

OSNOVO

cable transmission

РУКОВОДСТВО ПО НАСТРОЙКЕ

**Управление коммутатором с
помощью WEB интерфейса**

www.osnovo.ru



Оглавление

1. ВВЕДЕНИЕ	8
2. СОСТОЯНИЕ СИСТЕМЫ (STATUS)	9
2.1. Системная информация (System Information)	9
2.2. Журнал сообщений (Logging Message)	12
2.3. Статус портов (Port)	13
2.3.1. Статистика информации на портах (Statistics)	13
2.3.2. Таблица ошибок на портах (Error Disabled)	16
2.3.3. Использование полосы пропускания (Bandwidth Utilization)	18
2.4. Статистика агрегации каналов (Link Aggregation)	19
2.5. Информация в таблице MAC-адресов (MAC Address Table)	20
3. НАСТРОЙКИ СЕТИ (NETWORK)	22
3.1. Настройка DNS (DNS Configuration)	22
3.2. Настройка DNS-хостов (DNS Host Configuration)	24
3.3. Настройки системного времени (System Time)	26
4. ПОРТЫ (PORT)	28
4.1. Настройки портов коммутатора (Port Setting)	28
4.2. Отключение портов по ошибкам (Error Disabled)	32
4.3. Агрегация каналов (Link Aggregation)	34
4.3.1. Настройка групп (Group)	34
4.3.2. Настройки портов агрегации (Port Setting)	37
4.3.3. Настройки протокола LACP (LACP)	40
4.4. Настройки Energy Efficient Ethernet, IEEE 802.3az (EEE)	43
4.5. Настройка Jumbo Frame (Jumbo Frame)	45
5. VLAN	46
5.1. Настройки VLAN (VLAN)	46
5.1.1. Создание VLAN (Create VLAN)	47
5.1.2. Конфигурация VLAN (VLAN Configuration)	49
5.1.3. Настройка VLAN Membership (Membership)	51
5.1.4. Настройка портов VLAN (Port Setting)	54
5.2. Голосовая VLAN (Voice VLAN)	57
5.2.1. Свойства Voice VLAN (Property)	57
5.2.2. Голосовые OUI адреса (Voice OUI)	60
5.3. VLAN на основе протоколов (Protocol VLAN)	62
5.3.1. Группы протоколов VLAN (Protocol Group)	62

5.3.2. Привязка групп протоколов (Group Binding)	64
5.4. MAC VLAN	66
5.4.1. Настройка групп MAC-адресов (MAC Group)	66
5.4.2. Привязка групп MAC адресов (Group Binding).....	68
5.5. VLAN для видеонаблюдения (Surveillance VLAN)	71
5.5.1. Свойства (Property)	71
5.5.2. Настройка OUI адресов для видеонаблюдения (Surveillance OUI).....	74
5.6. GVRP (GARP VLAN Registration Protocol).....	76
5.6.1. Свойства (Property)	76
5.6.2. Настройка VLAN Membership (Membership)	79
5.6.3. Статистика GVRP (Statistics)	80
6. ТАБЛИЦА MAC-АДРЕСОВ (MAC ADDRESS TABLE)	83
6.1. Динамические адреса (Dynamic Address)	83
6.2. Статические MAC-адреса (Static Address)	84
6.3. Фильтрация MAC-адресов (Filtering Address).....	85
7. STP (SPANNING TREE PROTOCOL)	86
7.1. Свойства STP (Property)	87
7.2. Настройка портов STP (Port Setting).....	90
7.3. Настройка MST Instance (MST Instance)	93
7.4. Настройка портов MST (MST Port Setting).....	96
7.5. Статистика STP (Statistics)	99
8. ERPS (ETHERNET RING PROTECTION SWITCHING)	101
8.1. Общие настройки ERPS (Property)	102
8.2. Настройка ERPS Instance (ERPS Instance)	103
9. ОБНАРУЖЕНИЕ УСТРОЙСТВ (DISCOVERY).....	104
9.1. Протокол LLDP (Link Layer Discovery Protocol)	104
9.1.1. Свойства LLDP (Property)	104
9.1.2. Настройка портов LLDP (Port Setting).....	106
9.1.3. Политика сети LLDP-MED (MED Network Policy).....	109
9.1.4. Настройка портов LLDP-MED (MED Port Setting)	111
9.1.5. Просмотр пакетов LLDP (Packet View).....	113
9.1.6. Локальная информация (Local Information)	116
9.1.7. Соседние устройства (Neighbor)	119
9.1.8. Статистика LLDP (Statistics)	121
10. DHCP (DYNAMIC HOST CONFIGURATION PROTOCOL)	123

10.1. Настройка протокола DHCP (DHCP Property)	125
10.2. Настройка пула IP адресов DHCP (Address Pool Configuration).....	127
10.3. Настройка групп адресов VLAN-интерфейсов (VLAN IF Address Group Setting).....	129
10.4. Список клиентов DHCP (Client List)	131
10.5. Таблица статической привязки клиентов DHCP (Client Static Binding Table)	132
11. НАСТРОЙКА MULTICAST (IGMP, MLD, STATIC)	134
11.1. Общие настройки (General)	134
11.1.1. Свойства Multicast (Property)	134
11.1.2. Группы Multicast (Group Address)	136
11.1.3. Настройка Router портов (Router Port).....	138
11.1.4. Принудительная пересылка Multicast трафика (Forward All)	141
11.1.5. Ограничение на кол-во Multicast групп (Throttling)	144
11.1.6. Фильтрация Multicast групп (Filtering Profile).....	146
11.1.7. Привязка профилей фильтрации к портам (Filtering Binding).....	149
11.2. Настройка функции IGMP Snooping (IGMP Snooping).....	151
11.2.1. Свойства IGMP Snooping (Property)	151
11.2.2. Генератор запросов IGMP (Querier).....	155
11.2.3. Статистика IGMP Snooping (Statistics)	157
11.3. Настройка функции MLD Snooping (MLD Snooping).....	160
11.3.1. Свойства MLD Snooping (Property).....	160
11.3.2. Статистика MLD Snooping (Statistics).....	165
11.4. Настройка MVR (Multicast VLAN Registration).....	168
11.4.1. Свойства MVR (Property)	168
11.4.2. Настройка портов (Port Setting).....	170
11.4.3. Групповые адреса (Group Address).....	173
12. МАРШРУТИЗАЦИЯ (ROUTING)	177
12.1. Настройка IPv4 интерфейсов и маршрутизации (IPv4 Management and Interfaces).....	177
12.1.1. Настройка IPv4 интерфейсов в коммутаторе (IPv4 Interface).....	177
12.1.2. Маршрутизация IPv4 (IPv4 Routing)	179
12.1.3. ARP-таблица (ARP).....	180
12.2. Настройка IPv6 интерфейсов и маршрутизации (IPv6 Management Interface)	181

12.2.1. Настройка IPv6 интерфейсов в коммутаторе (IPv6 Interface).....	181
12.2.2. Таблица адресов IPv6 (IPv6 Address)	182
12.2.3. Маршрутизация IPv6 (IPv6 Routing)	182
12.2.4. Настройка IPv6 Neighbors (IPv6 Neighbors)	183
12.3. Управление маршрутизацией по протоколу RIP (RIP Routes Management)	185
12.4. Управление маршрутизацией по протоколу OSPF (OSPF Routes Management)	186
13. БЕЗОПАСНОСТЬ (SECURITY)	187
13.1. Настройки протокола RADIUS (RADIUS)	187
13.2. Настройки протокола TACACS+ (TACACS+).....	192
13.3. AAA (Аутентификация, Авторизация и Учет пользователей)	196
13.3.1. Списки методов AAA (Method List)	196
13.3.2. Аутентификация входа (Login Authentication).....	201
13.4. Управление доступом к коммутатору (Management Access).....	203
13.4.1. VLAN управления (Management VLAN)	203
13.4.2. Настройка способов и сервисов управления коммутатором (Management Service)	205
13.4.3. ACL для управления коммутатором (Management ACL)	208
13.4.4. Правила ACE для управления коммутатором (Management ACE)	210
13.5. Менеджер аутентификации (Authentication Manager)	215
13.5.1. Свойства Authentication Manager (Property).....	215
13.5.2. Настройки портов для аутентификации (Port Setting).....	222
13.5.3. Локальные учетные записи MAC-Based (MAC-Based Local Account).....	227
13.5.4. Локальные учетные записи WEB-аутентификации (WEB-Based Local Account)	232
13.5.5. Просмотр сессий аутентификации (Sessions).....	236
13.6. Защита портов (Port Security)	239
13.7. Настройка изоляции портов (Protected Port)	241
13.8. Настройка функции Storm Control (Storm Control).....	245
13.9. Защита от DoS-атак (Denial of Service)	248
13.9.1. Глобальные настройки функции DOS (Property).....	248
13.9.2. Настройки портов (Port Setting)	252
13.10. Dynamic ARP Inspection (DAI).....	254
13.10.1. Глобальные настройки DAI (Property).....	254
13.10.2. Статистика работы DAI (Statistics)	259

13.11. DHCP Snooping	262
13.11.1. Глобальные настройки (Property).....	262
13.11.2. Статистика работы DHCP Snooping (Statistics)	265
13.11.3. Настройка Option 82 (Option82 Property).....	267
13.11.4. Настройка Circuit ID в Option 82 (Option 82 Circuit ID)	271
13.12. IP Source Guard	273
13.12.1. Настройка портов (Port Setting).....	273
13.12.2. Таблица привязок IP/MAC адресов (IMPV Binding).....	276
13.12.3. Сохранение базы данных (Save Database)	279
14. ACL (ACCESS CONTROL LIST)	281
14.1. MAC ACL (ACL на основе MAC-адресов)	281
14.2. MAC ACE (Правила ACL для MAC-адресов)	283
14.3. IPv4 ACL (Access Control List для IPv4)	288
14.4. IPv4 ACE (Правила ACL для IPv4)	290
14.5. IPv6 ACL (Access Control List для IPv6)	296
14.6. IPv6 ACE (Правила ACL для IPv6)	298
14.7. Привязка ACL (ACL Binding)	306
15. НАСТРОЙКА QOS (QOS)	309
15.1. Общие настройки QoS (General)	309
15.1.1. Основные параметры QoS (Property)	309
15.1.2. Планирование очередей (Queue Scheduling)	314
15.1.3. Сопоставление CoS (CoS Mapping)	317
15.1.4. Сопоставление DSCP (DSCP Mapping)	319
15.1.5. Сопоставление IP Precedence (IP Precedence Mapping)	322
15.2. Ограничение скорости (Rate Limit)	325
15.2.1. Входящий/Исходящий порт (Ingress/Egress Port).....	325
15.2.2. Ограничение скорости для исходящих очередей (Egress Queue)	328
16. ИНСТРУМЕНТЫ ДИАГНОСТИКИ (DIAGNOSTICS)	334
16.1. Ведение журналов событий (Logging)	334
16.1.1. Основные параметры (Property)	334
16.1.2. Удаленный сервер для отправки логов (Remote Server)	338
16.2. Зеркалирование портов (Mirroring)	340
16.3. Инструмент проверки связи (Ping)	342
16.4. Трассировка маршрута (Traceroute)	344
16.5. Тестирование медных кабелей (Copper Test)	346

16.6. Инструмент диагностики SFP модулей (Fiber Module)	348
16.7. Обнаружение однонаправленных соединений UDLD (UniDirectional Link Detection)	351
16.7.1. Свойства (Property)	351
16.7.2. Соседние устройства (Neighbor)	354
17. ПАРАМЕТРЫ УПРАВЛЕНИЯ КОММУТАТОРОМ (MANAGEMENT)	357
17.1. Учетные записи пользователей (User Account)	357
17.2. Управление прошивкой коммутатора (Firmware)	360
17.2.1. Обновление/Резервное копирование (Upgrade/Backup)	360
17.2.2. Активный образ прошивки (Active Image)	365
17.3. Конфигурация (Configuration)	368
17.3.1. Обновление/Резервное копирование конфигурации (Upgrade/Backup)	368
17.3.2. Сохранение конфигурации (Save Configuration)	374
17.4. Настройка SNMP (SNMP)	377
17.4.1. SNMP View (View)	377
17.4.2. Группы SNMP (Group)	379
17.4.3. Настройка SNMP community (Community)	384
17.4.4. Пользователи SNMP (User)	388
17.4.5. Идентификатор Engine (Engine ID)	394
17.4.6. Настройка SNMP Trap Event (Trap Event)	398
17.4.7. Уведомления SNMP (Notification)	400
17.5. Настройка RMON (Remote Monitoring)	406
17.5.1. Статистика RMON (Statistics)	406
17.5.2. История RMON (History)	410
17.5.3. События RMON (Event)	417
17.5.4. Тревожные сообщения RMON (Alarm)	422

1. Введение

В этом руководстве описано использование WEB-интерфейса управления (Web UI) для настройки параметров управляемых коммутаторов данной серии.

Поддерживаемые браузеры

Веб-интерфейс совместим со следующими браузерами:

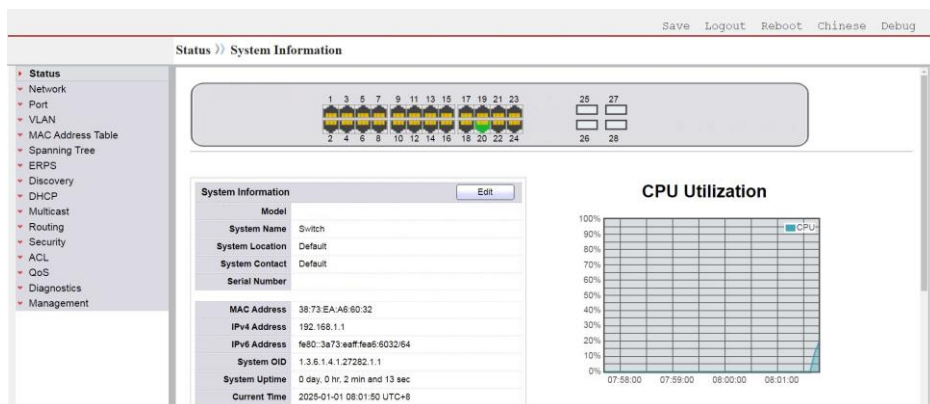
- Internet Explorer 8 и выше
- Firefox 20.0 и выше
- Chrome 23.0 и выше
- Safari 5.1.7 и выше

Интерфейс пользователя

- **Левая панель** содержит меню настроек.
- **Верхняя строка** отображает текущее состояние портов:
 - Зеленые индикаторы - порт активен (link up)
 - Черные индикаторы - порт неактивен (link down)
- **Панель инструментов** (расположена ниже изображения коммутатора) предоставляет быстрый доступ к часто используемым функциям.
- **Основная рабочая область** отображает параметры конфигурации.

Внимание!

Количество основных портов и SFP портов, описываемое в данном руководстве, может отличаться.



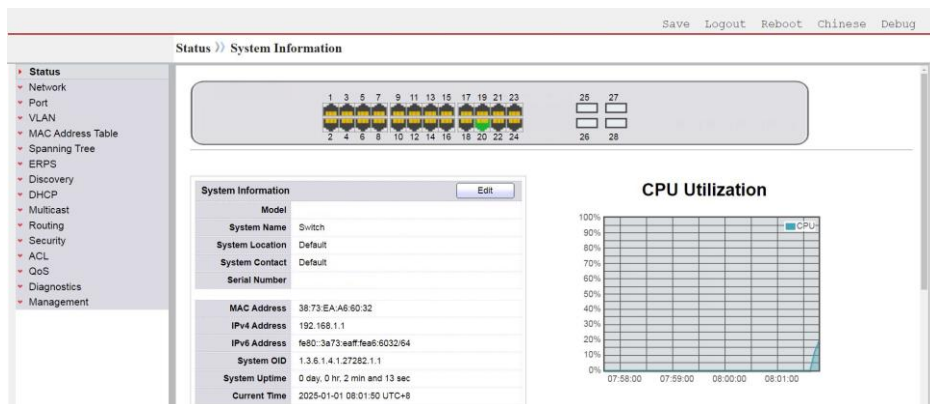
2. Состояние системы (Status)

Раздел «Состояние системы (Status)» отображает системную информацию и текущий статус работы устройства.

2.1. Системная информация (System Information)

Чтобы открыть страницу с системной информацией (System Information):

Перейдите в раздел «Status» → «System Information».



На этой странице отображается:

- Графическое представление панели коммутатора (Switch panel)
- Загрузка ЦП (CPU utilization)
- Использование памяти (Memory utilization)
- Другие текущие системные параметры

Дополнительные возможности:

Страница позволяет редактировать некоторые системные параметры (system information).

Параметр	Описание
Model	Название модели коммутатора
System Name	Системное имя коммутатора. Также используется как префикс в CLI (например, "Switch>" или "Switch#")
System Location	Информация о физическом расположении коммутатора
System Contact	Контактная информация, связанная с коммутатором
MAC Address	Базовый MAC-адрес коммутатора
IPv4 Address	Текущий IPv4-адрес системы
IPv6 Address	Текущий IPv6-адрес системы
System OID	Идентификатор объекта системы для SNMP
System Uptime	Общее время работы с момента последней загрузки
Current Time	Текущее системное время
Loader Version	Версия загрузочного образа
Loader Date	Дата сборки загрузочного образа
Firmware Version	Версия текущей прошивки
Firmware Date	Дата сборки текущей прошивки
Telnet	Текущее состояние сервиса Telnet (включен/выключен)
SSH	Текущее состояние сервиса SSH (включен/выключен)
HTTP	Текущее состояние сервиса HTTP (включен/выключен)
HTTPS	Текущее состояние сервиса HTTPS (включен/выключен)
SNMP	Текущее состояние сервиса SNMP (включен/выключен)

Для изменения системных параметров нажмите кнопку **Edit (изменить)** в заголовке таблицы.

Status >> System Information

Edit System Information

System Name

Switch

System Location

Default

System Contact

Default

Apply

Close

Параметр	Описание
System Name	Название системы коммутатора. Используется как префикс в командной строке (CLI) для каждой строки ("Switch>" или "Switch#")
System Location	Физическое местоположение коммутатора (здание, этаж, помещение и т.д.)
System Contact	Контактная информация ответственного лица или отдела (телефон, email и т.п.)

Примечания:

1. Для редактирования необходимо иметь соответствующие права доступа администратора
2. Изменения вступают в силу немедленно после сохранения
3. Имя системы (System Name) не должно содержать специальных символов и пробелов
4. Рекомендуется указывать актуальную контактную информацию для оперативного решения проблем

2.2. Журнал сообщений (Logging Message)

Для просмотра журнальных сообщений, хранящихся в RAM и Flash памяти:

Перейдите в раздел **Status > Logging Message**.

Status >> Logging Message

Logging Message Table

Viewing RAM

Showing All entries

Showing 1 to 3 of 3 entries

Log ID	Time	Severity	Description
1	Jan 01 2020 08:01:12	notice	AAA-0-CONNECT: New http connection for user admin, source 192.168.1.100 ACCEPTED
2	Jan 01 2020 08:00:07	notice	PORT-5-LINK_UP: Interface GigabitEthernet8 link up
3	Jan 01 2020 00:00:05	notice	SYSTEM-5-COLDSTART: Cold startup

Clear Refresh

First Previous 1 Next Last

Поля журнала сообщений

Параметр	Описание
Log ID	Идентификатор записи журнала
Time	Временная метка сообщения
Severity	Уровень важности сообщения (критическое, предупреждение, информационное и т.д.)
Description	Текстовое описание события

Управление журналом

Параметр	Описание
Viewing	Режим просмотра журнала:
	RAM – отображает сообщения, хранящиеся в оперативной памяти
	Flash – отображает сообщения, сохранённые в энергонезависимой памяти

Параметр	Описание
Clear	Очистка всех записей журнала
Refresh	Обновление списка

Примечания:

1. Сообщения в RAM памяти теряются при перезагрузке устройства
2. Сообщения в Flash памяти сохраняются после перезагрузки
3. Уровень важности (Severity) помогает фильтровать критически важные события
4. Для сохранения журнала рекомендуется периодически экспортировать данные

2.3. Статус портов (Port)

Страница конфигурации портов отображает сводную информацию и статус портов.

2.3.1. Статистика информации на портах (Statistics)

Чтобы открыть страницу счётчиков портов:

Перейдите в раздел **Status > Port > Statistics**.

На этой странице отображаются:

- Стандартные счётчики сетевого трафика из MIB:
 - **Interfaces** (Интерфейсы)
 - **Ethernet-like** (Ethernet-статистика)
 - **RMON** (Удалённый мониторинг)
- Счётчики **Interfaces** и **Ethernet-like** отображают ошибки в трафике каждого порта.
- Счётчики **RMON** показывают общее количество переданных кадров разных типов и размеров.

Кнопка **Clear (Очистить)** – сбрасывает счётчики выбранного порта.

Port	GE1 ▾
MIB Counter	☒ All ☐ Interface ☐ Etherlike ☐ RMON
Refresh Rate	☐ None ☐ 5 sec ☒ 10 sec ☐ 30 sec

Clear

Interface

ifInOctets	0
ifInUcastPkts	0
ifInNUcastPkts	0
ifInDiscards	0
ifOutOctets	0
ifOutUcastPkts	0
ifOutNUcastPkts	0
ifOutDiscards	0
ifInMulticastPkts	0
ifInBroadcastPkts	0
ifOutMulticastPkts	0
ifOutBroadcastPkts	0

Etherlike

dot3StatsAlignmentErrors	0
dot3StatsFCSErrors	0
dot3StatsSingleCollisionFrames	0
dot3StatsMultipleCollisionFrames	0
dot3StatsDeferredTransmissions	0
dot3StatsLateCollisions	0
dot3StatsExcessiveCollisions	0
dot3StatsFrameTooLongs	0
dot3StatsSymbolErrors	0
dot3ControlInUnknownOpCodes	0
dot3InPauseFrames	0
dot3OutPauseFrames	0

RMON	
etherStatsDropEvents	0
etherStatsOctets	0
etherStatsPkts	0
etherStatsBroadcastPkts	0
etherStatsMulticastPkts	0
etherStatsCRCAlignErrors	0
etherStatsUnderSizePkts	0
etherStatsOverSizePkts	0
etherStatsFragments	0
etherStatsJabbers	0
etherStatsCollisions	0
etherStatsPkts64Octets	0
etherStatsPkts65to127Octets	0
etherStatsPkts128to255Octets	0
etherStatsPkts256to511Octets	0
etherStatsPkts512to1023Octets	0
etherStatsPkts1024to1518Octets	0

Параметры статистики

Параметр	Описание
Port	Выберите порт для отображения статистики.
MIB Counter	Выберите тип счётчика:
	All – все счётчики
	Interface – счётчики интерфейсов (ошибки, сбросы)
	Etherlike – Ethernet-статистика (коллизии, ошибки CRC)
	RMON – статистика по типам и размерам кадров
Refresh Rate	Автообновление страницы (в секундах) для актуальных данных.

Примечания:

1. **MIB (Management Information Base)** – база данных для мониторинга сетевых устройств.
2. **RMON (Remote Monitoring)** – расширенная статистика для анализа трафика.
3. Очистка счётчиков (**Clear**) не влияет на работу портов, только обнуляет статистику.

2.3.2. Таблица ошибок на портах (Error Disabled)

Чтобы просмотреть статус портов, отключённых из-за ошибок:

Перейдите в раздел **Status > Port > Error Disabled**

Status >> Port >> Error Disabled

Error Disabled Table

☐	Port	Reason	Time Left (sec)
☐	GE1	---	---
☐	GE2	---	---
☐	GE3	---	---
☐	GE4	---	---
☐	GE5	---	---
☐	GE6	---	---
☐	GE7	---	---
☐	GE8	---	---
☐	GE9	---	---
☐	GE10	---	---
☐	GE11	---	---
☐	GE12	---	---
☐	GE13	---	---
☐	GE14	---	---
☐	GE15	---	---
☐	GE16	---	---
☐	GE17	---	---
☐	GE18	---	---
☐	GE19	---	---
☐	GE20	---	---
☐	GE21	---	---
☐	GE22	---	---
☐	GE23	---	---
☐	GE24	---	---
☐	TE1	---	---
☐	TE2	---	---
☐	TE3	---	---
☐	TE4	---	---
☐	LAG1	---	---
☐	LAG2	---	---
☐	LAG3	---	---
☐	LAG4	---	---
☐	LAG5	---	---
☐	LAG6	---	---
☐	LAG7	---	---
☐	LAG8	---	---

Refresh Recover

Информация о портах в состоянии *Error Disabled*

Параметр	Описание
Port (Порт)	Номер интерфейса/порта.
Reason (Причина отключения)	Порт может быть отключён по одной из следующих причин:
	BPDU Guard – Обнаружен BPDU-кадр (защита от петель STP)
	UDLD – Обрыв двусторонней связи (UniDirectional Link Detection)
	Self Loop – Обнаружена петля на порту
	Broadcast Flood – Превышен лимит broadcast-трафика
	Unknown Multicast Flood – Превышен лимит неизвестного multicast-трафика
	Unicast Flood – Превышен лимит unicast-трафика
	ACL – Нарушение правил ACL (Access Control List)
	Port Security Violation – Нарушение безопасности порта (MAC-фильтрация)
	DHCP rate limit – Превышена частота DHCP-запросов
	ARP rate limit – Превышена частота ARP-запросов
Time Left (sec)	Оставшееся время (в секундах) до автоматического восстановления порта.

Примечания:

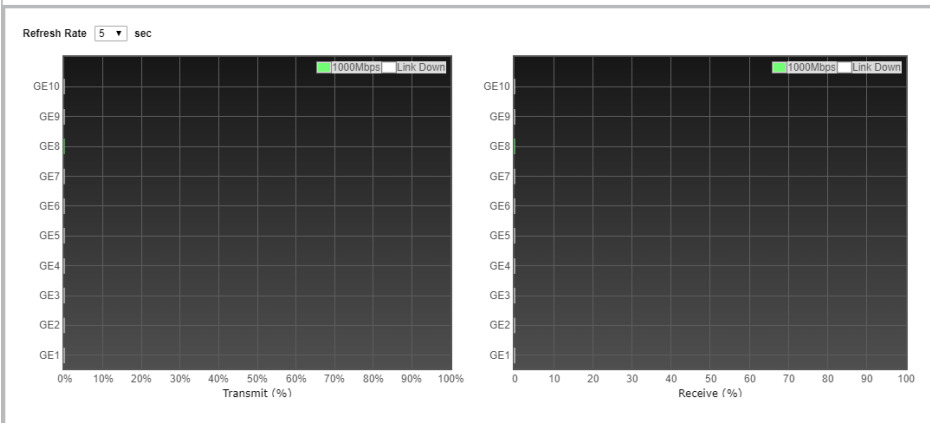
1. Состояние **Error Disabled** – защитный механизм, предотвращающий сетевые аномалии.
2. Для восстановления работы порта:
 - Дождаться истечения **Time Left** (автовосстановление),
 - Вручную включить порт через CLI/Web-интерфейс после устранения причины ошибки.
3. **BPDU Guard** и **Port Security** – частые причины отключения в безопасных сетях.

2.3.3. Использование полосы пропускания (Bandwidth Utilization)

Чтобы открыть страницу мониторинга использования полосы пропускания:

Перейдите в раздел **Status > Port > Bandwidth Utilization**.

Status >> Port >> Bandwidth Utilization



Функциональные возможности данной страницы WEB интерфейса:

- Отображение текущей загрузки полосы пропускания для каждого порта в реальном времени
- Автоматическое обновление данных с заданным интервалом

Параметр	Описание
Refresh Rate	Интервал автоматического обновления данных (в секундах). Позволяет получать актуальную информацию о загрузке полосы пропускания.

Рекомендации по использованию:

- Для детального анализа установите меньший интервал обновления

- Для долговременного мониторинга рекомендуется использовать большие интервалы
- Данные могут быть полезны для выявления перегруженных портов и оптимизации сети

2.4. Статистика агрегации каналов (Link Aggregation)

Для отображения статуса агрегации каналов:

Перейдите в раздел **Status > Link Aggregation**.

Status >> Link Aggregation

Link Aggregation Table

Q

LAG	Name	Type	Link Status	Active Member	Inactive Member
LAG 1	---	---	---		
LAG 2	---	---	---		
LAG 3	---	---	---		
LAG 4	---	---	---		
LAG 5	---	---	---		
LAG 6	---	---	---		
LAG 7	---	---	---		
LAG 8	---	---	---		

Параметры агрегированных каналов

Параметр	Описание
LAG	Идентификатор агрегированного канала
Name	Описание агрегированного порта
Type	Тип агрегации:
	Static (Статическая) - порты в группе всегда являются активными участниками
	LACP (Dynamic) - порты являются кандидатами, активные участники определяются протоколом LACP
Link Status	Текущее состояние связи агрегированного порта
Active Member	Список активных портов в составе агрегированного канала

Параметр	Описание
Inactive Member	Список неактивных портов в составе агрегированного канала

Примечания:

1. **Статическая агрегация** не требует дополнительных протоколов, но менее гибкая
2. **LACP (IEEE 802.3ad)** обеспечивает динамическое управление составом агрегированного канала

Рекомендации:

- Для критически важных соединений рекомендуется использовать LACP
- Количество портов в агрегированной группе должно соответствовать возможностям оборудования
- Мониторинг статуса помогает выявлять проблемы в работе агрегированных каналов

2.5. Информация в таблице MAC-адресов (MAC Address Table)

Для отображения таблицы MAC-адресов:

Перейдите в раздел **Status > MAC Address Table**.

Данная страница WEB интерфейса отображает все записи MAC-адресов на коммутаторе, включая:

- Статические MAC-адреса, добавленные администратором
- Динамические MAC-адреса, изученные оборудованием автоматически

Для управления предусмотрены кнопки:

- Кнопка **Clear (Очистить)** - удаляет все динамические записи
- Кнопка **Refresh (Обновить)** - получает актуальные записи MAC-адресов

Status >> MAC Address Table

MAC Address Table

Showing entries Showing 1 to 2 of 2 entries

VLAN	MAC Address	Type	Port
1	00:E0:4C:00:00:00	Management	CPU
1	00:0E:C6:D8:58:EC	Dynamic	GE8

Clear Refresh

First Previous 1 Next Last

Параметры таблицы MAC-адресов

Параметр	Описание
VLAN	Идентификатор VLAN, к которой принадлежит MAC-адрес
MAC Address	Физический адрес устройства
Type	Тип MAC-адреса:
	Management - базовый MAC-адрес устройства для управления
	Static - добавлен администратором вручную
	Dynamic - изучен коммутатором автоматически
Port	Тип порта:
	CPU - порт процессора для управления устройством
	Other - обычный порт коммутатора

Примечания:

1. Статические записи сохраняются после перезагрузки устройства
2. Динамические записи имеют ограниченное время жизни (aging time)
3. Таблица MAC-адресов используется для коммутации кадров в сети

Рекомендации:

- Регулярно проверяйте таблицу MAC-адресов для анализа подключенных устройств
- Используйте статические записи для критически важных устройств в сети
- Очистка динамических записей может быть полезна при диагностике сети

3. Настройки сети (Network)

Раздел **Настройки сети (Network)** предназначен для настройки сетевых интерфейсов коммутатора и параметров подключения к удалённым серверам.

3.1. Настройка DNS (DNS Configuration)

DNS (Domain Name System) – это система доменных имен, используемая для преобразования удобных для пользователя имен (например, example.com) в IP-адреса.

Как настроить DNS:

Перейдите в раздел **Network > DNS**

Network >> DNS

DNS Configuration

DNS Status: ☐ Disable ☒ Enable

DNS Default Name: (1 to 255 alphanumeric characters)

Apply

DNS Server Configuration

Search:

Preference	DNS Server
0 results found.	

Add Delete

Параметры DNS

Параметр	Описание
DNS Status	Включение/отключение функции DNS.
DNS Default Name	Введите доменное имя по умолчанию (например, example.com).

Network >> DNS

Add DNS Server

IPv4/IPv6 Address

Apply

Close

DNS Server Configuration

☐	Preference	DNS Server
☐	1	3.3.3.3

Add

Delete

Добавление DNS-серверов

1. Нажмите кнопку **Add (Добавить)**, чтобы указать DNS-серверы (например, 8.8.8.8 или 1.1.1.1).
2. Нажмите **Apply (Применить)**, чтобы сохранить настройки.

Примечания:

1. DNS используется для:
 - Доступа к сетевым устройствам по именам (вместо IP-адресов).
 - Подключения к интернет-ресурсам.

2. Рекомендуемые DNS-серверы:

- Google: 8.8.8.8, 8.8.4.4
- Cloudflare: 1.1.1.1, 1.0.0.1

Пример настройки:

- **DNS Default Name:** switch.local
- **DNS-серверы:** 192.168.1.1 (локальный), 8.8.8.8 (резервный).

3.2. Настройка DNS-хостов (DNS Host Configuration)

Для настройки локальных DNS-записей:

1. Перейдите в раздел **Network > Hosts**.
2. Нажмите кнопку **Add (Добавить)**, чтобы открыть интерфейс настройки.

The screenshot shows the 'Network >> Hosts' configuration page. It contains two main sections: 'DNS Host Configuration' and 'Dynamic Host Mapping'. Both sections have a search bar and a table with columns for Host and IPv4/IPv6 Address. The 'DNS Host Configuration' section has 'Add' and 'Delete' buttons. The 'Dynamic Host Mapping' section has a 'Clear' button.

Network >> Hosts

DNS Host Configuration

Search: []

☐	Host	IPv4/IPv6 Address
0 results found.		

Add Delete

Dynamic Host Mapping

Search: []

Host	Total	Elapsed	Type	IPv4/IPv6 Address
0 results found.				

Clear

Add Host

Host		(1 to 255 alphanumeric charact
IPv4/IPv6 Address		

Параметры хоста

Параметр	Описание
Host	Имя устройства (например, camera1).
IPv4/IPv6 Address	Соответствующий IP-адрес (например, 192.168.1.100).

Примечания:

1. Локальные DNS-записи позволяют обращаться к устройствам по именам **без использования внешнего DNS-сервера**.
2. Пример использования:
 - switch1.local → 192.168.1.1
 - nvr.local → 192.168.1.50

Рекомендации:

- Используйте понятные имена для удобства управления сетью.
- Обновляйте записи при изменении IP-адресов устройств.

3.3. Настройки системного времени (System Time)

Для настройки системного времени:

Перейдите в раздел **Network > System Time**.

Network >> System Time

Source

☐ SNTP
☐ From Computer
☒ Manual Time

Time Zone

UTC +8:00

SNTP

Address Type

☒ Hostname
☐ IPv4

Server Address

Server Port

123 (1 - 65535, default 123)

Manual Time

Date

2024-01-01 YYYY-MM-DD

Time

08:41:08 HH:MM:SS

Daylight Saving Time

Type

☒ None
☐ Recurring
☐ Non-recurring
☐ USA
☐ European

Offset

60 Min (1 - 1440, default 60)

Recurring

From: Day Sun Week First Month Jan Time
To: Day Sun Week First Month Jan Time

Non-recurring

From: YYYY-MM-DD HH:MM
To: YYYY-MM-DD HH:MM

Operational Status

Current Time

2024-01-01 08:41:08 UTC+8

Apply

Функционал данной страницы WEB интерфейса:

- Настройка источника времени (NTP, компьютер, ручной ввод)
- Установка часового пояса
- Конфигурация летнего времени (DST)

Настройки системного времени

Параметр	Описание
Source (Источник)	Выберите источник синхронизации времени:
	SNTP – синхронизация с NTP-сервером
	From Computer – использование времени компьютера (браузера)
	Manual Time – ручная установка времени
Time Zone (Часовой пояс)	Выберите часовой пояс из списка

Настройки SNTP (при выборе источника SNTP)

Параметр	Описание
Address Type	Тип адреса NTP-сервера (IPv4/имя хоста)
Server Address	Адрес или доменное имя NTP-сервера
Server Port	Порт NTP-сервера (по умолчанию: 123)

Установка времени вручную (Manual Time)

Параметр	Описание
Date (Дата)	Укажите дату вручную
Time (Время)	Укажите время вручную

Настройки летнего времени (Daylight Saving Time)

Параметр	Описание
Type (Тип)	Режим летнего времени:
	Disable – отключено
	Recurring – ежегодное (с фиксированными датами)
	Non-Recurring – разовое (с указанием конкретных дат)
	USA – по стандарту США (2-е воскресенье марта –

Параметр	Описание
	1-е воскресенье ноября)
	European – по стандарту ЕС (последнее воскресенье марта – октября)
Offset (Смещение)	Величина коррекции времени (обычно +1 час)
Recurring From/To	Даты начала/окончания для ежегодного режима
Non-recurring From/To	Конкретные даты для разового режима

Примечания:

1. **SNTP** требует доступа к NTP-серверу в сети.
2. Часовой пояс влияет на все источники времени.
3. Для **летнего времени** можно выбрать предустановки (США/Европа) или задать вручную.

4. Порты (Port)

Раздел **Port** предназначен для настройки параметров портов коммутатора.

4.1. Настройки портов коммутатора (Port Setting)

Для настройки параметров портов:

1. Перейдите в раздел **Port > Port Setting**.
2. Выберите порт и нажмите кнопку **«Edit» (Изменить)** для редактирования конфигурации.

Port Setting Table

Q

☐	Entry	Port	Type	Description	State	Link Status	Speed	Duplex	Flow Control
☐	1	GE1	1000M Copper		Enabled	Down	Auto	Auto	Disabled
☐	2	GE2	1000M Copper		Enabled	Down	Auto	Auto	Disabled
☐	3	GE3	1000M Copper		Enabled	Down	Auto	Auto	Disabled
☐	4	GE4	1000M Copper		Enabled	Down	Auto	Auto	Disabled
☐	5	GE5	1000M Copper		Enabled	Down	Auto	Auto	Disabled
☐	6	GE6	1000M Copper		Enabled	Down	Auto	Auto	Disabled
☐	7	GE7	1000M Copper		Enabled	Down	Auto	Auto	Disabled
☐	8	GE8	1000M Copper		Enabled	Down	Auto	Auto	Disabled
☐	9	GE9	1000M Copper		Enabled	Down	Auto	Auto	Disabled
☐	10	GE10	1000M Copper		Enabled	Down	Auto	Auto	Disabled
☐	11	GE11	1000M Copper		Enabled	Down	Auto	Auto	Disabled
☐	12	GE12	1000M Copper		Enabled	Down	Auto	Auto	Disabled
☐	13	GE13	1000M Copper		Enabled	Down	Auto	Auto	Disabled
☐	14	GE14	1000M Copper		Enabled	Down	Auto	Auto	Disabled
☐	15	GE15	1000M Copper		Enabled	Down	Auto	Auto	Disabled
☐	16	GE16	1000M Copper		Enabled	Down	Auto	Auto	Disabled
☐	17	GE17	1000M Copper		Enabled	Down	Auto	Auto	Disabled
☐	18	GE18	1000M Copper		Enabled	Up	Auto (1000M)	Auto (Full)	Disabled (Off)
☐	19	GE19	1000M Copper		Enabled	Down	Auto	Auto	Disabled
☐	20	GE20	1000M Copper		Enabled	Down	Auto	Auto	Disabled
☐	21	GE21	1000M Copper		Enabled	Down	Auto	Auto	Disabled
☐	22	GE22	1000M Copper		Enabled	Down	Auto	Auto	Disabled
☐	23	GE23	1000M Copper		Enabled	Down	Auto	Auto	Disabled
☐	24	GE24	1000M Copper		Enabled	Down	Auto	Auto	Disabled
☐	25	TE1	10G Fiber		Enabled	Down	Auto	Auto	Disabled
☐	26	TE2	10G Fiber		Enabled	Down	Auto	Auto	Disabled
☐	27	TE3	10G Fiber		Enabled	Down	Auto	Auto	Disabled
☐	28	TE4	10G Fiber		Enabled	Down	Auto	Auto	Disabled

Edit

Текущее состояние портов

Параметр	Описание
Port	Идентификатор порта
Type	Тип порта (медиа)
Description	Описание порта
State	Состояние порта:
	Enabled (Вкл.) – порт активирован
	Disabled (Выкл.) – порт деактивирован
Link Status	Текущее состояние соединения:
	Up – соединение установлено
	Down – соединение отсутствует

Параметр	Описание
Speed	Текущая скорость порта (настройка и фактическое состояние)
Duplex	Режим дуплекса (настройка и фактическое состояние)
Flow Control	Управление потоком (настройка и фактическое состояние)

Port >> Port Setting

Edit Port Setting

PortGE7-GE10

Description

State☒ Enable

Speed

☒ Auto

☐ Auto - 10M

☐ Auto - 100M

☐ Auto - 1000M

☐ Auto - 10M/100M

☐ 10M

☐ 100M

☐ 1000M

☐ 10G

Duplex

☒ Auto

☐ Full

☐ Half

Flow Control

☐ Auto

☐ Enable

☒ Disable

Apply

Close

Настройка порта (изменение настроек)

Параметр	Описание
Port	Выбранный порт
Description	Описание порта
State	Состояние порта:
	Enabled (Вкл.)
	Disabled (Выкл.)
Speed	Настройка скорости:

Параметр	Описание
	Auto – автосогласование (все скорости)
	Auto-10M – только 10 Мбит/с
	Auto-100M – только 100 Мбит/с
	Auto-1000M – только 1000 Мбит/с
	Auto-10M/100M – 10/100 Мбит/с
	10M – фиксированная 10 Мбит/с
	100M – фиксированная 100 Мбит/с
	1000M – фиксированная 1000 Мбит/с
	10G – фиксированная 10 Гбит/с (если поддерживается коммутатором)
Duplex	Режим дуплекса:
	Auto – автосогласование
	Half – полудуплекс (только 10/100 Мбит/с)
	Full – полный дуплекс (1000 Мбит/с и выше)
Flow Control	Управление потоком:
	Auto – автосогласование
	Enabled – включено
	Disabled – выключено

Примечания:

1. **Автосогласование (Auto-negotiation)** рекомендуется для большинства сценариев работы.
2. **Flow Control** помогает предотвратить потерю пакетов при перегрузке.
3. Для гигабитных и более скоростных соединений обязателен **полный дуплекс (Full Duplex)**.

4.2. Отключение портов по ошибкам (Error Disabled)

Для настройки параметров автоматического отключения портов:

Перейдите в раздел **Port > Error Disabled**

Port >> Error Disabled

Recovery Interval

300

Sec (30 - 86400)

BPDU Guard

☐ Enable

UDLD

☐ Enable

Self Loop

☐ Enable

Broadcast Flood

☐ Enable

Unknown Multicast Flood

☐ Enable

Unicast Flood

☐ Enable

ACL

☐ Enable

Port Security

☐ Enable

DHCP Rate Limit

☐ Enable

ARP Rate Limit

☐ Enable

Apply

Основные параметры

Параметр	Описание
Recover Interval	Интервал автоматического восстановления порта (в секундах) после ошибки.

Причины отключения портов

Параметр	Описание
BPDU Guard	Автоматическое отключение порта при получении BPDU-кадров (защита от петель STP).
UDLD	Автоматическое отключение порта при нарушении двусторонней связи (UniDirectional Link Detection).

Параметр	Описание
Self Loop	Автоматическое отключение порта при обнаружении петли.
Broadcast Flood	Автоматическое отключение порта при превышении лимита broadcast-трафика.
Unknown Multicast Flood	Автоматическое отключение порта при превышении лимита неизвестного multicast-трафика.
Unicast Flood	Автоматическое отключение порта при превышении лимита unicast-трафика.
ACL	Автоматическое отключение порта при нарушении правил ACL (Access Control List).
Port Security	Автоматическое отключение порта при нарушении правил безопасности порта (Port Security).
DHCP rate limit	Автоматическое отключение порта при превышении лимита DHCP-запросов.
ARP rate limit	Автоматическое отключение порта при превышении лимита ARP-запросов.

Примечания:

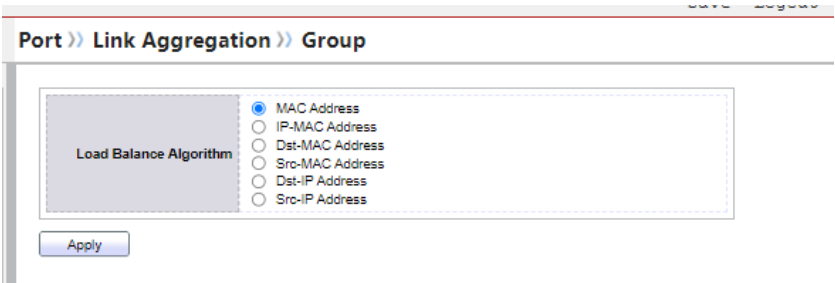
1. **Recover Interval** – порт автоматически восстановится через указанное время (0 = ручное включение).
2. **BPDU Guard** и **Port Security** – наиболее частые причины отключения в защищённых сетях.

4.3. Агрегация каналов (Link Aggregation)

4.3.1. Настройка групп (Group)

Для настройки агрегированных групп:

Перейдите в раздел **Port > Link Aggregation > Group**



Алгоритм балансировки нагрузки

Параметр	Описание
Load Balance Algorithm	Алгоритм распределения нагрузки в агрегированной группе:
	MAC Address – на основе MAC-адресов источника и назначения
	IP-MAC Address – на основе комбинации IP и MAC-адресов
	Dst-MAC Address – на основе MAC-адреса назначения
	Src-MAC Address – на основе MAC-адреса источника
	Dst-IP Address – на основе IP-адреса назначения
	Src-IP Address – на основе IP-адреса источника

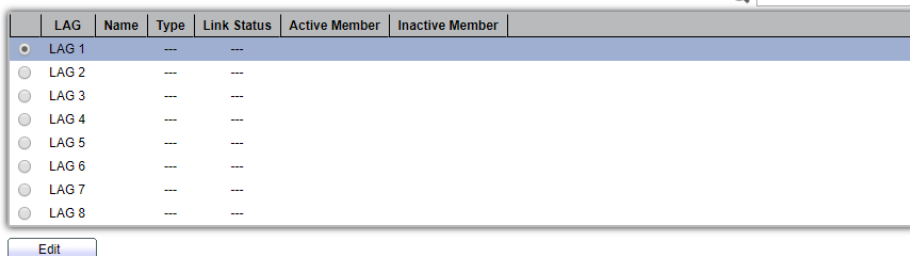
Примечания:

1. **Алгоритмы балансировки** определяют, как трафик распределяется между портами в агрегированной группе.
2. Рекомендации по выбору алгоритма:
 - **Mac Address/IP-MAC** – для общего использования (универсальный вариант).
 - **Dst-IP/Src-IP** – если в сети преобладает трафик между конкретными IP-адресами (например, серверами).
 - **Dst-MAC/Src-MAC** – для сетей с большим количеством устройств.

Пример настройки:

- **Алгоритм: IP-MAC Address** (оптимален для смешанного трафика).

Link Aggregation Table



LAG	Name	Type	Link Status	Active Member	Inactive Member
☒ LAG 1	---	---	---		
☐ LAG 2	---	---	---		
☐ LAG 3	---	---	---		
☐ LAG 4	---	---	---		
☐ LAG 5	---	---	---		
☐ LAG 6	---	---	---		
☐ LAG 7	---	---	---		
☐ LAG 8	---	---	---		

Edit

Список агрегированных групп

Параметр	Описание
LAG	Идентификатор LAG-группы
Name	Описание группы
Type	Тип агрегации:
	Static – порты всегда активны в группе
	LACP – активные порты определяются протоколом LACP

Параметр	Описание
Link Status	Текущее состояние группы (активна/неактивна)
Active Member	Список активных портов в группе
Inactive Member	Список неактивных портов в группе

Port >> Link Aggregation >> Group

[Edit Link Aggregation Group](#)

LAG 1

Name

Type

☒ Static

☐ LACP

Member

Available Port

GE3

GE4

GE5

GE6

GE7

GE8

GE9

GE10

➔

➞

Selected Port

GE1

GE2

Apply

Close

Настройка группы (редактирование)

Параметр	Описание
LAG	Идентификатор выбранной LAG-группы
Name	Описание группы
Type	Тип агрегации:
	Static – статическая агрегация
	LACP – динамическая агрегация (с использованием протокола LACP)
Member	Выбор портов для включения в группу

Примечания:

1. **Статическая агрегация (Static)** проще в настройке, но менее гибкая.
2. **LACP (IEEE 802.3ad)** обеспечивает автоматическое управление составом группы.
3. Алгоритм **src-dst-mac-ip (IP-MAC Address)** обеспечивает более равномерное распределение трафика.

Рекомендации:

- Для критически важных соединений используйте **LACP**.

4.3.2. Настройки портов агрегации (Port Setting)

Для настройки параметров портов в агрегированной группе:

1. Перейдите в раздел **Port > Link Aggregation > Port Setting**.
2. Выберите порт LAG и нажмите кнопку **«Edit» (Изменить)** для редактирования конфигурации.

Port >> Link Aggregation >> Port Setting

Port Setting Table

	LAG	Type	Description	State	Link Status	Speed	Duplex	Flow Control
☐	LAG 1			Enabled	Down	Auto	Auto	Disabled
☐	LAG 2			Enabled	Down	Auto	Auto	Disabled
☐	LAG 3			Enabled	Down	Auto	Auto	Disabled
☐	LAG 4			Enabled	Down	Auto	Auto	Disabled
☐	LAG 5			Enabled	Down	Auto	Auto	Disabled
☐	LAG 6			Enabled	Down	Auto	Auto	Disabled
☐	LAG 7			Enabled	Down	Auto	Auto	Disabled
☐	LAG 8			Enabled	Down	Auto	Auto	Disabled

Edit

Текущее состояние портов LAG

Параметр	Описание
LAG	Имя агрегированного порта
Type	Тип порта (медиа)
Description	Описание порта
State	Административное состояние:
	Enabled (Вкл.) – порт активирован
	Disabled (Выкл.) – порт деактивирован
Link Status	Текущее состояние соединения:
	Up – соединение установлено
	Down – соединение отсутствует
Speed	Текущая скорость порта (настройка и фактическое состояние)
Duplex	Режим дуплекса (настройка и фактическое состояние)
Flow Control	Управление потоком (настройка и фактическое состояние)

Port » Link Aggregation » Port Setting

[Edit Port Setting](#)

Port

LAG1

Description

State

☒ Enable

Speed

☒ Auto
☐ 10M
☐ 100M
☐ 1000M
☐ 10G
☐ Auto - 10M
☐ Auto - 100M
☐ Auto - 1000M
☐ Auto - 10M/100M

Flow Control

☐ Auto
☐ Enable
☒ Disable

Apply

Close

Редактирование настроек портов LAG

Параметр	Описание
Port	Выбранные порты
Description	Описание порта
State	Состояние порта
	Enable (Вкл.)
	Disable (Выкл.)
Speed	Настройка скорости:
	Auto – автосогласование (все скорости)
	Auto-10M – только 10 Мбит/с
	Auto-100M – только 100 Мбит/с
	Auto-1000M – только 1000 Мбит/с
	Auto-10M/100M – 10/100 Мбит/с
	10M – фиксированная 10 Мбит/с
	100M – фиксированная 100 Мбит/с
	1000M – фиксированная 1000 Мбит/с
	10G – фиксированная 10 Гбит/с (если поддерживается коммутатором)
Flow Control	Управление потоком:
	Auto – автосогласование
	Enabled – включено
	Disabled – выключено

Примечания:

1. Для портов в агрегированной группе рекомендуется использовать **одинаковые настройки** скорости и дуплекса.
2. **Автосогласование (Auto-negotiation)** – предпочтительный режим для большинства сценариев.

3. **Flow Control** помогает предотвратить перегрузку буферов портов.

Рекомендации:

- Для гигабитных соединений используйте **1000M Full Duplex**.
- При использовании LACP убедитесь, что все порты группы имеют **одинаковые настройки**.

4.3.3. Настройки протокола LACP (LACP)

Для конфигурации параметров протокола LACP:

1. Перейдите в раздел **Port > Link Aggregation > LACP**.
2. Выберите порты и нажмите кнопку **«Edit» (Изменить)** для настройки.

Port >> Link Aggregation >> LACP



The screenshot shows a configuration window for LACP. It features a label 'System Priority' next to a text input field containing the value '32768'. To the right of the input field is a hint text '(1 - 65535, default 32768)'. Below the input field is a button labeled 'Apply'.

Глобальные параметры LACP

Параметр	Описание
System Priority	Приоритет системы LACP (влияет на выбор активного устройства при агрегации).

Q

☐	Entry	Port	Port Priority	Timeout
☐	1	GE1	1	Long
☐	2	GE2	1	Long
☐	3	GE3	1	Long
☐	4	GE4	1	Long
☐	5	GE5	1	Long
☐	6	GE6	1	Long
☐	7	GE7	1	Long
☐	8	GE8	1	Long
☐	9	GE9	1	Long
☐	10	GE10	1	Long
☐	11	GE11	1	Long
☐	12	GE12	1	Long
☐	13	GE13	1	Long
☐	14	GE14	1	Long
☐	15	GE15	1	Long
☐	16	GE16	1	Long
☐	17	GE17	1	Long
☐	18	GE18	1	Long
☐	19	GE19	1	Long
☐	20	GE20	1	Long
☐	21	GE21	1	Long
☐	22	GE22	1	Long
☐	23	GE23	1	Long
☐	24	GE24	1	Long
☐	25	TE1	1	Long
☐	26	TE2	1	Long
☐	27	TE3	1	Long
☐	28	TE4	1	Long

Edit

Текущие настройки портов LACP

Параметр	Описание
Port	Имя порта
Port Priority	Приоритет порта в LACP (чем меньше значение, тем выше приоритет).
Timeout	Интервал отправки LACP-пакетов:
	Long (Длинный) – 30 секунд (рекомендуется для стабильных сетей)
	Short (Короткий) – 1 секунда (быстрое обнаружение изменений)

Edit LACP Port Setting

Port	GE1-GE3	
Port Priority	1	(1 - 65535, default 1)
Timeout	☒ Long ☐ Short	

Редактирование настроек портов LACP

Параметр	Описание
Port	Выбранные порты
Port Priority	Укажите приоритет порта (0–65535, чем меньше – тем выше приоритет).
Timeout	Выберите интервал отправки LACP-пакетов:
	• Long (Длинный) – 30 секунд
	• Short (Короткий) – 1 секунда

Примечания:

1. **System Priority** определяет, какое устройство будет "активным" в агрегированной группе.
2. **Port Priority** влияет на выбор активных портов при избыточной конфигурации.
3. **Short Timeout** обеспечивает быструю реакцию на изменения, но увеличивает нагрузку на сеть.

Рекомендации:

- Для стабильных сетей используйте **Long Timeout (30 сек)**.
- Для критически важных соединений установите **более высокий приоритет (меньшее значение)**.

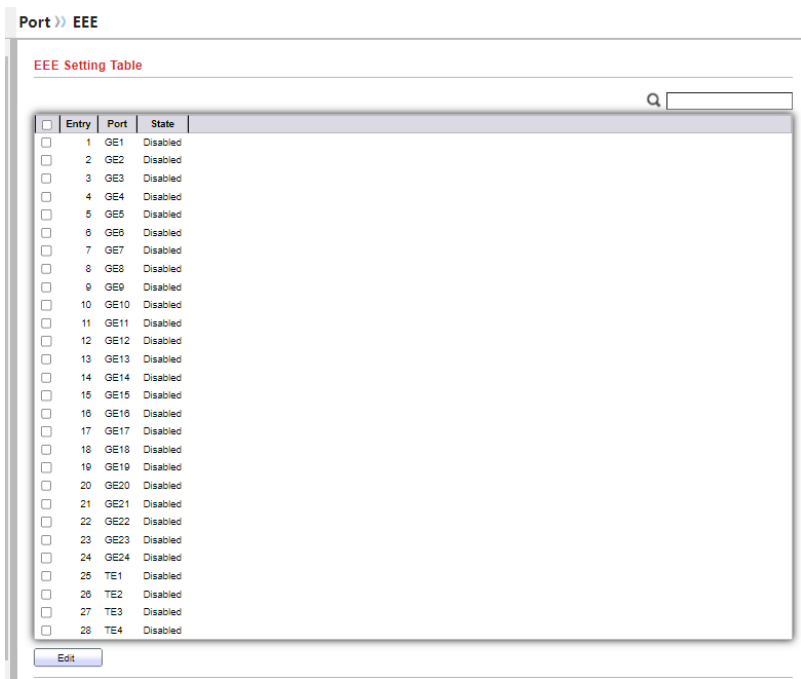
4.4. Настройки Energy Efficient Ethernet, IEEE 802.3az (EEE)

Для настройки параметров EEE:

Перейдите в раздел **Port > EEE**.

Функционал страницы:

Позволяет настроить энергоэффективный режим работы Ethernet-портов (IEEE 802.3az).



Текущие параметры EEE

Параметр	Описание
Port	Идентификатор порта
State	Состояние EEE:
	Enabled - EEE включен
	Disabled - EEE выключен

Параметр	Описание
Operational Status	Фактический статус работы EEE:
	Enabled - EEE активен
	Disabled - EEE неактивен

Port >> EEE

[Edit EEE Setting](#)

Port

GE1-GE3

State

☒ Enable

Apply

Close

Настройки EEE (редактирование)

Параметр	Описание
Port	Выбранные порты для настройки
State	Управление режимом EEE:
	Enable - включить EEE
	Disable - выключить EEE

Примечания:

1. Energy Efficient Ethernet (IEEE 802.3az) позволяет снизить энергопотребление портов при низкой нагрузке
2. Для работы EEE требуется поддержка на обоих концах соединения
3. Включение EEE может незначительно увеличить задержку передачи данных

Рекомендации:

- Включите EEE для портов, где критично энергопотребление
- Для портов с чувствительными к задержкам приложениями (VoIP, видео) рекомендуется отключить EEE

4.5. Настройка Jumbo Frame (Jumbo Frame)

Для настройки параметров Jumbo Frame:

Перейдите в раздел **Port > Jumbo Frame**.

Функционал страницы:

Позволяет настроить поддержку кадров увеличенного размера (Jumbo Frame) на коммутаторе.

Port >> Jumbo Frame

Jumbo Frame

☐ Enable

10000

Byte (1518 - 10000, default 1522)

Apply

Параметр	Описание
Jumbo Frame	Включение/выключение поддержки Jumbo Frame:
	Enabled - при активации позволяет настраивать максимальный размер кадра
	Disabled - используется стандартный максимальный размер кадра (1522 байта)

Примечания:

1. Jumbo Frame поддерживают передачу кадров размером до 9000+ байт (вместо стандартных 1522 байт)
2. Для работы Jumbo Frame требуется поддержка на всех устройствах пути передачи
3. Использование Jumbo Frame может:
 - Увеличить пропускную способность для передачи «тяжелого» трафика
 - Снизить нагрузку на процессор
 - Уменьшить количество прерываний

Рекомендации:

- Включайте Jumbo Frame только если вся сеть поддерживает эту функцию
- Оптимально использовать для:
 - Серверных соединений
 - Хранилищ данных (SAN)
 - Видеотрафика
- Стандартное значение (1522 байта) подходит для большинства обычных сетевых задач

5. VLAN

Виртуальная локальная сеть (**VLAN**) – это группа устройств с общими требованиями, которые взаимодействуют так, как если бы они находились в одном широковещательном домене, независимо от их физического расположения. VLAN обладает теми же характеристиками, что и физическая локальная сеть (**LAN**), но позволяет объединять устройства, даже если они подключены к разным коммутаторам.

Порты–участники в VLAN настраиваются программно, без необходимости физического перемещения устройств или изменения подключений.

5.1. Настройки VLAN (VLAN)

Раздел **VLAN** предназначен для настройки параметров виртуальных локальных сетей.

5.1.1. Создание VLAN (Create VLAN)

Чтобы создать VLAN:

Перейдите в раздел **VLAN > VLAN > Create VLAN**.

Функционал страницы:

- Добавление или удаление идентификаторов VLAN (**VLAN ID**)
- Просмотр всех VLAN, добавленных вручную (**статически**) или автоматически (**через GVRP**)
- Возможность редактирования имени VLAN

VLAN >> VLAN >> Create VLAN

VLAN

Available VLAN

VLAN 2

VLAN 3

VLAN 4

VLAN 5

VLAN 6

VLAN 7

VLAN 8

VLAN 9

Created VLAN

VLAN 1

Apply

VLAN Table

Showing All entries

Showing 1 to 1 of 1 entries

VLAN

Name

Type

VLAN Interface State

1

default

Default

Disabled

Edit

Delete

First

Previous

1

Next

Last

Настройки VLAN

Параметр	Описание
Available VLAN	Список доступных VLAN, которые еще не созданы.
	Выберите VLAN из левого окна и перенесите в правое для добавления.
Created VLAN	Список созданных VLAN.
	Выберите VLAN из правого окна и перенесите в левое для удаления.

Edit VLAN Name

Name	VLAN0002
Apply	Close

Параметр	Описание
Name	Введите имя VLAN (уникальное для каждой VLAN).

Примечания:

- VLAN ID** – числовой идентификатор (1–4094), где:
 - 1** – используется по умолчанию для управления.
 - 2–1001** – стандартный диапазон для пользовательских VLAN.
 - 1006–4094** – расширенный диапазон (требует поддержки на оборудовании).
- GVRP (GARP VLAN Registration Protocol)** – протокол для автоматической регистрации VLAN между коммутаторами.

Рекомендации:

- Используйте понятные имена (например, "Office" или "Servers") для удобства управления.
- Избегайте удаления VLAN, которые используются активными устройствами.

5.1.2. Конфигурация VLAN (VLAN Configuration)

Для настройки портов – учатстинков в VLAN:

- 1. Перейдите в раздел **VLAN > VLAN > VLAN Configuration**.
- 2. Выберите VLAN ID для настройки.

VLAN >> VLAN >> VLAN Configuration

VLAN Configuration Table

VLAN

default

Entry	Port	Mode	Membership		PVID	Forbidden
1	GE1	Trunk	☐ Excluded	☐ Tagged	☒ Untagged	☒
2	GE2	Trunk	☐ Excluded	☐ Tagged	☒ Untagged	☒
3	GE3	Trunk	☐ Excluded	☐ Tagged	☒ Untagged	☒
4	GE4	Trunk	☐ Excluded	☐ Tagged	☒ Untagged	☒
5	GE5	Trunk	☐ Excluded	☐ Tagged	☒ Untagged	☒
6	GE6	Trunk	☐ Excluded	☐ Tagged	☒ Untagged	☒
7	GE7	Trunk	☐ Excluded	☐ Tagged	☒ Untagged	☒
8	GE8	Trunk	☐ Excluded	☐ Tagged	☒ Untagged	☒
9	GE9	Trunk	☐ Excluded	☐ Tagged	☒ Untagged	☒
10	GE10	Trunk	☐ Excluded	☐ Tagged	☒ Untagged	☒
11	GE11	Trunk	☐ Excluded	☐ Tagged	☒ Untagged	☒
12	GE12	Trunk	☐ Excluded	☐ Tagged	☒ Untagged	☒
13	GE13	Trunk	☐ Excluded	☐ Tagged	☒ Untagged	☒
14	GE14	Trunk	☐ Excluded	☐ Tagged	☒ Untagged	☒
15	GE15	Trunk	☐ Excluded	☐ Tagged	☒ Untagged	☒
16	GE16	Trunk	☐ Excluded	☐ Tagged	☒ Untagged	☒
17	GE17	Trunk	☐ Excluded	☐ Tagged	☒ Untagged	☒
18	GE18	Trunk	☐ Excluded	☐ Tagged	☒ Untagged	☒
19	GE19	Trunk	☐ Excluded	☐ Tagged	☒ Untagged	☒
20	GE20	Trunk	☐ Excluded	☐ Tagged	☒ Untagged	☒
21	GE21	Trunk	☐ Excluded	☐ Tagged	☒ Untagged	☒
22	GE22	Trunk	☐ Excluded	☐ Tagged	☒ Untagged	☒
23	GE23	Trunk	☐ Excluded	☐ Tagged	☒ Untagged	☒
24	GE24	Trunk	☐ Excluded	☐ Tagged	☒ Untagged	☒
25	TE1	Trunk	☐ Excluded	☐ Tagged	☒ Untagged	☒
26	TE2	Trunk	☐ Excluded	☐ Tagged	☒ Untagged	☒
27	TE3	Trunk	☐ Excluded	☐ Tagged	☒ Untagged	☒
28	TE4	Trunk	☐ Excluded	☐ Tagged	☒ Untagged	☒
29	LAG1	Trunk	☐ Excluded	☐ Tagged	☒ Untagged	☒
30	LAG2	Trunk	☐ Excluded	☐ Tagged	☒ Untagged	☒
31	LAG3	Trunk	☐ Excluded	☐ Tagged	☒ Untagged	☒
32	LAG4	Trunk	☐ Excluded	☐ Tagged	☒ Untagged	☒
33	LAG5	Trunk	☐ Excluded	☐ Tagged	☒ Untagged	☒
34	LAG6	Trunk	☐ Excluded	☐ Tagged	☒ Untagged	☒
35	LAG7	Trunk	☐ Excluded	☐ Tagged	☒ Untagged	☒
36	LAG8	Trunk	☐ Excluded	☐ Tagged	☒ Untagged	☒

Apply

Параметры конфигурации VLAN

Параметр	Описание
VLAN	Выберите VLAN ID для настройки.
Port	Физический интерфейс порта.
Mode	Режим VLAN на порту (отображается текущее состояние).

Параметр	Описание
Membership	Настройка членства порта в VLAN:
	Forbidden – порт запрещён в VLAN (блокировка)
	Excluded – порт исключён из VLAN (по умолчанию)
	Tagged – порт передаёт трафик с тегами VLAN (для межкоммутаторных соединений)
	Untagged – порт передаёт трафик без тегов (для конечных устройств)
PVID	Отображает, является ли VLAN PVID (Port VLAN ID) для порта.

Ключевые термины:

- **Tagged (Тегированный)** – используется для соединений между коммутаторами (802.1Q).
- **Untagged (Не тегированный)** – для подключения конечных устройств (ПК, IP-камеры).
- **PVID (Port VLAN ID)** – VLAN по умолчанию для untagged-трафика на порту.

Пример настройки:

- **Порт 1:** Untagged в VLAN 10 (офисные ПК)
- **Порт 24:** Tagged в VLAN 10 и 20 (магистраль к другому коммутатору)

Примечания:

1. **Forbidden** – полностью блокирует VLAN на порту.
2. **Excluded** – порт не принадлежит VLAN, но может быть добавлен.

5.1.3. Настройка VLAN Membership (Membership)

Для просмотра и настройки портов участников в VLAN:

Перейдите в раздел **VLAN > VLAN > Membership**

VLAN >> VLAN >> Membership

Membership Table

q

	Entry	Port	Mode	Administrative VLAN	Operational VLAN
☐	1	GE1	Trunk	1UP	1UP
☐	2	GE2	Trunk	1UP	1UP
☐	3	GE3	Trunk	1UP	1UP
☐	4	GE4	Trunk	1UP	1UP
☐	5	GE5	Trunk	1UP	1UP
☐	6	GE6	Trunk	1UP	1UP
☐	7	GE7	Trunk	1UP	1UP
☐	8	GE8	Trunk	1UP	1UP
☐	9	GE9	Trunk	1UP	1UP
☐	10	GE10	Trunk	1UP	1UP
☐	11	GE11	Trunk	1UP	1UP
☐	12	GE12	Trunk	1UP	1UP
☐	13	GE13	Trunk	1UP	1UP
☐	14	GE14	Trunk	1UP	1UP
☐	15	GE15	Trunk	1UP	1UP
☐	16	GE16	Trunk	1UP	1UP
☐	17	GE17	Trunk	1UP	1UP
☐	18	GE18	Trunk	1UP	1UP
☐	19	GE19	Trunk	1UP	1UP
☐	20	GE20	Trunk	1UP	1UP
☐	21	GE21	Trunk	1UP	1UP
☐	22	GE22	Trunk	1UP	1UP
☐	23	GE23	Trunk	1UP	1UP
☐	24	GE24	Trunk	1UP	1UP
☐	25	TE1	Trunk	1UP	1UP
☐	26	TE2	Trunk	1UP	1UP
☐	27	TE3	Trunk	1UP	1UP
☐	28	TE4	Trunk	1UP	1UP
☐	29	LAG1	Trunk	1UP	1UP
☐	30	LAG2	Trunk	1UP	1UP
☐	31	LAG3	Trunk	1UP	1UP
☐	32	LAG4	Trunk	1UP	1UP
☐	33	LAG5	Trunk	1UP	1UP
☐	34	LAG6	Trunk	1UP	1UP
☐	35	LAG7	Trunk	1UP	1UP
☐	36	LAG8	Trunk	1UP	1UP

Edit

Текущие параметры портов

Параметр	Описание
Port	Физический интерфейс порта.
Mode	Режим VLAN на порту (например, Access, Trunk, Hybrid).
Administrative	Список VLAN, назначенных порту администратором

Параметр	Описание
VLAN	(настроенные вручную).
Operational VLAN	Фактический список VLAN, в которых работает порт. Может отличаться от Administrative VLAN.

VLAN » VLAN » Membership

Edit Port Setting

Port

GE2

Mode

Trunk

Membership

1UP

☐ Forbidden

☐ Excluded

☒ Tagged

☐ Untagged

☐ PVID

Apply

Close

Настройка портов-участников VLAN

Параметр	Описание
Port	Выбранный порт.
Mode	Текущий режим VLAN порта.
Membership	Настройка порта участника VLAN. Выберите VLAN из левого списка. Укажите тип порта – участника:
	Forbidden – порт запрещён в VLAN.
	Tagged – порт передаёт трафик с тегами VLAN (для

Параметр	Описание
	магистральных соединений).
	Untagged – порт передаёт трафик без тегов (для конечных устройств).
	PVID – VLAN по умолчанию для untagged-трафика.

Ключевые особенности:

- **Administrative VLAN и Operational VLAN:**
 - Administrative – настройки, введённые вручную.
 - Operational – фактические VLAN, которые активны на порту (например, после применения GVRP).
- **PVID (Port VLAN ID):**
 - Автоматически назначается для untagged-трафика.
 - Нельзя изменить, если порт находится в определённых режимах (например, Forbidden).

Пример настройки:

- **Порт 1:**
 - **Mode:** Access
 - **Untagged VLAN:** 10
 - **PVID:** 10
- **Порт 24:**
 - **Mode:** Trunk
 - **Tagged VLAN:** 10, 20, 30
 - **PVID:** 1 (управление)

5.1.4. Настройка портов VLAN (Port Setting)

Для настройки параметров VLAN на портах:

Перейдите в раздел **VLAN > VLAN > Port Setting**.

VLAN >> VLAN >> Port Setting

Port Setting Table

☐	Entry	Port	Mode	PVID	Accept Frame Type	Ingress Filtering	Uplink	TPID
☐	1	GE1	Trunk	1	All	Enabled	Disabled	0x8100
☐	2	GE2	Trunk	1	All	Enabled	Disabled	0x8100
☐	3	GE3	Trunk	1	All	Enabled	Disabled	0x8100
☐	4	GE4	Trunk	1	All	Enabled	Disabled	0x8100
☐	5	GE5	Trunk	1	All	Enabled	Disabled	0x8100
☐	6	GE6	Trunk	1	All	Enabled	Disabled	0x8100
☐	7	GE7	Trunk	1	All	Enabled	Disabled	0x8100
☐	8	GE8	Trunk	1	All	Enabled	Disabled	0x8100
☐	9	GE9	Trunk	1	All	Enabled	Disabled	0x8100
☐	10	GE10	Trunk	1	All	Enabled	Disabled	0x8100
☐	11	GE11	Trunk	1	All	Enabled	Disabled	0x8100
☐	12	GE12	Trunk	1	All	Enabled	Disabled	0x8100
☐	13	GE13	Trunk	1	All	Enabled	Disabled	0x8100
☐	14	GE14	Trunk	1	All	Enabled	Disabled	0x8100
☐	15	GE15	Trunk	1	All	Enabled	Disabled	0x8100
☐	16	GE16	Trunk	1	All	Enabled	Disabled	0x8100
☐	17	GE17	Trunk	1	All	Enabled	Disabled	0x8100
☐	18	GE18	Trunk	1	All	Enabled	Disabled	0x8100
☐	19	GE19	Trunk	1	All	Enabled	Disabled	0x8100
☐	20	GE20	Trunk	1	All	Enabled	Disabled	0x8100
☐	21	GE21	Trunk	1	All	Enabled	Disabled	0x8100
☐	22	GE22	Trunk	1	All	Enabled	Disabled	0x8100
☐	23	GE23	Trunk	1	All	Enabled	Disabled	0x8100
☐	24	GE24	Trunk	1	All	Enabled	Disabled	0x8100
☐	25	TE1	Trunk	1	All	Enabled	Disabled	0x8100
☐	26	TE2	Trunk	1	All	Enabled	Disabled	0x8100
☐	27	TE3	Trunk	1	All	Enabled	Disabled	0x8100
☐	28	TE4	Trunk	1	All	Enabled	Disabled	0x8100
☐	29	LAG1	Trunk	1	All	Enabled	Disabled	0x8100
☐	30	LAG2	Trunk	1	All	Enabled	Disabled	0x8100
☐	31	LAG3	Trunk	1	All	Enabled	Disabled	0x8100
☐	32	LAG4	Trunk	1	All	Enabled	Disabled	0x8100
☐	33	LAG5	Trunk	1	All	Enabled	Disabled	0x8100
☐	34	LAG6	Trunk	1	All	Enabled	Disabled	0x8100
☐	35	LAG7	Trunk	1	All	Enabled	Disabled	0x8100
☐	36	LAG8	Trunk	1	All	Enabled	Disabled	0x8100

Edit

Текущие параметры портов

Параметр	Описание
Port	Идентификатор порта.
Mode	Текущий режим VLAN порта (Hybrid, Access, Trunk).

Параметр	Описание
PVID	Port VLAN ID (идентификатор VLAN по умолчанию для untagged-трафика).
Accept Frame Type	Тип принимаемых кадров (зависит от режима).
Ingress Filtering	Состояние фильтрации входящего трафика (вкл./выкл.).
Uplink	Режим uplink (используется для восходящих соединений).
TPID	Tag Protocol Identifier (идентификатор тега VLAN)

VLAN >> VLAN >> Port Setting

Edit Port Setting

Port

GE7

Mode

☐ Hybrid
☐ Access
☒ Trunk
☐ Tunnel

PVID

(1 - 4094)

Accept Frame Type

☒ All
☐ Tag Only
☐ Untag Only

Ingress Filtering

☒ Enable

Uplink

☒ Enable

TPID

0x9100 ▾

Apply

Close

Редактирование параметров портов

Параметр	Описание
Port	Выбранный порт для настройки.

Параметр	Описание
Mode	Выберите режим VLAN:
	Hybrid – поддерживает все функции IEEE 802.1Q (тегированные и untagged-кадры).
	Access – принимает только untagged-кадры и принадлежит одной VLAN.
	Trunk – передаёт тегированные кадры для нескольких VLAN.
PVID	Укажите PVID (1–4094). Доступно только для режимов Hybrid и Trunk .
Accepted Type	Тип принимаемых кадров (только для режима Hybrid):
	All – все кадры (тегированные и untagged).
	Tag only – только тегированные кадры.
	Untag Only – все кадры (тегированные и untagged).
Ingress Filtering	Включите/отключите фильтрацию входящего трафика (только для Hybrid режима).
Uplink	Включите/отключите режим uplink (только для Trunk режима).
TPID	Выберите TPID (например, 0x8100 для стандартного VLAN). Доступно только для Trunk режима

Примечания:

1. Режимы портов:

- **Access** – для подключения конечных устройств (ПК, камеры).
- **Trunk** – для соединения между коммутаторами.
- **Hybrid** – гибкий режим (поддержка тегированных и untagged-кадров).

2. **PVID** – VLAN, в которую попадает untagged-трафик.
3. **Ingress Filtering** – если включено, порт отбрасывает кадры с тегами VLAN, в которых он не состоит.

Примеры конфигурации:

- **Access-порт (PVID=10):**
 - Режим: Access
 - Принимает только untagged-трафик и относит его к VLAN 10.
- **Trunk-порт (PVID=1, Tagged VLANs=10,20,30):**
 - Режим: Trunk
 - Передаёт тегированные кадры для VLAN 10, 20, 30.
 - Untagged-трафик попадает в VLAN 1 (управление).

5.2. Голосовая VLAN (Voice VLAN)

Раздел **Voice VLAN** предназначен для настройки VLAN, оптимизированной для передачи голосового трафика (VoIP).

5.2.1. Свойства Voice VLAN (Property)

Для настройки глобальных параметров и параметров портов Voice VLAN:

Перейдите в раздел **VLAN > Voice VLAN > Property**

VLAN >> Voice VLAN >> Property

State	☐ Enable
VLAN	None ▼
CoS / 802.1p Remarking	☐ Enable 6 ▼
Aging Time	1440 Min (30 - 65536, default 1440)

Apply

Глобальные настройки Voice VLAN

Параметр	Описание
State	Включение/отключение функции Voice VLAN.
VLAN	Идентификатор Voice VLAN (не может совпадать с VLAN по умолчанию).
Cos/802.1p	Приоритет VLAN (VPT) для голосового трафика (0–7).
Remarking	Включение/отключение перемаркировки приоритета (802.1p).
Aging Time	Время жизни записей Voice VLAN (по умолчанию: 1440 минут).

Port Setting Table

☐	Entry	Port	State	Mode	QoS Policy
☐	1	GE1	Disabled	Auto	Voice Packet
☐	2	GE2	Disabled	Auto	Voice Packet
☐	3	GE3	Disabled	Auto	Voice Packet
☐	4	GE4	Disabled	Auto	Voice Packet
☐	5	GE5	Disabled	Auto	Voice Packet
☐	6	GE6	Disabled	Auto	Voice Packet
☐	7	GE7	Disabled	Auto	Voice Packet
☐	8	GE8	Disabled	Auto	Voice Packet
☐	9	GE9	Disabled	Auto	Voice Packet
☐	10	GE10	Disabled	Auto	Voice Packet
☐	11	GE11	Disabled	Auto	Voice Packet
☐	12	GE12	Disabled	Auto	Voice Packet
☐	13	GE13	Disabled	Auto	Voice Packet
☐	14	GE14	Disabled	Auto	Voice Packet
☐	15	GE15	Disabled	Auto	Voice Packet
☐	16	GE16	Disabled	Auto	Voice Packet
☐	17	GE17	Disabled	Auto	Voice Packet
☐	18	GE18	Disabled	Auto	Voice Packet
☐	19	GE19	Disabled	Auto	Voice Packet
☐	20	GE20	Disabled	Auto	Voice Packet
☐	21	GE21	Disabled	Auto	Voice Packet
☐	22	GE22	Disabled	Auto	Voice Packet
☐	23	GE23	Disabled	Auto	Voice Packet
☐	24	GE24	Disabled	Auto	Voice Packet
☐	25	TE1	Disabled	Auto	Voice Packet
☐	26	TE2	Disabled	Auto	Voice Packet
☐	27	TE3	Disabled	Auto	Voice Packet
☐	28	TE4	Disabled	Auto	Voice Packet
☐	29	LAG1	Disabled	Auto	Voice Packet
☐	30	LAG2	Disabled	Auto	Voice Packet
☐	31	LAG3	Disabled	Auto	Voice Packet
☐	32	LAG4	Disabled	Auto	Voice Packet
☐	33	LAG5	Disabled	Auto	Voice Packet
☐	34	LAG6	Disabled	Auto	Voice Packet
☐	35	LAG7	Disabled	Auto	Voice Packet
☐	36	LAG8	Disabled	Auto	Voice Packet

Таблица текущих параметров портов

Параметр	Описание
Port	Идентификатор порта.
State	Состояние Voice VLAN на порту (вкл./выкл.).
Mode	Режим работы Voice VLAN (Auto/Manual).
QoS Policy	Тип пакетов, к которым применяются QoS-атрибуты.

VLAN » Voice VLAN » Property

Edit Port Setting

Port	GE1
State	☐ Enable
Mode	☒ Auto ☐ Manual
QoS Policy	☒ Voice Packet ☐ All

Apply

Close

Редактирование параметров портов

Параметр	Описание
Port	Выбранный порт.
State	Включение/отключение Voice VLAN на порту.
Mode	Выберите режим работы:
	Auto – автоматическое добавление порта в Voice VLAN при обнаружении голосового трафика.
	Manual – ручное добавление порта в Voice VLAN.
QoS Policy	Политика QoS:
	Voice Packet – QoS применяется только к пакетам с MAC-адресами из OUI-таблицы.
	All – QoS применяется ко всем пакетам в Voice VLAN.

Примечания:

- 1. **OUI (Organizationally Unique Identifier)** – идентификатор производителя VoIP-устройств (например, Cisco, Yealink).
- 2. **Режим Auto** удобен для IP-телефонов, которые автоматически определяются по MAC-адресу.
- 3. **Приоритет (802.1p)** обеспечивает качество обслуживания (QoS) для голосового трафика.

5.2.2. Голосовые OUI адреса (Voice OUI)

Для настройки OUI-адресов VoIP-устройств:

Перейдите в раздел **VLAN > Voice VLAN > Voice OUI**.

VLAN >> Voice VLAN >> Voice OUI

Voice OUI Table

Showing All entries

Showing 1 to 8 of 8 entries

OUI

Description

00:E0:BB3COM

00:03:6BCisco

00:E0:75Veritel

00:D0:1EPingtel

00:01:E3Siemens

00:60:B9NEC/Philips

00:0F:E2H3C

00:09:6EAvaya

Add

Edit

Delete

First

Previous

1

Next

Last

Текущие OUI-адреса

Параметр	Описание
OUI	MAC-адрес производителя VoIP-устройства (первые 6 символов, например, 00-01-02).
Description	Описание производителя (например, "Cisco IP Phone").

Add Voice OUI

OUI	: :
Description	

Edit Voice OUI

OUI	00:E0:BB
Description	3COM

Добавление/редактирование OUI

Параметр	Описание
OUI	Введите OUI MAC-адрес (формат: XX-XX-XX или XXXXXX). Нельзя изменить при редактировании.
Description	Укажите описание (например, модель устройства или производитель).

Примечания:

1. **OUI (Organizationally Unique Identifier)** – уникальный идентификатор производителя сетевых устройств.
2. По умолчанию в таблице есть 8 предопределённых OUI (например, для Cisco).
3. Голосовая VLAN автоматически распознаёт трафик от устройств с указанными OUI.

Пример добавления OUI:

- **OUI:** A4-B1-C2
- **Description:** "Yealink IP Phone T4 Series"

Рекомендации:

- Добавляйте OUI для всех VoIP-устройств в сети.
- Используйте описания для удобства управления (например, "3CX Phones")

5.3. VLAN на основе протоколов (Protocol VLAN)

Раздел **Protocol VLAN** позволяет настраивать VLAN на основе типа протокола в заголовке пакета.

5.3.1. Группы протоколов VLAN (Protocol Group)

Для настройки групп протоколов:

Перейдите в раздел **VLAN > Protocol VLAN > Protocol Group**.

VLAN >> Protocol VLAN >> Protocol Group

Protocol Group Table

Showing entries Showing 1 to 3 of 3 entries

☐	Group ID	Frame Type	Protocol Value
☐	1	Ethernet_II	0x3333
☐	2	IEEE802.3_LLC_Other	0x4444
☐	3	RFC_1042	0x5555

Текущие группы протоколов

Параметр	Описание
Group ID	Идентификатор группы
Frame Type	Тип кадра
Protocol Value	Значение протокола в HEX формате. Пакеты с этим значением относятся к указанной VLAN.

Add Protocol Group

Group ID	4 ▼
Frame Type	Ethernet_II ▼
Protocol Value	0x (0x600 ~ 0xFFFE)

Edit Protocol Group

Group ID	1
Frame Type	Ethernet_II ▼
Protocol Value	0x 3333 (0x600 ~ 0xFFFE)

Добавление/редактирование группы

Параметр	Описание
Group ID	Выберите ID группы (1–8).
Frame Type	Укажите тип кадра из списка.
	Ethernet_II (например, для IP-трафика).
	IEEE802.3_LLC_Other (для протоколов с LLC-заголовком).
	RFC_1042 (для инкапсуляции IPX/SPX).
Protocol Value	Введите значение протокола (например, 0x0800 для IPv4). Пакеты с этим значением относятся к указанной VLAN.

Примечания:

- Protocol VLAN** используется для разделения трафика по типу протокола (например, IPv4, IPX, AppleTalk).
- Примеры Protocol Value:**

➤ 0x0800 – IPv4

- 0x0806 – ARP
- 0x8137 – IPX

Рекомендации:

- Для VoIP-трафика можно создать отдельную группу с типом **Ethernet_II** и значением 0x0800.
- Группы 1–8 позволяют гибко классифицировать трафик без использования тегов VLAN.

5.3.2. Привязка групп протоколов (Group Binding)

Для привязки групп протоколов к портам:

Перейдите в раздел **VLAN > Protocol VLAN > Group Binding**.

VLAN >> Protocol VLAN >> Group Binding

Group Binding Table

Showing All entries

Showing 1 to 1 of 1 entries

Q

	Port	Group ID	VLAN
☐	GE1	1	22

Add

Edit

Delete

First

Previous

1

Next

Last

Текущие привязки

Параметр	Описание
Port	Порт, привязанный к группе протоколов.
Group ID	Идентификатор группы протоколов (1–8).
VLAN	VLAN ID, назначаемый пакетам, соответствующим группе.

Add Group Binding

Port

Available Port

Selected Port

GE1

Note: Only VLAN Hybrid port can be set Protocol VLAN

Group ID 1 ▼

VLAN 2222 (1 - 4094)

Apply

Close

Настройка привязки

Параметр	Описание
Port	Выберите порты для привязки/отвязки от группы. Только порты в режиме Hybrid.
Group ID	Выберите Group ID (1–8) для ассоциации с портом.
VLAN	Укажите VLAN ID для пакетов, соответствующих группе.

Ключевые особенности:

1. **Только Hybrid-порты** могут быть привязаны к Protocol VLAN.
2. Пакеты, соответствующие группе, автоматически попадают в указанную VLAN.

Пример настройки:

- Порт 1:
 - **Group ID:** 1 (IPv4, 0x0800)
 - **VLAN:** 10

- Порт 2:
 - Group ID: 2 (IPX, 0x8137)
 - VLAN: 20

Примечания:

- Для работы Protocol VLAN убедитесь, что порты находятся в **Hybrid-режиме** (см. раздел 5.1.4).
- Приоритет Protocol VLAN выше, чем у Port-based VLAN.

5.4. MAC VLAN

Раздел **MAC VLAN** позволяет классифицировать трафик на основе MAC-адресов и назначать его определенным VLAN.

5.4.1. Настройка групп MAC-адресов (MAC Group)

Для настройки групп MAC-адресов:

Перейдите в раздел **VLAN > MAC VLAN > MAC Group**.

VLAN >> MAC VLAN >> MAC Group

MAC Group Table

Showing All entries Showing 1 to 3 of 3 entries

	Group ID	MAC Address	Mask
☐	1	02:03:04:05:06:07	48
☐	2	04:05:06:07:08:09	9
☐	3	AA:BB:CC:DD:EE:FF	32

Add Edit Delete

First Previous 1 Next Last

Текущие группы MAC-адресов

Параметр	Описание
Group ID	Уникальный идентификатор группы (1–2147483647).
MAC Address	MAC-адрес для классификации трафика.
Mask	Маска MAC-адреса (определяет, какие биты учитываются при классификации).

VLAN » MAC VLAN » MAC Group

Add MAC Group

Group ID		(1 - 2147483647)
MAC Address		
Mask		(9 - 48)

Edit MAC Group

Group ID	1	
MAC Address	02:03:04:05:06:07	
Mask	48	(9 - 48)

Добавление/редактирование группы

Параметр	Описание
Group ID	Введите уникальный ID группы (1–2147483647). Только при добавлении.
MAC Address	Укажите MAC-адрес (формат: XX-XX-XX-XX-XX-XX или XXXX.XXXX.XXXX).
Mask	Задайте маску для MAC-адреса (например, FF-FF-FF-00-00-00 для совпадения по первым 3 байтам).

Примечания:

1. **MAC VLAN** назначает VLAN на основе исходного MAC-адреса пакета.
2. **Маска** позволяет группировать устройства по производителю (OUI) или другим критериям.
 - Пример: Маска FF-FF-FF-00-00-00 + MAC 00-1A-2B-XX-XX-XX охватывает все устройства конкретного вендора.

Пример настройки:

- **Group ID:** 100
- **MAC Address:** 00-1A-2B-33-44-55
- **Mask:** FF-FF-FF-00-00-00 (совпадение для всех устройств с OUI 00-1A-2B).

Рекомендации:

- Используйте MAC VLAN для:
 - Автоматического распределения IP-телефонов в Voice VLAN.
 - Изоляции устройств IoT в отдельной VLAN.

5.4.2. Привязка групп MAC адресов (Group Binding)

Для привязки групп MAC-адресов к портам:

Перейдите в раздел **VLAN > MAC VLAN > Group Binding**.

VLAN >> MAC VLAN >> Group Binding

Group Binding Table

Showing All entries

Showing 1 to 1 of 1 entries

Port

Group ID

VLAN

GE1

1

3333

Add

Edit

Delete

First

Previous

1

Next

Last

Текущие привязки

Параметр	Описание
Port	Порт, привязанный к группе MAC-адресов.
Group ID	Идентификатор группы MAC (1–2147483647).
VLAN	VLAN ID, назначаемый пакетам, соответствующим группе.

VLAN >> MAC VLAN >> Group Binding

Add Group Binding

Port

Available Port

Selected Port

GE1

Note: Only VLAN Hybrid port can be set MAC VLAN

Group ID

1

VLAN

(1 - 4094)

Apply

Close

69

SEC.RU

Короткий путь к информации

Скачено с sec.ru

Port	GE1	
Group ID	1	
VLAN	3333	(1 - 4094)

Apply

Close

Настройка привязки

Параметр	Описание
Port	Выберите порты для привязки/отвязки. Только порты в режиме Hybrid.
Group ID	Выберите Group ID для ассоциации с портом.
VLAN	Укажите VLAN ID для пакетов, соответствующих группе MAC.

Ключевые особенности:

1. **Только Hybrid-порты** поддерживают привязку к MAC VLAN.
2. Пакеты с MAC-адресами, соответствующими группе, автоматически попадают в указанную VLAN.

Пример настройки:

- **Порт 1:**
 - **Group ID:** 100 (MAC-адреса 00-1A-2B-XX-XX-XX)
 - **VLAN:** 30 (VLAN для IP-телефонов)

Примечания:

- Убедитесь, что порты находятся в **Hybrid-режиме** (см. раздел 5.1.4).
- Приоритет MAC VLAN выше, чем у Port-based VLAN, но ниже, чем у Protocol VLAN.

5.5. VLAN для видеонаблюдения (Surveillance VLAN)

Раздел **Surveillance VLAN** предназначен для настройки VLAN, оптимизированной для передачи трафика видеокамер и систем безопасности.

5.5.1. Свойства (Property)

Для настройки глобальных параметров и параметров портов **Surveillance VLAN**:

Перейдите в раздел **VLAN > Surveillance VLAN > Property**

VLAN >> Surveillance VLAN >> Property

State	☒ Enable
VLAN	VLAN0002 ▾
CoS / 802.1p Remarking	☒ Enable 6 ▾
Aging Time	1440 Min (30 - 65536, default 1440)

Apply

Глобальные настройки Surveillance VLAN

Параметр	Описание
State	Включение/отключение функции Surveillance VLAN.
VLAN	Идентификатор Surveillance VLAN (не может совпадать с VLAN по умолчанию).
Cos/802.1p	Приоритет VLAN (VPT) для видео-трафика (0 –7).
Remarking	Включение/отключение перемаркировки приоритета (802.1p).
Aging Time	Время жизни записей Surveillance VLAN (по умолчанию: 1440 минут).

Port Setting Table

☐	Entry	Port	State	Mode	QoS Policy
☐	1	GE1	Disabled	Auto	Video Packet
☐	2	GE2	Disabled	Auto	Video Packet
☐	3	GE3	Disabled	Auto	Video Packet
☐	4	GE4	Disabled	Auto	Video Packet
☐	5	GE5	Disabled	Auto	Video Packet
☐	6	GE6	Disabled	Auto	Video Packet
☐	7	GE7	Disabled	Auto	Video Packet
☐	8	GE8	Disabled	Auto	Video Packet
☐	9	GE9	Disabled	Auto	Video Packet
☐	10	GE10	Disabled	Auto	Video Packet
☐	11	GE11	Disabled	Auto	Video Packet
☐	12	GE12	Disabled	Auto	Video Packet
☐	13	GE13	Disabled	Auto	Video Packet
☐	14	GE14	Disabled	Auto	Video Packet
☐	15	GE15	Disabled	Auto	Video Packet
☐	16	GE16	Disabled	Auto	Video Packet
☐	17	GE17	Disabled	Auto	Video Packet
☐	18	GE18	Disabled	Auto	Video Packet
☐	19	GE19	Disabled	Auto	Video Packet
☐	20	GE20	Disabled	Auto	Video Packet
☐	21	GE21	Disabled	Auto	Video Packet
☐	22	GE22	Disabled	Auto	Video Packet
☐	23	GE23	Disabled	Auto	Video Packet
☐	24	GE24	Disabled	Auto	Video Packet
☐	25	TE1	Disabled	Auto	Video Packet
☐	26	TE2	Disabled	Auto	Video Packet
☐	27	TE3	Disabled	Auto	Video Packet
☐	28	TE4	Disabled	Auto	Video Packet
☐	29	LAG1	Disabled	Auto	Video Packet
☐	30	LAG2	Disabled	Auto	Video Packet
☐	31	LAG3	Disabled	Auto	Video Packet
☐	32	LAG4	Disabled	Auto	Video Packet
☐	33	LAG5	Disabled	Auto	Video Packet
☐	34	LAG6	Disabled	Auto	Video Packet
☐	35	LAG7	Disabled	Auto	Video Packet
☐	36	LAG8	Disabled	Auto	Video Packet

Текущие параметры портов

Параметр	Описание
Port	Идентификатор порта.
State	Состояние Surveillance VLAN на порту (вкл./выкл.).
Mode	Режим работы Surveillance VLAN (Auto/Manual).
QoS Policy	Тип пакетов, к которым применяются QoS-атрибуты.

Edit Port Setting

Port	GE6
State	☒ Enable
Mode	☒ Auto ☐ Manual
QoS Policy	☒ Video Packet ☐ All

Редактирование параметров портов

Параметр	Описание
Port	Выбранный порт.
State	Включение/отключение Surveillance VLAN на порту.
Mode	Выберите режим работы:
	Auto – автоматическое добавление порта в VLAN при обнаружении видео-трафика.
	Manual – ручное добавление порта в VLAN.
QoS Policy	Политика QoS:
	Video Packet – QoS применяется только к пакетам с MAC-адресами из OUI-таблицы.
	All – QoS применяется ко всем пакетам в Surveillance VLAN.

Примечания:

1. **OUI (Organizationally Unique Identifier)** – идентификатор производителя камер (например, Hikvision, Dahua).
2. **Режим Auto** удобен для IP-камер, которые автоматически определяются по MAC-адресу.
3. **Приоритет (802.1p)** обеспечивает минимальные задержки для видео-трафика.

Рекомендации:

- Используйте **VLAN ID**, отличный от VLAN по умолчанию (VID 1).
- Для IP-камер с PoE предпочтителен режим **Auto**.
- Настройте **QoS Policy** на **Video Packet** для приоритизации видео-потоков.

5.5.2. Настройка OUI адресов для видеонаблюдения (Surveillance OUI)

Для настройки OUI-адресов устройств видеонаблюдения (IP-камер, видеорегистраторов):

Перейдите в раздел **VLAN > Surveillance VLAN > Surveillance OUI**.

VLAN >> Surveillance VLAN >> Surveillance OUI

Surveillance OUI Table

Showing All entriesShowing 0 to 0 of 0 entries

OUI

Description

0 results found.

Add

Edit

Delete

First

Previous

1

Next

Last

Текущие OUI-адреса

Параметр	Описание
OUI	MAC-адрес производителя (первые 6 символов, например, A0-B1-C2).
Description	Описание устройства (например, "Hikvision IP Camera").

74

SEC.RU | Короткий путь к информации

Скачано с sec.ru

Add Surveillance OUI

OUI	: :
Description	

Добавление/редактирование OUI

Параметр	Описание
OUI	Введите OUI MAC-адрес (формат: XX-XX-XX). Не редактируется при изменении записи.
Description	Укажите описание устройства.

Примечания:

- OUI** позволяет автоматически классифицировать трафик от камер в Surveillance VLAN.
- Примеры OUI популярных производителей:
 - Hikvision: 34-CE-00, A4-42-3B
 - Dahua: B8-78-26, D4-EE-07
 - Axis: 00-40-8C, AC-CC-8E

Рекомендации:

- Добавляйте OUI всех камер в сети для автоматического определения.
- Используйте описания для удобства управления (например, "Камера купольная Hikvision DS-2CD2143G0").

5.6. GVRP (GARP VLAN Registration Protocol)

5.6.1. Свойства (Property)

Для настройки глобальных и портовых параметров GVRP:

Перейдите в раздел **VLAN > GVRP > Property**

VLAN >> GVRP >> Property

State ☐ Enable

Operational Timeout

Join	20 ms
Leave	60 ms
LeaveAll	1000 ms

Apply

Глобальные настройки GVRP

Параметр	Описание
State	Включение/отключение функции GVRP:
	Enable – активирует динамическую регистрацию VLAN между коммутаторами.
Operational Timeout	Таймауты GVRP:
	Join – время ожидания присоединения к VLAN.
	Leave – время ожидания выхода из VLAN.
	Leave All – время ожидания полного выхода из всех VLAN.

☐	Entry	Port	State	VLAN Creation	Registration
☐	1	GE1	Disabled	Enabled	Normal
☐	2	GE2	Disabled	Enabled	Normal
☐	3	GE3	Disabled	Enabled	Normal
☐	4	GE4	Disabled	Enabled	Normal
☐	5	GE5	Disabled	Enabled	Normal
☐	6	GE6	Disabled	Enabled	Normal
☐	7	GE7	Disabled	Enabled	Normal
☐	8	GE8	Disabled	Enabled	Normal
☐	9	GE9	Disabled	Enabled	Normal
☐	10	GE10	Disabled	Enabled	Normal
☐	11	GE11	Disabled	Enabled	Normal
☐	12	GE12	Disabled	Enabled	Normal
☐	13	GE13	Disabled	Enabled	Normal
☐	14	GE14	Disabled	Enabled	Normal
☐	15	GE15	Disabled	Enabled	Normal
☐	16	GE16	Disabled	Enabled	Normal
☐	17	GE17	Disabled	Enabled	Normal
☐	18	GE18	Disabled	Enabled	Normal
☐	19	GE19	Disabled	Enabled	Normal
☐	20	GE20	Disabled	Enabled	Normal
☐	21	GE21	Disabled	Enabled	Normal
☐	22	GE22	Disabled	Enabled	Normal
☐	23	GE23	Disabled	Enabled	Normal
☐	24	GE24	Disabled	Enabled	Normal
☐	25	TE1	Disabled	Enabled	Normal
☐	26	TE2	Disabled	Enabled	Normal
☐	27	TE3	Disabled	Enabled	Normal
☐	28	TE4	Disabled	Enabled	Normal
☐	29	LAG1	Disabled	Enabled	Normal
☐	30	LAG2	Disabled	Enabled	Normal
☐	31	LAG3	Disabled	Enabled	Normal
☐	32	LAG4	Disabled	Enabled	Normal
☐	33	LAG5	Disabled	Enabled	Normal
☐	34	LAG6	Disabled	Enabled	Normal
☐	35	LAG7	Disabled	Enabled	Normal
☐	36	LAG8	Disabled	Enabled	Normal

Edit

Текущие параметры портов

Параметр	Описание
Port	Имя порта.
State	Состояние GVRP на порту (вкл./выкл.).
VLAN Creation	Возможность создания динамических VLAN.
Registration	Режим регистрации:
	Normal – стандартный режим.
	Fixed – только статические VLAN.
	Forbidden – запрет динамических VLAN.

Edit Port Setting

Port	GE1,GE3
State	☐ Enable
VLAN Creation	☒ Enable
Registration	☒ Normal ☐ Fixed ☐ Forbidden

Apply

Close

Настройка параметров портов

Параметр	Описание
Port	Выбранные порты.
State	Включение/отключение GVRP на порту.
Vlan Creation	Разрешение создания динамических VLAN на порту.
Register Mode	Выберите режим регистрации:
	Normal – полная поддержка GVRP.
	Fixed – передача только статических VLAN.
	Forbidden – разрешён только трафик VLAN по умолчанию.

Примечания:

- GVRP** упрощает управление VLAN в крупных сетях, автоматически распространяя информацию о VLAN между коммутаторами.
- Режимы портов:**
 - **Normal** – рекомендуется для портов, подключённых к другим коммутаторам.
 - **Fixed/Forbidden** – для портов с конечными устройствами (повышает безопасность).

Рекомендации:

- Для динамических VLAN используйте **Join Timeout = 20 сек, Leave Timeout = 60 сек.**
- На edge-портах (ПК, камеры) активируйте режим **Forbidden.**

5.6.2. Настройка VLAN Membership (Membership)

Для просмотра и управления VLAN, зарегистрированными через GVRP:

Перейдите в раздел **VLAN > GVRP > Membership.**

VLAN >> GVRP >> Membership

Membership Table

Showing All entries Showing 1 to 1 of 1 entries

VLAN	Member	Dynamic Member	Type
1	GE1-GE10,LAG1-LAG8		Static

First Previous 1 Next Last

Информация о VLAN

Параметр	Описание
VLAN ID	Идентификатор VLAN.
Member	Порты-участники VLAN (включая статические и динамические).
Dynamic Member	Порты, добавленные автоматически через GVRP.
Type	Тип VLAN:
	Static – создана вручную.
	Dynamic – зарегистрирована через GVRP.

Примечания:

- 1. **Динамические VLAN** автоматически появляются/исчезают при изменении топологии сети.
- 2. **Статические VLAN** требуют ручной настройки и не удаляются GVRP.

Пример:

- **VLAN 10:**
 - **Member:** Port 1 (Static), Port 5 (Dynamic)
 - **Vlan Type:** Static

5.6.3. Статистика GVRP (Statistics)

Для просмотра статистики работы GVRP на портах:

Перейдите в раздел **VLAN > GVRP > Statistics**

VLAN >> GVRP >> Statistics

Port

GE1

Statistics

☒ All

☐ Receive

☐ Transmit

☐ Error

Refresh Rate

☐ None

☐ 5 sec

☒ 10 sec

☐ 30 sec

Clear

Параметры отображения статистики

Параметр	Описание
Port	Идентификатор порта.

Параметр	Описание
Statistics	Тип отображаемой статистики:
	All – вся статистика (прием, передача, ошибки).
	Receive – только входящие сообщения GVRP.
	Transmit – только исходящие сообщения GVRP.
	Error – только ошибочные сообщения.
Refresh Rate	Частота обновления данных:
	None – без автоматического обновления.
	5 sec – каждые 5 секунд.
	10 sec – каждые 10 секунд.
	30 sec – каждые 30 секунд.

Receive	
Join empty	0
Empty	0
Leave Empty	0
Join In	0
Leave In	0
Leave All	0
Transmit	
Join empty	0
Empty	0
Leave Empty	0
Join In	0
Leave In	0
Leave All	0
Error	
Invalid Protocol ID	0
Invalid Attribute Type	0
Invalid Attribute Value	0
Invalid Attribute Length	0
Invalid Event	0

Детальная статистика GVRP

Параметр	Описание
Join Empty	Количество полученных/переданных сообщений Join Empty.
Empty	Количество полученных/переданных сообщений Empty.
Leave Empty	Количество полученных/переданных сообщений Leave Empty.
Join In	Количество полученных/переданных сообщений Join In.
Leave In	Количество полученных/переданных сообщений Leave In.
Leave All	Количество полученных/переданных сообщений Leave All.
Invalid Protocol ID	Количество ошибок "Неверный ID протокола".
Invalid Attribute Type	Количество ошибок "Неверный тип атрибута".
Invalid Attribute Value	Количество ошибок "Неверное значение атрибута".
Invalid Attribute Length	Количество ошибок "Неверная длина атрибута".
Invalid Event	Количество ошибок "Неверное событие".

Примечания:

1. **Join/Leave** – сообщения о подключении/отключении VLAN.
2. Высокое количество ошибок может указывать на:
 - Несовместимость оборудования.
 - Проблемы с кабелями или портами.

Рекомендации:

- Для диагностики используйте **Refresh Rate = 5 sec.**
- Очищайте статистику (**Clear**) после изменений конфигурации.

6. Таблица MAC-адресов (MAC Address Table)

Раздел **MAC Address Table** отображает динамические MAC-адреса и позволяет настраивать статические записи.

6.1. Динамические адреса (Dynamic Address)

Для настройки времени старения динамических MAC-адресов:

Перейдите в раздел **MAC Address Table > Dynamic Address**.

MAC Address Table >> Dynamic Address

Aging Time

300

Sec (10 - 630, default 300)

Apply

Dynamic Address Table

Showing All entries

Showing 1 to 1 of 1 entries

Q

	VLAN	MAC Address	Port
☐	1	00:0E:C6:D8:58:EC	GE8

Refresh

Add Static Address

First

Previous

1

Next

Last

Параметр	Описание
Aging Time	Время (в секундах), в течение которого запись хранится в таблице MAC-адресов.
	Диапазон: 10–630 секунд.
	По умолчанию: 300 секунд (5 минут).

Примечания:

1. **Динамические MAC-адреса** автоматически добавляются в таблицу при прохождении трафика через порт.
2. **Слишком короткое** время старения (Aging Time) может привести к:
 - Увеличению широковещательного трафика (частые запросы ARP).
 - Нестабильности коммутации в целом.
3. **Слишком долгое** время старения (Aging Time) занимает память коммутатора.

Рекомендации:

- Для сетей с мобильными устройствами (Wi-Fi) используйте **300 секунд**.
- Для статичных сетей (серверы) можно увеличить до **600 секунд**.

6.2. Статические MAC-адреса (Static Address)

Для просмотра и настройки статических MAC-адресов:

Перейдите в раздел **MAC Address Table > Static Address**.

MAC Address Table >> Static Address

Static Address Table

Showing All entries Showing 0 to 0 of 0 entries

☐	VLAN	MAC Address	Port
0 results found.			

Параметры статических записей

Параметр	Описание
----------	----------

Параметр	Описание
VLAN	Укажите VLAN, чтобы отобразить или очистить записи MAC-адресов.
MAC Address	MAC-адрес устройства, для которого настроена статическая переадресация трафика.
Port	Порт, к которому привязан MAC-адрес.

Примечания:

1. **Статические MAC-адреса** не удаляются автоматически и имеют приоритет над динамическими.
2. Используйте для:
 - Критически важных устройств (серверы, маршрутизаторы).
 - Защиты от спуфинга MAC-адресов.

Пример:

- **MAC Address:** 00:1A:2B:3C:4D:5E
- **VLAN:** 10
- **Port:** GigabitEthernet 1/0/24

6.3. Фильтрация MAC-адресов (Filtering Address)

Для настройки фильтрации MAC-адресов:

Перейдите в раздел **MAC Address Table > Filtering Address**.

MAC Address Table >> Filtering Address

Filtering Address Table

Showing All entries Showing 1 to 1 of 1 entries

VLAN

MAC Address

1

00:00:00:00:00:02

Add

Edit

Delete

First

Previous

1

Next

Last

Параметры фильтрации

Параметр	Описание
VLAN	VLAN ID, к которому применяется фильтр (опционально).
MAC Address	Укажите MAC-адрес, пакеты с которым будут отбрасываться.

Примечания:

1.

Фильтрация блокирует трафик от/к указанному MAC-адресу.

2.

Используйте для:

➤

Блокировки неавторизованных устройств.

➤

Защиты от атак (например, MAC-флудинг).

Пример:

•

MAC Address: 00:1A:2B:3C:4D:5E

•

VLAN: 10 (если нужно ограничить фильтр конкретной VLAN)

7. STP (Spanning Tree Protocol)

STP (Spanning Tree Protocol) – канальный протокол. Основной задачей STP является устранение петель в топологии произвольной сети

86

“ »

SEC.RU

Короткий путь к информации

Скачено с sec.ru

Ethernet, в которой есть один или более сетевых мостов, связанных избыточными соединениями. STP решает эту задачу, автоматически блокируя соединения, которые в данный момент для полной связности коммутаторов являются избыточными.

7.1. Свойства STP (Property)

Для настройки глобальных параметров STP:

Перейдите в раздел **Spanning Tree > Property**.

Spanning Tree >> Property

State

☐ Enable

Operation Mode

☐ STP
☒ RSTP
☐ MSTP

Path Cost

☒ Long
☐ Short

BPDU Handling

☐ Filtering
☒ Flooding

Priority

(0 - 61440, default 32768)

Hello Time

Sec (1 - 10, default 2)

Max Age

Sec (6 - 40, default 20)

Forward Delay

Sec (4 - 30, default 15)

Tx Hold Count

(1 - 10, default 6)

Region Name

Revision

(0 - 65535, default 0)

Max Hop

(1 - 40, default 20)

Operational Status

Bridge Identifier

32768-00:E0:4C:00:00:00

Designated Root Bridge

0-00:00:00:00:00:00

Root Port

N/A

Root Path Cost

0

Topology Change Count

0

Last Topology Change

0D/0H/0M/0S

Apply

Основные параметры STP

Параметр	Описание
----------	----------

Параметр	Описание
State	Включение/отключение STP на коммутаторе.
Operation Mode	Режим работы STP:
	STP – стандартный протокол (IEEE 802.1D).
	RSTP – Rapid STP (IEEE 802.1w).
	MSTP – Multiple STP (IEEE 802.1s).
Path Cost	Метод расчета стоимости пути:
	Long – диапазон 1–200,000,000.
	Short – диапазон 1–65,535.
BPDU Handling	Обработка BPDU при отключенном STP:
	Filtering – блокировка BPDU.
	Flooding – широковещательная рассылка BPDU.
Priority	Приоритет коммутатора (0–61440 с шагом 4096). Чем меньше значение, тем выше вероятность стать корневым мостом.
Hello Time	Интервал отправки BPDU (1–10 секунд).
Max Age	Максимальное время ожидания BPDU (6–40 секунд).
Forward Delay	Время перехода порта в состояние Forwarding (4–30 секунд).
TX Hold Count	Максимальное количество BPDU в секунду (1–10).
Region Name	Имя региона MSTP (до 32 символов). По умолчанию – MAC-адрес коммутатора.
Revision	Номер ревизии MSTP (0–65535).
Max Hops	Максимальное количество прыжков (хопов) BPDU в регионе MSTP (1–40).

Текущее состояние STP

Параметр	Описание
Bridge Identifier	Идентификатор моста (приоритет + MAC).
Designated Root Identifier	Идентификатор корневого моста.
Root Port	Порт, ведущий к корневому мосту.
Root Path Cost	Суммарная стоимость пути к корневому мосту.
Topology Change Count	Количество изменений топологии.
Last Topology Change	Время последнего изменения топологии.

Примечания:

1. **RSTP/MSTP** рекомендуется для современных сетей (быстрее реагируют на изменения).
2. **Приоритет:**
 - По умолчанию: 32768.
 - Для назначения корневым мостом установите **0** или **4096**.

Пример настройки:

- **Operation Mode:** RSTP
- **Priority:** 4096
- **Hello Time:** 2 сек
- **Forward Delay:** 15 сек

7.2. Настройка портов STP (Port Setting)

Для настройки параметров STP на портах:

Перейдите в раздел **Spanning Tree > Port Setting**.

☐	Entry	Port	State	Path Cost	Priority	BPDU Filter	BPDU Guard	Operational Edge	Operational Point-to-Point	Port Role	Port State
☐	1	GE1	Disabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled
☐	2	GE2	Disabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled
☐	3	GE3	Disabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled
☐	4	GE4	Disabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled
☐	5	GE5	Disabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled
☐	6	GE6	Disabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled
☐	7	GE7	Disabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled
☐	8	GE8	Disabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled
☐	9	GE9	Disabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled
☐	10	GE10	Disabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled
☐	11	GE11	Disabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled
☐	12	GE12	Disabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled
☐	13	GE13	Disabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled
☐	14	GE14	Disabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled
☐	15	GE15	Disabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled
☐	16	GE16	Disabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled
☐	17	GE17	Disabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled
☐	18	GE18	Disabled	20000	128	Disabled	Disabled	Disabled	Enabled	Disabled	Forwarding
☐	19	GE19	Disabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled
☐	20	GE20	Disabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled
☐	21	GE21	Disabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled
☐	22	GE22	Disabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled
☐	23	GE23	Disabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled
☐	24	GE24	Disabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled
☐	25	TE1	Disabled	2000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled
☐	26	TE2	Disabled	2000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled
☐	27	TE3	Disabled	2000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled
☐	28	TE4	Disabled	2000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled
☐	29	LA01	Disabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled
☐	30	LA02	Disabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled
☐	31	LA03	Disabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled
☐	32	LA04	Disabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled
☐	33	LA05	Disabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled
☐	34	LA06	Disabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled
☐	35	LA07	Disabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled
☐	36	LA08	Disabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled

Текущие параметры портов

Параметр	Описание
Port	Идентификатор порта.
State	Текущее состояние STP на порту (вкл./выкл.).
Path Cost	Стоимость пути STP (влияет на выбор корневого пути).
Priority	Приоритет порта (0–240 с шагом 16).
BPDU Filter	Фильтрация BPDU (вкл./выкл.).
BPDU Guard	Защита от BPDU (вкл./выкл.).
Operational Edge	Режим Edge Port (автоматический переход в Forwarding).

Параметр	Описание
Operational Point-to-Point	Режим точка-точка (зависит от дуплекса).
Port Role	Роль порта: Disabled, Master, Root, Designated, Alternative, Backup.
Port State	Состояние порта: Disabled, Discarding, Learning, Forwarding.
Designated Bridge	Идентификатор назначенного моста.
Designated Port ID	Идентификатор назначенного порта.
Designated Cost	Стоимость пути назначенного порта.

Spanning Tree >> Port Setting

Edit Port Setting

Port	GE1-GE4
State	☒ Enable
Path Cost	0 (0 - 200000000) (0 = Auto)
Priority	128 ▼
Edge Port	☐ Enable
BPDU Filter	☐ Enable
BPDU Guard	☐ Enable
Point-to-Point	☒ Auto ☐ Enable ☐ Disable
Port State	Disabled
Designated Bridge	0-00:00:00:00:00:00
Designated Port ID	128-1
Designated Cost	20000
Operational Edge	False
Operational Point-to-Point	False

Apply

Close

Редактирование параметров портов

Параметр	Описание
State	Включение/отключение STP на порту.
Path Cost	Укажите стоимость пути (1–200,000,000 для Long , 1–65,535 для Short).
Priority	Приоритет порта (0–240, шаг 16).
Edge Port	Режим Edge Port:
	Enable – для портов, подключенных к конечным устройствам (быстрый переход в состояние Forwarding).
	Disable – для соединений между коммутаторами.
BPDU Filter	Блокировка отправки/приема BPDU:
	Enable – фильтрация активирована.
	Disable – фильтрация отключена.
BPDU Guard	Защита от BPDU (отключение порта при получении BPDU):
	Enable – защита активирована.
	Disable – защита отключена.
Point-to-Point	Режим точка-точка:
	Auto – определяется автоматически (полный дуплекс = точка-точка).
	Enable – принудительное включение.
	Disable – принудительное отключение.

Примечания:

1. **Edge Port** следует включать только для портов, подключенных к конечным устройствам (ПК, IP-телефоны).
2. **BPDU Guard** защищает от петель при ошибочном подключении коммутатора к Edge Port.

3. **Path Cost** влияет на выбор корневого пути (меньшее значение = предпочтительный путь).

Пример настройки:

- **Порт 1 (Edge Port):**
 - **State:** Enabled
 - **Edge Port:** Enable
 - **BPDU Guard:** Enable
- **Порт 24 (Trunk):**
 - **Path Cost:** 2000
 - **Priority:** 32

7.3. Настройка MST Instance (MST Instance)

Для настройки MSTP (Multiple Spanning Tree Protocol):

Перейдите в раздел **Spanning Tree > MST Instance**.

Spanning Tree >> MST Instance

MST Instance Table

	MSTI	Priority	Bridge Identifier	Designated Root Bridge	Root Port	Root Path Cost	Remaining Hop	VLAN
○	0	32768	32768-00:E0:4C:00:00:00	0-00:00:00:00:00:00	N/A	0	0	1-4094
○	1	32768	32768-00:E0:4C:00:00:00	0-00:00:00:00:00:00	N/A	0	0	
○	2	32768	32768-00:E0:4C:00:00:00	0-00:00:00:00:00:00	N/A	0	0	
○	3	32768	32768-00:E0:4C:00:00:00	0-00:00:00:00:00:00	N/A	0	0	
○	4	32768	32768-00:E0:4C:00:00:00	0-00:00:00:00:00:00	N/A	0	0	
○	5	32768	32768-00:E0:4C:00:00:00	0-00:00:00:00:00:00	N/A	0	0	
○	6	32768	32768-00:E0:4C:00:00:00	0-00:00:00:00:00:00	N/A	0	0	
○	7	32768	32768-00:E0:4C:00:00:00	0-00:00:00:00:00:00	N/A	0	0	
○	8	32768	32768-00:E0:4C:00:00:00	0-00:00:00:00:00:00	N/A	0	0	
○	9	32768	32768-00:E0:4C:00:00:00	0-00:00:00:00:00:00	N/A	0	0	
○	10	32768	32768-00:E0:4C:00:00:00	0-00:00:00:00:00:00	N/A	0	0	
○	11	32768	32768-00:E0:4C:00:00:00	0-00:00:00:00:00:00	N/A	0	0	
○	12	32768	32768-00:E0:4C:00:00:00	0-00:00:00:00:00:00	N/A	0	0	
○	13	32768	32768-00:E0:4C:00:00:00	0-00:00:00:00:00:00	N/A	0	0	
○	14	32768	32768-00:E0:4C:00:00:00	0-00:00:00:00:00:00	N/A	0	0	
○	15	32768	32768-00:E0:4C:00:00:00	0-00:00:00:00:00:00	N/A	0	0	

Edit

Текущие параметры MST Instance

Параметр	Описание
MSTI	Идентификатор MST Instance (0–15).
Priority	Приоритет моста для указанного MST Instance (0–61440, шаг 4096).
Bridge Identifier	Идентификатор моста (приоритет + MAC) для MST Instance.
Designated Root Bridge	Идентификатор корневого моста для MST Instance.
Root Port	Корневой порт для MST Instance.
Root Path Cost	Стоимость пути к корневому мосту.
Remaining Hop	Оставшееся количество прыжков (хопов) BPDU.
VLAN	Список VLAN, сопоставленных с MST Instance.

Spanning Tree » MST Instance

Edit MST Instance Setting

MSTI	1	
VLAN	Available VLAN	Selected VLAN
	1	
	2	
	3	
	4	
	5	
	6	
	7	
8		
Priority	32768	(0 - 61440, default 32768)
Bridge Identifier	32768-00:E0:4C:00:00:00	
Designated Root Bridge	0-00:00:00:00:00:00	
Root Port		
Root Path Cost	0	
Remaining Hop	0	

Apply

Close

Настройка MST Instance

Параметр	Описание
VLAN	Выберите VLAN для сопоставления с MST Instance.
Priority	Укажите приоритет моста (0–61440, шаг 4096). Чем меньше значение, тем выше вероятность стать корневым мостом.

Примечания:

1. **MSTI 0** (по умолчанию) включает все VLAN, не назначенные вручную другим MST Instance.
2. **Приоритет:**
 - По умолчанию: 32768.
 - Для назначения корневым мостом установите **0** или **4096**.

Пример настройки:

- **MSTI 1:**
 - **VLAN:** 10, 20, 30
 - **Priority:** 4096
- **MSTI 2:**
 - **VLAN:** 40, 50
 - **Priority:** 8192

7.4. Настройка портов MST (MST Port Setting)

Для настройки параметров портов в MSTP:

Перейдите в раздел **Spanning Tree > MST Port Setting**.

Spanning Tree >> MST Port Setting

MST Port Setting Table

MSTI 0

	Entry	Port	Path Cost	Priority	Port Role	Port State	Mode	Type	Designated Bridge	Designated Port ID	Designated Cost	Remu
☐	1	GE1	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-1	0	
☐	2	GE2	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-2	0	
☐	3	GE3	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-3	0	
☐	4	GE4	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-4	0	
☐	5	GE5	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-5	0	
☐	6	GE6	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-6	0	
☐	7	GE7	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-7	0	
☐	8	GE8	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-8	0	
☐	9	GE9	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-9	0	
☐	10	GE10	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-10	0	
☐	11	GE11	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-11	0	
☐	12	GE12	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-12	0	
☐	13	GE13	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-13	0	
☐	14	GE14	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-14	0	
☐	15	GE15	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-15	0	
☐	16	GE16	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-16	0	
☐	17	GE17	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-17	0	
☐	18	GE18	20000	128	Disabled	Forwarding	RSTP	Boundary	0-00:00:00:00:00:00	128-18	0	
☐	19	GE19	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-19	0	
☐	20	GE20	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-20	0	
☐	21	GE21	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-21	0	
☐	22	GE22	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-22	0	
☐	23	GE23	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-23	0	
☐	24	GE24	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-24	0	
☐	25	TE1	2000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-25	0	
☐	26	TE2	2000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-26	0	
☐	27	TE3	2000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-27	0	
☐	28	TE4	2000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-28	0	
☐	29	LAG1	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-29	0	
☐	30	LAG2	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-30	0	
☐	31	LAG3	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-31	0	
☐	32	LAG4	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-32	0	
☐	33	LAG5	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-33	0	
☐	34	LAG6	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-34	0	
☐	35	LAG7	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-35	0	

Текущие параметры портов MST

Параметр	Описание
MSTI	Идентификатор MST Instance (0–15).
Port	Идентификатор порта.
Path Cost	Стоимость пути порта для указанного MST Instance.
Priority	Приоритет порта (0–240, шаг 16).
Port Role	Роль порта: Disabled, Master, Root, Designated, Alternative, Backup.
Port State	Состояние порта: Disabled, Discarding, Learning, Forwarding.
Mode	Режим STP на порту (STP/RSTP/MSTP).
Type	Тип порта:
	Boundary – подключен к устройству вне региона MST.
	Internal – подключен к устройству внутри региона MST.
Designated Bridge	Идентификатор назначенного моста.
Designated Port ID	Идентификатор назначенного порта.
Designated Cost	Стоимость пути назначенного порта.
Remaining Hop	Оставшееся количество прыжков (хопов) BPDU.

Edit MST Port Setting

MSTI	0
Port	GE1-GE4
Path Cost	0 (0 - 200000000) (0 = Auto)
Priority	128 ▾
Port Role	Disabled
Port State	Disabled
Mode	RSTP
Type	Boundary
Designated Bridge	0-00:00:00:00:00:00
Designated Port ID	128-1
Designated Cost	20000
Remaining Hop	20

Редактирование параметров портов

Параметр	Описание
Path Cost	Укажите стоимость пути порта для MST Instance.
Priority	Укажите приоритет порта (0–240, шаг 16).

Примечания:

1. **Path Cost** влияет на выбор корневого пути в рамках MST Instance.
2. **Тип порта:**
 - **Boundary** – требует особого внимания (риск петель между регионами).
 - **Internal** – стандартный порт внутри региона MST.

Пример настройки:

- **MSTI 1, Порт 24:**
 - **Path Cost:** 2000
 - **Priority:** 32
 - **Type:** Boundary

7.5. Статистика STP (Statistics)

Для просмотра статистики работы STP:

Перейдите в раздел **Spanning Tree > Statistics**.

Spanning Tree >> Statistics

Statistics Table

Refresh Rate 0 sec

	Entry	Port	Receive BPDU			Transmit BPDU		
			Config	TCN	MSTP	Config	TCN	MSTP
☐	1	GE1	0	0	0	0	0	0
☐	2	GE2	0	0	0	0	0	0
☐	3	GE3	0	0	0	0	0	0
☐	4	GE4	0	0	0	0	0	0
☐	5	GE5	0	0	0	0	0	0
☐	6	GE6	0	0	0	0	0	0
☐	7	GE7	0	0	0	0	0	0
☐	8	GE8	0	0	0	0	0	0
☐	9	GE9	0	0	0	0	0	0
☐	10	GE10	0	0	0	0	0	0
☐	11	GE11	0	0	0	0	0	0
☐	12	GE12	0	0	0	0	0	0
☐	13	GE13	0	0	0	0	0	0
☐	14	GE14	0	0	0	0	0	0
☐	15	GE15	0	0	0	0	0	0
☐	16	GE16	0	0	0	0	0	0
☐	17	GE17	0	0	0	0	0	0
☐	18	GE18	0	0	0	0	0	0
☐	19	GE19	0	0	0	0	0	0
☐	20	GE20	0	0	0	0	0	0
☐	21	GE21	0	0	0	0	0	0
☐	22	GE22	0	0	0	0	0	0
☐	23	GE23	0	0	0	0	0	0
☐	24	GE24	0	0	0	0	0	0
☐	25	TE1	0	0	0	0	0	0
☐	26	TE2	0	0	0	0	0	0
☐	27	TE3	0	0	0	0	0	0
☐	28	TE4	0	0	0	0	0	0
☐	29	LAG1	0	0	0	0	0	0
☐	30	LAG2	0	0	0	0	0	0
☐	31	LAG3	0	0	0	0	0	0
☐	32	LAG4	0	0	0	0	0	0
☐	33	LAG5	0	0	0	0	0	0
☐	34	LAG6	0	0	0	0	0	0
☐	35	LAG7	0	0	0	0	0	0

Параметры статистики

Параметр	Описание
Refresh Rate	Частота автоматического обновления статистики.
Receive BPDU (Config)	Количество полученных BPDU типа Configuration .
Receive BPDU (TCN)	Количество полученных BPDU типа Topology Change Notification (TCN) .

Параметр	Описание
Receive BPDU (MSTP)	Количество полученных BPDU для MSTP .
Transmit BPDU (Config)	Количество отправленных BPDU типа Configuration .
Transmit BPDU (TCN)	Количество отправленных BPDU типа TCN .
Transmit BPDU (MSTP)	Количество отправленных BPDU для MSTP .

Параметр	Описание
Clear	Очистка статистики для выбранных интерфейсов.
View	Просмотр статистики для интерфейса.

Spanning Tree » Statistics

STP Port Statistic

Port	GE7
Refresh Rate	☒ None ☐ 5 sec ☐ 10 sec ☐ 30 sec
Receive BPDU	
Config	0
TCN	0
MSTP	0
Transmit BPDU	
Config	0
TCN	0
MSTP	0

Refresh

Clear

Close

Примечания:

1. **BPDU (Bridge Protocol Data Unit)** – служебные кадры STP для обмена информацией между коммутаторами.
 - **Configuration BPDU** – используются для построения дерева.
 - **TCN BPDU** – уведомления об изменении топологии.
2. Высокое количество **TCN BPDU** может указывать на нестабильность сети.

Рекомендации:

- Для диагностики используйте **Refresh Rate = 5 sec**.
- Очищайте статистику (**Clear**) после изменений конфигурации.

8. ERPS (Ethernet Ring Protection Switching)

ERPS – протокол защиты кольцевых сетей Ethernet, разработанный ITU-T. Обеспечивает телекоммуникационную надежность с быстрой сходимостью (<50 мс).

Ключевые термины ERPS

1. **ERPS Instance**
 - Аналог домена ERPP.
 - Группа коммутаторов с одинаковым **ID экземпляра** и **Control VLAN**.
2. **Control VLAN**
 - VLAN для передачи служебных кадров ERPS.
3. **RPL (Ring Protection Link)**
 - Заблокированная в штатном режиме связь для предотвращения петель.
4. **Типы узлов:**
 - **RPL Owner** – узел с портом, блокирующим RPL.

- **RPL Neighbour** – узел, подключенный к RPL Owner.
- **Common** – обычные узлы.

5. Состояния портов:

- **Forwarding** – передача трафика и R-APS сообщений.
- **Discarding** – только прием/отправка R-APS.
- **Disable** – порт отключен.

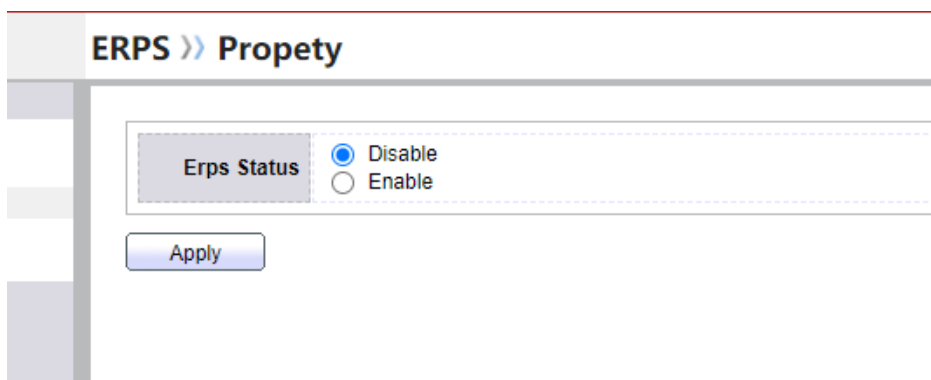
6. Режимы работы:

- **Revertive** – автоматическое восстановление RPL после устранения неисправности.
- **Non-Revertive** – RPL остается разблокированным после восстановления.

8.1. Общие настройки ERPS (Property)

Чтобы включить/отключить ERPS:

Перейдите в раздел **ERPS > Property**.



The screenshot shows a web interface for configuring ERPS properties. The breadcrumb path is 'ERPS >> Property'. The main configuration area is titled 'Erps Status' and contains two radio buttons: 'Disable' (which is selected) and 'Enable'. Below these buttons is an 'Apply' button.

Параметр	Описание
Disable	Отключить ERPS (по умолчанию)
Enable	Включить ERPS

8.2. Настройка ERPS Instance (ERPS Instance)

Для управления экземплярами ERPS:

1. Перейдите в раздел **ERPS > ERPS Instance**.
2. Возможности:
 - Изменение/удаление (Edit/Delete).
 - Просмотр параметров.

ERPS >> ERPS Instance

Erps Instance (0 - 15)

Apply

ERPS Instance Setting

☐	Instance	Ring Status	MeI	Control Vlan	WTR Time	Guard Time	Work Mode	Ring ID	Ring Type	Pr
☐	Ins0	---					---			
☐	Ins1	---					---			
☐	Ins2	---					---			
☐	Ins3	---					---			
☐	Ins4	---					---			
☐	Ins5	---					---			
☐	Ins6	---					---			
☐	Ins7	---					---			
☐	Ins8	---					---			
☐	Ins9	---					---			
☐	Ins10	---					---			
☐	Ins11	---					---			
☐	Ins12	---					---			
☐	Ins13	---					---			
☐	Ins14	---					---			
☐	Ins15	---					---			

EditDelete

Примечания:

- Все узлы кольца должны использовать одинаковые **Control VLAN** и **ID экземпляра**.
- Для RPL Owner/RPL Neighbour требуется ручное назначение портов.

9. Обнаружение устройств (Discovery)

9.1. Протокол LLDP (Link Layer Discovery Protocol)

LLDP – односторонний протокол для обмена информацией между сетевыми устройствами. Не требует подтверждения получения данных.

9.1.1. Свойства LLDP (Property)

Для настройки глобальных параметров LLDP:

Перейдите в раздел **Discovery > LLDP > Property**.

SAVE LOGOUT RES

Discovery >> LLDP >> Property

LLDP

State

☒ Enable

LLDP Handling

☐ Filtering

☐ Bridging

☒ Flooding

TLV Advertise Interval

30

Sec (5 - 32767, default 30)

Hold Multiplier

4

(2 - 10, default 4)

Reinitializing Delay

2

Sec (1 - 10, default 2)

Transmit Delay

2

Sec (1 - 8191, default 2)

LLDP-MED

Fast Start Repeat Count

3

(1 - 10, default 3)

Apply

Параметры LLDP

Параметр	Описание
State	Включение/отключение LLDP на коммутаторе.
LLDP Handling	Действие при отключенном LLDP:
	Filtering – удаление LLDP-кадров.

Параметр	Описание
	Bridging – передача только членам VLAN (аналог flooding с учетом VLAN).
	Flooding – передача на все порты.
TLV Advertise Interval	Интервал отправки LLDP-кадров (по умолчанию: 30 сек, диапазон: 5–32767 сек).
Holdtime Multiplier	Множитель для TTL (время жизни данных). Диапазон: 2–10 (по умолчанию: 4).
Reinitialization Delay	Задержка перед повторной инициализацией порта (1–10 сек, по умолчанию: 2 сек).
Transmit Delay	Задержка между отправкой LLDP-кадров (1–8191 сек, по умолчанию: 3 сек).
Fast Start Repeat Count	Количество быстрых повторов при поднятии линка (1–10, по умолчанию: 3).

Примечания:

1. **TLV (Type-Length-Value)** – блоки данных в LLDP-кадрах (информация о портах, VLAN, PoE и т.д.).
2. **Holdtime = Интервал × Множитель** (например, 30 сек × 4 = 120 сек).
3. **Fast Start** ускоряет обнаружение устройств при включении порта.

Рекомендации:

- Для VoIP устройств и IP-камер используйте интервал **30 сек** и **Holdtime Multiplier = 4**.
- На edge-портах активируйте **Filtering** для безопасности.

9.1.2. Настройка портов LLDP (Port Setting)

Для настройки параметров LLDP на портах:

1. Перейдите в раздел **Discovery > LLDP > Port Setting**.
2. Выберите порт и нажмите **Edit (Изменить)**.

Discovery >> LLDP >> Port Setting

Port Setting Table

☐	Entry	Port	Mode	Selected TLV
☐	1	GE1	Normal	802.1 PVID
☐	2	GE2	Normal	802.1 PVID
☐	3	GE3	Normal	802.1 PVID
☐	4	GE4	Normal	802.1 PVID
☐	5	GE5	Normal	802.1 PVID
☐	6	GE6	Normal	802.1 PVID
☐	7	GE7	Normal	802.1 PVID
☐	8	GE8	Normal	802.1 PVID
☐	9	GE9	Normal	802.1 PVID
☐	10	GE10	Normal	802.1 PVID
☐	11	GE11	Normal	802.1 PVID
☐	12	GE12	Normal	802.1 PVID
☐	13	GE13	Normal	802.1 PVID
☐	14	GE14	Normal	802.1 PVID
☐	15	GE15	Normal	802.1 PVID
☐	16	GE16	Normal	802.1 PVID
☐	17	GE17	Normal	802.1 PVID
☐	18	GE18	Normal	802.1 PVID
☐	19	GE19	Normal	802.1 PVID
☐	20	GE20	Normal	802.1 PVID
☐	21	GE21	Normal	802.1 PVID
☐	22	GE22	Normal	802.1 PVID
☐	23	GE23	Normal	802.1 PVID
☐	24	GE24	Normal	802.1 PVID
☐	25	TE1	Normal	802.1 PVID
☐	26	TE2	Normal	802.1 PVID
☐	27	TE3	Normal	802.1 PVID
☐	28	TE4	Normal	802.1 PVID

Edit

Discovery >> LLDP >> Port Setting

Edit Port Setting

Port	GE1	
Mode	☐ Transmit ☐ Receive ☒ Normal ☐ Disable	
Optional TLV	Available TLV Port Description System Name System Description System Capabilities 802.3 MAC-PHY	Selected TLV 802.1 PVID
802.1 VLAN Name	Available VLAN VLAN 1 VLAN 2 VLAN 3	Selected VLAN

Apply Close

Параметры портов LLDP

Параметр	Описание
Port	Выберите порт для настройки (или All Ports для всех портов).
Mode	Режим работы LLDP:
	Disable – отключение отправки и получения LLDP-кадров.
	RX Only – только прием LLDP-кадров.
	TX Only – только отправка LLDP-кадров.
	TX And RX – отправка и прием LLDP-кадров (рекомендуется).
Optional TLV	Выберите дополнительные TLV (можно несколько):
	System Name – имя устройства.
	Port Description – описание порта.
	System Description – описание системы.
	System Capability – возможности устройства (коммутатор, маршрутизатор и т.д.).
	802.3 MAC-PHY – информация о скорости и дуплексе.
	802.3 Link Aggregation – поддержка агрегации каналов.
	802.3 Maximum Frame Size – максимальный размер кадра.
	Management Address – IP-адрес управления.
	802.1PVID – PVID порта.
802.1 VLAN Name	Выберите VLAN Name ID для отправки (можно несколько).

Примечания:

1. Режимы LLDP:

- **TX And RX** используется для взаимодействия с соседними устройствами (например, коммутаторами, IP-телефонами).
- **RX Only** подходит для мониторинга сети без раскрытия информации о коммутаторе.

2. TLV (Type-Length-Value):

- **System Capability** помогает определить тип устройства (например, Switch, Router).
- **Management Address** упрощает удаленное управление.

Пример настройки:

- **Порт 1 (подключен к IP-телефону):**
 - **Mode:** TX And RX
 - **Optional TLV:** System Name, Port Description, Management Address
- **Порт 24 (магистраль):**
 - **Mode:** TX And RX
 - **Optional TLV:** 802.3 Link Aggregation, 802.1PVID

9.1.3. Политика сети LLDP-MED (MED Network Policy)

Для настройки политик QoS для устройств LLDP-MED (например, VoIP):

- 1. Перейдите в раздел **Discovery > LLDP > MED Network Policy**.
- 2. Нажмите **Add (Добавить)** или **Edit (Изменить)** для создания/редактирования политики.

Discovery >> LLDP >> MED Network Policy

MED Network Policy Table

Showing All entries Showing 1 to 1 of 1 entries

☐	Policy ID	Application	VLAN	VLAN Tag	Priority	DSCP	
☐	1	Voice Signaling	2	Tagged	0	0	

Add Edit Delete First Previous 1 Next Last

Add MED Network Policy

Policy ID

1

Application

Voice

VLAN

Range (0 - 4095)

VLAN Tag

Tagged

Untagged

Priority

0

DSCP

0

Apply

Close

Параметры политики

Параметр	Описание
Policy ID	Идентификатор политики (1–65535).
Application	Тип трафика:
	Voice – голосовой трафик (VoIP).
	Voice Signaling – оповещение VoIP (SIP, H.323).
	Guest Voice – гостевой голосовой трафик.
	Softphone Voice – голосовой трафик с ПО-

Параметр	Описание
	телефонов.
	Video Conferencing – видеоконференции.
	App Streaming Video – потоковое видео.
VLAN	VLAN ID для трафика (1–4094).
VLAN Tag	Тип VLAN:
	Tagged – тегированные кадры.
	Untagged – нет тегов.
Priority	Приоритет L2 (0–7, где 7 – наивысший).
DSCP	Значение DSCP (0–63) для QoS на L3.

Примечания:

1. **LLDP-MED (Media Endpoint Discovery)** – расширение LLDP для мультимедийных устройств (IP-телефоны, камеры).
2. **Примеры DSCP:**
 - **Voice:** EF (46)
 - **Video Conferencing:** AF41 (34)

Рекомендации:

- Для VoIP используйте:
 - **Priority:** 6
 - **DSCP:** 46 (EF)
- Для видеотрафика:
 - **Priority:** 4
 - **DSCP:** 34 (AF41)

9.1.4. Настройка портов LLDP-MED (MED Port Setting)

Для настройки параметров LLDP-MED на портах:

- 1. Перейдите в раздел **Discovery > LLDP > MED Port Setting**.
- 2. Выберите порт и нажмите **Edit (Изменить)**.

Discovery >> LLDP >> MED Port Setting

MED Port Setting Table

	Entry	Port	State	Network Policy		Location	Inventory
				Active	Application		
☐	1	GE1	Enabled	Yes		No	No
☐	2	GE2	Enabled	Yes		No	No
☐	3	GE3	Enabled	Yes		No	No
☐	4	GE4	Enabled	Yes		No	No
☐	5	GE5	Enabled	Yes		No	No
☐	6	GE6	Enabled	Yes		No	No
☐	7	GE7	Enabled	Yes		No	No
☐	8	GE8	Enabled	Yes		No	No
☐	9	GE9	Enabled	Yes		No	No
☐	10	GE10	Enabled	Yes		No	No
☐	11	GE11	Enabled	Yes		No	No
☐	12	GE12	Enabled	Yes		No	No
☐	13	GE13	Enabled	Yes		No	No
☐	14	GE14	Enabled	Yes		No	No
☐	15	GE15	Enabled	Yes		No	No
☐	16	GE16	Enabled	Yes		No	No
☐	17	GE17	Enabled	Yes		No	No
☐	18	GE18	Enabled	Yes		No	No
☐	19	GE19	Enabled	Yes		No	No
☐	20	GE20	Enabled	Yes		No	No
☐	21	GE21	Enabled	Yes		No	No
☐	22	GE22	Enabled	Yes		No	No
☐	23	GE23	Enabled	Yes		No	No
☐	24	GE24	Enabled	Yes		No	No
☐	25	TE1	Enabled	Yes		No	No
☐	26	TE2	Enabled	Yes		No	No
☐	27	TE3	Enabled	Yes		No	No
☐	28	TE4	Enabled	Yes		No	No

Edit

Discovery >> LLDP >> MED Port Setting

Edit MED Port Setting

Port

GE1

State

☒ Enable

Optional TLV

Available TLV

Location
Inventory

Selected TLV

Network Policy

Network policy

Available Policy

Selected Policy

Location

Coordinate

16 pairs of hexadecimal characters

Chvis

8 - 100 pairs of hexadecimal characters

ECS ELIN

10 - 25 pairs of hexadecimal characters

Apply

Close

Основные параметры портов

Параметр	Описание
Port	Выберите порт или All Ports для настройки всех портов.
State	Включение/отключение LLDP-MED на порту.
Optional TLV	Дополнительные TLV (можно выбрать несколько):
	Network Policy – передача политик QoS (например, для VoIP).
	Location – информация о местоположении устройства.
	Inventory – данные о модели и производителе устройства.
Network Policy	Привязка политик QoS (должны быть созданы в разделе MED Network Policy).

Параметры местоположения (Location)

Параметр	Описание
Coordinate	Географические координаты (широта/долгота).
Civic	Адрес в текстовом формате (например, "ул. Ленина, д. 1").
ECS ELIN	Номер экстренного вызова (Emergency Call Service ELIN).

Примечания:

1. **LLDP-MED** используется для:
 - Автоматической настройки VoIP-телефонов (VLAN, QoS).
 - Передачи информации о местоположении для экстренных вызовов.
2. **Inventory TLV** помогает идентифицировать модель устройства (например, "Cisco IP Phone 7960").

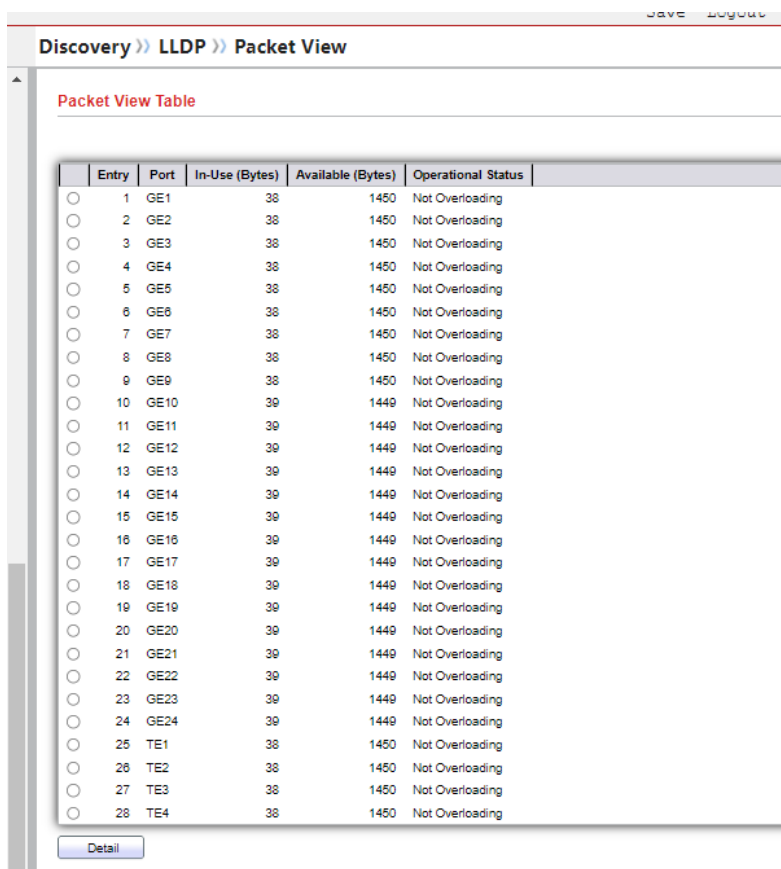
Пример настройки:

- **Порт 1 (IP-телефон):**
 - **State:** Enable
 - **Optional TLV:** Network Policy, Inventory
 - **Network Policy:** 1 (Voice), 2 (Voice Signaling)

9.1.5. Просмотр пакетов LLDP (Packet View)

Для анализа перегрузки LLDP-пакетов:

Перейдите в раздел **Discovery > LLDP > Packet View**.



Discovery >> LLDP >> Packet View

Packet View Table

	Entry	Port	In-Use (Bytes)	Available (Bytes)	Operational Status
☐	1	GE1	38	1450	Not Overloading
☐	2	GE2	38	1450	Not Overloading
☐	3	GE3	38	1450	Not Overloading
☐	4	GE4	38	1450	Not Overloading
☐	5	GE5	38	1450	Not Overloading
☐	6	GE6	38	1450	Not Overloading
☐	7	GE7	38	1450	Not Overloading
☐	8	GE8	38	1450	Not Overloading
☐	9	GE9	38	1450	Not Overloading
☐	10	GE10	39	1449	Not Overloading
☐	11	GE11	39	1449	Not Overloading
☐	12	GE12	39	1449	Not Overloading
☐	13	GE13	39	1449	Not Overloading
☐	14	GE14	39	1449	Not Overloading
☐	15	GE15	39	1449	Not Overloading
☐	16	GE16	39	1449	Not Overloading
☐	17	GE17	39	1449	Not Overloading
☐	18	GE18	39	1449	Not Overloading
☐	19	GE19	39	1449	Not Overloading
☐	20	GE20	39	1449	Not Overloading
☐	21	GE21	39	1449	Not Overloading
☐	22	GE22	39	1449	Not Overloading
☐	23	GE23	39	1449	Not Overloading
☐	24	GE24	39	1449	Not Overloading
☐	25	TE1	38	1450	Not Overloading
☐	26	TE2	38	1450	Not Overloading
☐	27	TE3	38	1450	Not Overloading
☐	28	TE4	38	1450	Not Overloading

Detail

Сводная информация по портам

Параметр	Описание
Port	Имя порта.
In-Use (Bytes)	Количество байт, занятых LLDP-информацией в пакете.
Available (Bytes)	Свободное место для дополнительных TLV (макс. размер пакета: 1500 байт).
Operational Status	Статус перегрузки: Normal или Overloading.

Discovery >> LLDP >> Packet View	
Packet View Detail	
Port	GE12
Mandatory TLVs	
Size (Bytes)	22
Operational Status	Transmitted
MED Capabilities	
Size (Bytes)	0
Operational Status	Transmitted
MED Location	
Size (Bytes)	0
Operational Status	Transmitted
MED Network Policy	
Size (Bytes)	0
Operational Status	Transmitted
MED Inventory	
Size (Bytes)	0
Operational Status	Transmitted
MED Extended Power via MDI	
Size (Bytes)	0
Operational Status	Transmitted
802.3 TLVs	
Size (Bytes)	0
Operational Status	Transmitted
Optional TLVs	
Size (Bytes)	0
Operational Status	Transmitted
802.1 TLVs	
Size (Bytes)	8
Operational Status	Transmitted
Total	
In-Use (Bytes)	30

Детальная информация (для выбранного порта)

Параметр	Описание
Mandatory TLVs	Размер обязательных TLV (например, Chassis ID, Port ID). Статус: Sent или Overloading.
MED Capabilities	Размер TLV возможностей LLDP-MED.
MED Location	Размер TLV местоположения.
MED Network Policy	Размер TLV политик QoS.
MED Inventory	Размер TLV инвентарной информации.
MED Extended Power via MDI	Размер TLV информации о PoE.
802.3 TLVs	Размер TLV стандарта 802.3 (MAC/PHY, агрегация).
Optional TLVs	Размер дополнительных TLV (System Name, Description).
802.1 TLVs	Размер TLV стандарта 802.1 (VLAN, PVID).
Total	Общий размер LLDP-пакета.

Примечания:

1. **Перегрузка (Overloading)** возникает, если суммарный размер TLV превышает 1500 байт.
2. Решения:
 - Отключите неиспользуемые TLV (например, **MED Inventory**).
 - Уменьшите количество политик в **MED Network Policy**.

Пример:

- **Порт 1:**
 - **In-Use:** 1420 байт
 - **Available:** 80 байт
 - **Status:** Normal

9.1.6. Локальная информация (Local Information)

Для просмотра сведений о локальном устройстве в LLDP:

Перейдите в раздел **Discovery > LLDP > Local Information**.

Discovery >> LLDP >> Local Information

Device Summary

Chassis ID Subtype	MAC address
Chassis ID	00:E0:4C:00:00:00
System Name	Switch
System Description	RTL9301
Supported Capabilities	Bridge, Router
Enabled Capabilities	Bridge, Router
Port ID Subtype	Local

Port Status Table

Port Status Table

Q

	Entry	Port	LLDP State	LLDP-MED State
☐	1	GE1	Normal	Enabled
☐	2	GE2	Normal	Enabled
☐	3	GE3	Normal	Enabled
☐	4	GE4	Normal	Enabled
☐	5	GE5	Normal	Enabled
☐	6	GE6	Normal	Enabled
☐	7	GE7	Normal	Enabled
☐	8	GE8	Normal	Enabled
☐	9	GE9	Normal	Enabled
☐	10	GE10	Normal	Enabled
☐	11	GE11	Normal	Enabled
☐	12	GE12	Normal	Enabled
☐	13	GE13	Normal	Enabled
☐	14	GE14	Normal	Enabled
☐	15	GE15	Normal	Enabled
☐	16	GE16	Normal	Enabled
☐	17	GE17	Normal	Enabled
☐	18	GE18	Normal	Enabled
☐	19	GE19	Normal	Enabled
☐	20	GE20	Normal	Enabled
☐	21	GE21	Normal	Enabled
☐	22	GE22	Normal	Enabled
☐	23	GE23	Normal	Enabled
☐	24	GE24	Normal	Enabled
☐	25	TE1	Normal	Enabled
☐	26	TE2	Normal	Enabled
☐	27	TE3	Normal	Enabled
☐	28	TE4	Normal	Enabled

Detail

Основная информация об устройстве

Параметр	Описание
Chassis ID Subtype	Тип идентификатора шасси (например, MAC-адрес).
Chassis ID	Идентификатор шасси. Если выбран MAC – отображается MAC-адрес коммутатора.
System Name	Имя коммутатора (например, "Switch-1").
System Description	Описание системы (модель, версия ПО).
Capabilities Supported	Поддерживаемые функции: Bridge, Router, WLAN AP и др.
Capabilities Enabled	Активные функции устройства.
Port ID Subtype	Тип идентификатора порта (например, MAC, Interface Name).
LLDP Status	Режим работы LLDP: Tx/Rx, Tx Only, Rx Only, Disabled.
LLDP Med Status	Состояние LLDP-MED: Enabled или Disabled.

Discovery » LLDP » Local Information

Local Information Detail

Chassis ID Subtype	MAC address
Chassis ID	00:E0:4C:00:00:00
System Name	Switch
System Description	RTL9301
Supported Capabilities	Bridge, Router
Enabled Capabilities	Bridge, Router
Port ID	GE2
Port ID Subtype	Local
Port Description	

Management Address Table				
Address Subtype	Address	Interface Subtype	Interface Number	
0 results found.				

MAC/PHY Detail	
Auto-Negotiation Supported	N/A
Auto-Negotiation Enabled	N/A
Auto-Negotiation Advertised Capabilities	N/A
Operational MAU Type	N/A

802.3 Detail	
802.3 Maximum Frame Size	N/A

802.3 Link Aggregation	
Aggregation Capability	N/A
Aggregation Status	N/A
Aggregation Port ID	N/A

MED Detail	
Capabilities Supported	Capabilities , Network policy
Current Capabilities	Capabilities , Network policy
Device Class	Network Connectivity
Hardware Revision	N/A
Firmware Revision	N/A
Software Revision	N/A
Serial Number	N/A
Manufacturer Name	N/A
Model Name	N/A
Asset ID	N/A

Location Information	
Civic	N/A
Coordinate	N/A
EC\$ ELIN	N/A

Network Policy Table				
Application Type	VLAN	VLAN Type	Priority	DSCP
0 results found.				

Close

Детальная информация о порте

Нажмите кнопку **Detail** для выбранного порта, чтобы просмотреть:

- **Port ID** – идентификатор порта.
- **Port Description** – описание порта.
- **MED Capabilities** – поддержка LLDP-MED.

Примечания:

- 1. **System Name** и **System Description** помогают идентифицировать устройство в сети.
- 2. **Capabilities** указывают на роль устройства (например, Bridge для L2-коммутатора).

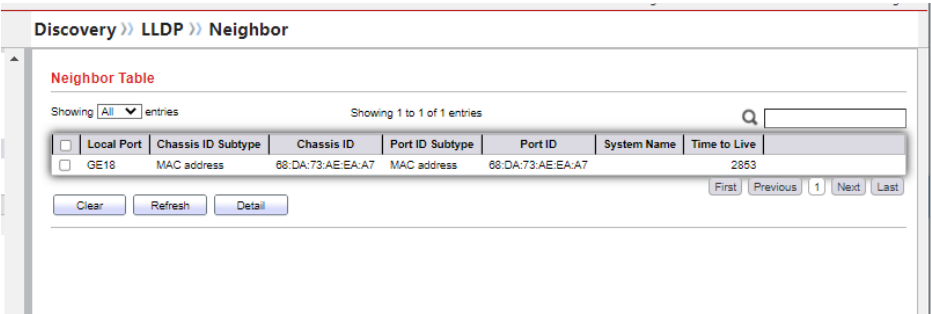
Пример:

- **Chassis ID:** 00:1A:2B:3C:4D:5E (MAC)
- **System Name:** "Core-Switch-3"
- **Capabilities Enabled:** Bridge, Router

9.1.7. Соседние устройства (Neighbor)

Для просмотра информации об устройствах, обнаруженных через LLDP:

Перейдите в раздел **Discovery > LLDP > Neighbor**.



Список соседних устройств

Параметр	Описание
Local Port	Локальный порт, к которому подключено устройство.
Chassis ID Subtype	Тип идентификатора шасси (например, MAC-адрес).

Параметр	Описание
Chassis ID	Идентификатор шасси соседнего устройства.
Port ID Subtype	Тип идентификатора порта (например, Interface Name).
Port ID	Идентификатор порта соседнего устройства.
System Name	Имя соседнего устройства (если опубликовано).
Time to Live (TTL)	Время жизни записи (в секундах) до удаления из таблицы.

Детальная информация

Нажмите кнопку **Detail** для выбранного устройства, чтобы просмотреть:

- **System Description** – описание системы (модель, версия ПО).
- **Capabilities** – функции устройства (Router, Switch, Phone и т.д.).
- **Management Address** – IP-адрес для управления.

Примечания:

1. **TTL** обновляется при получении новых LLDP-кадров.
2. **Port ID** помогает идентифицировать интерфейс на удаленном устройстве.

Пример записи:

- **Local Port:** GE18
- **Chassis ID:** 00:1B:2C:3D:4E:5F
- **System Name:** "Access-Switch-2"
- **TTL:** 120 сек

9.1.8. Статистика LLDP (Statistics)

Для просмотра статистики работы LLDP:

Перейдите в раздел **Discovery > LLDP > Statistics**.

Discovery >> LLDP >> Statistics

Global Statistics

Insertions	1
Deletions	0
Drops	0
AgeOuts	0

Statistics Table

☐	Entry	Port	Transmit Frame	Receive Frame			Receive TLV		Neighbor Timeout
			Total	Total	Discard	Error	Discard	Unrecognized	
☐	1	GE1	0	0	0	0	0	0	0
☐	2	GE2	0	0	0	0	0	0	0
☐	3	GE3	0	0	0	0	0	0	0
☐	4	GE4	0	0	0	0	0	0	0
☐	5	GE5	0	0	0	0	0	0	0
☐	6	GE6	0	0	0	0	0	0	0
☐	7	GE7	0	0	0	0	0	0	0
☐	8	GE8	0	0	0	0	0	0	0
☐	9	GE9	0	0	0	0	0	0	0
☐	10	GE10	0	0	0	0	0	0	0
☐	11	GE11	0	0	0	0	0	0	0
☐	12	GE12	0	0	0	0	0	0	0
☐	13	GE13	0	0	0	0	0	0	0
☐	14	GE14	0	0	0	0	0	0	0
☐	15	GE15	0	0	0	0	0	0	0
☐	16	GE16	0	0	0	0	0	0	0
☐	17	GE17	0	0	0	0	0	0	0
☐	18	GE18	188	0	0	0	0	0	0
☐	19	GE19	0	0	0	0	0	0	0
☐	20	GE20	0	0	0	0	0	0	0
☐	21	GE21	0	0	0	0	0	0	0
☐	22	GE22	0	0	0	0	0	0	0
☐	23	GE23	0	0	0	0	0	0	0
☐	24	GE24	0	0	0	0	0	0	0
☐	25	TE1	0	0	0	0	0	0	0
☐	26	TE2	0	0	0	0	0	0	0
☐	27	TE3	0	0	0	0	0	0	0
☐	28	TE4	0	0	0	0	0	0	0

Глобальная статистика

Параметр	Описание
Insertions	Количество успешно добавленных записей о соседних устройствах.
Deletions	Количество удаленных записей (вручную или из-за отключения LLDP).
Drops	Количество отклоненных записей из-за нехватки ресурсов.
Age Outs	Количество записей, удаленных по истечении времени жизни (TTL).

Статистика по портам

Параметр	Описание
Port	Идентификатор порта.
Transmit Frame Total	Общее количество отправленных LLDP-кадров.
Receive Frame Total	Общее количество полученных LLDP-кадров.
Receive Frame Discard	Количество отброшенных LLDP-кадров (например, из-за ошибок).
Receive Frame Error	Количество невалидных LLDP-кадров.
Receive TLV Discard	Количество отброшенных TLV (например, неподдерживаемые типы).
Receive TLV Unrecognized	Количество нераспознанных TLV.
Neighbor Timeout	Количество записей, удаленных по таймауту.

Примечания:

1. **Высокий уровень ошибок (Receive Frame Error)** может указывать на:
 - Повреждение кадров в сети.
 - Несовместимость оборудования.

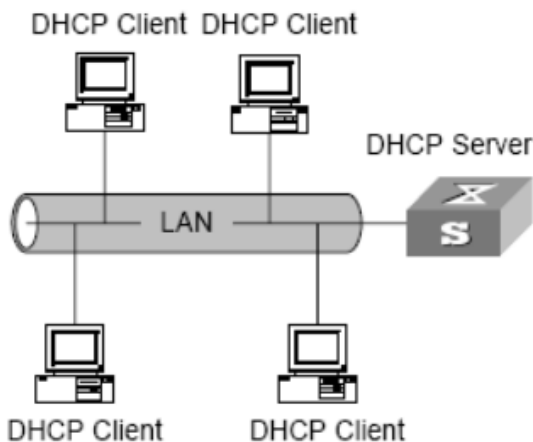
2. **Unrecognized TLV** – нормально для устройств разных производителей.

Рекомендации:

- Если **Drops** > 0, попробуйте увеличить размер таблицы LLDP
- Мониторинг **Age Outs** поможет выявить проблемы с подключением.

10. DHCP (Dynamic Host Configuration Protocol)

DHCP – это протокол динамической настройки хостов, разработанный для автоматического распределения IP-адресов и других сетевых параметров (маска подсети, шлюз, DNS) в компьютерных сетях.



Принцип работы DHCP

1. **Режим клиент/сервер:**
 - **DHCP-клиент** (ПК, телефон, IoT-устройство) запрашивает конфигурацию.
 - **DHCP-сервер** (роутер, коммутатор, сервер) назначает параметры на основе политик.

2. Типичный сценарий:

- Один DHCP-сервер обслуживает множество клиентов.
- Подходит для сетей с мобильными устройствами (Wi-Fi, ноутбуки).

Решаемые задачи

- **Динамическое выделение IP:** Автоматизация при изменении местоположения устройств.
- **Ограничение адресов:** Пул адресов для временного использования (например, гостевые сети).
- **Централизованное управление:** Настройка VLAN, QoS через DHCP-опции.

Пример DHCP-опций:

- **Option 3:** Шлюз по умолчанию.
- **Option 6:** DNS-серверы.
- **Option 66:** TFTP-сервер (для IP-телефонов).

10.1. Настройка протокола DHCP (DHCP Property)

Для включения/отключения DHCP-сервера и настройки портов:

Перейдите в раздел **DHCP > Property**

DHCP >> Property

State ☐ Enable

Static Binding First ☐ Enable

Apply

DHCP Port Setting Table

Q

☐	Entry	Port	State
☐	1	GE1	Disabled
☐	2	GE2	Disabled
☐	3	GE3	Disabled
☐	4	GE4	Disabled
☐	5	GE5	Disabled
☐	6	GE6	Disabled
☐	7	GE7	Disabled
☐	8	GE8	Disabled
☐	9	GE9	Disabled
☐	10	GE10	Disabled
☐	11	GE11	Disabled
☐	12	GE12	Disabled
☐	13	GE13	Disabled
☐	14	GE14	Disabled
☐	15	GE15	Disabled
☐	16	GE16	Disabled
☐	17	GE17	Disabled
☐	18	GE18	Disabled
☐	19	GE19	Disabled
☐	20	GE20	Disabled
☐	21	GE21	Disabled
☐	22	GE22	Disabled
☐	23	GE23	Disabled

Глобальные параметры DHCP

- **Состояние DHCP-сервера:** Включено (Enable) / Отключено (Disable).
- **Список портов:** Отображает текущие настройки DHCP для каждого порта.

Настройка портов

1. Нажмите кнопку **Edit (Изменить)** для выбранного порта.
2. Параметры:
 - **State:** Включить/отключить функцию DHCP-сервера на порту.

Edit Port Setting

Port	GE1
State	☐ Enable

Apply Close

Примечания:

1. Для портов со значением **State = Enable** клиенты смогут получать IP-адреса.
2. Рекомендуется отключать DHCP на портах, подключенных к другим DHCP-серверам (во избежание конфликтов).

Пример:

- Порт 1 (клиентская VLAN):
 - State: **Enable**
- Порт 24 (магистраль):
 - State: **Disable**

10.2. Настройка пула IP адресов DHCP (Address Pool Configuration)

Для создания и управления пулами DHCP IP адресов:

Перейдите в раздел **DHCP > IP Pool Setting**.

The screenshot shows the 'DHCP > IP Pool Setting' page. At the top, there's a section titled 'IP Pool Table'. Below it, a dropdown menu shows 'All' entries, and a status line indicates 'Showing 0 to 0 of 0 entries'. A table with columns 'Pool', 'Section', 'Start Address', 'End Address', 'Gateway', 'Mask', 'DNS Primary Server', and 'DNS Second Server' is shown, but it is empty. Below the table, it says '0 results found.' and there are 'Add', 'Edit', and 'Delete' buttons.

На данной странице отображается список всех настроенных пулов с параметрами

- **Имя пула**
- **Диапазон IP-адресов**
- **Маска подсети**
- **Шлюз**
- **DNS-серверы (основной и резервный)**

The screenshot shows the 'DHCP > IP Pool Setting' page with the configuration form for a new IP pool. The form includes fields for 'Pool' (with a note '(1 to 32 alphanumeric characters)'), 'Gateway', 'Mask', 'IP Address Section' (with a 'Section' dropdown set to '1'), 'Start Address', 'End Address', 'DNS Primary Server' (with an 'Enable' checkbox), 'DNS Second Server' (with an 'Enable' checkbox), 'option 43' (with radio buttons for 'ascii' and 'hex'), and 'Lease time' (with fields for '1', 'Day', 'Hour', and 'Minute'). At the bottom, there are 'Apply' and 'Close' buttons.

Добавление/редактирование пула

1. Нажмите **Add (Добавить)** или **Edit (Изменить)**.
2. Укажите параметры:

Параметр	Описание
Pool	Уникальное имя пула адресов (например, "Office-VLAN10").
Gateway	Основной шлюз (например, 192.168.1.1).
Mask	Маска подсети (например, 255.255.255.0).
IP Address Section	Диапазон адресов (например, 192.168.1.100–192.168.1.200).
DNS Primary Server	Основной DNS-сервер (например, 8.8.8.8, 1.1.1.1).
DNS Second Server	Резервный DNS-сервер (например, 8.8.8.8, 1.1.1.1).
Lease Time	Время аренды адреса (например, 24 часа).

3. Сохраните настройки (**Apply**)

Примечания:

- Исключите статические IP-адреса из пула (например, серверы).
- Для гостевых сетей используйте короткое время аренды (2–4 hours).

Пример:

- **Pool:** Guest-WiFi
- **IP Address Section:** 192.168.10.50–192.168.10.150
- **Lease Time:** 4 hours

10.3. Настройка групп адресов VLAN-интерфейсов (VLAN IF Address Group Setting)

Для привязки DHCP-пулов к VLAN-интерфейсам:

Перейдите в раздел **DHCP > VLAN IF Address Group Setting**.

DHCP >> VLAN IF Address Group Setting

Vlan Interface Address Pool Table

Interface:

DHCP Server Group:

DHCP Server Group Table

Group ID	Group IP Address	Bind VLAN Interface
0 results found.		

На данной странице отображается таблица с привязками:

- **Interface** – название VLAN интерфейса (должен быть создан заранее).
- **DHCP Server Group** – выбор пула DHCP серверов, к которому будет привязан VLAN выбранный ранее.
- **Group ID** – идентификатор группы VLAN.
- **Group ID address** – адрес группы VLAN-интерфейсов.
- **Bind VLAN Interface** – связанные с группой VLAN интерфейсы.

DHCP >> VLAN IF Address Group Setting

DHCP Server Group Table

DHCP Server Group

1 ▼

Group IP Address

Apply

Close

Добавление/редактирование группы

1. Нажмите **Add (Добавить)** или **Edit (Изменить)**.
2. Укажите параметры:

Параметр	Описание
DHCP Server Group	Выберите группу из списка (должна быть создана заранее).
Interface IP	IP-адрес VLAN-интерфейса (например, 192.168.10.1/24).

3. Сохраните изменения.

Примечания:

- Группы серверов позволяют распределять нагрузку между несколькими DHCP-серверами.
- Для резервирования настройте **минимум 2 сервера** в группе.

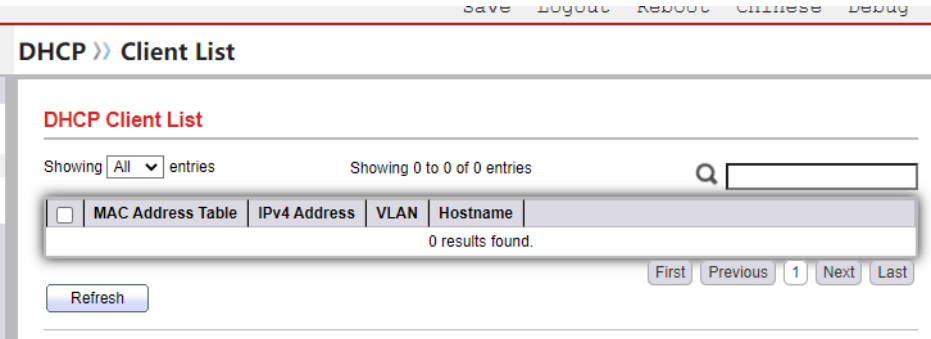
Пример:

- **VLAN 10:**
 - **Interface IP:** 192.168.10.1/24
 - **DHCP Server Group:** "Office-Servers"

10.4. Список клиентов DHCP (Client List)

Для просмотра информации о клиентах, получивших IP-адреса через DHCP:

Перейдите в раздел **DHCP > Client List**.



Информация о клиентах

Параметр	Описание
MAC Address Table	Физический адрес (MAC) клиентского устройства.
IPv4 Address	Выданный клиенту IPv4 адрес.
VLAN	Идентификатор VLAN, в которой находится клиент.
Hostname	Имя устройства (если предоставлено клиентом).

Примечания:

- Список обновляется автоматически при получении новых DHCP-запросов.
- Для принудительного обновления нажмите кнопку **Refresh (Обновить)**.

Пример записи:

- **IPv4:** 192.168.1.100
- **MAC:** 00:1A:2B:3C:4D:5E
- **VLAN:** 10
- **Port:** GE4

10.5. Таблица статической привязки клиентов DHCP (Client Static Binding Table)

Для настройки фиксированных (статических) IP-адресов для клиентов:

Перейдите в раздел **DHCP > Client Static Binding Table**.

DHCP >> Client Static Binding Table

Static Binding Table

Showing **All** entries Showing 0 to 0 of 0 entries

☐ **MAC Address Table** **IPv4 Address** **VLAN** **User Name**

0 results found.

Add **Delete** **First** **Previous** **1** **Next** **Last**

На данной странице отображается таблица с привязанными IP-адресами:

- **MAC Address Table** – физический (MAC) адрес устройства.
- **IPv4 Address** – закрепленный за клиентом IPv4 адрес.
- **VLAN** – идентификатор VLAN.
- **User Name** – описание

DHCP >> Client Static Binding Table

Static Binding Table Add

MAC Address	
VLAN	(1 - 4094)
IPv4 Address	
User Name	(1 - 32)

Apply

Close

Добавление новой привязки

1. Нажмите **Add (Добавить)**.
2. Заполните поля:

Параметр	Описание
MAC Address	MAC-адрес устройства (формат: XX-XX-XX-XX-XX-XX или XXXX.XXXX.XXXX).
VLAN	VLAN, в которой работает устройство.
IPv4 Address	Фиксированный IP-адрес (например, 192.168.1.50).
User Name	Комментарий

3. Сохраните настройки (**Apply**)

Примечания:

- Статические привязки имеют приоритет над динамическими.
- Используйте для:
 - Серверов
 - Сетевых принтеров.
 - IP-телефонов.

Пример:

- **IPv4:** 192.168.1.100
- **MAC:** 00-1A-2B-33-44-55
- **VLAN:** 10
- **User Name:** "Main Office Phone"

11. Настройка Multicast (IGMP, MLD, Static)

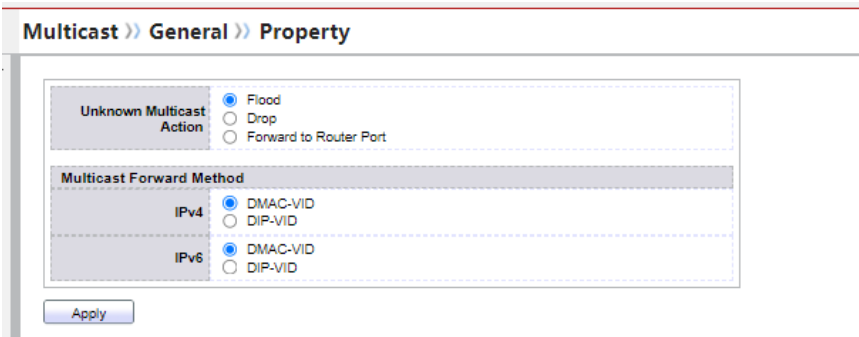
11.1. Общие настройки (General)

Раздел **General** предназначен для базовой конфигурации функций IGMP (IPv4) и MLD (IPv6).

11.1.1. Свойства Multicast (Property)

Для настройки методов мультикаст-маршрутизации:

Перейдите в раздел **Multicast > General > Property**.



Параметры обработки мультикаст-трафика

Параметр	Описание
Unknown Multicast Action	Действие для неизвестного мультикаст-трафика:
	Drop – отбрасывать пакеты.

Параметр	Описание
	Flood – отправлять на все порты (по типу широковещательного трафика).
	Forward to Router port – отправлять только на порты маршрутизаторов.
IPv4 Forward Method	Метод маршрутизации для IPv4:
	DMAC-VID – на основе MAC-адреса назначения + VLAN ID.
	DIP-VID – на основе IP-адреса назначения + VLAN ID.
IPv6 Forward Method	Метод маршрутизации для IPv6:
	DMAC-VID – на основе MAC-адреса назначения + VLAN ID.
	DIP-VID – на основе младших 32 бит IPv6-адреса + VLAN ID.

Примечания:

1. **Router port** – безопасный вариант, предотвращает flooding для трафика в пользовательских VLAN.
2. **DIP-VID** обеспечивает более точную маршрутизацию для IPv4/IPv6.

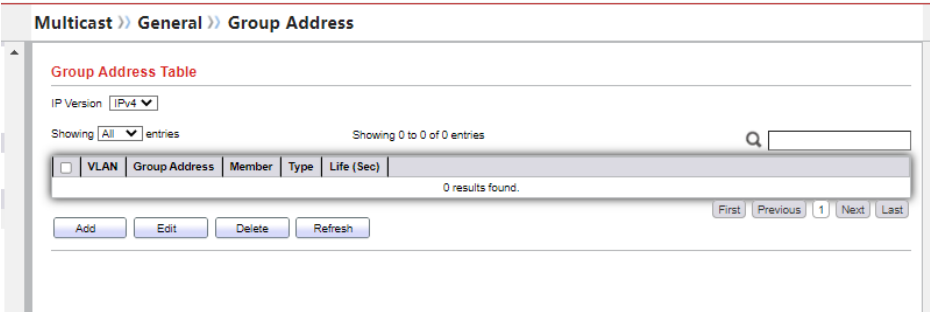
Рекомендации:

- Для IP-телевидения используйте **DIP-VID**.
- В средах с VoIP активируйте **Router port** для неизвестного трафика.

11.1.2. Группы Multicast (Group Address)

Для просмотра и управления мультикаст-группами:

Перейдите в раздел **Multicast > General > Group Address**.



Просмотр мультикаст-групп

Параметр	Описание
IP Version	Версия IP: IPv4 или IPv6.
VLAN	Идентификатор VLAN, к которой относится группа.
Group Address	IP-адрес мультикаст-группы (например, 239.255.255.250 для IPv4).
Member	Порта-участники группы.
Type	Тип группы: Static (ручная настройка) или Dynamic (автоматическое добавление через IGMP/MLD).
Life (Sec)	Время жизни динамической группы (в секундах).

Add Group Address

VLAN

1

IP Version

IPv4

Group Address

Member

Available Port

GE1

GE2

GE3

GE4

GE5

GE6

GE7

GE8

Selected Port

Apply

Close

Добавление/редактирование группы

Параметр	Описание
VLAN	Выберите VLAN для группы.
IP Version	Укажите версию IP (IPv4 или IPv6).
Group Address	Введите IP-адрес группы
Member	Выберите порты:
	Available Port – доступные порты.
	Selected Port – порты, включенные в группу.

Примечания:

- Динамические группы** автоматически добавляются при объединении клиентов через IGMPv3/MLDv2.
- Статические группы** используются для:

- Фиксации портов для критического трафика (например, видеонаблюдение).
- Ограничения доступа к мультикаст-потокам.

Пример настройки:

- **VLAN:** 10
- **IP Version:** IPv4
- **Group Address:** 239.1.1.1
- **Member Ports:** GE4, GE2

11.1.3. Настройка Router портов (Router Port)

Для управления Router портами в мультикаст-трафике:

Перейдите в раздел **Multicast > General > Router Port**.

Multicast >> General >> Router Port

Router Port Table

IP Version IPv4 ▾

Showing All ▾ entries Showing 1 to 1 of 1 entries Q

☐	VLAN	Member	Static Port	Forbidden Port	Life (Sec)
☐	1	GE1-GE3	GE1-GE3		

Add Edit Refresh First Previous 1 Next Last

Текущие порты маршрутизаторов

Параметр	Описание
IP Version	Версия IP: IPv4 (IGMP) или IPv6 (MLD).
VLAN	Идентификатор VLAN.
Member	Router порты (включая статические и динамические).
Static Port	Порты, назначенные вручную как Router порты

Параметр	Описание
Forbidden Port	Порты, запрещенные для работы в качестве Router портов
Life (Sec)	Время жизни динамически назначенного порта (в секундах).

Multicast >> General >> Router Port

Add Router Port

VLAN

Available VLAN

2
3

Selected VLAN

IP Version

IPv4 ▾

Type

☒ Static
☐ Forbidden

Port

Available Port

GE1
GE2
GE3
GE4
GE5
GE6
GE7
GE8

Selected Port

Apply

Close

Настройка портов маршрутизаторов

Параметр	Описание
VLAN	Выберите VLAN:
	Available VLAN – доступные VLAN.
	Selected VLAN – выбранные VLAN.
IP Version	Укажите версию IP (IPv4 или IPv6).
Type	Тип порта:

Параметр	Описание
	Static – статический порт.
	Forbidden – запрет на работу в качестве Router порта.
Port	Выберите порты:
	Available Port – доступные порты.
	Selected Port – выбранные порты.

Multicast >> General >> Router Port

Edit Router Port

VLAN	1	
IP Version	IPv4	
Type	☒ Static ☐ Forbidden	
Port	Available Port GE4 GE5 GE6 GE7 GE8 GE9 GE10 LAG1	Selected Port GE1 GE2 GE3

Apply Close

Примечания:

- Статические порты** используются для:
 - Подключения маршрутизаторов вручную (например, GE16).
 - Гарантированного прохождения мультикаст-трафика.
- Forbidden Port** блокирует IGMP/MLD-запросы на указанных портах.

Пример настройки:

- **VLAN:** 10
- **IP Version:** IPv4
- **Type:** Static
- **Selected Port:** GE16

11.1.4. Принудительная пересылка Multicast трафика (Forward All)

Для настройки принудительной пересылки мультикаст-трафика:

Перейдите в раздел **Multicast > General > Forward All**.

Multicast >> General >> Forward All

Forward All Table

IP Version IPv4

Showing All entries

Showing 1 to 2 of 2 entries

VLAN

Static Port

Forbidden Port

2

GE2-GE3

3

GE1-GE2

Add

Edit

Delete

First

Previous

1

Next

Last

Текущие настройки Forward All

Параметр	Описание
IP Version	Версия IP: IPv4 или IPv6.
VLAN	Идентификатор VLAN.
Static Port	Порты, на которые всегда пересылается мультикаст-трафик (даже без подписки IGMP/MLD).
Forbidden Port	Порты, на которые мультикаст-трафик никогда не пересылается.

Add Forward All

VLAN

Available VLAN

1

Selected VLAN

IP Version

IPv4

Type

☒ Static

☐ Forbidden

Port

Available Port

GE1

GE2

GE3

GE4

GE5

GE6

GE7

GE8

Selected Port

Apply

Close

Добавление/редактирование правил

Параметр	Описание
VLAN	Выберите VLAN:
	Available VLAN – доступные VLAN.
	Selected VLAN – выбранные VLAN.
IP Version	Укажите версию IP (IPv4 или IPv6).
Type	Тип правила:
	Static – трафик всегда пересылается на выбранные порты.
	Forbidden – трафик никогда не пересылается на выбранные порты.
Port	Выберите порты:
	Available Port – доступные порты.
	Selected Port – порты, к которым применяется правило.

Edit Forward All

VLAN	3
IP Version	IPv4
Type	☒ Static ☐ Forbidden
Port	Available Port GE3 GE4 GE5 GE6 GE7 GE8 GE9 GE10 Selected Port GE1 GE2

Apply Close

Примечания:

1. **Static Port** используется для:
 - IP-камер с Multicast передачей.
 - Устройств, не поддерживающих IGMP/MLD.
2. **Forbidden Port** блокирует Multicast трафик для:
 - Пользовательских портов (например, ПК).
 - Экономии полосы пропускания.

Пример настройки:

- **VLAN:** 20
- **IP Version:** IPv4
- **Type:** Static
- **Selected Port:** GE14 (для IP-камеры)

11.1.5. Ограничение на кол-во Multicast групп (Throttling)

Для настройки ограничений на количество мультикаст-групп на порту:

Перейдите в раздел **Multicast > General > Throttling**.

Multicast >> General >> Throttling

Throttling Table

IP Version IPv4 ▾

Q

☐	Entry	Port	Max Group	Exceed Action
☐	1	GE1	256	Deny
☐	2	GE2	256	Deny
☐	3	GE3	256	Deny
☐	4	GE4	256	Deny
☐	5	GE5	256	Deny
☐	6	GE6	256	Deny
☐	7	GE7	256	Deny
☐	8	GE8	256	Deny
☐	9	GE9	256	Deny
☐	10	GE10	256	Deny
☐	11	GE11	256	Deny
☐	12	GE12	256	Deny
☐	13	GE13	256	Deny
☐	14	GE14	256	Deny
☐	15	GE15	256	Deny
☐	16	GE16	256	Deny
☐	17	GE17	256	Deny
☐	18	GE18	256	Deny
☐	19	GE19	256	Deny
☐	20	GE20	256	Deny
☐	21	GE21	256	Deny
☐	22	GE22	256	Deny
☐	23	GE23	256	Deny
☐	24	GE24	256	Deny
☐	25	TE1	256	Deny
☐	26	TE2	256	Deny
☐	27	TE3	256	Deny
☐	28	TE4	256	Deny
☐	29	LAG1	256	Deny
☐	30	LAG2	256	Deny
☐	31	LAG3	256	Deny
☐	32	LAG4	256	Deny
☐	33	LAG5	256	Deny
☐	34	LAG6	256	Deny
☐	35	LAG7	256	Deny
☐	36	LAG8	256	Deny

Edit

Текущие ограничения

Параметр	Описание
IP Version	Версия IP: IPv4 (IGMP) или IPv6 (MLD).
Entry	Номер записи.
Port	Имя порта.
Max Group	Максимальное количество групп, которые порт может изучить (например, 50).
Exceed Action	Действие при превышении лимита: Deny или Replace.

Multicast » General » Throttling

Edit Throttling

Port	GE2,GE4
IP Version	IPv4
Max Group	256 (0 - 256)
Exceed Action	☒ Deny ☐ Replace

Редактирование ограничений

Параметр	Описание
Port	Выберите порт для настройки.
IP Version	Укажите версию IP (IPv4 или IPv6).
Max Group	Установите максимальное количество групп (например, 20 для VoIP).
Exceed Action	Выберите действие при превышении:
	Deny – новые группы игнорируются.
	Replace – случайная замена одной из существующих групп.

Примечания:

- 1. **Deny** рекомендуется для портов с критически важными группами (например, видеонаблюдение).
- 2. **Replace** подходит для клиентских портов с динамическими подписками (VoIP, IPTV).

Пример настройки:

- **Порт:** GE16
- **IP Version:** IPv4
- **Max Group:** 10
- **Exceed Action:** Replace

11.1.6. Фильтрация Multicast групп (Filtering Profile)

Для настройки фильтрации Multicast групп:

Перейдите в раздел **Multicast > General > Filtering Profile**.

Multicast >> General >> Filtering Profile

Filtering Profile Table

IP Version

IPv4

Showing

All

entries

Showing 1 to 1 of 1 entries

Q

	Profile ID	Start Address	End Address	Action
☐	1	224.1.1.1	224.1.2.3	Allow

Add

Edit

Delete

First

Previous

1

Next

Last

Текущие профили

Параметр	Описание
IP Version	Версия IP: IPv4 (IGMP) или IPv6 (MLD).
Profile ID	Идентификатор профиля.

Параметр	Описание
Start Address	Начальный адрес диапазона групп (например, 224.1.1.1).
End Address	Конечный адрес диапазона (например, 224.1.2.3).
Action	Действие: Allow (разрешить) или Deny (запретить).

Multicast » General » Filtering Profile

Add Profile

Profile ID

(1 - 128)

IP Version

IPv4 ▾

Start Address

End Address

Action

☒ Allow
☐ Deny

Apply

Close

Add Profile

Profile ID

(1 - 128)

IP Version

IPv4 ▾

Start Address

End Address

Action

☒ Allow
☐ Deny

Apply

Close

Добавление/редактирование профиля

Параметр	Описание
Profile ID	Уникальный ID профиля (1–128).

Параметр	Описание
IP Version	Выберите версию IP (IPv4 или IPv6).
Start Address	Укажите начальный адрес диапазона.
End Address	Укажите конечный адрес диапазона.
Action	Выберите действие:
	Allow – разрешить группы в диапазоне.
	Deny – блокировать группы в диапазоне.

Примечания:

1. **Диапазон адресов** можно задать как для одиночной группы (например, 224.1.1.1–224.1.1.1), так и для пула.
2. **Deny** полезен для блокировки нежелательного трафика (например, 224.255.255.250 для SSDP).

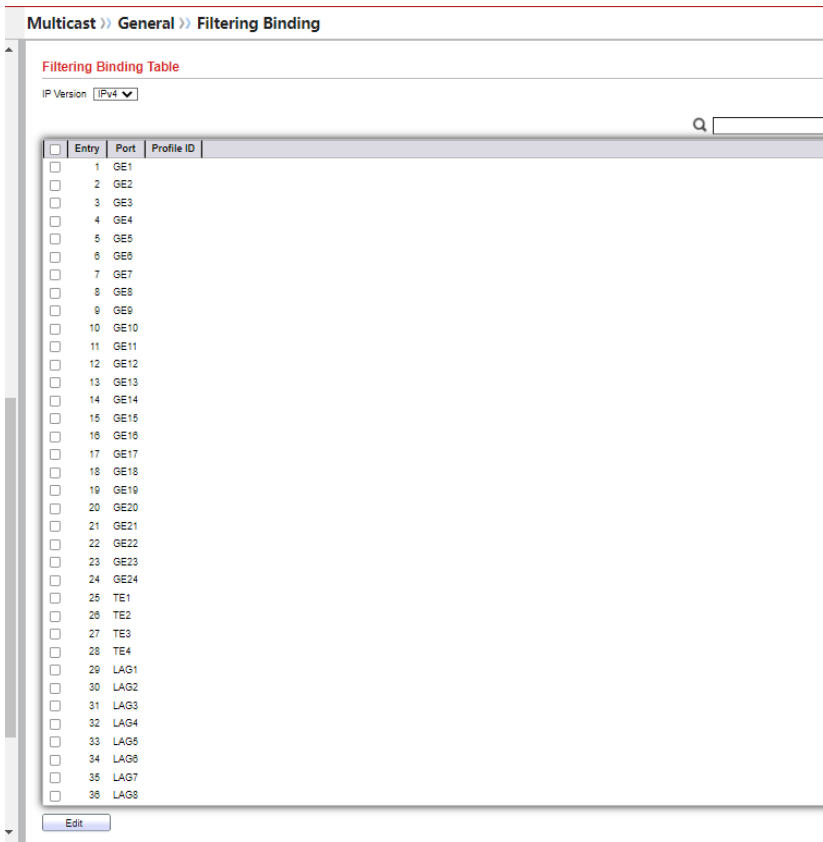
Пример настройки:

- **Profile ID:** 10
- **IP Version:** IPv4
- **Start Address:** 224.1.2.3
- **End Address:** 224.1.2.6
- **Action:** Allow

11.1.7. Привязка профилей фильтрации к портам (Filtering Binding)

Для привязки профилей фильтрации к портам:

Перейдите в раздел **Multicast > General > Filtering Binding**.



Текущие привязки

Параметр	Описание
Entry	Номер записи.
Port	Номер порта.
Profile ID	Идентификатор привязанного профиля (если есть).

Edit Filtering Binding

Port	GE1-GE2
IP Version	IPv4
Profile ID	☒ Enable 1 ▼

Редактирование привязки

Параметр	Описание
Port	Выберите порт для настройки.
IP Version	Укажите версию IP (IPv4 или IPv6).
Profile ID	Действие:
	Enable → выберите ID профиля из списка.
	Disable → удаляет привязку профиля к порту.

Примечания:

1. Профиль должен быть предварительно создан в разделе **Filtering Profile**.
2. Привязка позволяет:
 - Разрешить/запретить мультикаст-группы на конкретных портах.
 - Ограничить доступ к определенным потокам (например, видео).

Пример настройки:

- **Порт:** GE10
- **IP Version:** IPv4
- **Profile ID:** 10 (разрешает группы 239.1.1.1–239.1.1.50)

11.2. Настройка функции IGMP Snooping (IGMP Snooping)

IGMP Snooping – функция коммутатора для управления мультикаст-трафиком на уровне L2.

11.2.1. Свойства IGMP Snooping (Property)

Для настройки глобальных параметров IGMP Snooping:

Перейдите в раздел **Multicast > IGMP Snooping > Property**.

Multicast >> IGMP Snooping >> Property

State

☐ Enable

Version

☒ IGMPv2

☐ IGMPv3

Report Suppression

☒ Enable

Apply

VLAN Setting Table

Edit

Глобальные настройки

Параметр	Описание
State	Включение/отключение IGMP Snooping.
Version	Версия IGMP:
	IGMPv2 – базовая поддержка.
	IGMPv3 – поддержка v3 + обратная совместимость с v2.

Параметр	Описание
Report Suppression	Подавление лишних IGMPv2 Report-пакетов (оптимизация трафика).
Router Port Auto Learn	Автоматическое определение портов маршрутизаторов.
Query Robustness	Коэффициент надежности запросов (учитывает потери пакетов), (по умолчанию: 2).
Query Interval	Интервал отправки общих запросов (сек). По умолчанию: 125 сек.
Query Max Response Interval	Максимальное время ответа на запрос (1/10 сек). По умолчанию: 10 (1 сек).
Last Member Query Count	Количество Group-Specific запросов при получении Leave-сообщения. По умолчанию: 2.
Last Member Query Interval	Интервал Group-Specific запросов (с). По умолчанию: 1с.
Immediate Leave	Мгновенное удаление группы при получении Leave (только для портов с одним клиентом).

Multicast » IGMP Snooping » Property

Edit VLAN Setting

VLAN	3,5
State	☐ Enable
Router Port Auto Learn	☒ Enable
Immediate leave	☐ Enable
Query Robustness	2 (1 - 7, default 2)
Query Interval	125 Sec (30 - 18000, default 125)
Query Max Response Interval	10 Sec (5 - 20, default 10)
Last Member Query Counter	2 (1 - 7, default 2)
Last Member Query Interval	1 Sec (1 - 25, default 1)

Настройки VLAN

Параметр	Описание
VLAN	Выберите VLAN для настройки.
State	Включение или отключение IGMP Snooping для VLAN. Enable – включить IGMP Snooping для VLAN. Disable – отключить.
Router Port Auto Learn	Автоматическое обучение портов маршрутизатора (Router Port). Enable – включить определение через запросы Query, PIM, DVMRP. Disable – отключить.
Immediate Leave	Немедленный выход из группы при получении IGMP Leave. Enable – включить. Disable – отключить.
Query Robustness	Коэффициент надежности запросов (учитывает потери пакетов), (по умолчанию: 2).
Query Interval	Интервал отправки общих запросов (сек). По умолчанию: 125 сек.
Query Max Response Interval	Максимальное время ответа на запрос (1/10 сек). По умолчанию: 10 (1 сек).
Last Member Query Count	Количество Group-Specific запросов при получении Leave-сообщения. По умолчанию: 2.
Last Member Query Interval	Интервал Group-Specific запросов (с). По умолчанию: 1 с.

Operational Status	
Status	Disabled
Query Robustness	2
Query Interval	125 (Sec)
Query Max Response Interval	10 (Sec)
Last Member Query Counter	2
Last Member Query Interval	1 (Sec)

Параметр	Описание
Status	Состояние IGMP Snooping (вкл/выкл)
Query Robustness	Коэффициент надежности запросов (учитывает потери пакетов), (по умолчанию: 2).
Query Interval	Интервал отправки общих запросов (сек).
Query Max Response Interval	Максимальное время ответа на запрос (1/10 сек).
Last Member Query Count	Количество Group-Specific запросов при получении Leave-сообщения.
Last Member Query Interval	Интервал Group-Specific запросов (с).

Примечания:

1. **IGMPv3** рекомендуется для сетей с поддержкой SSM (Source-Specific Multicast).
2. **Immediate Leave** используйте только для портов с одним устройством (например, IP-камеры).

Пример настройки:

- **Глобально:**
 - **Version:** IGMPv3
 - **Query Interval:** 60 сек
- **VLAN 10:**
 - **Immediate Leave:** Enable

11.2.2. Генератор запросов IGMP (Querier)

Для настройки параметров IGMP Snooping Querier (генератор запросов IGMP) перейдите:

Multicast > IGMP Snooping > Querier

На этой странице настраиваются параметры Querier (генератора IGMP-запросов) для конкретных VLAN.

Multicast >> IGMP Snooping >> Querier

Querier Table

Q

	VLAN	State	Operational Status	Version	Querier Address
☐	1	Disabled	Disabled		
☐	2	Disabled	Disabled		
☐	3	Disabled	Disabled		
☐	5	Disabled	Disabled		
☐	10	Disabled	Disabled		

Edit

Таблица работы генератора запросов IGMP

Параметр	Описание
VLAN	ID VLAN, для которой настроен Querier
State	Состояние Querier (вкл./выкл.)
Operational Status	Фактический статус работы Querier
Querier Version	Версия IGMP (v2/v3)
Querier IP	IP-адрес Querier в VLAN

Edit Querier

VLAN	2,10
State	☒ Enable
Version	☒ IGMPv2 ☐ IGMPv3

Настройки для VLAN

Параметр	Описание
VLAN	Список VLAN для настройки
State	Включение/отключение функции Querier для выбранных VLAN: Enabled – Querier активен. Disabled – Querier отключен.
Version	Версия IGMP, используемая Querier: • IGMPv2 – Querier работает по IGMP версии 2. • IGMPv3 – Querier работает по IGMP версии 3 (требуется, чтобы IGMP Snooping также был в версии v3).

Примечания

1. **Querier** отвечает за отправку IGMP-запросов в сети, чтобы определить активные multicast-группы.

2. Если в VLAN нет маршрутизатора, поддерживающего IGMP, коммутатор может взять на себя роль **Querier** (генератор запросов IGMP), если функция включена.
3. Для работы **IGMPv3 Querier** необходимо, чтобы **IGMP Snooping** также был настроен на версию **v3**.

Пример настройки

- Выберите VLAN **10** в списке.
- Включите Querier (**State > Enabled**).
- Установите версию **IGMPv3** (если IGMP Snooping работает в v3).
- Сохраните изменения.

11.2.3. Статистика IGMP Snooping (Statistics)

Для просмотра статистики **IGMP Snooping** перейдите в раздел:

Multicast > IGMP Snooping > Statistics

На этой странице отображается статистика работы IGMP Snooping, а также есть возможность её сбросить.

Multicast >> IGMP Snooping >> Statistics	
Receive Packet	
Total	0
Valid	0
InValid	0
Other	0
Leave	0
Report	0
General Query	0
Special Group Query	0
Source-specific Group Query	0
Transmit Packet	
Leave	0
Report	0
General Query	0
Special Group Query	0
Source-specific Group Query	0
Clear Refresh	

Статистика полученных пакетов (Receive Packet)

Параметр	Описание
Total	Общее количество полученных IGMP-пакетов (включая IPv4 multicast-данные, направленные на CPU).
Valid	Количество корректно обработанных IGMP Snooping-пакетов.
Invalid	Количество некорректных IGMP Snooping-пакетов.
Other	Пакеты, не относящиеся к IGMP (ICMP-протокол ≠ 2) и не являющиеся IPv4 multicast-данными.
Leave	Количество полученных IGMP Leave-пакетов (запросы на выход из группы).
Report	Количество полученных IGMP Report-пакетов (запросы на присоединение к группе).
General Query	Количество полученных IGMP General Query-пакетов (общие запросы).
Special Group Query	Количество полученных IGMP Special Group Query-пакетов (специальные групповые запросы).
Source-specific Group Query	Количество полученных IGMP Source-Specific Group Query-пакетов (запросы для конкретного источника и группы).

Статистика переданных пакетов (Transmit Packet)

Параметр	Описание
Leave	Количество отправленных IGMP Leave-пакетов.
Report	Количество отправленных IGMP Report-пакетов.
General Query	Количество отправленных IGMP General Query-пакетов (включая запросы, отправленные через генератор запросов).
Special Group Query	Количество отправленных IGMP Special Group Query-пакетов (включая запросы, отправленные квайером).
Source-specific Group Query	Количество отправленных IGMP Source-Specific Group Query-пакетов.

Примечания

1. Статистика помогает анализировать состояние multicast-трафика и выявлять возможные проблемы (например, большое количество **Invalid**-пакетов может указывать на ошибки в настройках).
2. Для сброса статистики предусмотрена кнопка **Clear**

Пример использования статистики

- Если **Invalid**-пакетов слишком много:
 - Проверьте настройки **IGMP Snooping** и версию IGMP.

- Убедитесь, что в сети нет некорректных multicast-источников.
- Если **General Query** не приходят:
 - Проверьте, включен ли **Querier** для нужной VLAN.
 - Убедитесь, что маршрутизатор или коммутатор отправляет запросы.

11.3. Настройка функции MLD Snooping (MLD Snooping)

MLD Snooping – это IPv6-аналог IGMP Snooping, используемый для управления multicast-трафиком в IPv6-сетях.

11.3.1. Свойства MLD Snooping (Property)

Чтобы открыть страницу глобальных настроек **MLD Snooping** и параметров VLAN, перейдите в раздел:

Multicast > MLD Snooping > Property

Multicast >> MLD Snooping >> Property

State ☐ Enable

Version

☒ MLDv1 ☐ MLDv2

Report Suppression ☒ Enable

Apply

VLAN Setting Table

	VLAN	Operational Status	Router Port Auto Learn	Query Robustness	Query Interval	Query Max Response Interval	Last Member Query Counter	Last Member Query Interval	Immediate Leave
☐	1	Disabled	Enabled	2	125	10	2	1	Disabled
☐	2	Disabled	Enabled	2	125	10	2	1	Disabled
☐	3	Disabled	Enabled	2	125	10	2	1	Disabled
☐	5	Disabled	Enabled	2	125	10	2	1	Disabled
☐	10	Disabled	Enabled	2	125	10	2	1	Disabled

Edit

Глобальные настройки (Global Settings)

Параметр	Описание
State	Включение/отключение функции MLD Snooping: • Enable – MLD Snooping активен. • Disable – MLD Snooping выключен.
Version	Версия MLD Snooping: • MLDv1 – поддерживает только MLD версии 1. • MLDv2 – поддерживает MLDv2 (включая базовую совместимость с v1).
Report Suppression	Подавление MLDv1-отчетов: • Enable – включено подавление отчетов MLDv1. • Disable – функция отключена.
VLAN	ID VLAN, к которой применяются настройки MLD.
Operation Status	Статус работы MLD Snooping для VLAN.
Router Port Auto Learn	Автоматическое определение порта маршрутизатора: • Enable – коммутатор автоматически определяет порты маршрутизатора. • Disable – функция отключена.
Query Robustness	Коэффициент надежности запросов (учитывает потери пакетов), (по умолчанию: 2).
Query Interval	Интервал отправки общих запросов (в секундах).

Параметр	Описание
Query Max Response Interval	Максимальное время (в 1/10 секунды) для отправки ответного отчета после Membership Query.
Last Member Query Count	Количество Group-Specific Queries, отправляемых при получении Leave Group сообщения.
Last Member Query Interval	Интервал отправки Group-Specific Queries при получении Leave Group сообщения.
Immediate Leave	Мгновенный выход из группы при получении сообщения MLD Leave: • Enable – включен. • Disable – отключен.

Multicast » MLD Snooping » Property

Edit VLAN Setting

VLAN	5,10
State	☐ Enable
Router Port Auto Learn	☒ Enable
Immediate leave	☐ Enable
Query Robustness	2 (1 - 7, default 2)
Query Interval	125 Sec (30 - 18000, default 125)
Query Max Response Interval	10 Sec (5 - 20, default 10)
Last Member Query Counter	2 (1 - 7, default 2)
Last Member Query Interval	1 Sec (1 - 25, default 1)
Operational Status	
Status	Disabled
Query Robustness	2
Query Interval	125 (Sec)
Query Max Response Interval	10 (Sec)
Last Member Query Counter	2
Last Member Query Interval	1 (Sec)

Apply

Close

Настройка VLAN (VLAN Settings)

Параметр	Описание
VLAN	Выбранный список VLAN.
State	Включение MLD Snooping для VLAN: • Enable – MLD Snooping активен для VLAN. • Disable – функция отключена.
Router Port Auto Learn	Автоматическое определение порта маршрутизатора для VLAN: • Enable – включено (на основе Query, PIM, DVMRP). • Disable – отключено.
Immediate Leave	Мгновенный выход из группы при получении MLD Leave: • Enable – включен. • Disable – отключен.
Query Robustness	Настраиваемая устойчивость к потере пакетов (административная настройка).
Query Interval	Настраиваемый интервал отправки общих запросов (административная настройка).
Query Max Response Interval	Настраиваемое максимальное время ответа (в 1/10 секунды).
Last Member Query Counter	Настраиваемое количество Group-Specific Queries при Leave Group.
Last Member Query Interval	Настраиваемый интервал Group-Specific Queries при Leave Group.

Параметр	Описание
Operational Status	Текущий статус работы MLD Snooping (активен, только если включен глобально и для VLAN).
Status	Рабочий статус MLD Snooping.
Query Robustness	Текущая настройка устойчивости к потере пакетов.
Query Interval	Текущий интервал запросов.
Query Max Response Interval	Текущее максимальное время ответа.
Last Member Query Counter	Текущее количество Group-Specific Queries.
Last Member Query Interval	Текущий интервал Group-Specific Queries.

Примечания

1. **MLDv2** рекомендуется для современных сетей, так как поддерживает более сложные сценарии multicast-маршрутизации.
2. **Immediate Leave** ускоряет выход из группы, но может привести к преждевременному отключению трафика, если в VLAN остаются участники.

Пример настройки

- Включите **MLD Snooping** (State > **Enable**).
- Выберите версию **MLDv2**.
- Для VLAN 20 включите **Router Port Auto Learn** и **Immediate Leave**.
- Установите **Query Interval = 60** секунд.

- Сохраните настройки и перезагрузите коммутатор при необходимости.

11.3.2. Статистика MLD Snooping (Statistics)

Для просмотра статистики **MLD Snooping** перейдите в раздел:

Multicast > MLD Snooping > Statistics

Multicast >> MLD Snooping >> Statistics

Receive Packet		
Total		0
Valid		0
InValid		0
Other		0
Leave		0
Report		0
General Query		0
Special Group Query		0
Source-specific Group Query		0

Transmit Packet		
Leave		0
Report		0
General Query		0
Special Group Query		0
Source-specific Group Query		0

Статистика полученных пакетов (Receive Packet)

Параметр	Описание
Total	Общее количество полученных MLD-пакетов (включая IPv6 multicast-данные, направленные на CPU).
Valid	Количество корректно обработанных MLD Snooping-пакетов.
Invalid	Количество некорректных MLD Snooping-пакетов.
Other	Пакеты, не относящиеся к MLD (тип ICMPv6 ≠ MLD), не являющиеся IPv6 multicast-данными и не относящиеся к протоколам маршрутизации IPv6.
Leave	Количество полученных MLD Leave-пакетов (запросы на выход из группы).
Report	Количество полученных MLD Report-пакетов (запросы на присоединение к группе).
General Query	Количество полученных MLD General Query-пакетов (общие запросы).
Special Group Query	Количество полученных MLD Special Group Query-пакетов (специальные групповые запросы).
Source-specific Group Query	Количество полученных MLD Source-Specific Group Query-пакетов (запросы для конкретного источника и группы).

Статистика переданных пакетов (Transmit Packet)

Параметр	Описание
Leave	Количество отправленных MLD Leave-пакетов.
Report	Количество отправленных MLD Report-пакетов.
General Query	Количество отправленных MLD General Query-пакетов.
Special Group Query	Количество отправленных MLD Special Group Query-пакетов.
Source-specific Group Query	Количество отправленных MLD Source-Specific Group Query-пакетов.

Примечания

1. Статистика помогает анализировать работу multicast-трафика в IPv6-сетях и выявлять возможные проблемы (например, большое количество **Invalid**-пакетов может указывать на ошибки в настройках).
2. Для сброса статистики обычно предусмотрена кнопка **Clear** или аналогичная.

Пример использования статистики

- Если **Invalid**-пакетов слишком много:
 - Проверьте настройки **MLD Snooping** и версию MLD.
 - Убедитесь, что в сети нет некорректных multicast-источников.

11.4. Настройка MVR (Multicast VLAN Registration)

Используйте раздел **MVR** для настройки функции Multicast VLAN Registration, которая позволяет эффективно передавать multicast-трафик между разными VLAN.

11.4.1. Свойства MVR (Property)

Чтобы открыть страницу настройки **MVR**, перейдите в раздел:

Multicast > MVR > Property

Multicast >> MVR >> Property

State	☒ Enable
VLAN	2
Mode	☒ Compatible ☐ Dynamic
Group Start	224.1.1.1
Group Count	8 (1 - 128)
Query Time	1 Sec (1 - 10)

Operational Group

Maximum	128
Current	0

Apply

Параметры MVR

Параметр	Описание
State	Включение/отключение функции MVR: • Enable – MVR активен. • Disable – MVR выключен.
VLAN	ID VLAN, используемой для multicast-трафика MVR.

Параметр	Описание
Mode	Режим работы MVR: • Compatible – совместимый режим. • Dynamic – динамический режим (автоматическое определение участников группы на source-порте).
Group Start	Начальный адрес диапазона multicast-групп MVR.
Group Count	Количество multicast-групп в диапазоне.
Query Time	Время ожидания запроса после получения MVR Leave-пакета.
Maximum	Максимальное количество записей в базе данных MVR-групп.
Current	Текущее количество активных MVR-групп.

Примечания

1. **MVR** используется для оптимизации multicast-трафика в сетях с несколькими VLAN, уменьшая дублирование потоков.
2. В **Dynamic** режиме коммутатор автоматически определяет участников multicast-групп, что упрощает настройку, но может потреблять больше ресурсов.

Пример настройки

- Включите **MVR** (State > **Enable**).
- Укажите **VLAN 100** в качестве multicast-VLAN.
- Выберите режим **Dynamic**.

- Задайте диапазон групп:
 - **Group Start:** 239.0.0.1
 - **Group Count:** 10
- Установите **Query Time** = 2 секунды.
- Сохраните настройки.

11.4.2. Настройка портов (Port Setting)

Для настройки ролей портов MVR и параметра Immediate Leave перейдите в раздел:

Multicast > MVR > Port Setting

Multicast >> MVR >> Port Setting

Port Setting Table

☐	Entry	Port	Role	Immediate Leave
☐	1	GE1	None	Disabled
☐	2	GE2	None	Disabled
☐	3	GE3	None	Disabled
☐	4	GE4	None	Disabled
☐	5	GE5	None	Disabled
☐	6	GE6	None	Disabled
☐	7	GE7	None	Disabled
☐	8	GE8	None	Disabled
☐	9	GE9	None	Disabled
☐	10	GE10	None	Disabled
☐	11	GE11	None	Disabled
☐	12	GE12	None	Disabled
☐	13	GE13	None	Disabled
☐	14	GE14	None	Disabled
☐	15	GE15	None	Disabled
☐	16	GE16	None	Disabled
☐	17	GE17	None	Disabled
☐	18	GE18	None	Disabled
☐	19	GE19	None	Disabled
☐	20	GE20	None	Disabled
☐	21	GE21	None	Disabled
☐	22	GE22	None	Disabled
☐	23	GE23	None	Disabled
☐	24	GE24	None	Disabled
☐	25	TE1	None	Disabled
☐	26	TE2	None	Disabled
☐	27	TE3	None	Disabled
☐	28	TE4	None	Disabled
☐	29	LAG1	None	Disabled
☐	30	LAG2	None	Disabled
☐	31	LAG3	None	Disabled
☐	32	LAG4	None	Disabled
☐	33	LAG5	None	Disabled
☐	34	LAG6	None	Disabled
☐	35	LAG7	None	Disabled
☐	36	LAG8	None	Disabled

Edit

Таблица настройки портов MVR

Параметр	Описание
Entry	Номер записи в таблице.
Port	Имя порта.
Role	Роль порта в MVR: • None – порт не участвует в MVR. • Receiver – порт получает multicast-трафик. • Source – порт передает multicast-трафик.
Immediate Leave	Статус Immediate Leave: • Enable – включен мгновенный выход из группы. • Disable – отключен.

Multicast >> MVR >> Port Setting

Edit Port Setting

Port	GE1-GE2,GE4-GE5
Role	☒ None ☐ Receiver ☐ Source
Immediate Leave	☒ Enable

Apply

Close

Параметры настройки портов

Параметр	Описание
Port	Список выбранных портов.
Role	Назначение роли порта в MVR: • None – без роли. • Receiver – порт-получатель multicast-трафика. • Source – порт-источник multicast-трафика.
Immediate Leave	Включение/отключение Immediate Leave: • Enable – при получении Leave-пакета порт мгновенно выходит из группы. • Disable – стандартный режим обработки Leave-пакетов.

Примечания

1. **Source-порты** используются для подключения multicast-источников (например, видео-серверов).
2. **Receiver-порты** подключают конечных пользователей, которые должны получать multicast-трафик.
3. **Immediate Leave** ускоряет освобождение ресурсов при выходе клиента из группы, но может вызвать прерывание трафика, если в группе остаются другие подписчики.

Пример настройки

- Выберите порт GE10:
 - Установите роль **Source**.
 - Отключите **Immediate Leave**.

- Выберите порты **GE1-GE5**:
 - Назначьте роль **Receiver**.
 - Включите **Immediate Leave** для быстрого выхода клиентов.
- Сохраните конфигурацию.

11.4.3. Групповые адреса (Group Address)

Для просмотра и настройки multicast-групп MVR перейдите в раздел:

Multicast > MVR > Group Address

На этой странице отображаются все MVR-группы (динамически изученные или статически добавленные), а также их параметры.

Multicast >> MVR >> Group Address

Group Address Table

Showing All entries Showing 0 to 0 of 0 entries

VLAN	Group Address	Member	Type	Life (Sec)
0 results found.				

Таблица MVR-групп

Параметр	Описание
VLAN	ID VLAN, к которой относится MVR-группа.
Group Address	IP-адрес multicast-группы.
Member	Порт(ы)-участники группы.

Параметр	Описание
Type	Тип группы: • Static – статически настроенная группа. • Dynamic – динамически добавленная группа.
Life (Sec)	Время жизни динамической группы (в секундах).

Multicast >> MVR >> Group Address

Add Group Address

VLAN

2

Group Address

(224.1.1.1 - 224.1.1.1)

Member

Available Port

Selected Port

>

<

Apply

Close

Просмотр участников группы

Параметр	Описание
VLAN	ID VLAN MVR-группы.
Group Address	IP-адрес MVR-группы.

Параметр	Описание
Member	Участники группы: • Available Port – доступные порты для добавления (в совместимом режиме – только Receiver-порты, в динамическом – и Source-порты). • Selected Port – текущие порты-участники группы.

Edit Group Address

VLAN

2

Group Address

224.0.1.5

Member

Available Port

GE1
GE2
GE6
GE7
GE8
GE9
GE10
GE11

Selected Port

GE3
GE4
GE5

Apply

Close

Редактирование группы

Параметр	Описание
VLAN	ID VLAN редактируемой MVR-группы.
Group Address	IP-адрес редактируемой MVR-группы.

Параметр	Описание
Member	Настройка участников: • Available Port – порты, которые можно добавить в группу. • Selected Port – текущие участники группы.

Примечания

1. **Статические группы** требуют ручной настройки и не имеют времени жизни.
2. **Динамические группы** создаются автоматически при подключении клиентов и удаляются по истечении **Life (Sec)**.
3. В **динамическом режиме MVR** Source-порты могут автоматически добавляться в группы.

Пример настройки

- Для добавления статической группы:
 - Укажите **VLAN 100** и адрес **239.0.0.1**.
 - Выберите **Receiver-порты** (GE2-GE5) в **Selected Port**.
- Для проверки динамических групп:
 - Найдите группу с типом **Dynamic** и проверьте **Life (Sec)**.
- Сохраните изменения.

12. Маршрутизация (Routing)

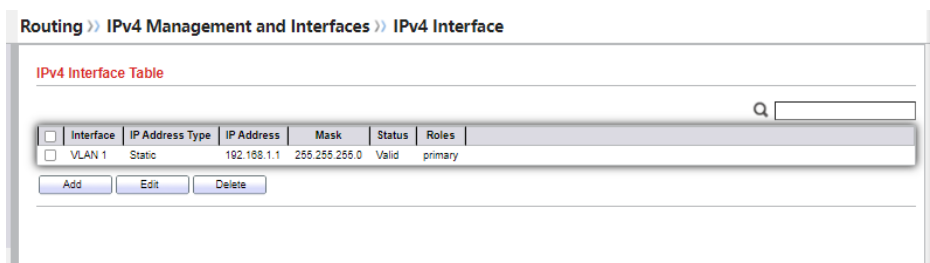
12.1. Настройка IPv4 интерфейсов и маршрутизации (IPv4 Management and Interfaces)

12.1.1. Настройка IPv4 интерфейсов в коммутаторе (IPv4 Interface)

Для настройки IPv4 интерфейсов (в том числе IP адреса коммутатора) перейдите в раздел:

Routing > IPv4 Management and Interfaces > IPv4 Interface

На этой странице отображаются текущие интерфейсы устройства с адресами IPv4.



Для изменения текущего IPv4 адреса коммутатора следует:

- 1) Выбрать (отметить галочкой) VLAN 1 (коммутатор) и нажать кнопку **Edit** (изменить);
- 2) В поле **IP Address** (IP адрес) ввести требуемый IP адрес (по умолчанию 192.168.1.1). В поле **Mask** (маска) требуется ввести значение маски (по умолчанию 255.255.255.0). Если требуется получать IP адрес от маршрутизатора через DHCP – выберите **Dynamic** в поле **Address Type** (тип IP адреса);
- 3) Нажмите кнопку **Apply** (принять), чтобы сохранить настройки. Старый IP адрес автоматически перестанет действовать;

- 4) Выполните повторный вход в WEB интерфейс, используя новый IP адрес.



Username:

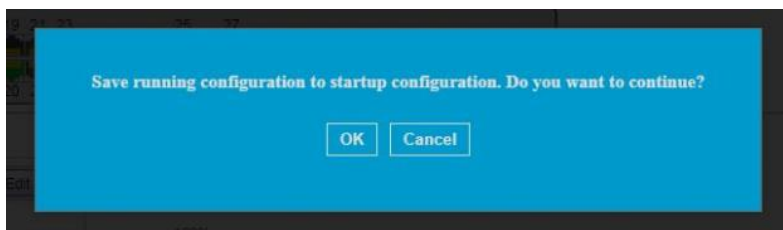
Password:

Language:

Login

Внимание!

Обязательно нажмите кнопку **Save** (сохранить), чтобы сохранить текущую конфигурацию коммутатора, как стартовую. В диалоговом окне (синий фон) нажмите кнопку **OK**. Данная операция позволит коммутатору помнить заданные настройки даже после кратковременного отключения от сети и перезагрузки. В противном случае после перезагрузки IP адрес вернется к предыдущему значению.



Чтобы добавить IPv4-адрес для другого VLAN:

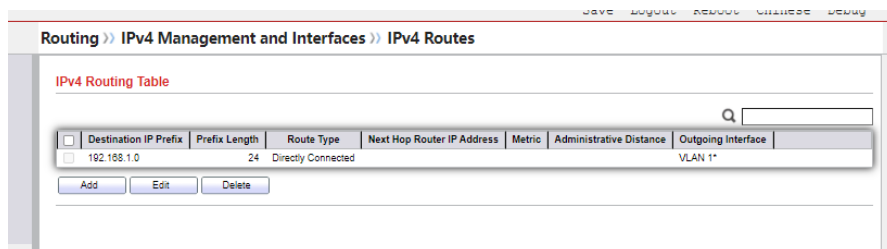
1. Нажмите **Add** (добавить).
2. Укажите:
 - Интерфейс (VLAN 2 и т.д.)
 - IPv4-адрес и маску подсети
3. Сохраните настройки (apply)

12.1.2. Маршрутизация IPv4 (IPv4 Routing)

Перейдите в раздел:

Routing > IPv4 Management and Interfaces > IPv4 Routing

Здесь отображается таблица IPv4-маршрутов.



Добавление постоянного (static) маршрута:

1. Нажмите **Add** (добавить)
2. Заполните поля:
 - Сеть назначения
 - Маска
 - Шлюз (Next Hop)
 - Интерфейс (VLAN 2 и т.д.)
3. Примените изменения (**apply**)

12.1.3. ARP-таблица (ARP)

Для просмотра ARP таблицы перейдите в раздел:

Routing > IPv4 Management and Interfaces > ARP

Routing >> IPv4 Management and Interfaces >> ARP

ARP Entry Age Out: Sec (15 - 21600, default 1200)

Clear ARP Table Entries:
☐ All
☐ Dynamic
☐ Static
☒ Normal Age Out

ARP Table

☐	Interface	IP Address	MAC Address	Status
☐	VLAN 1	192.168.1.34	68:da:73:ae:ea:a7	Dynamic

Routing >> IPv4 Management and Interfaces >> ARP

Add ARP

Interface: VLAN

Note: Only interfaces with an valid IPv4 address are available for selection

IP Address:

MAC Address:

Добавление постоянной (static) ARP-записи:

1. Нажмите **Add** (добавить)
2. Укажите:
 - IP-адрес
 - MAC-адрес
 - Интерфейс

3. Сохраните настройки (**apply**)

12.2. Настройка IPv6 интерфейсов и маршрутизации (IPv6 Management Interface)

12.2.1. Настройка IPv6 интерфейсов в коммутаторе (IPv6 Interface)

Для настройки IPv6 адресов перейдите в раздел:

Routing > IPv6 Management and Interfaces > IPv6 Interface

Routing >> IPv6 Management and Interfaces >> IPv6 Interface

IPv6 Unicast Routing ☐ Enable

Apply Cancel

IPv6 Interface Table

Interface	DHCPv6 Client			Auto Configuration	DAD Attempts
	Stateless	Information Refresh Time	Minimum Information Refresh Time		
☐ VLAN 1	Disabled	86400	600	Enabled	1

Add Edit Delete

Routing >> IPv6 Management and Interfaces >> IPv6 Interface

Add IPv6 Interface

Interface ☒ VLAN ☐ Loopback

Auto Configuration ☒ Enable

DAD Attempts (0 - 600, default 1)

DHCPv6 Client

Stateless ☐ Enable

Information Refresh Time (86400 - 4294967294, default 86400)

Minimum Information Refresh Time (600 - 4294967294, default 600)

Apply Close

Добавление IPv6-адреса:

1. Нажмите **Add** (добавить)

2. Выберите:

- Автоконфигурацию (DHCPv6 Client)
- Или вручную укажите IPv6-адрес.

3. Сохраните настройки (**apply**)

12.2.2. Таблица адресов IPv6 (IPv6 Address)

Для просмотра таблицы IPv6 адресов перейдите в раздел:

Routing > IPv6 Management and Interfaces > IPv6 Addresses

Routing >> IPv6 Management and Interfaces >> IPv6 Addresses

IPv6 Address Table

Interface: VLAN 1

Q []

☐	IPv6 Address Type	IPv6 Address	IPv6 Prefix Length	DAD Status
☐	Link Local	fe80::2e0:4cff:fe00:0	64	Active
☐	Multicast	#02::1::00:0		
☐	Multicast	#02::1		
☐	Multicast	#01::1		

12.2.3. Маршрутизация IPv6 (IPv6 Routing)

Для просмотра и настройки IPv6 маршрутизации перейдите в раздел:

Routing > IPv6 Management and Interfaces > IPv6 Routing

Routing >> IPv6 Management and Interfaces >> IPv6 Routes

IPv6 Routing Table

Q []

☐	Destination IP Prefix	Prefix Length	Route Type	Next Hop Router IP Address	Metric	Administrative Distance	Outgoing Interface
0 results found.							

Add IPv6 Static Route

IPv6 Prefix		
IPv6 Prefix Length		(0 - 128)
Next Hop Router IP Address		
Metric	1	(1 - 255, default 1)

Apply

Close

Добавление статического маршрута IPv6:

1. Нажмите **Add** (добавить)
2. Укажите:
 - IPv6-сеть назначения
 - Длину префикса
 - Шлюз (Next Hop)
3. Сохраните настройки (**apply**)

12.2.4. Настройка IPv6 Neighbors (IPv6 Neighbors)

Для настройки IPv6 Neighbors перейдите в раздел:

Routing > IPv6 Management and Interfaces > IPv6 Neighbors

Routing » IPv6 Management and Interfaces » IPv6 Neighbors

Clear Neighbor Table

☐ All
☐ Dynamic
☐ Static
☒ N/A

Apply

Cancel

IPv6 Neighbor Table

☐	Interface	IPv6 Address	MAC Address	Status	Router
0 results found.					

Add

Edit

Delete

Routing » IPv6 Management and Interfaces » IPv6 Neighbors

Add Neighbor

Interface

VLAN

IP Address

MAC Address

Apply

Close

Добавление постоянной (static) записи:

1. Нажмите **Add** (добавить)
2. Укажите:
 - IPv6-адрес
 - MAC-адрес
 - Интерфейс
3. Сохраните настройки (**apply**)

12.3. Управление маршрутизацией по протоколу RIP (RIP Routes Management)

Для настройки маршрутизации с помощью протокола RIP перейдите в раздел:

Routing > RIP Routes Management > RIP Routes Setting

Routing >> Rip Routes Management >> Rip Routes Setting

Rip Routes Info

Rip Routes status ☐ Enable

Apply

Network Setting table

Showing [All] entries Showing 0 to 0 of 0 entries

Network Ipv4 Address	Network Mask
0 results found.	

Add Delete First Previous 1 Next Last

Routing >> Rip Routes Management >> Rip Routes Setting

Network Setting table

Network Ipv4 Address

Network Mask

Apply Close

Чтобы настроить RIP маршрутизацию:

1. Активируйте **RIP Routes Status** (enable)
2. Нажмите **Add** (добавить) для добавления сети в маршрутизацию RIP
3. Сохраните настройки (**apply**)

12.4. Управление маршрутизацией по протоколу OSPF (OSPF Routes Management)

Для настройки маршрутизации с помощью протокола OSPF перейдите в раздел:

Routing > OSPF Routes Management > OSPF Routes Setting

Routing >> Ospf Routes Management >> Ospf Routes Setting

OSPF Routes Info

OSPF Routes status ☐ Enable

Apply

Area Network Setting table

Showing All entries Showing 0 to 0 of 0 entries

Area Id	Network Ipv4 Address	Network Mask
0 results found.		

Add Delete First Previous 1 Next Last

Routing >> Ospf Routes Management >> Ospf Routes Setting

Area Network Setting table

Area Id	A.B.C.D
Network Ipv4 Address	
Network Mask	

Apply Close

Чтобы настроить OSPF маршрутизацию:

1. Активируйте **OSPF Routes Status** (enable)
2. Нажмите **Add** (добавить) для добавления сети в маршрутизацию OSPF.
3. Сохраните настройки (**apply**)

Примечания

1. **Постоянные (static) маршруты** рекомендуются для небольших сетей с фиксированной топологией.
2. **RIP** маршрутизация подходит для простых сетей, **OSPF** маршрутизация – для крупных и сложных.
3. Для IPv6 обязательно настройте протокол **NDP (Neighbor Discovery Protocol)**.

Пример настройки OSPF

- Включите **OSPF Routes Status**
- Добавьте сеть **192.168.1.0/24** в зону **0.0.0.0 (Backbone)**.
- Укажите интерфейс, подключенный к этой сети.
- Сохраните конфигурацию.

13. Безопасность (Security)

Используйте раздел **Security** для настройки функций безопасности коммутатора.

13.1. Настройки протокола RADIUS (RADIUS)

RADIUS – расширенный протокол удаленной аутентификации пользователей, представляет собой ключевой элемент в обеспечении безопасности и управлении доступом в сетях.

Для настройки параметров протокола RADIUS перейдите:

Security > RADIUS

На этой странице можно добавлять, редактировать или удалять RADIUS-серверы, а также изменять их параметры по умолчанию.

Use Default Parameter

Retry	3	(1 - 10, default 3)
Timeout	3	Sec (1 - 30, default 3)
Key String		

Apply

Глобальные параметры RADIUS

Параметр	Описание
Retry	Количество попыток подключения к серверу (по умолчанию 3).
Timeout	Время ожидания ответа от сервера (в секундах) (по умолчанию 3).
Key String	Общий ключ (пароль) для аутентификации на RADIUS-сервере.

RADIUS Table

Showing All entries Showing 1 to 1 of 1 entries Q

☐	Server Address	Server Port	Priority	Retry	Timeout	Usage
☐	192.168.1.98	1812	1	3	3	All

AddEditDelete

FirstPrevious1NextLast

Настройки RADIUS-серверов

Параметр	Описание
Server Address	IP-адрес или доменное имя RADIUS-сервера.
Server Port	Порт RADIUS-сервера (обычно <u>1812</u> для аутентификации).
Priority	Приоритет сервера (чем меньше число, тем выше приоритет). При аутентификации сначала используется сервер с наивысшим приоритетом.
Retry	Количество попыток подключения для этого сервера.
Timeout	Время ожидания ответа (в секундах) для этого сервера.
Usage	Тип аутентификации: • Login – для входа на коммутатор. • 802.1x – для аутентификации клиентов по стандарту 802.1X. • All – для всех типов.

Add RADIUS Server

Address Type	☒ Hostname ☐ IPv4 ☐ IPv6	
Server Address	192.168.1.98	
Server Port	1812	(0 - 65535, default 1812)
Priority	1	(0 - 65535)
Key String	☒ Use Default 	
Retry	☒ Use Default 3 (1 - 10, default 3)	
Timeout	☒ Use Default 3 Sec (1 - 30, default 3)	
Usage	☐ Login ☐ 802.1X ☒ All	

Security » RADIUS

Edit RADIUS Server

Server Address	192.168.1.98	
Server Port	1812	(0 - 65535, default 1812)
Priority	1	(0 - 65535)
Key String	☒ Use Default 	
Retry	☒ Use Default 3 (1 - 10, default 3)	
Timeout	☒ Use Default 3 Sec (1 - 30, default 3)	
Usage	☐ Login ☐ 802.1X ☒ All	

Добавление/редактирование RADIUS-сервера

Параметр	Описание
Address Type	Тип адреса сервера: • Hostname – доменное имя. • IPv4 – IPv4-адрес. • IPv6 – IPv6-адрес.
Server Address	Адрес сервера (в зависимости от выбранного типа).
Server Port	Порт сервера.
Priority	Приоритет сервера (1 – наивысший).
Retry	Количество попыток подключения.
Timeout	Время ожидания ответа.
Usage	Тип аутентификации (Login, 802.1X, All).

Примечания

1. **RADIUS** используется для централизованной аутентификации пользователей и устройств.
2. Для работы **802.1X** необходимо указать сервер с типом **802.1x** или **All**.
3. Рекомендуется настраивать несколько серверов с разными приоритетами для отказоустойчивости.

Пример настройки

- **Глобальные параметры:**
 - **Retry:** 3
 - **Timeout:** 5 сек.
 - **Key String:** secret123
- **Добавление сервера:**
 - **Address Type:** IPv4
 - **Server Address:** 192.168.1.100
 - **Server Port:** 1812
 - **Priority:** 1
 - **Retry:** 2
 - **Timeout:** 3 сек.
 - **Usage:** All
- Сохраните настройки (**Apply**)

13.2. Настройки протокола TACACS+ (TACACS+)

TACACS+ это протокол безопасности, разработанный компанией Cisco.

Для настройки параметров TACACS+ перейдите:

Security > TACACS+

На этой странице можно добавлять, редактировать или удалять TACACS+-серверы, а также изменять их параметры по умолчанию.

Security >> TACACS+

The screenshot shows a web interface for configuring TACACS+ parameters. At the top, there is a red banner with the text "Use Default Parameter". Below this, there are two input fields: "Timeout" with the value "5" and "Key String" which is empty. To the right of the "Timeout" field, there is a text label "Sec (1 - 30, default 5)". At the bottom of the configuration area, there is a blue "Apply" button.

Глобальные параметры TACACS+

Параметр	Описание
Timeout	Время ожидания ответа от сервера (в секундах) по умолчанию.
Key String	Общий ключ (пароль) для аутентификации на TACACS+-сервере.

TACACS+ Table

Showing **All** entries Showing 1 to 1 of 1 entries

☐	Server Address	Server Port	Priority	Timeout
☐	192.168.1.97	49	1	5

Настройки TACACS+-серверов

Параметр	Описание
Server Address	IP-адрес или доменное имя TACACS+-сервера.
Server Port	Порт TACACS+-сервера (как правило – 49).
Priority	Приоритет сервера (чем меньше число, тем выше приоритет). При аутентификации сначала используется сервер с наивысшим приоритетом.
Timeout	Время ожидания ответа (в секундах) для этого сервера.

Add TACACS+ Server

Address Type	☒ Hostname ☐ IPv4 ☐ IPv6	
Server Address	192.168.1.97	
Server Port	49	(0 - 65535, default 49)
Priority	1	(0 - 65535)
Key String	☒ Use Default 	
Timeout	☒ Use Default 5 Sec (1 - 30, default 5)	

Edit TACACS+ Server

Server Address	192.168.1.97	
Server Port	49	(0 - 65535, default 49)
Priority	1	(0 - 65535)
Key String	☒ Use Default 	
Timeout	☒ Use Default 5 Sec (1 - 30, default 5)	

Добавление/редактирование TACACS+-сервера

Параметр	Описание
Address Type	Тип адреса сервера: • Hostname – доменное имя. • IPv4 – IPv4-адрес. • IPv6 – IPv6-адрес.
Server Address	Адрес сервера (в зависимости от выбранного типа).
Server Port	Порт сервера.
Priority	Приоритет сервера (1 – наивысший).
Timeout	Время ожидания ответа.

Примечания

1. **TACACS+** обеспечивает централизованную аутентификацию, авторизацию и учёт (AAA) для сетевых устройств.
2. В отличие от RADIUS, TACACS+ использует TCP (как правило – 49) и поддерживает более детальный контроль доступа.
3. Рекомендуется настраивать несколько серверов с разными приоритетами для отказоустойчивости.

Пример настройки

- **Глобальные параметры:**
 - **Timeout:** 5 сек.
 - **Key String:** tacacs_key_123
- **Добавление сервера:**

- **Address Type:** IPv4
- **Server Address:** 192.168.1.101
- **Server Port:** 49
- **Priority:** 1
- **Timeout:** 3 сек.
- Сохраните настройки (**Apply**)

13.3. AAA (Аутентификация, Авторизация и Учет пользователей)

13.3.1. Списки методов AAA (Method List)

Для настройки списков методов аутентификации перейдите:

Security > AAA > Method List

На этой странице WEB интерфейса можно создавать, редактировать и удалять списки методов аутентификации (список "default" нельзя удалить). Коммутатор будет последовательно пытаться аутентифицировать пользователя с помощью указанных методов - если первый метод не сработает, будет использован следующий и т.д.

Security >> AAA >> Method List

Method List Table

Showing All entries Showing 1 to 2 of 2 entries

☐	Name	Sequence
☐	default	(1) Local
☐	TEST	(1) TACACS+

Таблица списков методов AAA

Параметр	Описание
Name	Уникальное имя списка методов аутентификации.

Последовательность методов AAA

Параметр	Описание
None	Разрешает доступ без аутентификации.
Local	Использует локальную базу учетных записей коммутатора.
TACACS+	Аутентификация через TACACS+ сервер.
RADIUS	Аутентификация через RADIUS сервер.
Enable	Использует пароль коммутатора для аутентификации.

Edit Method List

Name	TEST
Method 1	☐ Empty ☐ None ☐ Local ☐ Enable ☐ RADIUS ☒ TACACS+
Method 2	☒ Empty ☐ None ☐ Local ☐ Enable ☐ RADIUS ☐ TACACS+
Method 3	☐ Empty ☐ None ☒ Local ☐ Enable ☐ RADIUS ☐ TACACS+
Method 4	☒ Empty ☐ None ☐ Local ☐ Enable ☐ RADIUS ☐ TACACS+

Настройка списка методов AAA

Параметр	Описание
Name	Уникальное имя списка методов.

Приоритетные методы аутентификации

Параметр	Описание
Method 1	Первичный метод аутентификации (наивысший приоритет).

Параметр	Описание
	• None – Разрешает доступ без аутентификации. • Local – Использует локальную базу учетных записей коммутатора. • TACACS+ – Аутентификация через TACACS+ сервер. • RADIUS – Аутентификация через RADIUS сервер. • Enable – Использует пароль коммутатора для аутентификации
Method 2	Вторичный метод аутентификации. • None – Разрешает доступ без аутентификации. • Local – Использует локальную базу учетных записей коммутатора. • TACACS+ – Аутентификация через TACACS+ сервер. • RADIUS – Аутентификация через RADIUS сервер. • Enable – Использует пароль коммутатора для аутентификации
Method 3	Третий метод аутентификации. • None – Разрешает доступ без аутентификации. • Local – Использует локальную базу учетных записей коммутатора. • TACACS+ – Аутентификация через TACACS+ сервер. • RADIUS – Аутентификация через RADIUS сервер. • Enable – Использует пароль коммутатора для аутентификации
Method 4	Четвертый метод аутентификации.

Параметр	Описание
	• None – Разрешает доступ без аутентификации. • Local – Использует локальную базу учетных записей коммутатора. • TACACS+ – Аутентификация через TACACS+ сервер. • RADIUS – Аутентификация через RADIUS сервер. • Enable – Использует пароль коммутатора для аутентификации

Примечания

1. Рекомендуемая последовательность:
 - TACACS+/RADIUS (основной метод)
 - Local (резервный метод)
 - Enable (аварийный доступ)
2. При использовании **TACACS+/RADIUS**:
 - **Failed** означает проблемы с подключением к серверу
 - Для локального метода - отсутствие пользователя в базе
3. Список **Default** содержит базовые настройки и не может быть удален.

Пример настройки

- Имя списка "Admin_Access":
 - **Method 1:** TACACS+
 - **Method 2:** RADIUS
 - **Method 3:** Local
 - **Method 4:** Enable
- Для общего доступа:

- **Method 1:** RADIUS
- **Method 2:** Local
- Для аварийного доступа:
 - **Method 1:** Enable

13.3.2. Аутентификация входа (Login Authentication)

Для настройки политик аутентификации для различных способов управления коммутатором перейдите:

Security > AAA > Login Authentication

На этой странице можно назначить списки методов аутентификации (из раздела 13.3.1) для всех способов доступа к коммутатору.

Security >> AAA >> Login Authentication

Console	default ▼	(1) Local
Telnet	default ▼	(1) Local
SSH	TEST ▼	(1) TACACS+
HTTP	default ▼	(1) Local
HTTPS	TEST ▼	(1) TACACS+

Apply

Настройки аутентификации

Параметр	Описание
Console	Список аутентификации для доступа через порт Console на коммутаторе.

Параметр	Описание
Telnet	Список аутентификации для способа управления коммутатором через Telnet.
SSH	Список аутентификации для способа управления коммутатором через SSH.
HTTP	Список аутентификации для способа управления коммутатором через WEB-интерфейс по HTTP.
HTTPS	Список аутентификации для способа управления коммутатором через веб-интерфейса по защищенному протоколу HTTPS.

Примечания

1. Для каждого интерфейса можно выбрать любой созданный ранее список методов (например, **Default** или **Admin_Access**).
2. Рекомендуется:
 - Для **Console** оставить Local/Enable на случай аварийного доступа
 - Для **SSH/HTTPS** использовать строгую аутентификацию (TACACS+/RADIUS + Local)
 - Для **Telnet/HTTP** либо отключить эти сервисы, либо назначить строгую аутентификацию

Пример настройки

1. **Console**: default (Local > Enable)
2. **SSH/HTTPS**: Admin_Access (TACACS+ > RADIUS > Local)
3. **Telnet/HTTP**: None (отключить эти сервисы в настройках сервисов)

13.4. Управление доступом к коммутатору (Management Access)

Раздел **Management Access** позволяет настраивать параметры доступа к управлению коммутатором.

13.4.1. VLAN управления (Management VLAN)

Для настройки Management VLAN перейдите:

Security > Management Access > Management VLAN

На этой странице можно назначить VLAN, через который разрешено управление коммутатором (например, через HTTP, HTTPS, SNMP и другие протоколы).

Security >> Management Access >> Management VLAN

Management VLAN

1 - default

Note: Change Management VLAN may cause connection interrupted

Apply

Параметры управляющего VLAN

Параметр	Описание
Management VLAN	Выберите VLAN, который будет использоваться для управления коммутатором. • Только подключения из этого VLAN будут разрешены. • Все остальные подключения (из других VLAN) будут блокироваться. VLAN 1 – VLAN управления по умолчанию.

Примечания

1. Безопасность:

- Назначение отдельного VLAN для управления повышает безопасность, изолируя управляющий трафик от пользовательского.
- Рекомендуется использовать **нестандартный VLAN ID** (не VLAN 1) в целях безопасности.

2. Совместимость:

- Убедитесь, что выбранный VLAN существует и настроен на коммутаторе.
- Для доступа к устройству из другого VLAN потребуется маршрутизация между VLAN.

3. Протоколы:

- Настройка применяется ко всем протоколам управления:
 - WEB-интерфейс (HTTP/HTTPS)
 - Telnet/SSH
 - SNMP
 - Другие сервисы (например, RADIUS/TACACS+)

Пример настройки

1. Создайте отдельный VLAN для управления (например, **VLAN 100**).
2. Назначьте ему IP-адрес (если требуется доступ из других сетей).
3. На этой странице выберите **Management VLAN = 100**.
4. Сохраните настройки.

13.4.2. Настройка способов и сервисов управления коммутатором (Management Service)

Для настройки сервисов управления перейдите:

Security > Management Access > Management Service

На этой странице можно включать/отключать сервисы доступа к управлению, а также настраивать параметры безопасности сессий.

Security >> Management Access >> Management Service

Management Service		
Telnet	☐	Enable
SSH	☐	Enable
HTTP	☒	Enable
HTTPS	☐	Enable
SNMP	☐	Enable

Session Timeout		
Console	10	Min (0 - 65535, default 10)
Telnet	10	Min (0 - 65535, default 10)
SSH	10	Min (0 - 65535, default 10)
HTTP	10	Min (0 - 65535, default 10)
HTTPS	10	Min (0 - 65535, default 10)

Password Retry Count		
Console	3	(0 - 120, default 3)
Telnet	3	(0 - 120, default 3)
SSH	3	(0 - 120, default 3)

Silent Time		
Console	0	Sec (0 - 65535, default 0)
Telnet	0	Sec (0 - 65535, default 0)
SSH	0	Sec (0 - 65535, default 0)

Apply

Включение/отключение различных способов управления коммутатором

Параметр	Описание
Telnet	Включение/отключение доступа к CLI через Telnet. <i>(Не рекомендуется из-за отсутствия шифрования)</i>
SSH	Включение/отключение защищенного доступа к CLI через SSH. <i>(Рекомендуется для безопасного управления коммутатором)</i>
HTTP	Включение/отключение доступа к WEB-интерфейсу по HTTP <i>(Не рекомендуется для производственных сетей)</i>
HTTPS	Включение/отключение доступа к WEB-интерфейсу по HTTPS <i>(Рекомендуется для безопасного доступа)</i>
SNMP	Включение/отключение управления коммутатором через протокол SNMP.

Параметры безопасности

Параметр	Описание
Session Timeout	Время неактивности (в минутах), после которого сессия управления автоматически завершается. 0 = отсутствие таймаута. <i>(Рекомендуется: 10-30 минут)</i>
Password	Максимальное количество неудачных попыток ввода

Параметр	Описание
Retry Count	пароля перед блокировкой. <i>(Рекомендуется: 3-5 попыток)</i>
Silent Time	Время блокировки (в минутах) после превышения числа попыток ввода пароля. <i>(Рекомендуется: 5-15 минут)</i>

Рекомендации по настройке

1. Безопасные протоколы:

- По возможности всегда используйте **SSH** вместо Telnet и **HTTPS** вместо HTTP.
- Отключите Telnet и HTTP в производственных средах в целях повышения безопасности.

2. Таймаут сессии:

- Установите 30 минут для баланса между безопасностью и удобством.

3. Защита от перебора паролей:

- Password Retry Count = 3
- Silent Time = 10 минут

4. SNMP:

- Включайте только при необходимости, используйте SNMPv3 с шифрованием.

Пример конфигурации

1. Включите:

- **SSH и HTTPS**

2. Отключите:

➤ **Telnet и HTTP**

3. Установите:

- Session Timeout = 30
- Password Retry Count = 3
- Silent Time = 10

Внимание! После отключения Telnet/HTTP убедитесь, что SSH/HTTPS работают корректно.

13.4.3. ACL для управления коммутатором (Management ACL)

Для настройки ACL (Access Control List) для управления коммутатором перейдите:

Security > Management Access > Management ACL

На этой странице можно создавать и удалять правила ACL, ограничивающие доступ к интерфейсам управления коммутатором.

Security >> Management Access >> Management ACL

ACL Name

Apply

Management ACL Table

Showing **All** entries Showing 1 to 3 of 3 entries

	ACL Name	State	Rule
☐	aaa	Deactive	0
☐	bbb	Deactive	0
☐	ccc	Deactive	0

Active Deactive Delete

First Previous **1** Next Last

Основные параметры

Параметр	Описание
ACL Name	Уникальное имя ACL.
State	Статус ACL (активен/неактивен).
Rule	Количество правил в ACL.

Добавление/удаление правил Management ACL

1. Создание ACL:

- Введите имя ACL (например, MGMT_ACCESS).
- Нажмите **Apply**

2. Настройка правил:

- Укажите:
 - **Тип правила** (разрешить/запретить)
 - **IP-адрес/подсеть** источника
 - **Протокол** (SSH, HTTPS и т.д.)
 - **Порт** (если требуется)

3. Активация ACL:

- Выберите созданный ACL и нажмите **Active**

Примечания

1. Цель создания Management ACL:

- Ограничить доступ к управлению коммутатором только с доверенных IP-адресов.

2. Рекомендации:

- Разрешите только подсети администраторов (например, 192.168.1.0/24).
- Запретите все остальные подключения.

Внимание!

Не удаляйте активные ACL – это может привести к потере доступа к коммутатору!

Пример настройки

1. Создайте ACL с именем ADMIN_ACCESS.
2. Добавьте правила:
 - Разрешить 192.168.1.0/24 для SSH/HTTPS.
 - Запретить все остальные IP.
3. Активируйте ACL.

13.4.4. Правила ACE для управления коммутатором (Management ACE)

Для настройки правил ACE (Access Control Entry) в рамках ACL перейдите:

Security > Management Access > Management ACE

На этой странице WEB интерфейса можно добавлять, редактировать и удалять правила ACE, которые определяют, какие IP-адреса и сервисы могут управлять коммутатором.

Security >> Management Access >> Management ACE

Management ACE Table

ACL Name aaa

Showing All entries Showing 1 to 2 of 2 entries

☐	Priority	Action	Service	Port	Address / Mask
☐	1	Deny	Snmp	GE1,GE3,GE6	N/A
☐	2	Deny	Snmp	GE1,GE4	N/A

Add Edit Delete

First Previous 1 Next Last

Просмотр существующих правил ACE

Параметр	Описание
ACL Name	Имя ACL, к которому относится правило.
Priority	Приоритет правила (чем меньше число, тем выше приоритет).
Action	Действие: Permit (разрешить) или Deny (запретить).
Service	Способ/сервис управления, к которому применяется правило (HTTP, SSH и т.д.).
Port	Порт(ы), к которым применяется правило.
Address / Mask	Исходный IP-адрес и маска подсети.

Security » Management Access » Management ACE

Add Management ACE

ACL Name	aaa		
Priority	1	(1 - 65535)	
Service	☐ All ☐ Http ☐ Https ☒ Snmp ☐ SSH ☐ Telnet		
Action	☐ Permit ☒ Deny		
Port	Available Port GE1 GE2 GE3 GE4 GE5 GE6 GE7 GE8	→ ←	Selected Port
IP Version	☒ All ☐ IPv4 ☐ IPv6		
IPv4	/ 255.255.255.255		
IPv6	/ 128 (1 - 128)		

Edit Managemet ACE

ACL Name	aaa	
Priority	1	
Service	☐ All ☐ Http ☐ Https ☒ Snmp ☐ SSH ☐ Telnet	
Action	☐ Permit ☒ Deny	
Port	Available Port GE2 GE4 GE5 GE7 GE8 GE9 GE10 LAG1	Selected Port GE1 GE3 GE6
IP Version	☒ All ☐ IPv4 ☐ IPv6	
IPv4	/ 255.255.255.255	
IPv6	/ 128 (1 - 128)	
Apply Close		

Добавление/редактирование правил ACE

Параметр	Описание
ACL Name	Выберите ACL, к которому добавляется правило.
Priority	Приоритет (1 – наивысший). <i>Доступно только при добавлении.</i>
Service	Сервис/способ управления коммутатором: All – все сервисы.

Параметр	Описание
	HTTP/HTTPS – WEB-интерфейс. SSH/Telnet – CLI. SNMP – управление через SNMP протокол.
Action	Действие: Permit – разрешить доступ. Deny – запретить доступ.
Port	Выберите порт(ы) для применения правила.
IP Version	Версия IP: All – все адреса. IPv4 – только IPv4. IPv6 – только IPv6.
IPv4	Укажите IPv4-адрес и маску подсети (например, 192.168.1.0/24).
IPv6	Укажите IPv6-адрес и префикс (например, 2001:db8::/32).

Примечания

1. Порядок обработки:

- Правила ACE обрабатываются по приоритету (от высшего к низшему).
- После совпадения с правилом дальнейшая проверка прекращается.

2. Ограничения:

- Нельзя редактировать/удалять правила в активном ACL.

- Нельзя добавлять новые правила ACE в активный ACL (сначала отключите его).

3. Рекомендации:

- Сначала добавляйте разрешающие правила для доверенных IP, затем запрещающие для всех остальных.
- Для SSH/HTTPS используйте только Permit для административных подсетей.

Пример настройки

1. Выберите список, например – ACL ADMIN_ACCESS.
2. Добавьте правило:
 - **Priority:** 1
 - **Service:** SSH
 - **Action:** Permit
 - **IP Version:** IPv4
 - **IPv4:** 192.168.1.0/24
3. Добавьте второе правило:
 - **Priority:** 2
 - **Service:** All
 - **Action:** Deny
 - **IP Version:** All

Результат: Разрешен доступ по SSH только из 192.168.1.0/24, все остальные подключения к коммутатору запрещены.

13.5. Менеджер аутентификации (Authentication Manager)

13.5.1. Свойства Authentication Manager (Property)

Для настройки параметров менеджера аутентификации перейдите:

Security > Authentication Manager > Property

На этой странице можно настроить глобальные параметры аутентификации и конфигурации для отдельных портов.

Security >> Authentication Manager >> Property

Authentication Type

Guest VLAN

MAC-Based User ID Format

☐ 802.1x

☐ MAC-Based

☐ WEB-Based

☐ Enable

1

▼

XXXXXXXXXXXX ▼

Apply

Глобальные настройки аутентификации

Параметр	Описание
Authentication Type	Включение типов аутентификации: 802.1X – стандартная аутентификация по IEEE 802.1X MAC-Based – аутентификация по MAC-адресу WEB-Based – аутентификация через WEB-интерфейс

Параметр	Описание
Guest VLAN	Включение гостевого VLAN (требуется указать VLAN ID)
MAC-Based User ID Format	Формат MAC-адреса для аутентификации (20 вариантов, включая верхний/нижний регистр и разделители :, -, .) • XXXXXXXXXXXXX • xxxxxxxxxxxxx • XX:XX:XX:XX:XX:XX • xx:xx:xx:xx:xx:xx • XX-XX-XX-XX-XX-XX • xx-xx-xx-xx-xx-xx • XX.XX.XX.XX.XX.XX • xx.xx.xx.xx.xx.xx • XXXX:XXXX:XXXX • xxxx:xxxx:xxxx • XXXX-XXXX-XXXX • xxxx-xxxx-xxxx • XXXX.XXXX.XXXX • xxxx.xxxx.xxxx • XXXXXX:XXXXXX • xxxxxx:xxxxxx • XXXXXX-XXXXXX • xxxxxx-xxxxxx XXXXXX.XXXXXX xxxxxx.xxxxxx

Q

☐	Entry	Port	Authentication Type			Host Mode	Order	Method	Guest VLAN	VLAN Assign Mode	
			802.1x	MAC-Based	WEB-Based						
☐	1	GE1	Disabled	Disabled	Disabled	Multiple Authentication	802.1x	RADIUS	Disabled	Static	
☐	2	GE2	Disabled	Disabled	Disabled	Multiple Authentication	802.1x	RADIUS	Disabled	Static	
☐	3	GE3	Disabled	Disabled	Disabled	Multiple Authentication	802.1x	RADIUS	Disabled	Static	
☐	4	GE4	Disabled	Disabled	Disabled	Multiple Authentication	802.1x	RADIUS	Disabled	Static	
☐	5	GE5	Disabled	Disabled	Disabled	Multiple Authentication	802.1x	RADIUS	Disabled	Static	
☐	6	GE6	Disabled	Disabled	Disabled	Multiple Authentication	802.1x	RADIUS	Disabled	Static	
☐	7	GE7	Disabled	Disabled	Disabled	Multiple Authentication	802.1x	RADIUS	Disabled	Static	
☐	8	GE8	Disabled	Disabled	Disabled	Multiple Authentication	802.1x	RADIUS	Disabled	Static	
☐	9	GE9	Disabled	Disabled	Disabled	Multiple Authentication	802.1x	RADIUS	Disabled	Static	
☐	10	GE10	Disabled	Disabled	Disabled	Multiple Authentication	802.1x	RADIUS	Disabled	Static	
☐	11	GE11	Disabled	Disabled	Disabled	Multiple Authentication	802.1x	RADIUS	Disabled	Static	
☐	12	GE12	Disabled	Disabled	Disabled	Multiple Authentication	802.1x	RADIUS	Disabled	Static	
☐	13	GE13	Disabled	Disabled	Disabled	Multiple Authentication	802.1x	RADIUS	Disabled	Static	
☐	14	GE14	Disabled	Disabled	Disabled	Multiple Authentication	802.1x	RADIUS	Disabled	Static	
☐	15	GE15	Disabled	Disabled	Disabled	Multiple Authentication	802.1x	RADIUS	Disabled	Static	
☐	16	GE16	Disabled	Disabled	Disabled	Multiple Authentication	802.1x	RADIUS	Disabled	Static	
☐	17	GE17	Disabled	Disabled	Disabled	Multiple Authentication	802.1x	RADIUS	Disabled	Static	
☐	18	GE18	Disabled	Disabled	Disabled	Multiple Authentication	802.1x	RADIUS	Disabled	Static	
☐	19	GE19	Disabled	Disabled	Disabled	Multiple Authentication	802.1x	RADIUS	Disabled	Static	
☐	20	GE20	Disabled	Disabled	Disabled	Multiple Authentication	802.1x	RADIUS	Disabled	Static	
☐	21	GE21	Disabled	Disabled	Disabled	Multiple Authentication	802.1x	RADIUS	Disabled	Static	
☐	22	GE22	Disabled	Disabled	Disabled	Multiple Authentication	802.1x	RADIUS	Disabled	Static	
☐	23	GE23	Disabled	Disabled	Disabled	Multiple Authentication	802.1x	RADIUS	Disabled	Static	
☐	24	GE24	Disabled	Disabled	Disabled	Multiple Authentication	802.1x	RADIUS	Disabled	Static	
☐	25	TE1	Disabled	Disabled	Disabled	Multiple Authentication	802.1x	RADIUS	Disabled	Static	
☐	26	TE2	Disabled	Disabled	Disabled	Multiple Authentication	802.1x	RADIUS	Disabled	Static	
☐	27	TE3	Disabled	Disabled	Disabled	Multiple Authentication	802.1x	RADIUS	Disabled	Static	
☐	28	TE4	Disabled	Disabled	Disabled	Multiple Authentication	802.1x	RADIUS	Disabled	Static	

Edit

Таблица аутентификации по портам

Параметр	Описание
Port	Имя порта
Authentication Type	Состояние типов аутентификации для порта: 802.1X MAC-Based WEB-Based С параметрами Disbale (откл) Enable (вкл)

Параметр	Описание
Host Mode	Режим аутентификации устройств: Multiple Authentication – каждое устройство аутентифицируется отдельно Multiple Hosts – одно устройство проходит аутентификацию для всех (не поддерживает WEB-Based) Single Host – только одно устройство
Order	Порядок проверки типов аутентификации (WEB-Based всегда последний) • 802.1x • MAC-Based • WEB-Based • 802.1x MAC-Based • 802.1x WEB-Based • MAC-Based 802.1x • WEB-Based 802.1x • 802.1x MAC-Based WEB-Based • 802.1x WEB-Based MAC-Based
Method	Методы аутентификации (для MAC/WEB): Local – локальная база аутентификации Radius – удаленный сервер RADIUS Local Radius – сначала локальная, затем RADIUS аутентификация. RadiusLocal – сначала RADIUS, затем локальная аутентификация
Guest VLAN	Включение гостевого VLAN для порта

Параметр	Описание
	С параметрами Disable (откл) Enable (вкл)
VLAN Assign Mode	Режим назначения VLAN (только для RADIUS аутентификации): Disable – игнорировать VLAN из RADIUS Reject – требовать VLAN от RADIUS Static – использовать VLAN из RADIUS (если настроено)

Security » Authentication Manager » Property

Edit Port Mode

Port	GE1-GE3	
Authentication Type	☐ 802.1x ☐ MAC-Based ☐ WEB-Based	
Host Mode	☒ Multiple Authentication ☐ Multiple Hosts ☐ Single Host	
Order	Available Type MAC-Based WEB-Based	Select Type 802.1x
Method	Available Method Local	Select Method RADIUS
Guest VLAN	☐ Enable ☐ Disable	
VLAN Assign Mode	☐ Reject ☒ Static	

Apply

Close

Параметр	Описание
Port	Имя порта
Authentication Type	Выбор типа аутентификации для порта: 802.1X MAC-Based WEB-Based
Host Mode	Режим аутентификации устройств: Multiple Authentication – каждое устройство аутентифицируется отдельно Multiple Hosts – одно устройство проходит аутентификацию для всех (не поддерживает WEB-Based) Single Host – только одно устройство
Order	Порядок проверки типов аутентификации (WEB-Based всегда последний) • 802.1x • MAC-Based • WEB-Based • 802.1x MAC-Based • 802.1x WEB-Based • MAC-Based 802.1x • WEB-Based 802.1x • 802.1x MAC-Based WEB-Based • 802.1x WEB-Based MAC-Based
Method	Методы аутентификации (для MAC/WEB):

Параметр	Описание
	Local – локальная база аутентификации Radius – удаленный сервер RADIUS Local Radius – сначала локальная, затем RADIUS аутентификация. RadiusLocal – сначала RADIUS, затем локальная аутентификация
Guest VLAN	Включение гостевого VLAN для порта
VLAN Assign Mode	Режим назначения VLAN (только для RADIUS аутентификации): Disable – игнорировать VLAN из RADIUS Reject – требовать VLAN от RADIUS Static – использовать VLAN из RADIUS (если настроено)

Примечания

1. **WEB-Based** аутентификация всегда должна быть последней в порядке проверки.
2. Для **802.1X** поддерживается только метод **Radius**.
3. В режиме **Multiple Hosts** WEB-аутентификация недоступна.

Пример настройки

- **Глобальные параметры:**
 - Включите **802.1X** и **MAC-Based**.
 - Выберите формат MAC-адреса: XX-XX-XX-XX-XX-XX.
- **Для порта GE1:**

- **Host Mode:** Multiple Authentication
- **Order:** 802.1X → MAC-Based
- **Method:** Radius
- **VLAN Assign Mode:** Static
- **Для порта GE2 (гостевой доступ):**
 - Включите **Guest VLAN** (VLAN 100).
 - **Order:** WEB-Based
 - **Method:** Local Radius

13.5.2. Настройки портов для аутентификации (Port Setting)

Для настройки параметров аутентификации на портах перейдите:

Security > Authentication Manager > Port Setting

На этой странице WEB интерфейса можно настроить режимы контроля доступа, таймеры и параметры аутентификации для каждого порта.

Security >> Authentication Manager >> Port Setting

Port Setting Table

	Entry	Port	Port Control	Reauthentication	Max Hosts	Common Timer			802.1x Parameters			
						Reauthentication	Inactive	Quiet	TX Period	Supplicant Timeout	Server Timeout	Max Requ
☐	1	GE1	Disabled	Disabled	256	3600	60	60	30	30	30	30
☐	2	GE2	Disabled	Disabled	256	3600	60	60	30	30	30	30
☐	3	GE3	Disabled	Disabled	256	3600	60	60	30	30	30	30
☐	4	GE4	Disabled	Disabled	256	3600	60	60	30	30	30	30
☐	5	GE5	Disabled	Disabled	256	3600	60	60	30	30	30	30
☐	6	GE6	Disabled	Disabled	256	3600	60	60	30	30	30	30
☐	7	GE7	Disabled	Disabled	256	3600	60	60	30	30	30	30
☐	8	GE8	Disabled	Disabled	256	3600	60	60	30	30	30	30
☐	9	GE9	Disabled	Disabled	256	3600	60	60	30	30	30	30
☐	10	GE10	Disabled	Disabled	256	3600	60	60	30	30	30	30
☐	11	GE11	Disabled	Disabled	256	3600	60	60	30	30	30	30
☐	12	GE12	Disabled	Disabled	256	3600	60	60	30	30	30	30
☐	13	GE13	Disabled	Disabled	256	3600	60	60	30	30	30	30
☐	14	GE14	Disabled	Disabled	256	3600	60	60	30	30	30	30
☐	15	GE15	Disabled	Disabled	256	3600	60	60	30	30	30	30
☐	16	GE16	Disabled	Disabled	256	3600	60	60	30	30	30	30
☐	17	GE17	Disabled	Disabled	256	3600	60	60	30	30	30	30
☐	18	GE18	Disabled	Disabled	256	3600	60	60	30	30	30	30
☐	19	GE19	Disabled	Disabled	256	3600	60	60	30	30	30	30
☐	20	GE20	Disabled	Disabled	256	3600	60	60	30	30	30	30
☐	21	GE21	Disabled	Disabled	256	3600	60	60	30	30	30	30
☐	22	GE22	Disabled	Disabled	256	3600	60	60	30	30	30	30
☐	23	GE23	Disabled	Disabled	256	3600	60	60	30	30	30	30
☐	24	GE24	Disabled	Disabled	256	3600	60	60	30	30	30	30
☐	25	TE1	Disabled	Disabled	256	3600	60	60	30	30	30	30
☐	26	TE2	Disabled	Disabled	256	3600	60	60	30	30	30	30
☐	27	TE3	Disabled	Disabled	256	3600	60	60	30	30	30	30
☐	28	TE4	Disabled	Disabled	256	3600	60	60	30	30	30	30

Edit

Параметр	Описание
Port	Имя порта
Port Control	Режим контроля доступа: Disable – аутентификация отключена (все устройства имеют доступ) Force Authorized – порт принудительно открыт Force Unauthorized – порт принудительно закрыт Auto – доступ только после успешной аутентификации
Reauthentication	Повторная аутентификация: Enabled – периодическая проверка Disabled – одноразовая аутентификация
Max Hosts	Максимальное число устройств (для режима Multiple Authentication)
Параметры таймера	
Reauthentication	Интервал повторной аутентификации (сек)
Inactive	Время неактивности до отключения (сек)
Quiet	Время блокировки после неудачных попыток (сек)
Параметры 802.1X	
TX Period	Интервал между EAP-запросами (сек)
Supplicant Timeout	Таймаут ожидания ответа от клиента (сек)

Параметр	Описание
Server Timeout	Таймаут ожидания ответа от сервера (сек)
Max Request	Максимальное число попыток запроса

Security » Authentication Manager » Port Setting

Edit Port Setting

Port	GE5	
Port Control	☒ Disabled ☐ Force Authorized ☐ Force Unauthorized ☐ Auto	
Reauthentication	☐ Enable	
Max Hosts	256	(1 - 256, default 256)
Common Timer		
Reauthentication	3600	Sec (300 - 2147483647, default 3600)
Inactive	60	Sec (60 - 65535, default 60)
Quiet	60	Sec (0 - 65535, default 60)
802.1x Parameters		
TX Period	30	Sec (1 - 65535, default 30)
Supplicant Timeout	30	Sec (1 - 65535, default 30)
Server Timeout	30	Sec (1 - 65535, default 30)
Max Request	2	(1 - 10, default 2)
Web-Based Parameters		
Max Login	☐ Infinite 3	(3 - 10, default 3)

Apply

Close

Параметр	Описание
Port	Порт
Port Control	Режим контроля доступа: Disable – аутентификация отключена (все устройства имеют доступ) Force Authorized – порт принудительно открыт Force Unauthorized – порт принудительно закрыт Auto – доступ только после успешной аутентификации
Reauthentication	Повторная аутентификация: Enabled – периодическая проверка (повторная аутентификация) включена
Max Hosts	Максимальное число устройств (для режима Multiple Authentication). От 1 до 256 (значение по умолчанию 256)
Параметры таймера	
Reauthentication	Интервал повторной аутентификации (сек). От 300 до 2147483647сек (значение по умолчанию 3600 сек)
Inactive	Время неактивности до отключения (сек) От 60 до 65535сек (значение по умолчанию 60сек)
Quiet	Время блокировки после неудачных попыток (сек) От 60 до 65535сек (значение по умолчанию 60сек)
Параметры 802.1X	

Параметр	Описание
TX Period	Интервал между EAP-запросами (сек) От 1 до 65535сек (значение по умолчанию 30сек)
Supplicant Timeout	Таймаут ожидания ответа от клиента (сек) От 1 до 65535сек (значение по умолчанию 30сек)
Server Timeout	Таймаут ожидания ответа от сервера (сек) От 1 до 65535сек (значение по умолчанию 30сек)
Max Request	Максимальное число попыток запроса. От 1 до 10 попыток (значение по умолчанию 2)
Параметры WEB аутентификации (WEB based)	
Max Login	Максимальное число неудачных попыток входа (рекомендуется 3-5, значение по умолчанию – 3) Infinite – не ограниченное количество попыток.

Рекомендации по настройке

1. Для **офисных портов**:
 - **Port Control**: Auto
 - **Reauthentication**: Enabled (3600 сек)
 - **Max Hosts**: 1-3
2. Для **гостевых портов**:
 - **Port Control**: Auto
 - **WEB-Based** аутентификация
 - **Max Login**: 3
3. Для **серверных портов**:
 - **Port Control**: Force Authorized

Пример конфигурации

1. Порт GE1 (офисный):

- **Port Control:** Auto
- **Reauthentication:** 3600 сек
- **802.1X Params:** TX Period=30, Max Request=2

2. Порт GE2 (гостевой):

- **Port Control:** Auto
- **WEB-Based Param:** Max Login=3
- **Quiet Timer:** 300 сек

13.5.3. Локальные учетные записи MAC-Based (MAC-Based Local Account)

Для настройки локальных учетных записей MAC-адресов перейдите:

Security > Authentication Manager > MAC-Based Local Account

На этой странице можно добавлять, редактировать и удалять локальные записи для MAC-аутентификации.

Security >> Authentication Manager >> MAC-Based Local Account

MAC-Based Local Account Table

Showing All entries Showing 1 to 1 of 1 entries

	MAC Address	Control	VLAN	Timeout (Sec)	
				Reauthentication	Inactive
☐	00:00:00:00:00:0A	Force Authorized	N/A	3600	60

1

Таблица локальных учетных записей MAC-Based

Параметр	Описание
MAC Address	MAC-адрес устройства (формат: XX-XX-XX-XX-XX-XX). Каждый MAC-адрес может быть добавлен только один раз.
Control	Тип контроля доступа: Force Authorized – устройство всегда получает доступ Force Unauthorized – устройство всегда блокируется
VLAN	VLAN, назначаемый устройству после аутентификации.
Timeout (Reauthentication)	Интервал повторной аутентификации (в секундах).
Timeout (Inactive)	Время неактивности до отключения (в секундах).

Security >> Authentication Manager >> MAC-Based Local Account

Add MAC-Based Local Account

MAC Address	
Port Control	☐ Force Authorized ☒ Force Unauthorized
VLAN	☐ User Defined 1 (1 - 4094)
Assigned Timer	
Reauthentication	☐ User Defined 3600 Sec (300 - 2147483647)
Inactive	☐ User Defined 60 Sec (60 - 65535)

Security >> Authentication Manager >> MAC-Based Local Account

Edit MAC-Based Local Account

MAC Address	00:00:00:00:00:0A	
Port Control	☒ Force Authorized ☐ Force Unauthorized	
VLAN	☐ User Defined 1 (1 - 4094)	
Assigned Timer		
Reauthentication	☒ User Defined 3600	Sec (300 - 2147483647)
Inactive	☒ User Defined 60	Sec (60 - 65535)

Добавление/редактирование учетной записи MAC-Based

Параметр	Описание
MAC Address	MAC-адрес устройства (формат: XX-XX-XX-XX-XX-XX). Каждый MAC-адрес может быть добавлен только один раз.
Control	Тип контроля доступа: Force Authorized – устройство всегда получает доступ Force Unauthorized – устройство всегда блокируется
VLAN	VLAN, назначаемый устройству после аутентификации. (1-4094)
Timeout (Reauthentication)	Интервал повторной аутентификации (сек) От 300 до 2147483647сек (Значение по умолчанию 3600сек)
Timeout (Inactive)	Время неактивности до отключения (сек) От 60 до 65535сек (Значение по умолчанию 60сек)

Нажмите кнопку **Apply** (применить), чтобы применить настройки.

Примечания

1. Использование:

- Для устройств без поддержки 802.1X (принтеры, камеры).

- Для статического назначения VLAN по MAC-адресу.
2. **Приоритет:**
 - Локальные записи имеют приоритет над RADIUS-аутентификацией, если включен метод **Local** или **Local Radius**.
 3. **Формат MAC-адреса:**
 - Должен соответствовать выбранному в глобальных настройках (см. раздел **13.5.1**).

Пример настройки

1. **Добавление принтера:**
 - **MAC Address:** 00-1A-2B-3C-4D-5E
 - **Control:** Force Authorized
 - **VLAN:** 10
 - **Timeout (Reauthentication):** 86400 (1 день)
2. **Блокировка устройства:**
 - **MAC Address:** 00-1E-4F-AB-CD-EF
 - **Control:** Force Unauthorized
3. **Гостевой доступ:**
 - **MAC Address:** A0-B1-C2-D3-E4-F5
 - **VLAN:** 100
 - **Timeout (Inactive):** 1800 (30 минут)

13.5.4. Локальные учетные записи WEB-аутентификации (WEB-Based Local Account)

Для настройки локальных учетных записей веб-аутентификации перейдите:

Security > Authentication Manager > WEB-Based Local Account

На этой странице можно добавлять, редактировать и удалять учетные записи для аутентификации через WEB-интерфейс.

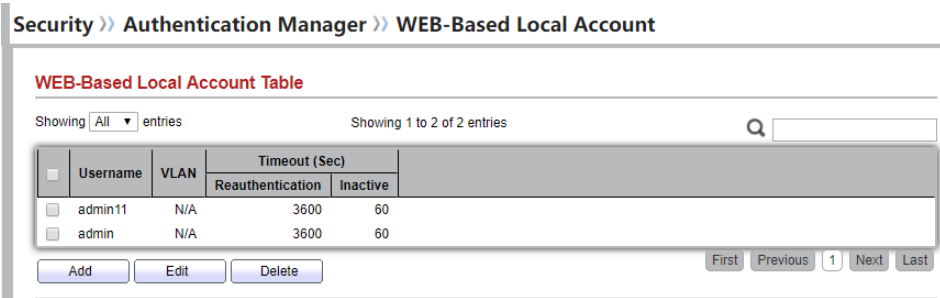


Таблица учетных записей WEB-Based

Параметр	Описание
Username	Логин пользователя
VLAN	VLAN, назначаемый после успешной аутентификации
Timeout (Reauthentication)	Интервал повторной аутентификации (сек)
Timeout (Inactive)	Таймаут неактивности до отключения (сек)

Security » Authentication Manager » WEB-Based Local Account

Add WEB-Based Local Account

Username	admin11	
Password	*****	
Confirm Password	*****	
VLAN	☐ User Defined 1 (1 - 4094)	
Assigned Timer		
Reauthentication	☒ User Defined 3600 Sec (300 - 2147483647)	
Inactive	☒ User Defined 60 Sec (60 - 65535)	
Apply Close		

Security » Authentication Manager » WEB-Based Local Account

Edit WEB-Based Local Account

Username	admin11	
Password		
Confirm Password	*****	
VLAN	☐ User Defined (1 - 4094)	
Assigned Timer		
Reauthentication	☒ User Defined 3600 Sec (300 - 2147483647)	
Inactive	☒ User Defined 60 Sec (60 - 65535)	
Apply Close		

Добавление/редактирование учетной записи

Параметр	Описание
Username	Уникальное имя пользователя (регистрозависимое)
Password	Пароль (мин. сложность: 8 символов, буквы+цифры)
Confirm Password	Подтверждение пароля
VLAN	VLAN ID для пользователя (опционально) 1-4094.
Timeout (Reauthentication)	Интервал повторного ввода пароля (сек) (0 = никогда) От 300 до 2147483647сек (Значение по умолчанию 3600сек)
Timeout (Inactive)	Время неактивности пользователя до автоматического выхода (сек) От 60 до 65535сек (Значение по умолчанию 60сек)

Примечания

1. Использование:

- Для гостевого доступа (Wi-Fi, конференц-залы).
- Когда RADIUS-сервер недоступен.

2. Безопасность:

- Пароли хранятся в зашифрованном виде.
- Рекомендуется:
 - Минимум 12 символов

- Смена паролей каждые 90 дней

3. Таймауты:

- **Reauthentication:** 14400 сек (4 часа) для офисных пользователей
- **Inactive:** 900 сек (15 мин) для гостевых зон

Пример настройки

1. Офисный сотрудник:

- **Username:** employee1
- **Password:** N7sK#p92qX!z
- **VLAN:** 10
- **Reauthentication:** 28800 (8 часов)

2. Гостевой доступ:

- **Username:** guest
- **Password:** Welcome123
- **VLAN:** 100
- **Inactive Timeout:** 1800 (30 мин)

3. Администратор:

- **Username:** admin
- **Password:** \$Adm1nP@ss
- **Reauthentication:** 0 (требуется только при входе)

Внимание! Для критичных систем используйте только RADIUS-аутентификацию!

13.5.5. Просмотр сессий аутентификации (Sessions)

Для просмотра и управления активными сессиями аутентификации перейдите:

Security > Authentication Manager > Sessions

На этой странице отображаются все текущие сессии аутентификации с возможностью принудительного завершения.

Security >> Authentication Manager >> Sessions

Sessions Table

Showing

All

 entries

Showing 0 to 0 of 0 entries

Q

	Session ID	Port	MAC Address	Current Type	Status	Operational Information				Authorized Information		
						VLAN	Session Time	Inactivated Time	Quiet Time	VLAN	Reauthentication Period	Inactive Timeout
0 results found.												

Clear

Refresh

FirstPrevious1NextLas

Информация о сессиях

Поле	Описание
Session ID	Уникальный идентификатор сессии
Port	Порт подключения устройства
MAC Address	MAC-адрес устройства
Current Type	Тип аутентификации: 802.1X – стандартная аутентификация MAC-Based – по MAC-адресу

Поле	Описание
	WEB-Based – через веб-интерфейс
Status	Статус сессии: Disabled – готова к удалению Running – в процессе аутентификации Authorized – успешная аутентификация Unauthorized – доступ запрещен Locked – временная блокировка Guest – доступ через гостевой VLAN
Operational (VLAN)	Текущий VLAN устройства
Operational (Session Time)	Время с момента авторизации
Operational (Inactivated)	Время неактивности устройства
Operational (Quiet Time)	Время до разблокировки (для статуса Locked)
Authorized (VLAN)	VLAN, назначенный при аутентификации
Authorized (Reauthentication Period)	Интервал повторной аутентификации
Authorized (Inactive Timeouts)	Таймаут неактивности

Кнопка **Clear** – принудительное завершение выбранной сессии.

Кнопка **Refresh** – обновить список сессий аутентификации

Примечания

1. **Locked** статус возникает после превышения числа неудачных попыток входа (см. **Max Login** в разделе **13.5.2**).
2. Для **гостевых сессий** VLAN может отличаться от назначенного при аутентификации.

Пример использования

1. **Проблема:** Устройство 00:1A:2B:3C:4D:5E не может аутентифицироваться.
 - Проверьте **Status**:
 - Если **Locked** – устройство временно заблокировано.
 - Если **Unauthorized** – проверьте настройки RADIUS/MAC-адреса.
2. **Решение:**
 - Для сброса выберите сессию и нажмите **Clear**.

13.6. Защита портов (Port Security)

Для настройки защиты портов перейдите:

Security > Port Security

На этой странице WEB интерфейса коммутатора есть возможность ограничить количество MAC-адресов на порту и задать действия при превышении лимита.

Security >> Port Security

State ☐ Enable

Rate Limit Packet / Sec (1 - 600, default 100)

Apply

Port Security Table

Q

	Entry	Port	State	Address Limit	Total	Configured	Violate Number	Violate Action	Sticky
☐	1	GE1	Disabled	1	0	0	0	Protect	Disabled
☐	2	GE2	Disabled	1	0	0	0	Protect	Disabled
☐	3	GE3	Disabled	1	0	0	0	Protect	Disabled
☐	4	GE4	Disabled	1	0	0	0	Protect	Disabled
☐	5	GE5	Disabled	1	0	0	0	Protect	Disabled
☐	6	GE6	Disabled	1	0	0	0	Protect	Disabled
☐	7	GE7	Disabled	1	0	0	0	Protect	Disabled
☐	8	GE8	Disabled	1	0	0	0	Protect	Disabled
☐	9	GE9	Disabled	1	0	0	0	Protect	Disabled
☐	10	GE10	Disabled	1	0	0	0	Protect	Disabled

Edit

Настройки защиты портов

Параметр	Описание
Port	Выберите порт(ы) для настройки.

Параметр	Описание
State	Состояние защиты порта: Disable – функция отключена. Enable – функция включена.
MAC Address	Максимальное количество разрешенных MAC-адресов на порту (1-1024).
Action	Действие при превышении лимита: Forward – пропускать новые MAC-адреса (только логирование). Discard – блокировать пакеты с новыми MAC-адресами. Shutdown – отключать порт при нарушении.

Примечания

1. Использование:

- Защита от MAC-флудинга и несанкционированного доступа.
- Рекомендуется для портов с фиксированными устройствами (IP-телефоны, принтеры).

2. Рекомендуемые настройки:

- **Офисные порты:** MAC Address = 2-3 (компьютер + телефон).
- **Серверные порты:** Action = Discard.
- **Гостевые порты:** Action = Shutdown для полной изоляции.

Внимание!

Режим **Shutdown** требует ручного включения порта после срабатывания.

Пример настройки

1. Порт **GE1** (рабочее место):

- **State:** Enable
- **MAC Address:** 2
- **Action:** Discard

2. Порт **GE24** (сервер):

- **State:** Enable
- **MAC Address:** 1
- **Action:** Shutdown

13.7. Настройка изоляции портов (Protected Port)

Для настройки изолированных портов перейдите в следующий раздел:

Security > Protected Port

На этой странице WEB интерфейса есть возможность включить режим изоляции портов, который запрещает взаимодействие между защищенными (protected) портами, разрешая только обмен с незащищенными портами.

Protected Port Table



☐	Entry	Port	State
☐	1	GE1	Unprotected
☐	2	GE2	Unprotected
☐	3	GE3	Unprotected
☐	4	GE4	Unprotected
☐	5	GE5	Unprotected
☐	6	GE6	Unprotected
☐	7	GE7	Unprotected
☐	8	GE8	Unprotected
☐	9	GE9	Unprotected
☐	10	GE10	Unprotected
☐	11	LAG1	Unprotected
☐	12	LAG2	Unprotected
☐	13	LAG3	Unprotected
☐	14	LAG4	Unprotected
☐	15	LAG5	Unprotected
☐	16	LAG6	Unprotected
☐	17	LAG7	Unprotected
☐	18	LAG8	Unprotected

Список защищенных/незащищенных портов

Параметр	Описание
Port	Номер порта
State	Режим изоляции: Protected – порт изолирован (не может обмениваться данными с другими защищенными портами) Unprotected – стандартный режим работы

Edit Protected Port

Port	GE1-GE3
State	☒ Protected

Apply Close

Выбор типа порта для функции изоляции портов

Параметр	Описание
Port	Номер порта
State	Режим изоляции: Protected – порт изолирован (не может обмениваться данными с другими защищенными портами) Unprotected – стандартный режим работы

Примечания**1. Применение:**

- Изоляция пользователей в общедоступных сетях (гостевые Wi-Fi, интернет-кафе).
- Защита критичных устройств (серверы, камеры) от несанкционированного доступа с других портов.

2. Особенности:

- Защищенные порты **могут** взаимодействовать с:
 - Незащищенными портами
 - Внешними сетями (через маршрутизатор)

- Запрещено взаимодействие **между защищенными портами** на одном коммутаторе.

3. Ограничения:

- Не влияет на широковещательный трафик (ARP, DHCP).
- Для полной изоляции требуется сочетать с функцией **Private VLAN**.

Пример настройки

1. Гостевые порты (GE1-GE12):

- **State:** Protected
- Результат: Гостевые пользователи не могут обмениваться данными между собой, но имеют доступ в интернет.

2. Серверные порты (GE23-GE24):

- **State:** Unprotected
- Результат: Серверы доступны со всех портов.

3. Порт администратора (GE20):

- **State:** Unprotected
- Результат: Полный доступ ко всем устройствам.

Важно!

Для управления защищенными портами используйте незащищенный порт или удаленный доступ (SSH/Web-интерфейс).

13.8. Настройка функции Storm Control (Storm Control)

Для настройки защиты от нежелательного трафика (broadcast, multicast, unicast) перейдите:

Security > Storm Control

Security >> Storm Control

Mode

☐ Packet / Sec
☒ Kbits / Sec

IFG

☒ Exclude
☐ Include

Apply

Port Setting Table

Q

	Entry	Port	State	Broadcast		Unknown Multicast		Unknown Unicast		Action
				State	Rate (Kbps)	State	Rate (Kbps)	State	Rate (Kbps)	
☐	1	GE1	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop
☐	2	GE2	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop
☐	3	GE3	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop
☐	4	GE4	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop
☐	5	GE5	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop
☐	6	GE6	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop
☐	7	GE7	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop
☐	8	GE8	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop
☐	9	GE9	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop
☐	10	GE10	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop

Edit

Глобальные настройки

Параметр	Описание
Mode	Единицы измерения: Packet/Sec – контроль по количеству пакетов Kbits/Sec – контроль по объему трафика
IFG	Учет межпакетного интервала (20 байт):

Параметр	Описание
	Excluded – не учитывается Included – учитывается

Security >> Storm Control

Edit Port Setting

Port	GE1	
State	☐ Enable	
Broadcast	☐ Enable	
	10000	Kbps (16 - 1000000, default 10000)
Unknown Multicast	☐ Enable	
	10000	Kbps (16 - 1000000, default 10000)
Unknown Unicast	☐ Enable	
	10000	Kbps (16 - 1000000, default 10000)
Action	☒ Drop ☐ Shutdown	

Apply

Close

Настройки портов

Параметр	Описание
Port	Выбранные порты
State	Включение Storm Control: Enable – активировать функцию

Параметр	Описание
Broadcast	Лимит для broadcast-трафика (1-262143 pps или 16-1000000 Kbps)
Unknown Multicast	Лимит для неизвестного multicast-трафика
Unknown Unicast	Лимит для неизвестного unicast-трафика
Action	Действие при превышении объема трафика: Drop – отбрасывание пакетов Shutdown – отключение порта

Рекомендации

1. Типовые значения:

- **Broadcast:** 100-1000 pps
- **Multicast:** 500 pps
- **Unicast:** 1000 pps

2. Критические порты:

- Используйте **Shutdown** для серверных портов.

3. Мониторинг:

- Логируйте события превышения лимитов.

Пример настройки

1. Глобально:

- **Unit:** Kbits/Sec
- **IFG:** Included

2. Порт GE1:

- **Broadcast:** 500 Kbps
- **Action:** Drop

3. Порт GE24:

- **Unknown Unicast:** 1000 Kbps
- **Action:** Shutdown

13.9. Защита от DoS-атак (Denial of Service)

Функция защиты от DoS-атак предотвращает перегрузку коммутатора за счет блокировки вредоносного трафика.

13.9.1. Глобальные настройки функции DOS (Property)

Для настройки перейдите по следующему пути:

Security > DoS > Property

Security » DoS » Property

POD	☒ Enable
Land	☒ Enable
UDP Blat	☒ Enable
TCP Blat	☒ Enable
DMAC = SMAC	☒ Enable
Null Scan Attack	☒ Enable
X-Mas Scan Attack	☒ Enable
TCP SYN-FIN Attack	☒ Enable
TCP SYN-RST Attack	☒ Enable
ICMP Fragment	☒ Enable
TCP-SYN	☒ Enable Note: Source Port < 1024
TCP Fragment	☒ Enable Note: Offset = 1
Ping Max Size	☒ Enable IPv4 ☒ Enable IPv6 512 Byte (0 - 65535, default 512)
TCP Min Hdr size	☒ Enable 20 Byte (0 - 31, default 20)
IPv6 Min Fragment	☒ Enable 1240 Byte (0 - 65535, default 1240)
Smurf Attack	☒ Enable 0 Netmask Length (0 - 32, default 0)

Apply

Параметр	Описание	Рекомендации
POD	Защита от атаки Ping of Death	Всегда включать
Land	Блокировка пакетов, где IP отправителя = IP получателя	Включить
UDP Blat	Блокировка UDP-пакетов с одинаковыми портами	Для серверов

Параметр	Описание	Рекомендации
TCP Blat	Блокировка TCP-пакетов с одинаковыми портами	Для серверов
DMAC = SMAC	Блокировка пакетов с одинаковыми MAC-адресами	Включить
Null Scan Attack	Защита от NULL-сканирования	Включить
X-Mas Scan Attack	Защита от X-Mas сканирования (пакеты с FIN/URG/PSH)	Включить
TCP SYN-FIN Attack	Блокировка пакетов с SYN+FIN флагами	Включить
TCP SYN-RST Attack	Блокировка пакетов с SYN+RST флагами	Включить
ICMP Fragment	Блокировка фрагментированных ICMP-пакетов	Включить
TCP-SYN(SPORT<1024)	Блокировка SYN-пакетов с портом <1024	Опционально
TCP Fragment (Offset=1)	Блокировка TCP-фрагментов со смещением=1	Включить
Ping Max Size	Макс. размер ICMP-пакетов (0-65535, по умолч. 512)	512-1024 байт
IPv4 Ping Max Size	Проверка размера ICMPv4 пакетов	Включить

Параметр	Описание	Рекомендации
IPv6 Ping Max Size	Проверка размера ICMPv6 пакетов	Для IPv6-сетей
TCP Min Hdr Size	Мин. размер TCP-заголовка (0-31, по умолч. 20)	20 байт
IPv6 Min Fragment	Мин. размер IPv6-фрагментов (по умолч. 1240)	1240 байт
Smurf Attack	Защита от Smurf-атак (маска 0-32)	Включить

Рекомендации

1. Базовые настройки:

- Включите все защиты, кроме **TCP-SYN(SPORT<1024)** (может блокировать легитимный трафик).
- Для **Ping Max Size** установите 1024 байта.

2. Серверные порты:

- Активируйте **UDP Blat** и **TCP Blat**.

3. IPv6-сети:

- Включите **IPv6 Ping Max Size** и **IPv6 Min Fragment**.

Пример конфигурации

1. Включите основные защиты:

- POD, Land, DMAC=SMAC, X-Mas Scan

2. Для корпоративной сети:

- **Ping Max Size:** 1024
- **TCP Min Hdr Size:** 20

3. Для серверов:

- **TCP SYN-FIN Attack:** Enable
- **TCP Blat:** Enable

13.9.2. Настройки портов (Port Setting)

Для включения/отключения защиты от DoS на конкретных портах перейдите:

Security > DoS > Port Setting

Security >> DoS >> Port Setting

Port Setting Table

☐	Entry	Port	State
☐	1	GE1	Disabled
☐	2	GE2	Disabled
☐	3	GE3	Disabled
☐	4	GE4	Disabled
☐	5	GE5	Disabled
☐	6	GE6	Disabled
☐	7	GE7	Disabled
☐	8	GE8	Disabled
☐	9	GE9	Disabled
☐	10	GE10	Disabled
☐	11	LAG1	Disabled
☐	12	LAG2	Disabled
☐	13	LAG3	Disabled
☐	14	LAG4	Disabled
☐	15	LAG5	Disabled
☐	16	LAG6	Disabled
☐	17	LAG7	Disabled
☐	18	LAG8	Disabled

Edit

Параметры настройки

Поле	Описание
Port	Номер порта или интерфейса.
State	Состояние защиты от DoS:
	Enable – активация защиты (применяются глобальные правила из раздела 13.9.1).
	Disable – отключение защиты для порта.

Рекомендации по настройке

1. Обязательные порты для защиты:

- Порт uplink (подключение к вышестоящему оборудованию)
- Серверные порты
- Порт управления (если выделен)

2. Порты для отключения защиты:

- Внутренние доверенные порты (например, между коммутаторами stack)
- Порты с VoIP-телефонами (если возникают ложные срабатывания)

Пример конфигурации

1. Активация защиты:

- Порт GE24 (uplink): **Enable**
- Порт GE1-GE5 (серверы): **Enable**

2. Отключение защиты:

- Порт GE10 (IP-телефон): **Disable** (если мешает работе)
- Порт GE23-GE24 (межкоммутаторные соединения): **Disable**

Внимание! После изменений проверьте доступность устройств на этих портах.

13.10. Dynamic ARP Inspection (DAI)

13.10.1. Глобальные настройки DAI (Property)

Для настройки защиты от ARP-спуфинга перейдите:

Security > Dynamic ARP Inspection > Property

Security >> Dynamic ARP Inspection >> Property

The screenshot shows the configuration interface for Dynamic ARP Inspection (DAI) properties. It includes a 'State' section with an 'Enable' checkbox. Below this, there are two lists: 'Available VLAN' and 'Selected VLAN'. The 'Available VLAN' list contains 'VLAN 1'. There are arrows between the two lists to move items. At the bottom, there is an 'Apply' button.

Глобальные параметры DAI

Параметр	Описание
State	Включение/отключение DAI на устройстве
VLAN	Выбор VLAN, в которых будет работать DAI (перемещение между боксами Available VLAN и Selected VLAN)

Port Setting Table



☐	Entry	Port	Trust	Source MAC Address	Destination MAC Address	IP Address	Rate Limit	
☐	1	GE1	Disabled	Disabled	Disabled	Disabled	Unlimited	
☐	2	GE2	Disabled	Disabled	Disabled	Disabled	Unlimited	
☐	3	GE3	Disabled	Disabled	Disabled	Disabled	Unlimited	
☐	4	GE4	Disabled	Disabled	Disabled	Disabled	Unlimited	
☐	5	GE5	Disabled	Disabled	Disabled	Disabled	Unlimited	
☐	6	GE6	Disabled	Disabled	Disabled	Disabled	Unlimited	
☐	7	GE7	Disabled	Disabled	Disabled	Disabled	Unlimited	
☐	8	GE8	Disabled	Disabled	Disabled	Disabled	Unlimited	
☐	9	GE9	Disabled	Disabled	Disabled	Disabled	Unlimited	
☐	10	GE10	Disabled	Disabled	Disabled	Disabled	Unlimited	
☐	11	LAG1	Disabled	Disabled	Disabled	Disabled	Unlimited	
☐	12	LAG2	Disabled	Disabled	Disabled	Disabled	Unlimited	
☐	13	LAG3	Disabled	Disabled	Disabled	Disabled	Unlimited	
☐	14	LAG4	Disabled	Disabled	Disabled	Disabled	Unlimited	
☐	15	LAG5	Disabled	Disabled	Disabled	Disabled	Unlimited	
☐	16	LAG6	Disabled	Disabled	Disabled	Disabled	Unlimited	
☐	17	LAG7	Disabled	Disabled	Disabled	Disabled	Unlimited	
☐	18	LAG8	Disabled	Disabled	Disabled	Disabled	Unlimited	

Edit

Таблица DAI для портов

Параметр	Описание	Рекомендуемое значение
Trust	Доверенный порт (пропускает все ARP-пакеты без проверки)	Включить для портов маршрутизаторов
Source MAC Validation	Проверка соответствия MAC отправителя в ARP и Ethernet-заголовке	Включить
Destination MAC Validation	Проверка MAC получателя в ARP-пакетах	Включить
IP Address Validation	Проверка IP-адресов (блокировка 0.0.0.0, 255.255.255.255 и multicast)	Включить
Allow Zero	Разрешение IP 0.0.0.0 (требуется для некоторых VoIP-устройств)	Отключить
Rate Limit	Лимит ARP-пакетов в секунду (0 = без лимита)	15-30 pps

Edit Port Setting

Port	GE1	
Trust	☒	Enable
Source MAC Address	☒	Enable
Destination MAC Address	☒	Enable
IP Address	☒	Enable
	☒	Allow Zero (0.0.0.0)
Rate Limit	20	pps (1 - 50, default 0), 0 is Unlimited

Настройка портов для DAI

Параметр	Описание
Port	Номер порта
Trust	Доверенный порт (пропускает все ARP-пакеты без проверки) Enable – включить.
Source MAC Validation	Проверка соответствия MAC отправителя в ARP и Ethernet-заголовке Enable – включить.
Destination MAC Validation	Проверка MAC получателя в ARP-пакетах Enable – включить.

Параметр	Описание
IP Address	Проверка IP-адресов (блокировка 0.0.0.0, 255.255.255.255 и multicast) Enable – включить.
Allow Zero	Разрешение IP 0.0.0.0 (требуется для некоторых VoIP-устройств) Enable – включить.
Rate Limit	Лимит ARP-пакетов в секунду (0 = без лимита) От 1 до 50.

Рекомендации

1. Обязательные настройки:

- Включите **IP/MAC Validation** для всех пользовательских портов.
- Для uplink-портов активируйте **Trust**.

2. VoIP-оборудование:

- Если устройства используют 0.0.0.0, включите **Allow Zero** только для их портов.

3. Защита от флуда:

- Установите **Rate Limit = 30 pps** для пользовательских портов.

Пример конфигурации

1. VLAN:

- Активируйте DAI для VLAN 10 (пользователи) и VLAN 20 (серверы).

2. Порт GE24 (маршрутизатор):

- **Trust:** Enable
- **Rate Limit:** 0

3. Порт GE1 (компьютер):

- **Source/Destination MAC Validation:** Enable
- **Rate Limit:** 30

Внимание! DAI требует предварительной настройки **DHCP Snooping** для работы с динамическими IP.

13.10.2. Статистика работы DAI (Statistics)

Для просмотра статистики работы Dynamic ARP Inspection (DAI) перейдите:

Security > Dynamic ARP Inspection > Statistics

На этой странице отображаются данные о работе функции защиты от ARP-спуфинга.

Statistics Table

☐	Entry	Port	Forward	Source MAC Failure	Destination MAC Failure	Source IP Validation Failure	Destination IP Validation Failure	IP-MAC Mismatch Failure
☐	1	GE1	0	0	0	0	0	0
☐	2	GE2	0	0	0	0	0	0
☐	3	GE3	0	0	0	0	0	0
☐	4	GE4	0	0	0	0	0	0
☐	5	GE5	0	0	0	0	0	0
☐	6	GE6	0	0	0	0	0	0
☐	7	GE7	0	0	0	0	0	0
☐	8	GE8	0	0	0	0	0	0
☐	9	GE9	0	0	0	0	0	0
☐	10	GE10	0	0	0	0	0	0
☐	11	LAG1	0	0	0	0	0	0
☐	12	LAG2	0	0	0	0	0	0
☐	13	LAG3	0	0	0	0	0	0
☐	14	LAG4	0	0	0	0	0	0
☐	15	LAG5	0	0	0	0	0	0
☐	16	LAG6	0	0	0	0	0	0
☐	17	LAG7	0	0	0	0	0	0
☐	18	LAG8	0	0	0	0	0	0

Clear

Refresh

Параметры статистики

Параметр	Описание
Entry	Номер записи
Port	Идентификатор порта
Forwarded	Количество корректных ARP-пакетов, пропущенных системой
Source MAC Failures	Количество пакетов, заблокированных из-за несоответствия MAC-адреса отправителя (в ARP и Ethernet-заголовке)
Destination MAC	Количество пакетов, заблокированных из-за

Параметр	Описание
Failures	несоответствия MAC-адреса получателя
Source IP Validation Failures	Количество пакетов, заблокированных из-за невалидного IP-адреса отправителя (0.0.0.0, multicast и т.д.)
Destination IP Validation Failures	Количество пакетов, заблокированных из-за невалидного IP-адреса получателя
IP-MAC Mismatch Failures	Количество пакетов, заблокированных из-за несоответствия IP и MAC в таблице IP Source Guard

Анализ статистики

1. Нормальная работа:

- **Forwarded** > 0, остальные счетчики = 0 или минимальны.

2. Проблемные ситуации:

- Высокие значения **Source MAC Failures** – возможен ARP-спуфинг.
- **IP-MAC Mismatch** > 0 – несоответствие IP и MAC в сети (проверьте настройки DHCP).

3. Действия:

- При частых блокировках проверьте:
 - Корректность настроек **Trust**-портов
 - Работу легитимных сервисов (например, VoIP)

Пример использования

1. Порт GE1:

- **Forwarded:** 1500
- **Source MAC Failures:** 2 (норма)

2. Порт GE5:

- **IP-MAC Mismatch Failures:** 50 – требуется проверка подключенного устройства.

13.11. DHCP Snooping

13.11.1. Глобальные настройки (Property)

Для защиты от DHCP-атак перейдите:

Security > DHCP Snooping > Property

Security >> DHCP Snooping >> Property

The screenshot displays the configuration page for DHCP Snooping properties. At the top, the breadcrumb navigation shows 'Security >> DHCP Snooping >> Property'. The main configuration area is enclosed in a dashed border and contains the following elements:

- State:** A checkbox labeled 'Enable' is currently unchecked.
- VLAN List:** A table-like structure with two columns: 'Available VLAN' and 'Selected VLAN'.
 - The 'Available VLAN' column contains a list box with 'VLAN 1' selected.
 - The 'Selected VLAN' column is currently empty.
 - Between the two columns are two arrow buttons: a right-pointing arrow (>) and a left-pointing arrow (<).
- Buttons:** An 'Apply' button is located at the bottom left of the configuration area.

Глобальные параметры

Параметр	Описание
State	Включение/отключение DHCP Snooping
VLAN	Выбор VLAN для мониторинга (перемещение между боксами Available VLAN и Selected VLAN)

Port Setting Table

						Q	
☐	Entry	Port	Trust	Verify Chaddr	Rate Limit		
☐	1	GE1	Disabled	Disabled	Unlimited		
☐	2	GE2	Disabled	Disabled	Unlimited		
☐	3	GE3	Disabled	Disabled	Unlimited		
☐	4	GE4	Disabled	Disabled	Unlimited		
☐	5	GE5	Disabled	Disabled	Unlimited		
☐	6	GE6	Disabled	Disabled	Unlimited		
☐	7	GE7	Disabled	Disabled	Unlimited		
☐	8	GE8	Disabled	Disabled	Unlimited		

Таблица портов с настройкой DHCP Snooping

Параметр	Описание
Trust	Доверенный порт (пропускает DHCP-серверы)
Verify Chaddr	Проверка соответствия MAC в DHCP и Ethernet-заголовке
Rate Limit	Лимит DHCP-пакетов (0 = без ограничений)

Edit Port Setting

Port	GE1	
Trust	☒ Enable	
Verify Chaddr	☒ Enable	
Rate Limit	0	pps (1 - 300, default 0), 0 is Unlimited

Настройки портов для DHCP Snooping

Параметр	Описание	Рекомендации
Trust	Доверенный порт (пропускает DHCP-серверы)	Включить для портов легитимных DHCP-серверов
Verify Chaddr	Проверка соответствия MAC в DHCP и Ethernet-заголовке	Включить для пользовательских портов
Rate Limit	Лимит DHCP-пакетов (0 = без ограничений)	30-100 pps для пользовательских портов

Рекомендации

1. **Обязательная настройка** для работы:
- Dynamic ARP Inspection (раздел 13.10)

➤ IP Source Guard

2. Правила применения:

- **Trust** включается ТОЛЬКО для портов DHCP-серверов
- **Verify Chaddr** блокирует подмену MAC в DHCP-запросах

Пример конфигурации

- VLAN 10: DHCP Snooping включен
- Порт GE24 (DHCP-сервер): Trust=Enable, Rate Limit=0
- Порт GE1: Verify Chaddr=Enable, Rate Limit=30

Внимание! После включения DHCP Snooping клиенты получают IP только от доверенных серверов.

13.11.2. Статистика работы DHCP Snooping (Statistics)

Для просмотра статистики работы **DHCP Snooping** перейдите:

Security > DHCP Snooping > Statistics

На этой странице WEB интерфейса отображаются данные о работе защиты от неавторизованных DHCP-серверов и подмены MAC-адресов.

Security >> DHCP Snooping >> Statistics								
Statistics Table								
	Entry	Port	Forward	Chaddr Check Drop	Untrust Port Drop	Untrust Port with Option82 Drop	Invalid Drop	
☐	1	GE1	0	0	0	0	0	
☐	2	GE2	0	0	0	0	0	
☐	3	GE3	0	0	0	0	0	
☐	4	GE4	0	0	0	0	0	
☐	5	GE5	0	0	0	0	0	
☐	6	GE6	0	0	0	0	0	
☐	7	GE7	0	0	0	0	0	

Параметры статистики

Параметр	Описание
Port	Идентификатор порта
Forwarded	Количество корректных DHCP-пакетов, пропущенных коммутатором
Chaddr Check Drop	Количество пакетов, заблокированных из-за несоответствия MAC в DHCP-запросе (chaddr) и Ethernet-заголовке
Untrusted Port Drop	Количество DHCP-ответов, заблокированных на недоверенных портах (попытка работы неавторизованного DHCP-сервера)
Untrusted Port with Option82 Drop	Количество пакетов с Option 82, заблокированных на недоверенных портах
Invalid Drop	Количество пакетов, заблокированных из-за других ошибок (некорректный формат, неверные поля и т.д.)

Анализ статистики

1. Нормальная работа:

- **Forwarded** > 0, остальные счетчики = 0 или минимальны.

2. Проблемные ситуации:

- **Untrusted Port Drop** > 0 – попытка подключения неавторизованного DHCP-сервера.
- **Chaddr Check Drop** > 0 – возможна подмена MAC-адресов в сети.

3. Действия:

- При высоких значениях **Untrusted Port Drop** проверьте подключение сетевых устройств к портам.
- Если **Invalid Drop** растет – возможны проблемы с легитимными DHCP-запросами (например, от VoIP-устройств).

Пример использования

1. Порт GE1:

- **Forwarded:** 500
- **Untrusted Port Drop:** 0 (норма)

2. Порт GE5:

- **Untrusted Port Drop:** 10 – обнаружен неавторизованный DHCP-сервер.

13.11.3. Настройка Option 82 (Option82 Property)

Option 82 помогает идентифицировать источник DHCP-запросов в распределенных сетях.

Для конфигурации DHCP Option 82 перейдите:

Security > DHCP Snooping > Option82 Property

Remote ID

☐ User Defined

Operational Status

Remote ID

00:e0:4c:00:00:00 (Switch Mac in Byte Order)

Apply

Глобальные настройки Option 82

Параметр	Описание
User Defined	Включение Remote-ID, определяемого администратором (по умолчанию используется MAC коммутатора)
Remote ID	Пользовательский идентификатор (до 63 символов)

Port Setting Table

☐	Entry	Port	State	Allow Untrust
☐	1	GE1	Disabled	Drop
☐	2	GE2	Disabled	Drop
☐	3	GE3	Disabled	Drop
☐	4	GE4	Disabled	Drop
☒	5	GE5	Disabled	Drop
☐	6	GE6	Disabled	Drop
☐	7	GE7	Disabled	Drop

Таблица с настройками Option 82 на портах

Параметр	Описание
State	Включение Option 82 на порту Enable – включить Disable – выключить
Allow Untrusted	Действие для Option 82 на недоверенных портах: Keep – оставить оригинальный Option 82 Replace – заменить на данные коммутатора Drop – блокировать пакеты

Security >> DHCP Snooping >> Option82 Property

Edit Port Setting

Port

GE5

State

☒ Enable

Allow Untrust

☐ Keep

☒ Drop

☐ Replace

Apply

Close

Настройка Option 82 на портах

Параметр	Описание
State	Включение Option 82 на порту

Параметр	Описание
	Enable – включить Disable – выключить
Allow Untrusted	Действие для Option 82 на недоверенных портах: Keep – оставить оригинальный Option 82 Replace – заменить на данные коммутатора Drop – блокировать пакеты

Рекомендации

1. Типовые сценарии:

- **Keep:** Для доверенных портов с VoIP-устройствами
- **Replace:** Для пользовательских портов (унификация данных)
- **Drop:** Для строгой безопасности

2. Формат Remote-ID:

- Используйте понятные идентификаторы (например, Floor1-Switch3)

Пример настройки:

- User Defined: Enable
- Remote ID: "BuildingA-Switch1"
- Порт 1/0/1: State=Enable, Allow Untrusted=Replace
- Порт 1/0/24: State=Disable

13.11.4. Настройка Circuit ID в Option 82 (Option 82 Circuit ID)

Для настройки **Circuit ID** в DHCP Option 82 перейдите:

Security > DHCP Snooping > Option82 Circuit ID

Security >> DHCP Snooping >> Option82 Circuit ID

Option82 Circuit ID Table

Showing All entries Showing 1 to 2 of 2 entries

☐	Port	VLAN	Circuit ID
☐	GE1	1	rainbow
☐	GE2	2	WWW

1

Таблица настроек **Circuit ID**

Параметр	Описание
Port	Порт, к которому применено правило
VLAN	VLAN (опционально)
Circuit ID	Заданный идентификатор Circuit ID

Security >> DHCP Snooping >> Option82 Circuit ID

Add Option82 Circuit ID

Port

GE5

VLAN

2

(1 - 4094) (Keep empty to set without VLAN)

Circuit ID

dddd

Port

GE1

VLAN

1

Circuit ID

rainbow

Apply

Close

Добавление/редактирование Circuit ID

Параметр	Описание
Port	Выбор порта (только при добавлении)
VLAN	VLAN ID (необязательно)
Circuit ID	Уникальный идентификатор Circuit ID (строка)

Рекомендации

1. Назначение:
- Идентификация физического расположения клиента (например, PortGE3-VLAN10).

➤ Совместно с **Remote ID** (из раздела **13.11.3**) формирует полную информацию об агенте.
2. Формат:
- Рекомендуется использовать понятные имена:

▪ Floor2-Room5-Port8

▪ SW1-Port24-VLAN20

Пример настройки:

- Порт: GE5
- VLAN: 10
- Circuit ID: "BuildingA-Floor1-Port5"

Примечание: Если VLAN не указан, Circuit ID применяется ко всем VLAN на порту.

13.12. IP Source Guard

13.12.1. Настройка портов (Port Setting)

Для защиты от IP-спуфинга перейдите:

Security > IP Source Guard > Port Setting

Security >> IP Source Guard >> Port Setting

Port Setting Table

☐	Entry	Port	State	Verify Source	Current Entry	Max Entry
☐	1	GE1	Disabled	IP	0	Unlimited
☐	2	GE2	Disabled	IP	0	Unlimited
☐	3	GE3	Disabled	IP	0	Unlimited
☐	4	GE4	Disabled	IP	0	Unlimited
☐	5	GE5	Disabled	IP	0	Unlimited
☐	6	GE6	Disabled	IP	0	Unlimited

Параметры портов

Параметр	Описание
Port	Идентификатор порта

Параметр	Описание
State	Состояние IP Source Guard: Enable – защита активна Disable – отключена
Verify Source	Режим проверки: IP – только IP-адрес IP-MAC – IP и MAC-адрес
Current Binding Entry	Текущее количество привязок IP/MAC
Max Binding Entry	Максимальное число привязок (0 = без ограничений)

Security >> IP Source Guard >> Port Setting

Edit Port Setting

Port	GE1	
State	☒ Enable	
Verify Source	☒ IP ☐ IP-MAC	
Max Entry	20	(1 - 50, default 0), 0 is Unlimited

Apply

Close

Параметр	Описание
Status	Включение/отключение функции
Verify Source	Уровень проверки: IP – базовая защита IP-MAC – строгая проверка
Max Binding Entry	Лимит привязок

Примечания

Для работы необходимы:

- **DHCP Snooping** (раздел 13.11)
- Статические привязки IP-MAC (если нет DHCP).

Пример настройки:

- Порт GE1: Verify Source: IP-MAC, Max Binding Entry: 2
- Порт GE10 (VoIP): Verify Source: IP, Max Binding Entry: 1

Внимание! При включенном **IP-MAC** режиме устройства со статическими IP требуют ручной привязки.

13.12.2. Таблица привязок IP/MAC адресов (IMPV Binding)

Для просмотра и управления привязками IP/MAC-адресов перейдите:

Security > IP Source Guard > IMPV Binding

Security >> IP Source Guard >> IMPV Binding

IP-MAC-Port-VLAN Binding Table

Showing All entries Showing 1 to 2 of 2 entries

☐	Port	VLAN	MAC Address	IP Address	Binding	Type	Lease Time
☐	GE1	22	44-55-66-77-88-99	2.2.2.2 / 255.255.255.255	IP-MAC-Port-VLAN	Static	N/A
☐	GE1	33	00-00-00-00-00-0A	3.3.3.3 / 255.255.255.255	IP-MAC-Port-VLAN	Static	N/A

AddEditDelete

Просмотр существующих привязок

Параметр	Описание
Port	Порт привязки
VLAN	VLAN привязки
MAC Address	MAC-адрес устройства (только для IP-MAC-привязок)
IP Address	IP-адрес (маска всегда /32 для IP-MAC)
Binding Type	Тип привязки: Static – создана вручную Dynamic – получена через DHCP Snooping
Lease Time	Время жизни динамической записи (только для DHCP)

Add IP-MAC-Port-VLAN Binding

Port	GE1 ▾	
VLAN	33	(1 - 4094)
Binding	☒ IP-MAC-Port-VLAN ☐ IP-Port-VLAN	
MAC Address	00:00:00:00:00:0A	
IP Address	3.3.3.3	/ 255.255.255.255

ApplyClose

Edit IP-MAC-Port-VLAN Binding

Port	GE1 ▾	
VLAN	33	
Binding	IP-MAC-Port-VLAN	
MAC Address	00:00:00:00:00:0A	
IP Address	3.3.3.3	/ 255.255.255.255

ApplyClose

Добавление/редактирование привязок

Параметр	Описание
Port	Выбор порта
VLAN	Указание VLAN (опционально)
Binding Mode	Режим привязки: IP-MAC-Port-VLAN – строгая привязка по

Параметр	Описание
	IP+MAC+порту+VLAN IP-Port-VLAN – привязка только по IP
MAC Address	Ввод MAC-адреса (требуется для IP-MAC-Port-VLAN)
IP Address/Mask	Ввод IP-адреса и маски (маска только для IP-Port-VLAN)

Рекомендации

- Для статических устройств** (серверы, принтеры):
 - Используйте **IP-MAC-Port-VLAN** с ручным вводом данных.
 - Пример:
 - Port: GE5, VLAN: 10
 - MAC: 00-1A-2B-3C-4D-5E, IP: 192.168.1.100
- Для динамических IP устройств:**
 - Привязки автоматически создаются через **DHCP Snooping** (тип **Dynamic**).
- Очистка:**
 - Динамические записи удаляются после прошествия времени, указанного в **Lease Time**.
 - Статические – только вручную.

Пример использования

- Проблема:** Устройство с статическим IP не работает.
 - Проверьте таблицу привязок:

- Если записи нет – добавьте вручную.
- Если есть несоответствие MAC – исправьте.

2. Для VoIP:

- Режим **IP-Port-VLAN** (без жесткой привязки MAC).

13.12.3. Сохранение базы данных (Save Database)

Для резервного копирования динамических привязок DHCP Snooping перейдите:

Security > IP Source Guard > Save Database

Security >> IP Source Guard >> Save Database

Type	☐ None ☐ Flash ☒ TFTP	
Filename	33333	
Address Type	☒ Hostname ☐ IPv4	
Server Address	192.168.1.100	
Write Delay	300	Sec (15 - 86400, default 300)
Timeout	300	Sec (0 - 86400, default 300)

Apply

Настройки сохранения записей в базу

Параметр	Описание
Type	Способ сохранения: None – отключено Flash – сохранение во внутреннюю память TFTP – отправка на TFTP-сервер
Filename	Имя файла для резервной копии Например: dhcp_bindings_backup.cfg
Address Type	Тип адреса TFTP-сервера (только для Type=TFTP) Hostname – доменное имя IPv4 – IP-адрес
Server Address	Адрес TFTP-сервера Например: 192.168.1.100 или tftp.example.com
Write Delay	Задержка перед сохранением (сек) По умолчанию: 300. Диапазон от 15 до 86400
Timeout	Таймаут операции (сек) По умолчанию: 300. Диапазон от 15 до 86400

Рекомендации

1. Для надежности:

- Используйте **TFTP** с указанием сервера.
- Пример настроек:

- Type: TFTP
- Filename: dhcp_bindings_\$(date).cfg
- Address Type: IPv4
- Server Address: 192.168.1.100

2. Для локального хранения:

- Type: Flash
- Filename: backup_dhcp_bindings.cfg

3. Автоматизация:

- При **Write Delay=300** изменения сохраняются каждые 5 минут.

14. ACL (Access Control List)

14.1. MAC ACL (ACL на основе MAC-адресов)

Для создания и управления ACL на уровне MAC-адресов перейдите:

ACL > MAC ACL

Создание ACL

Параметр	Описание
ACL Name	Уникальное имя ACL (до 32 символов). Пример: BLOCK_UNAUTHORIZED_MAC

ACL Table

Showing All entries

Showing 1 to 3 of 3 entries

☐	ACL Name	Rule	Port
☐	AAAA	0	
☐	SSSS	0	
☐	DDDD	0	

Delete

Таблица существующих ACL

Параметр	Описание
ACL Name	Имя созданного ACL
Rule	Количество правил (ACE) в ACL
Port	Список портов, к которым применен ACL

Применение:

- Блокировка устройств по MAC-адресу.
- Ограничение доступа к портам.

Пример:

1. Введите имя ACL (например, GUEST_RESTRICTION).
2. Нажмите **Apply** (принять)
3. Перейдите в раздел **MAC ACE (14.2)** для добавления правил.

Внимание! Удаление ACL возможно только если он не привязан к портам.

14.2. MAC ACE (Правила ACL для MAC-адресов)

Для настройки правил фильтрации трафика на уровне MAC-адресов перейдите:

ACL > MAC ACE

ACL >> MAC ACE

ACE Table

ACL Name AAAA

Showing All entries

Showing 1 to 2 of 2 entries

	Sequence	Action	Source MAC		Destination MAC		Ethertype	VLAN	802.1p	
			Address	Mask	Address	Mask			Value	Mask
☐	1	Permit	Any	Any	Any	Any	Any	Any	Any	Any
☐	22	Shutdown	Any	Any	Any	Any	Any	Any	Any	Any

Add

Edit

Delete

Таблица правил MAC ACE

Параметр	Описание
ACL Name	Выбор ACL, к которому добавляется правило
Showing	Показывать все записи в таблице или часть записей.
Sequence	Приоритет правила (1 – наивысший). Правила обрабатываются по возрастанию.
Action	Действие:

Параметр	Описание
	Permit – разрешить трафик
	Deny – заблокировать трафик
	Shutdown – заблокировать трафик и отключить порт
Source MAC	Фильтр по MAC-адресу отправителя:
	Any – любые адреса
	User Defined – конкретный MAC или диапазон
Destination MAC	Фильтр по MAC-адресу получателя (аналогично Source MAC)
	Any – любые адреса
	User Defined – конкретный MAC или диапазон
Ethertype	Тип Ethernet-фрейма (например, 0x0800 для IPv4, 0x86DD для IPv6)
	Any – любой тип
	Или 0x0800 для IPv4, 0x86DD для IPv6
VLAN ID	Фильтр по VLAN ID
	Any – любой VLAN
	или VLAN ID
802.1p Value	Приоритет QoS (0-7)

Параметр	Описание
	0-7 – приоритет от 0 до 7 Any – любой приоритет

ACL >> MAC ACE

Add ACE

ACL Name	AAAA	
Sequence	1 (1 - 2147483647)	
Action	☒ Permit ☐ Deny ☐ Shutdown	
Source MAC	☒ Any / (Address / Mask)	
Destination MAC	☒ Any / (Address / Mask)	
Ethertype	☒ Any 0x (0x600 ~ 0xFFFF)	
VLAN	☒ Any 1 (1 - 4094)	
802.1p	☒ Any / (Value / Mask) (0 - 7)	
Apply Close		

Edit ACE

ACL Name	AAAA	
Sequence	22	
Action	☐ Permit ☐ Deny ☒ Shutdown	
Source MAC	☒ Any / (Address / Mask)	
Destination MAC	☒ Any / (Address / Mask)	
Ethertype	☒ Any 0x (0x600 ~ 0xFFFF)	
VLAN	☒ Any 1 (1 - 4094)	
802.1p	☒ Any / (Value / Mask) (0 - 7)	
Apply Close		

Настройка правил MAC ACE

Параметр	Описание
ACL Name	Выбор ACL, к которому добавляется правило
Sequence	Приоритет правила (1 – наивысший). Правила обрабатываются по возрастанию.
Action	Действие:
	Permit – разрешить трафик
	Deny – заблокировать трафик
	Shutdown – заблокировать трафик и отключить порт
Source MAC	Фильтр по MAC-адресу отправителя:
	Any – любые адреса
	User Defined – конкретный MAC или диапазон (с маской, например 00:1A:2B:00:00:00/FF:FF:FF:00:00:00)
Destination MAC	Фильтр по MAC-адресу получателя (аналогично Source MAC)
Ethertype	Тип Ethernet-фрейма (например, 0x0800 для IPv4, 0x86DD для IPv6)
VLAN ID	Фильтр по VLAN ID (номер 1-4094 или Any)

Параметр	Описание
802.1p Value	Приоритет QoS (0-7). Маска указывает биты для проверки (например, маска 0x7 проверяет все 3 бита).

Примеры настройки

1. **Блокировка устройства по MAC:**
 - **Action:** Deny
 - **Source MAC:** User Defined
(00:1A:2B:3C:4D:5E/FF:FF:FF:FF:FF:FF)
 - **Destination MAC:** Any
2. **Разрешение только VoIP-трафика (VLAN 100, 802.1p=5):**
 - **Action:** Permit
 - **Ethertype:** User Defined (0x0800)
 - **VLAN ID:** User Defined (100)
 - **802.1p Value:** User Defined (5, маска 0x7)
3. **Защита от спама (широковещательный трафик):**
 - **Action:** Deny
 - **Destination MAC:** User Defined
(FF:FF:FF:FF:FF:FF/FF:FF:FF:FF:FF:FF)

Внимание!

- Правила нельзя изменить/удалить, если ACL привязан к порту.

14.3. IPv4 ACL (Access Control List для IPv4)

Для создания и управления ACL на уровне IPv4-адресов перейдите:

ACL > IPv4 ACL

ACL >> IPv4 ACL

ACL Name

Apply

Создание IPv4 ACL

Параметр	Описание
ACL Name	Уникальное имя ACL (до 32 символов). Пример: BLOCK_UNAUTHORIZED_IP

ACL >> IPv4 ACL

ACL Name

Apply

ACL Table

Showing All entries

Showing 1 to 3 of 3 entries

	ACL Name	Rule	Port
☐	IP11	0	
☐	IP23	0	
☐	IP8	0	

Delete

Таблица существующих IPv4 ACL

Параметр	Описание
ACL Name	Имя созданного ACL
Rule	Количество правил (ACE) в ACL
Port	Список портов, к которым применен ACL

Применение:

- Фильтрация трафика по IP-адресам/подсетям.
- Ограничение доступа к сервисам (например, веб-интерфейсу).

Пример создания:

1. Введите имя ACL (например, RESTRICT_WEB_ACCESS).
2. Нажмите **Apply** (принять).
3. Перейдите в раздел **IPv4 ACE (14.4)** для добавления правил.

Внимание!

- Удаление ACL возможно только если он не привязан к портам.
- Для правил с масками используйте CIDR-формат (192.168.1.0/24).

14.4. IPv4 ACE (Правила ACL для IPv4)

Для настройки правил фильтрации IPv4-трафика перейдите:

ACL → IPv4 ACE

ACL >> IPv4 ACE

ACE Table

ACL Name IP11

Showing All entries Showing 1 to 1 of 1 entries

	Sequence	Action	Protocol	Source IP		Destination IP		Source Port	Destination Port	TCP Flags	Type of Service		ICMP	
				Address	Mask	Address	Mask				DSCP	IP Precedence	Type	Code
☐	23	Permit	Any (IP)	Any	Any	Any	Any				Any		Any	

Add

Edit

Delete

Таблица правил IPv4 ACE

Параметр	Описание
ACL Name	Выбор ACL, к которому добавляется правило
Sequence	Приоритет (1 – наивысший). Правила обрабатываются по возрастанию.
Action	Действие:
	Permit – разрешить трафик
	Deny – заблокировать трафик
	Shutdown – заблокировать трафик и отключить порт
Protocol	Протокол:
	Any – все протоколы

Параметр	Описание
	TCP/UDP/ICMP и др. – конкретный протокол
	Protocol ID – номер протокола (например, 47 для GRE)
Source IP	IP-адрес отправителя:
	Any – любые адреса
	User Defined – конкретный IP/подсеть (например, 192.168.1.0/24)
Destination IP	IP-адрес получателя.
	Any – любые адреса
	User Defined – конкретный MAC или диапазон
Source Port	Порт отправителя (только для TCP/UDP):
	Any – все порты
	Single – один порт
	Range – диапазон портов
Destination Port	Порт получателя (аналогично Source Port)
	Any – все порты
	Single – один порт
	Range – диапазон портов
TCP Flags	Флаги TCP (только для протокола TCP): SYN, ACK, FIN и др.
Type of Service	Приоритет трафика:
	DSCP (0-63)

Параметр	Описание
	IP Precedence (0-7)
ICMP Type/Code	Тип и код ICMP (только для ICMP):
	Echo Request (8/0)
	Destination Unreachable (3/1)

ACL » IPv4 ACE

Add ACE

ACL Name	IP11	
Sequence	1 (1 - 2147483647)	
Action	☒ Permit ☐ Deny ☐ Shutdown	
Protocol	☒ Any ☐ Select ICMP	
	☐ Define 0 (0 - 255)	
Source IP	☒ Any / (Address / Mask)	
Destination IP	☒ Any / (Address / Mask)	
Type of Service	☒ Any ☐ DSCP 0 (0 - 63) ☐ IP Precedence 0 (0 - 7)	
Source Port	☒ Any ☐ Single 0 (0 - 65535) ☐ Range - (0 - 65535)	
Destination Port	☒ Any ☐ Single 0 (0 - 65535) ☐ Range - (0 - 65535)	
TCP Flags	Urg: ☐ Set ☐ Unset ☒ Don't care Ack: ☐ Set ☐ Unset ☒ Don't care Psh: ☐ Set ☐ Unset ☒ Don't care Rst: ☐ Set ☐ Unset ☒ Don't care	

Edit ACE

ACL Name	IP11
Sequence	23
Action	☒ Permit ☐ Deny ☐ Shutdown ☐ Any
Protocol	☒ Select ICMP ☐ Define (0 - 255)
Source IP	☒ Any / (Address / Mask)
Destination IP	☒ Any / (Address / Mask)
Type of Service	☐ DSCP (0 - 63) ☐ IP Precedence (0 - 7) ☐ Any
Source Port	☐ Single (0 - 65535) ☐ Range - (0 - 65535) ☐ Any
Destination Port	☐ Single (0 - 65535) ☐ Range - (0 - 65535)
TCP Flags	Urg: ☐ Set ☐ Unset ☐ Don't care Ack: ☐ Set ☐ Unset ☐ Don't care Psh: ☐ Set ☐ Unset ☐ Don't care Rst: ☐ Set ☐ Unset ☐ Don't care Syn: ☐ Set ☐ Unset ☐ Don't care Fin: ☐ Set ☐ Unset ☐ Don't care ☐ Any
ICMP Type	☒ Select Echo Reply ☐ Define (0 - 255) ☐ Any
ICMP Code	☐ Define (0 - 255)

Настройка правил IPv4 ACE

Параметр	Описание
ACL Name	Выбор ACL, к которому добавляется правило
Sequence	Приоритет (1 – наивысший). Правила обрабатываются по возрастанию.

Параметр	Описание
Action	Действие:
	Permit – разрешить трафик
	Deny – заблокировать трафик
	Shutdown – заблокировать трафик и отключить порт
Protocol	Протокол:
	Any – все протоколы
	SELECT (выбор). TCP/UDP/ICMP и др. – конкретный протокол
	DEFINE (определенный протокол) Protocol ID – номер протокола (например, 47 для GRE) 0- 255
Source IP	IP-адрес отправителя:
	Any – любые адреса
	User Defined – конкретный IP/подсеть (например, 192.168.1.0/24)
Destination IP	IP-адрес получателя (аналогично Source IP)
Type of Service	Приоритет трафика: DSCP (0-63) IP Precedence (0-7)
Source Port	Порт отправителя (только для TCP/UDP):
	Any – все порты

Параметр	Описание
	Single – один порт (например, 80 для HTTP)
	Range – диапазон портов (например, 5000-6000)
Destination Port	Порт получателя (аналогично Source Port)
TCP Flags	Флаги TCP (только для TCP): SYN, ACK, FIN и др.
ICMP Type	Тип ICMP (только для ICMP):
	Echo Request (8/0)
	Destination Unreachable (3/1)
	Define – определенный (0-255)
ICMP Code	Код ICMP Any – любой Define – определенный (0-255)

Примеры настройки

1. Блокировка доступа к WEB-интерфейсу:

- **Action:** Deny
- **Protocol:** TCP
- **Destination Port:** 80 (HTTP), 443 (HTTPS)
- **Source IP:** Any

2. Разрешение только ICMP Ping:

- **Action:** Permit
- **Protocol:** ICMP

- **ICMP Type:** Echo Request (8)
- **ICMP Code:** 0

3. Защита от SYN-флуда:

- **Action:** Deny
- **Protocol:** TCP
- **TCP Flags:** SYN
- **Destination Port:** Any

Внимание!

- Для правил с **Shutdown** порт включается вручную в **Port Settings**.
- Порядок правил критичен: первое совпадение определяет действие.

14.5. IPv6 ACL (Access Control List для IPv6)

Для создания и управления ACL на уровне IPv6-адресов перейдите:

ACL > IPv6 ACL

ACL >> IPv6 ACL

ACL Name

Apply

Создание IPv6 ACL

Параметр	Описание
ACL Name	Уникальное имя ACL (до 32 символов)

ACL Table

Showing All ▾ entries Showing 1 to 3 of 3 entries

☐	ACL Name	Rule	Port
☐	IP61	0	
☐	IP62	0	
☐	IP89	0	

Delete

Таблица существующих IPv6 ACL

Параметр	Описание
ACL Name	Имя созданного ACL
Rule	Количество правил (ACE) в ACL
Port	Список портов, к которым применен ACL

Ключевые особенности

Применение:

- Фильтрация IPv6-трафика (например, блокировка служебных диапазонов fe80::/10 или ff00::/8).
- Ограничение доступа к сервисам.

Пример создания:

- Введите имя ACL (например, ALLOW_IPV6_HTTP).
- Нажмите **Apply** (принять).
- Перейдите в раздел **IPv6 ACE (14.6)** для добавления правил.

Внимание!

- Удаление ACL возможно только если он не привязан к портам.
- Для IPv6-префиксов используйте формат CIDR (например, 2001:db8::/32).

14.6. IPv6 ACE (Правила ACL для IPv6)

Для настройки правил фильтрации IPv6-трафика перейдите:

ACL > IPv6 ACE

ACL >> IPv6 ACE

ACE Table

ACL Name IPv61 ▾

Showing All ▾ entries

Showing 1 to 1 of 1 entries

	Sequence	Action	Protocol	Source IP		Destination IP		Source Port	Destination Port	TCP Flags	Type of Service		ICMP	
				Address	Prefix	Address	Prefix				DSCP	IP Precedence	Type	Code
☐	22334	Permit	Any (IP)	Any	Any	Any	Any				Any		Any	

Таблица правил IPv6 ACE

Параметр	Описание
ACL Name	Выбор ACL, к которому добавляется правило
Sequence	Приоритет (1 — наивысший). Правила

Параметр	Описание
	обрабатываются по возрастанию.
Action	Действие:
	Permit — разрешить трафик
	Deny — заблокировать трафик
	Shutdown — заблокировать трафик и отключить порт
Protocol	Протокол:
	Any — все протоколы
	TCP/UDP/ICMPv6 — конкретный протокол
	Protocol ID — номер протокола (например, 58 для ICMPv6)
Source IP	IPv6-адрес отправителя:
	Any — любые адреса
	User Defined — конкретный IPv6/префикс (например, 2001:db8::/32)
Destination IP	IPv6-адрес получателя (аналогично Source IP)
	Any – любые адреса
	User Defined – конкретный IPv6/префикс
Source Port	Порт отправителя (только для TCP/UDP):
	Any — все порты

Параметр	Описание
	Single — один порт (например, 80 для HTTP)
	Range — диапазон портов (например, 5000-6000)
Destination Port	Порт получателя (аналогично Source Port) Any – все порты Single – один порт Range – диапазон портов
TCP Flags	Флаги TCP (только для TCP): SYN, ACK, FIN и др.
Type of Service	Приоритет трафика:
	DSCP (0-63)
	IP Precedence (0-7)
ICMPv6 Type/Code	Тип и код ICMPv6 (только для ICMPv6):
	Echo Request
	Neighbor Solicitation

Add ACE

ACL Name	IP61	
Sequence	1 (1 - 2147483647)	
Action	☒ Permit ☐ Deny ☐ Shutdown ☒ Any	
Protocol	☐ Select TCP ☐ Define (0 - 255)	
Source IP	☒ Any / (Address / Prefix (0 - 128))	
Destination IP	☒ Any / (Address / Prefix (0 - 128))	
Type of Service	☐ DSCP (0 - 63) ☐ IP Precedence (0 - 7) ☒ Any	
Source Port	☐ Single (0 - 65535) ☐ Range - (0 - 65535) ☒ Any	
Destination Port	☐ Single (0 - 65535) ☐ Range - (0 - 65535)	
TCP Flags	Urg: ☐ Set ☐ Unset ☒ Don't care Ack: ☐ Set ☐ Unset ☒ Don't care Psh: ☐ Set ☐ Unset ☒ Don't care Rst: ☐ Set ☐ Unset ☒ Don't care Syn: ☐ Set ☐ Unset ☒ Don't care Fin: ☐ Set ☐ Unset ☒ Don't care ☒ Any	
ICMP Type	☐ Select Destination Unreachable ☐ Define (0 - 255) ☒ Any	
ICMP Code	☐ Define (0 - 255)	

Apply

Close

Edit ACE

ACL Name	IP61	
Sequence	22334	
Action	☒ Permit ☐ Deny ☐ Shutdown	
Protocol	☒ Any ☐ Select TCP ▾ ☐ Define (0 - 255)	
Source IP	☒ Any / (Address / Prefix (0 - 128))	
Destination IP	☒ Any / (Address / Prefix (0 - 128))	
Type of Service	☒ Any ☐ DSCP (0 - 63) ☐ IP Precedence (0 - 7)	
Source Port	☒ Any ☐ Single (0 - 65535) ☐ Range - (0 - 65535)	
Destination Port	☒ Any ☐ Single (0 - 65535) ☐ Range - (0 - 65535)	
TCP Flags	Urg: ☐ Set ☐ Unset ☒ Don't care Ack: ☐ Set ☐ Unset ☒ Don't care Psh: ☐ Set ☐ Unset ☒ Don't care Rst: ☐ Set ☐ Unset ☒ Don't care Syn: ☐ Set ☐ Unset ☒ Don't care Fin: ☐ Set ☐ Unset ☒ Don't care ☒ Any	
ICMP Type	☐ Select Destination Unreachable ▾ ☐ Define (0 - 255)	
ICMP Code	☒ Any ☐ Define (0 - 255)	

Apply

Close

Настройка правил IPv6 ACE

Параметр	Описание
ACL Name	Выбор ACL, к которому добавляется правило
Sequence	Приоритет (1 — наивысший). Правила обрабатываются по возрастанию.
Action	Действие:
	Permit — разрешить трафик
	Deny — заблокировать трафик
	Shutdown — заблокировать трафик и отключить порт
Protocol	Протокол:
	Any — все протоколы
	Select (выбор) – TCP/UDP/ICMPv6 (конкретный протокол)
	Protocol ID — номер протокола (например, 58 для ICMPv6) От 0 до 255
Source IP	IPv6-адрес отправителя:
	Any — любые адреса
	User Defined — конкретный IPv6/префикс (например, 2001:db8::/32)
Destination IP	IPv6-адрес получателя (аналогично Source IP)
	Any – любые адреса
	User Defined – конкретный IPv6/префикс

Параметр	Описание
Type of Service	Приоритет трафика:
	DSCP (0-63)
	IP Precedence (0-7)
Source Port	Порт отправителя (только для TCP/UDP):
	Any — все порты
	Single — один порт (например, 80 для HTTP)
	Range — диапазон портов (например, 5000-6000)
Destination Port	Порт получателя (аналогично Source Port) Any – все порты Single – один порт Range – диапазон портов
TCP Flags	Флаги TCP (только для TCP): SYN, ACK, FIN и др.
ICMPv6 Type	Тип ICMPv6: Echo Request Destination Unreachable Neighbor Solicitation Define – определенный (0-255)
ICMPv6 Code	Тип и код ICMPv6 (только для ICMPv6):
	Any – любой
	Define – определенный (0-255)

Примеры настройки

1. Блокировка служебного IPv6-трафика:

- **Action:** Deny
- **Source IP:** fe80::/10 (link-local)
- **Destination IP:** ff00::/8 (multicast)

2. Разрешение ICMPv6 для NDP:

- **Action:** Permit
- **Protocol:** ICMPv6
- **ICMP Type:** 135 (Neighbor Solicitation), 136 (Neighbor Advertisement)

3. Ограничение доступа к WEB-серверу:

- **Action:** Permit
- **Protocol:** TCP
- **Destination Port:** 80, 443
- **Destination IP:** 2001:db8:100::1/128

Внимание!

- Для **Shutdown** порт включается вручную в **Port Settings**.
- Используйте **DSCP** для QoS в IPv6-сетях.

14.7. Привязка ACL (ACL Binding)

Для применения ACL к портам перейдите:

ACL > ACL Binding

ACL >> ACL Binding

ACL Binding Table

	Entry	Port	MAC ACL	IPv4 ACL	IPv6 ACL
☐	1	GE1			
☐	2	GE2			
☐	3	GE3			
☐	4	GE4			
☐	5	GE5			
☐	6	GE6			
☐	7	GE7			
☐	8	GE8			
☐	9	GE9			
☐	10	GE10			
☐	11	LAG1			
☐	12	LAG2			
☐	13	LAG3			
☐	14	LAG4			
☐	15	LAG5			
☐	16	LAG6			
☐	17	LAG7			
☐	18	LAG8			

Bind

Unbind

Edit

Таблица привязок ACL

Параметр	Описание
Entry	Номер записи в таблице
Port	Порт коммутатора

Параметр	Описание
MAC ACL	Имя привязанного MAC ACL (если есть)
IPv4 ACL	Имя привязанного IPv4 ACL (если есть)
IPv6 ACL	Имя привязанного IPv6 ACL (если есть)

ACL >> ACL Binding

Add ACL Binding

Port	GE1
	Note: ACL without any rules cannot be bound
MAC ACL	AAAA ▼
IPv4 ACL	IP11 ▼
IPv6 ACL	None ▼

Edit ACL Binding

Port	GE1
	Note: ACL without any rules cannot be bound
MAC ACL	AAAA ▼
IPv4 ACL	IP11 ▼
IPv6 ACL	None ▼

Настройка привязки ACL

Параметр	Описание
Port	Выбор порта
MAC ACL	Выбор MAC ACL из списка
IPv4 ACL	Выбор IPv4 ACL из списка
IPv6 ACL	Выбор IPv6 ACL из списка

Ограничения:

- К одному порту можно привязать только **один тип ACL** (MAC, IPv4 или IPv6).
- Привязка нового ACL автоматически заменяет старый ACL.

Рекомендации:

- **Для пользовательских портов:**
 - MAC ACL – фильтрация по MAC-адресам
 - IPv4/IPv6 ACL – контроль доступа к сервисам
- **Для серверных портов:**
 - IPv4/IPv6 ACL с разрешением только нужных протоколов

Пример настройки:

- **Порт GE1:**
 - **MAC ACL:** BLOCK_UNKNOWN_MAC

➤ Порт GE24 (сервер):

- IPv4 ACL: ALLOW_WEB_ACCESS

Внимание!

Изменения вступают в силу сразу после сохранения настроек.

15. Настройка QoS (QoS)

QoS (Quality of Service) – это набор технологий, которые позволяют оптимизировать передачу данных в сети, обеспечивая приоритет разным типам трафика. Это значит, что важные данные, такие как голос или видео, передаются с минимальными задержками и потерями, даже при перегрузке сети.

15.1. Общие настройки QoS (General)

15.1.1. Основные параметры QoS (Property)

Для настройки глобальных параметров QoS перейдите:

QoS > General > Property

The screenshot shows the configuration page for QoS, specifically the 'General > Property' tab. The page has a breadcrumb trail at the top: 'QoS >> General >> Property'. Below this, there is a configuration area with a dashed border. On the left side of this area is a grey box with the label 'Trust Mode'. To the right of this box, there are two sections: 'State' with an 'Enable' checkbox, and 'Trust Mode' with four radio button options: 'CoS' (which is selected), 'DSCP', 'CoS-DSCP', and 'IP Precedence'. At the bottom left of the configuration area is an 'Apply' button.

Глобальные настройки QoS

Параметр	Описание
State	Включение/отключение QoS (enable/disable)
Trust Mode	Режим приоритезации трафика:
	CoS – приоритет определяется по полю 802.1p в теге VLAN. Если тег отсутствует, используется значение CoS по умолчанию для порта.
	DSCP – приоритет определяется по полю DSCP (6 бит) в IP-заголовке. Не-IP трафик направляется в очередь Best Effort (0).
	CoS-DSCP – гибридный режим: для IP-трафика используется DSCP, для остального – CoS.
	IP Precedence – устаревший аналог DSCP (3 бита)

Port Setting Table

	Entry	Port	CoS	Trust	Remarking		
					CoS	DSCP	IP Precedence
☐	1	GE1	0	Enabled	Disabled	Disabled	Disabled
☐	2	GE2	0	Enabled	Disabled	Disabled	Disabled
☐	3	GE3	0	Enabled	Disabled	Disabled	Disabled
☐	4	GE4	0	Enabled	Disabled	Disabled	Disabled
☐	5	GE5	0	Enabled	Disabled	Disabled	Disabled
☐	6	GE6	0	Enabled	Disabled	Disabled	Disabled
☐	7	GE7	0	Enabled	Disabled	Disabled	Disabled
☐	8	GE8	0	Enabled	Disabled	Disabled	Disabled
☐	9	GE9	0	Enabled	Disabled	Disabled	Disabled
☐	10	GE10	0	Enabled	Disabled	Disabled	Disabled
☐	11	LAG1	0	Enabled	Disabled	Disabled	Disabled
☐	12	LAG2	0	Enabled	Disabled	Disabled	Disabled
☐	13	LAG3	0	Enabled	Disabled	Disabled	Disabled
☐	14	LAG4	0	Enabled	Disabled	Disabled	Disabled
☐	15	LAG5	0	Enabled	Disabled	Disabled	Disabled
☐	16	LAG6	0	Enabled	Disabled	Disabled	Disabled
☐	17	LAG7	0	Enabled	Disabled	Disabled	Disabled
☐	18	LAG8	0	Enabled	Disabled	Disabled	Disabled

Edit

Настройки QoS для портов

Параметр	Описание
Port	Имя порта
CoS	Приоритет по умолчанию (0-7), если тег 802.1p отсутствует
Trust	Определяет, учитывается ли глобальный Trust Mode для порта: Enabled – порт доверяет приоритету, указанному в трафике. Disabled – весь трафик получает приоритет Best Effort (0).
Remarking (CoS)	Перезапись поля 802.1p в теге VLAN: Enabled – коммутатор может изменять значение CoS. Disabled – оригинальное значение сохраняется.
Remarking (DSCP)	Перезапись значения DSCP в IP-заголовке
Remarking (IP Precedence)	Перезапись значения IP Precedence

Edit Port Setting

Port	GE1-GE3
CoS	0 (0 - 7)
Trust	☒ Enable
Remarking	
CoS	☐ Enable
DSCP	☐ Enable
IP Precedence	☐ Enable

Параметр	Описание
Port	Имя порта
CoS	Приоритет по умолчанию (0-7), если тег 802.1p отсутствует
Trust	Определяет, учитывается ли глобальный Trust Mode для порта: Enabled – порт доверяет приоритету, указанному в трафике. Disabled – весь трафик получает приоритет Best Effort (0).
Remarking (CoS)	Перезапись поля 802.1p в теге VLAN: Enabled – коммутатор может изменять значение CoS. Disabled – оригинальное значение сохраняется.
Remarking (DSCP)	Перезапись значения DSCP в IP-заголовке

Параметр	Описание
Remarking (IP Precedence)	Перезапись значения IP Precedence

Рекомендации

1. Глобальные параметры:

- Для VoIP: **Trust Mode = CoS** (приоритезация по тегу VLAN).
- Для IP-трафика: **Trust Mode = DSCP**.

2. Настройки портов:

- **Trust=Enabled** для портов с доверенным оборудованием (маршрутизаторы, IP-телефоны).
- **CoS=6** для VoIP-портов (если не используется тегирование).
- **Remarking** включается для граничных портов.

Пример настройки:

- Trust Mode: CoS-DSCP
- Порт GE1 (VoIP):
- CoS: 6
- Trust: Enabled
- Remarking (CoS): Enabled

Внимание!

- При **Trust=Disabled** весь трафик на порту получает приоритет **Best Effort (0)**
- Режим **Remarking** изменяет приоритеты трафика «на лету» – рекомендуется осторожное использование этого режима.

15.1.2. Планирование очередей (Queue Scheduling)

Для настройки алгоритмов обработки трафика в очередях перейдите:

QoS > General > Queue Scheduling

Коммутатор поддерживает **8 очередей** на каждый интерфейс, где:

- **Очередь 8** – наивысший приоритет.
- **Очередь 1** – низший приоритет.

Алгоритмы планирования

Алгоритм	Описание
Strict Priority (SP)	Трафик из очереди с наивысшим приоритетом (8) передается первым . Остальные очереди обрабатываются только после ее опустошения.
Weighted Round Robin (WRR)	Трафик передается пропорционально весу (weight) очереди (чем больше вес, тем больше пакетов обрабатывается).

Гибридный режим:

В коммутаторе предусмотрена возможность комбинировать SP и WRR.

Например:

- Очереди 6–8: **Strict Priority** (критичный трафик).
- Очереди 1–5: **WRR** (фоновый трафик).

Queue Scheduling Table

Queue	Method				
	Strict Priority	WRR	Weight	WRR Bandwidth (%)	
1	☐	☒	1	33.33%	
2	☐	☒	2	66.67%	
3	☒	☐	3		
4	☒	☐	4		
5	☒	☐	5		
6	☒	☐	9		
7	☒	☐	13		
8	☒	☐	15		

Параметры настройки очередей

Параметр	Описание
Queue	Номер очереди (1–8).
Strict Priority	Включение алгоритма SP для очереди.
WRR	Включение алгоритма WRR для очереди.
Weight	Вес очереди (1–255) – актуально только для WRR.
WRR Bandwidth	Процент полосы пропускания для WRR-очередей.

Примеры настройки

1. Приоритезация VoIP (Strict Priority, SP)

- Очередь 8: Strict Priority = Enable (VoIP, CoS=6)
- Очередь 7: Strict Priority = Enable (Видео, CoS=5)
- Очереди 1–6: WRR = Enable, Weight = 10 (фоновый трафик)

2. Пропорциональное распределение (WRR)

- Очередь 8: WRR, Weight = 50 (важный трафик)
- Очередь 7: WRR, Weight = 30
- Очереди 1–6: WRR, Weight = 5 (низкоприоритетный трафик)

3. Гибридный режим

- Очереди 7–8: Strict Priority = Enable (VoIP и видео)
- Очереди 1–6: WRR = Enable, Weight = 20 (WEB серфинг, почта)

Рекомендации

1. Для VoIP и реального времени:

- Используйте **Strict Priority** для очередей 6–8.
- Назначьте CoS 5–7 этим очередям (в разделе **15.1.3 CoS Mapping**).

2. Для балансировки нагрузки:

- Настройте **WRR** с весами, например:
 - Очередь 4 (CoS=3): Weight = 30
 - Очередь 3 (CoS=2): Weight = 20

3. Мониторинг:

- Проверяйте статистику очередей, чтобы избежать перегрузки.

Внимание!

- Приоритет SP всегда превосходит WRR.
- Вес WRR влияет только на **относительную** пропускную способность.

15.1.3. Сопоставление CoS (CoS Mapping)

Для настройки привязки приоритетов CoS (802.1p) к очередям перейдите:

QoS > General > CoS Mapping

QoS >> General >> CoS Mapping

CoS to Queue Mapping

CoS	Queue
0	2 ▼
1	1 ▼
2	3 ▼
3	4 ▼
4	5 ▼
5	6 ▼
6	7 ▼
7	8 ▼

Apply

CoS → Queue (Назначение очередей)

Определяет, в какую очередь попадет трафик на основе тега 802.1p. Для нетэгированных кадров используется CoS по умолчанию.

Параметр	Описание
CoS	Значение приоритета (0 – 7), где: • 0 – (низший) • 7 – (высший)
Queue	Номер очереди (1–8), куда направляется трафик.

Queue to CoS Mapping

Queue	CoS
1	1 ▼
2	0 ▼
3	2 ▼
4	3 ▼
5	4 ▼
6	5 ▼
7	6 ▼
8	7 ▼

Apply

Queue → CoS (Перемаркировка приоритетов)

Задаёт новое значение 802.1p для трафика, выходящего из указанной очереди.

Параметр	Описание
Queue	Номер очереди (1 – 8).
CoS	Новое значение 802.1p (0 – 7) для перемаркировки.

Рекомендации по настройке

- Для VoIP и видео в реальном времени:**
 - Назначьте высокие приоритеты CoS (5–7) на высокоуровневые очереди (6–8).
- Для перемаркировки (Mapping):**
 - Если трафик из очереди 3 должен выходить с низким приоритетом: *Queue 3 → CoS 1*

Внимание!

- Настройки **CoS > Queue** и **Queue > CoS** работают **независимо**.
- Перемаркировка полезна для граничных портов, где нужно изменить приоритет перед отправкой в другую сеть.

15.1.4. Сопоставление DSCP (DSCP Mapping)

Для настройки привязки значений DSCP к очередям и обратной перемаркировки перейдите в следующий раздел:

QoS > General > DSCP Mapping

QoS >> General >> DSCP Mapping

DSCP to Queue Mapping

DSCP	Queue	DSCP	Queue	DSCP	Queue	DSCP	Queue
0 [CS0]	1 ▼	16 [CS2]	3 ▼	32 [CS4]	5 ▼	48 [CS6]	7 ▼
1	1 ▼	17	3 ▼	33	5 ▼	49	7 ▼
2	1 ▼	18 [AF21]	3 ▼	34 [AF41]	5 ▼	50	7 ▼
3	1 ▼	19	3 ▼	35	5 ▼	51	7 ▼
4	1 ▼	20 [AF22]	3 ▼	36 [AF42]	5 ▼	52	7 ▼
5	1 ▼	21	3 ▼	37	5 ▼	53	7 ▼
6	1 ▼	22 [AF23]	3 ▼	38 [AF43]	5 ▼	54	7 ▼
7	1 ▼	23	3 ▼	39	5 ▼	55	7 ▼
8 [CS1]	2 ▼	24 [CS3]	4 ▼	40 [CS5]	6 ▼	56 [CS7]	8 ▼
9	2 ▼	25	4 ▼	41	6 ▼	57	8 ▼
10 [AF11]	2 ▼	26 [AF31]	4 ▼	42	6 ▼	58	8 ▼
11	2 ▼	27	4 ▼	43	6 ▼	59	8 ▼
12 [AF12]	2 ▼	28 [AF32]	4 ▼	44	6 ▼	60	8 ▼
13	2 ▼	29	4 ▼	45	6 ▼	61	8 ▼
14 [AF13]	2 ▼	30 [AF33]	4 ▼	46 [EF]	6 ▼	62	8 ▼
15	2 ▼	31	4 ▼	47	6 ▼	63	8 ▼

Apply

DSCP → Queue (Назначение очередей)

Определяет, в какую очередь попадет **IP-трафик** на основе значения DSCP (6 бит в IP-заголовке).

Параметр	Описание
DSCP	Значение Differentiated Services Code Point (или DSCP (0–63)): • 0 – Best Effort • 46 (EF) – Expedited Forwarding (VoIP) • 34 (AF41) – Video
Queue	Номер очереди (1–8).

Queue to DSCP Mapping

Queue	DSCP
1	0 [CS0] ▼
2	8 [CS1] ▼
3	16 [CS2] ▼
4	24 [CS3] ▼
5	32 [CS4] ▼
6	40 [CS5] ▼
7	48 [CS6] ▼
8	56 [CS7] ▼

Apply

Queue → DSCP (Перемаркировка DSCP)

Задаёт **новое значение DSCP** для трафика, выходящего из указанной очереди.

Параметр	Описание
Queue	Номер очереди (1–8).
DSCP	Новое значение DSCP (0–63).

Рекомендации

1. Критичный трафик (VoIP, видео):

- Назначьте DSCP EF (46) и AF41 (34) на высокоприоритетные очереди (7–8).

DSCP 46 → Queue 8

DSCP 34 → Queue 7

2. Перемаркировка:

- Если трафик из очереди 3 должен выходить с низким приоритетом:

Queue 3 → DSCP 10

3. Совместимость с CoS:

- При **Trust Mode = CoS-DSCP** настройки DSCP применяются только к IP-трафику.

Пример настройки

1. Назначение очередей:

DSCP 46 → *Queue 8*

DSCP 34 → *Queue 7*

DSCP 0–32 → *Queue 1–6*

2. Перемаркировка на выходе:

Queue 8 → *DSCP 46*

Queue 1 → *DSCP 0*

Внимание!

- DSCP-перемаркировка не влияет на тег 802.1p (если не включен **CoS-DSCP Trust Mode**).
- Для VoIP используйте **EF (46)** и **Strict Priority** для очереди 8.

15.1.5. Сопоставление IP Precedence (IP Precedence Mapping)

Для настройки привязки значений IP Precedence к очередям и обратной перемаркировки перейдите в следующий раздел WEB интерфейса:

QoS > General > IP Precedence Mapping

QoS >> General >> IP Precedence Mapping

IP Precedence to Queue Mapping

IP Precedence	Queue
0	1 ▼
1	2 ▼
2	3 ▼
3	4 ▼
4	5 ▼
5	6 ▼
6	7 ▼
7	8 ▼

Apply

IP Precedence → Queue (Назначение очередей)

Определяет, в какую очередь попадет трафик на основе значения IP Precedence (3 бита в IP-заголовке).

Параметр	Описание
IP Precedence	Приоритет (0–7), где: • 0 – Routine (Best Effort) • 7 – Network Control (Highest)
Queue	Номер очереди (1–8).

Queue to IP Precedence Mapping

Queue	IP Precedence
1	0 ▼
2	1 ▼
3	2 ▼
4	3 ▼
5	4 ▼
6	5 ▼
7	6 ▼
8	7 ▼

Apply

Queue → IP Precedence (Перемаркировка)

Задаёт **новое значение IP Precedence** для трафика, выходящего из очереди.

Параметр	Описание
Queue	Номер очереди (1–8).
IP Precedence	Новое значение (0–7).

Рекомендации

1. Устаревший стандарт:

- IP Precedence (3 бита) заменен на DSCP (6 бит).
Используйте только для совместимости со старым оборудованием.

2. Сопоставление с DSCP:

- IP Precedence 5 $\approx$ DSCP 40 (CS5) – для VoIP.

Внимание!

- Настройки **не влияют** на DSCP/CoS, если не включена соответствующая перемаркировка.
- Для современных сетей предпочтительнее функция **DSCP Mapping**.

15.2. Ограничение скорости (Rate Limit)

15.2.1. Входящий/Исходящий порт (Ingress/Egress Port)

Для настройки ограничения скорости на портах перейдите в следующий раздел WEB интерфейса:

QoS > Rate Limit > Ingress/Egress Port

QoS >> Rate Limit >> Ingress / Egress Port

Ingress / Egress Port Table

	Entry	Port	Ingress		Egress		
			State	Rate (Kbps)	State	Rate (Kbps)	
☐	1	GE1	Disabled		Disabled		
☐	2	GE2	Disabled		Disabled		
☐	3	GE3	Disabled		Disabled		
☐	4	GE4	Disabled		Disabled		
☐	5	GE5	Disabled		Disabled		
☐	6	GE6	Disabled		Disabled		
☐	7	GE7	Disabled		Disabled		
☐	8	GE8	Disabled		Disabled		
☐	9	GE9	Disabled		Disabled		
☐	10	GE10	Disabled		Disabled		

Edit

Текущие настройки

Параметр	Описание
Port	Имя порта

Параметр	Описание
Ingress (State)	Состояние ограничения входящей скорости: • Enabled – включено • Disabled – выключено
Ingress (Rate)	Макс. входящая скорость (Кбит/с)
Egress (State)	Состояние ограничения исходящей скорости
Egress (Rate)	Макс. исходящая скорость (Кбит/с)

QoS » Rate Limit » Ingress / Egress Port

Edit Ingress / Egress Port

Port	GE1-GE3	
Ingress	☒ Enable	
	1000000	Kbps (16 - 1000000)
Egress	☒ Enable	
	1000000	Kbps (16 - 1000000)

Редактирование настроек

Параметр	Описание
Port	Выбор порта

Параметр	Описание
Ingress	Включение/выключение ограничения входящего трафика. При включении требуется указать Rate в Кбит/с
Egress	Включение/выключение ограничения исходящего трафика. При включении требуется указать Rate в Кбит/с

Рекомендации

1. **Для аплинк-портов:**
 - Установите **Egress Rate** = 90% от физической скорости (например, 900 Мбит/с для 1 Гбит/с).
2. **Для пользовательских портов:**
 - **Ingress Rate = 10 Мбит/с** – защита от флуда.
3. **Формат значения:**
 - Указывается в **битах в секунду** (например, 10000000 = 10 Мбит/с).

Пример настройки

1. **Порт GE1 (гостевой Wi-Fi):**
Ingress: Enabled, Rate = 5000000 (5 Мбум/с)
Egress: Enabled, Rate = 10000000 (10 Мбум/с)
2. **Порт GE24 (аплинк):**
Egress: Enabled, Rate = 900000000 (900 Мбум/с)

Внимание!

- Ограничение **Ingress** работает на аппаратном уровне и отбрасывает избыточные пакеты.
- **Egress** ограничение формирует очередь (без потерь, если включен QoS).

15.2.2. Ограничение скорости для исходящих очередей (Egress Queue)

Для настройки ограничения скорости передачи данных для отдельных очередей на портах перейдите в следующий раздел:

QoS > Rate Limit > Egress Queue

QoS >> Rate Limit >> Egress Queue

Egress Queue Table

#	Entry	Port	Queue 1		Queue 2		Queue 3		Queue 4		Queue 5		Queue 6		Queue 7	
			State	CIR (Kbps)	State	CIR (Kbps)	State	CIR (Kbps)	State	CIR (Kbps)	State	CIR (Kbps)	State	CIR (Kbps)	State	CIR (Kbps)
☐	1	GE1	Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled	
☐	2	GE2	Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled	
☐	3	GE3	Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled	
☐	4	GE4	Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled	
☐	5	GE5	Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled	
☐	6	GE6	Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled	
☐	7	GE7	Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled	
☐	8	GE8	Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled	
☐	9	GE9	Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled	
☐	10	GE10	Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled	

Edit

Текущие настройки ограничения скорости очередей

Параметр	Описание
Port	Идентификатор порта

Параметр	Описание
Queue 1 (State)	Состояние ограничения скорости для очереди 1: • Enabled – ограничение включено • Disabled – ограничение выключено
Queue 1 (CIR)	Гарантированная скорость передачи (Committed Information Rate) для очереди 1 в битах в секунду
Queue 2 (State)	Состояние ограничения скорости для очереди 2: • Enabled – ограничение включено • Disabled – ограничение выключено
Queue 2 (CIR)	Гарантированная скорость передачи (Committed Information Rate) для очереди 2 в битах в секунду
Queue 3 (State)	Состояние ограничения скорости для очереди 3: • Enabled – ограничение включено • Disabled – ограничение выключено
Queue 3 (CIR)	Гарантированная скорость передачи (Committed Information Rate) для очереди 3 в битах в секунду
Queue 4 (State)	Состояние ограничения скорости для очереди 4: • Enabled – ограничение включено • Disabled – ограничение выключено
Queue 4 (CIR)	Гарантированная скорость передачи (Committed Information Rate) для очереди 4 в битах в секунду

Параметр	Описание
Queue 5 (State)	Состояние ограничения скорости для очереди 5: • Enabled – ограничение включено • Disabled – ограничение выключено
Queue 5 (CIR)	Гарантированная скорость передачи (Committed Information Rate) для очереди 5 в битах в секунду
Queue 6 (State)	Состояние ограничения скорости для очереди 6: • Enabled – ограничение включено • Disabled – ограничение выключено
Queue 6 (CIR)	Гарантированная скорость передачи (Committed Information Rate) для очереди 6 в битах в секунду
Queue 7 (State)	Состояние ограничения скорости для очереди 7: • Enabled – ограничение включено • Disabled – ограничение выключено
Queue 7 (CIR)	Гарантированная скорость передачи (Committed Information Rate) для очереди 7 в битах в секунду
Queue 8 (State)	Состояние ограничения скорости для очереди 8: • Enabled – ограничение включено • Disabled – ограничение выключено
Queue 8 (CIR)	Гарантированная скорость передачи (Committed Information Rate) для очереди 8 в битах в секунду

Edit Egress Queue

Port	GE1-GE3	
Queue 1	☒ Enable	1000000 Kbps (16 - 1000000)
Queue 2	☒ Enable	1000000 Kbps (16 - 1000000)
Queue 3	☒ Enable	1000000 Kbps (16 - 1000000)
Queue 4	☒ Enable	1000000 Kbps (16 - 1000000)
Queue 5	☐ Enable	1000000 Kbps (16 - 1000000)
Queue 6	☐ Enable	1000000 Kbps (16 - 1000000)
Queue 7	☐ Enable	1000000 Kbps (16 - 1000000)
Queue 8	☐ Enable	1000000 Kbps (16 - 1000000)

Apply

Close

Настройка ограничений скорости

Параметр	Описание
Port	Выбор порта для настройки
Queue 1	Включение/выключение ограничения скорости и задание значения CIR для очереди 1

Параметр	Описание
Queue 2	Включение/выключение ограничения скорости и задание значения CIR для очереди 2
Queue 3	Включение/выключение ограничения скорости и задание значения CIR для очереди 3
Queue 4	Включение/выключение ограничения скорости и задание значения CIR для очереди 4
Queue 5	Включение/выключение ограничения скорости и задание значения CIR для очереди 5
Queue 6	Включение/выключение ограничения скорости и задание значения CIR для очереди 6
Queue 7	Включение/выключение ограничения скорости и задание значения CIR для очереди 7
Queue 8	Включение/выключение ограничения скорости и задание значения CIR для очереди 8

Рекомендации

1. Для критически важного трафика (VoIP, видео):

- Очереди 7-8 (высший приоритет):
 - Включите ограничение скорости

- Установите CIR = 20-30% от общей пропускной способности порта
2. **Для стандартного трафика:**
 - Очереди 3-6:
 - CIR = 40-50% от общей пропускной способности
 3. **Для фонового трафика:**
 - Очереди 1-2:
 - CIR = 10-20% от общей пропускной способности

Внимание!

1. **Совместимость:**
 - Настройки применяются только при включенном QoS
 - Для очередей в режиме Strict Priority ограничение скорости может быть менее эффективным
2. Для достижения оптимальной производительности сумма всех CIR на порту не должна превышать 90% от его физической пропускной способности.

16. Инструменты диагностики (Diagnostics)

В данном разделе WEB интерфейса содержатся инструменты и механизмы диагностики работы коммутатора.

16.1. Ведение журналов событий (Logging)

16.1.1. Основные параметры (Property)

Для управления системой журналирования перейдите в следующий раздел WEB интерфейса:

Diagnostics > Logging > Property

Diagnostics >> Logging >> Property

State	☒ Enable
Aggregation	☒ Enable
Aging Time	300 Sec (15 - 3600, default 300)
Console Logging	
State	☒ Enable
Minimum Severity	Notice Note: Emergency, Alert, Critical, Error, Warning, Notice
RAM Logging	
State	☒ Enable
Minimum Severity	Notice Note: Emergency, Alert, Critical, Error, Warning, Notice
Flash Logging	
State	☐ Enable
Minimum Severity	Notice Note: Emergency, Alert, Critical, Error, Warning, Notice
Apply	

Глобальные настройки функции ведения журналов

Параметр	Описание
State	Включение/отключение системы ведения журналов: • Enable – активация функции ведения журналов • Disable – полное отключение (логи не сохраняются нигде)

1. Вывод сообщений в консоль (Console)

Параметр	Описание
State	Вывод логов (сообщений о событиях) в консоль: • Enable – вывод сообщений в консоль • Disable – отключение вывода сообщений
Minimum Severity	Минимальный уровень важности сообщений: • Emergency (0) – аварийные • Alert (1) – тревожные • Critical (2) – критически важные • Error (3) – об ошибках • Warning (4) – предупреждающие • Notice (5) – уведомления • Informational (6) – информационные • Debug (7) – отладочные

Вывод сообщений в оперативную память (RAM)

Параметр	Описание
State	Вывод сообщений в буфер оперативной памяти • Enable – включено • Disable – отключено
Minimum Severity	Минимальный уровень важности сообщений: • Emergency (0) – аварийные • Alert (1) – тревожные • Critical (2) – критически важные • Error (3) – об ошибках • Warning (4) – предупреждающие • Notice (5) – уведомления • Informational (6) – информационные • Debug (7) – отладочные

3. Вывод сообщений в встроенную постоянная память (Flash)

Параметр	Описание
State	Сохранение логов во внутреннюю память устройства (Flash) • Enable – включено • Disable – отключено
Minimum Severity	Минимальный уровень важности сообщений: • Emergency (0) – аварийные

Параметр	Описание
	• Alert (1) – тревожные • Critical (2) – критически важные • Error (3) – об ошибках • Warning (4) – предупреждающие • Notice (5) – уведомления • Informational (6) – информационные • Debug (7) – отладочные

Рекомендации

1. **Для мониторинга в реальном времени:**
 - Включите **Console Logging** с уровнем **Warning** (4).
2. **Для сбора истории событий:**
 - Активируйте **Flash Logging** с уровнем **Informational** (6).

Пример настройки:

Global State: Enable

Console:

- *State: Enable*
- *Minimum Severity: Warning*

RAM:

- *State: Enable*
- *Minimum Severity: Error*

Flash:

- *State: Enable*
- *Minimum Severity: Informational*

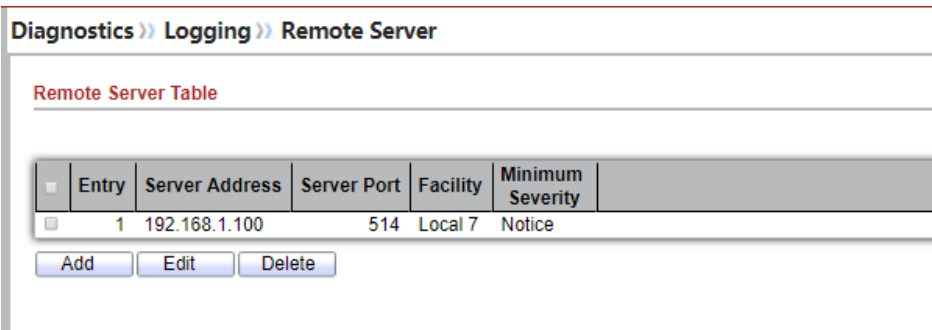
Внимание!

- Логи в **RAM** очищаются после перезагрузки.
- Логи в **Flash** сохраняются, но могут перезаписываться при заполнении памяти.

16.1.2. Удаленный сервер для отправки логов (Remote Server)

Для настройки отправки логов на внешний сервер (например, syslog) перейдите в следующий раздел WEB интерфейса:

Diagnostics > Logging > Remote Server



Параметры сервера для отправки логов

Параметр	Описание
Server Address	IP-адрес или доменное имя сервера для отправки логов
Server Port	Порт сервера (обычно 514 для syslog)

Параметр	Описание
Facility	Категория сообщений: • local0–local7 – пользовательские категории
Severity	Минимальный уровень важности сообщений: • Emergency (0) – аварийные • Alert (1) – тревожные • Critical (2) – критически важные • Error (3) – об ошибках • Warning (4) – предупреждающие • Notice (5) – уведомления • Informational (6) – информационные • Debug (7) – отладочные

Рекомендации

1. Типовая конфигурация для мониторинга:

Server Address: 192.168.1.100

Server Port: 514

Facility: local4

Severity: Warning

2. Для отладки:

- Установите **Severity = Debug** (учтите, что это увеличит объем логов).

3. Безопасность:

- Используйте **VPN** или **TLS** протоколы для защиты логов, если сервер находится в другой сети.

16.2. Зеркалирование портов (Mirroring)

Для доступа к настройкам зеркалирования (функция для контроля трафика на порту путем копирования его на другой порт) перейдите в следующий раздел WEB интерфейса:

Diagnostics > Mirroring

Diagnostics >> Mirroring

Mirroring Table

	Session ID	State	Monitor Port	Ingress Port	Egress Port	
☐	1	Disabled	---	---	---	
☐	2	Disabled	---	---	---	
☐	3	Disabled	---	---	---	
☐	4	Disabled	---	---	---	

Edit

* Allow the monitor port to send or receive normal packets

Параметры таблицы настройки зеркалирования

Параметр	Описание
Session ID	Выберите идентификатор сессии зеркалирования
State	Выберите состояние сессии зеркалирования: • Enabled: активировать зеркалирование на основе порта • Disabled: отключить зеркалирование

Параметр	Описание
Monitor Port	Выберите порт мониторинга для сессии зеркалирования и укажите, могут ли обычные пакеты передаваться или приниматься через этот порт
Ingress port	Выберите исходные RX-порты (прием трафика) для зеркалирования
Egress ports	Выберите исходные TX-порты (передача трафика) для зеркалирования

Рекомендации:

- Зеркалирование портов полезно для анализа сетевого трафика и диагностики проблем
- Порт мониторинга не должен использоваться для передачи критического трафика, так как его производительность может снизиться

Пример настройки:

- Перейдите в раздел Diagnostics > Mirroring;
- Выберите Session ID (например, 1);
- Установите State в значение Enabled;
- Укажите Monitor Port (например, Port 24);
- Выберите Ingress port (например, Port 1-5) для копирования входящего трафика;
- Выберите Egress ports (например, Port 6-10) для копирования исходящего трафика;
- Сохраните настройки.

16.3. Инструмент проверки связи (Ping)

Для использования функции PING в коммутаторе перейдите в следующий раздел WEB интерфейса:

Diagnostic > Ping

Diagnostics >> Ping

Address Type

Server Address

Count

☒ Hostname

☐ IPv4

☐ IPv6

(1 - 65535)

Ping

Stop

Ping Result

Packet Status

Status	N/A
Transmit Packet	0
Receive Packet	0
Packet Lost	0%

Round Trip Time

Min	0.0 ms
Max	0.0 ms
Average	0.0 ms

Параметр	Описание
Address Type	Укажите тип адреса: • Hostname - доменное имя

Параметр	Описание
	• IPv6 - адрес IPv6 • IPv4 - адрес IPv4
Server Address	Укажите IP адрес удаленного сервера, связь с которым надо проверить посредством PING
Count	Задайте количество отправляемых ICMP запросов PING

Рекомендации:

- Функция PING используется для проверки доступности сетевых устройств
- Для диагностики соединения рекомендуется отправлять 3-5 запросов
- При использовании доменного имени убедитесь в правильности настроек DNS

Пример использования:

1. Перейдите в раздел Diagnostic > Ping;
2. Установите Address Type = IPv4;
3. Введите Server Address = 192.168.1.1;
4. Установите Count = 5;
5. Нажмите PING для выполнения проверки;
6. Анализируйте результаты (время ответа, процент потерь)

16.4. Трассировка маршрута (Traceroute)

Для выполнения трассировки маршрута перейдите в следующий раздел WEB интерфейса:

Diagnostic > Traceroute

Diagnostics >> Traceroute

Address Type

Server Address

Time to Live

☒ Hostname
☐ IPv4

☐ User Defined
 (2 - 255, default 30)

Apply

Stop

Traceroute Result

Параметр	Описание
Address Type	Выберите тип адреса: • Hostname - доменное имя • IPv4 - IPv4 адрес
Server	Укажите адрес целевого устройства, проверку

Параметр	Описание
Address	маршрута к которому требуется выполнить.
Time to Live	Укажите максимальное количество переходов (hops) для трассировки

Рекомендации:

- Трассировка маршрута помогает определить путь прохождения пакетов и выявить проблемные участки сети
- Для локальных сетей обычно достаточно значения TTL 15-20
- При использовании доменного имени убедитесь в работоспособности DNS-резолвинга

Пример использования:

1. Перейдите в раздел Diagnostic > Traceroute;
2. Установите Address Type = IPv4;
3. Введите Server Address = 8.8.8.8;
4. Установите Time to Live = 30;
5. Нажмите Apply для выполнения трассировки;
6. Анализируйте результаты (узлы на пути, время отклика)

16.5. Тестирование медных кабелей (Copper Test)

Для диагностики медных кабелей перейдите в следующий раздел WEB интерфейса:

Diagnostic > Copper Test

Diagnostics >> Copper Test

PortGE1

Copper Test

Copper Test Result

Cable Status

Port

N/A

Result

N/A

Length

N/A

Параметры тестирования

Параметр	Описание
Port	Выберите интерфейс для проведения теста

Результаты тестирования

Параметр	Описание
Port	Тестируемый интерфейс

Параметр	Описание
Result	Результат теста: OK - исправная линия Short Cable - короткое замыкание Open Cable - обрыв линии Impedance Mismatch - несоответствие импеданса Line Drive - проблема с драйвером линии
Length	Расстояние до места неисправности (в метрах)

Рекомендации:

1. Тестирование рекомендуется проводить при:
 - Первоначальном монтаже сети
 - Возникновении проблем с подключением
 - Плановом техническом обслуживании
2. Для получения точных результатов:
 - Отключите кабель от активного оборудования
 - Убедитесь в чистоте контактов разъемов
 - Проверяйте каждый порт отдельно

Пример использования:

1. Перейдите в раздел Diagnostic > Copper Test;
2. Выберите Port = GE1;
3. Нажмите Copper Test;
4. Дождитесь завершения теста (10-30 секунд);
5. Проанализируйте результаты:
 - При Result: OK - кабель исправен

- При других результатах - проверьте указанный участок кабеля

Внимание!

Для точного определения места неисправности используйте специализированные кабельные тестеры. Результаты работы инструмента Copper Test в коммутаторе могут быть использованы только для ознакомления.

16.6. Инструмент диагностики SFP модулей (Fiber Module)

Данная страница WEB интерфейса отображает статус SFP модулей, т рабочую информацию, передаваемую трансиверами SFP. Некоторые данные могут быть недоступны для модулей, не поддерживающих стандарт цифрового мониторинга SFF-8472.

Diagnostic > Fiber Module

Diagnostics >> Fiber Module							
Fiber Module Table							
	Port	Temperature (C)	Voltage (V)	Current (mA)	Output Power (mW)	Input Power (mW)	OE Present
○	GE9	N/S	N/S	N/S	N/S	N/S	Remove
○	GE10	N/S	N/S	N/S	N/S	N/S	Remove
							Loss
							Loss
Refresh Detail							

Fiber Module Status

Port	GE9
OE Present	Remove
Loss of Signal	Loss
Transceiver Type	Unknown
Connector Type	Unknown
Ethernet Compliance Code	Unknown
Transmission Media	Unknown
Wavelength	N/S
Bitrate	N/S
Vendor OUI	N/S
Vendor Name	N/S
Vendor PN	N/S
Vendor Revision	N/S
Vendor SN	N/S
Date Code	0-00-00
Temperature (C)	N/S
Voltage (V)	N/S
Current (mA)	N/S
Output Power (mW)	N/S
Input Power (mW)	N/S

Refresh Close

Параметры оптических модулей

Параметр	Описание
Port	Номер интерфейса/порта
Temperature	Температура трансивера (°C)
Voltage	Напряжение питания (В)
Current	Ток смещения передатчика (mA)
Output Power	Выходная мощность передатчика (мВт)

Параметр	Описание
Input Power	Уровень принимаемого сигнала (мВт)
Transmitter Fault	Состояние неисправности передатчика
OE Present	Индикатор готовности модуля (питание подано, данные доступны)
Loss of Signal	Индикатор потери сигнала

Кнопка Refresh (обновить) нужна для обновления информации об используемых SFP модулях.

Рекомендации:

1. Регулярно проверяйте ключевые параметры:
 - Температура (норма: 0...+70°C)
 - Мощность передатчика и принимаемого сигнала
 - Напряжение питания (стандартное значение: 3.3В)
2. Критические состояния:
 - **Transmitter Fault** = Yes - неисправность передатчика
 - **Loss of Signal** = Yes - отсутствие сигнала
 - Выход параметров за допустимые пределы

Пример мониторинга:

1. Перейдите в раздел Diagnostic > Fiber Module
2. Выберите интересующий SFP порт (например, GE10);
3. Проверьте основные параметры:

- Output Power > -7 dBm (оптимально)
 - Input Power в допустимом диапазоне
 - Отсутствие аварийных индикаторов
4. Для проблемных портов нажмите **Detail** для получения детальной информации
 5. Используйте **Refresh** для обновления данных об SFP модуле

Внимание!

Допустимые значения параметров зависят от конкретной модели SFP-модуля. Для точной диагностики сверяйтесь с технической документацией производителя модуля.

16.7. Обнаружение однонаправленных соединений UDLD (UniDirectional Link Detection)

16.7.1. Свойства (Property)

Для настройки параметров UDLD перейдите в следующий раздел WEB интерфейса:

Diagnostics > UDLD > Property

Diagnostics >> UDLD >> Property

Message Time

Sec (1 - 90, default 15)

Apply

Глобальные настройки UDLD

Параметр	Описание
Message Time	Интервал отправки UDLD-сообщений (1-90 секунд)

Port Setting Table

☐	Entry	Port	Mode	Bidirectional State	Operational Status	Neighbor	
☐	1	GE1	Disabled	Unknown		0	
☐	2	GE2	Disabled	Unknown		0	
☐	3	GE3	Disabled	Unknown		0	
☐	4	GE4	Disabled	Unknown		0	
☐	5	GE5	Disabled	Unknown		0	
☐	6	GE6	Disabled	Unknown		0	
☐	7	GE7	Disabled	Unknown		0	
☐	8	GE8	Disabled	Unknown		0	
☐	9	GE9	Disabled	Unknown		0	
☐	10	GE10	Disabled	Unknown		0	

Edit

Статус портов

Параметр	Описание
Mode	Текущий режим работы UDLD на интерфейсе
Bidirectional State	Состояние двунаправленной связи
Operational Status	Текущий операционный статус
Neighbor	Количество обнаруженных устройств – соседей

Edit Port Setting

Port	GE1
Mode	☒ Disabled ☐ Normal ☐ Aggressive
Apply Close	

Настройки порта:

Параметр	Описание
Port	Выбранный порт для настройки
Mode	Режим работы UDLD: • Disabled - функция отключена • Normal - обычный режим (переход в состояние Link Up One) • Aggressive - агрессивный режим (переход в состояние Re-Establish)

Рекомендации:

1. Для критически важных соединений используйте агрессивный режим
2. Оптимальный интервал сообщений - 15-30 секунд
3. Регулярно проверяйте статус bidirectional state на ключевых портах

Пример настройки:

1. Перейдите в раздел Diagnostics > UDLD > Property;
2. Установите Message Time = 20;
3. Выберите порт для настройки;
4. Установите Mode = Aggressive (для важных соединений);
5. Нажмите Apply (принять) для сохранения

Внимание!

Режим Aggressive обеспечивает более быстрое обнаружение проблем, но может создавать дополнительную нагрузку на оборудование.

16.7.2. Соседние устройства (Neighbor)

Для просмотра информации о соседних устройствах перейдите в раздел WEB интерфейса:

Diagnostics > UDLD > Neighbor

Diagnostics >> UDLD >> Neighbor								
Neighbor Table								
Entry	Expiration Time	Current Neighbor State	Device ID	Device Name	Port ID	Message Interval	Timeout Interval	
0 results found.								
Refresh								

Таблица устройств-соседей:

Параметр	Описание
Entry	Индекс записи
Expiration Time	Время до удаления записи (age out)
Current Neighbor State	Текущее состояние соседнего устройства
Device ID	Идентификатор соседнего устройства
Device Name	Имя соседнего устройства
Port ID	Идентификатор порта подключения
Message Interval	Интервал отправки сообщений соседним устройством
Timeout Interval	Таймаут соседнего устройства

Рекомендации:

1. Регулярно проверяйте состояние соседей (Current Neighbor State) на критически важных соединениях
2. Обращайте внимание на:
 - Неожиданные изменения Device ID/Name - могут указывать на несанкционированное подключение
 - Увеличение Expiration Time - может свидетельствовать о проблемах связи

3. Для важных соединений сравнивайте Message Interval с локальными настройками

Пример использования:

1. Перейдите в раздел Diagnostics > UDLD > Neighbor;
2. Проверьте:
 - Соответствие Device Name ожидаемым соседним устройствам
 - Стабильность Current Neighbor State (должно быть "Bidirectional")
 - Соответствие Port ID ожидаемым точкам подключения
3. Для проблемных соединений:
 - Сравните Message Interval с настройками на обоих концах
 - Проверьте Expiration Time (резкие изменения могут указывать на нестабильность связи)

Внимание!

Информация обновляется динамически. Для актуальных данных может потребоваться обновление страницы (кнопка Refresh).

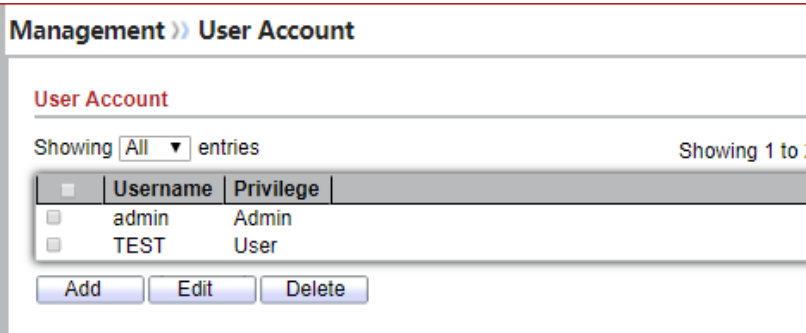
17. Параметры управления коммутатором (Management)

Раздел управления позволяет настраивать параметры управления коммутатором.

17.1. Учетные записи пользователей (User Account)

Для управления учетными записями перейдите в следующий раздел:

Management > User Account



Примечание: Учетная запись по умолчанию (admin/admin) не может быть удалена.

Таблица учетных записей

Параметр	Описание
Username	Имя пользователя
Privilege	Уровень привилегий:

Параметр	Описание
	• Admin (15) - полный доступ к настройкам • User (1) - только просмотр настроек

Management » User Account

Add User Account

Username

Password

Confirm Password

Privilege

admin

.....

☒ Admin

☐ User

Apply

Close

Management » User Account

Edit User Account

Username

Password

Confirm Password

Privilege

TEST

.....

☐ Admin

☒ User

Apply

Close

Диалог добавления/редактирования пользователя

Параметр	Описание
Username	Имя пользователя (латинские буквы/цифры)

Параметр	Описание
Password	Пароль пользователя
Confirm Password	Подтверждение пароля
Privilege	Уровень доступа: • Admin - полные права (редактирование/чтение/запись) • User - только чтение

Рекомендации по безопасности:

1. Сразу после первого входа измените пароль администратора
2. Создавайте индивидуальные учетные записи для каждого администратора
3. Для обычных сотрудников используйте учетные записи с уровнем User
4. Пароль должен содержать:
 - Не менее 8 символов
 - Заглавные и строчные буквы
 - Цифры и специальные символы

Пример настройки:

1. Перейдите в настройки Management > User Account;
2. Нажмите "Add" для создания новой записи;
3. Заполните поля:
 - Username: network_admin
 - Password: Str0ngP@ss2023

- Confirm Password: Str0ngP@ss2023
- Privilege: Admin

4. Нажмите "Apply" для сохранения настроек

Внимание!

Регулярно обновляйте пароли (рекомендуется каждые 3-6 месяцев) и удаляйте неиспользуемые учетные записи.

17.2. Управление прошивкой коммутатора (Firmware)

17.2.1. Обновление/Резервное копирование (Upgrade/Backup)

Для управления прошивкой коммутатора перейдите в следующий раздел:

Management > Firmware > Upgrade/Backup

Management >> Firmware >> Upgrade / Backup

Action	☒ Upgrade ☐ Backup
Method	☐ TFTP ☒ HTTP
Filename	选择文件 未选择任何文件

Обновление через HTTP

Параметр	Описание
Action	Выберите операцию с прошивкой: • Upgrade - обновление прошивки • Backup - резервное копирование
Method	Способ передачи прошивки: • HTTP - через веб-интерфейс • TFTP - через TFTP-сервер
Filename	Выберите файл прошивки с локального компьютера через браузер

Management » Firmware » Upgrade / Backup

Action	☒ Upgrade ☐ Backup
Method	☒ TFTP ☐ HTTP
Address Type	☒ Hostname ☐ IPv4 ☐ IPv6
Server Address	
Filename	

Apply

Обновление через TFTP

Параметр	Описание
Address Type	Тип адреса сервера:

Параметр	Описание
	• Hostname - доменное имя • IPv4 – адрес IPv4 • IPv6 – адрес IPv6
Server Address	Адрес TFTP-сервера
Filename	Имя файла прошивки на сервере

Management » Firmware » Upgrade / Backup

Action
Method
Firmware

☐ Upgrade
☒ Backup

☐ TFTP
☒ HTTP

☒ Image0
☐ Image1

Apply

Резервное копирование через HTTP

Параметр	Описание
Firmware	Выбор раздела прошивки: • Image0 - раздел 0 • Image1 - раздел 1

Action	☐ Upgrade ☒ Backup
Method	☒ TFTP ☐ HTTP
Firmware	☒ Image0 ☐ Image1
Address Type	☒ Hostname ☐ IPv4 ☐ IPv6
Server Address	
Filename	

Резервное копирование через TFTP

Дополнительные параметры:

Параметр	Описание
Action	Выберите операцию с прошивкой: • Upgrade - обновление прошивки • Backup - резервное копирование
Method	Способ передачи прошивки: • HTTP - через веб-интерфейс • TFTP - через TFTP-сервер
Firmware	Выбор раздела прошивки: • Image0 - раздел 0 • Image1 - раздел 1

Параметр	Описание
Address Type	Тип адреса сервера: • Hostname - доменное имя • IPv4 – адрес IPv4 • IPv6 – адрес IPv6
Server Address	Адрес TFTP-сервера
Filename	Имя для сохранения резервной копии

Рекомендации:

1. Перед обновлением:
 - Сделайте резервную копию текущей прошивки
 - Сохраните конфигурацию устройства
 - Убедитесь в стабильности питания
2. Процесс обновления:
 - Не прерывайте питание устройства
 - Не перезагружайте коммутатор
 - Дождитесь полного завершения процесса

Пример обновления через HTTP:

1. Перейдите в раздел Management > Firmware > Upgrade/Backup;
2. Установите:
 - Action: Upgrade
 - Method: HTTP
3. Выберите файл прошивки

4. Нажмите "Apply" для начала обновления
5. Дождитесь автоматической перезагрузки

Примечание: Время обновления может занимать 5-15 минут. После успешного обновления рекомендуется выполнить сброс к заводским настройкам и восстановить конфигурацию вручную.

17.2.2. Активный образ прошивки (Active Image)

Для управления активным образом прошивки перейдите в следующий раздел WEB интерфейса:

Management > Firmware > Active Image

Active Image

☒ Image0
☐ Image1

Note: the image was selected for the next boot

Active Image	
Firmware	Image0
Version	3.1.0.b10
Name	
Size	5882191 Bytes
Created	2022-09-22 16:53:53

Backup Image	
Firmware	Image1
Version	3.1.0.50153
Name	vmlinux.bix
Size	6284117 Bytes
Created	2022-10-09 18:32:26

Apply

Информация о прошивке

Параметр	Описание
Active Image	Выбор активного образа прошивки для следующей загрузки коммутатора
Firmware	Наименование прошивки
Version	Версия прошивки
Name	Название прошивки
Size	Размер образа прошивки
Created	Дата создания прошивки
Backup Image	Информация о резервном образе прошивки
Firmware	Наименование резервной прошивки
Version	Версия резервной прошивки
Name	Название резервной прошивки
Size	Размер образа резервной прошивки
Created	Дата создания резервной прошивки

Рекомендации:

1. При выборе активного образа:
 - Убедитесь, что выбранная версия прошивки стабильна
 - Проверьте совместимость с текущей конфигурацией
 - Для тестирования новых версий используйте неактивный раздел
2. Перед переключением:
 - Сохраните текущую конфигурацию
 - Запланируйте перезагрузку в период минимальной нагрузки на сеть
 - Имейте возможность быстро вернуть предыдущую версию прошивки

Пример настройки:

1. Перейдите в раздел Management > Firmware > Active Image;
2. Выберите нужный образ в поле **Active Image**:
 - Image0 (основной раздел)
 - Image1 (резервный раздел)
3. Проверьте информацию о версии:
 - Сравните версии в обоих разделах
 - Убедитесь в достаточном размере образа
4. Нажмите **Apply** для сохранения изменений
5. Выполните перезагрузку коммутатора для применения новой прошивки

Внимание!

После переключения активного образа рекомендуется:

- Проверить журналы системы на наличие ошибок
- Убедиться в работоспособности всех критических функций
- Протестировать работу сетевых интерфейсов

17.3. Конфигурация (Configuration)

17.3.1. Обновление/Резервное копирование конфигурации (Upgrade/Backup)

Для управления конфигурацией перейдите в следующей раздел WEB интерфейса:

Management > Configuration > Upgrade/Backup

Management >> Configuration >> Upgrade / Backup

Action

Method

Configuration

Filename

☒ Upgrade

☐ Backup

☐ TFTP

☒ HTTP

☒ Running Configuration

☐ Startup Configuration

☐ Backup Configuration

☐ RAM Log

☐ Flash Log

选择文件

未选择任何文件

Apply

Обновление конфигурации через HTTP

Параметр	Описание
Action	Выбор операции: • Upgrade - загрузка конфигурации • Backup - сохранение конфигурации

Параметр	Описание
Method	Метод передачи: • TFTP • HTTP
Configuration	Тип конфигурации: • Running Configuration - объединение полученной конфигурации с текущей • Startup Configuration - замена конфигурации в качестве стартовой • Backup Configuration - замена резервной конфигурации на новую
Filename	Выбор файла конфигурации

Management » Configuration » Upgrade / Backup

Action	☒ Upgrade ☐ Backup
Method	☒ TFTP ☐ HTTP
Configuration	☒ Running Configuration ☐ Startup Configuration ☐ Backup Configuration ☐ RAM Log ☐ Flash Log
Address Type	☒ Hostname ☐ IPv4 ☐ IPv6
Server Address	
Filename	

Apply

Обновление конфигурации через TFTP

Параметр	Описание
Action	Выбор операции: • Upgrade - загрузка конфигурации • Backup - сохранение конфигурации
Method	Метод передачи: • TFTP • HTTP
Configuration	Тип конфигурации: • Running Configuration - объединение полученной конфигурации с текущей • Startup Configuration - замена конфигурации в качестве стартовой • Backup Configuration - замена резервной конфигурации на новую
Address Type	Тип адреса: • Hostname • IPv4 • IPv6
Server Address	Адрес TFTP-сервера
Filename	Имя файла на сервере

Action	☐ Upgrade ☒ Backup
Method	☐ TFTP ☒ HTTP
Configuration	☒ Running Configuration ☐ Startup Configuration ☐ Backup Configuration ☐ RAM Log ☐ Flash Log

Apply

Резервное копирование через HTTP

Параметр	Описание
Action	Выбор операции: • Upgrade - загрузка конфигурации • Backup - сохранение конфигурации
Method	Метод передачи: • TFTP • HTTP
Configuration	Тип конфигурации: • Running Configuration – текущая конфигурация • Startup Configuration – стартовая конфигурация • Backup Configuration – резервная конфигурация • RAM Log – логи в оперативной памяти

Параметр	Описание
	коммутатора • Flash Log – логи в постоянной памяти коммутатора

Management » Configuration » Upgrade / Backup

Action	☐ Upgrade ☒ Backup
Method	☒ TFTP ☐ HTTP
Configuration	☒ Running Configuration ☐ Startup Configuration ☐ Backup Configuration ☐ RAM Log ☐ Flash Log
Address Type	☒ Hostname ☐ IPv4 ☐ IPv6
Server Address	
Filename	

Apply

Резервное копирование через TFTP

Параметр	Описание
Action	Выбор операции: • Upgrade - загрузка конфигурации • Backup - сохранение конфигурации

Параметр	Описание
Method	Метод передачи: • TFTP • HTTP
Configuration	Тип конфигурации: • Running Configuration – текущая конфигурация • Startup Configuration – стартовая конфигурация • Backup Configuration – резервная конфигурация • RAM Log – логи в оперативной памяти коммутатора • Flash Log – логи в постоянной памяти коммутатора
Address Type	Тип адреса: • Hostname • IPv4 • IPv6
Server Address	Адрес TFTP-сервера
Filename	Имя для сохранения файла

Рекомендации:

1. Регулярно сохраняйте конфигурацию:
 - Перед внесением изменений
 - После успешной настройки
 - По расписанию (еженедельно/ежемесячно)
2. Используйте разные имена для версий. Например:

- config_20240101_startup.cfg
- config_20240101_after_update.cfg

Пример резервного копирования стартовой прошивки:

1. Перейдите в раздел Management > Configuration > Upgrade/Backup
2. Установите:
 - Action: Backup
 - Method: HTTP
 - Configuration: Startup Configuration
3. Нажмите "Backup"
4. Сохраните файл на локальный компьютер

Внимание! При объединении конфигураций (Running) могут возникать конфликты настроек. Проверяйте изменения перед сохранением.

17.3.2. Сохранение конфигурации (Save Configuration)

Для управления конфигурационными файлами перейдите в следующий раздел WEB интерфейса:

Management > Configuration > Save Configuration

Management >> Configuration >> Save Configuration

Source File	☒ Running Configuration ☐ Startup Configuration ☐ Backup Configuration
Destination File	☒ Startup Configuration ☐ Backup Configuration

Apply Restore Factory Default

Параметры сохранения конфигурации

Параметр	Описание
Source File	Исходный файл конфигурации: • Running Configuration - текущая рабочая конфигурация • Startup Configuration - стартовая конфигурация • Backup Configuration - резервная копия конфигурации
Destination File	Целевой файл конфигурации: • Startup Configuration - сохранить как стартовую конфигурацию • Backup Configuration - сохранить как резервную копию конфигурации

Дополнительные функции:

- Кнопка **Restore Factory Default** - сброс настроек к заводским

Рекомендации:

1. Регулярно сохраняйте текущую конфигурацию (Running) в Startup:
 - После внесения изменений
 - Перед обновлением ПО
 - При стабильной работе оборудования
2. Сохраняйте резервные копии перед:
 - Крупными изменениями настроек
 - Обновлением прошивки
 - Изменением топологии сети

Пример использования:

1. Перейдите в раздел Management > Configuration > Save Configuration;
2. Выберите:
 - Source File: Running Configuration
 - Destination File: Startup Configuration
3. Нажмите "Apply" для сохранения
4. Для создания резервной копии:
 - Source File: Running Configuration
 - Destination File: Backup Configuration
5. Нажмите "Apply"

Внимание!

- Сброс к заводским настройкам (**Restore Factory Default**) требует перезагрузки устройства
- После сброса все текущие настройки будут потеряны
- Рекомендуется предварительно сохранить текущую конфигурацию

17.4. Настройка SNMP (SNMP)

17.4.1. SNMP View (View)

Для настройки и просмотра таблицы SNMP view перейдите в следующий раздел WEB интерфейса:

Management > SNMP > View

Management » SNMP » View

View Table

Showing All entriesShowing 1 to 1 of 1 entries

View	OID Subtree	Type
☐	all	.1 Included

AddDelete

FirstPrevious1NextLast

Параметр	Описание
View	Имя SNMP (максимальная длина - 30 символов)
OID Subtree	ASN.1 OID поддерева, включаемого/исключаемого из SNMP view
Type	Тип представления: • Include - включить указанные MIB • Exclude - исключить указанные MIB

Рекомендации:

1. Используйте осмысленные имена SNMP view, отражающие их назначение
2. Для безопасности рекомендуется:
 - Создавать минимально необходимые представления
 - Исключать чувствительные OID из публичных представлений
3. Проверьте корректность указанных OID

Пример создания SNMP view:

1. Перейдите в раздел Management > SNMP > View;
2. Нажмите "Add";
3. Заполните параметры:
 - View: limited_access
 - Subtree OID: 1.3.6.1.2.1.2 (интерфейсы)
 - View Type: Include
4. Нажмите "Apply"

Примечание: OID должны указываться в числовом формате (например, 1.3.6.1.2.1.1 для системной группы MIB-II).

17.4.2. Группы SNMP (Group)

Для настройки параметров SNMP-групп перейдите в следующий раздел WEB интерфейса:

Management > SNMP > Group

Management >> SNMP >> Group

Group Table

Showing [All] entries

Showing 1 to 3 of 3 entries

	Group	Version	Security Level	View		
				Read	Write	Notify
☐	G1	SNMPv1	No Security	all		
☐	G2	SNMPv1	No Security	all		
☐	G3	SNMPv1	No Security	all		

First Previous 1 Next Last

Configure **SNMP View** to associate a non-default view with a group.

Add

Edit

Delete

Основные параметры группы SNMP

Параметр	Описание
Group	Название SNMP-группы (до 30 символов)
Version	Версия SNMP: • SNMPv1 • SNMPv2c (community-based) • SNMPv3 (user security model)
Security Level	Уровень безопасности (для SNMPv3): • No Security - без аутентификации • Authentication - только аутентификация • Authentication and Privacy - аутентификация и шифрование

Параметр	Описание
Права доступа группы SNMP	
Read View	Представление для чтения
Write View	Представление для записи
Notify View	Представление для уведомлений (traps)

Management » SNMP » Group

Add Group

Group	G3
Version	☒ SNMPv1 ☐ SNMPv2 ☐ SNMPv3
Security Level	☒ No Security ☐ Authentication ☐ Authentication and Privacy
	☒ Read
	all ▼
View	☐ Write
	all ▼
	☐ Notify
	all ▼

Apply

Close

Диалог добавления SNMP группы

Параметр	Описание
Group	Название SNMP-группы (до 30 символов)
Version	Версия SNMP: • SNMPv1 • SNMPv2c (community-based) • SNMPv3 (user security model)
Security Level	Уровень безопасности (только для SNMPv3): • No Security - без аутентификации • Authentication - только аутентификация • Authentication and Privacy - аутентификация и шифрование
Права доступа группы SNMP	
Read View	Представление для чтения
Write View	Представление для записи
Notify View	Представление для уведомлений (traps)

Edit Group

Group

Version

Security Level

View

G2

☒ SNMPv1

☐ SNMPv2

☐ SNMPv3

☒ No Security

☐ Authentication

☐ Authentication and Privacy

☒ Read

all

☒ Write

all

☒ Notify

all

Apply

Close

Диалог редактирования SNMP группы

Параметр	Описание
Group	Название SNMP-группы (до 30 символов)
Version	Версия SNMP: • SNMPv1 • SNMPv2c (community-based) • SNMPv3 (user security model)
Security Level	Уровень безопасности (только для SNMPv3): • No Security - без аутентификации • Authentication - только аутентификация

Параметр	Описание
	• Authentication and Privacy - аутентификация и шифрование

Рекомендации по безопасности:

1. Для разных уровней доступа создавайте отдельные группы
2. Для SNMPv3 всегда используйте Authentication and Privacy
3. Ограничивайте Write-права минимально необходимыми OID
4. Регулярно пересматривайте назначенные права

Пример создания группы:

1. Перейдите в раздел Management > SNMP > Group;
2. Нажмите "Add";
3. Заполните параметры:
 - Group: network_admins
 - Version: SNMPv3
 - Security Level: Authentication and Privacy
 - Read View: full_access
 - Write View: config_access
 - Notify View: trap_events
4. Нажмите "Apply"

Внимание! Для SNMPv1/v2c community-строка выступает в роли аутентификатора. Используйте сложные community-строки вместо стандартных "public"/"private".

17.4.3. Настройка SNMP community (Community)

Для настройки параметров SNMP community перейдите:

Management > SNMP > Community

Management >> SNMP >> Community

Community Table

Showing

All

 entries Showing 1 to 3 of 3 entries

Q

☐	Community	Group	View	Access
☐	COMN1		all	Read-Only
☐	COMN2		all	Read-Only
☐	public		all	Read-Only

First

Previous

1

Next

Last

The access right of a community is defined by a group under advanced mode.
Configure **SNMP Group** to associate a group with a community.

Add

Edit

Delete

Таблица SNMP community

Параметр	Описание
Community	Имя SNMP community (до 20 символов)
Group	Связанная SNMP-группа (в Advanced-режиме)
View	SNMP view для доступа (в Basic-режиме)
Access	Уровень доступа: • Read-Only (только чтение) • Read-Write (чтение и запись)

Add Community

Community	
Type	☒ Basic ☐ Advanced
View	all ▼
Access	☒ Read-Only ☐ Read-Write
Group	G1 ▼

Диалог добавления SNMP community

Параметр	Описание
Community	Имя SNMP community (до 20 символов)
Type	Режим работы SNMP community: • Basic - прямое назначение прав • Advanced - привязка к группе
View	SNMP view
Access	Уровень доступа: • Read-Only (только чтение) • Read-Write (чтение и запись)

Edit Community

Community	COMN2
Type	☒ Basic ☐ Advanced
View	all ▼
Access	☒ Read-Only ☐ Read-Write
Group	G1 ▼

Диалог редактирования SNMP community

Параметр	Описание
Community	Имя SNMP community (до 20 символов)
Type	Режим работы SNMP community: • Basic - прямое назначение прав • Advanced - привязка к группе
View	SNMP view
Access	Уровень доступа: • Read-Only (только чтение) • Read-Write (чтение и запись)

Рекомендации по безопасности:

1. Никогда не используйте стандартные имена (public/private)
2. Для разных устройств используйте разные community-строки
3. Регулярно обновляйте community-строки (каждые 3-6 месяцев)
4. Для записи используйте сложные строки длиной не менее 12 символов

Пример настройки (Basic-режим):

1. Перейдите в раздел Management > SNMP > Community;
2. Нажмите "Add";
3. Заполните параметры:
 - Community: N3tW0rk_M0n1t0r
 - Type: Basic
 - View: read_only_view
 - Access: Read-Only
4. Нажмите "Apply"

Пример настройки (Advanced-режим):

1. Перейдите в раздел Management > SNMP > Community;
2. Нажмите "Add";
3. Заполните параметры:
 - Community: C0nF1g_Adm1n
 - Type: Advanced
 - Group: config_admins
4. Нажмите "Apply"

Внимание! В Advanced-режиме права доступа наследуются от связанной SNMP-группы. Этот режим рекомендуется для сложных конфигураций.

17.4.4. Пользователи SNMP (User)

Для настройки параметров SNMP-пользователей перейдите в раздел:

Management > SNMP > User

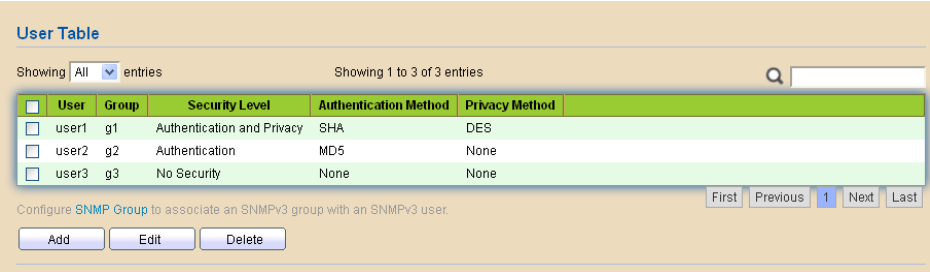


Таблица SNMP пользователей

Параметр	Описание
User	Имя пользователя (до 30 символов). Для SNMPv1/v2c должно совпадать с community-строкой
Group	Группа SNMP, к которой принадлежит пользователь
Security Level	Уровень безопасности: • No Security - без защиты • Authentication - только аутентификация • Authentication and Privacy - аутентификация и шифрование
Authentication Method	Метод аутентификации: • None (отсутствует) • MD5 (HMAC-MD5-96)

Параметр	Описание
	• SHA (HMAC-SHA-96)
Privacy Method	Метод шифрования: • None (отсутствует) • DES

Add User

User

Group

g31

Security Level

☒ No Security
☐ Authentication
☐ Authentication and Privacy

Authentication

Method

☒ None
☐ MD5
☐ SHA

Password

Privacy

Method

☒ None
☐ DES

Password

Apply

Close

Диалог добавления нового пользователя SNMP

Параметр	Описание
User	Имя пользователя (до 30 символов). Для SNMPv1/v2c должно совпадать с community-строкой

Параметр	Описание
Group	Группа SNMP, к которой принадлежит пользователь
Security Level	Уровень безопасности: • No Security - без защиты • Authentication - только аутентификация • Authentication and Privacy - аутентификация и шифрование
Authentication	
Method	Метод аутентификации: • None (отсутствует) • MD5 (HMAC-MD5-96) • SHA (HMAC-SHA-96)
Password	Пароль аутентификации (8-32 символа)
Privacy	
Method	Метод шифрования: • None (отсутствует) • DES
Password	Пароль шифрования (8-64 символа)

Edit User

User

user1

Group

g1

Security Level

☐ No Security
☐ Authentication
☒ Authentication and Privacy

Authentication

Method

☐ None
☐ MD5
☒ SHA

Password

Privacy

Method

☐ None
☒ DES

Password

Apply

Close

Диалог редактирования пользователя SNMP

Параметр	Описание
User	Имя пользователя (до 30 символов). Для SNMPv1/v2c должно совпадать с community-строкой
Group	Группа SNMP, к которой принадлежит пользователь
Security Level	Уровень безопасности: • No Security - без защиты • Authentication - только аутентификация • Authentication and Privacy - аутентификация и шифрование

Параметр	Описание
Authentication	
Method	Метод аутентификации: • None (отсутствует) • MD5 (HMAC-MD5-96) • SHA (HMAC-SHA-96)
Password	Пароль аутентификации (8-32 символа)
Privacy	
Method	Метод шифрования: • None (отсутствует) • DES
Password	Пароль шифрования (8-64 символа)

Рекомендации по безопасности:

- Для SNMPv3 всегда используйте:
 - Security Level: Authentication and Privacy
 - Authentication Method: SHA
 - Privacy Method: DES
- Пароли должны:
 - Быть не менее 12 символов
 - Содержать буквы, цифры и спецсимволы
 - Не совпадать с другими учетными данными

Пример создания пользователя:

1. Перейдите в раздел Management > SNMP > User;
2. Нажмите "Add";
3. Заполните параметры:
 - User: netadmin_snmp
 - Group: network_admins
 - Security Level: Authentication and Privacy
 - Authentication Method: SHA
 - Password: Str0ngAuthP@ss!
 - Privacy Method: DES
 - Privacy Password: EvenStr0ngerPriv@cy
4. Нажмите "Apply"

Внимание!

- Для SNMPv1/v2c настройки аутентификации и шифрования недоступны
- Пароли хранятся в зашифрованном виде в конфигурации
- Регулярно обновляйте пароли (рекомендуется каждые 3-6 месяцев)

17.4.5. Идентификатор Engine (Engine ID)

Для настройки локального и удаленного Engine ID перейдите:

Management > SNMP > Engine ID

Management >> SNMP >> Engine ID

Local Engine ID

Engine ID

☐ User Defined

80006a920300e04c000000 (10 - 64 Hexadecimal Characters)

Apply

Remote Engine ID Table

Showing All entries Showing 1 to 2 of 2 entries

	Server Address	Engine ID
☐	192.168.1.100	112223FDEDFE
☐	192.168.1.99	00004DADDDDDDD

Add

Edit

Delete

First

Previous

1

Next

Last

Локальный Engine ID

Параметр	Описание
Engine ID	Режим определения: • User Defined - ручной ввод (10-64 хех-символов, четное количество) • По умолчанию - автоматическая генерация на основе MAC-адреса и Enterprise ID

Таблица удаленных Engine ID

Параметр	Описание
Server Address	Адрес удаленного хоста
Engine ID	Идентификатор Engine удаленного SNMP-устройства (10-64 hex-символов)

Management >> SNMP >> Engine ID

Add Remote Engine ID

Address Type

Server Address

Engine ID

☒ Hostname

☐ IPv4

☐ IPv6

(10 - 64 Hexadecimal Characters)

Apply

Close

Диалог добавления Engine ID

Параметр	Описание
Address Type	Тип адреса • Hostname • IPv4 • IPv6
Server Address	Адрес удаленного хоста

Параметр	Описание
Engine ID	Идентификатор Engine удаленного SNMP-устройства (10-64 hex-символов)

Management » SNMP » Engine ID

Edit Remote Engine ID

Server Address

192.168.1.100

Engine ID

112223FDEDFE

(10 - 64 Hexadecimal Characters)

Apply

Close

Диалог изменения существующего Engine ID

Параметр	Описание
Server Address	Адрес удаленного хоста
Engine ID	Идентификатор Engine удаленного SNMP-устройства (10-64 hex-символов)

Рекомендации:

- Для совместимости между устройствами:
 - Используйте одинаковый формат Engine ID в пределах одной сети
 - Регистрируйте назначенные ID в документации
- При ручной настройке:

- Используйте осмысленные hex-значения
- Включайте идентификатор организации
- Сохраняйте записи о назначенных ID

Пример настройки:

1. Перейдите в раздел Management > SNMP > Engine ID;
2. Для локального Engine ID:
 - Выберите "User Defined"
 - Введите: 800007C00008ABCDEF12 (пример)
3. Для удаленного Engine ID:
 - Нажмите "Add"
 - Укажите:
 - Address Type: IPv4
 - Server Address: 192.168.1.100
 - Engine ID: 800007C00009FEDCBA98
 - Нажмите "Apply"

Примечание:

- Engine ID используется для безопасного обмена SNMPv3-сообщениями
- Изменение Engine ID сбрасывает все SNMPv3-ключи
- Для генерации ID можно использовать MAC-адрес устройства с префиксом предприятия

17.4.6. Настройка SNMP Trap Event (Trap Event)

Для настройки SNMP-трапов событий перейдите в следующий раздел:

Management > SNMP > Trap Event



Настройки трапов SNMP

Параметр	Описание
Authentication Failure	Генерация трапа при ошибке аутентификации (неверный community или пароль)
Link Up/Down	Трапы изменения состояния линка порта (up/down)
Cold Start	Трап при перезагрузке устройства по команде пользователя
Warm Start	Трап при перезагрузке устройства из-за сбоя питания

Рекомендации по настройке:

1. Обязательные SNMP трапы для мониторинга:
 - Link Up/Down - для отслеживания состояния портов
 - Authentication Failure - для выявления попыток несанкционированного доступа
2. Дополнительные настройки:
 - Для Cold/Warm Start укажите корректные community-строки
 - Настройте корректные адреса NMS-серверов

Пример включения SNMP трапов:

1. Перейдите в раздел Management > SNMP > Trap Event;
2. Активируйте нужные события:
 - ☒ Authentication Failure
 - ☒ Link Up/Down
 - ☒ Cold Start
3. Нажмите "Apply"

Внимание! Для работы трапов необходимо предварительно настроить:

- SNMP-community (для v1/v2c) или пользователей (для v3)
- Корректные Engine ID для SNMPv3

17.4.7. Уведомления SNMP (Notification)

Для настройки получателей SNMP-уведомлений перейдите:

Management > SNMP > Notification

Management >> SNMP >> Notification

Notification Table

Showing All entries Showing 1 to 2 of 2 entries

	Server Address	Server Port	Timeout	Retry	Version	Type	Community / User	Security Level
☐	192.168.1.110	162			SNMPv1	Trap	COMN1	No Security
☐	192.168.1.88	162			SNMPv1	Trap	COMN1	No Security

First Previous 1 Next Last

For SNMPv1,2 Notification, [SNMP Community](#) needs to be defined.
For SNMPv3 Notification, [SNMP User](#) must be created.

Add Edit Delete

Таблица уведомлений SNMP

Параметр	Описание
Server Address	IP-адрес или имя хоста получателя
Server Port	UDP-порт получателя (по умолчанию 162)
Timeout	Таймаут между SNMP уведомлениями (по умолчанию 15 сек)
Retry	Счетчик попыток SNMP уведомлений (по умолчанию 3)
Version	Версия SNMP: • SNMPv1 • SNMPv2 • SNMPv3

Параметр	Описание
Type	Тип уведомления: • Trap (однаправленные) • Inform (с подтверждением)
Community/User	Community-строка (SNMP v1/v2) или имя пользователя (SNMP v3)
Security Level	Уровень безопасности (SNMP v3): • No Security – без аутентификации • Authentication – аутентификация • Authentication and Privacy – аутентификация и шифрование.

Management » SNMP » Notification

Add Notification

Address Type
Server Address
Version
Type
Community / User
Security Level
Server Port
Timeout
Retry

☒ Hostname
☐ IPv4
☐ IPv6

☒ SNMPv1
☐ SNMPv2
☐ SNMPv3
☒ Trap
☐ Inform
COMN1 ▾
☒ No Security
☐ Authentication
☐ Authentication and Privacy
☒ Use Default
162 (1 - 65535, default 162)
☒ Use Default
15 Sec (1 - 300, default 15)
☒ Use Default
3 (1 - 255, default 3)

Apply Close

Диалог добавления *SNMP* уведомлений

Параметр	Описание
Address Type	Тип адреса • Hostname • IPv4 • IPv6
Server Address	IP-адрес или имя хоста получателя
Version	Версия SNMP: • SNMPv1 • SNMPv2 • SNMPv3
Type	Тип уведомления: • Trap (однаправленные) • Inform (с подтверждением)
Community/User	Community-строка (SNMP v1/v2) или имя пользователя (SNMP v3)
Security Level	Уровень безопасности (SNMP v3): • No Security – без аутентификации • Authentication – аутентификация • Authentication and Privacy – аутентификация и шифрование.
Server Port	UDP-порт получателя (по умолчанию 162)
Timeout	Таймаут между SNMP уведомлениями (по умолчанию 15 сек)

Параметр	Описание
Retry	Счетчик попыток SNMP уведомлений (по умолчанию 3)

Management » SNMP » Notification

Edit Notification

Server Address	192.168.1.110
Version	☒ SNMPv1 ☐ SNMPv2 ☐ SNMPv3
Type	☒ Trap ☐ Inform
Community / User	COMN1 ▾
Security Level	☒ No Security ☐ Authentication ☐ Authentication and Privacy
Server Port	☒ Use Default 162 (1 - 65535, default 162)
Timeout	☒ Use Default 15 Sec (1 - 300, default 15)
Retry	☒ Use Default 3 (1 - 255, default 3)

Apply Close

Диалог изменения SNMP уведомлений

Параметр	Описание
Address Type	Тип адреса • Hostname • IPv4 • IPv6

Параметр	Описание
Server Address	IP-адрес или имя хоста получателя
Version	Версия SNMP: • SNMPv1 • SNMPv2 • SNMPv3
Type	Тип уведомления: • Trap (однаправленные) • Inform (с подтверждением)
Community/User	Community-строка (SNMP v1/v2) или имя пользователя (SNMP v3)
Security Level	Уровень безопасности (SNMP v3): • No Security – без аутентификации • Authentication – аутентификация • Authentication and Privacy – аутентификация и шифрование.
Server Port	UDP-порт получателя (по умолчанию 162)
Timeout	Таймаут между SNMP уведомлениями (по умолчанию 15 сек)
Retry	Счетчик попыток SNMP уведомлений (по умолчанию 3)

Рекомендации:

1. Для критически важных уведомлений используйте Inform (с подтверждением)
2. Разделяйте трапы по версиям и получателям:
 - SNMPv1/v2c - для legacy-систем (устаревших)
 - SNMPv3 - для безопасной передачи
3. Для SNMPv3 всегда используйте максимальный уровень безопасности

Пример настройки:

1. Перейдите в раздел Management > SNMP > Notification;
2. Нажмите "Add";
3. Заполните параметры:
 - Address Type: IPv4
 - Server Address: 192.168.1.200
 - Version: SNMPv3
 - Type: Inform
 - User: snmp_admin
 - Security Level: Authentication and Privacy
 - Server Port: 162 (default)
 - Timeout: 20 (сек)
 - Retry: 5
4. Нажмите "Apply"

Внимание!

- SNMPv1 не поддерживает Inform-сообщения
- Для Inform-сообщений требуется больше ресурсов коммутатора
- Убедитесь, что брандмауэр разрешает трафик на указанный порт

17.5. Настройка RMON (Remote Monitoring)

17.5.1. Статистика RMON (Statistics)

Для просмотра RMON-статистики перейдите в следующий раздел WEB интерфейса:

Management > RMON > Statistics

Management >> RMON >> Statistics

Statistics Table

Refresh Rate 0 sec

	Entry	Port	Bytes Received	Drop Events	Packets Received	Broadcast Packets	Multicast Packets	CRC & Align Errors	Undersize Packets	Oversize Packets
☐	1	GE1	0	0	0	0	0	0	0	0
☐	2	GE2	0	0	0	0	0	0	0	0
☐	3	GE3	0	0	0	0	0	0	0	0
☐	4	GE4	0	0	0	0	0	0	0	0
☐	5	GE5	0	0	0	0	0	0	0	0
☐	6	GE6	0	0	0	0	0	0	0	0
☐	7	GE7	396656	0	2488	113	454	0	0	0
☐	8	GE8	0	0	0	0	0	0	0	0
☐	9	GE9	0	0	0	0	0	0	0	0
☐	10	GE10	0	0	0	0	0	0	0	0
☐	11	LAG1	0	0	0	0	0	0	0	0
☐	12	LAG2	0	0	0	0	0	0	0	0
☐	13	LAG3	0	0	0	0	0	0	0	0
☐	14	LAG4	0	0	0	0	0	0	0	0
☐	15	LAG5	0	0	0	0	0	0	0	0
☐	16	LAG6	0	0	0	0	0	0	0	0
☐	17	LAG7	0	0	0	0	0	0	0	0
☐	18	LAG8	0	0	0	0	0	0	0	0

Clear

Refresh

View

Таблица статистики RMON

Параметр	Описание
Entry	Номер записи в таблице
Port	Номер порта

Параметр	Описание
Bytes Received	Общее количество полученных байт (включая ошибки)
Drop Events	Количество отброшенных пакетов
Packets Received	Общее количество полученных пакетов
Broadcast Packets	Количество широковещательных пакетов
Multicast Packets	Количество multicast-пакетов
CRC & Align Errors	Ошибки CRC (контрольной суммы) и выравнивания
Undersize Packages	Пакеты менее 64 байт
Oversize Packages	Пакеты более 1518 байт
Fragments	Фрагментированные пакеты (<64 байт без ошибок)
Jabbers	Ошибочные пакеты (>1632 байт)
Collision	Количество коллизий
Frames of 64 Bytes	Количество полученных пакетов размером до 64 байт

Параметр	Описание
Frames of 65 to 127 Bytes	Количество полученных пакетов размером от 65 до 127 байт
Frames of 128 to 255 Bytes	Количество полученных пакетов размером от 128 до 256 байт
Frames of 256 to 511 Bytes	Количество полученных пакетов размером от 256 до 511 байт
Frames of 512 to 1024 Bytes	Количество полученных пакетов размером от 512 до 1024 байт
Frames Greater than 1024 Bytes	Количество полученных пакетов размером более 1024 байт

Управление

Кнопка	Описание
Clear	Сброс статистики для выбранных портов
View	Просмотр детальной статистики на выбранном порту

View Port Statistics

Port	GE1
Refresh Rate	☒ None ☐ 5 sec ☐ 10 sec ☐ 30 sec
Received Bytes (Octets)	0
Drop Events	0
Received Packets	0
Broadcast Packets Received	0
Multicast Packets Received	0
CRC & Align Errors	0
Undersize Packets	0
Oversize Packets	0
Fragments	0
Jabbers	0
Collisions	0
Frames of 64 Bytes	0
Frames of 65 to 127 Bytes	0
Frames of 128 to 255 Bytes	0
Frames of 256 to 511 Bytes	0
Frames Greater than 1024 Bytes	0

Рекомендации по анализу данных:

- Мониторинг ошибок:
 - CRC & Align Errors** > 1% от общего трафика - проверить кабель/порт
 - Collision** > 5% - возможны проблемы в сети
- Анализ распределения:
 - Преобладание **64 Bytes** - может указывать на атаки на сеть
 - Высокий % **Broadcast** пакетов (>20%) - возможен broadcast storm

Пример использования:

1. Перейдите в раздел Management > RMON > Statistics;
2. Выберите интересующий порт;
3. Нажмите **View** для детальной статистики;
4. Проанализируйте:
 - Общий объем трафика (Bytes Received)
 - Процент ошибок (CRC & Align Errors)
 - Распределение по размерам пакетов
5. Для сброса статистики нажмите **Clear**

Внимание! Статистика собирается с момента последнего сброса или включения порта. Для долгосрочного мониторинга используйте SNMP-мониторинг с внешней системой (Zabbix и т.д.)

17.5.2. История RMON (History)

Для настройки и просмотра RMON-истории перейдите:

Management > RMON > History

Management >> RMON >> History

History Table

Showing All entries Showing 1 to 2 of 2 entries

	Entry	Port	Interval	Owner	Sample	
					Maximum	Current
☐	1	GE1	1800	RAINBOW	50	50
☐	2	GE1	1800	CERR	50	50

First Previous 1 Next Last

The SNMP service is currently disabled.
For RMON configuration to be effective, the [SNMP service](#) must be enabled.

Add Edit Delete View

Таблица RMON

Параметр	Описание
Entry	Номер записи
Port	Номер порта для мониторинга
Interval	Интервал сбора данных (в секундах)
Owner	Владелец записи (0-31 символ)
Max Sample	Максимальное количество хранимых образцов
Current Sample	Текущее количество собранных образцов

Управление записями

Кнопка	Описание
Add	Добавить новую запись мониторинга
Edit	Изменить параметры сбора
Delete	Удалить запись мониторинга
View	Просмотр собранных данных

Add History

Entry	3	
Port	GE1 ▼	
Max Sample	50	(1 - 50, default 50)
Interval	1800	(1 - 3600, default 1800)
Owner		

Apply

Close

Диалог добавления записи RMON

Параметр	Описание
Entry	Номер записи
Port	Номер порта для мониторинга
Max Sample	Максимальное количество хранимых образцов (1-50)
Interval	Интервал сбора данных (в секундах, 1 – 3600сек)
Owner	Владелец записи (0-31 символ)

Edit History

Entry	2	
Port	GE1 ▼	
Max Sample	50	(1 - 50, default 50)
Interval	1800	(1 - 3600, default 1800)
Owner	CERR	

Apply

Close

Диалог редактирования записи RMON

Параметр	Описание
Entry	Номер записи
Port	Номер порта для мониторинга
Max Sample	Максимальное количество хранимых образцов (1-50)
Interval	Интервал сбора данных (в секундах, 1 – 3600сек)
Owner	Владелец записи (0-31 символ)

View History

Entry: 1

Showing All ▾ entries

Showing 0 to 0 of 0 entries

Sample No.	Drop Events	Bytes Received	Packets Received	Broadcast Packets	Multicast Packets	CRC & Align Errors	Undersize Packets	Oversize Packets
------------	-------------	----------------	------------------	-------------------	-------------------	--------------------	-------------------	------------------

0 results found.

Close

Параметры журнала RMON History

Параметр	Описание
Sample No.	Номер образца
Drop Events	Количество отброшенных пакетов
Bytes Received	Общее количество полученных байт
Packets Received	Общее количество полученных пакетов (включая ошибочные, multicast и broadcast)
Broadcast Packets	Количество корректных broadcast-пакетов (без учета multicast)
Multicast packets	Количество корректных multicast-пакетов
CRC & Align	Ошибки передачи данных

Параметр	Описание
Errors	
Undersize Packages	Количество пакетов размером менее 64 октетов
Oversize Packages	Количество пакетов размером более 1518 октетов
Fragments	Количество фрагментированных пакетов (<64 октетов, исключая служебные биты, но включая FCS)
Jabbers	Количество ошибочных пакетов (>1632 октетов), соответствующих критериям: • Длина пакета превышает MRU • Неверная CRC (контрольная сумма пакета) • Не обнаружены RX-ошибки
Utilization	Процент использования пропускной способности порта

Рекомендации по настройке:

1. Оптимальные параметры сбора данных:
 - **Interval:** 30-300 сек для долгосрочного анализа
 - **Max Sample:** 50-100 записей для недельного мониторинга
2. Для критичных портов:
 - Уменьшите интервал сбора (10-30 сек)
 - Увеличьте количество образцов (150-200)

Пример настройки:

1. Перейдите в раздел Management > RMON > History;
2. Нажмите "Add"
3. Заполните параметры:
 - Port: GE24
 - Interval: 60
 - Max Sample: 1440 (сутки с минутным интервалом)
 - Owner: Network_Admin
4. Нажмите "Apply"

Внимание!

- Данные сохраняются до перезагрузки коммутатора
- Для длительного хранения используйте внешние системы мониторинга
- Высокий % Utilization (>70%) требует анализа и оптимизации трафика

17.5.3. События RMON (Event)

Для настройки RMON-событий перейдите в следующий раздел WEB интерфейса коммутатора:

Management > RMON > Event

Management >> RMON >> Event

Event Table

Showing All entries Showing 1 to 2 of 2 entries

Entry	Community	Description	Notification	Time	Owner
☐ 1		Default Description	None		RAINBOW
☐ 2		Default Description	None		FEER

First Previous 1 Next Last

The SNMP service is currently disabled.
For RMON configuration to be effective, the [SNMP service](#) must be enabled.

Add Edit Delete View

Основные параметры событий

Параметр	Описание
Entry	Номер записи в журнале
Community	SNMP-community для отправки trap-сообщений
Description	Описание события (до 255 символов)
Notification	Тип уведомления: • None - без уведомления • Event Log - запись в лог • Trap - отправка SNMP-trap • Event Log and Trap - запись + trap

Параметр	Описание
Time	Время срабатывания события
Owner	Владелец события (до 31 символа)

Управление событиями (описание кнопок)

Действие (кнопка)	Описание
Add	Добавить новое событие
Edit	Изменить параметры события
Delete	Удалить событие

Management >> RMON >> Event

Add Event

Entry	3
Notification	☒ None ☐ Event Log ☐ Trap ☐ Event Log and Trap
Community	Default Community
Description	Default Description
Owner	

Apply Close

Диалог добавления события RMON

Параметр	Описание
Notification	Тип уведомления: • None - без уведомления • Event Log - запись в лог • Trap - отправка SNMP-trap • Event Log and Trap - запись + trap
Community	SNMP-community для отправки trap-сообщений
Description	Описание события (до 255 символов)
Owner	Владелец события (до 31 символа)

Management » RMON » Event

Edit Event

Entry	2
Notification	☒ None ☐ Event Log ☐ Trap ☐ Event Log and Trap
Community	
Description	Default Description
Owner	FEER

Диалог изменения события RMON

Параметр	Описание
Notification	Тип уведомления: • None - без уведомления • Event Log - запись в лог • Trap - отправка SNMP-trap • Event Log and Trap - запись + trap
Community	SNMP-community для отправки trap-сообщений
Description	Описание события (до 255 символов)
Owner	Владелец события (до 31 символа)

Management >> RMON >> Event

View Event Log

Entry: 2

Showing All entries Showing 0 to 0 of 0 entries

Log ID	Time	Description
0 results found.		

CloseFirstPrevious1NextLast

Параметры журнала событий

Параметр	Описание
Log ID	Уникальный идентификатор записи
Time	Время возникновения события

Параметр	Описание
Description	Описание зарегистрированного события

Рекомендации по настройке:

1. Для критических событий используйте "Event Log and Trap"
2. Настройте разные сообщества для:
 - Информационных событий (read-only)
 - Критических событий (read-write)
3. Используйте описательные имена владельцев:
 - "Network_Monitoring"
 - "Security_Alerts"

Пример настройки:

1. Перейдите в раздел Management > RMON > Event
2. Нажмите "Add" (добавить)
3. Заполните параметры:
 - Description: "High Port Utilization >80%"
 - Notification: Event Log and Trap
 - Community: critical_traps
 - Owner: Network_Operations
4. Нажмите "Apply" (принять)

Внимание!

- Для работы trap-уведомлений должна быть настроена SNMP-инфраструктура
- Логи событий сохраняются до перезагрузки устройства
- Регулярно экспортируйте логи для долговременного хранения

17.5.4. Тревожные сообщения RMON (Alarm)

Для настройки RMON-тревожных сообщений перейдите в следующий раздел WEB интерфейса:

Management > RMON > Alarm

Management >> RMON >> Alarm

Alarm Table

Showing All entries Showing 1 to 2 of 2 entries

	Entry	Port	Counter		Sampling	Interval	Owner	Trigger	Rising	
			Name	Value					Threshold	Event
☐	1	GE1	DropEvents	0	Absolute	100	RAINBOW	Rising	100	Default Descript
☐	2	GE1	DropEvents	0	Absolute	100	DDDEEE	Rising	100	Default Descript

The SNMP service is currently disabled.
For RMON configuration to be effective, the [SNMP service](#) must be enabled.

AddEditDelete

Основные параметры тревожных сообщений RMON

Параметр	Описание
Entry	Номер записи
Port	Порт для мониторинга
Counter	Счетчик отслеживаемых событий: - Drop Events – отброшенные пакеты - Received Bytes – принятые байты - Received Packets – принятые пакеты - Broadcast Packets – пакеты broadcast-трафика

Параметр	Описание
	• Multicast Packets – пакеты multicast-трафик • CRC and Align Error – ошибки CRC суммы • Undersize Packets – пакеты размером <64 байт • Oversize Packets – пакеты размером >1518 байт • Fragments – общее кол-во фрагментированных пакетов • Jabbers – общее вол-во ошибочных пакетов • Collisions – коллизии • Pkts64Octetes – кол-во пакетов размером 64 байта • Pkts65to127Octetes – кол-во пакетов размером от 65 до 127 байт • Pkts128to255Octetes – кол-во пакетов размером от 128 до 255 байт • Pkts256to511Octetes – кол-во пакетов размером от 256 до 511 байт • Pkts512to1023Octetes – кол-во пакетов размером от 512 до 1023 байт • Pkts1024to1518Octetes – кол-во пакетов размером от 1024 до 1518 байт
Sampling	Тип сэмплирования: • Absolute - абсолютное значение • Delta - разница с предыдущим замером
Interval	Интервал проверки (в секундах)
Owner	Владелец алерта (до 31 символа)

Параметр	Описание
Trigger	Параметр срабатывания тревоги RMON
Rising	- Rising Threshold – Порог срабатывания "тревоги" - Rising Event – Событие при превышении порога
Falling	- Falling Threshold – Порог срабатывания "нормы" - Falling Event – Событие при возврате к норме

Management » RMON » Alarm

Add Alarm

Entry	3	
Port	GE1 ▼	
Counter	Drop Events ▼	
Sampling	☒ Absolute ☐ Delta	
Interval	100	Sec (1 - 2147483647, default 100)
Owner		
Trigger	☒ Rising ☐ Falling ☐ Rising and Falling	
Rising		
Threshold	100	(0 - 2147483647, default 100)
Event	1 - Default Description ▼	
Falling		
Threshold	20	(0 - 2147483647, default 20)
Event	1 - Default Description ▼	

Параметр	Описание
Port	Порт для мониторинга
Counter	Счетчик отслеживаемых событий: • Drop Events – отброшенные пакеты • Received Bytes – принятые байты • Received Packets – принятые пакеты • Broadcast Packets – пакеты broadcast-трафика • Multicast Packets – пакеты multicast-трафик • CRC and Align Error – ошибки CRC суммы • Undersize Packets – пакеты размером <64 байт • Oversize Packets – пакеты размером >1518 байт • Fragments – общее кол-во фрагментированных пакетов • Jabbers – общее вол-во ошибочных пакетов • Collisions – коллизии • Pkts64Octetes – кол-во пакетов размером 64 байта • Pkts65to127Octetes – кол-во пакетов размером от 65 до 127 байт • Pkts128to255Octetes – кол-во пакетов размером от 128 до 255 байт • Pkts256to511Octetes – кол-во пакетов размером от 256 до 511 байт • Pkts512to1023Octetes – кол-во пакетов размером от 512 до 1023 байт • Pkts1024to1518Octetes – кол-во пакетов размером от 1024 до 1518 байт

Параметр	Описание
Sampling	Тип сэмплирования: • Absolute - абсолютное значение • Delta - разница с предыдущим замером
Interval	Интервал проверки (в секундах). Значение по умолчанию 100сек. Допустимый интервал значений 1 – 2147483647 сек
Owner	Владелец алерта (до 31 символа)
Trigger	Параметр срабатывания тревоги RMON • Rising – превышение • Falling – возврат к норме • Rising and falling – Превышение и возврат к норме
Rising	• Rising Threshold – Порог срабатывания "тревоги". По умолчанию 100. Допустимый интервал значений 0 – 2147483647. • Rising Event – Событие при превышении порога
Falling	• Falling Threshold – Порог срабатывания "нормы". По умолчанию 20. Допустимый интервал значений 0 – 2147483647. • Falling Event – Событие при возврате к норме

Edit Alarm

Entry	2	
Port	GE1 ▼	
Counter	Drop Events ▼	
Sampling	☒ Absolute ☐ Delta	
Interval	100	Sec (1 - 2147483647, default 100)
Owner	DDDEEE	
Trigger	☒ Rising ☐ Falling ☐ Rising and Falling	
Rising		
Threshold	100	(0 - 2147483647, default 100)
Event	1 - Default Description ▼	
Falling		
Threshold	20	(0 - 2147483647, default 20)
Event	1 - Default Description ▼	

Диалог изменения тревожных сообщений RMON

Параметр	Описание
Port	Порт для мониторинга
Counter	Счетчик отслеживаемых событий: - Drop Events – отброшенные пакеты - Received Bytes – принятые байты - Received Packets – принятые пакеты

Параметр	Описание
	• Broadcast Packets – пакеты broadcast-трафика • Multicast Packets – пакеты multicast-трафик • CRC and Align Error – ошибки CRC суммы • Undersize Packets – пакеты размером <64 байт • Oversize Packets – пакеты размером >1518 байт • Fragments – общее кол-во фрагментированных пакетов • Jabbers – общее вол-во ошибочных пакетов • Collisions – коллизии • Pkts64Octetes – кол-во пакетов размером 64 байта • Pkts65to127Octetes – кол-во пакетов размером от 65 до 127 байт • Pkts128to255Octetes – кол-во пакетов размером от 128 до 255 байт • Pkts256to511Octetes – кол-во пакетов размером от 256 до 511 байт • Pkts512to1023Octetes – кол-во пакетов размером от 512 до 1023 байт • Pkts1024to1518Octetes – кол-во пакетов размером от 1024 до 1518 байт
Sampling	Тип сэмплирования: • Absolute - абсолютное значение • Delta - разница с предыдущим замером
Interval	Интервал проверки (в секундах). Значение по умолчанию 100сек. Допустимый интервал значений 1 – 2147483647 сек

Параметр	Описание
Owner	Владелец алерта (до 31 символа)
Trigger	Параметр срабатывания тревоги RMON • Rising – превышение • Falling – возврат к норме • Rising and falling – Превышение и возврат к норме
Rising	• Rising Threshold – Порог срабатывания "тревоги". По умолчанию 100. Допустимый интервал значений 0 – 2147483647. • Rising Event – Событие при превышении порога
Falling	• Falling Threshold – Порог срабатывания "нормы". По умолчанию 20. Допустимый интервал значений 0 – 2147483647. • Falling Event – Событие при возврате к норме

Рекомендации по настройке:

1. Для критичных портов:

- Интервал: 30-60 сек
- Rising Threshold: 80% от критического значения
- Falling Threshold: 50% от критического значения

2. Примеры порогов:

- Broadcast: >100 пакетов/сек
- CRC Errors: >5 ошибок/интервал
- Utilization: >70%

Пример настройки:

1. Перейдите в раздел Management > RMON > Alarm
2. Нажмите "Add" (добавить)
3. Заполните параметры:
 - Port: GE24
 - Counter: CRC and Align Error
 - Sampling: Delta
 - Interval: 60
 - Rising Threshold: 10
 - Rising Event: High_CRC_Error
 - Falling Threshold: 2
 - Owner: Network_Security
4. Нажмите "Apply" (принять)

Внимание!

Для работы событий (Events) они должны быть предварительно созданы в разделе Management > RMON > Event.