

Hour: 03:00 ▼

Month: October ▼

Week: Last ▼

Day: Sunday ▼

Set Values
Refresh

Можно создать правило для перехода на летнее время.

- **Start Date**

Введите следующие значения для начала летнего времени:

- Hour
Укажите час.
- Month
Укажите месяц.
- Week
Укажите неделю.
Можно выбрать с первой по пятую недели, либо последнюю неделю месяца.
- Day
Укажите день недели.

- **End Date**

Введите следующие значения для окончания летнего времени:

- Hour
Укажите час.
- Month
Укажите месяц.
- Week
Укажите неделю.
Можно выбрать с первой по пятую недели, либо последнюю неделю месяца.
- Day
Укажите день недели.

6.4.10.4 SNTP Client

Синхронизация времени в сети

Протокол SNTP (Simple Network Time Protocol) предназначен для синхронизации времени в сети. Соответствующие пакеты отправляются в сеть с SNTP-сервера.

Примечание

Во избежание скачков времени убедитесь, что в сети имеется только один сервер времени.

Simple Network Time Protocol (SNTP) Client

Manual Setting
DST Overview
DST Configuration
SNTP Client
NTP Client
SIMATIC Time Client
NTP Server

☒ SNTP Client

Current System Time: 07/21/2021 14:42:16

Last Synchronization Time: 07/21/2021 14:41:49

Last Synchronization Mechanism: Manual

Time Zone: +00:00

Daylight Saving Time: inactive (offset + 0h)

SNTP Mode: Poll

Poll Interval[s]: 64

SNTP Server Address:

Select	SNTP Server Address	SNTP Server Port	Primary
☐	192.168.16.200	123	☒

1 entry.

Create Delete Set Values Refresh

Описание

Страница содержит следующие поля:

- **SNTP Client**
Активируйте или деактивируйте автоматическую синхронизацию времени по SNTP.
- **Current System Time**
Отображает текущую дату и текущее стандартное время, которые были получены от сервера. При указании часового пояса индикация времени корректируется соответствующим образом.
- **Last Synchronization Time**
Отображает, когда выполнялась последняя синхронизация времени.

- **Last Synchronization Mechanism**
Отображает, каким образом была выполнена последняя синхронизация времени. Доступны следующие типы:
 - Not set
Время не настроено.
 - Manual
Ручная настройка времени
 - SNTP
Автоматическая синхронизация времени по SNTP
 - NTP
Автоматическая синхронизация времени по NTP
 - SIMATIC
Автоматическая синхронизация времени с помощью пакета времени SIMATIC
 - PTP (только в устройствах, которые поддерживают PTP)
Автоматическая синхронизация времени по PTP
- **Time Zone**
Введите в этом поле используемый часовой пояс в формате «+/- ЧЧ:ММ». Часовой пояс указывается по стандартному всемирному времени UTC. Индикация времени в поле «Current System Time» корректируется соответствующим образом.
- **Daylight Saving Time**
Отображает, активирована ли перенастройка на летнее время.
 - active (offset +1 h)
Система была перенастроена на летнее время, то есть добавляется один час. Текущее системное время можно увидеть справа сверху в области выбора WBM. В поле «Current System Time» далее отображается стандартное время, включая часовой пояс.
 - inactive (offset +0 h)
Текущее системное время не изменяется.
- **SNTP Mode**
Выберите в раскрывающемся списке вид синхронизации. Возможны следующие типы синхронизации:
 - Listen
В этом режиме устройство является пассивным и принимает SNTP-пакеты, которые передают время. Настройки в полях ввода «SNTP Server Address» и «SNTP Server Port» в этом режиме влияния не имеют.
 - Poll
При выборе этого режима появляется поле ввода «Poll Intervall[s]» для дальнейшей конфигурации. Настройки в полях ввода «SNTP Server Address» и «SNTP Server Port» в этом режиме учитываются. В этом типе синхронизации устройство находится в активном состоянии и отправляет запрос времени на SNTP-сервер.
- **SNTP Server Address**
Введите IPv4-адрес SNTP-сервера.

- **SNTP Server Port**
Введите порт SNTP-сервера.
Можно выбрать следующие порты:
 - 123 (порт по умолчанию)
 - от 1025 до 36564
- **Poll Interval[s]**
Введите промежуток времени между двумя запросами времени. В этом поле указывается интервал опроса в секундах. Можно установить значения от 16 до 16284 секунд.

Порядок действий

1. Установите галочку в поле опции «SNTP Client», чтобы активировать автоматическую настройку времени.
2. В поле ввода «Time Zone» укажите местную разницу с мировым временем (UTC). Значение вводится в формате «+/-ЧЧ:ММ» (например, +02:00 для MESZ, центрально-европейского летнего времени), так как SNTP-сервер всегда отправляет время в формате UTC. Затем с помощью указания временной зоны это время пересчитывается в локальное время. В устройстве не производится перевод часов на летнее или зимнее время. Это также следует учитывать при вводе данных в поле ввода «Time Zone».
3. В раскрывающемся списке «SNTP Mode» можно выбрать следующие опции:
 - Listen
Для этого режима работы потребуется сконфигурировать следующее:
 - разница со временем, отправляемым сервером (этап 2)
 - Завершите конфигурацию на этапе 7.
 - Poll
Щёлкните кнопку «Set values». Отобразятся дополнительные поля для конфигурирования режима SNTP «Poll».
 Для этого режима работы потребуется сконфигурировать следующее:
 - разница со временем, отправляемым сервером (этап 2)
 - сервер времени (этап 4)
 - порт (этап 5)
 - интервал опроса (этап 6)
 - Завершите конфигурацию на этапе 7.
4. Введите в поле ввода «SNTP Server Address» IPv4-адрес SNTP-сервера, пакеты которого требуется использовать для синхронизации времени.
5. Введите в поле ввода «SNTP Server Port» порт, через который доступен SNTP-сервер. Порт можно использовать только в том случае, если указан IPv4-адрес SNTP-сервера.
6. Введите в поле ввода «Poll Interval[s]» интервал времени в секундах, по истечении которого требуется активировать новый запрос времени у сервера времени.
7. Щёлкните кнопку «Set values», чтобы сохранить изменения в устройстве.

6.4.10.5 NTP Client

Автоматическая настройка времени по NTP

Если синхронизация времени должна выполняться по протоколу NTP, то здесь можно выполнить соответствующие настройки.

Примечание

Во избежание скачков времени убедитесь, что в сети имеется только один сервер времени.

Network Time Protocol (NTP) Client

Manual Setting | DST Overview | DST Configuration | SNTP Client | **NTP Client** | SIMATIC Time Client | PTP Client

☐ NTP Client
☐ Secure NTP Client only

Current System Time: 08/16/2019 14:25:44

Last Synchronization Time: 08/15/2019 14:30:41

Last Synchronization Mechanism: Manual

Time Zone: +00:00

Daylight Saving Time: active (offset + 1h)

NTP Server Index: 1 ▼

Select	NTP Server Index	NTP Server Address	NTP Server Port	Poll Interval	Key ID	Hash Algorithm	Key	Key Confirmation
☐	1	192.168.1.250	123	64	1	DES		

1 entry.

Create Delete Set Values Refresh

Описание

Страница содержит следующие поля:

- NTP Client**
 Если этот пункт активирован, то устройство получает значение системного времени от NTP-сервера.
- Secure NTP Client only**
 Если этот пункт активирован, то устройство получает значение системного времени от защищённого NTP-сервера. Настройка применяется для всех записей сервера. Для активации защищённого NTP-клиента сконфигурируйте параметры для аутентификации (идентификатор ключа, алгоритм хеширования, ключ).
- Current System Time**
 Отображает текущую дату и текущее стандартное время, которые были получены от IE-коммутатора. При указании часового пояса индикация времени корректируется соответствующим образом.
- Last Synchronization Time**
 Отображает, когда выполнялась последняя синхронизация времени.

- **Last Synchronization Mechanism**
Отображает, каким образом была выполнена последняя синхронизация времени. Доступны следующие типы:
 - Not set
Время не настроено.
 - Manual
Ручная настройка времени
 - SNTP
Автоматическая синхронизация времени по SNTP
 - NTP
Автоматическая синхронизация времени по NTP
 - SIMATIC
Автоматическая синхронизация времени с помощью пакета времени SIMATIC
 - PTP (только в устройствах, которые поддерживают PTP)
Автоматическая синхронизация времени по PTP
- **Time Zone**
Введите в этом поле используемый часовой пояс в формате «+/- ЧЧ:ММ». Часовой пояс указывается по стандартному всемирному времени UTC. Индикация времени в поле «Current System Time» корректируется соответствующим образом.
- **Daylight Saving Time**
Отображает, активирована ли перенастройка на летнее время.
 - active (offset +1 h)
Система была перенастроена на летнее время, то есть добавляется один час. Текущее системное время можно увидеть справа вверху в области выбора WBM. В поле «Current System Time» далее отображается стандартное время, включая часовой пояс.
 - inactive (offset +0 h)
Текущее системное время не изменяется.
- **NTP Server Index**
Выберите индекс NTP-сервера. Можно сконфигурировать до четырёх NTP-серверов или SecureNTP-серверов. NTP-серверы опрашиваются в порядке индекса NTP-серверов. Применяется время первого найденного сервера. Если от NTP-сервера принимаются временные пакеты с меньшим значением яруса (stratum), то принимается это время. Переход на время с более низким значением яруса (stratum) занимает около 30 минут.

Таблица состоит из следующих столбцов:

- **Select**
Активируйте поле опций в подлежащей удалению строке.
- **NTP Server Index**
Индекс NTP-сервера.
- **NTP Server Address**
Введите IPv4-адрес NTP-сервера.

- **NTP Server Port**
Введите порт NTP-сервера.
Доступны следующие порты:
 - 123 (порт по умолчанию)
 - от 1025 до 36564
- **Poll Interval[s]**
Укажите промежуток времени между двумя запросами времени. Возможные значения: от 64 до 1024 секунд.

Следующие поля имеют значение только для защищённого NTP-клиента. Если поле опции «Secure NTP Client only» не активировано, то эти поля становятся неактивными:

- **Key ID**
Введите идентификатор ключа аутентификации.
- **Hash Algorithm**
Задайте формат ключа аутентификации.
- **Key**
Введите ключ аутентификации.
- **Key Confirmation**
Введите ключ аутентификации повторно для его подтверждения.

Порядок действий

Синхронизация времени через NTP-сервер

1. Установите галочку в поле опции «NTP Client», чтобы активировать автоматическую настройку времени по NTP.
2. В поле ввода «Time Zone» укажите местную разницу с мировым временем (UTC). Значение вводится в формате «+/-ЧЧ:ММ», так как NTP-сервер всегда отправляет время в формате UTC, например, +02:00 для MESZ, центрально-европейского летнего времени. Это время пересчитывается на локальное с помощью данных, указанных для часового пояса.
3. Выберите «NTP Server Index».
4. Щёлкните кнопку «Create».
В таблице создаётся строка для NTP-сервера.
5. Введите в «NTP Server Address» адрес NTP-сервера, пакеты которого требуется использовать для синхронизации времени.
6. Введите в «NTP Server Port» порт, через который доступен NTP-сервер. Порт можно изменять только в том случае, если указан адрес NTP-сервера.
7. Введите в столбце «Poll Interval» интервал времени в секундах, по истечении которого требуется активировать новый запрос времени у сервера времени.
8. Щёлкните кнопку «Set values».

Синхронизация времени через защищённый NTP-сервер

6.4 Меню «System»

Для синхронизации времени с помощью защищённого NTP-сервера потребуются следующие дополнительные шаги:

1. Установите галочку в поле опции «Secure NTP Client only», чтобы активировать автоматическую настройку времени по защищённому протоколу NTP.
2. Сконфигурируйте аутентификацию.
 - В поле «Key ID» введите идентификатор ключа аутентификации.
 - В поле «Hash Algorithm» выберите соответствующий формат.
 - В поле «Key» введите ключ аутентификации.

С помощью этих реквизитов выполняется аутентификация NTP-клиента на защищённом NTP-сервере. На защищённом NTP-сервере эти реквизиты должны быть в наличии.

3. Щёлкните кнопку «Set values».

6.4.10.6 SIMATIC Time Client

Настройка времени с помощью SIMATIC Time Client

Примечание

Во избежание скачков времени убедитесь, что в сети имеется только один сервер времени.

Описание

Страница содержит следующие поля:

- **SIMATIC Time Client**
Отметьте это поле опции для того, чтобы активировать устройство как SIMATIC Time Client.
- **Current System Time**
Отображает текущее системное время.

- **Last Synchronization Time**
Отображает, когда выполнялась последняя синхронизация времени.
- **Last Synchronization Mechanism**
Отображает, каким образом была выполнена последняя синхронизация времени.
Доступны следующие типы:
 - Not set
Время не настроено.
 - Manual
Ручная настройка времени
 - SNTP
Автоматическая синхронизация времени по SNTP
 - NTP
Автоматическая синхронизация времени по NTP
 - SIMATIC
Автоматическая синхронизация времени с помощью пакета времени SIMATIC
 - PTP (только в устройствах, которые поддерживают PTP)
Автоматическая синхронизация времени по PTP

Порядок действий

1. Установите галочку в поле опции «SIMATIC Time Client», чтобы активировать SIMATIC Time Client.
2. Щёлкните кнопку «Set values».

6.4.10.7 PTP-Client

Автоматическая синхронизация времени по PTP

На этой странице выполняется конфигурация синхронизации времени по протоколу Precision Time Protocol (PTP).

IEEE 1588 Precision Time Protocol (PTP) Client

Manual Setting	DST Overview	DST Configuration	SNTP Client	NTP Client	SIMATIC Time Client	PTP Client
----------------	--------------	-------------------	-------------	------------	---------------------	------------

☐ PTP Client

Current System Time: 12/08/2017 13:53:42

Last Synchronization Time: 12/08/2017 13:36:59

Last Synchronization Mechanism: Manual

Time Zone: +00:00

Daylight Saving Time: inactive (offset + 0h)

Set Values
Refresh

Описание

Страница содержит следующие поля:

- **PTP Client**
Отметьте это поле опции для того, чтобы активировать автоматическую синхронизацию времени по PTP.
- **Current System Time**
Отображает текущую дату и текущее стандартное время, которые были определены функцией синхронизации времени по сети. При указании часового пояса индикация времени корректируется соответствующим образом.
- **Last Synchronization Time**
Отображает, когда выполнялась последняя синхронизация времени.

- **Last Synchronization Mechanism**

Отображает последний момент синхронизации. Допустимы следующие методы:

- Not set
Время не настроено.
- Manual
Ручная настройка времени
- SNTP
Автоматическая синхронизация времени по SNTP
- NTP
Автоматическая синхронизация времени по NTP
- SIMATIC
Автоматическая синхронизация времени с помощью пакета времени SIMATIC
- PTP
Автоматическая синхронизация времени по PTP

- **Time Zone**

Введите в этом поле используемый часовой пояс в формате «+/- ЧЧ:ММ». Часовой пояс указывается по стандартному всемирному времени UTC. Индикация времени в поле «Current System Time» корректируется соответствующим образом.

- **Daylight Saving Time**

Отображает, активирована ли перенастройка на летнее время.

- active (offset +1 h)
Система была перенастроена на летнее время, то есть добавляется один час. Текущее системное время можно увидеть справа вверху в области выбора WBM. В поле «Current System Time» далее отображается стандартное время, включая часовой пояс.
- inactive (offset +0 h)
Текущее системное время не изменяется.

Порядок действий

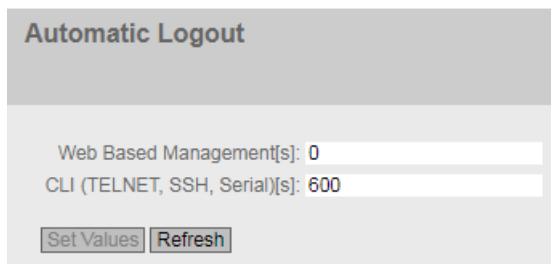
1. Установите галочку в поле опции «PTP Client», чтобы активировать автоматическую настройку времени по PTP.
2. При необходимости укажите часовой пояс.
3. Щёлкните кнопку «Set values».

6.4.11 Automatic Logout

Настройка функции Automatic Logout

На этой странице настраиваются интервалы времени, по истечении которых при неактивности пользователя автоматически выполняется выход из WBM или CLI.

После выполнения автоматического выхода потребуется вновь авторизоваться.



Automatic Logout

Web Based Management[s]: 0

CLI (TELNET, SSH, Serial)[s]: 600

Конфигурация

1. Введите в поле ввода «Web Based Management[s]» значение от 60 до 3600 секунд. При вводе значения 0 функция Automatic Logout деактивируется.
2. Введите в поле ввода «CLI (TELNET, SSH, Serial)[s]» значение от 60 до 600 секунд. При вводе значения 0 функция Automatic Logout деактивируется.
3. Щёлкните кнопку «Set values».

6.4.12 Конфигурация кнопки SELECT/SET

Доступность кнопок

В зависимости от вашего IE-коммутатора в вашем распоряжении имеются различные кнопки и функции, см. главу «Системные функции и оборудование (Страница 17)».

Функции кнопок

Подробное описание функции, которой можно управлять с помощью кнопки, можно найти в руководстве по эксплуатации устройства.

На этой странице можно включать или выключать функции кнопки.



SELECT/SET Button Configuration

☒ Restore Factory Defaults

☒ Set Fault Mask

Описание отображаемых полей

Возможны следующие функции:

- **Restore Factory Defaults**

При активации поля для опции с помощью кнопки можно выполнить функцию «Restore Factory Defaults».



ОСТОРОЖНО

Функция кнопки «Restore Factory Defaults» активна при пуске

Если деактивировать эту функцию в конфигурации, то деактивация активна только в ходе эксплуатации. При пуске, например, после отключения электропитания, функция активна до загрузки конфигурации, благодаря чему возможен бесконтрольный сброс устройства на заводские настройки. Это может приводить к нежелательным помехам в ходе эксплуатации в сети, так как потребуются заново сконфигурировать устройство. При этом также выполняется очистка вставленного PLUG и его сброс в состояние поставки.

- **Set Fault Mask**

При активации этого поля для опции с помощью кнопки можно задавать маску сообщения.

Порядок действий при конфигурации

1. Для использования функции активируйте соответствующее поле опции.
2. Щёлкните кнопку «Set values».

6.4.13 Syslog Client

Согласно RFC 3164 Syslog используется для передачи коротких незашифрованных текстовых сообщений по UDP в IP-сети. Для этого требуется сервер Syslog.

Обязательные условия для отправки записей журнала

- Функция Syslog активирована в устройстве.
- Функция Syslog активирована для соответствующего события.

6.4 Меню «System»

- В вашей сети находится сервер Syslog, способный принимать записи журналов. Так как в данном случае речь идёт о UDP-соединении, информация об исполнении отправителю не направляется.
- IP-адрес сервера Syslog внесён в память устройства.

System Logging (Syslog) Client

☐ Syslog Client

Syslog Server Address:

Select	Syslog Server Address	Server Port	TLS
☐	192.168.16.100	514	☐

1 entry.

Описание

Страница содержит следующие поля:

- **Syslog Client**
Активируйте или деактивируйте функцию Syslog.
- **Syslog Server Address**
Введите IP-адрес сервера Syslog.

Таблица содержит следующие столбцы

- **Select**
Выберите строку, которую необходимо удалить.
- **Syslog Server Address**
Отображает IP-адрес сервера Syslog.
- **Server Port**
Введите используемый порт сервера Syslog.
- **TLS**
При активации этого поля опции обмен данными с сервером Syslog зашифровывается.

Порядок действий

Активация функции

1. Активируйте поле опции «Syslog Client».
2. Щёлкните кнопку «Set values».

Создание новой записи

1. Введите в поле ввода «Syslog Server Address» IP-адрес сервера Syslog, на котором требуется сохранять записи журнала.
2. Щёлкните кнопку «Create». В таблицу добавляется новая строка.
3. Введите в поле ввода «Server Port» номер UDP-порта сервера.
4. Щёлкните кнопку «Set values».

Примечание

По умолчанию для сервера задан порт 514.

Изменение записи

1. Удалите запись.
2. Создайте новую запись.

Удаление записи

1. Установите флажок в строке, которую необходимо удалить.
2. Щёлкните кнопку «Delete». Все отмеченные записи удаляются, а индикация обновляется.

6.4.14 Ports

6.4.14.1 Overview

Обзор конфигурации портов

Эта страница отображает конфигурацию передачи данных для всех портов устройства. Выполнение конфигурации на этой странице невозможно.

Ports Overview						
Overview Configuration						
Port	Port Name	Port Type	Combo Port Media Type	Status	OperState	Link
P1.1		Switch-Port VLAN Hybrid	auto	enabled	up	up
P1.2		Switch-Port VLAN Hybrid	auto	enabled	up	up
P1.3		Switch-Port VLAN Hybrid	auto	enabled	up	up
P1.4		Switch-Port VLAN Hybrid	auto	enabled	up	up
Refresh						

(Продолжение таблицы)

6.4 Меню «System»

Mode	Negotiation	Flow Ctrl. Type	Flow Ctrl.	Maximum Nodes	Learnt Nodes	MAC Address	Blocked by
1G FD	enabled	☐	disabled	0	1	00-1b-1b-af-a2-05	-
1G FD	enabled	☐	disabled	0	1	00-1b-1b-af-a2-06	-
1G FD	enabled	☐	disabled	0	1	00-1b-1b-af-a2-07	-
1G FD	enabled	☐	disabled	0	1	00-1b-1b-af-a2-08	-

Описание отображаемых полей

Таблица состоит из следующих столбцов:

- **Port**
Отображает доступные порты. При щелчке порта открывается соответствующая страница конфигурации. Порт складывается из номера модуля и номера порта, например, порт 0.1 означает модуль 0, порт 1.
- **Port Name**
Отображает имя порта.
- **Port Type**
Отображает тип порта. Возможны следующие типы:
 - Switch Port VLAN Hybrid
 - Switch-Port VLAN Trunk
 - Switch-Port PVLAN Host
 - Switch-Port PVLAN Promiscuous
 - Switch Port VLAN Access
- **Combo Port Media Type**
Этот столбец содержит значение только в случае комбинированного порта. Отображает режим комбинированного порта:
 - auto
 - rj45
 - sfp
- **Status**
Отображает, включён порт или выключен. Обмен данными возможен только через включённый порт.

- **Operational State**
Отображает текущее рабочее состояние. Рабочее состояние зависит от конфигурации параметров «Status» и «Link». Имеются следующие возможности:
 - up
Для порта сконфигурирован статус «enabled», а порт имеет действующее соединение с сетью.
 - down
Для порта сконфигурирован статус «disabled» или «Link down», либо порт не имеет соединения.
 - not present
В модульных устройствах такой статус отображается, например, в том случае, если модуль носителя не вставлен.
- **Link**
Отображает статус соединения с сетью. Возможны следующие варианты статуса соединения:
 - up
Порт имеет действующее соединение с сетью, принимается сигнал «Link Integrity Signal».
 - down
Соединение прервано, потому что, например, подключённое устройство выключено.
- **Mode**
Отображает параметры передачи порта.
- **Negotiation**
Отображает, активирована ли или деактивирована автоматическая конфигурация.
- **Flow Ctrl. Type**
Указывает, активирован ли или деактивирован для порта контроль потока.
- **Flow Ctrl.**
Указывает, работает ли на этом порте контроль потока.
- **Maximum Nodes**
Количество запрограммированных MAC-адресов, при превышении которого выдаётся предупреждение. Если отображается значение «0», это значит, что функция деактивирована. Если указано значение больше «0», это значит, что функция активирована.
- **Learnt Nodes**
Количество MAC-адресов, которое запрограммировано для этого порта.

6.4 Меню «System»

- **MAC Address**
Отображает MAC-адрес порта.
- **Blocked by**
Отображает, почему порт находится в состоянии «blocked»:
 - -
Порт не блокирован.
 - Ring Redundancy
Порт относится к менеджеру резервирования. Если менеджер резервирования находится в состоянии «Passive», то один из портов кольца находится в состоянии «blocking».
 - Spanning Tree
Порт имеет статус «Discarding» в Spanning Tree. Порт является частью Spanning Tree, однако находится на резервном пути и деактивирован для обмена данными.
 - Loop Detection
Распознана петля, и в качестве реакции на петлю для порта сконфигурировано состояние «disable».
 - Link Check
На оптическом участке передачи распознана неисправность, и в качестве реакции для порта сконфигурировано состояние «disable».
 - Link Aggregation Member
Порт является частью Link Aggregation и деактивирован через LACP.
 - Link Aggregation (LoopD)
Порт является частью Link Aggregation. Распознана петля, и в качестве реакции на петлю для Link Aggregation сконфигурировано состояние «disable».
 - Link Aggregation (STP)
Порт является частью Link Aggregation. Spanning Tree переключило Link Aggregation в статус «Discarding».
 - Admin down
Для порта сконфигурирован статус «disabled», см. System > Ports > Configuration.
 - Link down
Для порта сконфигурирован статус «enabled», однако соединение отсутствует, см. System > Ports > Configuration.
 - Spannungsversorgung aus
Для порта сконфигурирован статус «Link down» или «Power down», см. System > Ports > Configuration.
 - Standby
На устройстве активирована функция резервирования в режиме ожидания. Порт является портом режима ожидания со статусом «Passive».
 - MRP-Interconnection
Порт представляет собой MRP Interconnection Port в статусе «blocking».

6.4.14.2 Configuration

Конфигурация портов

На этой странице можно конфигурировать все порты устройства.

Ports Configuration

Overview

Configuration

Port: P0.1

Status: enabled

Port Name:

MAC Address: 20-87-56-2b-6e-01

Mode Type: Auto negotiation

Mode: 1G FD

Negotiation: enabled

☐ Flow Ctrl. Type

Flow Ctrl.: disabled

Port Type: Switch-Port VLAN Hybrid

Combo Port Media Type: auto

☐ Nodes Monitoring

Maximum Nodes: 0

OperState: up

Link: up

Blocked by: -

NOA: Both

Set Values

Refresh

Описание отображаемых полей

Таблица состоит из следующих строк:

- **Port**
В раскрывающемся списке выберите порт, который необходимо сконфигурировать. Порт складывается из номера модуля и номера порта, например, порт 0.1 означает модуль 0, порт 1.
 - **Status**
Задайте, включён порт или выключен.
 - enabled
Порт включён. Обмен данными возможен только через включённый порт.
 - disabled
Порт выключен, однако соединение всё ещё установлено.
 - Link down
Порт выключен и соединение с партнёрским устройством сброшено.
-
- Примечание**
- Пониженное потребление тока**
- Для каждого оптического порта, установленного в состояние «link down», потребление тока устройства сокращается на 30 мА.
-
- Power down
Порт выключен.
 - **Port Name**
Введите здесь имя для порта.
 - **MAC Address**
Отображает MAC-адрес порта.

- **Mode Type**

В раскрывающемся списке выберите скорость и способ передачи данных портом. Для того, чтобы порт и партнёрский порт могли обмениваться данными друг с другом, настройки с обеих сторон должны совпадать.

При выборе режима «Auto Negotiation» эти параметры автоматически согласовываются с подключённым партнёрским портом.

Примечание

Режим «Auto Negotiation»

Если подключённый партнёр не поддерживает режим Auto Negotiation, то порт, к которому подключён этот партнёр, должен быть фиксированно настроен на параметры партнёра (скорость передачи данных, дуплексность).

Примечание

«Auto Negotiation» и Autocrossover

- SCALANCE XB-200/SCALANCE XC-200/XR-300WG: Если функция «Auto negotiation» выключается, выключается также функция «MDI/MDI-X Autocrossover». В этом случае следует использовать кроссированный кабель.
- SCALANCE XP-200: При выключении функции «Auto Negotiation» функция «MDI/MDI-X Autocrossover» остаётся активной.

Примечание

Режимы передачи данных в SCALANCE XR300 WG PoE

В 10-гигабитных портах устройства SCALANCE XR300 WG PoE также возможны режимы передачи данных «2,5 GBit/s full duplex» и «5 GBit/s full duplex». Функция «Auto Negotiation» может настраивать оба этих режима.

- **Mode**

Отображает скорость и способ передачи данных портом. Скорость передачи данных может составлять 10 Мбит/с, 100 Мбит/с, 1000 Мбит/с или 10 Гбит/с. В качестве способа передачи данных могут использоваться полнодуплексный (FD) или полудуплексный режим (HD).

- **Negotiation**

Отображает, активирована ли или деактивирована автоматическая конфигурация партнёрского порта.

6.4 Меню «System»

- **Flow Ctrl. Type**

Активируйте или деактивируйте функцию Flow Control (контроль потока) для порта.

Примечание

Для использования функции контроля потока активируйте контроль потока на соответствующих входных и выходных портах.

Если пакет направляется от входного порта с активированным контролем потока на выходной порт с активированным контролем потока, то пакет при перегрузке не отклоняется. Если управление потоком активировано только на входном порте, пакет при перегрузке может быть отклонён.

Примечание

Включение/выключение контроля потока с функцией «Auto Negotiation»

Контроль потока можно активировать или деактивировать только в том случае, если функция «Auto Negotiation» выключена. После этого функцию «Auto Negotiation» можно вновь активировать.

- **Flow Ctrl.**

Отображает, работает ли на этом порте контроль потока.

- **Port Type** (доступно не для всех групп устройств)
Выберите в раскрывающемся списке тип порта.

Примечание

Функции Private VLAN и аутентификация RADIUS

Если активировано присвоение VLAN через аутентификацию RADIUS для одного или нескольких портов сети VLAN, то эту сеть VLAN не потребуется дополнительно конфигурировать как Private VLAN.

Спектр функций Private VLAN в связи с присвоением VLAN через аутентификацию RADIUS может привести к не единообразному состоянию системы.

- Switch Port VLAN Hybrid
Порт отправляет тегированные и нетегированные пакеты. Он не является участником какой-либо сети VLAN автоматически.
- Switch-Port VLAN Trunk
Порт отправляет только тегированные пакеты и автоматически является участником любых сетей VLAN.
- Switch-Port PVLAN Host
Хост-порты относятся к Secondary PVLAN.
Подключайте к хост-портам устройства, которые должны обмениваться данными только с определенными устройствами сети PVLAN.
- Switch-Port PVLAN Promiscuous
Случайный порт (Promiscuous) относится к Primary PVLAN.
Подключайте к случайным портам (Promiscuous) устройства, которые должны обмениваться данными со всеми остальными устройствами сети PVLAN.
- Switch Port VLAN Access
Порты Access относятся к коммутатору провайдера, который поддерживает функцию туннеля VLAN Q-in-Q.
Подключайте к портам доступа (Access) клиентскую сеть.

6.4 Меню «System»

- **Combo Port Media Type**

Задайте режим комбинированного порта:

- auto
При выборе этого режима порт вставного трансивера будет иметь приоритет. Если вставной трансивер подключён, имеющееся соединение на стационарном порте RJ45 разъединяется. Если вставной трансивер не вставлен, то можно устанавливать соединение через стационарный порт RJ45.
- rj45
При выборе этого режима используется стационарный порт RJ45 вне зависимости от порта вставного трансивера. Если вставной трансивер вставлен, он деактивируется и обесточивается.
- sfr
При выборе этого режима используется порт вставного трансивера вне зависимости от стационарного порта RJ45. Если установлено соединение через RJ45, то оно разрывается, так как порт RJ45 обесточивается.

Заводской настройкой для комбинированных портов является режим auto.

Примечание

Автоматическая адаптация с помощью конфигурации PROFINET

При установлении соединения PROFINET настройка типа носителя комбинированного порта также автоматически адаптируется:

- Если сконфигурирован вставной трансивер, то тип носителя комбинированного порта устанавливается на «sfr».
- Если сконфигурирован порт RJ45, то тип носителя комбинированного порта устанавливается на «rj45».

Для автоматической адаптации тип носителя комбинированного порта необходимо установить на «auto».

Сконфигурируйте тип носителя вставного порта соответствующим образом с помощью WBM или CLI.

- **Nodes Monitoring**

Если это поле опций активировано, то при превышении максимального количества участников выдаётся предупреждение. При активации значение в поле ввода «Maximum Nodes» автоматически устанавливается на «1», при деактивации значение автоматически устанавливается на «0».

- **Maximum Nodes**

Количество запрограммированных MAC-адресов, при превышении которого выдаётся предупреждение. Если значение в этом поле ввода больше «0», то поле опций «Nodes Monitoring» автоматически активируется. Значение «0» автоматически деактивирует поле опций «Nodes Monitoring».

- **Operational State**

Отображает текущее рабочее состояние. Рабочее состояние зависит от конфигурации параметров «Status» и «Link». Имеются следующие возможности:

- up
Для порта сконфигурирован статус «enabled», а порт имеет действующее соединение с сетью.
- down
Для порта сконфигурирован статус «disabled» или «Link down», либо порт не имеет соединения.
- not present
В модульных устройствах такой статус отображается, например, в том случае, если модуль носителя не вставлен.

- **Link**

Отображает статус соединения с сетью. Имеются следующие возможности:

- up
Порт имеет действующее соединение с сетью, принимается сигнал «Link Integrity Signal».
- down
Соединение прервано, потому что, например, подключённое устройство выключено.

6.4 Меню «System»

- **Blocked by**
Отображает, почему порт находится в состоянии «blocked»:
 - -
Порт не блокирован.
 - Ring Redundancy
Порт относится к менеджеру резервирования. Если менеджер резервирования находится в состоянии «Passive», то один из портов кольца находится в состоянии «blocking».
 - Spanning Tree
Порт имеет статус «Discarding» в Spanning Tree. Порт является частью Spanning Tree, однако находится на резервном пути и деактивирован для обмена данными.
 - Loop Detection
Распознана петля, и в качестве реакции на петлю для порта сконфигурировано состояние «disable».
 - Link Check
На оптическом участке передачи распознана неисправность, и в качестве реакции для порта сконфигурировано состояние «disable».
 - Link Aggregation Member
Порт является частью Link Aggregation и деактивирован через LACP.
 - Link Aggregation (LoopD)
Порт является частью Link Aggregation. Распознана петля, и в качестве реакции на петлю для Link Aggregation сконфигурировано состояние «disable».
 - Link Aggregation (STP)
Порт является частью Link Aggregation. Spanning Tree переключило Link Aggregation в статус «Discarding».
 - Admin down
Для порта сконфигурирован статус «disabled», см. System > Ports > Configuration.
 - Link down
Для порта сконфигурирован статус «enabled», однако соединение отсутствует, см. System > Ports > Configuration.
 - Spannungsversorgung aus
Для порта сконфигурирован статус «Link down» или «Power down», см. System > Ports > Configuration.
 - Standby
На устройстве активирована функция резервирования в режиме ожидания. Порт является портом режима ожидания со статусом «Passive».
 - MRP-Interconnection State Change
Порт представляет собой MRP Interconnection Port в статусе «blocking».
- **NOA**
Эта функция доступна не для всех групп устройств, см. главу «Системные функции и оборудование».

Примечание

Эту функцию можно сконфигурировать только в том случае, если устройство работает в режиме Transparent Bridge (Layer 2 > VLAN > вкладка «General» > раскрывающийся список «Base Bridge Mode»: 802.1D Transparent Bridge). В случае конфигурации NOA в режиме «802.1Q VLAN Bridge» отображается сообщение об ошибке.

NOA (NAMUR Open Architecture) представляет собой концепцию обмена данными в промышленности с непрерывными технологическими процессами, предназначенную для передачи данных с полевого уровня в «облако». При этом SCALANCE XC-200 может принимать на себя функцию коммутатора NOA IT/OT и отделять чистые IT-сети от чистых OT-сетей. Кроме того, возможен обмен данными в обеих сетях. Коммутатор разделяет сети по портам, т. е. порт относится либо к IT-сети, либо к OT-сети, либо к обеим сетям. Выберите в раскрывающемся списке, к какой сети относится порт. Для вывода IT-данных или OT-данных порт должен иметь соответствующую конфигурацию. Выберите одну из следующих возможностей:

- Both
Порт относится и к IT-сети, и к OT-сети.
- IT
Порт относится к IT-сети.
- OT
Порт относится к OT-сети.

Изменение конфигурации порта

Щёлкните соответствующее поле, чтобы изменить конфигурацию.

Примечание

Оптические порты всегда работают в полнодуплексном режиме передачи данных и с максимальной скоростью передачи. Поэтому в оптических портах нельзя выполнять следующие настройки:

- Автоматическая конфигурация
- Скорость передачи данных
- Способ передачи данных

Примечание

При перегрузке порта устройство предотвращает или уменьшает обратное влияние на другие порты и классы приоритета (Class of Service) благодаря различным автоматизированным механизмам. При активированном контроле потока это также может приводить к отклонению пакетов.

Перегрузки порта возникают, когда устройство принимает больше пакетов, чем может отправить, например, вследствие различных скоростей передачи данных.

Порядок действий при конфигурации

1. Измените настройки в соответствии с вашей конфигурацией.
2. Щёлкните кнопку «Set values».

6.4.15 Fault Monitoring

6.4.15.1 Power Supply

Настройки для мониторинга источников питания

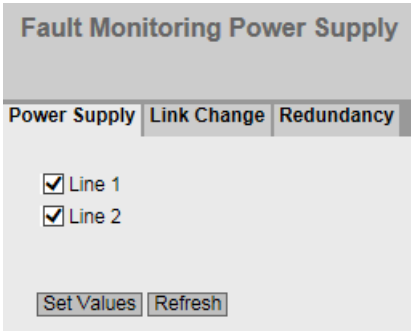
Сконфигурируйте, требуется ли системе оповещения контролировать источники питания. В зависимости от варианта аппаратного обеспечения имеются одно и два подключения питания (источник питания 1/источник питания 2). В случае электропитания с резервированием сконфигурируйте мониторинг для каждой отдельной подводящей линии.

В этом случае система оповещения сообщает об ошибке, если на контролируемом подключении (источник питания 1 или источник питания 2) отсутствует напряжение или имеется слишком низкое напряжение.

Примечание

Допустимые пределы рабочего напряжения см. в руководстве по эксплуатации устройства.

Ошибка ведёт к срабатыванию сигнального контакта и к активации светодиода ошибки и может в зависимости от конфигурации вызывать срабатывание ловушки, отправку сообщения электронной почты или внесение записи в таблицу протокола событий.



Порядок действий

1. Щёлкните поле опций перед соответствующим именем подключения, которое требуется контролировать, чтобы включить или выключить функцию контроля.
2. Щёлкните кнопку «Set values».

6.4.15.2 Link Change

Конфигурация контроля ошибок изменения состояния соединений

На этой странице можно сконфигурировать, будет ли срабатывать сообщение об ошибке при изменении состояния соединения с сетью.

При активированном контроле соединений подаётся сигнал ошибки в следующем случае:

- на порте должен иметься канал связи, но он отсутствует
- на порте не должен иметься канал связи, однако канал связи обнаружен

Ошибка ведёт к срабатыванию сигнального контакта и к активации светодиода ошибки и может в зависимости от конфигурации вызывать срабатывание ловушки, отправку сообщения электронной почты или внесение записи в таблицу протокола событий.

Port	Setting
P0.1	-
P0.2	-
P0.3	-
P0.4	-

Описание отображаемых полей

Таблица 1 состоит из следующих столбцов:

- **1-й столбец**
Отображает, что настройки действительны для всех портов.
- **Setting**
Выберите в раскрывающемся списке настройку. Имеются следующие возможности настройки:
 - «-» (деактивировано)
 - Up
 - Down
 - No Change: настройка в таблице 2 остаётся без изменений.
- **Copy to Table**
Если нажать кнопку, то настройка будет применена для всех портов таблицы 2.

Таблица 2 состоит из следующих столбцов:

- **Port**
Отображает доступные порты. Порт складывается из номера модуля и номера порта, например, порт 0.1 означает модуль 0, порт 1.
- **Setting**
Выберите в раскрывающемся списке настройку. Предлагаются следующие возможности:
 - Up
Обработка ошибок срабатывает при переходе порта в активное состояние. (от «Link down» до «Link up»)
 - Down
Обработка ошибок срабатывает при переходе порта в неактивное состояние. (от «Link up» до «Link down»)
 - «-» (деактивировано)
Обработка ошибок не срабатывает.

Порядок действий при конфигурации

Конфигурирование мониторинга ошибок для порта

1. Выберите в раскрывающемся списке варианты слотов/портов, статус соединения которых требуется контролировать.
2. Щёлкните кнопку «Set values».

Конфигурирование мониторинга ошибок для всех портов

1. Выберите в раскрывающемся списке «Setting» в столбце нужную настройку.
2. Щёлкните кнопку «Copy to Table». Настройка будет применена для всех портов таблицы 2.
3. Щёлкните кнопку «Set values».

6.4.15.3 Redundancy

На этой странице можно сконфигурировать, будет ли срабатывать сообщение об ошибке при изменении состояния соединения с резервированием.

Настройка

- **Redundancy Lost**

Если поле опции активировано, то при кольцевом переключении (MRP или HRP, заблокированный порт находится в переключенном состоянии) в соответствующем менеджере кольца активируется светодиод ошибки.

6.4.16 PROFINET

Настройки для PROFINET

На этой странице конфигурируется режим PROFINET.

Описание отображаемых полей

Страница содержит следующие поля:

- **PROFINET Device Diagnostics**
Отображает, активирована ли («On») или деактивирована («Off») функция PROFINET.
- **PROFINET Device Diagnostics for next boot**
Настройте, требуется ли активировать («On») или деактивировать («Off») PROFINET при следующем повторном пуске устройства.

Примечание

PROFINET и EtherNet/IP

При включении PROFINET выключается EtherNet/IP. Переключение между PROFINET и EtherNet/IP не влияет на DCP.

Примечание

PROFINET AR Status

Если соединение PROFINET установлено, то есть PROFINET имеет статус AR «Online», то PROFINET деактивировать невозможно.

- **PROFINET AR Status**

Это поле отображает статус соотношения соединения PROFINET. Это значит, например, что устройство имеет соединение «Online» или «Offline» с контроллером PROFINET.

Онлайн при этом означает, что соединение с контроллером PROFINET установлено, что последний загрузил свои данные в устройство, и что устройство может отправлять данные о статусе контроллеру PROFINET. В этом состоянии, которое также называется «in Data exchange», параметры, настроенные с помощью контроллера PROFINET, недоступны для конфигурирования.

- **PROFINET Name of Station**

В этом поле появляется имя устройства PROFINET в соответствии с конфигурацией аппаратного обеспечения STEP 7.

- **Restart with PROFINET Defaults**

Чтобы восстановить заводские настройки профиля PROFINET и выполнить повторный пуск устройства, щёлкните эту кнопку. Потребуется подтвердить повторный пуск в диалоговом окне. В диалоговом окне отобразятся настройки, которые специально адаптированы для работы с протоколом PROFINET.

ВНИМАНИЕ
При сбросе настроек профиля на значения по умолчанию IP-адрес также удаляется. После этого устройство доступно только через последовательный интерфейс, SINEC PNI или DHCP. При соответствующем подключении предварительно сконфигурированное устройство может стать причиной круговых пакетов и, соответственно, отказа обмена данными.

6.4.17 EtherNet/IP

6.4.17.1 EtherNet/IP

EtherNet Industrial Protocol (EtherNet/IP)

На этой странице конфигурируется протокол EtherNet/IP.

Описание

Страница содержит следующие поля:

- **EtherNet/IP Device Diagnostics**
Отображает, активирован ли («On») или деактивирован («Off») протокол EtherNet/IP.
- **EtherNet/IP Device Diagnostics for next boot**
Настройте, требуется ли активировать («On») или деактивировать («Off») EtherNet/IP при следующем повторном пуске устройства.

Примечание

EtherNet/IP и PROFINET

При включении EtherNet/IP выключается PROFINET. Переключение между EtherNet/IP и PROFINET не влияет на DCP.

Примечание

Статус PROFINET AR

Если соединение PROFINET установлено, то есть PROFINET имеет статус AR «Online», то EtherNet/IP деактивировать невозможно.

6.4 Меню «System»

- **EtherNet/IP DLR**
Настройте, должен ли протокол Device Level Ring (DLR) быть активирован («Enable») или деактивирован («Disable»).
- **EtherNet/IP DLR Ports**
Выберите в раскрывающихся списках оба порта DLR.
- **Restart with EtherNet/IP Defaults**
Для того, чтобы восстановить заводские настройки профиля EtherNet/IP и выполнить его повторный пуск, щёлкните эту кнопку. Потребуется подтвердить повторный пуск в диалоговом окне. В диалоговом окне отобразятся настройки, которые специально адаптированы для работы с протоколом EtherNet/IP.

ВНИМАНИЕ

Отказ обмена данными после сброса на настройки по умолчанию

При сбросе настроек профиля на значения по умолчанию IP-адрес также удаляется. После этого устройство становится доступным только через последовательный интерфейс, SINEC PNI или DHCP.

При соответствующем подключении предварительно сконфигурированное устройство может стать причиной круговых пакетов и, соответственно, отказа обмена данными.

6.4.17.2 DLR Status

Состояние Device Level Ring

Эта страница отображает данные о протоколе Device Level Ring (DLR). Конфигурирование параметров на этой странице невозможно.

EtherNet Industrial Protocol (EtherNet/IP) DLR Status

EtherNet/IP	DLR Status
Supervisor IP Address:	0.0.0.0
Supervisor MAC Address:	00-00-00-00-00-00
Ring Topology:	Linear
Ring State:	Fault
Node State:	Idle
Network Status:	Normal
VLAN ID:	0
Ring Port 1 Status:	Down
Ring Port 2 Status:	Down

Описание

Страница содержит следующие поля:

- **Supervisor IP Address**
IP-адрес устройства, которое принимает на себя функцию супервайзера DLR.
- **Supervisor MAC Address**
MAC-адрес устройства, которое принимает на себя функцию супервайзера DLR.
- **Ring Topology**
Топология сети обоих портов DLR.
- **Ring State**
Отображает, работает ли кольцо DLR надлежащим образом.
- **Node State**
Отображает состояние супервайзера DLR.
- **Network Status**
Отображает работоспособность сети.
- **VLAN ID**
Идентификатор VLAN для EtherNet/IP. Идентификатор VLAN «0» не поддерживается. В WBM идентификатор VLAN «0» отображается только в том случае, если EtherNet/IP DLR не активирован, и до тех пор, пока супервайзер не распознан. Конфигурация идентификатора VLAN для DLR зависит от устройства:
 - **SCALANCE XR-300WG PoE, SCALANCE XC-200 с кодом «G» в типовом обозначении (гигабитные версии) и SCALANCE XC216 4C**
DLR-VLAN не зависит от конфигурации VLAN устройства.
 - **Все остальные устройства**
DLR-VLAN зависит от конфигурации VLAN устройства.
Порты DLR EtherNet/IP автоматически добавляются как участники всех VLAN с идентификатором в диапазоне от 1 до 4095, вне зависимости от того, имеется ли VLAN в конфигурации устройства. В WBM порты DLR EtherNet/IP отображаются во всех доступных сетях VLAN с обозначением «E».
- **Ring Port 1 Status**
Статус порта DLR 1.
- **Ring Port 2 Status**
Статус порта DLR 2.

6.4.18 Модуль PLUG

6.4.18.1 Configuration

ВНИМАНИЕ

Запрещается извлекать или вставлять PLUG во время работы

PLUG разрешается извлекать и вставлять только в том случае, если устройство выключено.

Устройство с интервалом в одну секунду проверяет, вставлен ли PLUG. Если извлечь PLUG во время работы, это может привести к потере данных.

Информация о конфигурации C-PLUG

На этой странице отображается подробная информация о конфигурации, которая сохранена в C-PLUG. Кроме того, имеется возможность сбросить PLUG на «заводские настройки» или записать на него новое содержимое.

Примечание

Действие будет выполнено только после щелчка кнопки «Set values».

Это действие невозможно отменить.

Если после выбора вы решите отменить выполнение, щёлкните кнопку «Refresh». В результате данные на этой странице будут заново считаны из устройства, а выбранные значения будут отменены.

Примечание

Несовместимость с более старыми версиями прошивки со вставленным модулем PLUG

Установка более старой версии прошивки может привести к потере данных конфигурации. В этом случае сбросьте настройки устройства на заводские настройки после установки прошивки.

В этом случае, если в устройство вставлен модуль PLUG, то он после повторного пуска будет иметь статус «NOT ACCEPTED», так как на модуле PLUG будут все ещё находиться данные конфигурации предыдущей, более актуальной версии прошивки. Благодаря этому можно будет вернуться к предыдущей, более актуальной версии прошивки без потери данных конфигурации.

Если предыдущая конфигурация на PLUG более не требуется, то PLUG можно вручную удалить или заново описать в разделе «System > PLUG».

Описание отображаемых полей

Таблица состоит из следующих строк:

- **Status**
Отображает статус PLUG. Имеются следующие возможности:
 - ACCEPTED
В устройстве имеется PLUG с действительной и подходящей конфигурацией.
 - NOT ACCEPTED
На вставленном PLUG находится недействительная или несовместимая конфигурация.
 - NOT PRESENT
В устройство не вставлен C-PLUG.
 - FACTORY
PLUG вставлен и не содержит конфигурации. Этот статус также отображается в том случае, если PLUG отформатирован во время эксплуатации.
- **Device Group**
Отображает, C-PLUG какого семейства продукции SIMATIC NET использовался в предшествующей эксплуатации.

- **Device Type**
Отображает, C-PLUG какого типа устройства внутри семейства продукции использовался в предшествующей эксплуатации.
- **Configuration Revision**
Версия структуры конфигурации. Эти данные относятся к возможностям конфигурации, поддерживаемым устройством, и не связаны с конкретной конфигурацией аппаратного обеспечения. Соответственно, сведения о версии не изменяются, если добавляются или убираются дополнительные компоненты (например, модули или передатчики). Однако они могут изменяться при выполнении обновления прошивки.
- **File System**
Отображает тип файловой системы, имеющейся на PLUG.
- **File System Size**
Отображает максимальную ёмкость памяти файловой системы, имеющейся на PLUG, в байтах.
- **File System Usage**
Отображает занятую ёмкость памяти файловой системы на PLUG в байтах.
- **Info**
Отображает дополнительные данные об устройстве, которое использовало PLUG в ходе предшествующей эксплуатации, например, номер для заказа, типовое обозначение, а также рабочие версии аппаратного и программного обеспечения. Отображаемая версия программного обеспечения соответствует версии, в которой последний раз выполнялись изменения конфигурации. В случае статуса «NOT ACCEPTED» отображается дополнительная информация о причине проблемы.
- **Firmware on PLUG**
Если функция активирована (по умолчанию), то прошивка сохраняется на модуле PLUG. Таким образом, с помощью модуля PLUG можно выполнять автоматические обновления/откаты на более раннюю версию прошивки. В поле «Info» отображается, сохранена ли прошивка на модуле PLUG или нет.
- **Modify PLUG**
Выберите в раскрывающемся списке настройку. Для изменения конфигурации на C-PLUG вам предлагаются следующие возможности:
 - Write current configuration to PLUG
Эта опция доступна только в том случае, если PLUG имеет статус «NOT ACCEPTED» или «FACTORY».
Имеющаяся на внутреннем флэш-накопителе устройства конфигурация копируется на PLUG.
 - Erase PLUG to factory default
Удаляет все данные с PLUG и выполняет низкоуровневое форматирование.

Порядок действий при конфигурации

1. Настройки в этом поле можно выполнять только в том случае, если вы авторизованы как «администратор». Выберите здесь то, как вы хотите изменить содержимое PLUG.
2. Если требуется сохранить прошивку на модуле PLUG, активируйте поле опции «Firmware on PLUG».

3. Выберите в раскрывающемся списке «Modify PLUG» нужную опцию.
4. Щёлкните кнопку «Set values».

6.4.19 Ping

Доступность адреса в сети IPv4

С помощью функции проверки связи можно проверить, доступен ли определённый адрес IPv4 в сети.

The screenshot shows a web-based interface for a ping utility. At the top is a grey header with the word 'Ping'. Below the header, there are three main components: a text input field labeled 'Destination Address:', a text input field labeled 'Repeat:' with the value '3' entered, and a button labeled 'Ping'. Below these fields is a large, empty text area labeled 'Ping Output:'. At the bottom left of the interface is a button labeled 'Clear'.

Описание

Таблица состоит из следующих столбцов:

- **Destination Address**
Введите адрес IPv4 устройства.
- **Repeat**
Введите количество запросов проверки связи.
- **Ping**
Щёлкните эту кнопку, чтобы запустить функцию проверки связи.
- **Ping Output**
В этом поле отображаются результаты работы функции проверки связи.
- **Clear**
Щёлкните эту кнопку, чтобы очистить поле «Ping Output».

6.4.20 DCP Discovery

На этой странице можно выбрать интерфейс и выполнить поиск устройств, которые доступны через этот интерфейс и поддерживают DCP. Функция DCP Discovery ищет только устройства, которые находятся в той же подсети, что и интерфейс. Доступные устройства приводятся в таблице. В таблице можно проверять и корректировать сетевые параметры устройств. Для идентификации и конфигурирования устройств используется протокол Discovery Configuration Protocol (DCP).

Примечание

DCP Discovery

Функция доступна только в сети VLAN, ассоциированной с интерфейсом TIA. Интерфейс TIA конфигурируется в пункте System > Agent IP.

Discovery and Set via PROFINET Discovery and Configuration Protocol (DCP)

Timeout[s]: 5
Blink Own LEDs

Interface: vlan1
Discover

Port	MAC Address	Device Type	Device Name	IP Address	Mask Address	Gateway Address	Name Status	IP Status	Timeout[s]	Blink
P0.2	00-10-10-00-00-00	SCALANCE W-700		192.168.16.177	255.255.255.0	0.0.0.0	None	Discovered/IP	5	Blink
P0.2	00-10-10-00-00-00	SCALANCE X-500		192.168.16.150	255.255.255.0	0.0.0.0	None	Discovered/IP	5	Blink
P0.2	00-10-10-00-00-00	SCALANCE M-800		192.168.16.48	255.255.255.0	0.0.0.0	None	Discovered/IP	5	Blink
P0.2	00-10-10-00-00-00	SCALANCE M-800		192.168.16.50	255.255.255.0	0.0.0.0	None	Discovered/IP	5	Blink
P0.2	00-10-10-00-00-00	SCALANCE M-800		192.168.16.46	255.255.255.0	0.0.0.0	None	Discovered/IP	5	Blink
P0.2	00-10-10-00-00-00	SCALANCE S-600	securityxb10657	192.168.16.42	255.255.255.0	0.0.0.0	Discovered	Discovered/IP	5	Blink
P0.2	00-10-10-00-00-00	SCALANCE X-300		192.168.16.33	255.255.255.0	192.168.16.33	None	Discovered/IP	5	Blink
P0.2	00-10-10-00-00-00	SCALANCE X-400		192.168.16.144	255.255.255.0	0.0.0.0	None	Discovered/IP	5	Blink
P0.2	00-10-10-00-00-00	SCALANCE M-800		192.168.1.1	255.255.255.0	192.168.1.20	None	Discovered/IP	5	Blink
P0.2	00-10-10-00-00-00	SCALANCE X-500		192.168.16.155	255.255.255.0	0.0.0.0	None	Discovered/IP	5	Blink

1 - 10 of 20 entries
Show all
1
Next

Set Values
Refresh

Обязательное условие:

для коррекции сетевых параметров DCP требуется право записи на устройстве. Если доступ имеет защиту от записи, то конфигурация сетевых параметров невозможна.

На устройствах SCALANCE доступ конфигурируется в пункте меню System > Configuration.

Описание

Страница содержит следующие поля:

- Timeout[s]**
Выберите период, в течение которого будут мигать светодиоды.
- Blink Own LEDs**
Запуск мигания светодиодов устройства.

- **Interface**
Выберите нужный интерфейс.
- **Discover**
Запускает поиск устройств, которые могут быть доступны через выбранный интерфейс.
По окончании поиска доступные устройства приводятся в таблице. Длина таблицы ограничена 100 строками.

Таблица состоит из следующих столбцов:

- **Port**
Отображает порт, через который доступно устройство.
- **MAC Address**
Отображает MAC-адрес устройства.
- **Device Type**
Отображает, к какому семейству или группе продукции относится устройство.
- **Device Name**
При необходимости откорректируйте имя устройства PROFINET. Имя устройства должно соответствовать требованиям DNS.
Если имя устройства не используется, поле будет пустым.
- **IP Address**
При необходимости откорректируйте адрес IPv4 устройства.
Адрес IPv4 должен быть однозначным в пределах вашей сети и соответствовать сети.
Адрес IPv4 0.0.0.0 означает, что адрес IPv4 ещё не настроен.
- **Subnet Mask**
При необходимости откорректируйте маску подсети устройства.
- **Gateway Address**
При необходимости откорректируйте адрес IPv4 шлюза.
- **Name Status**
 - None: имя устройства не используется.
 - Discovered: используется настроенное имя устройства.
 - Configured: устройству присвоено новое имя устройства.
- **IP Status**
 - Discovered/IP: устройство использует статический IPv4-адрес.
 - Discovered/DHCP: устройство получило адрес IPv4 от DHCP-сервера.
 - Configured: устройству присвоен новый адрес IPv4.
- **Timeout[s]**
установите продолжительность для мигания. Когда время истекает, мигание прекращается.
- **Blink**
Заставляет мигать светодиоды порта выбранного устройства.

Порядок действий при конфигурации

1. Выберите интерфейс TIA.
2. Чтобы отобразить все устройства, доступные через интерфейс TIA, щёлкните кнопку «Discover».
3. Адаптируйте нужные характеристики.
4. Щёлкните кнопку «Set values».
Статус изменённых характеристик изменится на «Configured».
5. Чтобы удостовериться, что характеристики сохранились верно, снова щёлкните кнопку «Discover».
Статус изменённых характеристик изменится на «Discovered».

6.4.21 Power over Ethernet (PoE)

6.4.21.1 General

Настройки для Power over Ethernet (PoE)

На этой странице находится информация о мощности, передаваемой через IE-коммутатор посредством PoE.

Варианты PoE устройства SCALANCE XP-200 представляют собой оборудование PSE (Power Sourcing Equipment).

PSE	Maximum Power[W]	Allocated Power[W]	Power In Use[W]	Usage Threshold[%]
1	120	0	0	80

Описание отображаемых полей

- **PSE (доступно только для чтения)**
Отображает номер PSE.
- **Максимальная мощность [Вт]**
Максимальная мощность, которую одно устройство PSE предоставляет для питания устройств PoE. Для типа устройства SCALANCE XR326-2C PoE WG вы можете настроить максимальную мощность; для других устройств это поле доступно только для чтения.
- **Allocated Power [Вт] (только для чтения)**
Сумма мощности, зарезервированной PoE-устройствами согласно их «классификации».

- **Power In Use [Вт] (только для чтения)**
Сумма мощности, используемой оконечными устройствами.
- **Usage Threshold [%]**
Как только потребляемая оконечными устройствами мощность становится больше указанной здесь процентной доли, срабатывает событие.

6.4.21.2 Port

Настройки для портов

Для каждого отдельного PoE-порта можно задавать, должно ли выполняться энергоснабжение через Ethernet. Кроме того, для каждого подключённого потребителя можно задавать приоритет. Устройствам, для которых задан высокий приоритет, в случае необходимости отдаётся предпочтение в отношении электропитания в сравнении с остальными.

На этой странице отображается подробная информация об отдельных PoE-портах.

Power over Ethernet (PoE) Port

General | Port | Schedule

Port	Setting	Priority	Type	Use Custom Maximum Power	Custom Maximum Power[W]	Copy to Table
All ports	No Change	No Change	No Change	No Change	No Change	Copy to Table

Port	Setting	Priority	Type	Use Custom Maximum Power	Custom Maximum Power[W]	Primary Classification	Secondary Classification	Dual Signature PD	Status	Power[mW]	Voltage[V]	Current[mA]
P0.1	☒	low		☐	0	-	-	-	searching	0	0	0
P0.2	☒	low		☐	0	-	-	-	searching	0	0	0
P0.3	☒	low		☐	0	-	-	-	searching	0	0	0
P0.4	☒	low		☐	0	-	-	-	searching	0	0	0

Set Values Refresh

Описание отображаемых полей

Страница содержит две таблицы. В таблице 1 можно выполнять настройки и присваивать их одновременно всем портам. В таблице 2 можно выполнять различные настройки для каждого порта.

Таблица 1 состоит из следующих столбцов:

- **Port**
Отображает, что настройки действительны для всех портов.
- **Setting**
Выберите необходимую настройку.
Если выбрано значение «No Change», то запись в таблице 2 не изменяется.
- **Priority**
Выберите нужный приоритет.
Если выбрано значение «No Change», то запись в таблице 2 не изменяется.
- **Type**
Здесь можно ввести цепочку символов, которая более подробно описывает подключённое устройство. Максимальная длина составляет 255 символов.

- **Use Custom Maximum Power**
Выберите, следует ли использовать устанавливаемую пользователем максимальную мощность.
Если выбрано значение «No Change», то запись в таблице 2 не изменяется.
- **Custom Maximum Power [W]**
Укажите максимальную мощность, которую порт предоставляет для питания подключённого устройства.
Это значение учитывается только в том случае, если соответствующее поле опции «Use Custom Maximum Power» активировано.
Если введено значение «No Change», запись в таблице 2 не изменяется.
- **Copy to Table**
Если нажать эту кнопку, то настройки будут применены для всех портов таблицы 2.

Таблица 2 состоит из следующих столбцов:

- **Port**
Отображает сконфигурированные PoE-порты.
Порт складывается из номера модуля и номера порта, например, порт 0.1 означает модуль 0, порт 1.
- **Setting**
Разблокируйте электропитание PoE для этого порта или прервите его.
- **Priority**
Выберите в раскрывающемся списке приоритет, с которым этот порт будет учитываться в электропитании.
Существуют следующие возможности в порядке повышения значимости:
 - Low
 - High
 - Critical

Если мощности подключённого электропитания недостаточно для питания всех подключённых устройств, то в первую очередь обеспечивается питание устройств с более высоким приоритетом.
Если для двух портов указан одинаковый приоритет, то в случае необходимости предпочтительным становится порт с более низким номером.
- **Type**
Здесь можно ввести цепочку символов, которая более подробно описывает подключённое устройство. Максимальная длина составляет 255 символов.
- **Use Custom Maximum Power**
Если активировать это поле опции для порта, то будет использоваться заданная пользователем максимальная мощность.

- **Custom Maximum Power [W]**

Укажите максимальную мощность, которую порт предоставляет для питания подключённого устройства.

Это значение учитывается только в том случае, если соответствующее поле опции «Use Custom Maximum Power» активировано.

Заданная пользователем мощность сравнивается с диапазоном значений класса, который указан для подключённого устройства:

- Если заданная пользователем мощность находится в рамках класса подключённого устройства, то используется заданное пользователем значение.
- Если заданная пользователем мощность превышает класс подключённого устройства, то используется максимальное значение класса.
- Если заданная пользователем мощность ниже класса подключённого устройства, то используется минимальное значение класса.

Если потребляемая мощность подключённого устройства превышает заданную или используемую максимальную мощность, то подключённое устройство отключается.

- **Classification** (только для чтения)

В устройствах, которые могут обеспечивать питание потребителей энергии по стандартам IEEE802.af типа 1 или IEEE802.at типа 2.

Классификация устройства указывает класс устройства. Благодаря этому можно считывать максимальную мощность устройства.

- **Primary Classification** (доступно только для чтения)

В устройствах, которые могут обеспечивать питание потребителей энергии по стандартам IEEE802.af типа 1, IEEE802.at типа 2 или IEEE802.3bt типа 3.

Основная классификация устройства на этом порте.

- **Secondary Classification** (доступно только для чтения)

В устройствах, которые могут обеспечивать питание потребителей энергии по стандартам IEEE802.af типа 1, IEEE802.at типа 2 или IEEE802.3bt типа 3.

Второстепенная классификация устройства на этом порте.

- **Dual Signature PD** (доступно только для чтения)

В устройствах, которые могут обеспечивать питание потребителей энергии по стандартам IEEE802.af типа 1, IEEE802.at типа 2 или IEEE802.3bt типа 3.

Указывает, идёт ли речь в отношении подключённого энергопотребителя о Single Signature PD или о Dual Signature PD.

- **Yes**

Электропитание устройства на этом порте должно соответствовать основной классификации (Primary Classification) и второстепенной классификации (Secondary Classification).

- **No**

Электропитание устройства на этом порте должно соответствовать второстепенной классификации (Secondary Classification).

6.4 Меню «System»

- **Status** (доступно только для чтения)
Отображает, в каком состоянии находится порт.
Существуют следующие состояния:
 - disabled
Электропитание PoE для этого порта деактивировано.
 - delivering
Электропитание PoE для этого порта активировано и устройство подключено.
 - searching
Электропитание PoE для этого порта активировано, однако ни одно устройство не подключено.

Примечание

Если устройство подключено к порту, обладающему функцией PoE, то выполняется проверка того, достаточна ли мощность порта для подключённого устройства.

Если мощности порта недостаточно, но функция PoE активирована в пункте Setting, то порт всё равно сохраняет статус disabled. В этом случае порт деактивирован функцией PoE-Power Management.

- **Power [мВт]** (доступно только для чтения)
Отображает мощность, подаваемую на этот порт устройством SCALANCE.
- **Voltage [В]** (доступно только для чтения)
Отображает напряжение, подаваемое на этот порт.
- **Current [мА]** (доступно только для чтения)
Отображает силу тока, с помощью которого осуществляется питание устройства на этом порте.

6.4.21.3 Schedule

Временные ограничения для Power over Ethernet (PoE)

На этой странице конфигурируется период времени, в течение которого возможно электропитание через отдельные PoE-порты. Если потребители не эксплуатируются непрерывно, это может снизить расход энергии.

Power over Ethernet (PoE) Schedule Port

General | Port | Schedule

Port	Scheduled	Start Time	End Time	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday	Sunday	Copy to Table
All ports	No Change ▼	No Change	No Change	No Change ▼	No Change ▼	No Change ▼	No Change ▼	No Change ▼	No Change ▼	No Change ▼	Copy to Table

Port	Scheduled	Start Time	End Time	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday	Sunday
P0.1	☐			☐	☐	☐	☐	☐	☐	☐
P0.2	☐			☐	☐	☐	☐	☐	☐	☐
P0.3	☐			☐	☐	☐	☐	☐	☐	☐
P0.4	☐			☐	☐	☐	☐	☐	☐	☐

Set Values Refresh

Описание отображаемых полей

Страница содержит две таблицы. В таблице 1 можно выполнять настройки и присваивать их одновременно всем портам. В таблице 2 можно выполнять различные настройки для каждого порта.

Таблица 1 состоит из следующих столбцов:

- **Port**
Отображает, что настройки действительны для всех портов.
- **Setting**
Имеются следующие возможности:
 - **Activated**
Все поля опций во втором столбце таблицы 2 активируются.
 - **Deactivated**
Все поля опций во втором столбце таблицы 2 деактивируются.
 - **No Change**
Записи в таблице 2 остаются без изменений.
- **Start Time**
Введите время начала для электропитания с помощью функции PoE в формате **чч:мм**. Если выбран вариант «No Change», то записи в таблице 2 остаются без изменений.
- **End Time**
Введите время окончания для электропитания с помощью функции PoE в формате **чч:мм**. Если выбран вариант «No Change», то записи в таблице 2 остаются без изменений.
Если значение для времени окончания меньше, чем значение для времени начала, или если оба значения одинаковы, то прекращение электропитания через PoE приходится на следующий день недели.
- **Monday ... Sunday**
Имеются следующие возможности:
 - **Activated**
Все поля опций в столбце для соответствующего дня недели таблицы 2 активируются.
 - **Deactivated**
Все поля опций в столбце для соответствующего дня недели таблицы 2 деактивируются.
 - **No Change**
Записи в таблице 2 остаются без изменений.
- **Copy to Table**
Если нажать эту кнопку, то настройки будут применены для всех портов таблицы 2.

Таблица 2 состоит из следующих столбцов:

- **Port**
Отображает сконфигурированные PoE-порты. Порт складывается из номера модуля и номера порта, например, «порт 0.1» обозначает модуль 0, порт 1.
- **Setting**
Если поле опции активировано, то соответствующий порт обеспечивает питание через PoE только в течение сконфигурированного периода времени.

6.4 Меню «System»

- **Start Time**
Введите время начала для электропитания с помощью функции PoE в формате **ЧЧ:ММ**.
- **End Time**
Введите время окончания для электропитания с помощью функции PoE в формате **ЧЧ:ММ**.
- **Monday ... Sunday**
Активируйте поля опции для дней недели, в которые должно обеспечиваться электропитание через PoE.

6.4.22 Port Diagnostics

6.4.22.1 Cable Tester

На этой странице каждый отдельный порт Ethernet может выполнять независимую диагностику ошибок кабеля. Этот тест выполняется без извлечения кабеля, подключения кабельного тестера или установки кольцевого модуля на другом конце. Это позволяет точно локализовать короткие замыкания или обрывы линии на расстоянии нескольких метров.

Примечание

Помните о том, что этот тест допустим только в том случае, когда на тестируемом порте не установлено соединение для передачи данных.

Если же на тестируемом порте установлено соединение для передачи данных, то оно будет кратковременно разорвано.

Автоматическое восстановление соединения может не сработать, и в этом случае его потребуется выполнить вручную.

Cable Tester

Cable Tester

Port: P1.1

Run Test

Pair	Status	Distance
1-2	OK	unknown
3-6	OK	unknown
4-5	short-circuit	1
7-8	short-circuit	1

Refresh

Описание

Страница содержит следующие поля:

- **Port**
Выберите в раскрывающемся списке нужный порт.
- **Run Test**
Активирует диагностику ошибок. Результат отображается в таблице.

Таблица содержит следующие столбцы:

- **Pair**
Отображает пару жил в кабеле.

Примечание

Пары жил

В случае сетевых кабелей 10/100 Мбит пары жил 4-5 и 7-8 не используются.

При этом назначение пары жил / разводка контактов выполнено следующим образом (DIN EN 50173):

Пара 1 = контакты 1-2

Пара 2 = контакты 3-6

Пара 3 = контакты 4-5

Пара 4 = контакты 7-8

- **Status**
Отображает статус линии.
- **Distance**
Отображает расстояние до открытого конца кабеля, обрыва или до короткого замыкания в метрах. Значение расстояния имеет погрешность +/- 1 м.
Если статус «OK», то длина указывается как «unknown».

6.4.22.2 SFP Diagnostics

На этой странице выполняется независимая диагностика ошибок для каждого отдельного порта SFP. Этот тест выполняется без необходимости извлечения кабеля, подключения кабельного тестера или установки кольцевого модуля на другом конце.

Примечание

Помните о том, что этот тест допустим только в том случае, когда на тестируемом порте не установлено соединение для передачи данных. Если же на тестируемом порте установлено соединение для передачи данных, то оно будет кратковременно разорвано. Автоматическое восстановление соединения может не сработать, и в этом случае его потребуется выполнить вручную.

Small Form-factor Pluggable (SFP) Transceiver Diagnostics

Cable Tester

SFP Diagnostics

Port: P0.4

Name: SIEMENS

Model: SFP992-1

Revision: 1

Serial: NM0001MC1S0065

Nominal Bit Rate[MBit/s]: 10300

Max. Link (single mode)[m]: 80

Max. Link (50.0/125um)[m]: 80

Max. Link (62.5/125um)[m]: 30

	Current	Low	High
Temperature[°C]:	34.14	-5.0	75.0
Voltage[V]:	3.21	3.0	3.55
Current[mA]:	5.20	2.92	9.10
Rx Power[uW]:	0.0	63.0	891.2
Rx Power[dBm]:	-99.9	-12.0	0.5
Tx Power[uW]:	436.0	316.2	891.2
Tx Power[dBm]:	-3.6	-5.0	0.5

Refresh

Описание

Страница содержит следующие поля:

- **Port**
Выберите в раскрывающемся списке нужный порт.
- **Refresh**
Обновляет отображение значений настроенных портов. Результат отображается в таблице.

Значения отображаются в следующих полях:

- **Name**
Отображает имя интерфейса.
- **Modell**
Отображает вид интерфейса.
- **Revision**
Отображает выпуск аппаратного обеспечения SFP.
- **Serial**
Отображает серийный номер SFP.
- **Nominal Bit Rate[MBit/s]**
Отображает номинальную скорость передачи данных интерфейса в битах.

- **Max. Link (single mode)[m]**
Отображает максимальное расстояние в метрах, которое допустимо для этой среды.
- **Max. Link (50.0/125um)[m]**
Отображает максимальное расстояние в метрах, которое допустимо для этой среды.
- **Max. Link (62.5/125um)[m]**
Отображает максимальное расстояние в метрах, которое допустимо для этой среды.

Следующая таблица отображает значения используемого в этом порте вставного трансивера SFP:

Примечание

Отклонения отображаемых значений от технических данных

Отображаемые значения для минимальной и максимальной мощности передачи или приёма могут незначительно отличаться от значений, указанных в руководстве по эксплуатации. Определяющими являются значения, отображаемые на странице WBM.

- **Temperature[°C]**
Отображает температуру интерфейса.
- **Voltage[V]**
Отображает приложенное к интерфейсу напряжение в вольтах.
- **Current[mA]**
Отображает потребляемый интерфейсом ток в миллиамперах.
- **Rx Power[μW]/Rx Power[dBm]**
Отображает мощность приёма интерфейса в мкВт/дБмВт.
- **Tx Power[μW]/Tx Power[dBm]**
Отображает мощность передачи интерфейса в МкВт/дБмВт.
- **Столбец Current**
Отображает текущее значение.
- **Столбец Low**
Отображает самое низкое значение.
- **Столбец High**
Отображает самое высокое значение.

6.5 Меню «Layer 2»

6.5.1 Configuration

Конфигурация Layer 2

На этой странице выполняется базовая конфигурация функций Layer 2. На соответствующих страницах конфигурации этих функций возможны более подробные настройки. На страницах конфигурации можно также проверить настройки.

Примечание

Отображаемые параметры частично зависят от функций и устройств.

Layer 2 Configuration

☒ Dynamic MAC Aging

Redundancy Type: Ring with RSTP ▼

Redundancy Mode: MRP Auto-Manager ▼

☐ Standby

☐ MRP Interconnection

☐ Passive Listening

☒ RMON

Dynamic Multicast: - ▼

☐ GVRP

☐ Mirroring

☒ Loop Detection

PTP: off ▼

☐ RSTP+

Set Values
Refresh

Описание отображаемых полей

- **Dynamc MAC Aging**
Активируйте или деактивируйте механизм «Aging». Дополнительные настройки выполняются в пункте меню Layer 2 > Dynamic MAC Aging.
- **Redundancy Type**
Доступны следующие настройки:
 - «-» (деактивировано)
Функция резервирования активирована.
 - Spanning Tree
При выборе этой опции в раскрывающемся списке «Redundancy Mode» можно задать нужный режим резервирования.
 - Ring
При выборе этой опции в раскрывающемся списке «Redundancy Mode» можно задать нужный режим резервирования.
 - Ring with RSTP
При выборе этой опции режим совместимости для Spanning Tree фиксированно устанавливается на RSTP. В раскрывающемся списке «Redundancy Mode» выберите режим кольцевого резервирования.
Текущую настройку можно изменить в меню «Ring Redundancy» и «Spanning Tree».

Примечание

Ограничение для портов в случае опции «Ring with RSTP»

При активации опции «Ring with RSTP» в Spanning Tree не допускается присутствие следующих портов:

- Кольцевые порты
 - Порты Standby
 - Порты сопряжения для режима ожидания
 - Порты MRP Interconnection
-

- **RSTP+**
Активирует RSTP+. Это поле опции можно активировать только в том случае, если в качестве процедуры резервирования сконфигурирована MRP.

- **Redundancy Mode**

Если в раскрывающемся списке «Redundancy Type» выбрать вариант «Ring» или «Ring with RSTP», появятся следующие возможности для выбора:

- **Automatic Redundancy Detection**
Выберите эту настройку, чтобы выполнить автоматическое конфигурирование режима работы с резервированием.
В режиме «Automatic Redundancy Detection» устройство автоматически определяет, имеется ли в кольцевой сети устройство с ролью «HRP Manager». В этом случае устройство принимает на себя роль «HRP Client».
Если устройство с ролью HRP Manager найти не удаётся, то все устройства с настройкой «Automatic Redundancy Detection» или «MRP Auto-Manager» определяют между собой, какое устройство примет на себя роль «MRP Manager». При этом роль «MRP Manager» всегда принимает на себя устройство с наименьшим MAC-адресом. Остальные устройства автоматически переходят в режим «MRP Client».
- **MRP Auto-Manager**
В режиме «MRP Auto Manager» устройства определяют между собой, какое устройство примет на себя роль «MRP Manager». При этом роль «MRP Manager» всегда принимает на себя устройство с наименьшим MAC-адресом. Остальные устройства автоматически переходят в режим «MRP Client».
В отличие от настройки «Automatic Redundancy Detection» устройства не могут определить, имеется ли в кольцевой сети устройство с ролью «HRP Manager».
- **MRP Client**
Устройство принимает на себя роль MRP Client.
- **MRP Manager**
Устройство принимает на себя роль MRP Manager. Устройство не может автоматически принять на себя роль клиента.
- **HRP Client**
Устройство принимает на себя роль HRP Client.
- **HRP Manager**
Устройство принимает на себя роль HRP Manager.
При проектировании HRP-кольца одно устройство необходимо настроить в качестве «HRP Manager». Для остальных устройств необходимо выбрать настройку «HRP Client» или «Automatic Redundancy Detection».

Если в раскрывающемся списке «Redundancy Type» выбрать вариант «Spanning Tree», появятся следующие возможности для выбора:

- **STP**
Активирует Spanning Tree Protocol (STP). Типичное время реконфигурации для Spanning Tree составляет от 20 до 30 секунд. Дополнительные настройки выполняются в пункте меню Layer 2 > Spanning Tree.

- RSTP
Активирует Rapid Spanning Tree Protocol (RSTP). Если на порте распознан пакет Spanning Tree, то этот порт переключается с RSTP обратно на Spanning Tree. Дополнительные настройки выполняются в пункте меню Layer 2 > Spanning Tree.

Примечание

В случае RSTP возможно кратковременное образование петли с удвоением пакетов или ремонт пакетов. Если это неприемлемо в вашем варианте применения, то следует использовать более медленную стандартную процедуру Spanning Tree.

- MSTP
Активирует Multiple Spanning Tree Protocol (MSTP). Дополнительные настройки выполняются в пункте меню Layer 2 > Spanning Tree.

Если в раскрываемом списке «Redundancy Type» выбрать вариант «Ring with RSTP», то будет показан текущий режим резервирования Spanning Tree и кольцевого резервирования.

- **Standby**
Активируйте или деактивируйте функцию резервирования в режиме ожидания. Дополнительные настройки выполняются в пункте меню Layer 2 > Ring Redundancy.
- **MRP Interconnection**
Активируйте или деактивируйте функцию MRP Interconnection. Дополнительные настройки выполняются в пункте меню Layer 2 > Ring Redundancy > MRP Interconnection. Функцию MRP Interconnection можно активировать только при выполнении следующих требований:
 - Кольцевое резервирование включено.
 - В качестве режима кольцевого резервирования установлено «MRP Auto Manager» или «MRP Client».
 - Имеется активированное соединение MRP Interconnection.

Примечание

Настройте режим кольцевого резервирования «MRP Auto Manager» для двух устройств в каждом кольце, чтобы обеспечить возможность немедленной перенастройки кольца MRP в случае отказа даже одного из устройств.

- **Passive Listening**
Активируйте или деактивируйте функцию Passive Listening.
С помощью функции Passive Listening можно соединять сети Spanning Tree с MRP- или HRP-кольцами. Участники кольца перенаправляют BPDU Spanning Tree BPDU и тем самым реагируют на изменения топологии. При получении кадра смены топологии таблица MAC-адресов очищается.

- **RMON**

При активации этого поля опции функция Remote Monitoring (RMON) позволяет собирать, подготавливать и считывать по SNMP диагностические данные со станции сетевого управления, которая также поддерживает RMON. Эти диагностические данные, например профили нагрузки портов, позволяют своевременно выявлять и устранять проблемы в сети. Счётчики «Ethernet Statistics Counter» частично являются компонентом функции RMON. Если деактивировать RMON, то счётчик «Ethernet Statistic Counter» в пункте меню Information > Ethernet Statistics перестанет обновляться.

- **Dynamic Multicast**

Допускаются следующие настройки:

- «-» (деактивировано)
- IGMP Snooping
Активирует IGMP (Internet Group Management Protocol). Дополнительные настройки выполняются в пункте меню Layer 2 > Multicast > IGMP.
- GMRP
Активирует GMRP (GARP Multicast Registration Protocol). Дополнительные настройки выполняются в пункте меню Layer 2 > Multicast > GMRP.

Примечание

GMRP и IGMP невозможно использовать одновременно.

- **GVRP**

Активируйте или деактивируйте GVRP (GARP VLAN Registration Protocol). Дополнительные настройки выполняются в пункте меню Layer 2 > VLAN > GVRP.

- **Mirroring**

Активируйте или деактивируйте зеркалирование портов. Дополнительные настройки выполняются в пункте меню Layer 2 > Mirroring.

- **Loop Detection**

Активируйте или деактивируйте функцию Loop Detection. Она даёт возможность распознавать петли в сети. Дополнительные настройки выполняются в пункте меню Layer 2 > Loop Detection.

- **PTP**

Допускаются следующие настройки:

- off
Устройство не перенаправляет PTP-сообщения.
- transparent
Устройство не синхронизируется с устройством Master времени, однако перенаправляет PTP-сообщения между устройством Master времени и подлежащими синхронизации устройствами Slave.

Дополнительные настройки выполняются в пункте меню Layer 2 > PTP.

6.5.2 Quality of Service (QoS)

Для этого см. также главу «Технические основы», раздел «Quality of Service (Страница 90)».

6.5.2.1 General

Приоритеты передачи

На этой странице можно задавать приоритеты различных кадров. Кроме того, в зависимости от приоритета можно настраивать, в соответствии с каким методом будет определяться последовательность обработки кадров.

Описание отображаемых значений

Страница содержит следующие поля:

- **Broadcast Priority**
Задайте приоритет кадра широковещательной рассылки. Коммутатор отсортировывает кадр в соответствии с этим приоритетом в очередь (Queue). Распределение приоритетов по очередям конфигурируется в пункте меню Layer 2 > QoS > CoS Map.
- **Agent Priority**
Задайте приоритет кадра агента. Коммутатор отсортировывает кадр в очередь в соответствии с этим приоритетом. Распределение приоритетов по очередям конфигурируется в пункте меню Layer 2 > QoS > CoS Map.
- **Scheduling Mode**
Выберите, в какой последовательности кадры будут обрабатываться в очередях.
 - Strict Queueing
До тех пор, пока в очереди находятся кадры с высоким приоритетом, будут обрабатываться только такие кадры.
 - Weighted Fair Queueing
Даже в том случае, если в очереди находятся кадры с высоким приоритетом, иногда будут обрабатываться кадры и с низким приоритетом.

Примечание

Устройства, в которых схему обработки невозможно настроить, используют метод «Strict Queueing».

Порядок действий при конфигурации

1. Выберите в раскрывающихся списках «Broadcast Priority» и «Agent Priority», кадры с каким приоритетом будут подвергаться внутренней обработке.
2. Выберите в раскрывающемся списке «Scheduling Mode», в соответствии с каким методом будет определяться последовательности обработки кадров.
3. Щёлкните кнопку «Set values».

6.5.2.2 CoS Map

CoS Map

На этой странице можно распределять приоритеты CoS по различным очередям.

COS	Queue
0	2
1	1
2	1
3	2
4	3
5	3
6	4
7	4

Set Values Refresh

Описание отображаемых полей

Таблица состоит из следующих столбцов:

- **CoS**
Отображает приоритет CoS входящего кадра.
- **Queue**
Выберите в раскрывающемся списке очередь, которой будет присвоен приоритет CoS.
Чем выше номер очереди, тем выше приоритет обработки.

Классы услуг (CoS) по умолчанию распределены по очередям следующим образом:

COS	Устройства с 4 очередями	Устройства с 8 очередями
0	Очередь 2	Очередь 2
1	Очередь 1	Очередь 1
2	Очередь 1	Очередь 3
3	Очередь 2	Очередь 4

COS	Устройства с 4 очередями	Устройства с 8 очередями
4	Очередь 3	Очередь 5
5	Очередь 3	Очередь 6
6	Очередь 4	Очередь 7
7	Очередь 4	Очередь 8

Порядок действий при конфигурации

1. Для каждого значения в столбце «CoS» выберите очередь в раскрывающемся списке «Queue».
2. Щёлкните кнопку «Set values».

6.5.2.3 DSCP Mapping

Очередь DSCP

На этой странице можно распределять приоритеты DSCP по различным очередям (Queues).

Differentiated Services Code Point (DSCP) Mapping

General | CoS Map | **DSCP Map** | QoS Trust | CoS Port Remap

DSCP min	DSCP max	Queue	Copy to Table
0	63	1	Copy to Table

DSCP	Queue
0	1
1	1
2	1
3	1
4	1

Set Values Refresh

Описание отображаемых значений

Таблица 1 состоит из следующих столбцов:

- **DSCP min**
В раскрывающемся списке выберите минимальное значение диапазона кодов DSCP, которым необходимо присвоить очередь.
- **DSCP max**
В раскрывающемся списке выберите максимальное значение диапазона кодов DSCP, которым необходимо присвоить очередь.

- **Queue**
Выберите в раскрывающемся списке очередь перенаправления (приоритет отправки), которая будет присвоена диапазону кодов DSCP.
- **Copy to Table**
При нажатии этой кнопки коды DSCP в указанном диапазоне будут присвоены выбранной очереди перенаправления (приоритет отправки).

Таблица 2 состоит из следующих столбцов:

- **DSCP**
Отображает приоритет DSCP входящего кадра.
- **Queue**
Выберите в раскрывающемся списке очередь, которая будет присвоена приоритету DSCP.
Чем выше номер очереди, тем выше приоритет обработки.

Приоритеты DSCP по умолчанию распределены по очередям следующим образом:

Коды DSCP	Устройства с 4 очередями
0 - 15	Очередь 1
16 - 31	Очередь 2
32 - 47	Очередь 3
48 - 63	Очередь 4

Коды DSCP	Устройства с 8 очередями
0 - 7	Очередь 2
8 - 15	Очередь 1
16 - 23	Очередь 3
24 - 31	Очередь 4
32 - 39	Очередь 5
40 - 47	Очередь 6
48 - 55	Очередь 7
56 - 63	Очередь 8

Порядок действий при конфигурации

1. Выберите для каждого значения столбца «DSCP» очередь в раскрывающемся списке «Queue».
2. Щёлкните кнопку «Set values».

6.5.2.4 QoS Trust

Установите приоритет

На этой странице можно настроить по портам процедуру, в соответствии с которой пересылаемым кадрам назначается приоритет.

Quality of Service (QoS) Trust Mode		
General CoS Map DSCP Map QoS Trust CoS Port Remap		
Port	Trust Mode	Copy to Table
All ports	No Change	Copy to Table
Port	Trust Mode	
P0.1	Trust COS-DSCP	
P0.2	Trust COS-DSCP	
P0.3	Trust COS-DSCP	
P0.4	Trust COS-DSCP	
Set Values Refresh		

Описание отображаемых значений

Таблица 1 состоит из следующих столбцов:

- **Port**
Отображает, что настройка действительна для всех портов в таблице 2.
- **Trust Mode**
Выберите в раскрывающемся списке настройку. Имеются следующие варианты настройки:
 - No Trust
 - Trust COS
 - Trust DSCP
 - Trust COS-DSCP
 - No Change
 Таблица 2 осталась без изменений.
- **Copy to Table**
Если нажать кнопку, то настройка будет применена для всех портов таблицы 2.

Таблица 2 состоит из следующих столбцов:

- **Port**
Показывает конфигурируемые порты.
Обозначение порта складывается из номера модуля и номера порта, например, порт 0.1 означает модуль 0, порт 1.

- **Trust Mode**
Выберите в раскрывающемся списке необходимый режим:

Примечание

Приоритет порта получения конфигурируется на странице Layer 2 > VLAN > Port Based VLAN.

Настраивается назначение следующих приоритетов очереди на странице Layer 2 > QoS > CoS Map:

- порт получения
- Tег VLAN
- кадр широковещательной рассылки и агентский кадр

Настраивается назначение приоритета DSCP в очереди на странице Layer 2 > QoS > DSCP Mapping:

- No Trust
Коммутатор сортирует входящие кадры в очередь в соответствии с приоритетом порта получения.
Если в заголовке IP есть значение DSCP, оно не учитывается. Когда имеется тег VLAN, его значение приоритета заменяется значением приоритета порта получения.
- Trust COS
Если входящий кадр содержит тег VLAN, коммутатор сортирует его в очередь в соответствии с этим приоритетом.
Если кадр не содержит тег VLAN, коммутатор сортирует кадр в очередь в соответствии с приоритетом порта получения.
Если в заголовке IP есть значение DSCP, оно не учитывается.
- Trust DSCP
Если входящий кадр содержит приоритет DSCP, коммутатор сортирует его в очередь в соответствии с этим приоритетом.
Если кадр не содержит приоритета DSCP, коммутатор сортирует кадр в очередь в соответствии с приоритетом порта получения.
Когда кадр содержит тег VLAN, это не учитывается.
- Trust COS-DSCP
В случае входящего кадра выполняется последовательная проверка для определения, какой приоритет он содержит.
Если кадр содержит приоритет DSCP, он обрабатывается как в режиме «Trust DSCP».
Если кадр не содержит приоритета DSCP, коммутатор проверяет, содержит ли кадр тег VLAN. Если он содержит тег VLAN, коммутатор сортирует кадр в очередь в соответствии с приоритетом.
Если кадр не содержит ни приоритета DSCP, ни тега VLAN, коммутатор сортирует кадр в очередь в соответствии с приоритетом порта получения.

Порядок действий при конфигурации

1. Выберите в раскрывающемся списке необходимый Trust Mode.
2. Щёлкните кнопку «Set values».

6.5.2.5 CoS Port Remap

Изменить приоритет при отправке

На этой странице можно изменить зависимость между приоритетом при отправлении и получении кадра. Новый приоритет влияет только на следующие устройства, принимающие кадр.

Class of Service (CoS) Port Remap

General CoS Map DSCP Map QoS Trust CoS Port Remap

☐ CoS Remap

Port	Priority 0	Priority 1	Priority 2	Priority 3	Priority 4	Priority 5	Priority 6	Priority 7	Copy to Table		
All ports	No Change	▼	No Change	▼	No Change	▼	No Change	▼	No Change	▼	Copy to Table

Port	Priority 0	Priority 1	Priority 2	Priority 3	Priority 4	Priority 5	Priority 6	Priority 7								
P0.1	0	▼	1	▼	2	▼	3	▼	4	▼	5	▼	6	▼	7	▼
P0.2	0	▼	1	▼	2	▼	3	▼	4	▼	5	▼	6	▼	7	▼
P0.3	0	▼	1	▼	2	▼	3	▼	4	▼	5	▼	6	▼	7	▼
P0.4	0	▼	1	▼	2	▼	3	▼	4	▼	5	▼	6	▼	7	▼

Set Values Refresh

Описание отображаемых полей

Страница содержит следующие поля:

- **CoS Remap**
Включите или отключите отправку кадров с изменёнными приоритетами согласно таблице 2.

Таблица 1 состоит из следующих столбцов:

- **Port**
Показывает, что настройки действительны для всех портов в таблице 2.
- **Priority 0 - 7**
Приоритет столбца обозначает тот приоритет, с которым был получен кадр.
 - 0 - 7
Выберите приоритет, с которым должен отправляться кадр.
 - No Change
В таблице 2 без изменений.
- **Copy to Table**
Если нажать кнопку, то настройка будет применена для всех портов таблицы 2.

6.5 Меню «Layer 2»

Таблица 2 состоит из следующих столбцов:

- **Port**
Отображает все доступные порты. Порт складывается из номера модуля и номера порта, например, порт 0.1 означает модуль 0, порт 1.
- **Priority 0 - 7**
Приоритет столбца обозначает тот приоритет, с которым был получен кадр. В раскрывающемся списке выберите приоритет, с которым должен отправляться кадр.

Порядок действий при конфигурации

1. Установите флажок для «CoS Remap».
2. С помощью раскрывающегося списка выберите для каждого приоритета приёма на порте приоритет отправки.
3. Щёлкните кнопку «Set values».

6.5.3 Rate Control

Ограничение скорости передачи входящих и исходящих данных

На этой странице можно настроить ограничение скорости для отдельных портов. Можно указать категории пакетов, для которых должны применяться эти предельные значения.

Rate Control

	Limit Ingress Unicast (DLF)	Limit Ingress Broadcast	Limit Ingress Multicast	Limit Ingress Unicast	Total Ingress Rate pkts/s	Egress Rate kb/s	Copy to Table
All ports	No Change	No Change	No Change	No Change	No Change	No Change	Copy to Table

Port	Limit Ingress Unicast (DLF)	Limit Ingress Broadcast	Limit Ingress Multicast	Limit Ingress Unicast	Total Ingress Rate pkts/s	Egress Rate kb/s
P0.1	☐	☐	☐	☐	0	0
P0.2	☐	☐	☐	☐	0	0
P0.3	☐	☐	☐	☐	0	0
P0.4	☐	☐	☐	☐	0	0
P1.1	☐	☐	☐	☐	0	0

Set Values
Refresh

Описание отображаемых значений

Таблица 1 состоит из следующих столбцов:

- **1-й столбец**
Отображает, что настройки действительны для всех портов.
- **Ingress Unicast(DLF)-Limit / Ingress Broadcast-Limit / Ingress Multicast-Limit / Ingress Unicast-Limit**
Выберите в раскрывающемся списке нужный параметр.
 - Enabled: Включает функцию.
 - Disabled: Деактивирует функцию
 - No Change: Настройка в таблице 2 осталась без изменений.
- **Total Ingress Rate kb/s**
Задайте скорость передачи данных для всех входящих пакетов. Если введено значение «No Change», запись в таблице 2 не изменяется.
- **Egress Rate kb/s**
Задать скорость передачи данных для всех исходящих пакетов. Если введено значение «No Change», запись в таблице 2 остаётся неизменной.
- **Copy to Table**
Если нажать данную кнопку, то настройки будут применены для всех портов в Таблице 2.

Таблица 2 состоит из следующих столбцов:

- **Port**
Отображает все доступные порты. Порт складывается из номера модуля и номера порта, например, порт 0.1 означает модуль 0, порт 1.
- **Ingress Unicast (DLF)-Limit**
Активируйте или деактивируйте скорость передачи данных, чтобы ограничить входящие одноадресные пакеты с неразрешёнными адресами (Destination Lookup Failure).
- **Ingress Broadcast-Limit**
Активируйте или деактивируйте скорость передачи данных, чтобы ограничить входящие широковещательные пакеты.
- **Ingress Multicast-Limit**
Активируйте или деактивируйте скорость передачи данных, чтобы ограничить входящие многоадресные пакеты.
- **Ingress Unicast-Limit**
Активируйте или деактивируйте скорость передачи данных, чтобы ограничить входящие одноадресные пакеты.

- **Total Ingress Rate kb/s**

Задайте скорость передачи данных для всех входящих пакетов.

Примечание

Устройство ограничивает трафик до заданного значения, только в том случае если для соответствующего порта установлен хотя бы один флажок в следующих столбцах:

- Ingress Broadcast -Limit
- Ingress Multicast -Limit
- Ingress Unicast -Limit

В том случае если флажок не установлен, входящий трафик не ограничивается, даже если в поле «Total Ingress Rate pkts/s» введено значение. Когда установлено несколько флажков, решающее значение для ограничения трафика имеет сумма пакетов данных из всех активированных категорий.

- **Egress Rate kb/s**

Задайте скорость передачи данных для всех исходящих пакетов.

Примечание

Округление значений, отклонение от заданного значения

При вводе данных убедитесь, что интерфейс WBM округляет до правильных значений.

Если заданы значения для Total Ingress Rate и Egress Rate, то фактические значения во время эксплуатации могут незначительно отличаться от установленных значений.

Порядок действий при конфигурации

1. В строке конфигурируемого порта введите соответствующие значения в столбцы «Total Ingress Rate» и «Egress Rate».
2. Чтобы применить ограничение для входящих пакетов, установите флажки в строке. Значение в столбце «Egress Rate» используется для исходящих пакетов.
3. Щёлкните кнопку «Set values».

6.5.4 VLAN

6.5.4.1 Общая информация

Страница конфигурации VLAN

На этой странице задаётся, будет ли устройство прозрачно пересылать пакеты с тегами VLAN (режим без поддержки IEEE 802.1D/VLAN) или с учётом информации о VLAN (режим с поддержкой IEEE 802.1Q/VLAN). Когда устройство находится в режиме «802.1Q VLAN Bridge», можно задать сети VLAN и указать использование портов.

Параметры настройки на этой странице зависят от того, что было выбрано в поле «Base Bridge Mode».

Примечание

Изменение идентификатора агента VLAN

Если ПК для настройки напрямую подключён к устройству через Ethernet, и изменяется идентификатор сети VLAN агента (Agent VLAN ID), то после этого изменения устройство больше не будет доступно через Ethernet.

Virtual Local Area Network (VLAN) General

General GVRP Port Based VLAN

Bridge Mode: Customer

Base Bridge Mode: 802.1Q VLAN Bridge

Update Priority

VLAN ID:

Select	VLAN ID	Name	Status	Private VLAN Type	Primary VLAN ID	Priority	Update Priority	P0.1	P0.2
☐	1		Static	-		Do not force	☐	U	U
☐	2		Static	-		Do not force	☐	-	-

2 entries.

Create Delete Set Values Refresh

Описание отображаемых полей

Страница содержит следующие поля:

- **Bridge Mode**

Задайте роль устройства. Существуют следующие роли:

- Customer
Когда используется устройство с ролью «Customer», оно ведёт себя как стандартный IE-коммутатор.
- Provider
Когда используется устройство с ролью «Provider», помимо свойств роли «Customer», у него имеется возможность управления внешними тегами VLAN. В этой роли можно использовать функцию туннеля VLAN Q-in-Q.

Примечание

Роль «Provider» оказывает следующее влияние на тег VLAN: Все пакеты данных, которые отправляются не из порта доступа, получают тег VLAN. Если конфигурация VLAN других устройств не настроена соответствующим образом, могут возникнуть петли сети или сегменты сети больше не будут доступны.

- **Base Bridge Mode**

Примечание

Переключение режима Base Bridge Mode

Обратите внимание на раздел «Переключение режима Base Bridge Mode» в этой главе. В разделе описывается, как переключение влияет на существующую конфигурацию.

Выберите в раскрывающемся списке нужный режим: Возможны следующие режимы:

- 802.1Q VLAN Bridge
Переключает устройство в режим «VLAN-aware». В этом режиме учитывается информация о состоянии VLAN.
- 802.1D Transparent Bridge
Переключает устройство в режим «VLAN-unaware». В этом режиме теги VLAN не изменяются, а прозрачно пересылаются. Приоритет VLAN оценивается для технологии CoS. В этом режиме нет возможности создавать какие-либо сети VLAN. Доступна только одна сеть Management VLAN: VLAN 1.

- **Update Priority**

Когда активирован этот флажок, значение в столбце таблицы «Priority» вводится как новый Class of Service в тегах VLAN всех входящих кадров для данной сети VLAN.

- **VLAN ID**

Введите идентификатор сети VLAN в поле ввода «VLAN ID».
Диапазон значений: 1 ... 4094

Таблица состоит из следующих столбцов:

- **Select**
Выберите строку, которую необходимо удалить.
- **VLAN ID**
Отображает идентификатор сети VLAN. Идентификатор VLAN это (число от 1 до 4094), которое может быть задано только один раз при создании блока данных и не может быть изменено впоследствии. Для того чтобы внести изменения, необходимо удалить и воссоздать весь блок данных.
- **Name**
Введите имя для сети VLAN. Имя носит только информативный характер и не влияет на конфигурацию.
Длина: макс. 32 символа
- **Status**
Отображает тип состояния записи во внутренней таблице фильтра порта. Значение «Static», означает, что сеть VLAN была настроена пользователем как статическая.
- **Private VLAN Typ**
Отображает тип сети PVLAN.
- **Primary VLAN ID**
Отображает для вторичных сетей Secondary PVLANs идентификатор связанных первичных сетей Primary PVLANs.
- **Priority**
Выберите приоритет, который будет применяться в качестве нового класса обслуживания (CoS) для всех входящих кадров этой VLAN. Кадры далее обрабатываются коммутатором в соответствии с выбранным приоритетом, независимо от приоритета порта или приоритета для нетегированных кадров. Теги VLAN, содержащиеся в кадре, не изменяются.
Приоритет кадров останется неизменным «Do not force», если выбрать данный пункт. Кадры получают приоритет в соответствии с приоритетом порта или тегом VLAN.

- **Update Priority**

В этом столбце отображается состояние флажка «Update Priority» вверху страницы для всех сетей VLAN. Специальная настройка для сети VLAN недоступна.

- **Список портов**

задайте использование портов. Существуют следующие возможности:

- «-»
Порт не является участником данной сети VLAN.
При первоначальной настройке всем портам присваивается идентификатор «-».
- M
Порт является участником сети VLAN. Пакеты, отправленные в этой сети VLAN, пересылаются с соответствующим тегом VLAN.
- R
Порт является участником сети VLAN. Регистрация осуществляется с помощью пакета GVRP.
- U (Заглавная буква)
Порт является нетегированным участником VLAN. Пакеты, отправленные в этой сети VLAN, пересылаются без тега VLAN. С этого порта отправляются пакеты без тега VLAN.
- u (Строчная буква)
Порт является нетегированным участником сети VLAN, но сеть VLAN не сконфигурирована как порт VLAN. Пакеты, отправленные в этой сети VLAN, пересылаются без тега VLAN.
- F
Порт не является участником данной сети VLAN и не может стать участником этой VLAN, даже если он будет настроен как магистральный порт.
- T
Эта опция только отображается и не может быть выбрана в интерфейсе WBM.
Данный порт является магистральным портом и, таким образом, стал участником всех сетей VLAN.

Переключение режима Base Bridge Mode

VLAN-unaware (802.1D прозрачный мост) → VLAN-aware (802.1Q VLAN мост)

Если изменить режим Base Bridge Mode с VLAN-unaware на VLAN-aware, то это приведёт к следующим последствиям:

- Удаляются все статические и динамические записи одноадресной рассылки.
- Удаляются все статические и динамические записи многоадресной рассылки.
- В связующем дереве возможно настроить следующую совместимость протокола: STP, RSTP и MSTP.

VLAN-aware (802.1Q VLAN мост) → VLAN-unaware (802.1D прозрачный мост)

Если изменить режим Base Bridge Mode с VLAN-aware на VLAN-unaware, то это приведёт к следующим последствиям:

- Удаляются все конфигурации VLAN.
- Создаётся управляющая VLAN: VLAN 1.

- Удаляются все статические и динамические записи одноадресной рассылки.
- Удаляются все статические и динамические записи многоадресной рассылки.
- В связующем дереве возможно настроить следующую совместимость протокола: STP и RSTP.
- Вы не можете возможности использовать протокол GVRP.
- Нет возможности использовать гостевую VLAN.
- Сервер RADIUS не может принять назначение VLAN.
- Нет возможности настроить тип порта.
- Определённые правила доступа должны быть действительны для всех VLAN. На странице Security > Management ACL необходимо определить значение «1-4094» для параметра «VLANs Allowed».

Мост 802.1Q VLAN: Важные правила для сети VLAN

При настройке и эксплуатации сетей VLAN необходимо учитывать следующие правила:

- Пакеты с VLAN ID «0» обрабатываются как нетегированные пакеты, но сохраняют своё значение приоритета.
- По умолчанию все порты устройства отправляют пакеты без тега VLAN, чтобы конечный пользователь мог получать эти пакеты.
- В устройствах SCALANCE X для всех портов предварительно задан идентификатор сети VLAN «1».
- Когда конечный пользователь подключён к порту, исходящие пакеты должны отправляться без тега (статический порт доступа). Когда в порте есть ещё один коммутатор, пакет должен быть помечен тегом (Trunk Port).

Порядок действий при конфигурации

1. Когда «802.1Q VLAN Bridge» не настроен, выберите запись «802.1Q VLAN Bridge» в раскрывающемся списке «Base Bridge Mode». Щёлкните кнопку «Set values».
2. Введите идентификатор сети VLAN в поле ввода "VLAN ID".
3. Щёлкните кнопку «Create». В таблице создаётся новая запись. Поля стандартно заполнены знаком «-».
4. При необходимости введите имя для сети VLAN.
5. Задайте использование портов в сети VLAN. Например, если выбрать «М», порт станет участником сети VLAN. Пакеты, отправленные в этой сети VLAN, пересылаются с соответствующим тегом VLAN.
6. Щёлкните кнопку «Set values».

6.5.4.2 GVRP

Конфигурация функции протокола GVRP

Другое устройство может зарегистрироваться с определённым VLAN ID на порте устройства через пакет GVRP. Другое устройство может, например, быть конечным пользователем или коммутатором. Устройство также может отправлять пакеты GVRP через этот порт.

На этой странице можно активировать функцию GVRP для каждого порта.

Описание отображаемых полей

Страница содержит следующие поля:

- **GVRP**

Активируйте или деактивируйте функцию «GVRP».

Таблица 1 состоит из следующих столбцов:

- **1-й столбец**

Отображает, что настройки действительны для всех портов в таблице 2.

- **Setting**

Выберите в раскрывающемся списке настройку. Имеются следующие возможности настройки:

- Enabled
Активирует отправку пакетов GVRP.
- Disabled
Деактивирует отправку пакетов GVRP.
- No Change
В таблице 2 без изменений.

- **Copy to Table**

При нажатии кнопки настройка будет скопирована для всех портов в таблице 2.

Таблица 2 состоит из следующих столбцов:

- **Port**
Отображает все доступные порты. Порт складывается из номера модуля и номера порта, например, порт 0.1 означает модуль 0, порт 1.
- **Setting**
Активируйте или деактивируйте отправку пакетов GVRP.

Порядок действий при конфигурации

1. Установите флажок «GVRP».
2. Установите флажок рядом с каждым портом в столбце «Setting», чтобы активировать или деактивировать GVRP для данного порта.
Повторите процедуру для каждого порта, для которого необходимо активировать или деактивировать функцию.
3. Щёлкните кнопку «Set Values».

6.5.4.3 VLAN на базе портов

Обработка полученных пакетов

На этой странице задаётся конфигурация свойств порта для приёма пакетов.

Возможно настроить параметры на этой странице, только в том случае, если ранее на вкладке «General» ранее был выбран режим «Base Bridge Mode» «802.1Q VLAN Bridge».

Port Based Virtual Local Area Network (VLAN) Configuration

General
GVRP
Port Based VLAN

	Priority	Port VID	Acceptable Frames	Ingress Filtering	Copy to Table
All ports	No Change	No Change	No Change	No Change	Copy to Table

Port	Priority	Port VID	Acceptable Frames	Ingress Filtering
P0.1	0	VLAN1	All	☐
P0.2	0	VLAN1	All	☐
P0.3	0	VLAN1	All	☐

Set Values
Refresh

Описание отображаемых полей

Таблица 1 состоит из следующих столбцов:

- **1-й столбец**
Отображает, что настройки действительны для всех портов.
- **Priority / Port VID / Acceptable Frames / Ingress Filtering**
Выберите в раскрывающемся списке настройку. Если выбрано значение «No Change», то запись в таблице 2 не изменяется.
- **Copy to Table**
При нажатии кнопки настройка будет скопирована для всех портов в таблице 2.

Таблица 2 состоит из следующих столбцов:

- **Port**
Отображает доступные порты. Порт складывается из номера модуля и номера порта, например, порт 0.1 означает модуль 0, порт 1.
- **Priority**
Приоритет класса обслуживания (CoS), используемый в теге VLAN. Когда получен пакет без тега, ему присваивается этот приоритет. Приоритет определяет, как этот пакет обрабатывается по сравнению с другими пакетами.
Всего существует восемь приоритетов со значениями от 0 до 7, при этом 7 соответствует высшему приоритету (приоритет порта IEEE 802.1P).
В раскрывающемся списке выберите приоритет, с которым должен отправляться нетегированный пакет.
- **Port VID**
Выберите в раскрывающемся списке VLAN ID. Могут быть выбраны только те VLAN ID, которые были заданы на странице VLAN > General.
Когда полученный пакет не имеет тега VLAN, тег с указанным здесь VLAN ID добавляется и отправляется в соответствии с протоколом на порт.

- **Acceptable Frames**

Задайте типы принимаемых пакетов. Существуют следующие альтернативы:

- Tagged Frames Only
Устройство отклоняет все тегированные пакеты. В противном случае правила переадресации применяются в соответствии с конфигурацией.
- All
Устройство пересылает все пакеты.
- Untagged and Priority Tagged Only
Устройство отклоняет все тегированные пакеты. Устройство пересылает все нетегированные пакеты, а также пакеты с приоритетом (Priority Tagged Frames). В противном случае правила переадресации применяются в соответствии с конфигурацией.
Когда сконфигурирован режим Bridge Mode «Provider», данная настройка означает для устройства, что оно обрабатывает все входящие пакеты как нетегированные пакеты.

- **Ingress Filtering**

Задайте, будет ли оцениваться VID полученных пакетов.

Существуют следующие возможности:

- Активировано
VLAN ID полученных пакетов определяет их пересылку: для пересылки пакеты с тегом VLAN порт получения должен быть участником той же сети VLAN. На порте получения пакеты из неизвестных VLAN отклоняются.
- Деактивировано
Все пакеты пересылаются.

Порядок действий при конфигурации

1. В строке конфигурируемого порта щёлкните по соответствующему полю в таблице, чтобы сконфигурировать его.
2. Введите необходимые значения в поля ввода.
3. Выберите в раскрывающемся списке необходимые значения.
4. Щёлкните кнопку «Set values».

6.5.5 Private VLAN

6.5.5.1 General

Страница конфигурации частной сети VLAN

На этой странице можно задать типы сетей PVLAN и назначить для вторичной сети Secondary PVLANs первичную сеть Primary PVLAN.

VLAN ID	Private VLAN Type	Primary VLAN ID
1	-	-
10	Primary	-
11	Isolated	10
12	Community	10

Set Values Refresh

Описание отображаемых полей

Таблица состоит из следующих столбцов:

- **VLAN ID**
Отображает идентификатор сети VLAN.
- **Private VLAN Typ**
Задайте тип сети PVLAN.
 - -
Эти сети VLAN не являются частными сетями VLAN.
 - Primary
С помощью этого типа определяется Primary PVLAN. В сети PVLAN можно задать только одну первичную сеть Primary PVLAN. Сеть Primary PVLAN использует ID сети VLAN.
 - Isolated
С помощью этого типа определяется Secondary PVLAN. Устройства внутри Isolated Secondary PVLAN не могут обмениваться данными друг с другом через уровень 2. Сеть Secondary PVLAN имеет специальный VLAN ID.
 - Community
С помощью этого типа определяется Secondary PVLAN. Устройства в этой сети Secondary PVLAN могут обмениваться данными через уровень 2. Сеть Secondary PVLAN имеет специальный VLAN ID.
- **Primary VLAN-ID**
В разделе Secondary PVLANs выберите идентификатор VLAN для сети Primary PVLANs.

Порядок действий при конфигурации

1. Создайте необходимые сети VLAN на странице Layer 2 > VLAN > General.

Примечание

Все вторичные сети Secondary PVLANS должны быть известны на всех IE-коммутаторах PVLAN. Даже когда IE-коммутатор не имеет порта хоста в сети Secondary PVLAN, вторичная сеть Secondary PVLAN должна быть известна на IE-коммутаторе.

2. Перейдите на страницу Layer 2 > Private VLAN> General. Там имеется строка для каждой сети VLAN.
3. Задайте тип сети «Private VLAN» на этой странице.
4. Щёлкните кнопку «Set values».
5. Для вторичных сетей Secondary PVLANS задайте связанные первичные сети Primary PVLAN.
6. Щёлкните кнопку «Set values».
7. Выберите соответствующий тип порта Port Typ для необходимых портов на странице System > Ports > Configuration:
 - Switch-Port PVLAN Promiscuous
 - Switch-Port PVLAN Host
8. Задайте использование портов на странице Layer 2 > VLAN > General.
 - Для случайных портов, подключённых к другому случайному порту, выберите «М» во всех сетях PVLAN.
 - Для случайных портов, которые подключены к оконечному устройству, выберите настройку «и» (строчная буква) во всех сетях PVLAN.
В Primary PVLAN после сохранения настройка автоматически изменяется на «U» (заглавная буква).
 - Выберите настройку «и» (строчная буква) для портов хоста в первичной сети PVLAN и в соответствующей её вторичной сети PVLAN.
В Secondary PVLAN после сохранения настройка автоматически изменяется на «U» (заглавная буква).

Для входящих нетегированных кадров устанавливается идентификатор порта VLAN сети VLAN, в которой порт введён с настройкой «U» (заглавная буква).

6.5.5.2 IP Interface Mapping

Страница конфигурации частной сети VLAN

С помощью этой команды указывается, из каких вторичных сетей Secondary PVLANS должен быть доступен IP-интерфейс первичной сети Primary PVLANS.

Сконфигурируйте IP Interface Mapping для всех функций, для которых оконечное устройство из вторичной сети Secondary PVLAN должно связываться через IP-интерфейс с первичной сетью Primary PVLANS.

Примеры:

- Оконечное устройство во вторичной сети Secondary PVLANs сконфигурировано как DHCP-клиент. Настроен удалённый DHCP-сервер. Коммутатор PVLAN сконфигурирован как агент ретрансляции DHCP. Сконфигурируйте IP-интерфейс в первичной сети PVLAN агента ретрансляции DHCP. Назначьте вторичные сети PVLAN, в которых находятся клиенты DHCP, данному IP-интерфейсу.
- Коммутатор PVLAN сконфигурирован как маршрутизатор. Сконфигурируйте IP-интерфейс в первичной сети PVLAN маршрутизатора. Назначьте данному IP-интерфейсу вторичные сети PVLAN, которые содержат оконечные устройства, которые используют маршрутизатор в качестве шлюза.

Private Virtual Local Area Network (VLAN) IP Interface Mapping

General IP Interface Mapping

Interface:

Secondary VLAN ID:

Select	Interface	Secondary VLAN ID
☐	vlan10	11
☐	vlan10	12

2 entries.

Описание отображаемых полей

Страница содержит следующие поля:

- **Interface**
Выберите первичную сеть Primary PVLAN с IP-интерфейсом.
- **Secondary VLAN ID**
Выберите Secondary VLAN ID, с которого должен быть доступен IP-интерфейс первичной сети Primary PVLANs.

Таблица состоит из следующих столбцов:

- **Select**
Выберите строку, которую необходимо удалить.
- **Interface**
Отображает IP-интерфейс.
- **Secondary VLAN ID**
Отображает Secondary VLAN ID вторичной сети Secondary PVLANs, с которого должен быть доступен IP-интерфейс первичной сети Primary PVLANs.

Порядок действий при конфигурации

1. Создайте IP-интерфейс для первичной сети Primary PVLAN.
2. Выберите первичную сеть Primary PVLAN с IP-интерфейсом.
3. Выберите идентификатор Secondary VLAN ID.
4. Щёлкните кнопку «Create».

6.5.6 Provider Bridge

6.5.6.1 Туннельные порты

Страница конфигурации для Tunnel Ports

На этой странице активируется функция туннеля Q-in-Q VLAN. Пакеты, полученные через Tunnel Port, расширяются добавлением внешнего тегом VLAN, PVID порта.

Virtual Local Area Network (VLAN) Tunnel Ports

Tunnel Ports

Port	Setting	Copy to Table
All ports	No Change ▼	Copy to Table

Port	Setting	
P0.1	☐	
P0.2	☒	
P0.3	☐	
P0.4	☐	

Set Values
Refresh

Описание отображаемых полей

Таблица 1 состоит из следующих столбцов:

- **1-й столбец**
Отображает, что настройки действительны для всех портов в таблице 2.
- **Setting**
Выберите в раскрывающемся списке настройку. Имеются следующие возможности настройки:
 - Enabled
Активирует функцию туннеля Q-in-Q VLAN для всех портов.
 - Disabled
Деактивирует функцию туннеля Q-in-Q VLAN для всех портов.
 - No Change
Таблица 2 осталась без изменений.
- **Copy to Table**
Если нажать данную кнопку, то настройки будут применены для всех портов в Таблице 2.

Таблица 2 состоит из следующих столбцов:

- **Port**
Отображает все доступные порты. Порт складывается из номера модуля и номера порта, например, порт 0.1 означает модуль 0, порт 1.
- **Setting**
Активируйте или деактивируйте функцию для данного порта.

Порядок действий при конфигурации

Для того чтобы настроить порт как туннельный, выполните следующие действия:

1. Перейдите на страницу Layer 2 > VLAN> General.
2. Сконфигурируйте Bridge Mode «Provider».
3. Щёлкните кнопку «Set values».
Настройки порта уровня 2 (VLAN, связующее дерево) сбрасываются до заводских настроек, и устройство перезагружается.
4. Перейдите на страницу Layer 2 > VLAN> General.
5. Введите необходимый идентификатор VLAN.
6. Щёлкните кнопку «Create».
7. Перейдите на страницу Layer 2 > VLAN> Port Based VLAN.
8. В качестве порта выберите VLAN-идентификатор порта созданной сети VLAN.
9. В разделе «Acceptable Frames» для порта выберите настройку «Untagged and Priority Tagged Only».
10. Щёлкните кнопку «Set values».
11. Перейдите на страницу Layer 2 > VLAN> Port Mapping.
12. Выберите настройку «U» (заглавная буква) для порта в необходимой сети VLAN.

13. Выберите настройку «-» для порта во всех других сетях VLAN.
14. Щёлкните кнопку «Set values».
15. Отключите на порте следующие протоколы:
 - На странице Layer 2 > VLAN > GVRP установите флажок напротив «Setting».
 - На странице Layer 2 > Spanning Tree > CIST Port установите флажок напротив «Spanning Tree Status».
 - На странице Layer 2 > Multicast > GMRP установите флажок напротив «Setting».
16. Перейдите на страницу System > Ports > Configuration.
17. Выберите необходимый порт.
18. Выберите Port Тип «Switch-Port VLAN Access».
19. Щёлкните кнопку «Set values».
20. Перейдите на страницу Layer 2 > Provider-Bridge > Tunnel Ports.
21. Установите флажок для требуемого порта.
22. Щёлкните кнопку «Set values».
На странице Layer 2 > VLAN > Port Mapping после сохранения настройка автоматически изменится на «Q».

6.5.7 Mirroring

6.5.7.1 General

На этой странице можно включить или выключить функцию зеркалирования и выполнить основные настройки.

Примечание

Невозможно гарантировать, что при зеркалировании трафика будут зеркалированы все пакеты. Это больше всего зависит от нагрузки на зеркалируемые порты и количества сеансов. Для достижения максимальной точности рекомендуется ограничиться одним сеансом.

Обратите внимание на скорость передачи данных

Если максимальная скорость передачи данных зеркалированного порта выше скорости порта мониторинга, данные могут быть потеряны, и порт мониторинга больше не будет воспроизводить процессы на зеркалированном порте. Порт мониторинга может одновременно зеркалировать несколько портов.

Несколько исходных портов из одной сети VLAN

Если из сети VLAN выбрать более одного исходного порта для зеркалирования исходящего трафика (Egress Mirroring) на основе портов, неизвестные одноадресные и многоадресные пакеты, а также широковещательные пакеты пересылаются на целевой порт только один раз.

Настройки

Mirroring General

General | **Port**

☐ Mirroring
☒ Monitor Barrier

Select	Session ID	Session Type	Status	Dest. Port
☐	1	Port Based	v inactive	- v

1 entry.

Страница содержит следующие поля:

- **Mirroring**
Установите данный флажок, чтобы активировать или деактивировать зеркалирование.

Примечание

Необходимо отключить зеркалирование портов, если к порту мониторинга подключается стандартное оконечное устройство.

- **Monitor Barrier**
Установите данный флажок, чтобы активировать или деактивировать блокировку мониторинга.

Примечание

Влияние блокировки мониторинга

Если включить эту опцию, управление коммутатором через порт мониторинга больше не доступно. Изменяются следующие специфические для порта функции:

- Выключена функция DCP Forwarding.
- Выключена функция протокола LLDP.
- Включены одноадресная, многоадресная и широковещательная блокировка.

Предыдущие состояния этих функций не восстанавливаются после завершения работы блокировки мониторинга. Они сбрасываются до значений по умолчанию и, возможно, их придётся настроить заново.

Можно настроить эти функции вручную, даже если блокировка мониторинга включена. Таким образом, снова разрешается соответствующий трафик данных на порте мониторинга. Если это не желательно, убедитесь, что на интерфейс направляется только отслеживаемый трафик данных.

Когда зеркалирование отключено, упомянутые специальные функции порта сбрасываются до значений по умолчанию. Сброс происходит независимо от того, были ли функции настроены вручную или автоматически, путём включения блокировки мониторинга.

Таблица основных настроек содержит следующие поля:

- **Select**
Выберите строку, которую необходимо удалить.
- **Session ID**
Идентификатор сеанса присваивается автоматически при создании новой записи. Можно создать только один сеанс.
- **Session Typ**
Отображает тип сеанса зеркалирования
- **Status**
Отображает, активно ли зеркалирование.
- **Destination Port**
Выберите в раскрывающемся списке выходной порт, который будет зеркалироваться в данном сеансе.

Порядок действий

Создать сеанс зеркалирования

1. Включите зеркалирование.
2. Щёлкните кнопку «Create» для создания записи в таблице. Идентификатор сеанса создаётся автоматически.
3. Выберите порт назначения.
4. Щёлкните кнопку «Set Values», чтобы сохранить и активировать выбранные настройки.
5. Перейдите на следующую вкладку, чтобы сделать более детальные настройки идентификатора сеанса.

Удалить сеанс зеркалирования

1. В первом столбце установите флажок, чтобы отметить строку.
2. Щёлкните кнопку «Delete», чтобы удалить выделенную строку.

6.5.7.2 Порт

Зеркалирование портов

Можно настроить параметры на этой странице, только в том случае если идентификатор сеанса с типом сеанса «Port Based» (на основе порта) был создан на вкладке «General».

Port Mirroring Sources

General | **Port**

Session ID: 1

Port	Ingress Mirroring	Egress Mirroring
P0.1	☐	☐
P0.2	☐	☐
P0.3	☐	☐

Set Values Refresh

Описание отображаемых полей

Страница содержит следующие поля:

- **Session ID**
Отображает сеанс.
- **Port**
Отображает все доступные порты. Порт складывается из номера модуля и номера порта, например, порт 0.1 означает модуль 0, порт 1.

- **Ingress-Mirroring**
Активируйте или деактивируйте прослушивание входящих пакетов на необходимом порте.
- **Ingress-Mirroring**
Активируйте или деактивируйте прослушивание исходящих пакетов на необходимом порте.

Примечание

Зеркалирование для кольцевых портов

Если активировать функцию Mirroring на кольцевом порте, кольцевой порт отправляет тестовые кадры, даже если он находится в состоянии «link down».

Порядок действий при конфигурации

1. В таблице установите флажки в строке после порта для зеркалирования.
Выберите, хотите ли прослушивать входящие или исходящие пакеты.
Для того чтобы прослушивать весь трафик проходящий через порт, необходимо установить оба флажка.
2. Щёлкните кнопку «Set values».

6.5.8 Dynamic MAC Aging

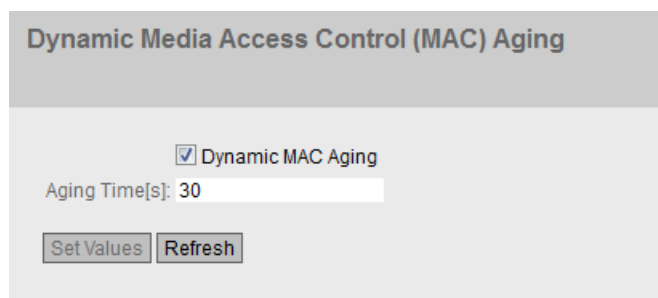
Настройки протокола и функциональность коммутатора

Устройство автоматически запоминает исходные адреса подключённых участников. Эта информация используется специально для пересылки пакетов с данными задействованным участникам. Таким образом, снижается нагрузка на сеть для других участников.

Если устройство не получает в течение определенного периода времени пакет, исходный адрес которой совпадает с полученным адресом, то оно удаляет полученный адрес.

Данный механизм обозначается как «Aging». Время старения предотвращает неправильную маршрутизацию пакетов, например, если окончное устройство подключено к другому порту.

Когда опция не активирована, устройство автоматически не удаляет полученные адреса.



Описание отображаемых полей

Страница содержит следующие поля:

- **Dynamic MAC Aging**
Активируйте или деактивируйте функцию автоматического время старения полученных MAC-адресов.
- **Aging Time[s]**
Введите время в секундах с шагом 15. По истечении этого периода полученный адрес удаляется, если устройство не получает дальнейших пакетов с данного адреса.
Диапазон значений: 15 - 630 секунд
Заводская настройка: 30

Примечание

Округление значений, отклонение от заданного значения

При вводе времени Aging Time обратите внимание, что оно округляется до правильных значений. Если вводится значение, которое не делится на 15, то значение автоматически округляется.

Порядок действий при конфигурации

1. Установите флажок «Dynamic MAC Aging».
2. Введите в поле ввода время в секундах Aging Time[s].
3. Щёлкните кнопку «Set values».

6.5.9 Ring Redundancy

6.5.9.1 Ring

Конфигурация кольцевого резервирования

Ring Redundancy

Ring

Standby

Link Check

MRP Interconnection

Ring ID:

1

☐ Ring Redundancy

Ring Redundancy Mode:

-

Ring Ports:

P0.7

P0.8

Domain Name:

default-mrpdomain

☐ Observer

Restart Observer

Restore Default

Ring ID	Domain Name	Ring Redundancy Mode	Ring Port 1	Ring Port 2
1	default-mrpdomain	-	P0.7	P0.8
2		-	P0.7	P0.8
3		-	P0.7	P0.8
4		-	P0.7	P0.8

Set Values

Refresh

- **Ring ID**
Выберите идентификатор кольцевой сети, которую необходимо сконфигурировать.
- **Ring Redundancy**
Если установить флажок напротив «Ring Redundancy», то будет включено кольцевое резервирование. Используются кольцевые порты, настроенные на этой странице.

- **Ring Redundancy Mode**

Здесь настраивается режим эксплуатации кольцевого резервирования.

Примечание

Когда настраивается несколько кольцевых сетей, необходимо выбрать режим кольцевого резервирования для каждой кольцевой сети «MRP Manager».

Доступны следующие режимы эксплуатации:

- **Automatic Redundancy Detection**
Выберите эту настройку, чтобы выполнить автоматическое конфигурирование режима работы с резервированием.
В режиме «Automatic Redundancy Detection» устройство автоматически определяет, имеется ли в кольцевой сети устройство с ролью «HRP Manager». В этом случае устройство принимает на себя роль «HRP Client».
Если устройство с ролью HRP Manager найти не удаётся, то все устройства с настройкой «Automatic Redundancy Detection» или «MRP Auto Manager» определяют между собой, какое устройство примет на себя роль «MRP Manager». При этом роль «MRP Manager» всегда принимает на себя устройство с наименьшим MAC-адресом. Остальные устройства автоматически переходят в режим «MRP Client».
- **MRP Auto-Manager**
В режиме «MRP Auto Manager» устройства определяют между собой, какое устройство примет на себя роль «MRP Manager». При этом роль «MRP Manager» всегда принимает на себя устройство с наименьшим MAC-адресом. Остальные устройства автоматически переходят в режим «MRP Client».
В отличие от настройки «Automatic Redundancy Detection» устройства не могут определить, имеется ли в кольцевой сети устройство с ролью «HRP Manager».
- **MRP Client**
Устройство принимает на себя роль MRP Client.
- **MRP Manager**
Устройство принимает на себя роль MRP Manager. Устройство не может автоматически принять на себя роль клиента.
- **HRP Client**
Устройство принимает на себя роль HRP Client.
- **HRP Manager**
Устройство принимает на себя роль HRP Manager.
При проектировании HRP-кольца одно устройство необходимо настроить в качестве «HRP Manager». Для всех остальных устройств необходимо выбрать настройку «HRP Client» или «Automatic Redundancy Detection».

- **Ring Ports**

Здесь задаются порты, которые будут использоваться в качестве кольцевых портов для кольцевого резервирования.

Примечание

Идентификатор Agent VLAN ID кольцевых портов

Для кольцевых портов необходимо настроить Agent VLAN ID. Таким образом, также можно настроить VLAN ID в диапазоне значений 1 ... 4094 для кольцевых портов.

Кольцевой порт, который выбирается в раскрывающемся списке слева, в HDR является «Isolated Port».

Заводская настройка задаёт следующие кольцевые порты:

Устройства	Заводская настройка кольцевых портов
XB208 XB216	P0.1 и P0.2
XB205-3	P0.7 и P0.8
XB213-3	P0.15 и P0.16
XC206-2G PoE XC206-2G PoE EEC XC206-2SFP XC206-2SFP G XC206-2SFP EEC XC206-2SFP G EEC XC208 XC208G XC208EEC XC208G EEC XC208G PoE XC216 XC216EEC XC216-4C XC216-4C G XC216-4C G EEC XC224 XC224-4C G XC224-4C G EEC	P0.1 и P0.2
XC216-3G PoE	P0.4 и P0.5
XC206-2	P0.7 и P0.8
XF-200BA	P1.1 и P2.1
XP208	P0.1 и P0.2
XP216	P0.10 и P0.12

6.5 Меню «Layer 2»

Устройства	Заводская настройка кольцевых портов
XR324WG XR328-4C WG (GE)	P0.1 и P0.2
XR326-2C PoE WG XR328-4C WG	P0.25 и P0.26

Группы портов для устройств с более чем 8 портами

Кольцевые порты MRP-кольца должны принадлежать одной группе логических портов.

XB-200

Устройство	Артикульный номер	Группа портов
SCALANCE XB216	6GK5 216-0BA00-2AB2 6GK5 216-0BA00-2TB2	Группа 1 Порт 1 ... Порт 8 Группа 2 Порт 9 ... Порт 16
SCALANCE XB213-3 (SC)	6GK5 213-3BD00-2AB2 6GK5 213-3BD00-2TB2	
SCALANCE XB213-3 (ST/BFOC)	6GK5 213-3BB00-2AB2 6GK5 213-3BB00-2TB2	
SCALANCE XB213-3LD	6GK5 213-3BF00-2AB2 6GK5 213-3BF00-2TB2	

XC-200

Устройство	Артикульный номер	Группа портов
SCALANCE XC216	6GK5 216-0BA00-2AC2	Группа 1 Порт 1 ... Порт 4 Порт 9 ... Порт 12 Группа 2 Порт 5 ... Порт 8 Порт 13 ... Порт 16
SCALANCE XC216 EEC	6GK5 216-0BA00-2FC2	
SCALANCE XC224	6GK5 224-0BA00-2AC2	Группа 1 Порт 1 ... Порт 8 Группа 2 Порт 9 ... Порт 12 Порт 17 ... Порт 20 Группа 3 Порт 13 ... Порт 16 Порт 21 ... Порт 24

XP-200

Устройство	Артикульный номер	Группа портов
SCALANCE XP216	6GK5 216-0HA00-2AS6	Группа 1 Порт 1 ... Порт 5, Порт 7
SCALANCE XP216	6GK5 216-0HA00-2TS6	
SCALANCE XP216 EEC	6GK5 216-0HA00-2ES6	Группа 2 Порт 6, порт 8, порт 9 Порт 11, порт 13, порт 15
SCALANCE XP216 PoE EEC	6GK5 216-0UA00-5ES6	
		Группа 3 Порт 10, Порт 12 Порт 14, порт 16

XR-300WG

Устройство	Артикульный номер	Группа портов
SCALANCE XR324WG	6GK5 324-0BA00-2AR3	Группа 1 Порт 1 ... Порт 4 Порт 13 ... Порт 16
SCALANCE XR324WG	6GK5 324-0BA00-3AR3	
		Группа 2 Порт 5 ... Порт 8 Порт 17 ... Порт 20
		Группа 3 Порт 9 ... Порт 12 Порт 21 ... Порт 24
SCALANCE XR328-4C WG	6GK5 328-4FS00-2AR3	Группа 1 Порт 1 ... Порт 4
SCALANCE XR328-4C WG	6GK5 328-4FS00-2RR3	
SCALANCE XR328-4C WG	6GK5 328-4FS00-3AR3	Группа 2 Порт 5 ... Порт 8 Порт 17 ... Порт 20
SCALANCE XR328-4C WG	6GK5 328-4FS00-3RR3	
SCALANCE XR328-4C WG	6GK5 328-4SS00-2AR3	Группа 3 Порт 9 ... Порт 12 Порт 21 ... Порт 24
SCALANCE XR328-4C WG	6GK5 328-4SS00-3AR3	
		Группа 4 Порт 25 ... Порт 28

Примечание

Пересылка потока RSPAN

Если устройству требуется пересылать потоки RSPAN, то должны быть выполнены два требования:

- Входящий и исходящий порт должны принадлежать к одной группе портов.
- Функция «Обучение» должна быть отключена для входящего порта. Это возможно только с помощью интерфейса командной строки CLI **нет одноадресного обучения Mac**.

H-Sync

H-Sync - это протокол уровня 2, который используется для синхронизации данных процесса в системах с избыточным управлением через сеть PROFINET. Следующее действительно для SIMATIC S7-1500R:

Оба контроллера подключаются с резервированием через кольцо MRP. При этом оба контроллера должны быть напрямую соединены друг с другом на одном пути. Оба контроллера настроены в качестве «MRP Auto Manager» таким образом, что один из контроллеров становится MRP Manager. Все остальные устройства в кольцевой сети являются MRP Client. Оба контроллера отправляют кадры H-Sync в обоих направлениях кольца (Provider). Полученные кадры H-Sync не пересылаются (Consumer). Все остальные устройства в кольцевой сети пересылают кадры H-Sync только между своими кольцевыми портами в обоих направлениях (Forwarder). На всех остальных портах кадры H-Sync фильтруются.

H-Sync является прозрачным протоколом для IE-коммутаторов. Какие коммутаторы IE можно использовать в качестве серверов пересылки строчной синхронизации можно узнать в главе «Системные функции и оборудование».

H-Sync настраивается только с помощью ПО STEP 7 Basic или Professional. Однако обратите внимание, что настройки, отклоняющиеся от следующих правил, могут привести к сложностям при конфигурировании:

– Процедура резервирования: Клиент MRP

- **Domain Name**

Выберите в раскрывающемся списке доменное имя. Каждое имя может быть присвоено только одной кольцевой сети.

Примечание

Если конфигурируется несколько резервных кольцевых сетей, нельзя использовать доменное имя «default-mrpdomain».

- **Observer**

Активировать/деактивировать наблюдателя. Функция «Observer» доступна только для колец HRP.

Кольцевой порт, выбранный в раскрывающемся списке слева, подключён к «Isolated Port» HRP Manager.

Наблюдатель отслеживает сбои в работе менеджера резервирования или неправильные конфигурации кольца HRP.

Если наблюдатель (Observer) активирован, при обнаружении ошибок он может прервать подключённое кольцо. Для этого наблюдатель переводит кольцевой порт в состояние «blocking». При устранении ошибки наблюдатель (Observer) снова включает порт.

- **Restart Observer**

Когда последовательно происходит большое количество ошибок, наблюдатель больше не может выключить самостоятельно свой порт. Кольцевой порт постоянно находится в состоянии «blocking». Об этом свидетельствует светодиод ошибки и текст сообщения.

После устранения проблемы можно снова включить порт с помощью кнопки «Restart Observer».

- **Restore Default**
Эта кнопка работает только в том случае, если активны несколько резервных колец. Нажмите эту кнопку, чтобы сбросить конфигурацию кольцевого резервирования до заводских настроек.
- **DNA Redundancy**
Активировать/деактивировать резервирование DNA. Можно активировать резервирование DNA только при соблюдении следующих условий:
 - Кольцевое резервирование включено.
 - «MRP Manager» или «MRP Client» настроен как режим Ring Redundancy Mode. Резервирование DNA возможно только с MRP.

Примечание

Подробное пошаговое описание конфигурации резервирования DNA можно найти в главе «Технические основы → Процедура резервирования → Резервирование доступа к дублированной сети (DNA Redundancy)».

Таблица состоит из следующих столбцов:

- **Ring ID**
Идентификатор кольца.
- **Domain Name**
Имя резервируемого домена.
- **Ring Redundancy Mode**
Процедура резервирования, используемая в данном кольце. Когда отображается «-», кольцевое резервирование не активировано.
- **Ring Port 1**
Первый кольцевой порт.
- **Ring-Port 2**
Второй кольцевой порт.

Порядок действий при конфигурации

1. Установите флажок «Ring Redundancy».
2. Выберите тип режима резервирования.
3. Назначьте кольцевые порты.
4. Щёлкните кнопку «Set values».

Восстановление заводских настроек

EtherNet / варианты IP/Industrial Ethernet

При восстановлении заводских настроек кольцевое резервирование отключается, а настройки кольцевого порта сбрасываются. Spanning Tree активировано.

Варианты PROFINET

При восстановлении заводских настроек включается кольцевое резервирование. Сброс до заводских настроек также сбрасывает настройки кольцевого порта. Если перед сбросом настроек использовались другие порты в качестве кольцевых, ранее правильно сконфигурированное устройство может вызвать заикливание пакетов и, следовательно, сбой обмена данными.

Изменение состояния кольцевых портов в управлении резервированием (HRP)

При настройке устройства управления резервированием, установите состояние кольцевых портов. Первый кольцевой порт переходит в состояние «blocking» а второй кольцевой порт в состояние «forwarding». Когда кольцевое резервирование активировано, можно менять состояние этих кольцевых портов.

Примечание

Обязательно сначала разомкните кольцо, чтобы не возникало заикливание пакетов.

Изменение кольцевых портов

Чтобы изменить кольцевые порты, выполните следующие действия:

1. Откройте кольцевую сеть.
2. Выберите новые кольцевые порты.
3. Перекоммутируйте кабели.
4. Закройте кольцевую сеть.

6.5.9.2 Standby

Резервное соединение кольцевых сетей

Резервирование в режиме ожидания позволяет соединения колец HRP с резервированием.

Для того чтобы установить соединение в режиме ожидания, настройте два соседних устройства в кольцевой сети как ведущее или ведомое в режиме ожидания. Ведущее и ведомое устройства в режиме ожидания должны быть подключены к двум устройствам в другом кольце через параллельные линии.

В неповреждённом состоянии сообщения проходят между двумя кольцами через ведущее устройство. Если линия ведущего устройства нарушена, ведомое устройство берёт на себя пересылку сообщений между двумя кольцами.

Активируйте резервирование в режиме ожидания для обоих партнёров в режиме ожидания и выберите порты, через которые устройство подключается к кольцам, которые необходимо связать.

В качестве имени «Standby Connection Name» для обоих партнёров в кольце должно быть задано уникальное имя, с помощью которого два связанных устройства идентифицируются как партнёры в режиме ожидания.

Примечание

Для того чтобы использовать эту функцию, необходимо активировать HRP.

Примечание

Когда соединение между ведущим и ведомым устройством в режиме Standby в линейной топологии восстанавливается после прерывания, может возникнуть кратковременное увеличение трафика.

Port	Setting
P0.1	☐
P0.2	☐
P0.3	☐
P0.4	☐

Описание отображаемых полей

- **Standby**
Активируйте или деактивируйте функцию режима ожидания.

Примечание

Когда два устройства соединены в режиме ожидания, функция «Standby» должна быть активирована на обоих устройствах.

- **Standby Connection Name**
Через это имя задаётся пара ведущее/ведомое устройство. Оба устройства должны быть в одном кольце.
Введите здесь имя для подключения в режиме ожидания. Оно должно быть идентично имени, введённому для партнёра в режиме ожидания. Имя может быть выбрано произвольно, но его разрешено использовать только для одной пары устройств во всей сети.

- **Force device to Standby Master**

Когда установлен этот флажок, устройство будет настроено как ведущее устройство в режиме ожидания независимо от его MAC-адреса.

- Когда данный флажок не установлен ни для одного из двух устройств, для которых активировано устройство управления в режиме ожидания, устройство с более высоким MAC-адресом берет на себя функцию ведущего устройства в режиме ожидания, при отсутствии ошибок.
- Когда этот параметр выбран для обоих устройств или когда свойство «Force device to Standby Master» (принудительно использовать ведущее устройство в режиме ожидания) поддерживается только одним устройством, то ведущее устройство в режиме ожидания также выбирается на основе MAC-адреса.

Этот вид распределения важен, в частности, при замене устройств. В зависимости от MAC-адреса предыдущее устройство с функцией Slave может принимать на себя роль Master в режиме ожидания.

Примечание

Если опция «Force device to Standby Master» соединения в режиме ожидания активирована на обоих устройствах, это может привести к заикливанию пакетов, и таким образом трафик может прерваться. Активируйте опцию «Force device to Standby Master» только на одном устройстве соединения в режиме ожидания.

- **Wait for Standby Partner**

- Активировано
Standby Connection активируется только тогда, когда между ведущим или ведомым устройством Standby и их партнером Standby установлено соединение. Это гарантирует, что резервное соединение действительно доступно до активации связи через соединение Standby.
- Деактивировано
Соединение в режиме ожидания активируется, даже если ведущее устройство в режиме ожидания ещё не установило соединение с ведомым устройством в режиме ожидания.
Это может вызвать заикливание пакетов и сбой обмена данными, если другое соединение в режиме ожидания уже было активировано. Несколько соединений в режиме ожидания могут возникнуть, например, из-за ошибок конфигурации, если для ведущего и ведомого устройства в режиме ожидания были назначены разные имена соединений в режиме ожидания.

- **Partner detect timeout [ms]**

Это поле ввода отображается только в том случае, если флажок «Wait for Standby Partner» деактивирован. В этом случае можно задать время, в течение которого устройство будет ожидать, пока оно не установит соединение в режиме ожидания. По истечении этого периода времени активируется соединение в режиме ожидания, даже если ведущее устройство в режиме ожидания ещё не установило соединение с ведомым устройством в режиме ожидания.

- **Port**

Выберите, какой порт будет портом в режиме ожидания. Подключение к другому кольцу происходит через порт в режиме ожидания.

Порт в режиме ожидания участвует в перенаправлении трафика. В случае без прерываний активен только порт в режиме ожидания ведущего устройства, который принимает трафик из подключённой сети по топологии кольца или шины HRP. Если соединение ведущего устройства или Ethernet через порт в режиме ожидания ведущего устройства разрывается, то порт в режиме ожидания ведущего устройства отключается и активируется резервный порт в режиме ожидания ведомого устройства. Таким образом восстанавливается функционирующее соединение через Ethernet в подключённом сегменте сети (топология кольца или шина HRP).

6.5.9.3 Link Check

Требования

Примечание

Изменение типа соединения для порта Combo: Оптическое → Электрическое

Когда проверка типа соединения активна на комбинированном порте с типом соединения «SFP» и необходимо активировать тип соединения «RJ45», сперва деактивируйте проверку Link Check.

- Нельзя включить Link Check на портах с пропускной способностью 10 Гбит/с.
- Функцию Link Check можно активировать только для оптических кольцевых портов кольцевой топологии HRP или MRP.
- Функция Link Check должна быть активирована на двух соседних устройствах (партнёрах по соединению) в пределах одного кольца HRP или MRP.
- Кольцевые порты, на которых активируется функция Link Check, должны быть соединены друг с другом.

Контроль оптических соединений в кольце

С помощью функции Link Check можно контролировать качество передачи данных на оптических участках внутри кольцевой сети HRP или MRP, идентифицировать неисправные участки передачи данных и отключать их при определённых условиях. Когда неисправный участок отключён, устройство управления резервированием может замкнуть кольцевую сеть и восстановить связь.

ВНИМАНИЕ

Убедитесь, что пакеты, используемые в функции Link Check для мониторинга оптических соединений, не вытесняются перегрузкой высокоприоритетными пакетами в сети.

Перегрузка высокоприоритетными пакетами может иметь, например, следующие причины:

- Петли коммутации сети, которые могут привести к копированию высокоприоритетных пакетов
- Изменение приоритетов пересылки пакетов

Примечание

Не активируйте функцию Link Check только для одного из двух партнёров по соединению. Это может привести к ошибочной реакции.

Примечание

Если функция Link Check активирована на всех устройствах в кольце одновременно, и несколько соединений в кольце нарушены, это приводит к фрагментации кольца.

1. Во время ввода в эксплуатацию включайте функцию Link Check сначала для одного участка соединения, затем для другого, активировав Link Check для обоих партнёров по соединению, которые подключены к одному участку.
2. Для обеспечения безошибочного соединения подождите в каждом случае 1 минуту перед активацией Link Check для следующего соединительного участка.

Link Check

Ring

Standby

Link Check

MRP Interconnection

Port	Setting	Reset
P0.1	☐	Reset
P0.2	☐	Reset

Set Values

Refresh

Описание отображаемых полей

Таблица содержит следующие столбцы:

- **Port**
Отображает доступные порты. Порт складывается из номера модуля и номера порта, например, порт 0.1 означает модуль 0, порт 1.
- **Setting**
С помощью этого флажка активируется или деактивируется функция проверки типа соединения для порта.
При активном контроле соединения можно увидеть количество отправленных и полученных тестовых пакетов функции Link Check на странице Information > Redundancy > Link Check.
- **Reset**
После сброса Link Check функция перезапускается на порте, а статистика сбрасывается.
Когда используется кнопка «Reset», настройки обоих партнёров по соединению должны быть сброшены в течение 30 секунд.

Примечание

Когда используется кнопка «Reset», могут образоваться кратковременные коммутационные петли и, следовательно, сбой обмена данными. Петля автоматически исчезает.

Если в вашем случае применения это неприемлемо, сбросьте функцию Link Check, отсоединив соединительный кабель и вновь подсоединив его.

Порядок действий при конфигурации

Включить проверку типа соединения

Для того чтобы активировать мониторинг кольцевого порта, выполните следующие действия:

1. Активируйте соответствующий флажок в столбце «Setting».
2. Щёлкните кнопку «Set values».

Выключить проверку типа соединения

Для того чтобы деактивировать мониторинг кольцевого порта, выполните следующие действия:

1. Удалите соответствующий флажок в столбце «Setting».
2. Щёлкните кнопку «Set values».

6.5.9.4 MRP-Interconnection

Резервное соединение кольцевых сетей

На этой странице создаются, удаляются и настраиваются соединения MRP Interconnection.

MRP Interconnection

Ring
Standby
Link Check
MRP Interconnection

☐ MRP Interconnection

Select	Interconnection Domain ID	Interconnection Domain Name	Interconnection Port	Wait (Manager)	Role/Position	Status
☐	1	MrpIntCon1	P3.4	☐	Primary Client	☐

1 entry.

Create
Delete
Set Values
Refresh

Описание

Страница содержит следующие поля:

- **MRP Interconnection**
Установите этот флажок, чтобы активировать MRP Interconnection для устройства. Функцию MRP Interconnection можно активировать только при выполнении следующих требований:
 - Кольцевое резервирование включено.
 - В качестве режима кольцевого резервирования установлено «MRP Auto Manager» или «MRP Client».
 - Имеется активированное соединение MRP Interconnection.

Примечание

Настройте режим кольцевого резервирования «MRP Auto Manager» для двух устройств в каждом кольце, чтобы обеспечить возможность немедленной перенастройки кольца MRP в случае отказа даже одного из устройств.

Таблица состоит из следующих столбцов:

- **Select**
Выберите строку, которую необходимо удалить.
- **Interconnection Domain ID**
Введите идентификатор соединения MRP Interconnection. При присвоении ID соблюдайте следующие правила:
 - Значение Interconnection ID не должно быть равным 0.
 - Для всех четырёх устройств, которые используются для соединения колец необходимо настроить одинаковый Interconnection ID.

- **Interconnection Domain Name**

Укажите необходимое имя для соединения MRP Interconnection. Также можно задать разные имена для четырёх устройств, которые используются для соединения кольцевых сетей. В качестве допустимых символов для имени можно использовать буквы от A до Z и от a до z, а также цифры от 0 до 9 и символ «-». В качестве первого и последнего символа имени нельзя использовать дефис. Имя межсетевого взаимодействия должно состоять как минимум из одного символа и иметь длину не более 240 символов.

- **Interconnection Port**

В этом раскрывающемся списке выберите порт, который используется для соединения межсетевого взаимодействия MRP. Обратите внимание на следующие ограничения:

- Порт не должен быть отключён или заблокирован. Нельзя активировать функцию «Unicast Blocking» для порта.
- Порт не должен использоваться для функции Link Aggregation.
- Порт не должен быть портом мониторинга функции «Mirroring».
- Порт не должен быть портом Spanning Tree.
- Порт не должен быть кольцевым портом.
- Порт не должен быть портом маршрутизатора.
- Порт не должен быть портом 802.1X Authenticator.
- Порт не должен быть портом 802.1X Supplicant.

- **Wait (Manager)**

Нельзя установить флажки в этом столбце для устройств с ролью «Client». Если активировать этот флажок для устройства с ролью «Manager», то устройство управления межсетевого взаимодействия MRP ожидает передачи данных, пока основной клиент для межсетевого взаимодействия MRP не будет готов к работе. Когда флажок не установлен, устройство управления межсетевого взаимодействия MRP начинает передачу данных после времени ожидания в 200 миллисекунд, независимо от состояния готовности основных клиентов.

- **Rolle/Position**

Имеется две роли «Manager» и «Client». Для клиентов также задаётся состояние («Primary» или «Secondary»). Таким образом, в этом раскрываемом списке доступны следующие варианты выбора:

- Manager
- Primary Client
- Secondary Client

- **Status**

Установите этот флажок, чтобы активировать соединения межсетевого взаимодействия MRP. Обратите внимание на следующие правила:

- Когда соединение межсетевого взаимодействия MRP не активировано, вы не можете включить соединения межсетевого взаимодействия MRP для устройства.
- Для количества активных соединений MRP Interconnection действуют следующие максимальные значения:

SCALANCE XC-200, SCALANCE XP-200 и SCALANCE XF-200BA

Два соединения

SCALANCE XB-200 и SCALANCE XR-300WG

Одно соединение

Порядок действий при конфигурации

Примечание

Подробное пошаговое описание конфигурации межсетевого взаимодействия MRP можно найти в главе «Технические основы → Процедура резервирования → Резервирование доступа → MRP Interconnection».

Необходимые условия для конфигурации

1. Соедините кабели в соответствии с запланированной топологией, за исключением следующих соединений:
 - Один канал связи в каждом кольце, т.е. кольца ещё не должны быть замкнуты.
 - Два устройства, предназначенные для вторичного подключения (MIM и Secondary Coupled MIC), пока не должны подключаться.
2. Назначьте IP-адрес каждому устройству, чтобы иметь возможность использовать интерфейс WBM.

Необходимые условия для конфигурации, если топология сети требует связующего дерева

1. Настройте совместимость протокола «RSTP» для Spanning Tree.
2. Деактивируйте режим Spanning Tree для кольцевых портов и портов MRP Interconnection.

Конфигурация кольцевого резервирования

Настройте следующие параметры кольцевого резервирования для каждого устройства:

1. Назначьте кольцевые порты.
2. Активируйте MRP.
3. Назначьте устройству роль MRP. Настройте режим кольцевого резервирования для двух устройств в каждом кольце «MRP Auto-Manager», чтобы обеспечить возможность незамедлительной перенастройки кольца MRP в случае отказа одного из устройств.

После конфигурирования всех устройств в обеих кольцевых сетях для MRP замкните обе кольцевые сети MRP, подключив кабели между устройствами, которые ещё не были соединены. Кабель между MIM и вторичным подключённым MIC пока не должен подключаться.

Конфигурация MRP Interconnection

При конфигурировании этих устройств необходимо придерживаться определенной последовательности, чтобы ПК для настройки всегда имел доступ к устройствам. Сначала сконфигурируйте устройства с соединением MRP Interconnection в кольце MRP, к которому не подключён ПК для настройки. Начните с устройства соединения межсетевого взаимодействия MRP, к которому не был подключён кабель. Необходимо провести следующие операции для каждого устройства:

1. Щёлкните кнопку «Create», чтобы создать в таблице с соединениями MRP Interconnection новую строку.
2. Настройте параметры для соединения межсетевого взаимодействия MRP, как было описано выше.
3. Установите флажок «MRP Interconnection» для включения MRP Interconnection.

После того, как сконфигурированы все устройства в обоих кольцах для MRP Interconnection подсоедините кабель для вторичного подключения между устройствами MIM и Secondary Coupled MIC. После этого соединение MRP Interconnection функционирует.

Примечание

Реконфигурация

Прежде чем перенастраивать топологию, разомкните кольцевую сеть, чтобы избежать закливания пакетов.

6.5.10 Spanning Tree

6.5.10.1 Общая информация

Основные настройки для Spanning Tree

Это базовая страница для связующего дерева. Выберите в раскрывающемся списке необходимый режим совместимости.

Дальнейшие настройки возможны на соответствующей странице конфигурации функций.

В зависимости от режима совместимости можно настроить необходимую функцию на соответствующей странице конфигурации.

Описание отображаемых полей

Страница содержит следующие поля:

- **Spanning Tree**
Активируйте или деактивируйте Spanning Tree.
- **Protocol Compatibility**
Выберите совместимость протокола. Доступны следующие настройки:
 - STP
 - RSTP
 - MSTP
- **RSTP+**
Протокол RSTP+ обеспечивает соединение сегмента сети, в котором активировано Spanning Tree, с кольцом MRP. Перед установкой этого флажка убедитесь, что выполнены следующие предварительные условия:
 - MRP необходимо активировать как режим резервирования.
 - При активированном кольцевом резервировании необходимо деактивировать кольцевые порты для Spanning Tree.

Если активирован протокол RSTP+, кольцевые порты как и часть кольца MRP, а также часть Spanning Tree становятся сегментом сети. Без протокола RSTP+ кольцевые порты не принадлежат сегменту сети связующего дерева.
- **RSTP+ MRP Interconnection Domain ID**
сконфигурируйте здесь идентификатор домена для протокола RSTP+MRP Interconnection. Это значение не должно совпадать с ID домена MRP Interconnection, который был сконфигурирован для активного соединения MRP Interconnection.

Порядок действий при конфигурации

1. Установите флажок напротив «Spanning Tree».
2. Выберите в раскрывающемся списке «Protocol Compatibility» необходимый режим совместимости.
3. Щёлкните кнопку «Set values».

6.5.10.2 CIST General

Конфигурация протокола MSTP-CIST

Страница состоит из следующих частей:

- В левой части страницы отображена конфигурация устройства.
- В средней части отображена конфигурация корневого моста, которая может быть выведена из пакетов Spanning Tree, полученных устройством.
- Правая часть отображает конфигурацию регионального корневого моста, которая может быть получена из пакетов по протоколу MSTP. Отображаемые данные видны только в том случае, если они активированы на странице General Spanning Tree и задана совместимость «Protocol Compatibility» протокола «MSTP». Это также относится к параметру «Bridge Max Hop Count». Когда устройство является корневым мостом, информация левой и правой части совпадают.

Common Internal Spanning Tree (CIST) General					
General	CIST General	CIST Port	MST General	MST Port	Enhanced Passive Listening Compatibility
Bridge Priority: 32768	Root Priority: 0	Regional Root Priority: 0			
Bridge Address: 00-00-00-00-00-00	Root Address: 00-00-00-00-00-00	Regional Root Address: 00-00-00-00-00-00			
Root Port: -	Root Cost: 0	Regional Root Cost: 0			
Topology Changes: 0	Last Topology Change: -	Region Name: 00:1b:1b:40:91:23			
Bridge Hello Time[s]: 2	Root Hello Time[s]: 2	Region Version: 0			
Bridge Forward Delay[s]: 15	Root Forward Delay[s]: 15				
Bridge Max Age[s]: 20	Root Max Age[s]: 20				
Bridge Max Hop Count: 20					
Reset Counters					
Set Values Refresh					

Описание отображаемых полей

Страница содержит следующие поля:

- **Bridge Priority / Root Priority**
На основании параметра Bridge Priority определяется, какое устройство будет Root-Bridge. Мост Bridge с наиболее высоким приоритетом корневой мост Root-Bridge. Чем меньше значение, тем выше приоритет. Когда в сети несколько устройств имеют одинаковый приоритет, то корневым мостом становится устройство, MAC-адрес которого имеет наименьшее числовое значение. Оба параметра, Bridge Priority и MAC Address, вместе образуют идентификатор моста. Так как Root Bridge управляет изменениями путей, то он из-за времени прохождения пакетов должен иметь как можно более близкое к центру расположение.
Значение приоритета моста - это целое число, кратное 4096. Диапазон значений: 0 - 61440
- **Bridge Address / Root Address**
Адрес моста отображает MAC-адрес устройства, а корневой адрес отображает MAC-адрес корневого моста.
- **Root Port**
Отображает порт, через который коммутатор обменивается данными с корневым мостом.
- **Root Cost**
Стоимость пути от данного устройства до корневого моста
- **Topology Changes / Last Topology Change**
Задаёт для устройства количество реконфигураций из-за механизма связующего дерева с момента последнего запуска. Для корневого моста время с момента последней реконфигурации отображается следующим образом:
 - Секунды: дополнение «sec» после указания числа
 - Минуты: дополнение «min» после указания числа
 - Часы: дополнение «hr» после указания числа
- **Bridge Hello Time[s] / Root Hello Time[s]**
Каждый мост регулярно отправляет конфигурационные пакеты (BPDU). Временной интервал между двумя конфигурационными пакетами называется временем приветствия - «Hello Time».
Заводская настройка: 2 секунды

Примечание

Настройка «Bridge Hello Time» возможна только с совместимостью Protocol Compatibility протокола RSTP. Когда задана совместимость Protocol Compatibility протокола MSTP используется параметр «Hello Time» на странице Layer 2 > Spanning Tree > CIST Port.

- **Bridge Forward Delay[s] / Root Forward Delay[s]**
Информация о новой конфигурации применяется мостом не непосредственно, а только по истечении периода времени, указанного в параметре «Forward Delay». Таким образом, гарантируется, что рабочий режим в соответствии с новой топологией запускается только тогда, когда все мосты получают необходимую информацию.
Заводская настройка: 15 секунд

- **Bridge Max Age[s] / Root Max Age[s]**
Если пакет BPDU старше заданного «Max Age», он отклоняется.
Заводская настройка: 20 секунд
- **Regional Root Priority**
Описание см. Приоритет моста / Приоритет корневого моста.
- **Regional Root Address**
MAC-адрес устройства.
- **Regional Root Cost**
Стоимость пути от данного устройства до корневого моста
- **Bridge Max Hop Count**
Этот параметр указывает, скольким участникам MSTP разрешено пройти протокол BPDU. Если получен пакет MSTP-BPDU, число переходов которого превышает заданное здесь значение, он отклоняется. Значение по умолчанию для этого параметра равно 20.
- **Region Name**
Введите имя региона MSTP, к которому относится данное устройство. По умолчанию здесь вводится MAC-адрес устройства. Это значение должно быть одинаковым на всех устройствах, относящихся к одному региону MSTP.
- **Region Version**
Введите номер версии региона MSTP, в котором находится устройство. Это значение должно быть одинаковым на всех устройствах, относящихся к одному региону MSTP.
- **Reset Counters**
Щёлкните эту кнопку, чтобы сбросить счётчики на этой странице.

Порядок действий при конфигурации

1. Введите, необходимые для конфигурации данные, в поля ввода.
2. Щёлкните кнопку «Set values».

6.5.10.3 Порт CIST

Конфигурация портов MSTP-CIST

Текущий статус конфигурации параметров порта отображается в таблице при вызове страницы.

Для настройки щёлкните соответствующие поля в таблице портов.

Common Internal Spanning Tree (CIST) Port

General	CIST General	CIST Port	MST General	MST Port	Enhanced Passive Listening Compatibility	
Spanning Tree Status Copy to Table All ports No Change Copy to Table						
Port	Spanning Tree Status	Priority	Cost Calc.	Path Cost	State	Fwd. Trans.
P0.1	☒	128	0	2000000	Disabled	0
P0.2	☒	128	0	2000000	Disabled	0
P0.3	☒	128	0	2000000	Disabled	0
P0.4	☒	128	0	2000	Disabled	0

(Продолжение таблицы)

Edge Type	Edge	P.t.P. Type	P.t.P.	Hello Time	Restr. Role	Restr. TCN	Limited TCN
Auto	☒	-	☒	2	☐	☐	☐
Auto	☒	-	☒	2	☐	☐	☐
Auto	☒	-	☒	2	☐	☐	☐
Auto	☒	-	☒	2	☐	☐	☐

Описание отображаемых полей

Таблица 1 состоит из следующих столбцов:

- **1-й столбец**
Отображает, что настройки действительны для всех портов в таблице 2.
- **Spanning Tree Status**
Выберите в раскрывающемся списке настройку. Имеются следующие возможности настройки:
 - Enabled
Порт интегрирован в связующее дерево.
 - Disabled
Порт не интегрирован в связующее дерево.
 - No Change
Таблица 2 осталась без изменений.
- **Copy to Table**
При нажатии кнопки настройка будет скопирована для всех портов в таблице 2.

Таблица 2 состоит из следующих столбцов:

- **Port**
Отображает все доступные порты. Порт складывается из номера модуля и номера порта, например, порт 0.1 означает модуль 0, порт 1.
 - **Spanning Tree Status**
Задайте, интегрирован ли порт в связующее дерево или нет.
-
- Примечание**
- Если для порта отключён параметр «Spanning Tree Status», то могут образоваться петли. Необходимо учитывать топологию.
-
- **Priority**
Введите приоритет порта. Приоритет оценивается только в том случае, если стоимость пути одинакова.
Значение должно делиться на 16. Если значение не делится на 16, то оно будет автоматически адаптировано.
Диапазон значений: 0 - 240.
Значение по умолчанию равняется 128.
 - **Cost Calc.**
Введите расчёт стоимости пути. Если введено значение «0», автоматически определённое значение отображается в поле «Path Cost».
 - **Path Cost**
Этот параметр предназначен для расчёта выбранного пути. В качестве пути выбирается путь с наименьшим значением. Если несколько портов устройства имеют одинаковое значение, то выбирается порт с самым низким номером.
Если значение в поле «Cost Calc.» равно «0», то отображается автоматически рассчитанное значение. Если введено значение, отличное от «0», то отображается значение поля «Cost Calc.».
Определение стоимости пути в основном ориентируется на скорость передачи данных. Чем выше достижимая скорость передачи, тем меньше значение стоимости пути.
Типовые значения стоимости пути в алгоритме Rapid Spanning Tree:
 - 10000 Мбит/с = 2000
 - 1000 Мбит/с = 20000
 - 100 Мбит/с = 200000
 - 10 Мбит/с = 2000000
 Значения параметров также можно задавать индивидуально.

- **Status**
Отображает текущий статус, в котором находится порт. Значения только отображаются и не могут быть изменены. Параметр «Status» зависит от настроенного протокола. Возможны следующие значения:
 - Disabled
Порт только принимает пакеты и не участвует в протоколах STP, MSTP и RSTP.
 - Discarding
В режиме работы «Discarding» принимаются пакеты BPDU. Другие исходящие или входящие пакеты отклоняются.
 - Listening
В этом состоянии пакеты BPDU, как принимаются и так отправляются. Порт задействован в алгоритме Spanning Tree.
 - Learning
Предварительный этап к состоянию «Forwarding», порт активно изучает топологию, (то есть адреса участников).
 - Forwarding
По истечении времени реконфигурации порт активен в сети, принимает и отправляет пакеты с данными.
- **Fwd. Trans**
Указывает количество переходов от состояния «Discarding» к состоянию «Forwarding».
- **Edge Type**
Задайте тип граничного порта «Edge Port». Имеются следующие возможности:
 - "-"
Граничный порт деактивирован. Порт рассматривается как «не граничный порт».
 - Admin
Выберите эту опцию, если на этом порте всегда имеется оконечное устройство. В противном случае каждый раз при изменении соединения запускается реконфигурация сети.
 - Auto
Выберите эту опцию, если необходимо, чтобы этот порт автоматически определял, подключено ли оконечное устройство. Когда соединение устанавливается в первый раз, порт рассматривается как «не граничный порт».
 - Admin/Auto
Выберите эту опцию, если на этом порте используется их комбинация. Когда соединение устанавливается в первый раз, порт рассматривается как «граничный порт».
- **Edge**
Отображает статус порта.
 - Активировано
На этом порте находится оконечное устройство.
 - Деактивировано
На этом порте подключено устройство Spanning Tree или Rapid Spanning Tree.

В случае оконечного устройства коммутатор может переключать порт быстрее, независимо от пакетов связующего дерева. Если, несмотря на этот параметр, получен пакет связующего дерева, порт автоматически переходит в состояние «Disabled».

- **P.t.P. Тип**

Выберите в раскрывающемся списке нужный параметр. Выбор зависит от установленных портов.

- «-»
Соединение точка-точка определяется автоматически. Когда порт установлен в полудуплексный режим, соединение точка-точка не предполагается
- P.t.P.
При полудуплексном режиме за основу берётся соединение точка-точка.
- Shared Media
При полнодуплексном режиме за основу не берётся соединение точка-точка.

Примечание

Соединение точка-точка означает прямое соединение между двумя устройствами. Совместное медиа-соединение, например, это соединение с сетевым концентратором.

- **P.t.P.**

Установленный флажок указывает, что рабочее состояние порта соответствует конфигурации в столбце «P.t.P. Тип».

- **Hello Time**

Введите интервал, по истечении которого мост отправляет конфигурационные пакеты (BPDU). По умолчанию выставлен интервал 2 секунды.

Диапазон значений: 1-2 секунды

Примечание

Настройка Hello Time для конкретного порта возможна только с совместимостью протокола MSTP Protocol Compatibility. Когда задана совместимость Protocol Compatibility протокола RSTP используется параметр «Bridge Hello Time» на странице Layer 2 > Spanning Tree > CIST General.

- **Restr. Role**

При установленном флажке, соответствующий порт не выбирается в качестве корневого порта, независимо от значения приоритета. Также при установленном флажке, порт с самым низким приоритетом не может стать корневым портом. Активируйте эту опцию, только в том случае если необходимо ограничить влияние мостов за пределами администрируемой области на топологию связующего дерева.

6.5 Меню «Layer 2»

- **Restr. TCN**

При установленном флажке, соответствующий порт не пересылает ни полученные, ни распознанные изменения топологии (Topology Change Notifications) на другие порты. Активируйте эту опцию, только в том случае, если необходимо ограничить влияние мостов за пределами администрируемой области на топологию связующего дерева.

- **Restr. TCN**

При установленном флажке, соответствующий порт принимает полученные и обнаруженные изменения топологии, но не пересылает изменения топологии другим портам. Можно активировать флажки в этом столбце только при соблюдении следующих условий:

- Протокол RSTP+ должен быть активирован.
- Флажок «Restr. TCN» должен быть удалён для этого порта.

Если указанные условия не выполнены, флажки в этом столбце неактивны и отображены серым цветом.

Порядок действий при конфигурации

1. Введите значения в поля ввода строки таблицы для конфигурируемых портов.
2. Выберите значения в раскрывающихся списках полей в строке таблицы конфигурируемого порта.
3. Щёлкните кнопку «Set values».

6.5.10.4 MST General

Конфигурация множественного связующего дерева

С помощью протокола MSTP, в дополнении к RSTP, можно управлять несколькими виртуальными локальными сетями в локальной сети с собственными деревьями RSTP.

Multiple Spanning Tree (MST) General

General
CIST General
CIST Port
MST General
MST Port
Enhanced Passive Listening Compatibility

MSTP Instance ID:

Select	MSTP Instance ID	Root Address	Root Priority	Bridge Priority	VLAN ID
☐	1	00-00-00-00-00-00	0	32768	

1 entry.

Create
Delete
Set Values
Refresh

Описание

Страница содержит следующее поле:

- **MSTP-Instanz-ID**

Введите номер экземпляра протокола MSTP.

Допустимые значения: 1 - 64

Таблица состоит из следующих столбцов:

- **Select**

Выберите строку, которую необходимо удалить.

- **Instance ID**

Отображает номер экземпляра протокола MSTP.

- **Root Address**

Отображает MAC-адрес корневого моста.

- **Root Priority**

Отображает приоритет корневого моста.

- **Bridge Priority**

Введите в это поле приоритет моста. Значение параметра Bridge Priority является целым числом, кратным 4096, с диапазоном значений от 0 до 61440.

- **VLAN-ID**

Введите идентификатор сети VLAN. Также можно задать области с начальным идентификатором, «-», конечным идентификатором. Несколько областей или идентификаторов разделены запятой «,».

Допустимые значения: 1 — 4094

Порядок действий

Создать новую запись

1. Введите номер экземпляра MSTP в поле «MSTP Instance ID».
2. Щёлкните кнопку «Create».
3. Введите идентификатор VLAN в поле «VLAN ID».
4. Введите приоритет моста в поле «Bridge Priority».
5. Щёлкните кнопку «Set values».

Удалить записи

1. Используйте флажки перед соответствующей строкой, чтобы отметить записи, которые необходимо удалить.
2. Щёлкните кнопку «Delete» для удаления отмеченных записей из памяти. Записи удаляются из памяти устройства, и отображение данной страницы обновляется.

6.5.10.5 MST Port

Конфигурация параметров порта множественного связующего дерева

На этой странице устанавливаются параметры для портов настроенных экземпляров множественного связующего дерева.

Multiple Spanning Tree (MST) Port

General

CIST General

CIST Port

MST General

MST Port

Enhanced Passive Listening Compatibility

MSTP Instance ID: 1

MSTP Status

Copy to Table

All ports
No Change

Copy to Table

Port	MSTP Instance ID	MSTP Status	Priority	Cost Calc.	Path Cost	State	Fwd. Trans.
P0.1	1	☒	128	0	200000	Forwarding	1
P0.2	1	☒	128	0	200000	Discarding	0
P0.3	1	☒	128	0	200000	Discarding	0
P0.4	1	☒	128	0	200000	Discarding	0

Set Values

Refresh

Описание отображаемых полей

Страница содержит следующее поле:

- **MSTP Instance ID**
Выберите в раскрывающемся списке идентификатор экземпляра MSTP.

Таблица 1 состоит из следующих столбцов:

- **1-й столбец**
Отображает, что настройки действительны для всех портов.
- **MSTP Status**
Выберите в раскрывающемся списке настройку. Имеются следующие возможности настройки:
 - Enabled
 - Disabled
 - No Change: Таблица 2 осталась без изменений.
- **Copy to Table**
При нажатии кнопки настройка будет скопирована для всех портов в таблице 2.

Таблица 2 состоит из следующих столбцов:

- **Port**
Отображает все доступные порты и агрегирование каналов.
- **MSTP Instanz ID**
идентификатор экземпляра MSTP.
- **MSTP Status**
Установите флажки для портов, относящихся к этому экземпляру.

- **Priority**
Введите приоритет порта. Приоритет оценивается только в том случае, если стоимость пути равна.
Значение должно делиться на 16. Если значение не делится на 16, то оно будет автоматически адаптировано.
Диапазон значений: 0 - 240.
Заводская настройка: 128
- **Cost Calc.**
Введите расчёт стоимости пути в поле ввода. Если введено значение «0», автоматически определенное значение отобразится в следующем поле «Path Cost».
- **Path Cos**
Стоимость пути от этого порта до корневого моста. В качестве пути выбирается путь с наименьшим значением. Когда несколько портов устройства имеют одинаковое значение, то выбирается порт с самым малым номером.
Если значение в поле «Cost Calc.» равно «0», то отображается автоматически рассчитанное значение. Если введено значение, отличное от «0», то отображается значение поля «Cost Calc.».
Определение стоимости пути в основном ориентируется на скорость передачи данных. Чем выше достижимая скорость передачи, тем ниже стоимость пути.
Типичные значения стоимости пути с протоколом быстрого связующего дерева:
 - 10000 Мбит/с = 2000
 - 1000 Мбит/с = 20000
 - 100 Мбит/с = 200000
 - 10 Мбит/с = 2000000
 Значения параметров также можно задавать индивидуально.
- **Status**
Отображает текущий статус, в котором находится порт. Значения только отображаются и не могут быть настроены. Для состояния возможны следующие значения:
 - **Discarding**
Порт обменивается информацией по протоколу MSTP, но не участвует в трафике.
 - **Blocked**
В режиме блокировки принимаются пакеты BPDU.
 - **Forwarding**
Порт принимает и отправляет пакеты с данными.
- **Fwd. Trans.**
Отображает количество изменений состояния Discarding - Forwarding или Forwarding - Discarding для порта.

Порядок действий при конфигурации

1. Введите значения в поля ввода строки таблицы для конфигурируемых портов.
2. Выберите значения в раскрывающихся списках полей в строке таблицы конфигурируемого порта.
3. Щёлкните кнопку «Set values».

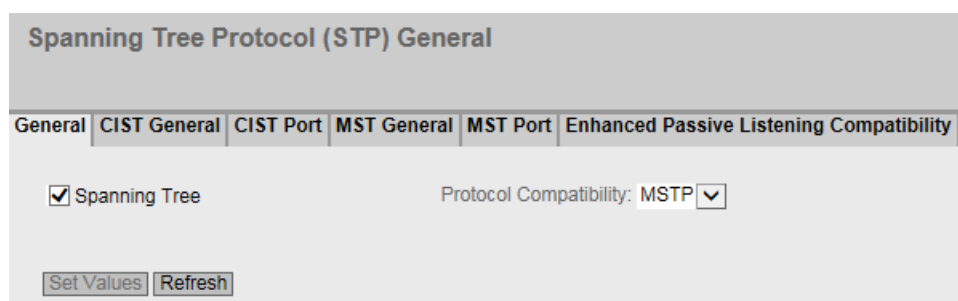
6.5.10.6 Enhanced Passive Listening Compatibility

Связующее дерево активировано.

Если активирован режим Улучшенной совместимости пассивного прослушивания, изменения топологии (Topology Change Notifications) отправляются через граничные порты RSTP. В сочетании с функцией «Edge Typ» (см. Layer 2 > Spanning Tree > CIST Port) этот параметр необходим для соединения сетей протокола связующего дерева с кольцами HRP. В противном случае кадры TCN не отправляются через граничные порты, но это необходимо для функции пассивного прослушивания для участников кольца.

Активировать функцию

На этой странице можно активировать функцию «Enhanced Passive Listening Compatibility».



Spanning Tree Protocol (STP) General

General | CIST General | CIST Port | MST General | MST Port | **Enhanced Passive Listening Compatibility**

☒ Spanning Tree Protocol Compatibility: MSTP ▼

Set Values Refresh

Описание отображаемых полей

Страница содержит следующее поле:

- **Enhanced Passive Listening Compatibility**
Активировать или деактивировать эту функцию для всего устройства.

Порядок действий при конфигурации

1. Активируйте или деактивируйте функцию «Enhanced Passive Listening Compatibility».
2. Щёлкните кнопку «Set Values»

6.5.11 Loop Detection

С помощью функции «Loop Detection» определяется, для каких портов необходимо активировать обнаружение петель. Специальные тестовые пакеты, пакеты обнаружения петель трафика, отправляются из соответствующих портов. Если эти пакеты отправляются обратно на устройство, значит имеется петля («Loop»).

«Local Loop» с участием данного устройства используется, когда пакеты снова получены на другом порте того же устройства. Когда отправленные пакеты снова получены на том же порте, на других компонентах сети возникает петля «Remote Loop».

Примечание

Петля является ошибкой в структуре сети, которую необходимо устранить. Обнаружение петель может помочь быстрее найти ошибку, но не исправит её. Обнаружение петель не подходит для увеличения доступности сети за счёт целевого установления петель.

Примечание

Обратите внимание, что обнаружение петель невозможно на следующих портах:

- Кольцевые порты
- Порты Standby
- Порты MRP Interconnection

Loop Detection

☒ Loop Detection
☐ VLAN Loop Detection

	Interval[ms]	Threshold	Timeout[s]	Remote Reaction	Local Reaction	Copy to Table
All ports	No Change	No Change	No Change	No Change	No Change	Copy to Table

Port	Setting	Interval[ms]	Threshold	Timeout[s]	Remote Reaction	Local Reaction	Status	Source Port	Source VLAN	Reset
P0.1	forwarder	1000	2	0	disable	disable	active	-	-	Reset
P0.2	forwarder	1000	2	0	disable	disable	active	-	-	Reset
P0.3	forwarder	1000	2	0	disable	disable	active	-	-	Reset
P0.4	forwarder	1000	2	0	disable	disable	active	-	-	Reset

Set Values Refresh

Описание отображаемых полей

Страница содержит следующие поля:

- **Loop Detection**
Активируйте или деактивируйте функцию обнаружение петель.
Когда опция активирована, устройство отправляет нетегированные кадры LLC.
- **VLAN Loop Detection**
Активируйте или деактивируйте функцию обнаружения петель для VLAN.
Когда опция активирована, устройство использует информацию о VLAN, заданную на соответствующем порте, для отправки кадров LLC.

Таблица 1 содержит следующие столбцы:

- **1-й столбец**
Отображает, что настройки действительны для всех портов в таблице 2.
- **Interval [ms] / Threshold / Timeout[s] / Remote Reaction / Local Reaction**
Задайте требуемые параметры.
- **Copy to Table**
При нажатии кнопки настройка будет скопирована для всех портов в таблице 2.

Таблица 2 содержит следующие столбцы:

- **Port**
Отображает доступные порты.
 - **Setting**
Укажите, как порт должен обрабатывать пакеты обнаружения петель трафика. Выберите в раскрывающемся списке одну из следующих опций:
-
- Примечание**
- Тестовые пакеты вызывают дополнительную нагрузку на сеть. Рекомендуется использовать только отдельные коммутаторы, например на ответвлениях кольца, которые должны быть настроены как «Sender», а остальные как «Forwarder».
-
- sender
Пакеты для обнаружения петель отправляются и пересылаются.
 - forwarder
Пакеты для обнаружения петель от других устройств пересылаются.
 - blocked
Пересылка пакетов для обнаружения петель заблокирована.
- **Interval[ms]**
Определяет интервал передачи пакетов обнаружения петель в миллисекундах.
 - **Threshold**
Введите число, чтобы определить, после скольких полученных пакетов обнаружения петель предполагается выход из петли.
 - **Timeout[s]**
Задайте время в секундах, по истечении которого устройство автоматически вернётся в состояние, в котором оно находилось до петли. Когда установлено значение «0», вам необходимо повторно активировать порт вручную после петли с помощью кнопки «RollBack». Также можете сбросить настройки порта, отсоединив и снова присоединив кабель к порту.
 - **Remote Reaction**
Задайте, как порт должен реагировать при возникновении удалённой петли. Выберите в раскрывающемся списке одну из двух опций:
 - No action: Петля не влияет на порт.
 - Disable: Порт блокируется.
 - **Local Reaction**
Задайте, как порт должен реагировать при возникновении локальной петли. Выберите в раскрывающемся списке одну из двух опций:
 - No action: Петля не влияет на порт.
 - Disable: Порт блокируется.
 - **Status**
Отображает, включено или выключено обнаружение петель для данного порта.
 - **Source Port**
Отображает порт получателя пакета для обнаружения петель, который вызвал последнюю реакцию.

- **Source Port**
В этом поле отображается идентификатор VLAN пакета для обнаружении петель, который вызвал последнюю реакцию.
Обязательное условие для этого установка флажка напротив "VLAN Loop Detection".
- **RollBack**
После устранения петли в сети нажмите кнопку «RollBack», чтобы сбросить порт.

Изменение настроенного статуса порта с помощью функции Loop Detection

Конфигурацию статуса порта можно изменить с помощью функции «Loop Detection». Например, если порт был деактивирован администратором (disabled), порт можно повторно активировать после перезапуска устройства с помощью «Loop Detection» (enabled). Состояние порта «Link down» не изменяется функцией «Loop Detection».

6.5.12 Link Aggregation

6.5.12.1 General

Объединение сетевых подключений для резервирования и увеличения пропускной способности

Функция Link Aggregation в соответствии со стандартом IEEE 802.3AD позволяет объединять несколько соединений между соседними устройствами для достижения более высокой пропускной способности и дополнительно для обеспечения надёжности.

Здесь порты на обоих связанных устройствах объединяются в группы соединений, и затем устройства подключаются друг к другу через эти порты. Протокол управления агрегированием каналов (LACP) из стандарта IEEE 802.3AD используется для правильного назначения портов связанному устройству.

Примечание

Если порт назначен для функции Link Aggregation, но не активен (например, в случае Link Down), отображаемые значения могут отличаться от значений, настроенных для Link Aggregation.

Если порт в функции Link Aggregation становится активным, отдельные настройки порта, например пересылка DCP, перезаписываются заданными в Link Aggregation значениями.

Отображение сконфигурированных групп соединений

Все сконфигурированные агрегирования каналов отображаются на этой странице.

Link Aggregation

General

LACP Timeout

Select	Port	Link Aggregation Name	MAC Address	Status	LACP	Frame Distribution	VLAN Mode	P0.1	P0.2
☐	AG1		08-00-07-70-84-b9	☒	off	Destination&Source MAC	Hybrid	-	-

1 entry.

Create

Delete

Set Values

Refresh

Описание отображаемых полей

Таблица состоит из следующих столбцов:

- Select**
 Выберите строку, которую необходимо удалить.
- Port**
 Отображает номер виртуального порта этого агрегирования каналов. Имя назначается внутри прошивки.
- Link Aggregation Name**
 Отображает имя агрегирования каналов. Это имя может быть указано пользователем при конфигурировании. Имя не является необходимым, но может быть полезно для различения различных агрегирований каналов.
- MAC Address**
 Отображает MAC-адрес.
- Status**
 Активируйте или деактивируйте агрегирование каналов.
- LACP**
 - On
Активирует отправку пакетов LACP.
 - Off
Деактивирует отправку пакетов LACP.
- Frame Distribution - Destination&Source MAC**
 Распределение пакетов по отдельным каналам агрегации основано на комбинации MAC-адреса назначения и источника.

- **VLAN Mode**

Задайте, как агрегирование каналов вводится в сети VLAN:

- Hybrid
Агрегирование каналов отправляет тегированные и нетегированные пакеты. Он не является автоматически участником сети VLAN.
- Trunk
Агрегирование каналов отправляет только тегированные пакеты и автоматически участвует во всех сетях VLAN.
- Access
Порт относится к коммутатору провайдера, который поддерживает функцию туннеля Q-in-Q VLAN.

- **Port**

Отображает порты, которые принадлежат этому агрегированию каналов. В раскрывающемся списке можно выбрать следующие значения:

- (Disabled)
Агрегирование каналов деактивировано.
- «a» (active)
Порт отправляет пакеты LACP и принимает участие в агрегировании каналов только в случае получения пакетов LACP.
- «p» (Passive)
Порт принимает участие в агрегировании каналов только в случае получения пакетов LACP.
- «o» (On)
Порт принимает участие в агрегировании каналов и не отправляет пакеты LACP.

Примечание

В рамках агрегирования каналов возможны только порты со следующей конфигурацией:

- все порты с «o»
 - все порты с «a» или «p».
-

Порядок действий при конфигурации

Основное перед конфигурированием

1. Сначала выберите порты, которые необходимо подключить к агрегированию каналов между устройствами.
2. Сконфигурируйте агрегирование каналов на устройствах.
3. Примените конфигурацию ко всем устройствам.
4. На последнем этапе проведите разводку кабелей.

Примечание

Если осуществлять разводку и соединение жгутов кабелей перед конфигурацией, возможно возникновение петель в сети. Рассматриваемая сеть будет серьезно перегружена или может произойти сбой.

Создание нового агрегирования каналов

1. Щёлкните кнопку «Create» для создания новой Link Aggregation. Таким образом, будет создана новая пустая строка.
2. Выберите порты, которые должны принадлежать к этому агрегированию каналов.
3. Щёлкните кнопку «Set values».

Удаление агрегирования каналов

1. Установите флажок в строке, которую необходимо удалить. Повторите процедуру для всех записей, которые необходимо удалить.
2. Щёлкните кнопку «Delete».

Изменение агрегирования каналов

1. В обзоре щёлкните соответствующую запись в таблице, чтобы изменить конфигурацию созданной Link Aggregation.
2. Произведите все изменения.
3. Щёлкните кнопку «Set values».

6.5.12.2 Время ожидания LACP

Конфигурирование времени ожидания LACP

Стандарт IEEE 802.3ad определяет два возможных значения длительности времени ожидания: «Long» (90 секунд) и «Short» (3 секунды). Это значение определяет временной интервал, через который отправляются пакеты LACPDU. Значение «Long» настроено как значение по умолчанию для всех портов. Для того чтобы включить симметричную конфигурацию LACP, можно дополнительно установить значение «Short». Выберите одно и то же значение времени ожидания для всех портов агрегирования каналов.

Link Aggregation Control Protocol (LACP) Timeout

General
LACP Timeout

Port	Setting	Copy to Table
All ports	No Change	Copy to Table

Port	Setting
P0.1	Long
P0.2	Long
P0.3	Long
P0.4	Long
P0.5	Long

Set Values
Refresh

Описание отображаемых полей

Таблица 1 состоит из следующих столбцов:

- **1-й столбец**
Отображает, что настройки действительны для всех портов в таблице 2.
- **Setting**
Выберите в раскрывающемся списке настройку. Имеются следующие возможности настройки:
 - Short
Значение времени ожидания LACP составляет 3 секунды.
 - Long
Значение времени ожидания LACP составляет 90 секунды..
 - No Change
Таблица 2 осталась без изменений.
- **Copy to Table**
Если нажать данную кнопку, то настройки будут применены для всех портов в Таблице 2.

Таблица 2 состоит из следующих столбцов:

- **Port**
Отображает все доступные порты. Порт складывается из номера модуля и номера порта, например, порт 0.1 означает модуль 0, порт 1.
- **Setting**
Выберите значение «Short» или «Long» для этого порта.

6.5.13 DCP Forwarding

Приложения

Протокол DCP используется в ПО STEP 7 и SINEC PNI для конфигурации и диагностики. В заводских настройках DCP активирован на всех портах, т.е. полученные пакеты DCP пересылаются на все порты. С помощью этой опции имеется возможность отключить пересылку пакетов для отдельных портов, например, чтобы изолировать отдельные области сети от конфигурации с помощью ПО SINEC PNI или разделить всю сеть на более мелкие подсети для настройки и диагностики.

Примечание

Конфигурация PROFINET

Поскольку в отношении DCP речь идёт о протоколе PROFINET, выполненная здесь конфигурация эффективна лишь в сети VLAN, связанной с интерфейсом TIA.

Все порты устройства отображаются на этой странице. Рядом с каждым отображаемым портом находится раскрывающийся список для выбора функций.

Discovery and Basic Configuration Protocol (DCP) Forwarding		
	Setting	Copy to Table
All ports	No Change ▼	Copy to Table
Port	Setting	
P0.1	Forward ▼	⬆ ⬇ ⬆
P0.2	Forward ▼	
P0.3	Forward ▼	
P0.4	Forward ▼	
Set Values Refresh		

Описание отображаемых значений

Таблица 1 состоит из следующих столбцов:

- **1-й столбец**
Отображает, что настройки действительны для всех портов в таблице 2.
- **Setting**
Выберите в раскрывающемся списке настройку. Если выбрано значение «No Change», то запись в таблице 2 не изменяется.
- **Copy to Table**
При нажатии кнопки настройка будет скопирована для всех портов в таблице 2.

Таблица 2 состоит из следующих столбцов:

- **Port**
Отображает доступные порты. Порт складывается из номера модуля и номера порта, например, порт 0.1 означает модуль 0, порт 1.
- **Setting**
Выберите в раскрывающемся списке, должен ли порт блокировать или пересылать исходящие пакеты DCP. Существуют следующие возможности на выбор:
 - Forward
Через этот порт пересылаются пакеты DCP.
 - Block
Через этот порт не пересылаются исходящие пакеты DCP. Приём по-прежнему возможен через этот порт.

Порядок действий при конфигурации

1. Выберите опцию в раскрывающемся списке в строке после номера порта, какие порты должны поддерживать отправку пакетов DCP.
2. Щёлкните кнопку «Set values».

6.5.14 LLDP

Определение топологии сети

Протокол LLDP (Link Layer Discovery Protocol) определён в стандарте IEEE 802.1AB.

LLDP - это протокол для определения топологии сети. Компоненты сети обмениваются информацией с соседними устройствами через протокол LLDP.

Сетевые компоненты, поддерживающие протокол LLDP, имеют LLDP-агент. LLDP-агент периодически отправляет собственную информацию и получает информацию от подключённых устройств. Полученная информация сохраняется в устройстве.

Приложения

Сеть PROFINET использует протокол LLDP для диагностики топологии. В заводских настройках протокол LLDP активирован для всех портов, т.е. пакеты LLDP отправляются и принимаются на всех портах. С помощью этой функции имеется возможность включить или выключить отправку и/или приём для каждого порта.

Setting	Copy to Table
All ports No Change	Copy to Table

Port	Setting
P0.1	Rx & Tx
P0.2	Rx & Tx
P0.3	Rx & Tx
P0.4	Rx & Tx

Set Values Refresh

Описание отображаемых полей

Таблица 1 состоит из следующих столбцов:

- **1-й столбец**
Отображает, что настройки действительны для всех портов.
- **Setting**
Выберите в раскрывающемся списке настройку. Если выбрано значение «No Change», то запись в таблице 2 не изменяется.
- **Copy to Table**
При нажатии кнопки настройка будет скопирована для всех портов в таблице 2.

Таблица 2 состоит из следующих столбцов:

- **Port**
Отображает доступные порты. Порт складывается из номера модуля и номера порта, например, порт 0.1 означает модуль 0, порт 1.
- **Setting**
Выберите в раскрывающемся списке, должен ли порт отправлять или получать пакеты LLDP. Существуют следующие возможности на выбор:
 - **Rx**
Этот порт может только принимать пакеты LLDP.
 - **Tx**
Этот порт может только отправлять пакеты LLDP.
 - **Rx & Tx**
Этот порт может отправлять и принимать пакеты LLDP.
 - **-**
Этот порт не может ни отправлять, ни принимать пакеты LLDP.

Порядок действий при конфигурации

1. Выберите в раскрывающемся списке «Setting» функции LLDP порта.
2. Щёлкните кнопку «Set values».

6.5.15 Fiber Monitoring Protocol

Требования

- Функцию Fiber Monitoring можно использовать только с диагностируемыми трансиверами. Смотри документацию к устройствам.
- Чтобы использовать функцию Fiber Monitoring, активируйте протокол LLDP. Информация Fiber Monitoring прикрепляется к пакетам LLDP.

Контроль оптических участков

С помощью функции Fiber Monitoring можно отслеживать мощность приёма и падение мощности на оптических линиях между двумя коммутаторами.

Если опция Fiber Monitoring активируется на оптическом порте, через пакеты LLDP устройство передаёт текущее значение мощности передачи порта своему партнёру по соединению. Параллельно с процессом отправки устройство проверяет, получает ли партнёр по соединению соответствующую информацию.

Независимо от того, получает ли коммутатор IE диагностическую информацию от своего партнёра по соединению, он отслеживает измеренную на оптическом порте мощность приёма на предмет установленных предельных значений.

Если у партнёра по соединению активирована функция Fiber Monitoring, партнёр по соединению передаёт текущее значение мощности передачи порта на устройство.

Устройство сравнивает полученное значение мощности передачи с фактически полученной мощностью. Падение мощности на участке происходит из-за разницы между принимаемой и передаваемой мощностью. Рассчитанное падение мощности также отслеживается для установленных предельных значений.

Если значение мощности приёма или величина падения мощности ниже или выше установленных предельных значений, запускается событие (Event). Можно установить два предельных значения для сообщений с разными уровнями серьёзности: «Warning» и «Critical».

В пункте меню System > Events > Configuration можно задать, как IE-коммутатор отображает событие.

Примечание

Когда активирована функция Fiber Monitoring и подключаемый диагностируемый трансивер извлекается, Fiber Monitoring автоматически деактивируется для данного порта, а установленные предельные значения и возможное состояние имеющейся ошибки удаляются.

Fiber Monitoring Protocol (FMP)					
Port	State	Rx Power [dBm] Maintenance Required (warning)	Rx Power [dBm] Maintenance Demanded (critical)	Power Loss [dB] Maintenance Required (warning)	Power Loss [dB] Maintenance Demanded (critical)
P0.1	☒	-4	-6	-50	-55
P0.2	☒	-25	-27	-50	-55
P0.4	☒	-10	-12	-50	-55

Описание отображаемых полей

В таблице можно определить контролируемые предельные значения измеренной принимаемой мощности и расчётного падения мощности.

- Port**
Отображает оптические порты, которые поддерживают функцию Fiber Monitoring. Это зависит от трансиверов.
- Status**
Активируйте или деактивируйте Fiber Monitoring.
По умолчанию функция деактивирована.
- Rx Power [dBm] Maintenance Required (Warning)**
Введите значение, при котором появится сообщение об ухудшении качества принимаемой мощности информирующее о уровне серьёзности «Warning».
Если ввести значение «0», мощность приёма не отслеживается.
Значение по умолчанию зависит от соответствующего трансивера.

6.5 Меню «Layer 2»

- **Rx Power [dBm] Maintenance Required (Critical)**
Введите значение, при котором появится сообщение об ухудшении качества принимаемой мощности информирующее о уровне серьезности «Critical».
Если ввести значение «0», мощность приёма не отслеживается.
Значение по умолчанию зависит от соответствующего трансивера.
- **Power Loss [dB] Maintenance Required (Warning)**
Введите значение, при котором появится сообщение информирующее о уровне серьезности «Warning» падения мощности соединения.
Если ввести значение «0», падение мощности не отслеживается.
Значение по умолчанию: -50 дБ
- **Power Loss [dB] Maintenance Demanded (Critical)**
Введите значение, при котором появится сообщение информирующее о уровне серьезности «Critical» падения мощности соединения.
Если ввести значение «0», падение мощности не отслеживается.
Значение по умолчанию: -55 дБ

Порядок действий при конфигурации

Активировать мониторинг оптических волокон

Для того чтобы активировать мониторинг порта, выполните следующие действия:

1. Установите соответствующий флажок в столбце «Status».
2. Для вашей архитектуры введите осмысленные значения, для которых необходимо получать информацию об ухудшении принимаемой мощности и падении мощности соединения.
3. Щёлкните кнопку «Set values».

Отключить мониторинг оптических волокон

Для того чтобы деактивировать мониторинг порта, выполните следующие действия:

1. Удалите соответствующий флажок в столбце «Status».
2. Щёлкните кнопку «Set values».

Для того чтобы деактивировать только мониторинг производительности Rx или падения мощности, выполните следующие действия:

1. Введите значение «0» в соответствующее поле.
2. Щёлкните кнопку «Set values».

6.5.16 Unicast

6.5.16.1 Фильтрация

Фильтрация адресов

В данной таблице показаны исходные адреса пакетов Unicast, которые были введены статически посредством параметризации пользователем.

На этой странице также задаются статические фильтры Unicast.

Зависимость от режима «Base Bridge Mode»

Отображаемые поля зависят выбора заданного режима «Base Bridge Mode». При изменении режима «Base Bridge Mode» существующие записи будут потеряны. На следующих рисунках показано различное содержание страницы интерфейса WBM для двух режимов работы «802.1Q VLAN Bridge» и «802.1D Transparent Bridge».

Базовый режим моста: 802.1Q VLAN Bridge

Filtering

Filtering Locked Ports Learning Blocking

VLAN ID:

MAC Address:

Select	VLAN ID	MAC Address	Status	Port
☐	1	00-1b-1b-72-55-a5	Static	P0.1

1 entry.

Create Delete Set Values Refresh

Базовый режим моста: 802.1D Transparent Bridge

Filtering

Filtering Locked Ports Learning Blocking

MAC Address:

Select	MAC Address	Status	Port
☐	00-1b-1b-a5-5d-55	Static	P0.1

1 entry.

Create Delete Set Values Refresh

Описание отображаемых полей

Страница может содержать следующие поля:

- **VLAN ID**
Выберите идентификатор VLAN, для которого статически конфигурируется новый MAC-адрес. Когда ничего не задано, используется настройка по умолчанию «VLAN1».
- **MAC Address**
Введите здесь MAC-адрес.

Таблица содержит следующие столбцы:

- **Select**
Выберите строку, которую необходимо удалить.
- **VLAN ID**
Отображает идентификатор VLAN, которому назначен данный MAC-адрес.
- **MAC Address**
Отображает MAC-адрес участника, который был запомнен устройством или сконфигурирован пользователем.
- **Status - Static**
Показывает состояние каждой записи адреса. Адрес был статически введен пользователем. Статические адреса хранятся постоянно, т. е. они не удаляются по истечении времени старения или при перезапуске устройства. Они должны быть удалены пользователем.
- **Port**
Отображает порт, через который можно осуществлять обмен данными с участником с заданным адресом. Полученные устройством пакеты, целевой адрес которых совпадает с этим адресом, будут переданы далее на этот порт.

Примечание

Можно указать только **один** порт для адресов Unicast.

Порядок действий при конфигурации

Выполнить следующие действия для редактирования записей.

Создать новую запись

1. В режиме «Base Bridge Mode: 802.1Q VLAN Bridge» выберите соответствующий идентификатор VLAN.
2. Введите MAC-адрес в поле ввода «MAC Address».
3. Щёлкните кнопку «Create» для создания новой записи в таблице.
4. Щёлкните кнопку «Refresh».
5. Выберите в раскрывающемся списке соответствующий порт.
6. Щёлкните кнопку «Set values».

Изменение записи

1. Выберите соответствующий порт из выпадающего меню.
2. Щёлкните кнопку «Set values».

Удаление записи

1. Установите флажок в строке, которую необходимо удалить.
Повторите процедуру для всех записей, которые необходимо удалить.
2. Щёлкните кнопку «Delete», чтобы удалить выбранные записи из таблицы фильтров.
3. Щёлкните кнопку «Refresh».

6.5.16.2 Locked Ports

Активация контроля доступа

На этой странице можно заблокировать отдельные порты для неизвестных участников.

Когда активирована функция блокировки порта, пакеты приходящие на этот порт с неизвестных MAC-адресов немедленно отклоняются. Пакеты от известных участников принимаются портом. Порт принимает только статические MAC-адреса, которые были ранее созданы вручную или с помощью функций «Start learning» и «Stop learning».

Для автоматического статического ввода всех подключённых участников существует функция автоматического запоминания (см. Layer 2 > Unicast > Learning).

Port	Setting
P0.1	☐
P0.2	☐
P0.3	☐
P0.4	☐

Set Values Refresh

Описание отображаемых полей

Таблица 1 состоит из следующих столбцов:

- **1-й столбец**
Отображает, что настройки действительны для всех портов в таблице 2.
- **Setting**
Выберите в раскрывающемся списке настройку. Имеются следующие возможности настройки:
 - Enabled
Активирует функцию блокировки порта.
 - Disabled
Деактивирует функцию блокировки порта.
 - No Change
Таблица 2 осталась без изменений.
- **Copy to Table**
При нажатии кнопки настройка будет скопирована для всех портов в таблице 2.

Таблица 2 состоит из следующих столбцов:

- **Port**
В этом столбце отображаются все порты, доступные в устройстве.
- **Setting**
Активируйте или деактивируйте функцию контроля доступа для порта..

Порядок действий при конфигурации

Активировать контроль доступа для одного порта

1. Установите флажок в соответствующей строке таблицы 2.
2. Чтобы применить изменения, щёлкните кнопку «Set Values».

Активировать контроль доступа для всех портов

1. В таблице 1 в раскрывающемся списке «Setting» выберите запись «Enabled».
2. Щёлкните кнопку «Copy to Table». Флажок активирован для всех портов в таблице 2.
3. Чтобы применить изменения, щёлкните кнопку «Set Values».

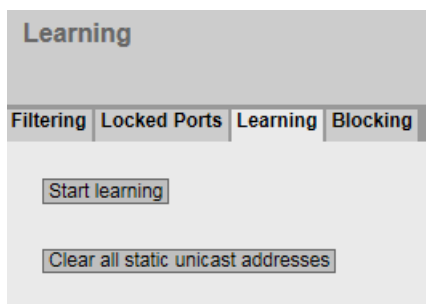
6.5.16.3 Обучение

Запустить / остановить процесс обучения

С помощью автоматического обучения все подключённые устройства могут быть автоматически статически занесены в таблицу фильтров Unicast. Процесс обучения завершается только после нажатия кнопки «Stop learning». Таким образом, обучение можно проводить в течение нескольких минут или, в больших сетях, в течение нескольких часов, чтобы найти всех участников. Можно найти лишь тех участников, которые отправляют пакеты во время процесса обучения. После последующего включения функции блокировки порта на соответствующие порты будут приниматься только пакеты от участников, известных после окончания процесса обучения (статические одноадресные записи).

Примечание

Если функция блокировки порта уже активна на отдельных портах до автоматического обучения, то адреса на этих портах не запоминаются. Таким образом, можно проводить обучение только на определенных портах. Для этого сначала активируйте функцию блокировки порта на портах, которые не должны запоминать адреса.



Порядок действий при конфигурации

Запоминание адресов

1. Нажмите кнопку «Start learning», чтобы начать процесс обучения.
После начала процесса обучения кнопка «Start learning» заменяется кнопкой «Stop learning».
Теперь устройство запоминает адреса подключённых устройств, пока процесс не будет остановлен.
2. Нажмите кнопку «Stop learning», чтобы завершить процесс обучения.
Затем кнопка «Stop learning» снова заменяется кнопкой «Start learning». Полученные записи сохраняются и отображаются в меню Layer 2 > Unicast > Filtering.

Примечание

При очень высокой скорости передачи данных, статически введенные адреса Unicast могут отображаться как изученные адреса в таблице Unicast. В этом случае рекомендуется следующий порядок действий:

1. Нажмите кнопку «Start learning», чтобы начать процесс обучения.
2. Запустить обмен данными.
3. Подождите, пока в таблице Unicast все MAC-адреса будут отображаться как «Learnt» в (меню Information > Unicast).
4. Заблокируйте порты (меню Layer 2 > Unicast > Locked Ports).
5. Нажмите кнопку «Stop learning», чтобы остановить процесс обучения.

Удалить все статические адреса Unicast

1. Нажмите кнопку «Clear all static unicast addresses», чтобы удалить все статические записи.

В больших сетях с очень высоким числом участников автоматическое обучение может привести к возникновению множества нежелательных статических записей. Для того чтобы не удалять их по отдельности, можно использовать эту кнопку для удаления всех статических записей. Эта функция деактивирована во время автоматического обучения.

Примечание

Удаление может занять некоторое время, в зависимости от числа записей.

6.5.16.4 Blocking

Блокировать пересылку неизвестных одноадресных пакетов

На этой странице пересылка неизвестных одноадресных пакетов заблокирована для отдельных портов.

Unknown Unicast Blocking

Filtering
Locked Ports
Learning
Blocking

Setting
Copy to Table

All ports
No Change
Copy to Table

Port	Setting
P0.1	☐
P0.2	☐
P0.3	☐

Set Values
Refresh

Описание отображаемых значений

Таблица 1 состоит из следующих столбцов:

- **1-й столбец**
Отображает, что настройки действительны для всех портов в таблице 2.
- **Setting**
Выберите в раскрывающемся списке настройку. Имеются следующие возможности настройки:
 - Enabled
Блокировка одноадресных пакетов активирована.
 - Disabled
Блокировка одноадресных пакетов деактивирована.
 - No Change
Таблица 2 осталась без изменений.
- **Copy to Table**
При нажатии кнопки настройка будет скопирована для всех портов в таблице 2.

Таблица 2 состоит из следующих столбцов:

- **Port**
Отображает доступные порты. Порт складывается из номера модуля и номера порта, например, порт 0.1 означает модуль 0, порт 1.

Примечание

Кольцевое резервирование/режим ожидания

Когда активировано кольцевое резервирование или режим ожидания, порты, настроенные для этого, исключаются из блокировки одноадресной рассылки.

- **Setting**
Активируйте или деактивируйте блокировку одноадресных пакетов.

Порядок конфигурации

Активировать блокировку для одного порта

1. Установите флажок в соответствующей строке таблицы 2.
2. Чтобы применить изменения, щёлкните кнопку «Set Values».

Активировать блокировку для всех портов

1. В таблице 1 в раскрывающемся списке «Setting» выберите запись «Enabled».
2. Щёлкните кнопку «Copy to Table». Флажок активирован для всех портов в таблице 2.
3. Чтобы применить изменения, щёлкните кнопку «Set Values».

6.5.17 Multicast

6.5.17.1 Groups

Применения многоадресной рассылки

В большинстве случаев пакет с адресом Unicast отправляется конкретному получателю. Когда приложение должно отправлять одни и те же данные нескольким получателям, объем отправляемых данных можно уменьшить, отправив данные всем с помощью многопунктового адреса. Для некоторых приложений существуют фиксированные многопунктовые адреса (NTP, IETF1-Audio, IETF1-Video и т. д.).

Снижение нагрузки на сеть

В отличие от пакетов Unicast, пакеты Multicast оказывают более высокую нагрузку на устройство. Как правило, пакеты Multicast отправляются на все порты. Существуют следующие возможности снижения нагрузки от пакетов Multicast:

- Статический ввод адресов в таблицу фильтрации Multicast.
- Динамический ввод адресов путём прослушивания пакетов параметризации IGMP (конфигурация IGMP).
- Активное динамическое распределение адресов через пакеты GMRP.

Все упомянутые процедуры приводят к тому, что пакеты Multicast отправляются только на те порты, для которых был введён соответствующий адрес.

Пункт меню «Multicast» отображает пакеты Multicast, которые в настоящее время введены в таблицу фильтров, с их портами назначения параметризованными пользователем (статически).

Зависимость от режима «Base Bridge Mode»

Отображаемые поля зависят выбора заданного режима «Base Bridge Mode». При изменении режима «Base Bridge Mode» существующие записи будут потеряны. На следующих рисунках показано различное содержание страницы интерфейса WBM для двух режимов работы «802.1Q VLAN Bridge» и «802.1D Transparent Bridge».

Базовый режим моста: 802.1Q VLAN Bridge

Multicast Configuration

Groups **IGMP** GMRP Blocking

VLAN ID: **VLAN1** ▼

MAC Address:

Select	VLAN ID	MAC Address	Status	P0.1	P0.2	P0.3
☐	1	01-00-5e-00-00-00	Static	-	-	-

1 entry.

Create Delete Set Values Refresh

Базовый режим моста: 802.1D Transparent Bridge

Multicast Configuration

Groups **IGMP** GMRP Blocking

MAC Address:

Select	MAC Address	Status	P0.1	P0.2	P0.3
☐	01-00-5a-00-00-00	Static	-	-	-

1 entry.

Create Delete Set Values Refresh

Описание отображаемых полей

Страница может содержать следующие поля:

- **VLAN ID**
Если щёлкнуть это текстовое поле, предлагается раскрывающийся список. Здесь можно выбрать идентификатор VLAN нового MAC-адреса, который необходимо настроить.
- **MAC Address**
Здесь вводится новый настраиваемый многопунктовый MAC-адрес.

Таблица состоит из следующих столбцов:

- **Select**
Выберите строку, которую необходимо удалить.
- **VLAN ID**
Здесь отображается идентификатор VLAN той сети VLAN, которой назначен многоадресный MAC-адрес из этой строки.
- **MAC Address**
Отображает многопунктовые MAC-адреса, запомненные устройством или сконфигурированные пользователем.

- **Status - Static**
Показывает состояние каждой записи адреса. Адрес был статически введен пользователем. Статические адреса хранятся постоянно, т. е. они не удаляются по истечении времени старения или при перезапуске устройства. Они должны быть удалены пользователем.
- **Список портов**
Для каждого порта имеется столбец. Принадлежность к группе многоадресной рассылки указано в каждом столбце. В раскрываемом списке доступны следующие возможности выбора:
 - M
(Member) Через этот порт отправляются пакеты Multicast.
 - R
(Registered) Участник группы Multicast, регистрация выполнена с помощью пакета GMRP.
 - I
(IGMP) Участник группы Multicast, регистрация выполнена с помощью пакета IGMP. Данное значение присваивается только динамически.
 - –
Не является участником группы Multicast. Через этот порт не отправляются пакеты Multicast с определенным MAC-адресом Multicast.
 - F
(Forbidden) Не является участником группы Multicast. Кроме того, этот адрес нельзя динамически запомнить через GMRP или IGMP.

Порядок действий при конфигурации

Создать новую запись

Примечание

Когда протокол GMRP активирован, нельзя создавать статические многоадресные записи.

1. В режиме «Base Bridge Mode: 802.1Q VLAN Bridge» выберите требуемый VLAN ID из раскрываемого списка «VLAN ID».
2. Введите в поле ввода «MAC Adress» MAC-адрес.
3. Щёлкните кнопку «Create». В таблице создаётся новая запись.
4. Задайте MAC-адреса соответствующим портам.
5. Щёлкните кнопку «Set values».

Удаление записи

1. Установите флажок в строке, которую необходимо удалить.
2. Щёлкните кнопку «Delete».
Все отмеченные записи удаляются, а их отображение обновляется.

Создание многопунктовых адресов уровня 2 с помощью сценария и GMRP

Когда необходимо создать несколько многопунктовых адресов уровня 2 с помощью сценария, протокол GMRP необходимо деактивировать во время выполнения сценария. Выполните следующие действия:

1. Если протокол GMRP активен, деактивируйте его. Конфигурирование протокола GMRP выполняется на странице Layer 2 > Multicast > GMRP.
2. Выполните скрипт.
3. Активируйте протокол GMRP только после того, как сценарий полностью завершится и будут созданы многопунктовые адреса уровня 2.

6.5.17.2 IGMP

Функция

Устройство поддерживает функции «IGMP Snooping» и «IGMP Querier». Когда пункт «IGMP Snooping» активирован, пакеты IGMP (Internet Group Management Protocol) оцениваются, и таблица фильтрации Multicast обновляется с учётом этой информации. Когда «IGMP Querier» также активирован, устройство отправляет запросы IGMP, которые запускают ответы от участников сети, поддерживающих протокол IGMP.

Время старения отслеживания IGMP

В этом меню можно задать время старения конфигурации IGMP. По истечении этого времени записи, созданные протоколом IGMP, удаляются из таблицы адресов, если они не обновлены новым пакетом IGMP.

Назначение применяется ко всем портам и сетям VLAN; специальная конфигурация невозможна.

Время старения отслеживания IGMP в зависимости от генератора запросов

IE-коммутатор как генератор запросов IGMP

Когда IE-коммутатор используется как генератор запросов IGMP, интервал запроса составляет 125 секунд. Установите значение параметра «IGMP Snooping Aging Time» как минимум на 250 секунд.

Другие генераторы запросов IGMP

Когда используется другой генератор запросов IGMP, значение поля «IGMP Snooping Aging Time» должно быть как минимум в два раза больше, чем интервал запроса.

Описание отображаемых полей

Internet Group Management Protocol (IGMP) Snooping & Querier

Groups IGMP GMRP Blocking MLD

☐ IGMP Snooping

IGMP Snooping Aging Time[s]: 300

☐ IGMP Querier

IGMP Snooping Switch IP Address: 0.0.0.0

IGMP Snooping Version: 3

Snooping Report Processing: Client Ports

Snooping Report Forward: Router Ports

VLAN ID	IGMP Snooping	IGMP Querier
1	☐	☐

Set Values Refresh

Страница содержит следующие поля:

- IGMP Snooping**
 Активируйте или деактивируйте отслеживания IGMP. Функция позволяет назначать IP-адреса группам многоадресной рассылки. Когда опция активирована, записи IGMP добавляются в таблицу фильтрации многоадресной маршрутизации и пересылаются пакеты IGMP.
- IGMP Snooping Aging Time[s]**
 Введите в это поле значение времени старения в секундах. Значение по умолчанию равно 300 секундам.
 Действительные значения: 130 - 1225 секунд
- IGMP Querier**
 Активируйте или деактивируйте «IGMP Querier». Устройство отправляет запросы IGMP.
- IGMP Snooping Switch IP-Address**
 Данный IP-адрес используется для отправки запросов протокола IGMP. Когда в сети отправлено несколько запросов генератора запросов IGMP, запрашивающая сторона с наименьшим IP-адресом берет на себя функцию генератора запросов. Когда IP-адрес установлен на 0.0.0.0, собственный IP-адрес используется для отправки запросов протокола IGMP. В качестве альтернативы можно ввести любой IP-адрес, чтобы иметь возможность при наличии нескольких генераторов запросов Querier задать в сети последовательность активного генератора запросов Querier.
- IGMP Snooping Version**
 Выберите в раскрывающемся списке IGMP Snooping Version.

- **Snooping Report Processing**

Возможны следующие настройки:

- Client Ports
Устройство обрабатывает соединения IGMP только на клиентских портах.
- All Ports
Устройство обрабатывает соединения IGMP только на клиентских портах.

- **Snooping Report Forward**

Возможны следующие настройки:

- All Ports
Устройство пересылает соединения IGMP на всех портах.
- Router Ports
Устройство пересылает соединения IGMP на порты маршрутизатора.
- Non Edge Ports
Устройство пересылает соединения IGMP на всех портах, которые не являются граничными портами.

Таблица состоит из следующих столбцов:

- **VLAN ID**

Идентификатор сети VLAN, для которого необходимо активировать IGMP Snooping или IGMP Querier.

- **IGMP Snooping**

Установите флажки в этом столбце для тех сетей VLAN, для которых необходимо активировать IGMP Snooping. Установки в этом столбце вступают в силу только при активации IGMP Snooping для устройства (первый флажок на этой странице).

- **IGMP Querier**

Установите флажки в этом столбце для тех сетей VLAN, для которых должен быть активирован IGMP Querier.

Если для устройства активирован флажок IGMP Snooping, а для сети VLAN активирован флажок IGMP Snooping, то выполняется IGMP Querier, когда в таблице активирован соответствующий флажок. Это действительно независимо от состояния флажка IGMP Querier для устройства.

Порядок действий при конфигурации

1. Установите флажок напротив «IGMP Snooping».
2. Введите в поле «IGMP Snooping Aging Time» значение времени старения в секундах.
3. Установите флажок напротив «IGMP Querier».
4. Щёлкните кнопку «Set values».

6.5.17.3 GMRP

Активация GMRP

На этой странице можно индивидуально задать для каждого порта, будет ли использоваться GMRP. Когда протокол GMRP деактивирован для порта, для него не выполняется регистрация, и порт не может отправлять пакеты GMRP.

Для функционирования протокола GMRP необходимо активировать эту функцию глобально и на портах.

GARP Multicast Registration Protocol (GMRP)

Groups | IGMP | **GMRP** | Blocking

☐ GMRP

Setting	Copy to Table
All ports No Change ▼	Copy to Table

Port	Setting
P0.1	☒
P0.2	☒
P0.3	☒

Set Values Refresh

Описание отображаемых полей

Страница содержит следующее поле:

- **GMRP**
Активируйте или деактивируйте функцию протокола GMRP.

Таблица 1 состоит из следующих столбцов:

- **1-й столбец**
Отображает, что настройки действительны для всех портов в таблице 2.
- **Setting**
Выберите в раскрывающемся списке настройку. Имеются следующие возможности настройки:
 - Enabled
Активирует отправку пакетов GMRP.
 - Disabled
Деактивирует отправку пакетов GMRP.
 - No Change
Таблица 2 осталась без изменений.
- **Copy to Table**
Если нажать данную кнопку, то настройки будут применены для всех портов в Таблице 2.

Таблица 2 состоит из следующих столбцов:

- **Port**
В этом столбце отображаются все порты, доступные в устройстве, а также агрегирования каналов.
- **Setting**
Используйте данный флажок, чтобы включить или отключить протокол GMRP для порта или агрегирование каналов.

Порядок действий при конфигурации

Активировать отправку пакетов GMRP для одного порта

1. Установите флажок «GMRP».
2. Установите флажок в соответствующей строке таблицы 2.
3. Чтобы применить изменения, щёлкните кнопку «Set Values».

Активировать отправку пакетов GMRP для всех портов

1. Установите флажок «GMRP».
2. В раскрывающемся списке «Setting» выберите запись «Enabled».
3. Щёлкните кнопку «Copy to Table». Флажок активирован для всех портов в таблице 2.
4. Чтобы применить изменения, щёлкните кнопку «Set Values».

6.5.17.4 Блокировка многоадресной рассылки

Блокировка пересылки неизвестных пакетов Multicast

На странице заблокирована пересылка неизвестных пакетов Multicast для отдельных портов.

Unknown Multicast Blocking	
Groups IGMP GMRP Blocking	
Setting Copy to Table	
All ports	No Change Copy to Table
Port	Setting
P0.1	☐
P0.2	☐
P0.3	☐
P0.4	☐
Set Values Refresh	

Описание отображаемых значений

Таблица 1 состоит из следующих столбцов:

- **1-й столбец**
Отображает, что настройки действительны для всех портов в таблице 2.
- **Setting**
Выберите в раскрывающемся списке настройку. Имеются следующие возможности настройки:
 - Enabled
Блокировка многоадресных пакетов активирована.
 - Disabled
Блокировка многоадресных пакетов деактивирована.
 - No Change
Таблица 2 осталась без изменений.
- **Copy to Table**
При нажатии кнопки настройка будет скопирована для всех портов в таблице 2.

Таблица 2 состоит из следующих столбцов:

- **Port**
Все доступные порты перечислены в этом столбце. Недоступные порты не отображаются.
- **Setting**
Активируйте или деактивируйте блокировку пакетов Multicast.

Порядок конфигурации

Активировать блокировку для одного порта

1. Установите флажок в соответствующей строке таблицы 2.
2. Чтобы применить изменения, щёлкните кнопку «Set Values».

Активировать блокировку для всех портов

1. В раскрывающемся списке «Setting» выберите запись «Enabled».
2. Щёлкните кнопку «Copy to Table». Флажок активирован для всех портов в таблице 2.
3. Чтобы применить изменения, щёлкните кнопку «Set Values».

6.5.18 Broadcast

Блокировка пересылки широковещательных пакетов

На этой странице пересылка широковещательных пакетов заблокирована для отдельных портов.

Примечание

Некоторые протоколы связи работают только при поддержке Broadcast. В подобных случаях блокировка может привести к сбою передачи данных. Блокируйте широковещательную рассылку только в том случае, если уверены, что можно обойтись без выбранных портов.

Broadcast Blocking

	Setting	Copy to Table
All ports	No Change ▾	Copy to Table

Port	Setting
P0.1	☐
P0.2	☐
P0.3	☐
P0.4	☐

Set Values Refresh

Описание отображаемых полей

Таблица 1 состоит из следующих столбцов:

- **1-й столбец**
Отображает, что настройки действительны для всех портов в таблице 2.
- **Setting**
Выберите в раскрывающемся списке настройку. Имеются следующие возможности настройки:
 - Enabled
Блокировка широковещательных пакетов активирована.
 - Disabled
Блокировка широковещательных пакетов деактивирована.
 - No Change
Таблица 2 осталась без изменений.
- **Copy to Table**
При нажатии кнопки настройка будет скопирована для всех портов в таблице 2.

Таблица 2 состоит из следующих столбцов:

- **Port**
Отображены все доступные порты.
- **Setting**
Активируйте или деактивируйте блокировку широковещательных пакетов.

Порядок действий при конфигурации

Активировать блокировку широковещательных пакетов для одного порта

1. Установите флажок в соответствующей строке таблицы 2.
2. Чтобы применить изменения, щёлкните кнопку «Set Values».

Активировать блокировку широковещательных пакетов для всех портов

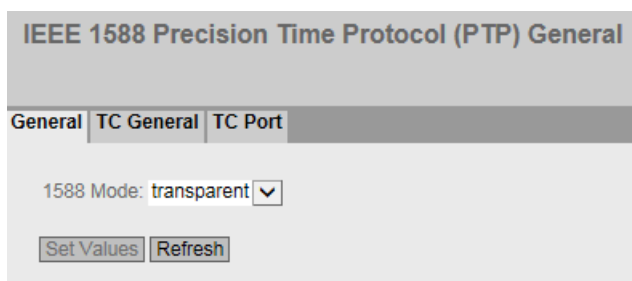
1. В раскрывающемся списке «Setting» в таблице 1 выберите запись «Enabled».
2. Щёлкните кнопку «Copy to Table». Флажок активирован для всех портов в таблице 2.
3. Чтобы применить изменения, щёлкните кнопку «Set Values».

6.5.19 PTP

6.5.19.1 General

Стандарт IEEE 1588 для устройств SCALANCE

Стандарт IEEE 1588v2 определяет механизмы, с помощью которых достигается высокоточная синхронизация времени устройств в сети. Устройства SCALANCE с соответствующим оборудованием поддерживают синхронизацию времени в соответствии со стандартом IEEE 1588v2. В состоянии поставки и после сброса до заводских настроек функция данных устройств отключена. Для того чтобы иметь возможность использовать протокол PTP, необходимо активировать эту функцию и настроить каждый порт находящийся на пути синхронизации, а также порты, которые заблокированы механизмами резервирования. Протокол PTP также может использоваться с механизмами резервирования в кольцевой сети, такими как HRP, Standby coupling для колец, MRP и RSTP. В следующих разделах описаны возможности конфигурации для управления через веб-интерфейс.



Конфигурация согласно стандарта IEEE 1588

На этой странице задаётся, как устройство должно обрабатывать сообщения PTP.

Mode 1588

Доступны следующие параметры настройки:

- **off**
Устройство не обрабатывает сообщения PTP. При этом сообщения PTP пересылаются в соответствии с правилами коммутатора.
- **transparent**
Устройство выполняет функцию Transparent Clock и пересылает PTP Messages другим участникам, создавая записи в поле исправления PTP Message.

6.5.19.2 TC основное

TC основное

Данная вкладка содержит основные настройки для PTP.

IEEE 1588 Precision Time Protocol (PTP) Transparent Clock (TC) General

General TC General TC Port

Delay Mechanism: peer to peer ▼

Domain Number: 0

VLAN ID: - ▼

Set Values Refresh

Конфигурирование прозрачных часов стандарт IEEE 1588

- **Delay Mechanism**

Задайте механизм задержки, с которым будет работать устройство:

- End-to-End

Используется механизм запроса-ответа задержки.

Примечание

При сквозной синхронизации с более чем 2 ведомыми устройствами могут возникать выбросы > 100 нс в смещении.

- Peer-to-Peer

Используется механизм одноранговой задержки.

- **Domain Number**

Введите здесь номер домена для устройства. Устройство SCALANCE может быть назначено только одному домену синхронизации.

- **VLAN ID**

Вариант настройки зависит от настроенного режима Base Bridge Mode в меню menu Layer 2 > VLAN > General:

- 802.1D Transparent Bridge

В раскрывающемся списке отображается знак «-», поскольку тег VLAN не действует в этом режиме работы. Устройство синхронизируется в каждой сети VLAN.

- 802.1Q VLAN Bridge

Все настроенные сети VLAN содержатся в раскрывающемся списке. Выберите сеть VLAN, в которой устройство должно синхронизироваться

6.5.19.3 TC Port

Настройки порта

Данная вкладка содержит основные настройки порта для PTP.

IEEE 1588 Precision Time Protocol (PTP) Transparent Clock (TC) Port

General TC General TC Port

	Setting	Transport Mechanism	Copy to Table
All ports	No Change v	No Change v	Copy to Table v

Port	Setting	Faulty Flag	Transport Mechanism
P1.1	☐	false	UDP IP v4 v
P1.2	☐	false	UDP IP v4 v
P1.3	☐	false	UDP IP v4 v
P1.4	☐	false	UDP IP v4 v

Конфигурирование параметров порта прозрачных часов стандарт IEEE 1588

Таблица 1 состоит из следующих столбцов:

- **1-й столбец**
Отображает, что настройки действительны для всех портов.
- **Setting**
Выберите необходимую настройку. Если выбрано значение «No Change», то запись в таблице 2 не изменяется.
- **Transport Mechanism**
Существуют следующие возможности настройки:
 - Ethernet
 - UDP IPv4
 - No Change
 Если выбрано значение «No Change», то запись в таблице 2 не изменяется.

В таблице 2 представлена подробная информация по отдельным портам:

- **Port**
Номер порта. В случае модульных устройств номер слота и номер порта отображаются разделёнными точкой.
Протокол PTP не поддерживается на портах SPF +.
- **Setting**
Статус порта. Возможны следующие значения:
 - Enabled
Порт не задействован в протоколе PTP.
 - Disabled
Порт обрабатывает сообщения PTP.

6.5 Меню «Layer 2»

- **Faulty Flag**

Статус ошибки, связанный с PTP.

- true
Произошла ошибка.
- wrong
На этом порте ошибок не обнаружено.

- **Transport Mechanism**

С помощью этой команды выбирается, как этот порт должен обрабатывать трафик сообщений PTP. Для портов устройства можно задать различные настройки, но соответствующий партнёр по обмену данными должен поддерживать выбранный механизм транспортировки. Существуют следующие возможности настройки:

- Ethernet
- UDP IPv4

6.5.20 RMON

6.5.20.1 Statistics

Статистика

На этой странице можно указать порты, для которых будет отображаться статистика RMON.

Статистика RMON отображается на экране «Information > Ethernet Statistics» во вкладках «Packet Size», «Frame Type» и «Packet Error».

Настройки

RMON Statistics Configuration

Statistics History

☒ RMON

Port: All ports

Select	Port
☐	P0.1
☐	P0.2
☐	P0.3
☐	P0.4

16 entries.

Create Delete Set Values Refresh

- **RMON**

Когда установлен этот флажок, удалённый мониторинг (RMON) позволяет устройству собирать диагностические данные, обрабатывать и считывать их через SNMP со станции управления сетью, которая также поддерживает RMON. Эти диагностические данные, например профили нагрузки портов, позволяют своевременно выявлять и устранять проблемы в сети.

Примечание

Когда протокол RMON деактивирован, статистика не удаляется, а поддерживается в актуальном состоянии.

- **Port**

Выберите порты, для которых должна отображаться статистика.

Таблица состоит из следующих столбцов:

- **Select**

Выберите строку, которую необходимо удалить.

- **Port**

Показывает порты, для которых должна отображаться статистика.

Порядок действий при конфигурации

Активация функции

1. Установите флажок «RMON».
2. Щёлкните кнопку «Set values». Функция «RMON» активирована.

Включить статистику RMON для портов

Примечание

Требование

Необходимо активировать функцию «RMON», чтобы можно было отобразить статистику RMON для порта.

1. В раскрывающемся списке «Port» выберите нужный порт или запись «All Ports».
2. Щёлкните кнопку «Create». Статистика RMON может отображаться для выбранного порта или для всех портов.

Выключить статистику RMON для портов

1. Активируйте строку, которую необходимо удалить, в столбце «Select».
2. Щёлкните кнопку «Delete». Статистика RMON не отображается для выбранного порта.

6.5.20.2 История

Образцы статистики

На этой странице можно указать, следует ли сохранять образцы статистики для порта. Можно задать, сколько записей следует сохранить и с какой периодичностью делать запись образцов.

Настройки

Setting	Buckets	Interval[s]	Copy to Table
All ports No Change	No Change	No Change	Copy to Table

Port	Setting	Buckets	Interval[s]
P0.1	☐	0	0
P0.2	☐	0	0
P0.3	☐	0	0
P0.4	☐	0	0

Set Values Refresh

Таблица 1 состоит из следующих столбцов:

- **1-й столбец**
Отображает, что настройки действительны для всех портов.
- **Setting**
Выберите необходимую настройку. Если выбрано значение «No Change», то запись в таблице 2 не изменяется.
- **Buckets**
Введите максимальное число образцов, которые должны быть сохранены одновременно. Если введено значение «No Change», запись в таблице 2 не изменяется.

- **Interval[s]**
Введите интервал, по истечении которого текущее состояние статистики должно быть сохранен как образец. Если введено значение «No Change», запись в таблице 2 не изменяется.

Примечание

При задании продолжительности интервала обратите внимание, что в качестве продолжительности интервала имеет смысл выбирать только кратное 3 секундам значение. Статистика обновляется каждые 3 секунды. В промежутках между ними выдаётся значение «0».

- **Copy to Table**
Если нажать эту кнопку, то настройки будут применены для всех портов таблицы 2.

Таблица 2 состоит из следующих столбцов:

- **Port**
Показывает порт, к которому относятся настройки.
- **Setting**
Активировать или деактивировать запись истории на соответствующий порт.
- **Buckets**
Введите максимальное число образцов, которые должны быть сохранены одновременно.
Максимальное количество записей может быть ограничено памятью устройства.
Диапазон значений: 1 - 65535
Заводская настройка: 24
- **Interval[s]**
Введите интервал, по истечении которого текущее состояние статистики должно быть сохранен как образец.
Диапазон значений: 1 — 3600
Заводская настройка: 3600

Примечание

При задании продолжительности интервала обратите внимание, что в качестве продолжительности интервала имеет смысл выбирать только кратное 3 секундам значение. Статистика обновляется каждые 3 секунды. В промежутках между ними выдаётся значение «0».

Порядок действий при конфигурации

Включить статистику RMON для отдельных портов

1. Установите флажок в соответствующей строке таблицы 2 «Setting».
Поля «Buckets» и «Interval[s]» активируются с заводскими настройками.
2. Введите необходимые значения в поля «Buckets» и «Interval[s]».
3. Щёлкните кнопку «Set values».

6.6 Меню «Layer 3»

Активировать статистику RMON для всех портов

1. В таблице 1 в раскрывающемся списке «Setting» выберите запись «Enabled».
2. Введите необходимые значения в поля «Buckets» и «Interval[s]». Если не будут изменены записи в обоих полях, то для всех портов будут использоваться заводские настройки.
3. Щёлкните кнопку «Copy to Table».
Настройки будут применены для всех портов в Таблице 2.
4. Щёлкните кнопку «Set values».

6.6 Меню «Layer 3»

6.6.1 Subnets

6.6.1.1 Overview

Создание подсетей

На этой странице можно создать несколько IP-интерфейсов VLAN для устройства.

Под подсетью всегда подразумевается сеть VLAN. IP-адрес задаётся на вкладке «Configuration».

Connected Subnets Overview

Overview
Configuration
Default Gateway

☐ Single Hop Inter-VLAN Routing

Interface: VLAN1

Select	Interface	TIA Interface	Interface Name	MAC Address	IP Address	Subnet Mask	Address Type	IP Assgn. Method	Address Collision Detection Status
☐	vlan1	-	vlan1	08-00-06-70-56-00	192.168.16.202	255.255.255.0	Primary	Static	Active
☐	vlan10	-	vlan10	08-00-06-70-56-00	192.168.1.10	255.255.255.0	Primary	Static	Active
☐	vlan13	yes	vlan13	08-00-06-70-56-00	0.0.0.0	0.0.0.0	Primary	Static	Idle
☐	vlan2	-	vlan2	08-00-06-70-56-00	1.1.1.1	255.255.255.0	Primary	Static	Idle

4 entries.

Create
Delete
Set Values
Refresh

Описание отображаемых значений

Страница содержит следующие поля:

- **Single Hop Inter-VLAN Routing**
Активируйте или деактивируйте маршрутизацию между локальными IP-интерфейсами.
- **Interface**
Выберите необходимый интерфейс, для которого настраиваете другую IP-подсеть.

Таблица состоит из следующих столбцов:

- **Select**
Выберите строку, которую необходимо удалить.
- **Interface**
Отображает интерфейс.
- **TIA Interface**
Отображает выбранный интерфейс TIA.
- **Interface Name**
Отображает название интерфейса.
- **MAC Address**
Отображает MAC-адрес.
- **IP Address**
Отображает IPv4-адрес подсети.
- **Subnet Mask**
Показывает маску подсети.
- **Address Type**
Отображает тип адреса. Возможны следующие значения:
 - Primary
Первый IPv4-адрес, настроенный для интерфейса IPv4.

- **IP Assgn. Method**
Показывает, метод с помощью которого назначается IPv4-адрес. Возможны следующие значения:
 - Static
IPv4-адрес является статическим. Введите настройки в полях «IP Address» и «Subnet Mask».
 - Dynamic (DHCP)
Устройство получает динамический IPv4-адрес от DHCPv4-сервера.
- **Address Collision Detection Status**
Когда в сети становятся активными новые IPv4-адреса, функция «Address Collision Detection Status» проверяет, могут ли возникать конфликты адресов. Таким образом, распознаются IPv4-адреса, которые должны быть назначены дважды.

Примечание

Функция не выполняет циклическую проверку.

В этом столбце отображается состояние функции. Возможны следующие значения:

- Idle
Интерфейс не активен и не имеет IPv4-адреса.
- Starting
Этот состояние обозначает фазу запуска. В этой фазе устройство сначала отправляет запрос о том, существует ли уже запланированный адрес IPv4. Если адрес ещё не присвоен, устройство отправляет сообщение о том, что с этого момента оно будет использовать этот IP-адрес.
- Conflict
Интерфейс не активен. Интерфейс пытается использовать уже назначенный IPv4-адрес.
- Defending
Интерфейс использует уникальный IPv4-адрес. Другой интерфейс пытается использовать тот же IPv4-адрес.
- Active
Интерфейс использует уникальный IPv4-адрес. Конфликты отсутствуют.
- Not supported
Функция обнаружения конфликтов адресов не поддерживается.
- Disabled
Функция обнаружения конфликтов адресов деактивирована.

Порядок действий при конфигурации

1. Выберите интерфейс в раскрывающемся списке «Interface».
2. Щёлкните кнопку «Create». В таблицу добавляется новая строка.
3. Щёлкните кнопку «Set values».
4. Сконфигурируйте подсеть на вкладке "Configuration".

6.6.1.2 Configuration

На этой странице можно настроить интерфейс протокола IPv4.

Connected Subnets Configuration

Overview | **Configuration** | Default Gateway

Interface (Name): **vlan1 (vlan1)** ▾

Status: **enabled** ▾

Interface Name: **vlan1**

MAC Address: **20-87-56-2b-6e-00**

☒ **DHCP**

IP Address: **192.168.178.27**

Subnet Mask: **255.255.255.0**

Address Type: **Primary**

☒ **TIA Interface**

Set Values **Refresh**

Описание отображаемых значений

Страница содержит следующие поля:

- **Interface (Name)**
Выберите в раскрывающемся списке интерфейс.
- **Status**
Задайте, включён или выключен интерфейс.
 - Enabled
Интерфейс включён. Обмен данными возможен только через включённый интерфейс.
 - Disabled
Интерфейс выключен.
- **Interface Name**
Введите здесь имя для интерфейса.
- **MAC Address**
Отображает MAC-адрес выбранного интерфейса.
- **DHCP**
Активируйте или деактивируйте DHCP-клиент для этого интерфейса IPv4.
- **IP Address**
Введите IPv4-адрес интерфейса. IPv4-адрес нельзя использовать более одного раза.
- **Subnet Mask**
Введите маску подсети для создаваемой подсети. Подсети на разных интерфейсах не должны перекрываться.

6.6 Меню «Layer 3»

- **address type**
Отображает тип адреса. Возможны следующие значения:
 - Primary
Первая подсеть интерфейса.
- **TIA Interface**
Выберите, должен ли этот интерфейс быть TIA Interface.

Порядок действий при конфигурации

1. Выберите интерфейс в раскрывающемся списке «Interface (Name)».
2. Введите имя интерфейса в поле «Interface Name».
3. Введите IPv4-адрес подсети в столбец «IP Address».
4. Введите маску подсети, принадлежащую IPv4-адресу, в столбце «Subnet Mask».
5. Щёлкните кнопку «Set values».

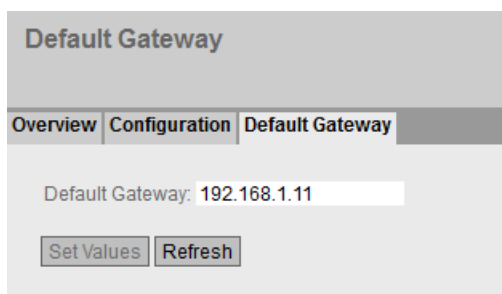
6.6.1.3 Default Gateway

Создание подсетей

На этой странице задаётся шлюз по умолчанию.

Примечание

Если для шлюза по умолчанию настраивается статический IP-адрес, DHCP автоматически деактивируется для интерфейса TIA. Это предотвращает перезапись адреса шлюза через DHCP. После этого можно повторно при необходимости активировать DHCP.



Описание отображаемых значений

Страница содержит следующие поля:

- **Default Gateway**
Введите IP-адрес интерфейса, который используется в качестве шлюза по умолчанию.

Порядок действий при конфигурации

1. Введите шлюз по умолчанию.
2. Щёлкните кнопку «Set values».

6.6.2 DHCP Relay Agent

6.6.2.1 General

DHCP Relay Agent

Когда DHCP Server находится не в той сети, что DHCP Client, то клиент не может связаться с сервером. Агент ретрансляции DHCP является посредником между DHCP Server и DHCP Client.

Если сконфигурировать опцию 82, агент DHCP Relay Agent распространяет пакеты на DHCP Server с помощью идентификатора канала и удалённого идентификатора.

Можно указать до 4-х серверов DHCP Server для DHCP Relay Agent. Когда DHCP Server недоступен, устройство может переключиться на другой DHCP Server.

Описание отображаемых значений

Страница содержит следующие поля:

- **DHCP Relay Agent**
Активируйте или деактивируйте DHCP Relay Agent.
- **Send Option 82**
Активируйте или деактивируйте опцию 82.

6.6 Меню «Layer 3»

- **Common Agent Address**
Активируйте или деактивируйте общий адрес агента.
Когда функция активирована, агент ретрансляции заменяет адрес порта получения в запросе DHCP на адрес интерфейса, который сконфигурирован в разделе "Common Agent Interface".
- **Common Agent Interfacee**
Агент ретрансляции использует IP-адрес интерфейса, выбранного здесь, в качестве адреса источника (giaddr) в запросах DHCP.
- **Server IP Address**
Введите IPv4-адрес DHCP-сервера.

Таблица состоит из следующих столбцов:

- **Select**
Выберите строку, которую необходимо удалить.
- **Server IP Address**
Отображает IPv4-адрес DHCP-сервера.

Порядок действий при конфигурации

1. Введите IPv4-адрес DHCP-сервера в поле ввода Server IP Address.
2. Щёлкните кнопку «Create». В таблице создаётся новая запись.
3. Установите флажок напротив «DHCP Relay Agent».
4. Установите флажок напротив «Send Option 82».
5. Щёлкните кнопку «Set values».

6.6.2.2 Option

Параметр DHCP Relay Agent

На этой странице можно установить параметры для DHCP-сервера, например, идентификатор канала.

Идентификатор канала описывает источник запроса DHCP, например, то какой порт получил запрос DHCP.

Задайте DHCP Server на вкладке «General».

Dynamic Host Configuration Protocol (DHCP) Relay Agent Option

General
Option

Global configuration

☒ Circuit ID Router Index
☐ Circuit ID Receive VLAN ID
☐ Circuit ID Receive Port

Remote ID: 00-5e-1d-d2-76-00

Interface specific configuration
Interface: vlan2

Select	Interface	Remote ID Type	Remote ID	Circuit ID Type	Circuit ID	Status
☐	vlan1	IP Address	192.168.16.155	Predefined	-	☒

1 entry.

Create
Delete
Set Values
Refresh

Описание отображаемых значений

Страница содержит следующие поля:

Глобальная конфигурация

- Circuit ID Router Index**
Активируйте или деактивируйте флажок. Когда этот флажок установлен, сгенерированный идентификатор канала добавляется к индексу маршрутизатора.
- Circuit ID Receive VLAN ID**
Активируйте или деактивируйте флажок. Когда этот флажок установлен, сгенерированный идентификатор канала добавляется к идентификатору VLAN.
- Circuit ID Receive Port**
Активируйте или деактивируйте флажок. Когда этот флажок установлен, сгенерированный идентификатор канала добавляется к порту получения.

Примечание

Необходимо выбрать хотя бы одну опцию.

Дополнительную информацию об индексе маршрутизатора (Circuit ID Router Index) и индексе порта (Circuit ID Receive Port) можно найти в таблице IfTable о протоколе SNMP.

Идентификатор VLAN можно найти на странице WBM Layer 2 > VLAN> General.

- Remote ID**
Отображает идентификатор устройства.

Конфигурация, зависящая от интерфейса

- Interface**
Выберите в раскрывающемся списке интерфейс.

Таблица состоит из следующих столбцов:

- **Select**
Выберите строку, которую необходимо удалить.
- **Interface**
Отображает интерфейс.
- **Remote ID Typ**
Выберите в раскрывающемся списке тип идентификатора устройства. Имеются следующие возможности:
 - IP Adress
IPv4-адрес устройства используется в качестве его идентификатора.
 - MAC Adress
MAC-адрес устройства используется в качестве его идентификатора.
 - Free Text
Если используется пункт «Free Text», то можно ввести имя устройства в качестве идентификатора устройства в поле «Remote ID».
- **Remote ID**
Введите имя устройства. Поле можно редактировать только в том случае, если выбрана запись «Free Text» в «Remote ID Typ».
- **Remote ID Typ**
Выберите в раскрывающемся списке тип идентификатора канала. Имеются следующие возможности:
 - Predefined
Идентификатор канала создаётся автоматически на базе индекса маршрутизатора, идентификатора VLAN или порта.
 - Free Number
Если используется «Free Number», можно ввести идентификатор в поле «Circuit ID».
- **Circuit ID**
Введите идентификатор канала. Поле можно редактировать только в том случае, если выбрана запись «Free Number» в «Circuit ID Typ».
- **Status**
Когда флажок установлен, DHCP Relay Agent активируется для соответствующего интерфейса. Когда в таблице создаётся новая строка, по умолчанию активируется DHCP Relay Agent.

Порядок действий при конфигурации

Для того чтобы установить параметры вручную, выполните следующие действия:

1. Активируйте необходимую опцию в «Global configuration»:
 - Circuit ID Router Index
 - Circuit ID Receive VLAN ID
 - Circuit ID Receive Port
2. Щёлкните кнопку «Set values».
3. Выберите интерфейс в раскрывающемся списке «Interface».

4. Щёлкните кнопку «Create». В таблицу добавляется новая строка.
5. Выберите необходимую запись в раскрывающемся списке «Remote ID Тип».
 - IP Address
IPv4-адрес устройства используется в качестве его идентификатора.
 - MAC Address
MAC-адрес используется в качестве идентификатора устройства.
 - Free Text
Введите идентификатор устройства в поле «Remote ID».
6. Выберите необходимую запись в раскрывающемся списке «Remote ID Тип».
 - Predefined
Сгенерированный идентификатор канала добавляется к индексу маршрутизатора.
 - Free Number
Введите идентификатор в поле «Circuit ID».
7. Щёлкните кнопку «Set values».

6.6.3 NAT

6.6.3.1 NAT

На этой странице веб интерфейса можно задать основные настройки для механизма NAT.

Network Address Translation (NAT) Protocol

NAT
Static
Pool
NAPT

☒ NAT

Idle Timeout[s]:

TCP Timeout[s]:

UDP Timeout[s]:

Interface Configuration

Interface: vlan1

☒ NAT

☒ NAPT

Interface	NAT	NAPT
vlan1	☒	☒

1 entry.

Описание

Страница содержит следующие поля:

- **NAT**
Активируйте или деактивируйте механизм NAT/NAPT для всего устройства. Когда активировано устройство функционирует как маршрутизатор NAT.
- **Idle Timeout[s]**
Введите необходимый интервал времени. По истечении заданного интервала времени устройство циклически проверяет, истекло ли время старения соединений TCP и UDP. Соединения, время жизни которых истекло за время с момента последней проверки, удаляются из таблицы «NAT Translations».
- **TCP Timeout[s]**
Введите необходимое время жизни для TCP-соединений. TCP-соединения сохраняются до тех пор, пока не прекращён обмен данными в течение указанного интервала времени. В зависимости от циклической проверки по истечении Idle Timeouts соединения удаляются из таблицы "NAT Translations".
- **UDP Timeout[s]**
Введите необходимое время жизни для UDP-соединений. UDP-соединения сохраняются до тех пор, пока не прекращён обмен данными в течение указанного интервала времени. В зависимости от циклической проверки по истечении Idle Timeouts соединения удаляются из таблицы "NAT Translations".
- **Interface**
Выберите в раскрывающемся списке IP-интерфейс, в котором необходимо настроить механизм NAT.
Как только был настроен интерфейс как интерфейс NAT, все дальнейшие настройки будут рассматриваться на основе данного интерфейса. Это означает, что это все сети, к которым можно получить доступ через интерфейс «Outside». Все остальные сети внутри «Inside».

Примечание

Когда сконфигурировано несколько интерфейсов NAT на одном устройстве, это означает, что сеть с точки зрения интерфейса NAT снаружи «Outside» и с точки зрения другого интерфейса NAT внутри «Inside».

- **NAT**
Активируйте или деактивируйте механизм NAT/NAPT для IP-интерфейса.
На вкладке «Pool» автоматически создаётся запись Из внешней сети к устройству можно получить доступ через IP-адрес IP-интерфейса.
Когда деактивирован NAT для IP-интерфейса и на интерфейсе NAT нет настроек, запись автоматически удаляется из таблицы.
- **NAPT**
Активируйте или деактивируйте NAPT для IP-интерфейса.

Таблица состоит из следующих столбцов:

- **Interface**
Интерфейс, на котором происходит конфигурация NAT.
- **NAT**
Показывает, активирован или деактивирован механизм NAT для выбранного IP-интерфейса.
NAT активен только в том случае, если активирован механизм NAT для всего устройства.
- **NAPT**
Показывает, активирован или деактивирован механизм NAPT для выбранного IP-интерфейса.
Механизм NAPT активен только в том случае, если активирован механизм NAT для всего устройства.
Автоматически активируется динамическое преобразование портов, если не выполняется никаких дополнительных настроек для NAPT.
По умолчанию устройство во внутренней сети недоступно из внешней сети. Если внутреннее устройство хочет обмениваться данными во внешней сети, то адрес Inside Local и IP-адрес IP-интерфейса дополняются портом и назначаются внутреннему устройству как адрес Inside Local и Inside Global. Внутреннее устройство может быть доступно из внешней сети через этот адрес Inside Global, пока не истечёт таймер соединения.

Порядок действий

Чтобы настроить механизм NAT/NAPT, выполните следующие действия:

1. Введите необходимый интервал времени.
2. Выберите необходимый IP-интерфейс.
3. Активирует механизм NAT/NAPT для выбранного IP-интерфейса.
4. Щёлкните кнопку «Set values».
5. Сделайте необходимые настройки для полей NAT/NAPT на вкладках NAT/NAPT.
6. Установите флажок «NAT» на этой вкладке.
7. Щёлкните кнопку «Set values».

6.6.3.2 Static

Можно настроить статические преобразования адресов 1:1 на этой странице интерфейса WBM.

Определяется, в какой адрес Inside Global должен быть преобразован адрес устройства Inside Local, и наоборот. Этот вариант позволяет устанавливать соединения в обоих направлениях. К устройству во внутренней сети можно получить доступ из внешней сети.

Network Address Translation (NAT) Static Configuration

NAT **Static** **Pool** **NAPT**

Interface:

Inside Local Address:

Inside Global Address:

	Interface	Inside Local Address	Inside Global Address
☐	vlan1	192.168.16.155	192.168.16.60

1 entry.

Описание

Страница содержит следующие поля:

- **Interface**
Выберите в раскрывающемся списке NAT-интерфейс, для которого необходимо выполнить дальнейшие настройки NAT.
- **Inside Local Address**
Введите фактический адрес устройства, которое должно быть доступно извне.
- **Inside Global Address**
Введите адрес, через который можно получить доступ к устройству извне.

Таблица состоит из следующих столбцов:

- **1-й столбец**
Установите флажок в строке, которую необходимо удалить.
- **Interface**
Интерфейс NAT, к которому относится настройка.
- **Inside Local Address**
Отображает фактический адрес устройства, которое должно быть доступно извне.
- **Inside Global Address**
Отображает адрес, через который можно получить доступ к устройству извне.

Порядок действий

Чтобы создать преобразование адресов 1:1, выполните следующие действия:

1. Выберите в раскрывающемся списке «Interface» NAT-интерфейс.
2. Введите в поле «Inside Local Address» фактический адрес устройства, которое должно быть доступно снаружи.
3. Введите в поле «Inside Global Address» адрес, через который можно получить доступ к устройству снаружи.

6.6.3.3 Pool

Можно настроить динамические преобразования адресов на этой странице интерфейса WBM.

По умолчанию устройство во внутренней сети недоступно из внешней сети. Если внутреннее устройство хочет обмениваться данными во внешней сети, то ему динамически назначается адрес Inside Global. Внутреннее устройство может быть доступно из внешней сети через этот адрес Inside Global, пока не истечёт таймер соединения.

Network Address Translation (NAT) Pool Configuration

NAT
Static
Pool
NAPT

Interface: vlan1

Inside Global Address:

Inside Global Address Mask:

	Interface	Inside Global Address	Inside Global Address Mask
☐	vlan1	192.168.16.155	255.255.255.255

1 entry.

Create
Delete
Refresh

Описание

Страница содержит следующие поля:

- **Interface**
Выберите в раскрывающемся списке NAT-интерфейс, для которого необходимо выполнить дальнейшие настройки NAT.
- **Inside Global Address**
Введите начальный адрес для динамического назначения адресов, по которым устройства должны быть доступны снаружи.

Примечание

Диапазон адресов для динамического преобразования адресов не должен содержать глобальный IP-адрес.

- **Inside Global Address Mask**
Введите маску внешней подсети.

Таблица состоит из следующих столбцов:

- **1-й столбец**
Установите флажок в строке, которую необходимо удалить.
- **Interface**
Интерфейс NAT, к которому относится настройка.

6.6 Меню «Layer 3»

- **Inside Global Address**
Отображает начальный адрес для динамического назначения адресов, по которым устройства должны быть доступны извне.
- **Inside Global Address Mask**
Отображает маску внешней подсети.

Порядок действий

Чтобы создать динамическое преобразование адресов, выполните следующие действия:

1. Выберите в раскрывающемся списке «Interface» NAT-интерфейс.
2. Введите в поле «Inside Global Address» начальный адрес для динамического назначения адресов, по которым устройства должны быть доступны снаружи.
3. Введите маску внешней подсети в поле «Inside Global Address Mask».

6.6.3.4 NATP

Можно настроить статические преобразования портов на этой странице интерфейса WBM.

Network Address Port Translation (NAPT)

NAT Static Pool NAPT

Interface:

Inside Local Address:

Service:

Start Port:

End Port:

Inside Global Port:

Protocol:

Description:

	Interface	Inside Local Address	Start Port	End Port	Protocol	Inside Global Address	Inside Global Port	Description
☐	vlan1	192.168.16.152	53	53	TCP	192.168.16.155	53	DNS

1 entry.

Create Delete Refresh

Описание

Страница содержит следующие поля:

- **Interface**
Выберите в раскрывающемся списке NAT-интерфейс, для которого необходимо выполнить дальнейшие настройки NAT.
- **Inside Local Address**
Введите фактический адрес устройства, которое должно быть доступно извне.

- **Service**
Выберите службу, для которой действительно преобразование порта.
Когда выбрана служба, тот же порт вводится в поля Start Port и End Port. Когда изменяется начальный порт, конечный порт будет изменён соответствующим образом.
Когда выбрана запись «-», можно свободно задать начальный и конечный порт.
- **Start Port**
Задайте порт Inside Local.
- **End Port**
В зависимости от выбора в раскрывающемся списке «Service» можно задать порт Inside Local, или будет отображаться один порт.
Когда задаются разные порты в полях Start Port и End Port, в поле Inside Global Port вводится один и тот же диапазон портов. Диапазон портов может быть преобразован только в аналогичный диапазон портов.
Когда задаются одинаковые порты в полях Start Port и End Port, в поле Inside Global Port значение не вводится.
- **Inside Global Port**
В зависимости от выбора в раскрывающемся списке «Service» можно задать порт, или будет отображаться один порт.
- **Protocol**
Выберите протокол, для которого действительно преобразование порта.
- **Description**
Введите описание для преобразования порта.

Таблица состоит из следующих столбцов:

- **1-й столбец**
Установите флажок в строке, которую необходимо удалить.
- **Interface**
Интерфейс NAT, к которому относится настройка.
- **Inside Local Address**
Отображает фактический адрес устройства, которое должно быть доступно извне.
- **Start Port**
Отображает начальный порт, которому назначен Inside Local Address.
- **End Port**
Показывает конечный порт, которому назначен Inside Local Address.
- **Protocol**
Отображает протокол, для которого действительно преобразование порта.
- **Inside Global Address**
Отображает адрес, через который можно получить доступ к устройству извне.
- **Inside Global Port**
Отображает порт, которому назначен Inside Local Address.
- **Description**
Отображает описание для преобразования порта.

Порядок действий

Чтобы создать статическое преобразование порта, выполните следующие действия:

1. Выберите в раскрывающемся списке «Interface» NAT–интерфейс.
2. Введите в поле «Inside Local Address» фактический адрес устройства, которое должно быть доступно снаружи.
3. Выберите службу.
4. В зависимости от выбора в раскрывающемся списке «Service» задайте начальный, конечный порты и порт Inside Global.
5. Выберите протокол.
6. Введите описание для преобразования порта.

6.7 Меню «Security»

6.7.1 Управление пользователями

Обзор управления пользователями

Доступ к устройству управляется настраиваемыми установками пользователя. Настройте каждого пользователя с одним паролем для аутентификации. Назначьте пользователям роли с соответствующими правами.

Аутентификация пользователей может выполняться локально устройством или внешним сервером RADIUS. Как должна происходить аутентификация можно настроить на странице Security > AAA > General.

Примечание

В случае переноса конфигурации устройства в ПО STEP7 (TIA Portal), настроенные пользователи не переносятся.

Локальный вход

Локальный вход пользователей через устройство осуществляется следующим образом:

1. Пользователь входит в систему со своим именем пользователя и паролем.
2. Устройство проверяет, существует ли запись для пользователя:
 - Если соответствующая запись существует, то пользователь входит в систему с правами связанной с ней роли.
 - Если нет соответствующей записи, то пользователь получает отказ в доступе.

Вход через внешний RADIUS-сервер

RADIUS (Remote Authentication Dial-In User Service) это протокол для аутентификации и авторизации пользователей серверами, на которых обеспечивается централизованное хранение данных пользователей.

Сервер RADIUS для промышленных сетей включён в программный инструмент ПО SINEC INS (Infrastructure Network Services). ПО SINEC INS предоставляет все необходимые службы для управления промышленными сетями, например, RADIUS-, Syslog-, NTP-, DHCP-, TFTP-, SFTP- и DNS-сервера.

Аутентификация пользователей через сервер RADIUS осуществляется следующим образом:

1. Пользователь входит в систему со своим именем пользователя и паролем.
2. Устройство отправляет запрос аутентификации с данными для входа на сервер RADIUS.
3. Сервер RADIUS выполняет проверку и сообщает о её результате устройству:
 - Сервер RADIUS сообщает об успешной аутентификации и возвращает устройству значение «Administrative User» для атрибута «Service Type»:
→ Пользователь вошёл в систему с правами чтения/записи.
 - Сервер RADIUS сообщает об успешной аутентификации и возвращает устройству другое или нулевое значение для атрибута «Service Type»:
→ Пользователь вошёл в систему с правами чтения/записи.
 - Сервер RADIUS сообщает устройству об ошибке аутентификации:
→ Пользователю отказано в доступе.

Назначение сети VLAN через сервер RADIUS или гостевую VLAN в режиме Base Bridge Mode «802.1Q VLAN Bridge»

Аутентификация с изменениями конфигурации сети VLAN

Если порт динамически назначается сетью VLAN во время аутентификации с использованием функции «RADIUS VLAN Assignment Allowed» или «Guest VLAN» доступны следующие параметры:

- Когда назначаемая VLAN не была создана на устройстве, аутентификация будет отклонена.
- Когда назначаемая VLAN была создана на устройстве.
 - Порт становится нетегированным участником назначенной VLAN, если он до этого им не являлся.
→ Таким образом, статическая конфигурация порта в этой сети VLAN может быть перезаписана и не восстановлена, если аутентификация отменена.
 - Идентификатор порта изменяется на идентификатор назначенной сети VLAN.

Примечание

Когда порт должен быть назначен только одной сети VLAN, тогда необходимо настроить конфигурацию VLAN вручную. Все порты, например по умолчанию нетегированные участники в «VLAN 1».

6.7 Меню «Security»

Если аутентификация отменена, например, канал отключён, то отменяются динамические изменения:

- Порт больше не является участником назначенной сети VLAN.
- Идентификатор порта сбрасывается до значения, которое было до аутентификации.

Примечание

Если идентификатор порта соответствует назначенному идентификатору порта перед аутентификацией, то порт остаётся нетегированным участником в этой VLAN.

Аутентификация без изменений конфигурации сети VLAN

Если VLAN не назначается во время аутентификации с применением функции «RADIUS VLAN Assignment Allowed» или же с помощью «Guest VLAN», то существующая конфигурация VLAN порта остаётся неизменной.

6.7.2 User

6.7.2.1 Local Users

Local Users

На этой странице создаются локальные пользователи Local Users с соответствующими правами.

Примечание

От прав авторизованного пользователя зависит, какие значения будут отображаться.

Local Users

Local Users
Roles
Groups

☒ Case Sensitive User Accounts

User Account:

Password Policy: **high**

Password:

Password Confirmation:

Role: **user**

Select	User Account	Role	Description
☐	admin	admin	System defined local user

1 entry.

Create
Delete
Set Values
Refresh

Описание

Страница содержит следующие поля:

- **Case Sensitive User Accounts**
Когда данный флажок установлен, имя пользователя чувствительно к регистру. Если были созданы имена пользователей, которые отличались только в верхнем и нижнем регистре, то больше нельзя отключить этот флажок.
- **User Account**
Введите имя пользователя. Имя должно соответствовать следующим условиям:
 - Оно должно быть уникальным.
 - Оно должно содержать от 1 до 32 символов.
 - Оно не должно содержать следующие символы: | ? " ; \$ °
Также не должно содержать символы Space и Delete.

Примечание

Имя пользователя не может быть изменено

После создания пользователя имя пользователя больше нельзя изменить.

Если имя пользователя должно быть изменено, пользователя необходимо удалить и создать нового пользователя.

Примечание

Заводская предварительная настройка пользователя «user»

Начиная с версии прошивки 2.1 заводская настройка пользователя «user» в состоянии поставки более недоступна.

Если обновить устройство до прошивки V2.1, сначала ещё будет доступен пользователь «user». Если сбросить настройки устройства на заводские настройки («Restore Factory Defaults and Restart»), то пользователь «user» удаляется.

Можно создать новых пользователей с ролью «user».

- **Password Policy**
Отображает, какая политика паролей используется в устройстве:

- **High**
Длина пароля: минимум 8 символов, максимум 32 символа
Минимум 1 прописная буква
Минимум 1 специальный символ
Минимум 1 цифра
- **Low**
Длина пароля: минимум 6 символов, максимум 32 символа
- **User Defined**
Детали политики паролей устанавливаются пользователем.

Можно настроить политику паролей устройства на странице Security > Passwords > Option.

- **Password**
Введите пароль. Надёжность пароля зависит от установленной политики паролей.

6.7 Меню «Security»

- **Password Confirmation**
Введите пароль ещё раз, для его подтверждения.
- **Role**
Выберите роль:
 - user
Право чтения: Пользователи с этой ролью могут читать параметры устройства, но не могут их изменять. Пользователи с этой ролью могут изменить свой пароль.
 - admin
Право чтения/записи: Пользователи с этой ролью могут как читать, так и изменять параметры устройства. Пользователи могут изменять пароли для всех учётных записей пользователей.

Таблица содержит следующие столбцы:

- **Select**
Установите флажок в строке, которую необходимо удалить.

Примечание

Предустановленные в заводских настройках и пользователи, вошедшие в систему, не могут быть удалены или изменены.

- **User Account**
Отображает имена пользователей.
- **Role**
Отображает роль пользователя.

Порядок действий

Примечание

Изменения в режиме «Trial»

Даже когда устройство находится в режиме «Trial» изменения, внесённые на этой странице, немедленно сохраняются.

Создать пользователя

1. Введите имя пользователя.
2. Введите пароль для пользователя.
3. Введите пароль ещё раз, для его подтверждения.
4. Задайте роль пользователя.
5. Щёлкните кнопку «Create».

Удаление пользователя

1. Установите флажок в строке, которую необходимо удалить.
2. Щёлкните кнопку «Delete». Записи удаляются, а страница обновляется.

6.7.2.2 Roles

Roles

На этой странице создаются роли, которые действительны локально на устройстве

Примечание

От прав авторизованного пользователя зависит, какие значения будут отображаться.

Select	Role	Function Right	Description
☐	user	1	System defined role, with readonly access to configuration data of this component.
☐	admin	15	System defined role, with read/write access to configuration data of this component.
☐	default	1	Internal role, for authenticated users without group/role mapping in this component.
☐	everybody	0	Internal role, assigned to users when authentication fails. Access will be denied.
☐	Maintenance	15	User defined role, with read/write access

5 entries.

Create Delete Set Values Refresh

Описание

Страница содержит следующее:

- **Role Name**
Введите имя роли. Имя должно соответствовать следующим условиям:
 - Оно должно быть уникальным.
 - Оно должно содержать от 1 до 64 символов.

Примечание

Имя роли не может быть изменено

После создания роли имя роли больше нельзя изменить.

Если имя роли необходимо изменить, роль должна быть удалена и создана новая роль.

Таблица содержит следующие столбцы:

- **Select**
Установите флажок в строке, которую необходимо удалить.

Примечание

Предустановленные в заводских настройках роли, не могут быть удалены или изменены.

- **Role**
Отображает имя роли.

6.7 Меню «Security»

- **Function Right**

Выберите функциональные права роли:

- **1**

Пользователи с этой ролью могут читать параметры устройства, но не могут их изменять. Пользователи с этой ролью могут изменить свой пароль.

- **15**

Пользователи с этой ролью могут как читать, так и изменять параметры устройства.

Примечание

Изменить права функции невозможно.

После того, как роль назначена, больше невозможно изменить функциональные права роли.

Когда необходимо изменить права роли, выполните следующие действия:

1. Удалите всех назначенных пользователей.
 2. Измените функциональные права роли.
 3. Снова назначьте роль.
-

- **Description**

Введите описание для роли. Описание отображается для предопределённых ролей. Текст описания может содержать до 100 символов.

Порядок действий

Создать роль

1. Введите имя роли.
2. Щёлкните кнопку «Create».
3. Выберите функциональные права роли.
4. Введите описание роли.
5. Щёлкните кнопку «Set values».

Удалить роль

1. Установите флажок в строке, которую необходимо удалить.
2. Щёлкните кнопку «Delete». Записи удаляются, а страница обновляется.

6.7.2.3 Groups

Группы пользователей

На этой странице можно связать группы и роли.

В этом примере группа «admins» связана с ролью «admin». Группа определяется на сервере RADIUS. Роль определяется локально на устройстве. Если сервер RADIUS

аутентифицирует пользователя и относит его к группе «admins», то этот пользователь получает на устройстве права роли «admin».

Примечание

От прав авторизованного пользователя зависит, какие значения будут отображаться.

Select	Group	Role	Description
☐	Administrators	admin	Mapping group Administrators (RADIUS) to role admin (device)

1 entry.

Create Delete Set Values Refresh

Описание

Страница содержит следующее:

- **Group Name**
Введите имя группы. Имя должно соответствовать группе на сервере RADIUS. Имя должно соответствовать следующим условиям:

- Оно должно быть уникальным.
- Оно должно содержать от 1 до 64 символов.
- Запрещены символы: § ? " ; :

Таблица содержит следующие столбцы:

- **Select**
Установите флажок в строке, которую необходимо удалить.
- **Group**
Отображает имя группы.
- **Role**
Выберите роль. Пользователи, прошедшие аутентификацию в связанной группе через сервер RADIUS, получают права этой роли на устройстве локально. Можно выбирать между предустановленными и самоопределёнными ролями, см. страницу Security >User> Roles.
- **Description**
Введите описание связи группы и роли. Текст описания может содержать до 100 символов.

Порядок действий

Свяжите группу с ролью

1. Введите имя группы.
2. Щёлкните кнопку «Create».

6.7 Меню «Security»

3. Выберите роль.
4. Задайте описание связи группы и роли.
5. Щёлкните кнопку «Set Values».

Удалить связь между группой и ролью

1. Установите флажок в строке, которую необходимо удалить.
2. Щёлкните кнопку «Delete». Записи удаляются, а страница обновляется.

6.7.3 Пароли

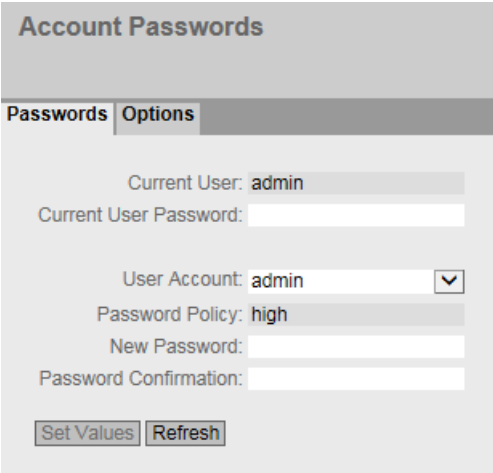
6.7.3.1 Пароли

Конфигурация паролей устройства

Примечание

Если вход в систему выполнен через сервер RADIUS, то невозможно изменять пароли локальных устройств.

На этой странице можно изменять пароли. Если выполнен вход в систему с правами чтения/записи, то можно изменить пароли для всех учётных записей пользователей. Когда выполнен вход в систему с правами чтения, можно изменять только свой собственный пароль.



Описание отображаемых значений

Страница содержит следующие поля:

- **Current User**
Отображает пользователя, который в настоящее время вошёл в систему.
- **Current User Password**
Введите пароль текущего авторизованного пользователя.
- **User Account**
Выберите пользователя, пароль которого необходимо изменить.
- **Password Policy**
Отображает, какая политика паролей используется при назначении Passwords .
 - **High**
Длина пароля: минимум 8 символов, максимум 32 символа
Минимум 1 прописная буква
Минимум 1 специальный символ
Минимум 1 цифра
 - **Low**
Длина пароля: минимум 6 символов, максимум 32 символа
 - **User Defined**
Пользовательская политика паролей

Можно настроить политику паролей устройства на странице Security > Passwords > Options.
- **New Password**
Введите новый пароль для выбранного пользователя.
Он не должно содержать следующие символы:
 - \$? " ; :
 - Также он не должен содержать символы Delete и пробел.
- **Password Confirmation**
Введите новый пароль ещё раз, для его подтверждения.

Порядок действий

Примечание

Когда осуществляется вход в систему с предварительно установленным пользователем «admin» в первый раз или после перезапуска «Restore Factory Defaults and Restart», вам будет предложено изменить пароль. Кроме того, появляется однократная возможность переименовать предустановленного пользователя «admin».

Заводские имя пользователя и пароль по умолчанию заданы следующим образом:

- admin: admin

Примечание

Изменение пароля в режиме «Trial»

Даже когда пароль изменяется в режиме «Trial», это изменение будет немедленно сохранено.

1. Введите пароль текущего авторизованного пользователя, в поле ввода «Current User Password».
2. Выберите в раскрывающемся списке «User Account» пользователя, пароль которого необходимо изменить.
3. Введите новый пароль для выбранного пользователя в поле ввода «New Password».
4. Повторите новый пароль в поле ввода «Password confirmation».
5. Щёлкните кнопку «Set values».

6.7.3.2 Options

На этой странице задаётся, какая политика паролей используется при назначении паролей.

Password Options

Passwords Options

Password Policy: high

New Password Policy: high ▼

Password Policy Details:

Minimum Password Length: 8

Minimum Number of Numeric Characters: 1

Minimum Number of Special Characters: 1

Minimum Number of Uppercase Letters: 1

Minimum Number of Lowercase Letters: 0

Set Values Refresh

Описание

- **Password Policy**
Отображает, какая политика паролей используется в настоящий момент.
- **New Password Policy**
Выберите в раскрывающемся списке необходимую настройку:
 - High
Длина пароля: минимум 8 символов, максимум 128 символов
Минимум 1 число
Минимум 1 специальный символ
Минимум 1 прописная буква
 - Low
Длина пароля: минимум 6 символов, максимум 128 символов
 - User Defined
Настройте необходимые требования к паролю в пункте меню «Password Policy Details».
- **Password Policy Details**
Когда выбрана политика паролей «high» или «low», отображаются соответствующие требования к паролям.
Если выбрана политика паролей «User Defined», то можно настроить требования к паролям.
 - Minimum Password Length
Задаёт минимальную длину пароля.
 - Минимальное количество цифр
Задаёт минимальное количество цифр, которое должен иметь пароль.
 - Минимальное число специальных символов
Задаёт минимальное число специальных символов, которое должен иметь пароль.
 - Минимальное число заглавных букв
Задаёт минимальное число заглавных букв, которое должен иметь пароль.
 - Минимальное число прописных букв
Задаёт минимальное число прописных букв, которое должен иметь пароль.

6.7.4 AAA

6.7.4.1 General

Регистрация абонентов сети

Используемое сокращение «AAA» означает «Authentication, Authorization, Accounting». Эта функция используется для идентификации и допуска абонентов сети, а также для предоставления им соответствующих служб.

На этой странице можно настроить вход в систему.

The screenshot shows a web-based configuration interface for a RADIUS Client. The 'General' tab is selected. Under 'Login Authentication', a dropdown menu is set to 'Local'. The 'NAS ID' field contains the text 'fsNas1'. At the bottom, there are two buttons: 'Set Values' and 'Refresh'.

Описание отображаемых полей

Страница содержит следующие поля:

Примечание

Чтобы иметь возможность использовать аутентификацию входа сервер «RADIUS», сервер RADIUS должен быть сохранен и сконфигурирован для аутентификации пользователя.

- **Login Authentication**

Задайте, как осуществляется вход в систему:

- Local
Аутентификация должна выполняться локально на устройстве.
- RADIUS
Аутентификация должна выполняться через сервер RADIUS.
- Local and RADIUS
Аутентификация может выполняться как через учётные записи пользователей, имеющих на устройстве (имя пользователя и пароль), так и через сервер RADIUS. Сначала выполняется поиск пользователя в локальной базе данных. Если пользователь отсутствует, то отправляется запрос RADIUS.
- RADIUS and fallback Local
Аутентификация должна выполняться через сервер RADIUS. Локальная аутентификация выполняется только в том случае, если сервер RADIUS недоступен в сети.

- **NAS ID**

Введите в это текстовое поле NAS ID (Network Access Server Identifier). NAS ID идентифицирует устройство, которое отправляет запрос на сервер RADIUS.

6.7.4.2 RADIUS Client

Аутентификация через внешний сервер

Концепция RADIUS основана на внешнем сервере аутентификации.

Каждая строка таблицы содержит данные доступа для одного сервера. Первым в порядке поиска запрашивается первичный сервер. Когда первичный сервер недоступен, вторичные серверы запрашиваются в указанном порядке.

Когда ни один из серверов не отвечает на запрос, аутентификация не осуществляется.

Remote Authentication Dial In User Service (RADIUS) Client

General | **RADIUS Client** | 802.1X Authenticator

RADIUS Authorization Mode: Standard
☐ Disconnect Packet

Select	Auth. Server Type	RADIUS Server Address	Server Port	Shared Secret
☐	Login & 802.1X v	0.0.0.0	1812	••••••
☐	Login & 802.1X v	10.0.0.1	1812	••••••

2 entries.

Продолжение таблицы:

Shared Secret Conf.	Max. Retrans.	Timeout[s]	Primary Server	Test	Test Result
	3	5	no v	Test	

Описание отображаемых полей

Страница содержит следующие поля:

- **RADIUS Authorization Mode**
 Режим RADIUS Authorization Mode задаёт для аутентификации входа в систему, как права назначаются пользователям в случае их успешной Authentication.
 - Standard
 В этом режиме пользователь входит в систему с правами администратора, если сервер возвращает устройству значение «Administrative User» для атрибута «Service Type». Во всех остальных случаях пользователь входит в систему с правами чтения.
 - Vendor Specific
 В этом режиме назначение прав зависит от того, возвращается ли сервер для пользователя группу и какую, а кроме того имеется ли запись для пользователя в таблице «External users accounts».
- **Disconnect Packet**
 Когда установлен этот флажок, устройство будет оценивать сообщения об отключении от сервера RADIUS.

6.7 Меню «Security»

Таблица состоит из следующих столбцов:

- **Select**
Выберите строку, которую необходимо удалить.
- **Auth. Server Type**
Выберите тип аутентификации, для которого следует использовать сервер.
 - Login
Сервер используется только для аутентификации при входе в систему.
 - 802.1X
Сервер используется только для аутентификации 802.1X.
 - Login & 802.1X
Сервер используется для обоих типов аутентификации.
- **RADIUS Server Address**
Введите IP-адрес сервера RADIUS.
- **Server Port**
Введите здесь входной порт на сервере RADIUS. Входной порт 1812 установлен по умолчанию. Диапазон значений 1 ... 65535.
- **Shared Secret**
Введите здесь свой идентификатор доступа. Диапазон значений от 1 до 128 символов.
- **Shared Secret Conf.**
Введите идентификатор доступа ещё раз для подтверждения.
- **Max. Retrans.**
Введите здесь максимальное количество повторов запроса.
Первоначальная попытка подключения повторяется на указанное здесь число до того, как будет опрошен другой сконфигурированный сервер RADIUS или до того, как вход в систему будет определён как неудавшийся. По умолчанию установлено 3 попытки, что означает 4 попытки подключения. Диапазон значений 1...5.
- **Timeout [s]**
Задайте время, в течение которого клиент будет ждать ответа от сервера RADIUS.
- **Primary Server**
Используйте опции раскрывающегося списка, чтобы указать, является ли этот сервер основным. Можно выбрать из опций «yes» или «no».

- **Test**
С помощью этой кнопки можно проверить, доступен ли заданный сервер RADIUS. Тест проводится однократно и не повторяется циклически.
 - **Test Result**
Отображает, доступен ли сервер RADIUS.
 - Not reachable
IP-адрес недоступен.
IP-адрес доступен, но сервер RADIUS не функционален.
 - Reachable, key not accepted
IP-адрес доступен, сервер RADIUS работает, но не принимает заданный Shared Secret.
 - Reachable, key not accepted
IP-адрес доступен, сервер RADIUS работает и принимает заданный Shared Secret.
- Результат теста не обновляется автоматически. Для того чтобы удалить результат теста, нажмите кнопку «Refresh».

Порядок действий при конфигурации

Добавить новый сервер

1. Щёлкните кнопку «Create». В таблице создаётся новая запись.
В таблицу занесены следующие стандартные значения:
 - Auth. Server Type Login & 802.1X
 - RADIUS Server Address: 0.0.0.0
 - Server Port: 1812
 - Max. Retrans. 3
 - Primary Server: Нет
 2. Введите следующие данные в поля ввода в соответствующей строке:
 - Необходимый тип сервера аутентификации
 - RADIUS Server Address
 - Server Port
 - Shared Secret
 - Shared Secret Confirmation
 - Max. Retrans. 3
 - Primary Server: yes/no
 3. Щёлкните кнопку «Set values».
 4. При необходимости проверьте доступность сервера RADIUS.
- Повторите процедуру для всех серверов, которые необходимо зарегистрировать.

6.7 Меню «Security»

Изменить сервер

1. Введите следующие данные в поля ввода в соответствующей строке:
 - RADIUS Server Address
 - Server Port
 - Shared Secret
 - Shared Secret Confirmation
 - Max. Retrans
 - Primary Server
2. Щёлкните кнопку «Set values».
3. При необходимости проверьте доступность сервера RADIUS.

Повторите процесс для всех серверов, запись которых необходимо изменить.

Удалить сервер

1. Установите флажок в первом столбце, которую перед строкой необходимо удалить, чтобы выделить запись для удаления.
Повторите процедуру для всех записей, которые необходимо удалить.
2. Щёлкните кнопку «Delete». Записи удаляются из памяти устройства, и данная страница обновляется.

6.7.4.3 Аутентификация пользователей 802.1X

Настроить доступ к сети

Оконечное устройство может получить доступ к сети только после того, как устройство проверит данные для входа на сервер аутентификации. Аутентификация может быть осуществляться через 802.1X или MAC-адрес.

Для аутентификации через 802.1X, как оконечное устройство, так и сервер аутентификации должны поддерживать протокол Protocol (Extensive Authentication Protocol).

Активация аутентификации для отдельных портов

Активируя соответствующие опции, можно индивидуально для каждого порта задать, будет ли активирована на этом порте защита доступа к сети в соответствии со стандартом IEEE 802.1X.

802.1X Authenticator

General | **RADIUS Client** | 802.1X Authenticator

☐ MAC Authentication
☐ Guest VLAN
802.1X Fallback Timeout[s]: 0
802.1X Fallback Retry Count: 3

	802.1X Auth. Control	802.1X Re-Authentication	Re-Authentication Timeout	Tx Timeout	MAC Authentication	MAC Auth. only on Timeout
All ports	No Change	No Change	No Change	No Change	No Change	No Change

Port	802.1X Auth. Control	802.1X Re-Authentication	Re-Authentication Timeout	Tx Timeout	MAC Authentication	MAC Auth. only on Timeout
P1.1	Force Authorized	☐	3600	5	☐	☐
P1.2	Force Authorized	☐	3600	5	☐	☐
P1.3	Force Authorized	☐	3600	5	☐	☐
P1.4	Force Authorized	☐	3600	5	☐	☐

RADIUS VLAN Assignment Allowed	Default VLAN ID	MAC Auth. Max Allowed Addresses	Guest VLAN	Guest VLAN ID	Guest VLAN Max Allowed Addresses	Copy to Table
No Change	No Change	No Change	No Change	No Change	No Change	Copy to Table

RADIUS VLAN Assignment Allowed	Default VLAN ID	MAC Auth. Max Allowed Addresses	Guest VLAN	Guest VLAN ID	Guest VLAN Max Allowed Addresses
☐	0	1	☐	1	1
☐	0	1	☐	1	1
☐	0	1	☐	1	1
☐	0	1	☐	1	1

Описание отображаемых полей

Страница содержит следующие поля:

- **MAC Authentication**
Активируйте или деактивируйте функцию MAC Authentication для устройства.
- **Guest VLAN**
Активируйте или деактивируйте функцию Guest VLAN для устройства.

- **802.1X Fallback Timeout [s]**
Задайте временной интервал в секундах, по истечении которого устройство будет повторно инициализировано на соответствующем порте при отсутствии MAC Authentication для 802.1X Authentication. Значение по умолчанию – 0 секунд, т.е. для аутентификации 802.1X нет времени ожидания возврата в исходный режим и повторной инициализации.
- **802.1X Fallback Retry Count**
Задайте, как часто порт повторно инициализируется для аутентификации 802.1X, если аутентификация MAC отсутствует.

Таблица 1 состоит из следующих столбцов:

- **1-й столбец**
Показывает, что настройки действительны для всех портов в таблице 2.
- **802.1X Auth. Control**
Выберите необходимую настройку.
Если выбрано значение «No Change», то запись в таблице 2 не изменяется.
- **802.1X Re-Authentication**
Выберите необходимую настройку.
Если выбрано значение «No Change», то запись в таблице 2 не изменяется.
- **Re-Authentication Timeout**
Выберите необходимую настройку.
Если выбрано значение «No Change», то запись в таблице 2 не изменяется.
- **Tx Timeout**
Значение указывает промежуток времени в секундах, по истечении которого отправляется пакет запроса EAP, если ни один клиент не отвечает. Если MAC Authentication активирована, после третьего пакета запроса EAP происходит переключение с 802.1X Authentication на MAC Authentication. Значение по умолчанию – 5 секунд. Если выбрано значение «No Change», то запись в таблице 2 не изменяется.
- **MAC Authentication**
Выберите необходимую настройку.
Если выбрано значение «No Change», то запись в таблице 2 не изменяется.
- **MAC Auth. only on Timeout**
Выберите необходимую настройку.
Если выбрано значение «No Change», то запись в таблице 2 не изменяется.
- **RADIUS VLAN Assignment Allowed**
Выберите необходимую настройку.
Если выбрано значение «No Change», то запись в таблице 2 не изменяется.

Примечание

Функции Private VLAN и аутентификация RADIUS

Если активировано присвоение VLAN через аутентификацию RADIUS для одного или нескольких портов сети VLAN, то эту сеть VLAN не потребуется дополнительно конфигурировать как Private VLAN.

Спектр функций Private VLAN в связи с присвоением VLAN через аутентификацию RADIUS может привести к не единообразному состоянию системы.

- **MAC Auth. Max Allowed Addresses**
Введите количество MAC-адресов, которым разрешено связываться через порт одновременно.
Если введено значение «No Change», запись в таблице 2 не изменяется.
- **Guest VLAN**
Выберите необходимую настройку.
Если выбрано значение «No Change», то запись в таблице 2 не изменяется.
- **Guest VLAN**
Введите идентификатор VLAN порта.
Если введено значение «No Change», запись в таблице 2 не изменяется.
- **Guest VLAN Max Allowed Addresses**
Введите количество конечных устройств, подключённых к этому порту одновременно, в поле «Guest VLAN».
Если введено значение «No Change», запись в таблице 2 не изменяется.
- **Copy to Table**
Если нажать эту кнопку, то настройки будут применены для всех портов таблицы 2.

Таблица 2 состоит из следующих столбцов:

- **Port**
В этом столбце отображаются все порты, доступные в данном устройстве.
- **802.1X Auth. Control**
Задайте аутентификацию порта:
 - Force Unauthorized
Обмен данными через порт заблокирован.
 - Force Authorized
Обмен данными через порт разрешён без ограничений.
Заводская настройка
 - Auto
Конечные устройства аутентифицируются на порте с использованием процедуры «802.1X».
Обмен данными через порт разрешён или заблокирован в зависимости от результата аутентификации.
- **802.1X Re-Authentication**
Активируйте эту опцию, если повторная аутентификация должна выполняться циклически для уже аутентифицированного конечного устройства.
- **Re-Authentication Timeout**
Задайте временной интервал в секундах, по истечении которого устройство будет повторно инициализировано на соответствующем порте. Значение по умолчанию составляет 3600 секунд.
- **Tx Timeout**
Значение указывает промежуток времени в секундах, по истечении которого отправляется пакет запроса EAP, если ни один клиент не отвечает. Если MAC Authentication активирована, после третьего пакета запроса EAP происходит переключение с 802.1X Authentication на MAC Authentication. Значение по умолчанию – 5 секунд.

- **MAC Authentication**
Активируйте эту опцию, если оконечные устройства должны проходить аутентификацию через процедуру «MAC Authentication». Если «802.1X Auth. Control» настроен на режим «Auto» и активировано «MAC Authentication», то время ожидания для процедуры «802.1X» составляет 5 секунд. Если для аутентификации на порте с помощью процедуры «802.1X» требуется ввод вручную, 5 секунд может быть недостаточно. Для того чтобы иметь возможность выполнять аутентификацию через «802.1X», отключите MAC-аутентификацию на этом порте.
- **MAC Auth. only on Timeout**
Когда флажок установлен, MAC-аутентификация возможна только после времени ожидания 802.1X, но не после неудавшейся аутентификации 802.1X. Когда флажок не установлен, MAC-аутентификация возможна, как после времени ожидания 802.1X, так и после неудавшейся аутентификации 802.1X.
- **RADIUS VLAN Assignment Allowed**
Сервер RADIUS сообщает IE-коммутатору, к какой сети VLAN должен принадлежать порт. Активируйте эту опцию, если необходимо учитывать информацию сервера. Порт может быть назначен соответствующей сети VLAN, только если VLAN была создана на устройстве. В противном случае аутентификация отклоняется.
- **MAC Auth. Max Allowed Addresses**
Введите количество MAC-адресов, которым разрешено связываться через порт одновременно.

Примечание

Когда устройство использует несколько MAC-адресов, все MAC-адреса должны быть аутентифицированы. Сохраните все MAC-адреса для аутентификации на сервере RADIUS. Введите соответствующее число в поле «MAC Auth. Max Allowed Addresses».

- **Guest VLAN**
Активируйте эту опцию, если оконечное устройство должно быть разрешено в "Guest VLAN" в случае неудавшейся аутентификации. Порт может быть назначен соответствующей сети VLAN, только если VLAN была создана на устройстве. В противном случае аутентификация отклоняется. Эта функция также называется «Authentication failed VLAN».
- **Guest VLAN**
Введите идентификатор VLAN гостевой сети VLAN.
- **Guest VLAN Max Allowed Addresses**
Введите количество оконечных устройств, подключённых к этому порту одновременно, в поле «Guest VLAN».

Порядок действий при конфигурации

Активировать аутентификацию для одного порта

1. Активируйте необходимые опции в соответствующей строке таблицы 2.
2. Чтобы применить изменения, щёлкните кнопку «Set Values».

Активировать аутентификацию для всех портов

1. Выберите необходимые опции в соответствующей строке таблицы 1.
2. Щёлкните кнопку «Copy to Table». Соответствующие настройки для всех портов приняты в таблице 2
3. Чтобы применить изменения, щёлкните кнопку «Set Values».

6.7.5 Management ACL

Описание конфигурации

На этой странице можно повысить безопасность своего устройства. Для того чтобы задать, какой станции с какого IP-адреса разрешён доступ к вашему устройству, настройте IP-адрес или весь диапазон адресов.

Можно задать, какие протоколы и через какие порты станция может получать доступ к устройству.

Management Access Control List

☐ Management ACL

IP Address:
 Subnet Mask:

Select	Rule Order	IP Address	Subnet Mask	VLANs Allowed	SNMP	TELNET	HTTP	HTTPS	SSH	P0.1	P0.2
☐	1	192.168.16.254	255.255.255.255	1-4094	☒	☒	☒	☒	☒	☒	☒

1 entry.

Описание отображаемых полей

Примечание

Перед активацией этой функции обратите внимание на следующее

Неверное конфигурирование может привести к потере доступа к устройству. Подобная ситуация разрешается сбросом устройство до заводских настроек и повторной его перенастройкой. Поэтому следует настроить правила доступа, которые позволят получить доступ к управлению, перед активацией функции.

Страница содержит следующие поля:

- **Management ACL**

Активируйте или деактивируйте контроль доступа к управлению IE-коммутатором. В состоянии поставки функция деактивирована.

Примечание

Когда функция деактивирована, есть неограниченный доступ к управлению IE-коммутатором. Настроенные правила доступа имеют силу, только при активированной функции.

- **IP Address**

Задайте IPv4-адрес или сетевой адрес, к которому должно применяться правило. Если используется IPv4-адрес 0.0.0.0, настройки применяются ко всем IPv4-адресам.

- **Subnet Mask**

Введите маску подсети для создаваемой подсети. Маска подсети 255.255.255.255 предназначена для определенного IPv4-адреса. Когда необходимо разрешить использование подсети, задайте, например, для подсети класса C 255.255.255.0. Маска подсети 0.0.0.0 применяется ко всем подсетям.

Таблица состоит из следующих столбцов:

- **Select**

Выберите строку, которую необходимо удалить.

- **Rule Order**

Отображает порядок, в котором проверяются правила ACL. Как только правило подходит, оно применяется. Следующие правила не рассматриваются.

- **IP Address**

Отображает IPv4-адрес.

- **Subnet Mask**

Отображает маску подсети.

- **VLANs Allowed**

- В режиме Base Bridge Mode «802.1Q VLAN Bridge»

Введите номер сети VLAN, в которой находится устройство. Только станция может получить доступ к устройству, если оно находится в данной сконфигурированной сети VLAN. Когда это поле ввода остаётся пустым, ограничения в отношении сети VLAN отсутствуют.

- В режиме Base Bridge Mode «802.1D Transparent Bridge»

Нельзя задать какие-либо правила доступа для сети VLAN. Правила применяются ко всем сетям VLAN.

Примечание

Совместимость с предыдущей прошивкой

Когда задаются определенные сети VLAN с версией прошивки <1.2, конфигурация сетей VLAN заменяется значением по умолчанию «1-4094» во время обновления прошивки.

- **SNMP**
Задайте, может ли станция (или IPv4-адрес) получить доступ к устройству по протоколу SNMP.
- **TELNET**
Задайте, может ли станция (или IPv4-адрес) получить доступ к устройству по протоколу TELNET.
- **HTTP**
Задайте, может ли станция (или IPv4-адрес) получить доступ к устройству по протоколу HTTP.
- **HTTPS**
Задайте, может ли станция (или IPv4-адрес) получить доступ к устройству по протоколу HTTPS.
- **SSH**
Задайте, может ли станция (или IPv4-адрес) получить доступ к устройству по протоколу SSH.
- **Px.y**
Задайте, может ли станция (или IPv4-адрес) получить доступ к устройству через этот порт.
Порт складывается из номера модуля и номера порта, например, порт 0.1 означает модуль 0, порт 1.

Порядок действий при конфигурации

Примечание

Перед активацией этой функции обратите внимание на следующее

Неверное конфигурирование может привести к потере доступа к устройству. Подобная ситуация разрешается сбросом устройства до заводских настроек и повторной его перенастройкой. Поэтому следует настроить правила доступа, которые позволят получить доступ к управлению, перед активацией функции.

Примечание

Обратите внимание на последовательность

Порядок, в котором создаются правила ACL, соответствует порядку, в котором правила проверяются. Как только правило подходит, оно применяется. Следующие правила не рассматриваются.

Создать новое правило

1. Введите IP-адрес в поле ввода «IP Adress».
2. Введите маску подсети в поле ввода «Subnet Mask».
3. Щёлкните кнопку «Create» для создания новой строки в таблице.
4. Сконфигурируйте записи в новой строке.
5. Щёлкните кнопку «Set Values», чтобы перенести новую запись на устройство.

Активация функции

1. Установите флажок напротив «Management ACL».
2. Щёлкните кнопку «Set Values», чтобы активировать настроенные правила доступа.

Изменить правило

1. Настройте данные правила, которое необходимо изменить.
2. Щёлкните кнопку «Set Values», чтобы перенести изменения на устройство.

Удалить сервер

1. Установите флажок в строке, которую необходимо удалить.
2. Повторите процедуру для каждой записи, которую необходимо удалить.
3. Щёлкните кнопку «Delete». Правила будут удалены, а страница обновлена.

6.7.6 Brute Force Prevention

Описание конфигурации

Под Brute Force Prevention понимается защита устройства от несанкционированного доступа путём перебора достаточно большого количества паролей. Для этого число попыток несанкционированного входа ограничено определенным промежутком времени.

Brute Force Prevention

User Specific BFP is Enabled

Acceptable Invalid Login Attempts Per User: 5

IP Specific BFP is Enabled

Acceptable Invalid IP Login Attempts Per IP: 10

Global Parameters

BFP Trigger Interval[min]: 5

BFP Automatic Reset Timer[min]: 12

User Specific BFP:

User	Failed Logins	Last Failed[s]	Blocked[s]	Clear
Unknown User	0	0	not blocked	Clear
admin	0	0	not blocked	Clear
Service	7	28	692	Clear

3 entries.

IP Specific BFP:

IP	Failed Logins	Last Failed[s]	Blocked[s]	Clear
192.168.178.2	0	0	not blocked	Clear

Set Values

Refresh

Описание отображаемых полей

Страница содержит следующие поля:

- **User Specific BFP is Enabled/User Specific BFP is Disabled**
Отображает, активирована ли специфическая для пользователя функция Brute Force Prevention.
Возможно ли активировать специфическую для пользователя функцию Brute Force Prevention, зависит от Login Authentication. Сконфигурируйте Login Authentication в меню Security > AAA > General в раскрывающемся списке «Login Authentication». Специфичная для пользователя функция Brute Force Prevention доступна для процедур «Local» и «Local and RADIUS» и не доступна для процедур «RADIUS» и «RADIUS and Fallback Local».
- **Acceptable Invalid Login Attempts Per User**
Максимальное число неудавшихся попыток входа в систему для IP-адреса, при котором возможность входа будет заблокирована. Все пользователи, которые не сконфигурированы как локальные пользователи для устройства, группируются под именем пользователя «UnknownUser».
Если задано значение «0», то специфическая для пользователя функция Brute Force Prevention деактивирована.
Значение по умолчанию равно «12».
- **IP Specific BFP is Enabled**
Отображает, активирована ли специфическая для IP функция Brute Force Prevention.
- **Acceptable Invalid Login Attempts pro IP**
Максимальное количество неудавшихся попыток входа в систему для IP-адреса, при котором возможность входа будет заблокирована.
Если задано значение «0», то специфическая для IP функция Brute Force Prevention деактивирована.
Значение по умолчанию равно «10».
- **BFP Trigger Intervall**
Время в минутах, значимое для подсчёта несанкционированных попыток входа в систему. Когда в течение этого периода достигнуто количество разрешённых неудавшихся попыток входа в систему (для каждого пользователя и IP-адреса), устройство блокирует вход на определенный период времени.
Несанкционированные попытки входа в систему для каждого пользователя и IP-адреса обрабатываются независимо друг от друга. Можно ввести значение от 5 до 255 минут. Значение по умолчанию составляет 5 минут.
- **BFP Automatic Reset Timer**
Время в минутах, в течение которого устройство блокирует вход из-за превышения максимального количества неудавшихся попыток входа. Можно задать значение от 0 до 255 минут.
Когда задано значение «0», вход в систему будет заблокирован на неопределённый срок после достижения максимального числа неудавшихся попыток входа.
Значение по умолчанию составляет 12 минут.

Таблица **User Specific BFP** состоит из следующих столбцов:

- **User**
Пользователь, совершивший попытку авторизации.
- **Failed Logins**
Число неудавшихся попыток входа в систему.

6.7 Меню «Security»

- **Last Failed Logins**
Время в секундах с момента последней неудавшейся попытки входа в систему. Чтобы отобразить текущее значение, щёлкните кнопку «Refresh».
- **Blocked**
Отображает статус пользователя:
 - Not blocked
Возможен вход с этим именем пользователя.
 - Временной промежуток
Временной промежуток в секундах, в течении которого вход с именем пользователя будет заблокирован. Чтобы отобразить текущее значение, щёлкните кнопку «Refresh».
Когда блокировка снимается по истечении времени, заданного в поле «BFP Automatic Reset Timer», статус пользователя меняется на «Not blocked».
 - indefinitely blocked
Вход с этим именем пользователя будет заблокирован до тех пор, пока блокировка не будет снята вручную или перезапущено устройство.
- **Delete**
Снимает блокировку пользователя и сбрасывает показания следующих индикаторов:
 - Значение в поле «Last Failed Logins» установлено на «0».
 - Состояние пользователя в поле «Blocked» установлен на «Not blocked».

Таблица **IP Specific BFP** разделена на следующие столбцы:

- **IP**
IP-адрес устройств для попытки входа в систему.
- **Failed Logins**
Число неудавшихся попыток входа в систему.
- **Last Failed Logins**
Временной промежуток в секундах с момента последней неудавшейся попытки входа в систему. Чтобы отобразить текущее значение, щёлкните кнопку «Refresh».

- **Blocked**

Показывает состояние IP-адреса:

- Not blocked
Возможен вход с этим IP-адресом.
- Временной промежуток
Время в секундах, в течение которого вход с данным IP-адресом будет заблокирован. Чтобы отобразить текущее значение, щёлкните кнопку «Refresh». Когда блокировка снимается по истечении времени, заданного в поле «BFP Automatic Reset Timer», статус IP-адреса меняется на «Not blocked».
- indefinitely blocked
Вход с этим IP-адресом будет заблокирован до тех пор, пока блокировка не будет снята вручную или перезапущено устройство.

- **Delete**

Снимает блокировку IP-адреса и сбрасывает показания следующих индикаторов:

- Значение в поле «Last Failed Logins» установлено на «0».
- Состояние IP-адреса в поле «Blocked» установлено на «Not blocked».

Устранение неполадок / FAQ

7.1 Загрузка новой прошивки через протокол TFTP без WBM и CLI

Микропрограммное обеспечение

Микропрограммное обеспечение зашифровано и закодировано. Предусмотрены меры для того, чтобы разрешить загрузку в устройство только микропрограммного обеспечения, созданного компанией Siemens.

Использование кнопки

Для загрузки новой прошивки используется кнопка. При использовании кнопки обязательно следуйте указаниям в соответствующих инструкциях.

Нажмите кнопку «RESET» на устройстве SCALANCE XB-200.

Нажмите кнопку «SELECT/SET» на устройстве SCALANCE XB-200.

Нажмите кнопку «SET» на устройстве SCALANCE XB-200BA.

Нажмите кнопку «RESET» на устройстве SCALANCE XB-200BA.

Нажмите кнопку «RESET» на устройстве SCALANCE XR-300WG.

Порядок действий в ОС Microsoft Windows

С помощью протокола TFTP на устройство можно загрузить новую прошивку. Для этого устройство не должно быть доступно ни через WBM, ни через CLI. Это может произойти в случае исчезновения напряжения во время обновления прошивки.

Перед нажатием кнопки обязательно следуйте указаниям в главе «AUTOHOTSPOT».

Чтобы загрузить новую прошивку через протокол TFTP, выполните следующие действия:

1. Обесточьте устройство.
2. Нажмите кнопку SELECT/SET и при нажатой кнопке снова подключите устройство к источнику питания.
3. Удерживайте кнопку нажатой до тех пор, пока не начнёт мигать красный светодиод ошибок «F».
4. Отпустите кнопку, когда красный светодиод ошибок «F» всё ещё мигает. Этот интервал времени длится несколько секунд. Загрузчик операционной системы устройства ожидает в этом состоянии новый файл прошивки, который можно загрузить по протоколу TFTP.
5. Подсоедините ПК с помощью кабеля Ethernet к порту сети Ethernet устройства.

7.2 Сообщения: SINEMA Configuration not accepted yet

6. С помощью DHCP или SINEC PNI присвойте устройству IP-адрес.
7. Перейдите по командной строке Windows в каталог, в котором находится файл с новой прошивкой и введите следующую команду:
`tftp -i <IP-адрес> put <файл прошивки>`

Примечание

В ОС Microsoft Windows протокол TFTP можно активировать в настройке:

«Панель управления» > «Программы и компоненты» > «Включение и отключение компонентов Windows» > «Клиент TFTP»

После полной передачи прошивки на устройство и проверки её действительности устройство автоматически перезапускается. Этот процесс может длиться несколько минут.

7.2 Сообщения: SINEMA Configuration not accepted yet

Если в области индикации отображается следующее сообщение, произошла ошибка при передаче конфигурации на устройство из ПО STEP 7 Basic / Professional V13 или выше:

SINEMA Configuration not accepted yet. With restart of device, all configuration changes will be lost.

Одна из возможных причин, например, то что устройство больше не доступно во время передачи.

При изменении параметра непосредственно в устройстве (WBM/CLI/SNMP), эти изменения будут потеряны при перезапуске устройства.

Способ устранения

1. Откройте соответствующий проект STEP 7 в ПО STEP 7 Basic / Professional.
2. Откройте представление проекта.
3. Выберите устройство в навигации проекта.
4. В контекстном меню выбранного устройства выберите команду «Go to Network Overview».
5. Выберите устройство в представлении сети.
6. В контекстном меню выбранного устройства выберите команду «SCALANCE Configuration interface > Save as Startup Configuration».

Результат

Конфигурация сохраняется на устройстве. Сообщение в области индикации больше не отображается. Изменение конфигурации, произведённое непосредственно на устройстве, больше не будет потеряно при перезапуске устройства.

7.3 Обмен данными конфигурации через файл с ПО STEP7 Basic/Professional

Можно использовать два типа файлов «RunningSINEMAConfig» и «SINEMAConfig» (пункт меню System > Load&Save > HTTP/TFTP/SFTP") для обмена данными конфигурации между устройством (WBM) и ПО STEP7 Basic/Professional через файл. Экспорт/импорт файла с использованием ПО STEP 7 Basic/Professional описан ниже.

Экспорт данных конфигурации через ПО STEP 7 Basic/Professional

Для того чтобы экспортировать данные конфигурации через ПО STEP 7 Basic/Professional, выполните следующие действия:

1. Откройте соответствующий проект STEP 7 в ПО STEP 7 Basic/Professional.
2. Откройте представление проекта.
3. Откройте представление сети или топологии.
4. Откройте каталог оборудования.
5. В каталоге оборудования перейдите к устройству с соответствующим артикульным номером.
6. Щелчком мыши выберите необходимое устройство.
7. Установите соответствующую версию прошивки, используя раскрывающийся список каталога оборудования.
8. Используйте перетаскивание, чтобы переместить устройство в представлении сети или топологии.
9. Выберите устройство в представлении сети или топологии.
10. Настройте устройство в окне инспектора в меню Properties > General.
11. Настройте устройство в окне инспектора в меню Properties > General в параметре «Control».
12. В группе параметров «File Loading / Save» нажмите кнопку «Save to file».
13. Выберите место для сохранения файла.
14. Укажите имя файла.
15. Щёлкните кнопку «Save».
Откроется диалоговое окно «Save config».
16. Назначьте пароль для шифрования файла.

Примечание

Этот пароль понадобится, если файл загружался в устройство через интерфейс WBM.

17. Нажмите кнопку «OK».

Импорт данных конфигурации через ПО STEP 7 Basic/Professional

Для того чтобы импортировать данные конфигурации через ПО STEP 7 Basic/Professional, выполните следующие действия:

1. Откройте соответствующий проект STEP 7 в ПО STEP 7 Basic/Professional.
2. Откройте представление проекта.
3. Откройте представление сети или топологии.
4. Откройте каталог оборудования.
5. В каталоге оборудования перейдите к устройству с соответствующим артикульным номером.
6. Щелчком мыши выберите необходимое устройство.
7. Установите соответствующую версию прошивки, используя раскрывающийся список каталога оборудования.
8. Используйте перетаскивание, чтобы переместить устройство в представлении сети или топологии.
9. Выберите устройство в представлении сети или топологии.
10. Настройте устройство в окне инспектора в меню Properties > General в параметре «Control».
11. В группе параметров «File Load / Save» нажмите кнопку «Load from file».
12. Выберите необходимый файл.
13. Щёлкните кнопку «Open».
Откроется диалоговое окно «Load config».
14. Назначьте пароль для дешифрования файла.

Примечание

Этот пароль задаётся в WBM в меню System > Load&Save > Passwords.

15. Нажмите кнопку «OK».

Приложение А

Сообщения системного журнала могут содержать следующие параметры:

Параметр	Описание	Возможные значения или пример
ip address	IPv4- или IPv6-адрес	IP-адрес согласно стандарта RFC1035 или RFC4291 раздел 2.2
src port порт назначения (dest port)	Порт представлен в виде десятичного числа. Формат: %d	0 ... 65535
dest mac src mac	MAC-адрес Формат: %02x:%02x:%02x;%02x:%02x:%02x	00:0C:29:2F:09:B3
protocol	Имя службы, которая сгенерировала это событие, или используемый протокол уровня 4. Формат: %s	Возможные значения для: UDP TCP WBM Telnet SSH TFTP SFTP
group	Строка символов, которая идентифицирует группу на основе её имени Формат: %s	ИТ-сервис
user name	Строка символов, идентифицирующая аутентифицированного пользователя по имени без пробелов Формат: %s	maier
action user name	Идентифицирует пользователя по имени. Это не аутентифицированный пользователь Формат: %s	Peter.Maier
role	Символическое имя для групповой роли Формат: %s	Администратор
time minute timeout	Число минут Формат: %d	44
failed login count	Количество неудачных попыток входа Формат: %d	10
max sessions	Количество сеансов Формат: %d	10
trigger pin	Строка символов для порта ввода/вывода, который инициировал событие без пробелов Формат: %s	D11
firewall rule	Строка для набора правил брандмауэра с пробелами Формат: %s	Rule1

Параметр	Описание	Возможные значения или пример
subject	Строка для темы в сертификате. Используется как часть аутентификации на основе сертификатов с пробелами и также должен содержать символы юникода. Формат: (% S) или (% S% S) для кода UTF8.	(Peter Maier)
config detail	Строка символов для конфигурации с пробелами Формат: %s	OpenVPN
connection name	Имя VPN-соединения	to_Baugruppe1
firewall accept	Выполнено действие брандмауэра (принятый пакет)	ACCEPT
firewall action reject	Действие брандмауэра выполнено (отклонённый пакет)	REJECT DROP
length	Длина сетевого пакета (в байтах) Формат: %d	52
network interface	Символическое имя сетевого интерфейса Формат: %s	vlan1

Примечание**Серьёзность**

Некоторые уровни серьёзности кратко изложены в прошивке:

- Info + Notice = Info
- Warning + Error = Warning
- Critical + Emergency = Critical

Идентификация и аутентификация пользователей (людей)

Текст сообщения	{Local interface}: User {user name} logged in.
Пример	Console: User admin logged in.
Пояснение	Действительные учётные данные вводятся при входе в систему.
Severity	Info
Facility	local0
Стандарт	МЭК 62443-3-3 Reference: SR 1.1

Текст сообщения	{Local interface}: User {user name} failed to log in.
Пример	Console: User admin failed to log in.
Пояснение	При входе в систему введено неверное имя пользователя или пароль.
Severity	Error
Facility	local0
Стандарт	МЭК 62443-3-3 Reference: SR 1.1

Текст сообщения	{Protocol}: User {User name} logged in from {IP address}.
Пример	WBM / UDP / TCP / Telnet / SSH / Console / PNIO / PB / OPC: User admin logged in from 192.168.0.1.
Пояснение	Действительные учётные данные, которые были введены при входе в систему.
Severity	Info
Facility	local0
Стандарт	МЭК 62443-3-3 Reference: SR 1.1

Текст сообщения	{Protocol}: User {User name} failed to log in from {IP address}.
Пример	WBM / UDP / TCP / Telnet / SSH / Console / PNIO / PB / OPC: User admin failed to log in from 192.168.0.1.
Пояснение	При входе в систему введено неверное имя пользователя или пароль.
Severity	Error
Facility	local0
Стандарт	МЭК 62443-3-3 Reference: SR 1.1

Текст сообщения	{Local interface}: User {user name} logged out.
Пример	Console: User admin logged out.
Пояснение	Сеанс пользователя завершён - выход из системы осуществлён.
Severity	Info
Facility	local0
Стандарт	МЭК 62443-3-3 Reference: SR 1.1

Текст сообщения	{protocol}: User {user name} logged out from {ip address}.
Пример	WBM / UDP / TCP / Telnet / SSH / Console / PNIO / PB / OPC: User admin logged out from 192.168.0.1.
Пояснение	Сеанс завершился, когда пользователь вышел из системы.
Severity	Info
Facility	local0
Стандарт	МЭК 62443-3-3 Reference: SR 1.1

Текст сообщения	{Local interface}: Default user {user name} logged in.
Пример	Console: Default user admin logged in.
Пояснение	Пользователь с именем пользователя и паролем по умолчанию вошёл в систему.
Severity	Info
Facility	local0
Стандарт	МЭК 62443-3-3 Reference: не указано (NERC-CIP 007-R5)

Текст сообщения	{protocol}: Default user {user name} logged in from {ip address}.
Пример	WBM / UDP / TCP / Telnet / SSH / Console / PNIO / PB / OPC: Default user <user name> logged in from 192.168.0.1.
Пояснение	Стандартный пользователь вошёл в систему, используя IP-адрес.
Severity	Info

Facility	local0
Стандарт	МЭК 62443-3-3 Reference: n/a (NERC-CIP 007-R5)

Текст сообщения	{Protocol}: {IP address} - No response from the RADIUS server.
Пример	WBM / UDP / TCP / Telnet / SSH / Console / PNIO / PB / OPC: 192.168.1.105 - No response from the RADIUS server.
Пояснение	Нет доступа к серверу или сервер не отвечает.
Severity	Error
Facility	local0
Стандарт	МЭК 62443-3-3 Reference: SR 1.1

Текст сообщения	{Protocol}: {IP address} - No response from the IdP server.
Пример	WBM / UDP / TCP / Telnet / SSH / Console / PNIO / PB / OPC: 192.168.1.105 - No response from the IdP server.
Пояснение	Нет доступа к серверу или сервер не отвечает.
Severity	Error
Facility	local0
Стандарт	МЭК 62443-3-3 Reference: SR 1.1

Управление учетной записью пользователя

Текст сообщения	{Protocol}: Password protection was enabled for resource {Resource}.
Пример	WBM: Password protection was enabled for resource FullReadAccess.
Пояснение	Для этого ресурса активирована защита паролем.
Severity	Notice
Facility	local0
Стандарт	МЭК 62443-3-3 Reference: SR 1.3

Текст сообщения	{Protocol}: Authentication was enabled.
Пример	WBM: Authentication was enabled.
Пояснение	Аутентификация активирована
Severity	Notice
Facility	local0
Стандарт	МЭК 62443-3-3 Reference: SR 1.3

Текст сообщения	{Protocol}: Password protection was disabled for resource {Resource}.
Пример	WBM: Password protection was disabled for resource FullReadAccess.
Пояснение	Защита паролем для этого ресурса деактивирована.
Severity	Notice
Facility	local0
Стандарт	МЭК 62443-3-3 Reference: SR 1.3

Текст сообщения	{Protocol}: Authentication was disabled.
Пример	WBM: Authentication was disabled.
Пояснение	Аутентификация деактивирована
Severity	Notice

Facility	local0
Стандарт	МЭК 62443-3-3 Reference: SR 1.3

Текст сообщения	{protocol}: User {user name} changed own password.
Пример	WBM: User admin changed own password.
Пояснение	Пользователь изменил свой пароль.
Severity	Notice
Facility	local0
Стандарт	МЭК 62443-3-3 Reference: SR1.3

Текст сообщения	{protocol}: User {user name} changed password of user {action user name}.
Пример	Telnet: User admin changed password of user test.
Пояснение	Пользователь изменил пароль другого пользователя.
Severity	Notice
Facility	local0
Стандарт	МЭК 62443-3-3 Reference: SR1.3

Текст сообщения	{Protocol}: User {User name} disabled user-account {Destination user name}.
Пример	WBM / UDP / TCP / Telnet / SSH / Console / PNIO / PB / OPC: User <User name> disabled user-account {Destination user name}.
Пояснение	Авторизованный пользователь блокирует учётную запись другого пользователя.
Severity	Notice
Facility	local0
Стандарт	МЭК 62443-3-3 Reference: SR 2.4

Текст сообщения	{Protocol}: User {User name} enabled user-account {Destination user name}.
Пример	WBM / UDP / TCP / Telnet / SSH / Console / PNIO / PB / OPC: User <User name> enabled user-account {Destination user name}.
Пояснение	Авторизованный пользователь блокирует учётную запись другого пользователя.
Severity	Notice
Facility	local0
Стандарт	МЭК 62443-3-3 Reference: SR 2.4

Текст сообщения	{Protocol}: Default admin account was changed to {User name}.
Пример	WBM / UDP / TCP / Telnet / SSH / Console / PNIO / PB / OPC: Default admin account was changed to maier.
Пояснение	Учётная запись администратора по умолчанию была изменена.
Severity	Notice
Facility	local0
Стандарт	МЭК 62443-3-3 Reference: SR 1.3

Текст сообщения	{Protocol}: Default user account was changed to {User name}.
Пример	WBM / UDP / TCP / Telnet / SSH / Console / PNIO / PB / OPC: Default user account was changed to <new user>.

Пояснение	Учётная запись по умолчанию была изменена.
Severity	Notice
Facility	local0
Стандарт	МЭК 62443-3-3 Reference: SR 1.3

Текст сообщения	{protocol}: User {user name} created user-account {action user name}.
Пример	WBM: User admin created user-account service.
Пояснение	Пользователь создал учётную запись.
Severity	Notice
Facility	local0
Стандарт	МЭК 62443-3-3 Reference: SR1.3

Текст сообщения	{Protocol}: User {User name} changed user-account {Destination user name} with role {Role}.
Пример	WBM / UDP / TCP / Telnet / SSH / Console / PNIO / PB / OPC: User admin changed user-account admin2 with role Administrator.
Пояснение	Администратор изменил существующую учётную запись.
Severity	Notice
Facility	local0
Стандарт	МЭК 62443-3-3 Reference: SR 1.3

Текст сообщения	{protocol}: User {user name} deleted user-account {action user name}.
Пример	WBM: User admin deleted user-account service.
Пояснение	Администратор удалил существующую учётную запись.
Severity	Notice
Facility	local0
Стандарт	МЭК 62443-3-3 Reference: SR1.3

Авторизация

Текст сообщения	{Protocol}: The firewall {Firewall rule} for User {User name} was granted. Timeout is {Timeout} min.
Пример	WBM / UDP / TCP / Telnet / SSH / Console / PNIO / PB / OPC: The firewall Rule 1 for User admin was granted. Timeout is 44 min.
Пояснение	Доступ к критическим ресурсам предоставлен.
Severity	Info
Facility	local0
Стандарт	МЭК 62443-3-3 Reference: не указано (NERC-CIP 005-R2)

Текст сообщения	{Protocol}: The firewall {Firewall rule} for {Trigger pin} was granted. Timeout is {Timeout} min.
Пример	WBM / UDP / TCP / Telnet / SSH / Console / PNIO / PB / OPC: The firewall Rule 1 for DI1 was granted. Timeout is 44 min.
Пояснение	Доступ к критическим ресурсам предоставлен.
Severity	Info
Facility	local0
Стандарт	МЭК 62443-3-3 Reference: не указано (NERC-CIP 005-R2)

Текст сообщения	{Protocol}: The firewall {Firewall rule} for User {User name} was denied.
Пример	WBM / UDP / TCP / Telnet / SSH / Console / PNIO / PB / OPC: The firewall Rule 1 for User admin was denied.
Пояснение	Доступ к важным ресурсам был отклонён.
Severity	Error
Facility	local0
Стандарт	МЭК 62443-3-3 Reference: SR 2.1

Текст сообщения	{Protocol}: The firewall {Firewall rule} for {Trigger pin} was denied.
Пример	WBM / UDP / TCP / Telnet / SSH / Console / PNIO / PB / OPC: The firewall Rule 1 for DI1 was denied.
Пояснение	Доступ к важным ресурсам был отклонён.
Severity	Error
Facility	local0
Стандарт	МЭК 62443-3-3 Reference: SR 2.1

Текст сообщения	{Protocol}: The firewall {Firewall rule} for User {User name} was denied by administrator.
Пример	WBM / UDP / TCP / Telnet / SSH / Console / PNIO / PB / OPC: The firewall Rule 1 for User maier was denied by administrator.
Пояснение	Доступ к важным ресурсам был отклонён.
Severity	Error
Facility	local0
Стандарт	МЭК 62443-3-3 Reference: SR 2.1

Управление идентификаторами

Текст сообщения	{Protocol}: User {User name} created group {Group} and assigned to role {Role}.
Пример	WBM: User admin created group it-service and assigned to role service.
Пояснение	Администратор создал группу и ему была назначена роль.
Severity	Примечание
Facility	local0
Стандарт	МЭК 62443-3-3 Reference: SR 1.4

Текст сообщения	{Protocol}: User {User name} deleted group {Group} and the role {Role} assignment.
Пример	WBM: User maier deleted group it-service and the role service assignment.
Пояснение	Администратор удалил имеющуюся группу и назначенную роль.
Severity	Notice
Facility	local0
Стандарт	МЭК 62443-3-3 Reference: SR 1.4

Текст сообщения	{Protocol}: User {User name} created role {Role}.
Пример	WBM / UDP / TCP / Telnet / SSH / Console / PNIO / PB / OPC: User <User name> created role <Role>.
Пояснение	Роль была создана.
Severity	Notice

Facility	local0
Стандарт	МЭК 62443-3-3 Reference: SR 4.7

Текст сообщения	{Protocol}: User {User name} deleted role {Role}.
Пример	WBM / UDP / TCP / Telnet / SSH / Console / PNIO / PB / OPC: User <User name> deleted role <Role>.
Пояснение	Роль была удалена.
Severity	Notice
Facility	local0
Стандарт	МЭК 62443-3-3 Reference: SR 4.8

Текст сообщения	{Protocol}: User {User name} changed role {Role}.
Пример	WBM / UDP / TCP / Telnet / SSH / Console / PNIO / PB / OPC: User <User name> changed role <Role>.
Пояснение	Роль была изменена.
Severity	Notice
Facility	local0
Стандарт	МЭК 62443-3-3 Reference: SR 4.9

Неудачные попытки авторизации

Текст сообщения	{User name} account is locked for {Time minute} minutes after {Failed login count} unsuccessful login attempts.
Пример	User service account is locked for 44 minutes after 10 unsuccessful login attempts.
Пояснение	При слишком большом количестве неудачных авторизаций в системе соответствующая учётная запись была заблокирована на определённый период времени.
Severity	Warning
Facility	local0
Стандарт	МЭК 62443-3-3 Reference: SR 1.11

{Protocol}: {IP address} is temporarily blocked for {Time second} seconds after {Failed login count} unsuccessful login attempts.

Пример	All: 192.168.1.105 is temporarily blocked for 600 seconds after 11 unsuccessful login attempts.
Пояснение	Функция BFA-предупреждения заблокировала IP-адрес на определённый период после слишком большого количества неудавшихся попыток авторизаций. В примере функция BFA-предупреждения заблокировала IP-адрес «192.168.1.105» после 11 неудавшихся попыток авторизации на 600 секунд.
Severity	Warning
Facility	local0
Стандарт	МЭК 62443-3-3 Reference: SR 1.11

Блокировка сеанса

Текст сообщения	The session of user {user name} was closed after {time} seconds of inactivity.
Пример	The session of user admin was closed after 60 seconds of inactivity.

Пояснение	Текущий сеанс по причине неактивности был заблокирован.
Severity	Warning
Facility	local0
Стандарт	МЭК 62443-3-3 Reference: SR 2.5

Завершение сеанса дистанционного доступа

Текст сообщения	{Protocol}: Remote session {Config detail} was closed after {Time second} seconds of inactivity.
Пример	WBM / UDP / TCP / Telnet / SSH / Console / PNIO / PB / OPC: Remote session OpenVPN was closed after 44 seconds of inactivity.
Пояснение	Удалённый сеанс был завершён после истечения времени неактивности.
Severity	Notice
Facility	local0
Стандарт	МЭК 62443-3-3 Reference: SR 2.6

Доступ через ненадёжные сети

Текст сообщения	{Protocol}: Remote access enabled via {Trigger condition}.
Пример	WBM / UDP / TCP / Telnet / SSH / Console / PNIO / PB / OPC: Remote access enabled via E/A-Pin.
Пояснение	Разрешается дистанционный доступ.
Severity	Info
Facility	local0
Стандарт	МЭК 62443-3-3 Reference: SR 1.13

Текст сообщения	{Protocol}: Remote access disabled via {Trigger condition}.
Пример	WBM / UDP / TCP / Telnet / SSH / Console / PNIO / PB / OPC: Remote access disabled via E/A-Pin.
Пояснение	Дистанционный доступ отклоняется.
Severity	Info
Facility	local0
Стандарт	МЭК 62443-3-3 Reference: SR 1.13

Текст сообщения	{Protocol}: User {User name} logged in from {IP address}.
Пример	WBM / UDP / TCP / Telnet / SSH / Console / PNIO / PB / OPC: User admin logged in from 192.168.1.105.
Пояснение	Пользователь успешно авторизовался на дистанционном устройстве.
Severity	Info
Facility	local0
Стандарт	МЭК 62443-3-3 Reference: SR 1.13

Текст сообщения	{Protocol}: User {User name} failed to login from {IP address}.
Пример	WBM / UDP / TCP / Telnet / SSH / Console / PNIO / PB / OPC: User admin failed to login from 192.168.1.105.
Пояснение	Пользователь не может авторизоваться на дистанционном устройстве.
Severity	Error

Facility	local0
Стандарт	МЭК 62443-3-3 Reference: SR 1.13

Текст сообщения	{Protocol}: User {User name} has logged out.
Пример	WBM / UDP / TCP / Telnet / SSH / Console / PNIO / PB / OPC: User admin has logged out.
Пояснение	Пользователь вышел из системы.
Severity	Info
Facility	local0
Стандарт	МЭК 62443-3-3 Reference: SR 1.13

Текст сообщения	{Protocol}: Connection from {IP address} established.
Пример	WBM / UDP / TCP / Telnet / SSH / Console / PNIO / PB / OPC: Connection from 192.168.1.105 established.
Пояснение	Соединение VPN установлено.
Severity	Info
Facility	local0
Стандарт	МЭК 62443-3-3 Reference: неприменимо (NERC-CIP 005-R1)

Текст сообщения	{Protocol}: Connection from {IP address} closed.
Пример	WBM / UDP / TCP / Telnet / SSH / Console / PNIO / PB / OPC: Connection from 192.168.1.105 closed.
Пояснение	Соединение VPN закрыто.
Severity	Info
Facility	local0
Стандарт	МЭК 62443-3-3 Reference: неприменимо (NERC-CIP 005-R1)

Текст сообщения	{Protocol}: Connection from {IP address} failed. Reason: {Reason}.
Пример	WBM / UDP / TCP / Telnet / SSH / Console / PNIO / PB / OPC: Connection from 192.168.1.105 failed. Reason: unsuccessful authentication.
Пояснение	Соединение VPN не удаётся установить по причине недействительной авторизации.
Severity	Error
Facility	local0
Стандарт	МЭК 62443-3-3 Reference: неприменимо (NERC-CIP 005-R3)

Идентификация и аутентификация устройств

{Protocol}: Device {Src mac} access granted.

Пример	WBM: Device 00:0C:29:2F:09:B3 access granted.
Пояснение	Доступ устройств разрешается вследствие успешной аутентификации порта. В этом примере разрешён доступ устройства с MAC-адресом источника «00:0C:29:2F:09:B3».
Severity	Info
Facility	local0
Стандарт	МЭК 62443-3-3 Reference: SR 1.2

Текст сообщения	{Protocol}: {IP address} access granted.
Пример	WBM / UDP / TCP / Telnet / SSH / Console / PNIO / PB / OPC: 192.168.1.105 access granted.
Пояснение	Доступ разрешён вследствие соответствия правилам брандмауэра или ACL.
Severity	Info
Facility	local0
Стандарт	МЭК 62443-3-3 Reference: SR 1.2

Текст сообщения	{Protocol}: {IP address} access granted.
Пример	WBM / UDP / TCP / Telnet / SSH / Console / PNIO / PB / OPC: 192.168.1.105 access granted.
Пояснение	Доступ разрешён через облачный коннектор.
Severity	Info
Facility	local0
Стандарт	МЭК 62443-3-3 Reference: SR 1.2

{Protocol}: Device {Src mac} access denied.

Пример	WBM: Device 00:0C:29:2F:09:B3 access denied.
Пояснение	Доступ устройств отклонён из-за безуспешной аутентификации порта. В этом примере отклонён доступ устройства с MAC-адресом источника «00:0C:29:2F:09:B3».
Severity	Error
Facility	local0
Стандарт	МЭК 62443-3-3 Reference: SR 1.2

Текст сообщения	{Protocol}: {IP address} access blocked.
Пример	WBM / UDP / TCP / Telnet / SSH / Console / PNIO / PB / OPC: 192.168.1.105 access blocked.
Пояснение	Доступ заблокирован из-за правил брандмауэра или списка управления доступом.
Severity	Error
Facility	local0
Стандарт	МЭК 62443-3-3 Reference: SR 1.2

Текст сообщения	{Protocol}: {IP address} access blocked.
Пример	WBM / UDP / TCP / Telnet / SSH / Console / PNIO / PB / OPC: 192.168.1.105 access blocked.
Пояснение	Доступ заблокирован через облачный коннектор.
Severity	Error
Facility	local0
Стандарт	МЭК 62443-3-3 Reference: SR 1.2

{Protocol}: Connection from device {IP address} subject {Subject} successfully established.

Пример	WBM: Connection from device 192.168.1.105 subject (Peter Maier) successfully established.
Пояснение	Аутентификация устройств была успешной. В примере было успешно установлено соединение устройства с IP-адресом «192.168.1.105» с устройством SINEC OS.
Severity	Info
Facility	local0
Стандарт	МЭК 62443-3-3 Reference: SR 1.2

{Protocol}: Connection from device {IP address} subject {Subject} failed.

Пример	WBM: Connection from device 192.168.1.105 subject (Peter Maier) failed.
Пояснение	Аутентификация устройств не удалась. В примере не удалось установить соединение устройства с IP-адресом «192.168.1.105» с устройством SINEC OS.
Severity	Error
Facility	local0
Стандарт	МЭК 62443-3-3 Reference: SR 1.2

Ограничение количества одновременных сеансов

Текст сообщения	{Protocol}: The maximum number of {Max sessions} concurrent login session exceeded.
Пример	WBM / UDP / TCP / Telnet / SSH / Console / PNIO / PB / OPC: The maximum number of 10 concurrent login sessions exceeded.
Пояснение	Превышено максимальное количество одновременных сеансов.
Severity	Warning
Facility	local0
Стандарт	МЭК 62443-3-3 Reference: SR 2.7

Защита контрольной информации

{Protocol}: User {User name} has cleared the logging buffer.

Пример	SSH: User admin has cleared the logging buffer.
Пояснение	Пользователь удалил журнал регистрации. В примере пользователь «admin» удалил локальный журнал регистрации.
Severity	Notice
Facility	local0
Стандарт	МЭК 62443-3-3 Reference: SR 3.9

Неподдельность**{Protocol}: User {User name} has changed the configuration.**

Пример	SSH: User admin has changed the configuration.
Пояснение	Пользователь изменил конфигурацию. В примере пользователь «admin» изменил конфигурацию.
Severity	Info
Facility	local0
Стандарт	МЭК 62443-3-3 Reference: SR 2.12

Текст сообщения	{Protocol}: User {User name} has deactivated {Config detail} configuration.
Пример	WBM / UDP / TCP / Telnet / SSH / Console / PNIO / PB / OPC: User admin has deactivated OpenVPN configuration.
Пояснение	Пользователь деактивировал определённые данные конфигурации.
Severity	Info
Facility	local0
Стандарт	МЭК 62443-3-3 Reference: SR 2.12

{Protocol}: User {User name} has initiated a reset to factory defaults.

Пример	SSH: User admin has initiated a reset to factory defaults.
Пояснение	Пользователь инициировал сброс настроек по умолчанию. В примере пользователь «admin» инициировал сброс настроек по умолчанию.
Severity	Info
Facility	local0
Стандарт	МЭК 62443-3-3 Reference: SR 2.12

Текст сообщения	Device configuration changed.
Пример	Device configuration changed.
Пояснение	Конфигурация устройства изменена на длительный период.
Severity	Info
Facility	local0
Стандарт	МЭК 62443-3-3 Reference: SR2.12

Целостность связи**{Protocol}: Integrity verification failed.**

Пример	Console: Integrity verification failed.
Пояснение	При проверке целостности связи сообщения была обнаружена ошибка целостности. Возможна связь только на основе сертификата.
Severity	Error
Facility	local0
Стандарт	МЭК 62443-3-3 Reference: SR 3.1

Целостность программного обеспечения и информации**Firmware integrity verification failed. Backup firmware started.**

Пример	Firmware integrity verification failed. Backup firmware started.
Пояснение	При проверке целостности прошивки была обнаружена ошибка целостности. Была загружена резервная прошивка.
Severity	Error
Facility	local0
Стандарт	МЭК 62443-3-3 Reference: SR 3.4

Текст сообщения	{Protocol}: Software integrity verification failed.
Пример	WBM: Software integrity verification failed.
Пояснение	При проверке целостности программного обеспечения была обнаружена ошибка целостности.
Severity	Error
Facility	local0
Стандарт	МЭК 62443-3-3 Reference: SR 3.4

Текст сообщения	Integrity violations in configuration data detected
Пример	Integrity violations in configuration data detected
Пояснение	При проверке целостности конфигурации была обнаружена ошибка целостности.
Severity	Error
Facility	local0
Стандарт	МЭК 62443-3-3 Reference: SR 3.4

Целостность сеанса**{Protocol}: Session ID verification failed.**

Пример	WBM: Session ID verification failed.
Пояснение	Идентификатор сеанса недействителен.
Severity	Error
Facility	local0
Стандарт	МЭК 62443-3-3 Reference: SR 3.8

Защита от DoS-событий**{Protocol}: Denial-of-Service (DoS) attack detected.**

Пример	Console: Denial-of-Service (DoS) attack detected.
Пояснение	Была распознана DoS-атака.
Severity	Alert
Facility	local0
Стандарт	МЭК 62443-3-3 Reference: SR 3.8

Резервное копирование данных в автоматизированных системах (резервное копирование)

Текст сообщения	{Protocol}: User {User name} created backup file.
Пример	WBM / UDP / TCP / Telnet / SSH / Console / PNIO / PB / OPC: User maier created backup file.
Пояснение	Пользователь создал резервную копию файла.
Severity	Notice
Facility	local0
Стандарт	МЭК 62443-3-3 Reference: SR 7.3

Текст сообщения	{Protocol}: User {User name} failed to create backup file.
Пример	WBM / UDP / TCP / Telnet / SSH / Console / PNIO / PB / OPC: User <user name> failed to create backup file.
Пояснение	Создание резервной копии файла пользователем не удалось.
Severity	Error
Facility	local0
Стандарт	МЭК 62443-3-3 Reference: SR 7.3

Восстановление автоматизированной системы

Текст сообщения	{Protocol}: User {User name} failed to apply backup file.
Пример	WBM / UDP / TCP / Telnet / SSH / Console / PNIO / PB / OPC: User <user name> failed to apply backup file.
Пояснение	Использование резервной копии файла пользователем не удалось.
Severity	Error
Facility	local0
Стандарт	МЭК 62443-3-3 Reference: SR 7.4

Текст сообщения	{protocol}: User {user name} loaded file type ConfigPack (restart required).
Пример	WBM: User admin loaded file type ConfigPack (restart required).
Пояснение	Конфигурация применяется.
Severity	Notice
Facility	local0
Стандарт	МЭК 62443-3-3 Reference: SR7.4

Текст сообщения	{protocol}: Failed to load file type Firmware.
Пример	WBM: Failed to load file type Firmware.
Пояснение	Выгрузка прошивки не удалась.
Severity	Warning
Facility	local0
Стандарт	МЭК 62443-3-3 Reference: SR7.4

Текст сообщения	{protocol}: Loaded file type Firmware {version} (restart required).
Пример	TFTP: Loaded file type Firmware V02.00.00 (restart required).
Пояснение	Прошивка успешно загружена.
Severity	Notice

Facility	local0
Стандарт	МЭК 62443-3-3 Reference: SR7.4

Текст сообщения	{protocol}: User {user name} loaded file type Firmware {version} (restart required).
Пример	WBM: User admin loaded file type Firmware V02.00.00 (restart required).
Пояснение	Пользователь успешно загрузил прошивку.
Severity	Notice
Facility	local0
Стандарт	МЭК 62443-3-3 Reference: SR7.4

Текст сообщения	{Protocol}: Software {Version} was activated.
Пример	WBM: Software V02.00.00 was activated.
Пояснение	Программное обеспечение успешно активировано.
Severity	Notice
Facility	local0
Стандарт	МЭК 62443-3-3 Reference: SR 7.4

Текст сообщения	{Protocol}: User {User name} activated the Software {Version}.
Пример	WBM: User <User name> activated the Software V02.00.00.
Пояснение	Пользователь успешно активировал ПО.
Severity	Notice
Facility	local0
Стандарт	МЭК 62443-3-3 Reference: SR 7.4

Текст сообщения	{Protocol}: Software activation failed.
Пример	WBM: Software activation failed.
Пояснение	Активация программного обеспечения не удалась.
Severity	Error
Facility	local0
Стандарт	МЭК 62443-3-3 Reference: SR 7.4

Текст сообщения	{Protocol}: User {User name} failed to activate Software {Version}.
Пример	WBM: User <User name> failed to activate Software V02.00.00.
Пояснение	Активация программного обеспечения пользователем не удалась.
Severity	Error
Facility	local0
Стандарт	МЭК 62443-3-3 Reference: SR 7.4

Указатель

1

1588, 371

A

ACL (список управления доступом), 357, 415

Aging Time, 363

ARP Keep Alive

Interval, 156

активировать/деактивировать, 155

B

BFP (защита от перебора паролей), 418

Broadcast, 369

Brute Force Prevention, 418

C

Class of Service, 282

Command Line Interface (CLI), 423

Configuration Mode, 156

CoS, 282

Очередь, 282

CoS (Class of Service), 83

CRC, 128

D

DCP Discovery, 264

DCP Forwarding, 347

DCP-сервер, 154, 347

DHCP

Client, 189

Host Options, 205

Relay Agent, 202

Сервер, 191

DNA, 74

DSCP, 283

DST

Летнее время, 221, 222

Dual Network Access (двойной сетевой доступ), 74

E

EtherNet/IP, 257

Ring Port Status, 258

Supervisor, 258

Порты DLR, 257

Статус DLR, 258

F

Fault Monitoring

Link Change, 253

Power Supply, 252

Redundancy, 254

G

GMRP, 366

Groups, 400

GVRP, 296

H

HRP, 318

HTTP

Загрузка/сохранение, 166

Порт, 153

Сервер, 153

HTTPS

Сервер, 153

I

IGMP, 363

L

LACP, 343

Layer 2, 276

Link Check, 121

Link Check Status, 121

LLDP, 133, 349

Local Users, 396

Loop Detection, 340

М

Management ACL, 415
Mirroring, 87
 Основное, 305
 Порт, 308
MRP Interconnection, 122, 324
 Принцип работы, 59
 Проектирование, 61
 Топология, 58
MSTP, 328, 336
 Параметр порта, 338
 Порт, 331
Multicast, 360

Н

NAPT
 конфигурировать, 392
NAT
 конфигурировать, 388, 390, 391
NAT Translations, 138
Negotiation, 241
NTP, 360
 Client, 229

Р

Packet Error
 Collisions, 128
 CRC, 128
 Fragments, 128
 Jabbers, 128
 Oversize, 128
 Undersize, 128
PoE, 266, 267
 Порт, 267
 Расписание, 270
Port Configuration, 243
Port Overview, 239
Power over Ethernet, 266
 Порт, 267
 Расписание, 270
PROFINET, 37, 255
PROFINET IO, 37
PTR, 371, 372
 Общая информация, 371
 Порт, 372
 Прозрачные часы, 371

Q

QoS (качество обслуживания), 285

R

RADIUS, 406
RMON
 История, 376
 Статистика, 374
Roles, 399
Routing
 Routing Table, 137
RSTP, 328
RSTP+
 Конфигурация, 44
 Свойства, 41
 Топология, 41

S

SFTP
 Загрузка/сохранение, 174
SINEC PNI, 347
SMTP
 Client, 154
SNMP, 88, 155, 207, 213
 SNMPv1, 88
 SNMPv2c, 88
 SNMPv3, 88
 Trap, 217
 Группы, 212
 Обзор, 143
SNMPv3
 Виды, 215
 Группы, 212
 Доступ, 213
 Пользователь, 210
 Уведомления, 217
Spanning Tree, 328
 Enhanced Passive Listening Compatibility, 340
 MSTP, 328
 Rapid Spanning Tree (высокоскоростное
 связующее дерево), 40
 RSTP, 328
 Информация, 113
SSH
 Порт, 152
 Сервер, 152
Standby, 318

STEP 7, 347
 STP, 328
 Syslog, 237
 Client, 154
 System Time, 219

Т

Telnet
 Порт, 152
 Сервер, 152
 TFTP
 Загрузка/сохранение, 170
 Time Method, 154

V

VLAN, 81
 Port VID (VLAN-идентификатор порта), 298
 VLAN ID, 84
 День, 298
 Конфигурация, 290
 Приоритет, 298
 Tag VLAN, 82

W

Web Based Management, 95
 Требование, 95
 Web Based Management (WBM), 423

A

авторизация
 через HTTP, 97
 через HTTPS, 97
 Алгоритм SHA, 213
 Артикул, 108
 Аутентификация, 210, 411

B

Версия аппаратного обеспечения, 108
 Версия программного обеспечения, 108
 Время
 NTP (Network Time Protocol), 229
 Precision Time Protocol, 234
 PTP-клиент, 234
 SIMATIC Time Client, 232
 SNTP (Simple Network Time Protocol), 225

Время UTC, 228, 230, 231
 ручная настройка, 219
 Синхронизация времени, 225, 229
 Системное время, 219
 Часовой пояс, 228, 231
 Время ожидания LACP, 346
 Время приветствия (Hello Time), 330
 Время сброса BFP, 418
 Время старения
 Dynamic MAC Aging, 309
 Вход, 418
 Выход из системы
 автоматически, 235

Г

географические координаты, 158
 Глоссарий, 12
 Глоссарий SIMATIC NET, 12
 Группы пользователей, 400
 Группы портов, 314

Д

Данные технического обслуживания, 108
 Диагностика SFP, 273
 Диагностика портов
 Диагностика SFP, 273
 Тест кабеля, 272
 Доступные системные функции, 17

З

Задержка пересылки, 330

И

Интервал срабатывания BFP, 418
 Информация
 802.1X Port Status, 149
 LLDP, 133
 MAC-Auth. Address Table, 150
 Security, 144, 147
 SNMP, 143
 Spanning Tree, 113
 Версии, 106
 Группы, 149
 Кольцевое резервирование, 117, 119
 Роль, 148
 Стартовая страница, 100

Таблица ARP, 109
Таблица журнала, 110

К

Кнопка, 236
Кнопка RESET, 236, 423
Кнопка SELECT/SET, 236, 423
Кнопка SET, 423
Код производителя, 108
Количественная структура, 21
Кольцевое резервирование, 311
 HRP, 278, 312
 MRP, 278, 312
 Standby, 318
 Кольцевые порты, 313
Контроль доступа, 355, 357
 автоматическое обучение, 357
Контроль скорости передачи, 288
Конфигурация порта, 251

М

Максимальное время жизни корневого моста (Root Max Age), 331
Максимальное время жизни моста (Bridge Max Age), 331
Максимальное число переходов моста (Bridge Max Hop Count), 331
Маска подсети, 33
Место монтажа, 158
Множественное связующее дерево, 331, 336
Модуль C-PLUG, 260
 Сохранение конфигурации, 262
 Форматирование, 262
Модуль PLUG, 260
 Модуль C-PLUG, (Модуль C-PLUG)
Мост, 330
 Корневой мост, 330
 Приоритет моста, 330

Н

Настройки безопасности, 213

О

Область применения, 9
Обнаружение петель, 340
Определение приоритета CoS, 83

П

Пароль, 402
 Опции, 405
Петля, 340
Повторный пуск, 162
Подсети
 Конфигурация (IPv4), 381
 Обзор (IPv4), 378
 Шлюз по умолчанию, 382
Порт
 Link Check, 121
 Конфигурация порта, 251
Приоритет, 285, 331
Проверка связи, 263
Производитель, 108
Протокол системных событий
 Агент, 237

Р

Режим Trust:, 285
Режим резервирования
 HRP, 47
Резервирование, 311, 318
Резервирование DNA, 76
Резервирование Standby, 70
Резервирование двойного сетевого доступа, 76
резервные сети, 329
Руководство SIMATIC NET, 12

С

Сброс, 162
Серийный номер, 108
Система
 General Information, 157
 Конфигурация, 151
Системное руководство, 11
Системные события
 Severity Filter, 183
 Конфигурация, 179
События
 Таблица журнала, 110
Состояние ошибки, 112
Стандарт IEEE 1588, 371
Стартовая страница, 100
Статистика ошибок пакетов, 127
Статистка Ethernet
 Frame Type, 126

History, 129
Interface Statistics, 124
Packet Error, 127
Packet Size, 125

Т

Таблица протокола событий, 110
Тест кабеля, 272
Тип носителя комбинированного порта, 240, 248
Тип ошибки
 Collisions, 128
 CRC, 128
 Fragments, 128
 Jabbers, 128
 Oversize, 128
 Undersize, 128

У

Узел–узел, 40
управление приоритетом, 285

Ф

Фильтр
 Конфигурация фильтра, 354

Э

Экземпляр MSTP, 338

