

**maiwe**

**Промышленный коммутатор Ethernet  
уровня 3**

# **WEB-Руководство пользователя**

➤ **MISCOM8036GX-4XGF-24GF-8GT**

Version: V1.0

## Уведомление об авторских правах

Все права защищены © Wuhan Maiwe Communications Co., Ltd.

является зарегистрированной торговой маркой Wuhan Maiwe Communications Co., Ltd.

Microsoft и Windows являются зарегистрированными торговыми марками корпорации Microsoft.

Все упомянутые в данном руководстве товарные знаки принадлежат соответствующим производителям.

## Заявление

Данное веб-руководство применимо к модели MISC0M8036GX-4XGF-24GF-8GT. Перед использованием данного руководства внимательно прочтите следующее лицензионное соглашение. Описанное в данном руководстве оборудование может использоваться только при условии вашего согласия с положениями лицензионного соглашения.

## Отказ от ответственности

Предоставление нашей компанией любой информации в данном руководстве не подразумевает предоставление соответствующих разрешений на ее использование.

Компания прилагает все усилия для обеспечения точности и применимости информации, содержащейся в данном руководстве. Однако компания не несет никакой ответственности за использование этой информации, а также не несет солидарной ответственности за ее применение. Продукты и руководства могут содержать технические или типографские ошибки.

Наша компания оставляет за собой право вносить изменения во все или часть данного руководства без предварительного уведомления.

Версия	Дата	Изменения
V1.0	2023.05	Создание файла

# Содержание

1	Веб-интерфейс устройства.....	13
1.1	Вход в сеть .....	13
1.2	Общие кнопки в веб-интерфейсе .....	15
1.3	Выход из веб-интерфейса .....	15
2	Системная информация .....	17
2.1	Системная информация .....	17
2.2	Статус порта.....	18
2.3	Загрузка ЦПУ .....	20
2.4	Системные настройки .....	20
3	Конфигурация портов .....	22
3.1	Конфигурация портов .....	22
3.2	Имя порта .....	25
3.3	Агрегирование портов .....	26
3.3.1	Конфигурация группы агрегации .....	26
3.3.2	Режим балансировки нагрузки .....	28
3.3.3	Статус группы агрегации.....	29
3.3.4	LACP .....	29
3.3.4.1	Конфигурация LACP .....	29
3.3.4.2	Состояние системы .....	31
3.3.4.3	Статус локального порта .....	31
3.3.4.4	Статус пирингового порта .....	33
3.3.4.5	Статистика кадров LACP .....	34
3.4	Зеркалирование портов .....	34
3.5	Статистика портов .....	37
3.5.1	Сводные статистические данные .....	38
3.5.2	Подробная статистика.....	39

3.5.3	Статистика управляющих кадров.....	42
4	Характеристики уровня 2 .....	43
4.1	VLAN .....	43
4.1.1	Глобальная конфигурация .....	43
4.1.2	Конфигурация SVL .....	44
4.1.3	Члены VLAN .....	45
4.1.4	Статус портов.....	46
4.2	Перевод VLAN.....	47
4.2.1	Конфигурация группы портов .....	47
4.2.2	Отображение VLAN .....	49
4.3	Расширенные настройки VLAN .....	50
4.3.1	MAC-VLAN .....	50
4.3.2	Протокол-VLAN .....	50
4.3.2.1	Протокол-Группа .....	50
4.3.2.2	Группа-VLAN .....	51
4.3.3	IP-VLAN .....	51
4.4	PVLAN.....	52
4.4.1	Конфигурация участников .....	52
4.4.2	Изоляция портов.....	53
4.5	Таблица адресов MAC .....	53
4.5.1	Конфигурация таблицы адресов.....	53
4.5.2	Запись MAC-адреса .....	55
4.6	IGMP-Snooping.....	56
4.6.1	Базовая конфигурация .....	56
4.6.2	Конфигурация VLAN .....	57
4.6.3	Статус .....	58
4.6.4	Информация о группе .....	60
4.6.5	Настройка фильтрации .....	60
4.6.6	Информация SFM.....	61

4.7	Фильтрация многоадресной рассылки.....	62
4.7.1	Файл конфигурации.....	62
4.7.2	Записи адресов.....	65
4.8	LLDP.....	65
4.8.1	Конфигурация LLDP .....	66
4.8.2	Информация о соседях.....	70
4.8.3	Статистика порта .....	71
5	Резервирование кольцевой сети.....	74
5.1	ERPS.....	74
5.1.1	Конфигурация ERPS .....	74
5.1.2	ERPS статус .....	77
5.2	Протокол связующего дерева (STP) .....	80
5.2.1	Конфигурация моста STP .....	81
5.2.2	Отображение экземпляров .....	83
5.2.3	Приоритет экземпляра .....	84
5.2.4	Порт CIST .....	84
5.2.5	Порт экземпляра.....	86
5.2.6	Статус моста .....	87
5.2.7	Статус порта.....	90
5.2.8	Статистика порта .....	91
5.3	Обнаружение петель .....	92
5.3.1	Конфигурация обнаружения петель.....	92
5.3.2	Статус обнаружения петель .....	94
6	Характеристики уровня 3 .....	96
6.1	Управление IP .....	96
6.1.1	Конфигурация IP .....	96
6.1.2	Информация IP .....	99
6.1.3	Таблица маршрутизации IPv4 .....	101
6.1.4	Таблица маршрутизации IPv6 .....	101

6.2	RIP (Протокол маршрутизации информации) .....	102
6.2.1	Глобальная конфигурация .....	102
6.2.2	Конфигурация сети .....	105
6.2.3	Конфигурация соседей .....	106
6.2.4	Пассивный интерфейс .....	107
6.2.5	Конфигурация интерфейса .....	107
6.2.6	Привязка значения метрики и фильтрация сообщений .....	108
6.2.7	Глобальный статус .....	109
6.2.8	Статус интерфейса .....	110
6.2.9	Информация о соседях .....	111
6.2.10	Таблица маршрутизации .....	111
6.3	OSPF (Открытый кратчайший путь в первую очередь) .....	112
6.3.1	Глобальная конфигурация .....	112
6.3.2	Конфигурация сети .....	116
6.3.3	Пассивный интерфейс .....	117
6.3.4	Конфигурация зоны .....	117
6.3.5	Региональная сертификация .....	118
6.3.6	Региональный охват .....	119
6.3.7	Конфигурация интерфейса .....	120
6.3.8	Конфигурация виртуального соединения .....	121
6.3.9	Глобальный статус .....	122
6.3.10	Area статус .....	123
6.3.11	Таблица статуса соседей .....	124
6.3.12	Статус интерфейса .....	125
6.3.13	Статус маршрутизации .....	126
6.3.14	LSDB (База данных состояния связей) .....	128
6.3.14.1	LSDB .....	128
6.3.14.2	LSDB маршрутизатора .....	129
6.3.14.3	Сеть LSDB .....	130

6.3.14.4	Суммарная информация LSDB .....	131
6.3.14.5	LSDB ASBR (Автономная система граничного маршрутизатора) .....	132
6.3.14.6	Внешняя информация LSDB .....	133
6.3.14.7	Внешняя LSDB NSSA (Необъявленные автономные системы) .....	134
7	Управление безопасностью .....	136
7.1	Уровни доступа .....	136
7.2	SSH (Secure Shell - Защищенная оболочка) .....	138
7.3	HTTPS (Защищённый протокол передачи гипертекста) .....	138
7.4	Методы аутентификации .....	140
7.5	Управление доступом .....	143
7.6	SNMP (Простой протокол управления сетью) .....	144
7.6.1	Настройка SNMP .....	145
7.6.2	SNMPv1/v2c сообщество (community string) .....	145
7.6.3	Пользователи SNMPv3 .....	146
7.6.4	Группа SNMP .....	147
7.6.5	Вид SNMP (view) .....	148
7.6.6	Аутентификация SNMP .....	149
7.6.7	Ловушки SNMP (Trap) .....	150
7.6.7.1	Хост назначения .....	150
7.6.7.2	Настройки источника .....	153
7.6.8	RMON (Удаленный мониторинг) .....	154
7.6.8.1	Конфигурация группы статистики .....	154
7.6.8.2	Информация о группе статистики .....	155
7.6.8.3	Конфигурация группы истории .....	156
7.6.8.4	Информация о группе истории .....	156
7.6.8.5	Конфигурация группы оповещений .....	158
7.6.8.6	Информация о группе сигнализации .....	160
7.6.8.7	Конфигурация группы событий .....	162
7.6.8.8	Информация о группе событий .....	163

7.7	Порт безопасности .....	164
7.7.1	Конфигурация порта .....	166
7.7.2	Конфигурация MAC-адреса .....	168
7.7.3	Глобальный статус .....	168
7.7.4	Статус порта .....	171
7.8	Аутентификация портов 802.1X .....	172
7.8.1	Протокол 802.1X .....	172
7.8.1.1	Стандарт 802.1X .....	172
7.8.1.2	Принцип работы 802.1X .....	172
7.8.1.3	802.1X аутентификации .....	175
7.8.2	Конфигурация порта .....	177
7.8.3	Статус устройства .....	181
7.8.4	Статус порта .....	184
7.9	AAA-сертификация .....	187
7.9.1	AAA .....	187
7.9.1.1	Введение в AAA .....	187
7.9.1.2	AAA принцип работы .....	187
7.9.2	RADIUS .....	189
7.9.2.1	Конфигурация RADIUS .....	189
7.9.2.2	RADIUS статус .....	191
7.9.2.3	Данные RADIUS .....	192
7.9.3	TACACS+ .....	195
7.9.3.1	Конфигурация TACACS+ .....	195
7.10	Конфигурация ACL .....	196
7.10.1	Управление портом .....	196
7.10.2	Ограничение скорости .....	198
7.10.3	Контроль доступа .....	199
7.10.4	ACL статус .....	205
7.11	Защита источника IPv4 .....	205

7.11.1	Конфигурация порта.....	205
7.11.2	Статические таблицы.....	207
7.11.3	Статус.....	207
7.12	Защита источника IPv6.....	207
7.12.1	Конфигурация порта.....	208
7.12.2	Статические таблицы.....	209
7.12.3	Информация.....	209
7.13	Защита ARP.....	210
7.13.1	Конфигурация порта.....	211
7.13.2	Конфигурация VLAN.....	212
7.13.3	Статические таблицы.....	213
7.13.4	Динамическая таблица.....	213
7.13.5	Информация о фильтрации ARP.....	214
8	Продвинутые функции.....	215
8.1	QoS (Качество обслуживания).....	215
8.1.1	Классификация портов.....	215
8.1.2	Политика портов.....	217
8.1.3	Стратегия очереди.....	218
8.1.4	Расписание портов.....	220
8.1.5	Формирование порта.....	223
8.1.6	Маркировка портов.....	224
8.1.7	DSCP порто.....	225
8.1.8	DSCP-QoS.....	227
8.1.9	Отображение DSCP.....	228
8.1.10	Классификация DSCP.....	229
8.1.11	Сопоставление записей.....	230
8.1.12	Экспорт сопоставления.....	231
8.1.13	QoS список управления.....	231
8.1.14	Стратегия управления бурей (избыточного трафика).....	233

8.1.15	Статистика QoS .....	234
8.1.16	QCL статус.....	235
8.2	DDM (Мониторинг диагностических данных) .....	236
8.2.1	Конфигурация DDM .....	236
8.2.2	Обзор DDM.....	237
8.2.3	DDM детали.....	238
8.3	Ping (Проверка связи) .....	239
8.3.1	Ping (IPv4).....	239
8.3.2	Ping (IPv6).....	240
8.4	Traceroute (Трассировка) .....	241
8.4.1	Traceroute (IPv4).....	241
8.4.2	Traceroute(IPv6).....	242
8.5	PTP.....	244
8.5.1	Руководство по настройке PTP .....	245
8.5.1.1	Конфигурация внешнего источника синхронизации.....	245
8.5.1.2	Настройка часов PTP .....	246
8.5.1.3	PTP статус.....	250
8.5.1.4	802.1AS статистика .....	252
8.5.2	Пример конфигурации PTP .....	253
8.5.2.1	Конфигурация предустановленного файла 1588.....	253
8.5.2.2	Конфигурация предустановленного файла 802.1AS.....	255
8.6	TSN .....	257
8.6.1	Определение.....	257
8.6.2	802.1Qbv.....	257
8.6.3	802.1CB .....	260
8.6.4	802.1Qbu.....	260
8.6.5	802.1Qci .....	260
8.6.6	TSN Руководство по конфигурации .....	261
8.6.6.1	TSN конфигурация .....	261

8.6.6.2	Конфигурация предварительного прерывания кадра .....	262
8.6.6.3	Статус предварительного прерывания кадра .....	263
8.6.6.4	TAS конфигурация .....	264
8.6.6.5	TAS статус .....	267
8.6.6.6	PSFP конфигурация .....	267
8.6.6.7	Статус параметров потока PSFP .....	270
8.6.6.8	Статус фильтрации потока PSFP .....	270
8.6.6.9	Статистика фильтрации потока PSFP .....	270
8.6.6.10	Статус управления потоком PSFP .....	271
8.6.6.11	FRER конфигурация .....	272
8.6.6.12	FRER статус .....	272
8.6.6.13	FRER статистика .....	273
9	Управление системой.....	274
9.1	Пользователь .....	274
9.2	DHCPv4 .....	276
9.2.1	Служба DHCPv4 .....	276
9.2.1.1	Режим обслуживания .....	277
9.2.1.2	Отсутствие выделения IP-адресов .....	278
9.2.1.3	Пул адресов .....	279
9.2.1.4	Статистика.....	286
9.2.1.5	Привязать IP.....	287
9.2.1.6	Отказ в выделении IP-адреса.....	289
9.2.2	Отслеживание DHCPv4.....	289
9.2.2.1	Настройка прослушивания .....	290
9.2.2.2	Таблица прослушивания.....	291
9.2.3	Перенаправление DHCPv4.....	292
9.2.3.1	Конфигурация реле .....	294
9.2.3.2	Статистика ретрансляции .....	295
9.2.4	Детализированная статистика DHCP .....	296

9.3	NTP (Служба сетевого времени).....	298
9.4	Время.....	299
9.5	Журнал .....	301
9.5.1	Конфигурация журнала.....	301
9.5.2	Информация о журнале .....	302
9.5.3	Подробные журналы .....	303
9.6	Управление файлами конфигурации .....	304
9.6.1	Сохранить как конфигурацию при запуске.....	304
9.6.2	Скачать.....	305
9.6.3	Загрузить .....	306
9.6.4	Активация.....	307
9.6.5	Удалить.....	307
9.7	Управление зеркалированием .....	308
9.7.1	Обновление.....	308
9.7.2	Выбор .....	308
9.8	Перезагрузка.....	309
9.9	Восстановление заводских настроек.....	309

# 1 Веб-интерфейс устройства

Веб-интерфейс устройства предоставляет графический интерфейс управления для обеспечения интуитивно понятного и удобного управления и обслуживания устройства.

## 1.1 Веб-вход

IP-адрес устройства по умолчанию и информация о вошедшем в систему пользователе показаны в таблице ниже.

Параметр	Значение по умолчанию
IP-Адрес	192.168.16.253
Маска подсети	255.255.255.0
Логин	admin
Пароль	admin

При входе в веб-интерфейс устройства необходимо убедиться, что терминальный ПК и устройство находятся в одном сетевом сегменте, или маршрут доступен.



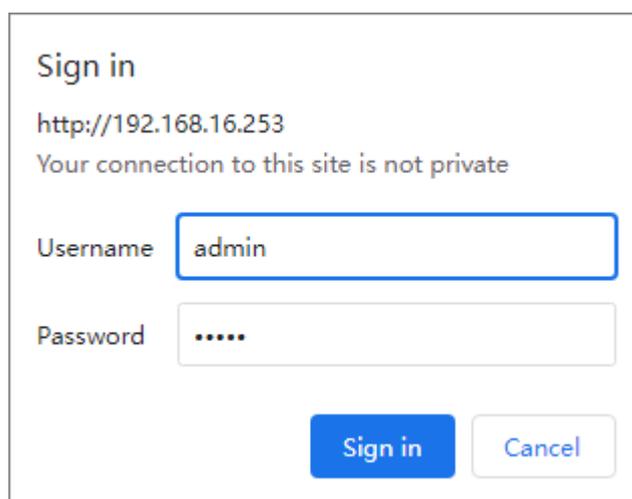
### Примечание:

- При доступе к веб-интерфейсу с терминального ПК через браузер рекомендуется использовать последнюю версию Google Chrome. Для других браузеров с ядром, таких как Internet Explorer (IE), Edge и Firefox, также рекомендуется использовать более новые версии. Например, для IE рекомендуется использовать версию 8.0 или выше.
- Если ПК и устройство находятся в разных сетевых сегментах, или маршрут недоступен, вы можете изменить IP-адрес ПК на такой, который принадлежит тому же сетевому сегменту, что и устройство, а затем подключиться к устройству напрямую. В системе Win7 для изменения IP-адреса перейдите в «Панель управления» > «Сеть и Интернет» > «Сетевые подключения» > «Локальное подключение» > «Свойства» > «Протокол интернета версии 4 (TCP/IPv4)» > «Свойства». В разделе «Использовать следующий IP-адрес» введите новый IP-адрес для вашего

ПК (например, 192.168.16.X, где X может быть любым числом от 1 до 254, кроме 253) и маску подсети (255.255.255.0).

Служба HTTP включена по умолчанию, что позволяет вам получить доступ к веб-интерфейсу с помощью этих шагов.

1. Непосредственно соедините ПК и сетевой интерфейс устройства сетевым кабелем.
2. Настройте IP-адрес ПК (например, 192.168.16.100) и маску подсети (например, 255.255.255.0) так, чтобы они находились в том же сетевом сегменте, что и устройство, для обеспечения взаимодействия.
3. Откройте браузер на ПК, введите IP-адрес устройства в адресную строку браузера, например «http://192.168.16.253», и нажмите Enter.
4. Введите имя пользователя и пароль по умолчанию на всплывающей странице входа, как показано на рисунке ниже. Имя пользователя администратора по умолчанию и



Sign in

http://192.168.16.253

Your connection to this site is not private

Username

Password

пароль устройства — оба «admin».

5. Нажмите кнопку «Войти», чтобы перейти на WEB-страницу.

## 1.2 Общие кнопки в веб-интерфейсе

Часто используемые кнопки и значки показаны на рисунке ниже

Button	Description
	Вернуться на главную страницу
	Выйти
Auto-refresh <input type="checkbox"/>	Автоматическое обновление
Port 1 ▾	Выбрать порт
Refresh	Обновить
Clear	Очистить статистику
Save	Сохранить
Reset	Отменить
Remove All	Удалить
Add New Entry	Добавить
<<	Главная страница списка
<<	Предыдущая страница
>>	Следующая страница
>>	Последняя страница
	Добавить
	Редактировать
	Удалить
	Переместить вверх
	Переместить вниз

## 1.3 Выйти из веб-интерфейса

Для выхода из веб-интерфейса управления сетью нажмите на значок выхода  « в верхнем правом углу.

 Важно:

Автоматический выход: Если пользователь в течение длительного времени не выполняет действий на странице настройки веб-интерфейса управления сетью (по умолчанию 10 минут), система автоматически завершит сеанс из-за истечения времени ожидания и вернется на страницу входа. Для продолжения работы после автоматического выхода необходимо выполнить повторный вход в систему.

Сохранение настроек: При выходе из веб-интерфейса управления сетью система не сохраняет текущие настройки автоматически. Во избежание потери несохраненных настроек после перезагрузки устройства рекомендуется сохранять текущую конфигурацию перед выходом из веб-интерфейса.

Сохранение конфигурации: В разделе «Управление системой» > «Управление файлами конфигурации» > «Сохранить как конфигурацию запуска» нажмите кнопку «Сохранить конфигурацию» для сохранения текущего файла конфигурации.

## 2 Системная информация

### 2.1 Системная информация

Страница системной информации отображает контактное лицо коммутатора, имя устройства, расположение, MAC-адрес, системное время, время запуска системы, дату выпуска программного обеспечения и версию кода, как показано на рисунке ниже.

System Information	
Auto-refresh <input type="checkbox"/> Refresh	
System	
Contact	
Name	
Location	
Hardware	
MAC Address	4c-93-a6-c4-14-c0
Time	
System Date	2023-06-30T15:03:24+00:00
System Uptime	0d 00:13:54
Software	
Software Date	2023-06-30T14:49:33+08:00
Code Revision	5b9eb29

Описание каждого элемента показано в таблице:

Параметр	Описание
System	<p>Отображение информации о системе устройства:</p> <ul style="list-style-type: none"> <li>• Контакт: контактная информация устройства.</li> <li>• Имя устройства: модель или имя устройства.</li> <li>• Расположение: информация о географическом положении устройства.</li> </ul> <p>Иллюстрация: В разделе «Сведения о системе» &gt; «Конфигурация системы» можно задать сведения о системе.</p>
Hardware	<p>Отображение информации об оборудовании устройства:</p> <ul style="list-style-type: none"> <li>• MAC-адрес: Физический MAC-адрес данного устройства.</li> </ul>
Time	<p>Отображение информации о времени устройства:</p> <ul style="list-style-type: none"> <li>• Системное время: текущая дата системы, время, часовой пояс и другая информация.</li> <li>• Время запуска системы: сколько времени требуется системе для работы после этого запуска.</li> </ul>

Software	<p>Отображение информации о программном обеспечении устройства:</p> <ul style="list-style-type: none"> <li>Дата выпуска программного обеспечения: дата изготовления программного обеспечения данного устройства.</li> <li>Версия кода: идентификатор управления версиями программного обеспечения коммутатора.</li> </ul>
----------	---

## 2.2 Статус порта

Страница состояния портов отображает информацию о состоянии портов коммутатора и информацию о сопоставлении имен портов, как показано ниже.

**Port State Overview** Auto-refresh  Refresh



**Interface Name to Port Number Map**

Interface Name	Port Number
Gi 1/1	1
Gi 1/2	2
Gi 1/3	3
Gi 1/4	4
Gi 1/5	5
Gi 1/6	6
Gi 1/7	7
Gi 1/8	8
Gi 1/9	9
Gi 1/10	10
Gi 1/11	11
Gi 1/12	12
Gi 1/13	13
Gi 1/14	14
Gi 1/15	15
Gi 1/16	16
Gi 1/17	17
Gi 1/18	18
Gi 1/19	19
Gi 1/20	20
Gi 1/21	21
Gi 1/22	22
Gi 1/23	23
Gi 1/24	24
Gi 1/25	25
Gi 1/26	26
Gi 1/27	27
Gi 1/28	28
Gi 1/29	29
Gi 1/30	30
Gi 1/31	31
Gi 1/32	32
10G 1/1	33
10G 1/2	34
10G 1/3	35
10G 1/4	36

Таблица ниже описывает каждый элемент параметров

Параметр	Описание
Port status	<p>Значок состояния порта выглядит следующим образом:</p> <ul style="list-style-type: none"> <li>RJ45 статус порта: <ul style="list-style-type: none"> <li>: Черный указывает на то, что порт не установил действующее соединение.</li> <li>: Зеленый указывает на то, что порт установил</li> </ul> </li> </ul>

Параметр	Описание
	<p>действующее соединение.</p> <ul style="list-style-type: none"> <li>◆ : Серый указывает на то, что порт отключен, и соединение невозможно.</li> <li>• SFP статус порта:                             <ul style="list-style-type: none"> <li>◆ : Черный указывает на то, что порт не установил действующее соединение</li> <li>◆ : Зеленый указывает на то, что порт установил действующее соединение.</li> <li>◆ : Серый указывает на то, что порт отключен, и соединение невозможно.</li> </ul> </li> </ul>
Параметр	Описание
Имя порта	Имя, соответствующее физическому порту.
Номер порта	Физический номер порта.

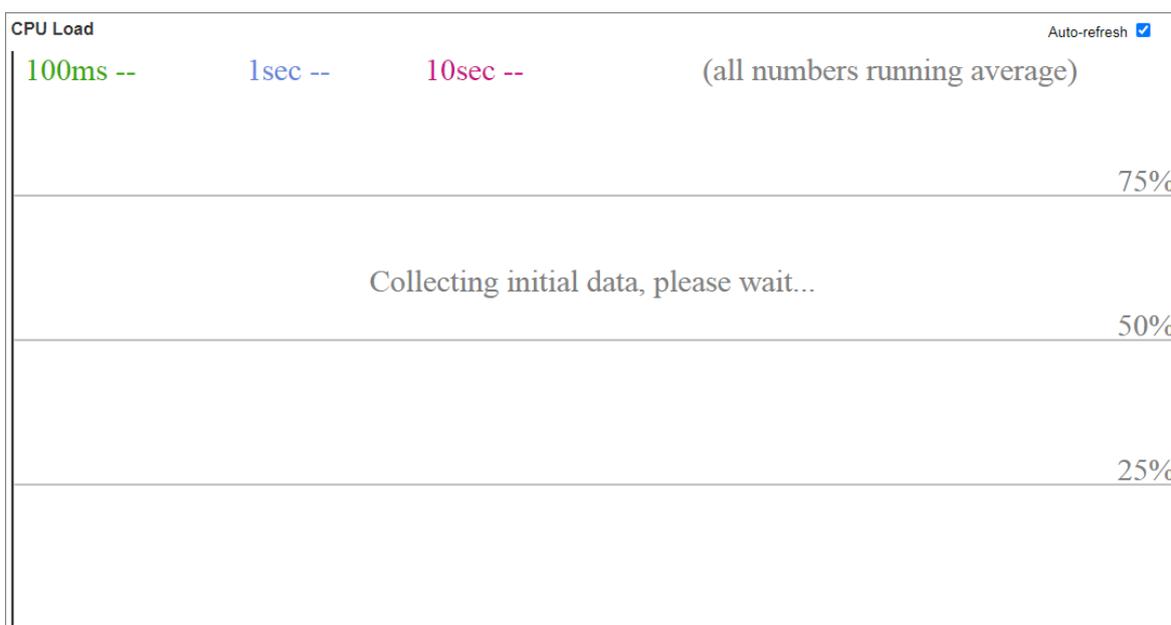
### Подробная статистика порта

Щелкните на порту Ethernet, чтобы просмотреть статистику различных типов кадров данных, полученных и отправленных портом, таких как кадры одноадресной передачи (unicast frames), кадры многоадресной передачи (multicast frames), кадры широковещательной передачи (broadcast frames), кадры различной длины в байтах, кадры из различных очередей, кадры с ошибками и т. Д. Для получения дополнительной информации см. главу «Конфигурация портов» Статистика портов».

Receive Total		Transmit Total	
Rx Packets	36771	Tx Packets	1425
Rx Octets	2826225	Tx Octets	770492
Rx Unicast	1223	Tx Unicast	1404
Rx Multicast	5211	Tx Multicast	13
Rx Broadcast	30240	Tx Broadcast	8
Rx Pause	0	Tx Pause	0
Receive Size Counters		Transmit Size Counters	
Rx 64 Bytes	29764	Tx 64 Bytes	450
Rx 65-127 Bytes	6077	Tx 65-127 Bytes	88
Rx 128-255 Bytes	322	Tx 128-255 Bytes	8
Rx 256-511 Bytes	235	Tx 256-511 Bytes	442
Rx 512-1023 Bytes	373	Tx 512-1023 Bytes	82
Rx 1024-1518 Bytes	0	Tx 1024-1518 Bytes	355
Rx 1519- Bytes	0	Tx 1519- Bytes	0
Receive Queue Counters		Transmit Queue Counters	
Rx Q0	36674	Tx Q0	1418
Rx Q1	0	Tx Q1	0
Rx Q2	0	Tx Q2	0
Rx Q3	0	Tx Q3	0
Rx Q4	0	Tx Q4	0
Rx Q5	0	Tx Q5	0
Rx Q6	0	Tx Q6	0
Rx Q7	0	Tx Q7	7
Receive Error Counters		Transmit Error Counters	
Rx Drops	0	Tx Drops	0
Rx CRC/Alignment	97	Tx Late/Exc. Coll.	0
Rx Undersize	0		
Rx Oversize	0		
Rx Fragments	0		
Rx Jabber	0		
Rx Filtered	5294		

## 2.3 Загрузка ЦПУ

Эта страница отображает информацию о нагрузке на центральный процессор коммутатора в виде рисунка SVG. Как показано ниже. Для нормального отображения элементов SVG необходимо убедиться, что ваш браузер поддерживает формат SVG. За конкретными решениями проблем с отображением обращайтесь к SVG Wiki.



## 2.4 Системные настройки

Ниже показана страница конфигурации системной информации. Она используется для настройки контактного лица, имени системы и местоположения коммутатора. Эти параметры соответствуют информации узлов sysContact, sysName и sysLocation в таблице MIB SNMP.

**System Information Configuration**

<b>System Contact</b>	<input type="text"/>
<b>System Name</b>	<input type="text"/>
<b>System Location</b>	<input type="text"/>

Таблица ниже описывает каждый элемент параметров:

Параметр	Описание
System contact	Информация о контактном лице устройства. Длина строки контактной информации системы составляет 0~255 байт и может включать все печатаемые символы с клавиатуры с кодами ASCII 32~126.
System name	Хостнейм устройства. Изменение имени системы также приведет к изменению командной строки. Строка имени системы может содержать строчные и заглавные буквы английского алфавита (A-Z, a-z), цифры (0-9) и дефисы (-). Не может содержать пробелы. Должно начинаться с буквы, и первый и последний символы не могут быть дефисами. Длина строки имени системы составляет 0~255 байт.
System location	Информация о физическом местоположении устройства. Длина строки местоположения системы составляет 0~255 байт и может включать все печатаемые символы с клавиатуры с кодами ASCII 32~126.

## 3 Конфигурация портов

### 3.1 Конфигурация портов

Функция конфигурации портов используется для настройки и отображения скорости, дуплекса, управления потоком, кадров Jumbo и т. Д. порта. Как показано ниже.

Port Configuration																	Refresh			
Port	Link	Warning	Current	Speed Configured	Adv Duplex		Adv speed					Flow Control			Maximum Frame Size	Excessive Collision Mode	Frame Length Check	FEC Mode		
					Fdx	Hdx	10M	100M	1G	2.5G	5G	10G	Enable	Curr Rx					Curr Tx	
1	<span style="color: green;">●</span>		100fdx	Automatic	<input checked="" type="checkbox"/>	<input type="checkbox"/>	10240	Discard	<input type="checkbox"/>	<>										
2	<span style="color: red;">●</span>	Down	Down	Automatic	<input checked="" type="checkbox"/>	<input type="checkbox"/>	10240	Discard	<input type="checkbox"/>	<>										
3	<span style="color: red;">●</span>	Down	Down	Automatic	<input checked="" type="checkbox"/>	<input type="checkbox"/>	10240	Discard	<input type="checkbox"/>	<>										
4	<span style="color: red;">●</span>	Down	Down	Automatic	<input checked="" type="checkbox"/>	<input type="checkbox"/>	10240	Discard	<input type="checkbox"/>	<>										
5	<span style="color: red;">●</span>	Down	Down	Automatic	<input checked="" type="checkbox"/>	<input type="checkbox"/>	10240	Discard	<input type="checkbox"/>	<>										
6	<span style="color: red;">●</span>	Down	Down	Automatic	<input checked="" type="checkbox"/>	<input type="checkbox"/>	10240	Discard	<input type="checkbox"/>	<>										
7	<span style="color: red;">●</span>	Down	Down	Automatic	<input checked="" type="checkbox"/>	<input type="checkbox"/>	10240	Discard	<input type="checkbox"/>	<>										
8	<span style="color: red;">●</span>	Down	Down	Automatic	<input checked="" type="checkbox"/>	<input type="checkbox"/>	10240	Discard	<input type="checkbox"/>	<>										
9	<span style="color: red;">●</span>	Down	Down	Automatic	<input checked="" type="checkbox"/>	<input type="checkbox"/>	10240	Discard	<input type="checkbox"/>	<>										
10	<span style="color: red;">●</span>	Down	Down	Automatic	<input checked="" type="checkbox"/>	<input type="checkbox"/>	10240	Discard	<input type="checkbox"/>	<>										
11	<span style="color: red;">●</span>	Down	Down	Automatic	<input checked="" type="checkbox"/>	<input type="checkbox"/>	10240	Discard	<input type="checkbox"/>	<>										
12	<span style="color: red;">●</span>	Down	Down	Automatic	<input checked="" type="checkbox"/>	<input type="checkbox"/>	10240	Discard	<input type="checkbox"/>	<>										
13	<span style="color: red;">●</span>	Down	Down	Automatic	<input checked="" type="checkbox"/>	<input type="checkbox"/>	10240	Discard	<input type="checkbox"/>	<>										
14	<span style="color: red;">●</span>	Down	Down	Automatic	<input checked="" type="checkbox"/>	<input type="checkbox"/>	10240	Discard	<input type="checkbox"/>	<>										
15	<span style="color: red;">●</span>	Down	Down	Automatic	<input checked="" type="checkbox"/>	<input type="checkbox"/>	10240	Discard	<input type="checkbox"/>	<>										
16	<span style="color: red;">●</span>	Down	Down	Automatic	<input checked="" type="checkbox"/>	<input type="checkbox"/>	10240	Discard	<input type="checkbox"/>	<>										
17	<span style="color: red;">●</span>	Down	Down	Automatic	<input checked="" type="checkbox"/>	<input type="checkbox"/>	10240	Discard	<input type="checkbox"/>	<>										
18	<span style="color: red;">●</span>	Down	Down	Automatic	<input checked="" type="checkbox"/>	<input type="checkbox"/>	10240	Discard	<input type="checkbox"/>	<>										
19	<span style="color: red;">●</span>	Down	Down	Automatic	<input checked="" type="checkbox"/>	<input type="checkbox"/>	10240	Discard	<input type="checkbox"/>	<>										
20	<span style="color: red;">●</span>	Down	Down	Automatic	<input checked="" type="checkbox"/>	<input type="checkbox"/>	10240	Discard	<input type="checkbox"/>	<>										
21	<span style="color: red;">●</span>	Down	Down	Automatic	<input checked="" type="checkbox"/>	<input type="checkbox"/>	10240	Discard	<input type="checkbox"/>	<>										
22	<span style="color: red;">●</span>	Down	Down	Automatic	<input checked="" type="checkbox"/>	<input type="checkbox"/>	10240	Discard	<input type="checkbox"/>	<>										
23	<span style="color: red;">●</span>	Down	Down	Automatic	<input checked="" type="checkbox"/>	<input type="checkbox"/>	10240	Discard	<input type="checkbox"/>	<>										
24	<span style="color: red;">●</span>	Down	Down	Automatic	<input checked="" type="checkbox"/>	<input type="checkbox"/>	10240	Discard	<input type="checkbox"/>	<>										
25	<span style="color: red;">●</span>	Down	Down	Automatic	<input checked="" type="checkbox"/>	<input type="checkbox"/>	10240	Discard	<input type="checkbox"/>	<>										
26	<span style="color: red;">●</span>	Down	Down	Automatic	<input checked="" type="checkbox"/>	<input type="checkbox"/>	10240	Discard	<input type="checkbox"/>	<>										
27	<span style="color: red;">●</span>	Down	Down	Automatic	<input checked="" type="checkbox"/>	<input type="checkbox"/>	10240	Discard	<input type="checkbox"/>	<>										
28	<span style="color: red;">●</span>	Down	Down	Automatic	<input checked="" type="checkbox"/>	<input type="checkbox"/>	10240	Discard	<input type="checkbox"/>	<>										
29	<span style="color: red;">●</span>	Down	Down	Automatic	<input checked="" type="checkbox"/>	<input type="checkbox"/>	10240	Discard	<input type="checkbox"/>	<>										
30	<span style="color: red;">●</span>	Down	Down	Automatic	<input checked="" type="checkbox"/>	<input type="checkbox"/>	10240	Discard	<input type="checkbox"/>	<>										
31	<span style="color: red;">●</span>	Down	Down	Automatic	<input checked="" type="checkbox"/>	<input type="checkbox"/>	10240	Discard	<input type="checkbox"/>	<>										
32	<span style="color: red;">●</span>	Down	Down	Automatic	<input checked="" type="checkbox"/>	<input type="checkbox"/>	10240	Discard	<input type="checkbox"/>	<>										
33	<span style="color: red;">●</span>	Down	Down	Automatic	<input checked="" type="checkbox"/>	<input type="checkbox"/>	10240	Discard	<input type="checkbox"/>	auto										
34	<span style="color: red;">●</span>	Down	Down	Automatic	<input checked="" type="checkbox"/>	<input type="checkbox"/>	10240	Discard	<input type="checkbox"/>	auto										
35	<span style="color: red;">●</span>	Down	Down	Automatic	<input checked="" type="checkbox"/>	<input type="checkbox"/>	10240	Discard	<input type="checkbox"/>	auto										
36	<span style="color: red;">●</span>	Down	Down	Automatic	<input checked="" type="checkbox"/>	<input type="checkbox"/>	10240	Discard	<input type="checkbox"/>	auto										

Таблица ниже описывает каждый элемент параметров:

Параметр	Описание
Port	Номер физического порта на коммутаторе.
Connection Status	Зеленый: Порт подключен и работает. Красный: Порт отключен.
Alarm	Сигнал тревоги: <ul style="list-style-type: none"> <li>Серый: нет тревоги для данного порта.</li> <li>Желтый: на порту есть тревога. Для просмотра информации о тревоге наведите курсор мыши на индикатор.</li> </ul>
Rate	Текущая скорость: отображает текущую скорость подключения порта.

Параметр	Описание
	<ul style="list-style-type: none"> <li>• HDX (Half Duplex) – Полудуплексный режим. FDX (Full Duplex) – Полный дуплексный режим.</li> <li>• Настройка скорости: позволяет выбрать режим скорости и дуплекса для порта. Доступны только те варианты, которые поддерживает порт. Значение по умолчанию – автоматическое согласование.</li> </ul> <p>Доступные варианты скорости-дуплекса:</p> <ul style="list-style-type: none"> <li>• Disable (Отключить): Отключить порт коммутатора.</li> <li>• Auto-negotiation (Автоматическое согласование): Автоматически согласовать скорость и дуплекс с подключенным устройством, выбрав максимально возможную скорость, которую поддерживает оба устройства</li> <li>• 10Mbps half-duplex (10 Мбит/с, полудуплекс)</li> <li>• 10Mbps full-duplex (10 Мбит/с, полный дуплекс)</li> <li>• 100Mbps half-duplex (100 Мбит/с, полудуплекс)</li> <li>• 100Mbps full-duplex (100 Мбит/с, полный дуплекс)</li> <li>• 1Gbps full-duplex (1 Гбит/с, полный дуплекс)</li> <li>• 2.5Gbps full-duplex (2.5 Гбит/с, полный дуплекс)</li> <li>• 5Gbps full-duplex (5 Гбит/с, полный дуплекс)</li> <li>• 10Gbps full-duplex (10 Гбит/с, полный дуплекс)</li> </ul>
Duplex mode	<p>Рекламирование возможностей дуплекса партнерам по соединению Эта функция позволяет коммутатору сообщать подключенным устройствам о режимах дуплекса, которые он поддерживает.</p> <ul style="list-style-type: none"> <li>• Полудуплекс (Half-duplex): отметьте этот флажок, чтобы указать, что порт может работать в полудуплексном режиме.</li> <li>• Полный дуплекс (Full duplex): отметьте этот флажок, чтобы указать, что порт может работать в полнодуплексном режиме.</li> </ul>
Rate mode	<p>Рекламирование возможностей скорости партнерам по соединению Эта функция позволяет коммутатору информировать подключенные устройства о скоростях передачи данных, которые он поддерживает.</p> <ul style="list-style-type: none"> <li>• 10M: отметьте этот флажок, чтобы указать, что порт может работать на скорости 10 Мбит/с.</li> <li>• 100M: отметьте этот флажок, чтобы указать, что порт может работать на скорости 100 Мбит/с.</li> </ul>

Параметр	Описание
	<ul style="list-style-type: none"> <li>• 1G: отметьте этот флажок, чтобы указать, что порт может работать на скорости 1 Гбит/с.</li> <li>• 2.5G: отметьте этот флажок, чтобы указать, что порт может работать на скорости 2.5 Гбит/с.</li> <li>• 5G: отметьте этот флажок, чтобы указать, что порт может работать на скорости 5 Гбит/с.</li> <li>• 10G: отметьте этот флажок, чтобы указать, что порт может работать на скорости 10 Гбит/с.</li> </ul>
Flow control	<p>Управление потоком на порту коммутатора. Функция управления потоком позволяет контролировать скорость передачи данных между устройствами, подключенными к порту, чтобы избежать переполнения буфера.</p> <ul style="list-style-type: none"> <li>• Включить (Enable): отметьте этот флажок, чтобы включить функцию управления потоком на порту.</li> <li>• Прием управляющих кадров (Receive flow control frames):                      ✓ : Порт может принимать кадры паузы (pause frames) для управления потоком. ✗ : Порт не может принимать кадры паузы для управления потоком.</li> <li>• Отправка управляющих кадров (Sending flow control frames):                      ✓ : Порт может отправлять кадры паузы для управления потоком. ✗ : Порт не может отправлять кадры паузы для управления потоком.</li> </ul>
Maximum frame length	<p>Максимальная длина кадров – это максимальный размер блока данных, который порт коммутатора может передать по сети.                      Значение для данного порта: 1518-10240 байт</p>
Excessive conflict handling mode	<p>Режим обработки коллизий определяет, как порт коммутатора будет реагировать на возникновение коллизий.</p> <ul style="list-style-type: none"> <li>• Отбросить (Discard): (Значение по умолчанию) после 16 попыток передачи с коллизией, порт отбрасывает кадр.</li> <li>• Перезапустить (Restart): после 16 попыток передачи с коллизией, порт перезапускает алгоритм отсрочки передачи (backoff algorithm).</li> </ul>
Frame length detection	<p>Установка этого флажка означает, что функция обнаружения длины кадров настроена; в противном случае функция обнаружения длины кадров не настроена.</p>
FEC mode	<p>FEC (Forward Error Correction) – это технология коррекции ошибок, которая позволяет обнаруживать и исправлять ошибки передачи данных в сети.</p>

Параметр	Описание
	<ul style="list-style-type: none"> <li>• Auto (Автоматически): (Значение по умолчанию) порт автоматически подстраивается под режим коррекции ошибок устройства, подключенного к нему.</li> <li>• Поддержка r-FEC (Support r-fec): включает режим коррекции ошибок r-FEC на порту.</li> <li>• Выкл. (Close): режим коррекции ошибок на порту отключен.</li> </ul>



**Замечания по настройке портов:**

Применение настроек: Параметры, указанные в первом столбце, будут применены ко всем портам, если не выбраны конкретные порты.

Сохранение настроек: после внесения изменений в конфигурацию портов, необходимо нажать кнопку «Сохранить (Save)» для их применения.

Отмена изменений: если вы внесли изменения в конфигурацию портов, но не сохранили их, то можете отменить изменения, нажав кнопку «Сброс (Reset)».

Обновление информации: для просмотра актуального состояния портов необходимо нажать кнопку «Обновить (Refresh)».

## 3.2 Имя порта

Соответствующее имя физического порта показано ниже:

**Interface Name to Port Number Map**

Interface Name	Port Number
Gi 1/1	1
Gi 1/2	2
Gi 1/3	3
Gi 1/4	4
Gi 1/5	5
Gi 1/6	6
Gi 1/7	7
Gi 1/8	8
Gi 1/9	9
Gi 1/10	10
Gi 1/11	11
Gi 1/12	12
Gi 1/13	13
Gi 1/14	14
Gi 1/15	15
Gi 1/16	16
Gi 1/17	17
Gi 1/18	18
Gi 1/19	19
Gi 1/20	20
Gi 1/21	21
Gi 1/22	22
Gi 1/23	23
Gi 1/24	24
Gi 1/25	25
Gi 1/26	26
Gi 1/27	27
Gi 1/28	28
Gi 1/29	29
Gi 1/30	30
Gi 1/31	31
Gi 1/32	32
10G 1/1	33
10G 1/2	34
10G 1/3	35
10G 1/4	36

Таблица ниже описывает каждый элемент параметров:

Параметр	Описание
Port name	Имя, соответствующее физическому порту
Port number	Физический номер порта.

### 3.3 Агрегация портов

#### 3.3.1 Конфигурация группы агрегации

Страница конфигурации группы агрегации показана ниже.



Параметр	Описание
	другим устройством, порт переходит в состояние расчета протокола.
Aggregation group configuration-reverse	<p>Этот параметр применяется только к группам агрегации с поддержкой LACP (Link Aggregation Control Protocol – протокол агрегации каналов). Включение функции резервирования (Rollover) позволяет сохранить за портом-участником группы агрегации с более высоким приоритетом статус активного порта.</p> <p>Например: порт с высоким приоритетом может перейти в неактивное состояние из-за отказа (failover). После восстановления работоспособности порта, если функция резервирования включена, порт с высоким приоритетом сможет повторно согласовать свое состояние и снова стать активным портом в группе. И наоборот: если функция резервирования отключена, то порт с высоким приоритетом после восстановления не сможет стать активным и останется неактивным.</p>
Aggregation group configuration-max. number of active ports	Этот параметр применяется только к группам агрегации с поддержкой LACP. Он определяет максимальное разрешенное количество активных объединенных портов LACP в агрегации.

### 3.3.2 Режим балансировки нагрузки

Страница конфигурации режима балансировки нагрузки показана ниже.

**Common Aggregation Configuration**

**Hash Code Contributors**

Source MAC Address

Destination MAC Address

IP Address

TCP/UDP Port Number

Save Reset

Таблица ниже описывает каждый элемент параметров:

Параметр	Описание
Source MAC address	MAC-адрес источника можно использовать для вычисления MAC-адреса источника кадра. Установите флажок, чтобы включить его; снимите флажок, чтобы отключить его. По умолчанию MAC-адрес источника включен.

Параметр	Описание
Destination MAC address	MAC-адрес назначения можно использовать для расчета MAC-адреса назначения кадра. По умолчанию MAC-адрес назначения отключен.
IP address	IP-адрес можно использовать для расчета IP-адресов источника и назначения кадра. По умолчанию IP-адреса включены.
TCP/UDP port number	Номер порта TCP/UDP можно использовать для расчета номеров портов TCP/UDP источника и назначения кадра. По умолчанию номера портов TCP/UDP включены.

### 3.3.3 Статус группы агрегации

Эта страница предназначена для просмотра состояния портов, объединенных в группы агрегации. Информация отображается в таблице, как показано ниже.

Aggregation Status						Auto-refresh <input type="checkbox"/>	Refresh
Aggr ID	Name	Type	Speed	Configured Ports	Aggregated Ports		
No aggregation groups							

Таблица ниже описывает каждый элемент параметров:

Параметр	Описание
Group ID	Уникальный идентификатор данного экземпляра агрегации.
Group name	Имя группы агрегации.
Type	Тип группы агрегации (статическая или LACP).
Rate	Общая скорость агрегации группы.
Configure member ports	Список портов, входящих в группу агрегации.
Aggregate member port	Отдельный порт-участник группы агрегации.

### 3.3.4 LACP

#### 3.3.4.1 LACP конфигурация

Эта страница позволяет пользователям проверить текущую конфигурацию портов LACP, как показано на рисунке ниже.

**LACP System Configuration**

System Priority

**LACP Port Configuration**

Port	LACP	Timeout	Prio
*		<> ▼	32768
1	No	Fast ▼	32768
2	No	Fast ▼	32768
3	No	Fast ▼	32768
4	No	Fast ▼	32768
5	No	Fast ▼	32768
6	No	Fast ▼	32768
7	No	Fast ▼	32768
8	No	Fast ▼	32768
9	No	Fast ▼	32768
10	No	Fast ▼	32768
11	No	Fast ▼	32768
12	No	Fast ▼	32768
13	No	Fast ▼	32768
14	No	Fast ▼	32768
15	No	Fast ▼	32768

Таблица ниже описывает каждый элемент параметров:

Параметр	Описание
<b>LACP system configuration</b>	<b>Настройка LACP системы</b>
System priority	<p>Для определения приоритета устройств на обоих концах агрегации портов, сторона с более высоким приоритетом становится активной стороной LACP. Чем меньше значение, тем выше приоритет.</p> <p>По умолчанию системный приоритет равен 32768. Если системные приоритеты совпадают, то в качестве активной стороны выбирается сторона с меньшим MAC-адресом.</p>
<b>LACP port configuration</b>	<b>Конфигурация LACP порта</b>
Port	Номер порта устройства
LACP	Отображает, включен ли в настоящее время протокол LACP на порту устройства
Timeout mode	<p>Настройте период ожидания для порта для получения сообщений LACP. Если локальный активный порт не получает сообщение протокола LACP, отправленное партнером, в установленный период ожидания, партнер считается недоступным, и активный порт выходит из работы.</p> <ul style="list-style-type: none"> <li>Быстрый: Локальный порт получает пакеты LACP раз в секунду, а таймаут составляет 3 секунды.</li> <li>Медленный: Локальный порт получает пакеты LACP раз в 30 секунд, а таймаут составляет 90</li> </ul>

Параметр	Описание
	секунд.
Port priority	Приоритет порта используется для различения приоритетов различных портов при выборе активных портов. Чем меньше значение, тем выше приоритет. По умолчанию приоритет порта составляет 32768.

### 3.3.4.2 Состояние системы

Эта страница предоставляет обзор состояния информации LACP на системном уровне. Подробности отображены в таблице ниже.

**LACP System Status** Auto-refresh  Refresh

**Local System ID**

Priority	MAC Address
32768	4c-93-a6-c4-14-c0

**Partner System Status**

Aggr ID	Partner System ID	Partner Prio	Partner Key	Last Changed	Local Ports
<i>No ports enabled or no existing partners</i>					

Таблица ниже описывает каждый элемент параметров:

Параметр	Описание
<b>Local system ID</b>	Локальный идентификатор системы
Priority	Приоритет локальной системы
MAC address	MAC-адрес локальной системы
<b>Peer system status</b>	Статус пирингового соединения
Group ID	Агрегатный идентификатор, связанный с этим экземпляром агрегата
Peer system ID	Идентификатор (MAC-адрес) устройства-партнера
Peer priority	Приоритет системы устройства-партнера
Peer key	Ключ устройства-партнера совпадает с идентификатором агрегации
Last change time	Время с момента последнего изменения этой агрегации
Local port number	Показывает, какие порты являются частью агрегации этого устройства

### 3.3.4.3 Статус локального порта

Эта страница предоставляет обзор состояния внутренних (то есть локальной системы) портов LACP. Отображаются только порты, входящие в группу LACP. Подробности представлены в таблице ниже.

LACP Internal Port Status											Auto-refresh <input type="checkbox"/>	Refresh
Port	State	Key	Priority	Activity	Timeout	Aggregation	Synchronization	Collecting	Distributing	Defaulted	Expired	
No LACP ports enabled												

Таблица ниже описывает каждый элемент параметров:

Параметр	Описание
Port	Номер порта.
Port status	Текущий статус порта. <ul style="list-style-type: none"> <li>Неактивный: указывает, что порт неактивен.</li> <li>Активный: указывает, что порт активен.</li> <li>Резервный: указывает, что порт находится в режиме ожидания.</li> </ul>
Key	Идентификатор агрегации этого порта. Только порты с тем же ключом на том же устройстве могут участвовать в агрегации.
Priority	Приоритет порта.
Master-slave state	Статус мастер-слейв порта в состоянии связи, значение - Активный или Пассивный.
Timeout mode	Режим тайм-аута для конфигурации порта (быстрый или медленный).
Aggregation ability	Указывает на возможность агрегации порта. <ul style="list-style-type: none"> <li>Да: указывает, что соединение можно агрегировать.</li> <li>Нет: указывает, что соединение является независимым и не может быть агрегировано.</li> </ul>
Whether to aggregate	Указывает, завершена ли текущая агрегация порта. <ul style="list-style-type: none"> <li>Да: указывает, что отправляемое соединение находится в состоянии IN_SYNC, то есть порт был назначен в правильную группу агрегации.</li> <li>Нет: указывает, что соединение находится в состоянии OUT_OF_SYNC, то есть порт не выбран в правильную группу агрегации.</li> </ul>
Package receiving status	Да означает, что текущая сборка пакетов для соединения включена, в противном случае - Нет.
Contract delivery status	Да означает, что отправка пакетов включена для текущего соединения, в противном случае - Нет.
Default state	Да означает, что информация о партнере, используемая этим концом, поступает из значения по умолчанию, настроенного администратором. "Нет" указывает на то, что информация о партнере, используемая локальным концом, поступает из полученного LACPDU.

Параметр	Описание
Timeout status	Да означает, что локальный автомат состояний приема пакетов находится в состоянии тайм-аута, "Нет" означает, что он не находится в состоянии тайм-аута.

### 3.3.4.4 Статус пирингового порта

Эта страница предоставляет обзор статуса всех портов партнеров LACP. Отображаются только порты, которые являются частью группы LACP. Как показано ниже:

LACP Neighbor Port Status														Auto-refresh <input type="checkbox"/>	Refresh
Port	State	Aggr ID	Partner Key	Partner Port	Partner Port Prio	Activity	Timeout	Aggregation	Synchronization	Collecting	Distributing	Defaulted	Expired		
No LACP neighbor status available															

Таблица ниже описывает каждый элемент параметров:

Параметр	Описание
Port	Номер порта.
State	Current port status. <ul style="list-style-type: none"> <li>Неактивный: указывает, что порт неактивен.</li> <li>Активный: указывает, что порт активен.</li> <li>Резервный: указывает, что порт находится в режиме ожидания</li> </ul>
Group ID	Идентификатор группы агрегации, назначенный порту.
Peer Key	Идентификатор агрегации порта партнера.
Peer port	Порт партнера, поддерживаемый портом устройства-партнера, фактически является локальным номером порта.
Peer port priority	Приоритет порта устройства-партнера.
Master-slave state	Статус мастер-слейв порта партнера в состоянии связи, значение - Active или Passive.
Timeout mode	Режим тайм-аута для конфигурации порта (быстрый или медленный).
Aggregation ability	Указывает на возможность агрегации порта партнера. <ul style="list-style-type: none"> <li>Да: указывает на возможность агрегации соединения.</li> <li>Нет: указывает на то, что соединение является независимым и не может быть агрегировано.</li> </ul>
Whether to aggregate	Указывает, завершена ли текущая агрегация порта партнера.

Параметр	Описание
	<ul style="list-style-type: none"> <li>Да: указывает, что отправляемое соединение находится в состоянии IN_SYNC, то есть порт был назначен правильной группе агрегации.</li> <li>Нет: указывает, что соединение находится в состоянии OUT_OF_SYNC, то есть порт не выбран в правильную группу агрегации.</li> </ul>
Package receiving status	"Yes" означает, что текущая передача пакетов с порта устройства-партнера включена, в противном случае - "Нет".
Contract delivery status	"Yes" означает, что текущая передача пакетов на порт устройства-партнера включена, в противном случае - "Нет".
Default state	"Yes" означает, что локальная информация, используемая устройством-партнером, поступает из значения по умолчанию, настроенного администратором. "Нет" указывает на то, что локальная информация, используемая устройством-партнером, поступает из полученного LACPDU.
Timeout status	"Yes" означает, что машина состояний приема пакетов устройства-партнера находится в состоянии ожидания истечения времени, а "Нет" означает, что она не находится в состоянии ожидания истечения времени.

### 3.3.4.5 Статистика кадров LACP

Эта страница предоставляет обзор статистики LACP для всех портов. Как показано ниже:

**LACP Statistics** Auto-refresh

Port	LACP Received	LACP Transmitted	Discarded	
			Unknown	Illegal
<i>No ports enabled</i>				

Таблица ниже описывает каждый элемент параметров:

Параметр	Описание
Port	Номер порта.
Number of LACP frames received	Показывает, сколько LACP-кадров получил каждый порт.
Number of LACP frames sent	Показывает, сколько LACP-кадров было отправлено с каждого порта.
Number of dropped frames	Показывает, сколько неизвестных или недопустимых LACP-кадров было отброшено на каждом порту.

## 3.4 Зеркальное отображение портов

Это используется для просмотра и настройки функции зеркалирования портов.

### Таблица конфигурации зеркала

Функция зеркалирования портов. Как показано ниже.

Mirror Configuration Table		
Session ID	Mode	Type
<a href="#">1</a>	Disabled	Local Mirror

Таблица ниже описывает каждый элемент параметров

Параметр	Описание
Mirror group ID	Номер группы зеркалирования. Нажмите на номер, чтобы перейти на страницу конфигурации.
Mode	Статус включения группы зеркалирования, включен/отключен.
Type	<p>Тип зеркалирования.</p> <ul style="list-style-type: none"> <li>Локальное зеркалирование: Исходный порт и порт назначения этой функции находятся на этом устройстве.</li> </ul>

### Конфигурация зеркала

Нажмите на номер группы зеркалирования, чтобы перейти на страницу конфигурации зеркалирования, как показано на рисунке ниже.

### Mirror Configuration

#### Global Settings

Session ID	1 ▼
Mode	Disabled ▼
Type	Local Mirror ▼

#### Source VLAN(s) Configuration

VLAN ID	<input style="width: 80%;" type="text"/>
---------	--

#### Port Configuration

Port	Source	Destination
*	<> ▼	<input type="checkbox"/>
Port 1	Disabled ▼	<input type="checkbox"/>
Port 2	Disabled ▼	<input type="checkbox"/>
Port 3	Disabled ▼	<input type="checkbox"/>
Port 4	Disabled ▼	<input type="checkbox"/>
Port 5	Disabled ▼	<input type="checkbox"/>
Port 6	Disabled ▼	<input type="checkbox"/>
Port 7	Disabled ▼	<input type="checkbox"/>
Port 8	Disabled ▼	<input type="checkbox"/>
Port 9	Disabled ▼	<input type="checkbox"/>
Port 10	Disabled ▼	<input type="checkbox"/>
Port 11	Disabled ▼	<input type="checkbox"/>
Port 12	Disabled ▼	<input type="checkbox"/>
Port 13	Disabled ▼	<input type="checkbox"/>
Port 14	Disabled ▼	<input type="checkbox"/>
Port 15	Disabled ▼	<input type="checkbox"/>
Port 16	Disabled ▼	<input type="checkbox"/>
Port 17	Disabled ▼	<input type="checkbox"/>
Port 18	Disabled ▼	<input type="checkbox"/>
Port 19	Disabled ▼	<input type="checkbox"/>
Port 20	Disabled ▼	<input type="checkbox"/>

Таблица ниже описывает каждый элемент параметров

Параметр	Описание
<b>Global configuration</b>	<b>Глобальная конфигурация</b>
Mirror group ID	Номер текущей настроенной группы зеркалирования, щелкните по выпадающему списку для выбора.
Mode	Включить/отключить функцию зеркалирования.
Type	Выберите включенную функцию зеркалирования на коммутаторе. <ul style="list-style-type: none"> <li>Локальное зеркалирование: Исходный порт и порт назначения этой функции находятся на этом устройстве.</li> </ul>

Параметр	Описание
<b>Source VLAN configuration</b>	Конфигурация исходных VLAN
VLAN ID	Коммутатор поддерживает зеркалирование на основе VLAN. Если вы хотите отслеживать некоторые VLAN на коммутаторе, вы можете установить выбранные VLAN в этом поле. Диапазон от 1 до 4095.
<b>Port configuration</b>	Конфигурация портов
Port	Установите логический порт.
Source port mirroring mode	<p>Выберите режим зеркалирования исходного порта.</p> <ul style="list-style-type: none"> <li>Отключено: не используется в качестве порта источника зеркалирования.</li> <li>Двухнаправленное зеркалирование: как передаваемые, так и принимаемые кадры зеркалируются на порт назначения.</li> <li>Зеркалирование входящего трафика: принимаемые кадры этого порта зеркалируются на порт назначения. Передаваемые кадры не зеркалируются.</li> <li>Зеркалирование исходящего трафика: передаваемые кадры этого порта зеркалируются на порт назначения. Принимаемые кадры не зеркалируются.</li> </ul>
Destination port	Выберите целевой порт.

 Уведомление:

В режиме зеркалирования можно выбрать только один порт назначения.

Целевой порт должен отключить обучение MAC-адресов.

### 3.5 Статистика порта

Эта функция используется для просмотра статистики принятых/переданных данных кадрами каждым портом.

### 3.5.1 Сводные статистические данные

Функция обзора статистики портов. Как показано ниже.

Port Statistics Overview										Auto-refresh <input type="checkbox"/>	Refresh	Clear
Port	Packets		Bytes		Errors		Drops		Filtered			
	Received	Transmitted	Received	Transmitted	Received	Transmitted	Received	Transmitted	Received			
1	59264	2863	4566108	1426234	97	0	0	0	8300			
2	0	0	0	0	0	0	0	0	0			
3	0	0	0	0	0	0	0	0	0			
4	0	0	0	0	0	0	0	0	0			
5	0	0	0	0	0	0	0	0	0			
6	0	0	0	0	0	0	0	0	0			
7	0	0	0	0	0	0	0	0	0			
8	0	0	0	0	0	0	0	0	0			
9	0	0	0	0	0	0	0	0	0			
10	0	0	0	0	0	0	0	0	0			
11	0	0	0	0	0	0	0	0	0			
12	0	0	0	0	0	0	0	0	0			
13	0	0	0	0	0	0	0	0	0			
14	0	0	0	0	0	0	0	0	0			
15	0	0	0	0	0	0	0	0	0			
16	0	0	0	0	0	0	0	0	0			
17	0	0	0	0	0	0	0	0	0			
18	0	0	0	0	0	0	0	0	0			
19	0	0	0	0	0	0	0	0	0			
20	0	0	0	0	0	0	0	0	0			
21	0	0	0	0	0	0	0	0	0			
22	0	0	0	0	0	0	0	0	0			
23	0	0	0	0	0	0	0	0	0			
24	0	0	0	0	0	0	0	0	0			
25	0	0	0	0	0	0	0	0	0			
26	0	0	0	0	0	0	0	0	0			
27	0	0	0	0	0	0	0	0	0			
28	0	0	0	0	0	0	0	0	0			
29	0	0	0	0	0	0	0	0	0			
30	0	0	0	0	0	0	0	0	0			
31	0	0	0	0	0	0	0	0	0			
32	0	0	0	0	0	0	0	0	0			
33	0	0	0	0	0	0	0	0	0			
34	0	0	0	0	0	0	0	0	0			
35	0	0	0	0	0	0	0	0	0			
36	0	0	0	0	0	0	0	0	0			

Таблица ниже описывает каждый элемент параметров

Параметр	Описание
Port	Номер порта. Щелкните на порту, чтобы перейти непосредственно на страницу подробной статистики соответствующего порта.
Frames	Количество принятых или отправленных портом кадров данных.
Number of bytes	Количество принятых или отправленных портом байт.
Error frame	Количество ошибочных кадров, принятых или отправленных портом.
Number of lost packets	Количество отброшенных пакетов, принятых или отправленных портом.
Frame filtering	Количество отфильтрованных кадров, принятых портом.

### 3.5.2 Подробная статистика

Функция подробной статистики отображается ниже.

Detailed Port Statistics Port 1			
		Port 1	Auto-refresh <input type="checkbox"/>
		Refresh	Clear
Receive Total		Transmit Total	
Rx Packets	59538	Tx Packets	2898
Rx Octets	4602409	Tx Octets	1441338
Rx Unicast	2515	Tx Unicast	2876
Rx Multicast	8302	Tx Multicast	14
Rx Broadcast	48624	Tx Broadcast	8
Rx Pause	0	Tx Pause	0
Receive Size Counters		Transmit Size Counters	
Rx 64 Bytes	48386	Tx 64 Bytes	1016
Rx 65-127 Bytes	9560	Tx 65-127 Bytes	177
Rx 128-255 Bytes	499	Tx 128-255 Bytes	9
Rx 256-511 Bytes	539	Tx 256-511 Bytes	919
Rx 512-1023 Bytes	554	Tx 512-1023 Bytes	136
Rx 1024-1518 Bytes	0	Tx 1024-1518 Bytes	641
Rx 1519- Bytes	0	Tx 1519- Bytes	0
Receive Queue Counters		Transmit Queue Counters	
Rx Q0	59441	Tx Q0	2891
Rx Q1	0	Tx Q1	0
Rx Q2	0	Tx Q2	0
Rx Q3	0	Tx Q3	0
Rx Q4	0	Tx Q4	0
Rx Q5	0	Tx Q5	0
Rx Q6	0	Tx Q6	0
Rx Q7	0	Tx Q7	7
Receive Error Counters		Transmit Error Counters	
Rx Drops	0	Tx Drops	0
Rx CRC/Alignment	97	Tx Late/Exc. Coll.	0
Rx Undersize	0		
Rx Oversize	0		
Rx Fragments	0		
Rx Jabber	0		
Rx Filtered	8433		

Таблица ниже описывает каждый элемент параметров

Параметр	Описание
Receive/Send Statistics	<p>Подсчитайте количество кадров, байт, одноадресных кадров, кадров многоадресной рассылки, широковещательных кадров и кадров приостановки, принятых/отправленных портом.</p> <ul style="list-style-type: none"> <li>• Количество принятых/отправленных кадров: подсчитывает количество кадров, принятых/отправленных портом.</li> <li>• Количество принятых/отправленных байт: подсчитывает количество байт, принятых/отправленных портом.</li> <li>• Количество принятых/отправленных одноадресных кадров: подсчитывает количество принятых/отправленных одноадресных кадров портом.</li> <li>• Количество принятых/отправленных кадров многоадресной рассылки: подсчитывает количество принятых/отправленных кадров многоадресной рассылки портом.</li> <li>• Количество принятых/отправленных широковещательных кадров: подсчитывает количество принятых/отправленных широковещательных кадров портом.</li> </ul>

Параметр	Описание
	<ul style="list-style-type: none"> <li>Количество принятых/отправленных кадров приостановки: подсчитывает количество принятых/отправленных кадров приостановки портом.</li> </ul>
Receive/send frame length statistics	<p>Подсчитайте количество длин кадров, принятых/отправленных портом.</p> <ul style="list-style-type: none"> <li>Количество принятых/отправленных кадров размером 64 байта: подсчитывает количество пакетов данных размером 64 байта, принятых/отправленных портом.</li> <li>Количество принятых/отправленных кадров размером от 65 до 127 байт: подсчитывает количество кадров размером от 65 до 127 байт, принятых/отправленных портом.</li> <li>Количество принятых/отправленных кадров размером от 128 до 255 байт: подсчитывает количество кадров размером от 128 до 255 байт, принятых/отправленных портом.</li> <li>Количество принятых/отправленных кадров размером от 256 до 511 байт: подсчитывает количество кадров размером от 256 до 511 байт, принятых/отправленных портом.</li> <li>Количество принятых/отправленных кадров размером от 512 до 1023 байт: подсчитывает количество кадров размером от 512 до 1023 байт, принятых/отправленных портом.</li> <li>Количество принятых/отправленных кадров размером от 1024 до 1518 байт: подсчитывает количество кадров размером от 1024 до 1518 байт, принятых/отправленных портом.</li> <li>Количество принятых/отправленных кадров размером 1519 байт и более: подсчитывает количество кадров размером 1519 байт и более, принятых/отправленных портом.</li> </ul>
Receive/send queue statistics	<p>Подсчитайте количество кадров в очереди, принятых/отправленных портом.</p> <ul style="list-style-type: none"> <li>Принять/отправить Q0: подсчитывает количество кадров, принятых/отправленных портом в очереди Q0.</li> <li>Принять/отправить Q1: подсчитывает количество кадров, принятых/отправленных портом в очереди Q1.</li> <li>Принять/отправить Q2: подсчитывает количество кадров, принятых/отправленных портом в очереди Q2.</li> <li>Принять/отправить Q3: подсчитывает количество кадров, принятых/отправленных портом в очереди Q3.</li> </ul>

Параметр	Описание
	<ul style="list-style-type: none"> <li>• Принять/отправить Q4: подсчитывает количество кадров, принятых/отправленных портом в очереди Q4.</li> <li>• Принять/отправить Q5: подсчитывает количество кадров, принятых/отправленных портом в очереди Q5.</li> <li>• Принять/отправить Q6: подсчитывает количество кадров, принятых/отправленных портом в очереди Q6.</li> <li>• Принять/отправить Q7: подсчитывает количество кадров, принятых/отправленных портом в очереди Q7.</li> </ul>
Receive error frame statistics	<p>Подсчитайте количество ошибочных кадров, полученных портом.</p> <ul style="list-style-type: none"> <li>• Количество принятых отброшенных кадров: подсчитывает количество отброшенных кадров, полученных портом.</li> <li>• Количество принятых кадров с ошибкой проверки/выравнивания: подсчитывает количество кадров с ошибкой CRC или выравнивания данных, полученных портом.</li> <li>• Количество принятых ультракоротких кадров: подсчитывает количество ультракоротких кадров, полученных портом.</li> <li>• Количество принятых кадров джамбо: подсчитывает количество кадров джамбо, полученных портом.</li> <li>• Количество принятых недопустимых фрагментов кадров: подсчитывает количество недопустимых ультракоротких кадров, полученных портом.</li> <li>• Количество принятых недопустимых кадров джамбо: подсчитывает количество недопустимых кадров джамбо, полученных портом.</li> <li>• Количество принятых отфильтрованных кадров: подсчитывает количество отфильтрованных кадров, полученных портом.</li> </ul>
Send error frame statistics	<p>Подсчитайте количество ошибочных кадров данных, отправленных портом.</p> <ul style="list-style-type: none"> <li>• Количество отправленных отброшенных кадров: подсчитывает количество отброшенных кадров, отправленных портом.</li> <li>• Количество отправленных конфликтных кадров: подсчитывает количество конфликтных кадров, отправленных портом.</li> </ul>

### 3.5.3 Статистика кадров управления

Функция статистики управляющих кадров отображается ниже.

Access Management Statistics			
Interface	Received Packets	Allowed Packets	Discarded Packets
HTTP	0	0	0
HTTPS	0	0	0
SNMP	0	0	0
TELNET	0	0	0
SSH	0	0	0

Auto-refresh  Refresh Clear

Таблица ниже описывает каждый элемент параметров:

Параметр	Описание
Protocol interface	Тип протокола для доступа к устройству: поддерживает доступ к устройству через протоколы HTTP, HTTPS, SNMP, TELNET и SSH.
Number of frames received	Подсчитайте количество принятых кадров.
Number of frames allowed	Подсчитайте количество разрешенных кадров.
Number of dropped frames	Подсчитайте количество отброшенных кадров.

## 4 Характеристики 2 уровня

### 4.1 VLAN

VLAN (Virtual Local Area Network) относится к технологии виртуальной локальной сети, которая разделяет физическую локальную сеть на несколько логических локальных сетей, и каждая VLAN является доменом широковещательной передачи. Хосты в VLAN обмениваются сообщениями через традиционные методы Ethernet-коммуникации. Хосты в разных VLAN не могут общаться напрямую и должны использовать сетевое оборудование уровня 3.

#### 4.1.1 Глобальная конфигурация

Global VLAN Configuration								
Allowed Access VLANs		1						
Ethertype for Custom S-ports		88A8						
Port VLAN Configuration								
Port	Mode	Port VLAN	Port Type	Ingress Filtering	Ingress Acceptance	Egress Tagging	Allowed VLANs	Forbidden VLANs
*	<>	1	<>	<input checked="" type="checkbox"/>	<>	<>	1	
1	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag All	1	
2	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag All	1	
3	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag All	1	
4	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag All	1	
5	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag All	1	
6	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag All	1	
7	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag All	1	
8	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag All	1	
9	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag All	1	
10	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag All	1	
11	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag All	1	
12	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag All	1	
13	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag All	1	
14	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag All	1	
15	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag All	1	
16	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag All	1	
17	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag All	1	
18	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag All	1	
19	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag All	1	

Таблица ниже описывает каждый элемент параметров

Параметр	Описание
<b>VLAN global configuration</b>	Глобальная конфигурация VLAN
List of VLANs allowed to access	Созданный список VLAN. VLAN можно использовать только после его создания.
TPID value of S-Custom-Port	TPID S-Custom-Port можно настроить и он независим от S-порта и C-порта.
<b>Port VLAN configuration</b>	Конфигурация VLAN порта
Port	Логический номер порта.

Параметр	Описание
Mode	Дополнительные режимы: Access, Trunk или Hybrid, по умолчанию Access.
Port VLAN	Определение VLAN ID по умолчанию (также называемого PVID) порта, который по умолчанию равен 1.
Port type	Дополнительные режимы: Unaware, C-порт, S-порт или S-Custom-порт, по умолчанию C-порт.
Inlet filtering	Гибридные порты позволяют изменять фильтрацию входящего трафика. Для Access и Trunk портов всегда включена фильтрация входящего трафика.
Acceptable frame types	Существует три режима: Только с метками, Только без меток и С метками и без меток. Изменять этот тип можно только для гибридных портов.
Exit mark	Существует три режима: Метки для всех, Без меток для всех и Без меток VLAN порта. Порты Trunk и Hybrid являются опциональными, а порты Access всегда используют режим Без меток для всех.
Allow through VLAN list	Для портов Trunk и Hybrid можно настроить несколько списков разрешенных VLAN, до 1-4095. Порты Access не настраиваются и фиксируются на PVID порта.
Disable through VLAN list	По умолчанию пусто, настраиваемо от 1 до 4095.



Уведомление:

Прежде чем VLAN начнет действовать на порту, создайте его в "Списке разрешенных VLAN для доступа"..

## 4.1.2 SVL конфигурация

В SVL одну или несколько VLAN отображают на FID. По умолчанию существует однозначное соответствие от VLAN к FID, и с использованием SVL несколько VLAN могут разделять один и тот же вход в таблицу MAC-адресов

**Shared VLAN Learning Configuration**

**Delete** **FID** **VLANs**

Add FID

Save Reset

Таблица ниже описывает каждый элемент параметров

Параметр	Описание
Delete	Удалите ранее назначенный FID.
FID	FID - это идентификатор, изученный в таблице MAC-адресов при применении SVL. Ни две строки в таблице не могут иметь один и тот же FID, и FID должен быть числом от 1 до 4095.
VLANs	Список VLAN, отображенных на FID. Допустимые VLAN находятся в диапазоне от 1 до 4095. Тот же VLAN может быть членом только одного FID. Если VLAN включен в два или более FID, будет отображено сообщение.

### 4.1.3 Члены VLAN

Эта страница предоставляет обзор статуса членства пользователя в VLAN.

VLAN Membership Status for Combined users Combined  Auto-refresh  Refresh

Start from VLAN  with  entries per page. << >>

VLAN ID	Port Members																																					
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36		
1	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

Таблица ниже описывает каждый элемент параметров

Параметр	Описание
VLAN ID	Отобразить идентификатор VLAN порта-участника.
Member port	Отобразить каждый порт-участник, соответствующий идентификатору VLAN.

## 4.1.4 Статус портов

Эта страница предоставляет статус портов VLAN.

VLAN Port Status for Combined users Combined ▾ Auto-refresh  Refresh

Port	Port Type	Ingress Filtering	Frame Type	Port VLAN ID	Tx Tag	Untagged VLAN ID	Conflicts
1	C-Port	<input checked="" type="checkbox"/>	All	1	Untag All		No
2	C-Port	<input checked="" type="checkbox"/>	All	1	Untag All		No
3	C-Port	<input checked="" type="checkbox"/>	All	1	Untag All		No
4	C-Port	<input checked="" type="checkbox"/>	All	1	Untag All		No
5	C-Port	<input checked="" type="checkbox"/>	All	1	Untag All		No
6	C-Port	<input checked="" type="checkbox"/>	All	1	Untag All		No
7	C-Port	<input checked="" type="checkbox"/>	All	1	Untag All		No
8	C-Port	<input checked="" type="checkbox"/>	All	1	Untag All		No
9	C-Port	<input checked="" type="checkbox"/>	All	1	Untag All		No
10	C-Port	<input checked="" type="checkbox"/>	All	1	Untag All		No
11	C-Port	<input checked="" type="checkbox"/>	All	1	Untag All		No
12	C-Port	<input checked="" type="checkbox"/>	All	1	Untag All		No
13	C-Port	<input checked="" type="checkbox"/>	All	1	Untag All		No
14	C-Port	<input checked="" type="checkbox"/>	All	1	Untag All		No
15	C-Port	<input checked="" type="checkbox"/>	All	1	Untag All		No
16	C-Port	<input checked="" type="checkbox"/>	All	1	Untag All		No
17	C-Port	<input checked="" type="checkbox"/>	All	1	Untag All		No
18	C-Port	<input checked="" type="checkbox"/>	All	1	Untag All		No
19	C-Port	<input checked="" type="checkbox"/>	All	1	Untag All		No
20	C-Port	<input checked="" type="checkbox"/>	All	1	Untag All		No
21	C-Port	<input checked="" type="checkbox"/>	All	1	Untag All		No
22	C-Port	<input checked="" type="checkbox"/>	All	1	Untag All		No
23	C-Port	<input checked="" type="checkbox"/>	All	1	Untag All		No
24	C-Port	<input checked="" type="checkbox"/>	All	1	Untag All		No
25	C-Port	<input checked="" type="checkbox"/>	All	1	Untag All		No
26	C-Port	<input checked="" type="checkbox"/>	All	1	Untag All		No
27	C-Port	<input checked="" type="checkbox"/>	All	1	Untag All		No
28	C-Port	<input checked="" type="checkbox"/>	All	1	Untag All		No
29	C-Port	<input checked="" type="checkbox"/>	All	1	Untag All		No
30	C-Port	<input checked="" type="checkbox"/>	All	1	Untag All		No
31	C-Port	<input checked="" type="checkbox"/>	All	1	Untag All		No
32	C-Port	<input checked="" type="checkbox"/>	All	1	Untag All		No
33	C-Port	<input checked="" type="checkbox"/>	All	1	Untag All		No
34	C-Port	<input checked="" type="checkbox"/>	All	1	Untag All		No
35	C-Port	<input checked="" type="checkbox"/>	All	1	Untag All		No
36	C-Port	<input checked="" type="checkbox"/>	All	1	Untag All		No

Таблица ниже описывает каждый элемент параметров

Параметр	Описание
Port	Логический порт настройки, содержащийся на одной строке.
Port type	Отображение типа порта (Unaware, C-Port, S-port или S-Custom-port)
Inlet filtering	Показать, желает ли данный пользователь включить фильтрацию входящего трафика.
Frame type	Отображение типов кадров, которые данный пользователь хочет настроить на порту.
Port VLAN ID	Отображение VLAN ID порта (PVID), который данный пользователь хочет установить для порта.
Send label	Отображение требований к отправке метки для данного пользователя на порту.
Untagged VLAN ID	Отображение VLAN ID, который пользователь хочет иметь без тега на выходе.

Параметр	Описание
Conflict	Показать, есть ли у двух пользователей конфликты в конфигурации VLAN порта.

## 4.2 Перевод VLAN

Перевод VLAN (VLAN translation) относится к преобразованию одного идентификатора VLAN в другой идентификатор VLAN на порте моста.

### 4.2.1 Конфигурация групп портов

На странице конфигурации групп портов, показанной на рисунке ниже.

VLAN Translation Port Configuration Auto-refresh  Refresh

Port	Group Configuration	
	Default	Group ID
*	<input type="checkbox"/>	<> ▾
1	<input type="checkbox"/>	1 ▾
2	<input type="checkbox"/>	2 ▾
3	<input type="checkbox"/>	3 ▾
4	<input type="checkbox"/>	4 ▾
5	<input type="checkbox"/>	5 ▾
6	<input type="checkbox"/>	6 ▾
7	<input type="checkbox"/>	7 ▾
8	<input type="checkbox"/>	8 ▾
9	<input type="checkbox"/>	9 ▾
10	<input type="checkbox"/>	10 ▾
11	<input type="checkbox"/>	11 ▾
12	<input type="checkbox"/>	12 ▾
13	<input type="checkbox"/>	13 ▾
14	<input type="checkbox"/>	14 ▾
15	<input type="checkbox"/>	15 ▾
16	<input type="checkbox"/>	16 ▾
17	<input type="checkbox"/>	17 ▾
18	<input type="checkbox"/>	18 ▾
19	<input type="checkbox"/>	19 ▾
20	<input type="checkbox"/>	20 ▾
21	<input type="checkbox"/>	21 ▾
22	<input type="checkbox"/>	22 ▾
23	<input type="checkbox"/>	23 ▾
24	<input type="checkbox"/>	24 ▾
25	<input type="checkbox"/>	25 ▾
26	<input type="checkbox"/>	26 ▾
27	<input type="checkbox"/>	27 ▾
28	<input type="checkbox"/>	28 ▾
29	<input type="checkbox"/>	29 ▾
30	<input type="checkbox"/>	30 ▾
31	<input type="checkbox"/>	31 ▾
32	<input type="checkbox"/>	32 ▾
33	<input type="checkbox"/>	33 ▾
34	<input type="checkbox"/>	34 ▾
35	<input type="checkbox"/>	35 ▾
36	<input type="checkbox"/>	36 ▾

Save Reset

Таблица ниже описывает каждый элемент параметров

Параметр	Описание
Port	Номер логического порта.
Group configuration	<ul style="list-style-type: none"> <li>По умолчанию: Отметьте "По умолчанию", чтобы восстановить порт в группу по умолчанию.</li> <li>Идентификатор группы: Преобразование VLAN разделено на группы, определяемые идентификатором группы.</li> </ul>

 **Внимание:**

Отметьте "По умолчанию" и нажмите "Настроить", чтобы инициализировать идентификатор группы.

## 4.2.2 Отображение VLAN

Страница отображения VLAN, показанная на рисунке ниже.

**VLAN Translation Mapping Table** Auto-refresh  Refresh Remove All

Group ID	Direction	VID	TVID	
				+

Таблица ниже описывает каждый элемент параметров

Параметр	Описание
Group ID	Отображение перевода VLAN разделено на группы, определяемые идентификатором группы.
Direction	Выберите направление входа, направление выхода или выберите все. <ul style="list-style-type: none"> <li>• Двухнаправленный: направление входа, направление выхода.</li> <li>• Вход: направление входа.</li> <li>• Выход: направление выхода.</li> </ul>
Source VID	Ссылаясь на отображенный идентификатор VLAN, то есть исходный VLAN. Допустимый диапазон идентификаторов VLAN составляет от 1 до 4095.
Translated VID	Ссылаясь на отображенный идентификатор VALN, то есть переведенный идентификатор VLAN, который находится в диапазоне от 1 до 4095.



Уведомление:

Когда режим настроен как "двухнаправленный", на входе, если идентификатор VLAN кадра равен настроенному VID, идентификатор VLAN кадра удаляется и помечается как TVID;

На выходе, если идентификатор VLAN кадра равен настроенному TVID, идентификатор VLAN кадра удаляется, а добавляется VID.

## 4.3 Расширенные настройки VLAN

### 4.3.1 MAC-VLAN

VLAN на основе MAC-адреса разделяет VLAN в соответствии с исходным MAC-адресом пакета. Когда устройство получает пакет с порта, оно сопоставляет запись MAC-VLAN на основе исходного MAC-адреса пакета. После успешного сопоставления оно добавляет соответствующий тег VLAN и затем пересылает пакет в соответствующий VLAN для передачи.

Как показано ниже:

**MAC-based VLAN Membership Configuration** Auto-refresh  Refresh

			Port Members																																			
Delete	MAC Address	VLAN ID	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36
Currently no entries present																																						

Add New Entry

Save Reset

Таблица ниже описывает каждый элемент параметров

Параметр	Описание
Delete	Удалите соответствующую запись.
MAC address	Исходный MAC-адрес.
VLAN ID	Тег VLAN ID, добавленный после успешного сопоставления.
Member port	Вы можете выбрать порты в списке для присоединения к группе отображения.

### 4.3.2 Протокол-VLAN

Протокольные VLAN делятся в соответствии с типом протокола и форматом инкапсуляции пакетов. После того как устройство получит пакет без тега VLAN с порта, оно будет сопоставлять запись протокольного VLAN в соответствии с типом протокола и форматом инкапсуляции пакета. После успешного сопоставления оно добавит соответствующий тег VLAN и затем перенаправит пакет в соответствующий VLAN для передачи.

#### 4.3.2.1 Протокол-группа

Как показано ниже:

**Protocol to Group Mapping Table** Auto-refresh

Delete	Frame Type	Value	Group Name
No Group entry found!			

Таблица ниже описывает каждый элемент параметров

Parameter	Description
Delete	Удалить соответствующую запись.
Frame type	Тип кадра, доступны три типа кадров: Ethernet, SNAP и LLC.
Value	Существуют различные диапазоны значений в зависимости от трех типов кадров.
Group name	Название созданной протокольной группы.

### 4.3.2.2 Группа-VLAN

Как показано ниже:

**Group Name to VLAN mapping Table** Auto-refresh

Delete	Group Name	VLAN ID	Port Members																																	
			1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34
Currently no entries present in the switch																																				

Таблица ниже описывает каждый элемент параметров

Параметр	Описание
Delete	Удалить соответствующую запись.
Group name	Имя протокольной группы для присоединения.
VLAN ID	Тег VLAN ID, добавленный после успешного сопоставления.
Member port	Порты в списке могут быть отмечены для присоединения к протокольной группе.

### 4.3.3 IP-VLAN

VLAN, основанные на подсетях IP, делятся на VLAN на основе исходного IP-адреса и маски подсети пакетов. После получения пакета с порта устройство будет сопоставлять запись подсети VLAN в соответствии с исходным IP-адресом и маской подсети пакета. После успешного сопоставления оно добавит соответствующий тег VLAN и затем пересылит пакет в соответствующий VLAN для передачи.

Как показано ниже:

Auto-refresh  Refresh

Delete	IP Address	Mask Length	VLAN ID	Port Members																																			
				1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36
Currently no entries present																																							

Add New Entry

Save Reset

Таблица ниже описывает каждый элемент параметров

Параметр	Описание
Delete	Удалить соответствующую запись.
IP address	Исходный IP-адрес.
Mask length	Длина маски исходного IP-адреса.
VLAN ID	Тег VLAN ID, добавленный после успешного сопоставления.
Member port	Порты в списке могут быть отмечены для присоединения к протокольной группе.

## 4.4 PVLAN

VLAN и PVLAN независимы друг от друга. Порт должен быть добавлен одновременно в один и тот же список VLAN и список PVLAN, чтобы пересылать данные пакеты. По умолчанию все порты присоединены к VLAN 1 и PVLAN 1.

### 4.4.1 Конфигурация участников

Как показано ниже.

Auto-refresh  Refresh

Delete	PVLAN ID	Port Members																																				
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	
<input type="checkbox"/>	1	<input checked="" type="checkbox"/>																																				

Add New Private VLAN

Save Reset

Таблица ниже описывает каждый элемент параметров

Параметр	Описание
Delete	Удалить соответствующую запись.
PVLAN ID	Настроенный идентификатор PVLAN.
Port member	Вы можете выбрать порты в списке для присоединения к группе PVLAN.

## 4.4.2 Изоляция портов

Конфигурация изоляции портов.

**Port Isolation Configuration** Auto-refresh

Port Number																																					
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36		
<input type="checkbox"/>																																					

Таблица ниже описывает каждый элемент параметров

Параметр	Описание
Port number	Вы можете выбрать порт в списке для присоединения к группе изоляции портов VLAN.



Уведомление:

Поддерживается несколько групп частных VLAN, но поддерживается только одна группа изоляции портов.

Группа изоляции разделяет только отмеченные порты друг от друга.

## 4.5 Таблица MAC-адресов

Таблица MAC-адресов - это таблица маршрутизации на основе портов уровня 2 и является основой для быстрой передачи пакетов. В таблице MAC-адресов содержится несколько записей маршрутизации, и каждая запись маршрутизации имеет соответствующий адрес MAC назначения, идентификатор VLAN порта и порт маршрутизации.

### 4.5.1 Конфигурация таблицы адресов

Страница таблицы MAC-адресов отображается на рисунке ниже.

**MAC Address Table Configuration**

**Aging Configuration**

Disable Automatic Aging

Aging Time  seconds

**MAC Table Learning**

	Port Members																																						
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36			
Auto	<input checked="" type="radio"/>																																						
Disable	<input type="radio"/>	<input type="radio"/>																																					
Secure	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>																																				

**VLAN Learning Configuration**

Learning-disabled VLANs

**Static MAC Table Configuration**

	Port Members																																							
Delete	VLAN ID	MAC Address	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36		
<input type="text"/>	<input type="text"/>	<input type="text"/>																																						

Таблица ниже описывает каждый элемент параметров

Параметр	Описание
<b>Aging time configuration</b>	<b>Информация о конфигурации времени старения</b>
MAC address not automatically aged	Отметьте, чтобы отключить функцию автоматического старения MAC-адресов.
MAC address aging time	Настраиваемое время старения адресов.
<b>MAC address table learning</b>	<b>Информация о изучении таблицы MAC-адресов</b>
Auto	Автоматически изучать MAC-адреса.
Off	Не изучать MAC-адреса.
Secure	Изучать только статические записи MAC-адресов
<b>VLAN learning configuration</b>	<b>Информация о конфигурации изучения VLAN</b>
List of VLANs prohibited from learning	Для этого идентификатора VLAN MAC-адреса не будет изучаться.
<b>Static MAC address table configuration</b>	<b>Конфигурация статической таблицы MAC-адресов</b>
Delete	Удалить текущую запись.
VLAN ID	Идентификатор VLAN, привязанный к статическому MAC-адресу.
MAC address	Статический MAC-адрес.
Member port	Порт-участник статической таблицы MAC-адресов.
Add new static entry	Добавить новую запись в статическую таблицу MAC и указать идентификатор VLAN, MAC-адрес и принадлежность порту для новой записи

## 4.5.2 Запись MAC-адреса

На этой странице отображается таблица MAC-адресов. Каждая запись маршрутизации содержит соответствующий адрес MAC назначения, идентификатор VLAN порта и порт маршрутизации.

Как показано ниже:

MAC Address Table			Port Members																																															
Type	VLAN	MAC Address	CPU	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36											
Dynamic	1	04-D9-F5-AF-5D-70	✓																																															
Dynamic	1	0C-9D-92-78-5E-7B	✓																																															
Dynamic	1	0C-9D-92-78-60-F2	✓																																															
Dynamic	1	0C-9D-92-BE-58-DC	✓																																															
Dynamic	1	14-DD-A9-7C-3C-46	✓																																															
Dynamic	1	24-4B-FE-97-6F-F3	✓																																															
Static	1	33-33-00-00-00-01	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓						
Static	1	33-33-FF-C4-14-C0	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓					
Static	1	4C-93-A6-C4-14-C0	✓																																															
Dynamic	1	50-EB-F6-2D-95-68	✓																																															
Dynamic	1	50-EB-F6-2D-95-D1	✓																																															
Dynamic	1	50-EB-F6-2E-78-29	✓																																															
Dynamic	1	50-FA-84-CB-35-51	✓																																															
Dynamic	1	58-11-22-06-19-B9	✓																																															
Dynamic	1	58-11-22-06-1D-1D	✓																																															
Dynamic	1	58-11-22-95-BC-3D	✓																																															
Dynamic	1	60-45-CB-88-67-1C	✓																																															
Dynamic	1	64-9D-99-17-AC-78	✓																																															
Dynamic	1	7C-10-C9-8C-C4-0A	✓																																															
Dynamic	1	7C-10-C9-8C-DC-75	✓																																															

Таблица ниже описывает каждый элемент параметров

Параметр	Описание
Тип	Обозначает, является ли данная запись MAC-адреса статической или динамической.
VLAN	Идентификатор VLAN записи.
MAC address	MAC-адрес записи.
Member port	Порт-участник записи.



Уведомление:

Если MAC-адрес настроен для отображения, начиная с XX-XX-XX-XX-XX-XX, страница будет отображаться, начиная со следующего адреса после этого MAC-адреса.

## 4.6 IGMP-Snooping

### 4.6.1 Базовая конфигурация

Веб-страница базовой конфигурации включает две части: "Глобальная конфигурация" и "Конфигурация портов".

Как показано ниже.

**IGMP Snooping Configuration**

Global Configuration			
Snooping Enabled	<input checked="" type="checkbox"/>		
Unregistered IPMCv4 Flooding Enabled	<input checked="" type="checkbox"/>		
IGMP SSM Range	232.0.0.0	/	8
Leave Proxy Enabled	<input type="checkbox"/>		
Proxy Enabled	<input type="checkbox"/>		

**Port Related Configuration**

Port	Router Port	Fast Leave	Throttling
*	<input type="checkbox"/>	<input type="checkbox"/>	<> ▾
1	<input type="checkbox"/>	<input type="checkbox"/>	unlimited ▾
2	<input type="checkbox"/>	<input type="checkbox"/>	unlimited ▾
3	<input type="checkbox"/>	<input type="checkbox"/>	unlimited ▾
4	<input type="checkbox"/>	<input type="checkbox"/>	unlimited ▾
5	<input type="checkbox"/>	<input type="checkbox"/>	unlimited ▾
6	<input type="checkbox"/>	<input type="checkbox"/>	unlimited ▾
7	<input type="checkbox"/>	<input type="checkbox"/>	unlimited ▾
8	<input type="checkbox"/>	<input type="checkbox"/>	unlimited ▾
9	<input type="checkbox"/>	<input type="checkbox"/>	unlimited ▾
10	<input type="checkbox"/>	<input type="checkbox"/>	unlimited ▾
11	<input type="checkbox"/>	<input type="checkbox"/>	unlimited ▾
12	<input type="checkbox"/>	<input type="checkbox"/>	unlimited ▾
13	<input type="checkbox"/>	<input type="checkbox"/>	unlimited ▾
14	<input type="checkbox"/>	<input type="checkbox"/>	unlimited ▾
15	<input type="checkbox"/>	<input type="checkbox"/>	unlimited ▾
16	<input type="checkbox"/>	<input type="checkbox"/>	unlimited ▾
17	<input type="checkbox"/>	<input type="checkbox"/>	unlimited ▾
18	<input type="checkbox"/>	<input type="checkbox"/>	unlimited ▾
19	<input type="checkbox"/>	<input type="checkbox"/>	unlimited ▾
20	<input type="checkbox"/>	<input type="checkbox"/>	unlimited ▾
21	<input type="checkbox"/>	<input type="checkbox"/>	unlimited ▾
22	<input type="checkbox"/>	<input type="checkbox"/>	unlimited ▾
23	<input type="checkbox"/>	<input type="checkbox"/>	unlimited ▾

Таблица ниже описывает каждый элемент параметров

Параметр	Описание
<b>Global configuration</b>	<b>Глобальная конфигурация:</b>
Snooping enabled	Переключатель глобальной активации функции IGMP-Snooping.

Параметр	Описание
Unknown IPv4 multicast flooding enabled	Переключатель разрешения распространения неизвестных IPv4-мультимедийных пакетов.
IGMP SSM scope	Диапазон адресов SSM мультимедийных адресов, формат адреса - x.y.z.w, где диапазон значений x составляет 224-239, диапазон значений y/z/w составляет 0-255, а диапазон значений маски подсети составляет 4-32.
Leave message proxy enabled	Включение прокси-сообщения IGMP Leave. После включения этой функции можно снизить ненужное перенаправление сообщений об уходе вверх по сети.
Agent enabled	Включение прокси-сервера IGMP. После включения этой функции устройство может проксировать опросы для отправки запросов вниз по потоку к участникам группы, поддерживать членство в группе и выполнять многоадресную пересылку на основе членства в группе.
<b>Port configuration</b>	<b>Конфигурация портов</b>
Port	Номер порта устройства.
router port	Настройка статических портов маршрутизатора.
Quickly leave the group	Включена функция быстрого выхода из группы.
Entry restrictions	Ограничение на количество записей адресов. После установки максимальное количество записей, которые определенный порт может изучить.

## 4.6.2 VLAN Конфигурация

Настройка VLAN используется для конфигурации ряда параметров функции IGMP-Snooping в конкретной VLAN, как показано на следующем рисунке.

VLAN ID	Snooping Enabled	Querier Election	Querier Address	Compatibility	PRI	RV	QI (sec)	QRI (0.1 sec)	LLQI (0.1 sec)	URI (sec)
1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	0.0.0.0	IGMP-Auto	0	2	125	100	10	1

Таблица ниже описывает каждый элемент параметров

Параметр	Описание
VLAN ID	Номер идентификатора VLAN.
Snooping enabled	Переключатель активации функции IGMP-Snooping в конкретной VLAN.
Querier election	Переключатель выбора опросника.
Querier IP address	Настройка адреса опросника. Этот IPv4-адрес используется в качестве исходного адреса протокольного пакета. Если адрес опросника не настроен, система использует IPv4-адрес

Параметр	Описание
	управления IP-интерфейса, связанного с этой VLAN. Если IPv4-адрес управления не установлен, система использует IPv4-адрес управления IP-интерфейса, связанного с этой VLAN, или любой доступный IPv4-адрес управления; в противном случае система использует значение по умолчанию - 192.0.2.1.
Protocol version	<p>Настройка версии протокола.</p> <ul style="list-style-type: none"> <li>• Автоматическое распознавание IGMP: автоматическое адаптирование версии IGMP.</li> <li>• IGMPv1: принудительное использование IGMPv1.</li> <li>• IGMPv2: принудительное использование IGMPv2.</li> <li>• IGMPv3: принудительное использование IGMPv3.</li> </ul>
Priority	Приоритет, диапазон значений от 0 до 7, 7 - самый высокий приоритет, значение по умолчанию - 0.
Robustness coefficient	Коэффициент надежности, диапазон значений от 1 до 255, значение по умолчанию - 2.
Query interval (seconds)	Интервал запроса, временной интервал для отправки опросных сообщений общей группы опросником. Диапазон значений от 1 до 31744, значение по умолчанию - 125.
Maximum query response interval (0.1 seconds)	Максимальное время ответа на запрос опросника общей группы, диапазон значений от 0 до 31744, значение по умолчанию - 100.
Specific group query message interval (0.1 seconds)	Интервал времени для отправки запросов сообщений о конкретной группе. Диапазон значений от 0 до 31744, значение по умолчанию - 10.
Interval of unsolicited report messages (seconds)	Интервал времени для активной отправки сообщений о состоянии, диапазон значений от 1 до 31744, значение по умолчанию - 1 секунда.

### 4.6.3 Статус

Эта веб-страница разделена на две части: информацию о статистике состояния IGMP-Snooping и информацию о состоянии портов маршрутизатора, как показано на рисунке ниже.



## 4.6.4 Информация о группе

Эта веб-страница отображает все записи MAC-адресов, как показано на рисунке ниже..

**IGMP Snooping Group Information** Auto-refresh  Refresh |<< >>

Start from VLAN  and group address  with  entries per page.

		Port Members																																			
VLAN ID	Groups	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36
		No more entries																																			

Каждая запись адреса в информации о группе IGMP-Snooping содержит три части: идентификатор VLAN, адрес группы и список членов группы.

## 4.6.5 Настройка фильтрации

Эта веб-страница указывает конфигурационный файл фильтрации для конкретного порта. Перед этим необходимо настроить файл конфигурации фильтрации многоадресной рассылки. Если на системе отсутствует файл конфигурации фильтрации многоадресной рассылки, нельзя указать файл конфигурации для порта.

Как показано ниже.

**IGMP Snooping Port Filtering Profile Configuration**

Port	Filtering Profile
1	 - v
2	 - v
3	 - v
4	 - v
5	 - v
6	 - v
7	 - v
8	 - v
9	 - v
10	 - v
11	 - v
12	 - v
13	 - v
14	 - v
15	 - v
16	 - v
17	 - v
18	 - v
19	 - v
20	 - v
21	 - v
22	 - v
23	 - v
24	 - v
25	 - v
26	 - v
27	 - v
28	 - v
29	 - v
30	 - v
31	 - v
32	 - v
33	 - v
34	 - v
35	 - v
36	 - v

Save Reset

Нажмите на значок ниже "Фильтр", чтобы просмотреть правила фильтрации, настроенные в конфигурационном файле.

### 4.6.6 SFM информация

SFM (Source Filtering Multicast) - это многоадресная фильтрация источника. На этой веб-странице отображается вся информация о записях SFM, как показано на следующем рисунке.

**IGMP SFM Information** Auto-refresh  Refresh |<< >>

Start from VLAN  and Group  with  entries per page.

VLAN ID	Group	Port	Mode	Source Address	Type	Hardware Filter/Switch
No more entries						

Информация, содержащаяся в записи информации о SFM слева направо: идентификатор VLAN, IPv4-адрес группы, номер порта, режим фильтрации (ВКЛЮЧАТЬ/ИСКЛЮЧАТЬ), адрес источника, тип (Разрешить/Запретить) и аппаратное переключение.

## 4.7 Фильтрация многоадресной рассылки

### 4.7.1 Файл конфигурации

Эта страница предоставляет конфигурацию, связанную с профилем IPMC.

Профиль IPMC используется для развертывания контроля доступа к IP-мультимедийным потокам. Позволяет создать 64 файла для каждого подмножества, с до 128 соответствующими правилами.

**IPMC Profile Configurations**

Global Profile Mode

**IPMC Profile Table Setting**

Delete	Profile Name	Profile Description	Rule
<input type="button" value="Add New IPMC Profile"/>			
<input type="button" value="Save"/> <input type="button" value="Reset"/>			

Таблица ниже описывает каждый элемент параметров

Параметр	Описание
Global profile mode	Включить или отключить глобальное разбиение IPMC на подмножества. Только когда режим глобального разбиения включен, система начинает фильтрацию на основе настроек подмножеств.

Параметр	Описание
<b>Multicast filteri configuration file table</b>	<b>Таблица файла конфигурации фильтрации многоадресной рассылки:</b>
Delete	Отметьте, чтобы удалить запись. Указанные записи будут удалены при следующем сохранении.
Configuration file name	Название таблицы, используемой для индексации подмножества. Каждая запись имеет уникальное имя, состоящее из не более 16 буквенно-цифровых символов. Обязательно должна быть хотя бы одна буква.
Configuration file description	Дополнительное пояснение к подмножеству, состоящее из 64 буквенно-цифровых символов. В описании не допускаются пробелы или символы пробела. Используйте "" или "-" для разделения описательных предложений.
Rule	<p>При создании подмножества нажмите кнопку  для входа на страницу настройки правил указанного подмножества. Нажатие кнопки  отобразит сводку о указанном подмножестве. Вы можете использовать следующие кнопки для управления или просмотра правил для определенного профиля:</p> <ul style="list-style-type: none"> <li> Перечисляет правила, связанные с указанным подмножеством.</li> <li> Регулирует правила, связанные с указанным подмножеством.</li> </ul>

Нажмите кнопку "  ", чтобы перейти на страницу настройки правил.

На этой странице предоставляются настройки фильтрации правил для определенного профиля IPMS. Она отображает настроенные записи правил в порядке приоритета. Первая запись правила имеет самый высокий приоритет при поиске, а последняя запись правила

имеет самый низкий приоритет при поиске.

**IPMC Profile [1] Rule Settings (In Precedence Order)**

Profile Name & Index	Entry Name	Address Range	Action	Log	
1	1	- ▾	~ Deny ▾	Disable ▾	

Таблица ниже описывает каждый элемент параметров

Параметр	Описание
Template file name & index	Название указанного шаблона для ассоциации. Это поле нельзя редактировать.
Item name	Укажите имя диапазона адресов, используемого этим правилом. Для выбора в списке доступны только существующие записи адресов профиля. При отправке формы настройки правил нельзя выбрать "None" ("-") для этого поля.
Adress range	Соответствующий диапазон адресов для выбранной записи профиля. Это поле нельзя редактировать и автоматичес
Action	<p>Опишем действие обучения, когда получен кадр присоединения/отчета с групповым адресом, совпадающим с диапазоном адресов, заданным в правиле.</p> <ul style="list-style-type: none"> <li>Запретить (Deny): удалить групповые адреса, совпадающие с указанным диапазоном в правиле.</li> <li>Разрешить (Allow): обучиться групповым адресам, совпадающим с указанным диапазоном в правиле.</li> </ul>
Log	<p>Опишем предпочтение ведения журнала при получении кадра присоединения/отчета с групповым адресом, совпадающим с диапазоном адресов, заданным в правиле.</p> <ul style="list-style-type: none"> <li>Включено (Enabled): регистрировать соответствующую информацию для групповых адресов, совпадающих с диапазоном, указанным в правиле.</li> <li>Отключено (Disabled): не регистрировать соответствующую информацию для групповых адресов, совпадающих с диапазоном, указанным в правиле.</li> </ul>
Rule management button	<p>Вы можете управлять правилами и соответствующими приоритетами с помощью следующих кнопок:</p> <ul style="list-style-type: none"> <li>: Добавляет новое правило перед текущей записью правила.</li> </ul>

Параметр	Описание
	<ul style="list-style-type: none"> <li>⊗: Удаляет текущую запись правила.</li> <li>⬆: Перемещает текущую запись правила вверх по списку.</li> <li>⬇: Перемещает текущую запись правила вниз по списку.</li> </ul>

## 4.7.2 Записи адресов

Эта страница предоставляет настройки для диапазонов адресов, используемых в профиле IPMC. Запись адреса используется для указания диапазона адресов, который будет ассоциирован с профилем IPMC. Она позволяет создавать до 128 записей адресов в системе.

**IPMC Profile Address Configuration** Refresh | << >>

Navigate Address Entry Setting in IPMC Profile by  entries per page.

Delete	Entry Name	Start Address	End Address
<input type="button" value="Add New Address (Range) Entry"/>			
<input type="button" value="Save"/> <input type="button" value="Reset"/>			

Таблица ниже описывает каждый элемент параметров

Параметр	Описание
Delete	Отметьте для удаления записи. Указанные записи будут удалены при следующем сохранении.
Item name	Имя, используемое для индексации таблицы записей адресов. Каждая запись имеет уникальное имя, состоящее из не более 16 буквенно-цифровых символов. Обязательно должна быть хотя бы одна буква.
Starting address	Начальный адрес IPv4/IPv6 мультимедийной группы, который будет использоваться в качестве диапазона адресов.
Ending address	Конечный адрес IPv4/IPv6 мультимедийной группы, который будет использоваться в качестве диапазона адресов.

## 4.8 LLDP

LLDP (Link Layer Discovery Protocol) - это протокол обнаружения уровня канала, определенный в IEEE802.1ab. LLDP - это стандартный метод обнаружения уровня 2, который может организовать управляющий адрес, идентификацию устройства и другую информацию локального устройства и опубликовать ее на соседние устройства. После получения этой информации соседнее устройство будет использовать ее в стандартной базе

управляющей информации. Она сохраняется в форме MIB (базы управляющей информации) для запроса и определения статуса связи сетевой системы управления.

TIA (Ассоциация телекоммуникационной промышленности Америки) разработала протокол под названием протокол обнаружения уровня канала - обнаружение конечных точек средств связи (LLDP-MED) для определения определенных расширений для улучшения автоматизированного управления определенными типами сетевого оборудования (например, IP-телефонами и т. д.). В LLDP-MED определяются возможности подключенного устройства и его включение. Затем он будет продолжать отправлять пакеты LLDP-MED, пока удаленное устройство, к которому он подключен, не перестанет иметь возможности LLDP-MED. LLDP-MED поддерживает следующие три типа конечных точек:

Категория 1: Базовая конечная точка участника. Например, контроллер IP-связи.

Категория 2: Конечные точки, поддерживающие мультимедийную передачу данных.

Примеры включают медиа-шлюзы и конференц-мосты.

Категория 3: Конечные точки, поддерживающие конечных пользователей IP-связи.

Например, IP-телефоны и программные телефоны.

CDP (Cisco Discovery Protocol) и LLDP (Link Layer Discovery Protocol) - это оба протокола обнаружения соседей, которые могут работать в среде IEEE 802 (Ethernet). Оба протокола выполняют практически одно и то же, основное отличие состоит в поставщике. CDP - это проприетарный протокол Cisco, в то время как LLDP - это открытый стандартный протокол. Фактически, CDP расшифровывается как протокол обнаружения Cisco, а LLDP - как протокол обнаружения уровня канала. Опять же, оба работают точно так же.

### 4.8.1 LLDP конфигурация

LLDP - страница настройки отображена на рисунке ниже.

**LLDP Configuration**

**LLDP Parameters**

Tx Interval	30	seconds
Tx Hold	4	times
Tx Delay	2	seconds
Tx Reinit	2	seconds

**LLDP Interface Configuration**

Interface	Mode	Optional TLVs							
		CDP aware	Trap	Port Descr	Sys Name	Sys Descr	Sys Capa	Mgmt Addr	
* <>	<>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>					
GigabitEthernet 1/1	Disabled	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>					
GigabitEthernet 1/2	Disabled	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>					
GigabitEthernet 1/3	Disabled	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>					
GigabitEthernet 1/4	Disabled	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>					
GigabitEthernet 1/5	Disabled	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>					
GigabitEthernet 1/6	Disabled	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>					
GigabitEthernet 1/7	Disabled	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>					
GigabitEthernet 1/8	Disabled	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>					
GigabitEthernet 1/9	Disabled	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>					
GigabitEthernet 1/10	Disabled	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>					
GigabitEthernet 1/11	Disabled	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>					
GigabitEthernet 1/12	Disabled	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>					
GigabitEthernet 1/13	Disabled	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>					
GigabitEthernet 1/14	Disabled	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>					
GigabitEthernet 1/15	Disabled	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>					
GigabitEthernet 1/16	Disabled	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>					
GigabitEthernet 1/17	Disabled	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>					
GigabitEthernet 1/18	Disabled	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>					

Таблица ниже описывает каждый элемент параметров

Параметр	Описание
<b>LLDP parameters</b>	<b>Конфигурация параметров LLDP</b>
Sending interval	Интервал отправки кадров LLDP: Переключатель периодически отправляет LLDP-кадры своим соседям для обновления информации о сети. Интервал отправки между LLDP-кадрами определяется этим значением. Значение по умолчанию для интервала отправки составляет 30 секунд, и значение может варьироваться от 5 до 32768.
TTL multiplier	TTL множитель: Каждый кадр LLDP содержит информацию с TTL (временем жизни). Эта переменная служит множителем для интервала отправки и используется для расчета значения TTL в кадре LLDP. Значение по умолчанию для множителя TTL составляет 4, и администраторы могут изменить диапазон значений на любое значение от 2 до 10. (TTL = интервал отправки * множитель TTL).
Send delay	Задержка отправки при изменении конфигурации: Если произошли изменения конфигурации, такие как изменение IP-адреса, новые LLDP-кадры будут отправлены немедленно. Когда конфигурация устройства часто меняется, интервал времени между

Параметр	Описание
	отправкой LLDP-кадров не будет менее этого значения. Значение задержки отправки не может быть больше четверти параметра интервала отправки. Диапазон значений - любое значение от 1 до 8192. Значение по умолчанию - 2.
Send initialization delay	Задержка инициализации порта: Этот параметр - это время задержки для повторных попыток инициализации при переключении из режима работы LLDP TX и TXRX в режим RX и Disable. LLDP будет отправлять кадры выключения для сообщения соседям, что ранее сохраненная информация устарела. Эта переменная контролирует временную задержку между кадрами выключения и новой инициализацией. Значение по умолчанию для времени задержки инициализации порта составляет 2 секунды, и администратор может изменить диапазон значений на любое значение от 1 до 10.
<b>LLDP interface configuration</b>	<b>Конфигурация интерфейса LLDP</b>
Interface	Логическое имя интерфейса коммутатора.
Operating mode	<ul style="list-style-type: none"> <li>Выберите режим работы интерфейса LLDP. Режимы следующие:</li> <li>Только прием: принимать только кадры LLDP и не отправлять кадры LLDP.</li> <li>Только отправка: отправлять только кадры LLDP и не принимать кадры LLDP.</li> <li>Не отправлять/не принимать: не отправлять и не принимать кадры LLDP.</li> <li>Отправка/прием: и отправлять, и принимать кадры LLDP.</li> </ul>
CDP discovery	<p>Когда выбрано, это используется для декодирования кадров CDP. Коммутатор не будет отправлять кадры CDP. Кадры CDP будут декодироваться только при включенном LLDP на порту. Только те части CDP, которые могут быть сопоставлены с соответствующими полями в таблице соседей LLDP, будут декодироваться, а другие части будут отброшены (неизвестные CDP TLV и отброшенные CDP не будут отображаться в статистике LLDP). CDP TLV сопоставляется с таблицей соседей LLDP следующим образом:</p> <ul style="list-style-type: none"> <li>Поле "Device ID" CDP TLV сопоставляется с полем "Chassis ID" LLDP;</li> </ul>

Параметр	Описание
	<ul style="list-style-type: none"> <li>• Поле "Address" CDP TLV сопоставляется с полем "Management Address" LLDP. Этот CDP TLV адреса может содержать несколько адресов, но в таблице соседей LLDP отображается только первый адрес;</li> <li>• Поле "Port ID" CDP TLV сопоставляется с полем "Port ID" LLDP;</li> <li>• Поле "Version and Platform" CDP TLV сопоставляется с полем "System Description" LLDP;</li> <li>• Поле "Port ID" CDP TLV сопоставляется с полем "Port ID" LLDP;</li> <li>• Поле "Port ID" CDP TLV сопоставляется с полем "Port ID" LLDP;</li> <li>• Поле "Port ID" CDP TLV сопоставляется с полем "Port ID" LLDP;</li> <li>• Поле "Port ID" CDP TLV сопоставляется с полем "Port ID" LLDP.</li> </ul> <p>Иллюстрация: И CDP, и LLDP поддерживают поле "system capabilities", но возможности CDP больше, чем у LLDP. Эти возможности отображаются в поле "other" таблицы соседей LLDP; Если "CDP Discovery" отключено на всех интерфейсах, коммутатор будет пересылать кадры CDP, полученные от соседей; если "CDP Discovery" включено хотя бы на одном интерфейсе, все кадры CDP будут завершаться на коммутаторе.</p> <p>Примечание: Когда "CDP discovery" отключено на интерфейсе, информация CDP не будет немедленно удалена, но будет удалена по истечении времени удержания.</p>
Trap	<p>При выборе этой опции будут отправляться SNMP-трапы при изменении таблицы информации о соседних устройствах на интерфейсе.</p>
Optional TLVs	<ul style="list-style-type: none"> <li>• Описание порта: Дополнительный TLV. При выборе этой опции в LLDP передается информация об описании порта.</li> </ul>

Параметр	Описание
	<ul style="list-style-type: none"> <li>Имя системы: Дополнительный TLV. При выборе этой опции в LLDP передается информация об имени системы.</li> <li>Описание системы: Дополнительный TLV. При выборе этой опции в LLDP передается информация об описании системы.</li> <li>Функция системы: Дополнительный TLV. При выборе этой опции в LLDP передается информация о функции системы.</li> <li>Управляющий адрес: Дополнительный TLV. При выборе этой опции в LLDP передается информация об управляющем адресе.</li> </ul>

## 4.8.2 Информация о соседях

Страница с информацией о соседях отображена на рисунке ниже.

LLDP Neighbor Information							Auto-refresh <input type="checkbox"/>	Refresh
LLDP Remote Device Summary								
Local Interface	Chassis ID	Port ID	Port Description	System Name	System Capabilities	Management Address		
No neighbor information found								

Таблица ниже описывает каждый элемент параметров

Параметр	Описание
Local interface	Интерфейс, на котором был получен кадр LLDP.
Device MAC	Chassis ID - это идентификатор кадра LLDP соседа, обычно представленный MAC-адресом.
Device port	Port ID - это идентификация порта соседа.
Device port description	Описание порта соседа, объявленное соседом.
system name	Описание системного имени соседа, объявленное соседом.
System functions	<p>Описание функциональности системы соседа, объявленное соседом. Когда функция включена, после неё ставится (+). Если функция отключена, после неё ставится (-). Возможные функции следующие:</p> <ul style="list-style-type: none"> <li>Others</li> <li>Repeater (Репитер)</li> </ul>

Параметр	Описание
	<ul style="list-style-type: none"> <li>• Bridge (Мост)</li> <li>• WLAN access point (Точка доступа WLAN)</li> <li>• Router (Маршрутизатор)</li> <li>• Telephone (Телефон)</li> <li>• Cable equipment (Кабельное оборудование)</li> <li>• Site only (client) (Только клиент на сайте)</li> <li>• Reserved (Зарезервировано)</li> </ul>
Management address	Управляющий адрес — это адрес соседнего устройства, используемый более высокими сущностями, чтобы оно могло быть обнаружено системой управления сетью. Например, это может быть IP-адрес соседа.

### 4.8.3 Статистика порта

Статистические значения разделены на глобальные счетчики и локальные счетчики. Глобальные относятся к статистике всего коммутатора, а локальные - к статистике порта.

LLDP Global Counters		Auto-refresh <input type="checkbox"/>	Refresh	Clear					
<b>Global Counters</b>									
Clear global counters <input checked="" type="checkbox"/>									
Neighbor entries were last changed 2023-06-30T14:49:31+00:00 (2100 secs. ago)									
Total Neighbors Entries Added	0								
Total Neighbors Entries Deleted	0								
Total Neighbors Entries Dropped	0								
Total Neighbors Entries Aged Out	0								
<b>LLDP Statistics Local Counters</b>									
Local Interface	Tx Frames	Rx Frames	Rx Errors	Frames Discarded	TLVs Discarded	TLVs Unrecognized	Org. Discarded	Age-Outs	Clear
GigabitEthernet 1/1	0	0	0	0	0	0	0	0	<input checked="" type="checkbox"/>
GigabitEthernet 1/2	0	0	0	0	0	0	0	0	<input checked="" type="checkbox"/>
GigabitEthernet 1/3	0	0	0	0	0	0	0	0	<input checked="" type="checkbox"/>
GigabitEthernet 1/4	0	0	0	0	0	0	0	0	<input checked="" type="checkbox"/>
GigabitEthernet 1/5	0	0	0	0	0	0	0	0	<input checked="" type="checkbox"/>
GigabitEthernet 1/6	0	0	0	0	0	0	0	0	<input checked="" type="checkbox"/>
GigabitEthernet 1/7	0	0	0	0	0	0	0	0	<input checked="" type="checkbox"/>
GigabitEthernet 1/8	0	0	0	0	0	0	0	0	<input checked="" type="checkbox"/>
GigabitEthernet 1/9	0	0	0	0	0	0	0	0	<input checked="" type="checkbox"/>
GigabitEthernet 1/10	0	0	0	0	0	0	0	0	<input checked="" type="checkbox"/>
GigabitEthernet 1/11	0	0	0	0	0	0	0	0	<input checked="" type="checkbox"/>
GigabitEthernet 1/12	0	0	0	0	0	0	0	0	<input checked="" type="checkbox"/>
GigabitEthernet 1/13	0	0	0	0	0	0	0	0	<input checked="" type="checkbox"/>
GigabitEthernet 1/14	0	0	0	0	0	0	0	0	<input checked="" type="checkbox"/>
GigabitEthernet 1/15	0	0	0	0	0	0	0	0	<input checked="" type="checkbox"/>

Таблица ниже описывает каждый элемент параметров

Параметр	Описание
LLDP overall statistical value	Общая статистика LLDP

Параметр	Описание
Clear overall statistics	После проверки нажмите кнопку "Очистить", чтобы очистить глобальный счетчик.
Neighbor information last updated time	Показывает, когда была последний раз добавлена или удалена запись. Также отображает время, прошедшее с момента последнего обнаружения изменений.
The number of all added neighbor information	Показывает количество новых записей, добавленных с момента перезапуска коммутатора.
The number of deleted neighbor information	Показывает количество новых записей, удаленных с момента перезапуска коммутатора.
The number of discarded neighbor information	Показывает количество кадров LLDP, сброшенных из-за заполнения таблицы входа.
All expired neighbor information	Показывает количество записей, удаленных из-за истечения времени TTL.
<b>LLDP Statistics Local Calculator</b>	<b>Локальный калькулятор статистики LLDP</b>
Local interface	Интерфейс для приема или отправки кадров LLDP.
Total number of messages sent	Общее количество отправленных на этом интерфейсе кадров LLDP.
Total number of messages received	Общее количество принятых на этом интерфейсе кадров LLDP.
Number of error messages received	Общее количество кадров LLDP, принятых на этом интерфейсе, содержащих какие-либо ошибки.
Number of packets dropped	Если кадр LLDP принят с интерфейса и внутренняя таблица коммутатора переполнена, кадр LLDP будет подсчитан и отброшен. Это состояние называется "слишком много соседей" в стандарте LLDP. Когда таблица еще не содержит Chassis ID или удаленный порт ID в кадре, кадр требует новой записи в таблице. Записи удаляются из таблицы, когда данный интерфейс становится недоступным или когда LLDP получает кадр о выключении или когда запись устаревает.
Total number of dropped TLVs	Каждый кадр LLDP содержит несколько кусков информации, называемых TLV (TLV — это сокращение от "Type Length Value"). Если TLV сформирован неправильно, он будет подсчитан и отброшен.
Total number of unknown TLVs	Количество принятых кадров LLDP с правильными TLV, но неизвестного типа, которые были отброшены.

Параметр	Описание
Number of unsupported TLVs dropped	Если TLV в принятом кадре LLDP не поддерживается, он будет подсчитан и отброшен.
Number of expired neighbors	Кадры LLDP содержат информацию о времени устаревания. Если в течение времени устаревания не получены новые кадры, информация о LLDP будет удалена, и счетчик увеличится.
Clear	Если установлен флажок, счетчики на конкретном интерфейсе будут очищены после нажатия кнопки "Очистить".

# 5 Резервирование кольцевой сети

## 5.1 ERPS

Ethernet Ring Protection Switching (ERPS) - это протокол защиты кольца Ethernet на уровне канала связи. Он предотвращает штормы широковещания, вызванные петлями данных при полной конфигурации кольца. Когда соединение на кольце разрывается, связь между узлами кольца может быть быстро восстановлена, и скорость сходимости высока.

### 5.1.1 ERPS конфигурация

На странице отображается информация о конфигурации ERPS, как показано на рисунке ниже. На этой странице будет отображаться вся сконфигурированная информация о группе кольцевой сети ERPS.

ERPS Configuration																				Auto-refresh	Refresh			
ERPS #	RPL		Ver	Type	VC	Interconnect		Port0		Port1		Ring Id	Node Id	Level	Control		Rev	Guard	WTR	Hold Off	Enable	Oper	Warning	
	Mode	Port				Instance	Prop	Port	SF	Port	SF				VLAN	PCP								

Нажмите на значок добавления, чтобы перейти на страницу конфигурации ERPS, как показано на рисунке ниже.

ERPS Configuration

Configuration

ERPS #	Version	Type	VC	Interconnect		Port If		RingId	NodeId	Level	Control		Rev	Guard	WTR	HoldOff	Enable
				Instance	Prop	Port0	Port1				VLAN	PCP					
0	v2	Major	<input checked="" type="checkbox"/>		<input type="checkbox"/>	1	1	1	00:00:00:00:00:00	7	1	7	<input checked="" type="checkbox"/>	500	300	0	<input type="checkbox"/>

Signal Fail Trigger

Port0				Port1			
Type	Domain	Service	MEPID	Type	Domain	Service	MEPID
Link			0	Link			0

Protected VLANs

VLAN ID:

Ring Protection Link

RPL Mode	RPL Port
None	RingPort0

Save Reset Cancel

Таблица ниже описывает каждый элемент параметров

Параметр	Описание
<b>Configuration</b>	<b>Конфигурация</b>
ERPS example	ID экземпляра кольца ERPS.
Version	Версия протокола ERPS, доступные версии: V1 или V2.
Ring network type	Тип сети кольца ERPS: <ul style="list-style-type: none"> <li>Основной: указывает на основное кольцо.</li> </ul>

Параметр	Описание
	<ul style="list-style-type: none"> <li>Подкольцо: указывает на подкольцо.</li> <li>Межподкольцо: представляет собой подкольцо на узле межсоединения.</li> </ul>
Virtual channel	Виртуальный канал, если отмечено, значит включено, если не отмечено, значит отключено.
Interconnection Properties	<ul style="list-style-type: none"> <li>Основное кольцо, к которому принадлежит: ID основного кольца, к которому принадлежит подкольцо узла межсоединения.</li> <li>Уведомление о изменении топологии: статус уведомления об обнаружении топологии. Отметьте, чтобы включить эту функцию.</li> </ul>
Ring port	<ul style="list-style-type: none"> <li>Порт0: порт кольца, Порт0 представляет восточный порт, только Порт0 действует в режиме Межподкольцо.</li> <li>Порт1: порт кольца, Порт1 представляет западный порт.</li> </ul>
Ring ID	ID кольца используется для уникальной идентификации кольца ERPS. Тот же ID кольца должен быть сконфигурирован на всех узлах в одном и том же кольце ERPS.
Node ID	ID узла кольца.
MD/MEG level	Уровень сообщений R-APS.
Control VLAN	<ul style="list-style-type: none"> <li>VLAN: VLAN управления, то есть протокольный VLAN, VLAN, передаваемый в протокольных пакетах ERPS.</li> <li>PCP: приоритет PCP протокольных сообщений ERPS.</li> </ul>
Switchback mode	То есть реверсивный, устанавливает режим реверсии кольца. Если отмечено, это означает реверсию, если не отмечено, это означает отсутствие реверсии.
Guard	Таймер охранного времени, который запускается, когда порт обнаруживает восстановление связи, используется для предотвращения остаточных сообщений R-APS из-за задержки при онлайн-пересылке, вызывающей ненужные встряски в сети. Перед истечением этого таймера интерфейс больше не будет обрабатывать все пакеты R-APS. Этот таймер влияет на производительность восстановления связи при множественных точках отказа.
WTR	Таймер WTR. В режиме реверсии этот таймер запускается, когда владелец узла получает сообщение NR в состоянии MS или FS. Он используется для предотвращения блокировки и повторного включения порта RPL в кольцевой сети из-за махания сети. Перед истечением этого таймера RPL продолжает пересылку, и неисправный узел отправляет сообщения NR. В течение этого периода, если владелец узла снова получает сообщение SF, это означает, что в кольцевой сети все еще существует неисправное

Параметр	Описание
	соединение. Таймер отключается непосредственно, и RPL продолжает пересылку. В противном случае после истечения таймера владелец узла блокирует RPL, отправляет сообщение (NR, RB), чтобы уведомить временно заблокированную точку об освобождении и одновременно обновляет запись MAC-адреса.
Hold Off	Таймер задержки запускается, когда порт обнаруживает отказ связи, замедляя скорость сообщения об ошибке. При отказе соединения ожидайте истечения времени таймера задержки и повторно сообщайте об ошибке, если она по-прежнему существует. Это дает службовому уровню возможность восстановить соединение и избежать ненужного сообщения об ошибке. Длина этого таймера будет влиять на скорость сообщения об ошибке соединения и производительность переключения соединения при возникновении ошибки.
Enable	Переключатель включения кольца, если отмечен, означает, что кольцо включено, если снят, то кольцо выключено.
<b>SF trigger</b>	<b>Конфигурация механизма срабатывания сигнала SF</b>
Port0/Port1	<ul style="list-style-type: none"> <li>Тип: режим срабатывания сигнала SF, Link означает срабатывание на основе статуса соединения порта, MEP означает срабатывание на основе MEP, установленного на порту.</li> <li>Имя домена: действительно в режиме MEP, это доменное имя MEP, настроенное на порту.</li> <li>Сервер: действительно в режиме MEP, это имя сервера MEP, настроенное на порту.</li> <li>MEPID: действительно в режиме MEP, это идентификатор MEP, настроенный на порту.</li> </ul>
<b>Protect VLAN</b>	<b>Защитная VLAN</b>
VLAN ID	Список защитных VLAN. Тот же самый защитный VLAN должен быть настроен на всех узлах в том же ERPS кольцевом экземпляре.
<b>RPL configuration</b>	<b>Конфигурация RPL</b>
Node type	Роль узла ERPS. Варианты, следующие: <ul style="list-style-type: none"> <li>None: обозначает обычный узел;</li> <li>Owner: обозначает узел-владелец;</li> <li>Neighbor: обозначает соседний узел.</li> </ul>
RPL port	Порт RPL узла ERPS.

## 5.1.2 ERPS статус

Интерфейс отображения статуса ERPS.

ERPS Status											Auto-refresh <input type="checkbox"/> Refresh		
ERPS #	Oper	Warning	State	TxRapsActive	cFOPTo	Tx Info						SMAC	
						UpdateTimeSecs	Request	Version	Rb	Dnf	Bpr	Node Id	SMAC
No entry exists													

Таблица ниже описывает каждый элемент параметров

Параметр	Описание
ERPS example	Идентификатор экземпляра группы кольцевой сети ERPS.
Operating status	Статус работы экземпляра ERPS. Зеленая иконка указывает на отсутствие проблем с работой. Красная иконка указывает на отключение экземпляра ERPS или наличие ошибки в конфигурации.
Alarm information	Для сигналов тревог работы экземпляра ERPS серые иконки указывают на отсутствие тревог, желтые иконки указывают на наличие тревог, и требуется проверка конфигурации.
Ring status	Существует 6 состояний узлов кольцевой сети ERPS, включая состояние Init, состояние Idle, состояние Protection, состояние Pending, состояние MS и состояние FS.
Transmitting R-APS messages	Указывает, отправлять ли пакеты R-APS на кольцевой порт.
R-APS reception time	Указывает, есть ли таймаут приема R-APS на кольцевом порту.
Send message	<p>Информация о пакетах R-APS, отправленных текущим узлом, отображается в этом списке. Конкретно, он включает следующую информацию:</p> <ul style="list-style-type: none"> <li>• <b>Время обновления:</b> Время последнего обновления статуса узла ERPS. Это время относительно времени запуска устройства.</li> <li>• <b>Запрос:</b> Тип сообщения.</li> <li>• <b>Версия:</b> Версия протокола ERPS, 0 представляет V1, 1 представляет V2.</li> <li>• <b>Rb:</b> Статус RPL-связи, × указывает, что связь RPL не заблокирована, и √ указывает, что связь RPL заблокирована.</li> <li>• <b>Dnf:</b> Уведомляет, следует ли обновить таблицу MAC-адресов, √ означает, что таблица MAC-адресов не обновляется, × означает, что таблица MAC-адресов обновляется.</li> </ul>

Параметр	Описание
	<ul style="list-style-type: none"><li>• Врг: Порт RPL.</li><li>• Идентификатор узла: Идентификатор узла, переданный в сообщении R-APS, связан с конфигурацией. По умолчанию это MAC-адрес порта.</li><li>• SMAC: MAC-адрес источника, используемый пакетами R-APS. По умолчанию это MAC-адрес порта.</li></ul>

**Уведомление:**

При конфигурации порта кольцевой сети ERPS необходимо отключить функцию связующего дерева для этого порта.

На странице "Конфигурация ERPS" и странице "Статус ERPS" щелкните соответствующую ссылку экземпляра ERPS, чтобы перейти на страницу отображения информации о состоянии ERPS..

**ERPS Status** Auto-refresh

**Configuration**

ERPS #	Ver	Type	VC	Prop	Port0	Port1	Ring Id	Node Id	Level	VLAN	PCP	Rev	Guard	WTR	HoldOff	Enable
1	v2	Major	✓	✗	1	2	1	00:00:00:00:00:00	7	1	7	✓	500	300	0	✗

**Status**

Oper	Warning	State	TxRapsActive	cFOPTo	UpdateTimeSecs	Request	Version	Rb	Dnf	Bpr	Node Id	SMAC
<span style="color: red;">●</span>	<span style="color: gray;">●</span>	Init	✗	✗	0	No Request	0	✗	✗	RingPort0	00:00:00:00:00:00	00:00:00:00:00:00

**Status Ports**

Parameter	Port0	Port1
Blocked	✗	✗
Signal Fail	✗	✗
Failure of Protocol - Provisioning Mismatch	✗	✗
UpdateTimeSecs	0	0
Request state	No Request	No Request
Version of received R-APS. 0 means v1 etc	0	0
RPL blocked bit of R-APS info	✗	✗
Do Not Flush bit of R-APS info	✗	✗
Blocked Port Reference of R-APS info	RingPort0	RingPort0
Node ID of this request	00:00:00:00:00:00	00:00:00:00:00:00
Source MAC address used in the request/state	00:00:00:00:00:00	00:00:00:00:00:00

**Counters**

Counter type	Port0	Port1
Received erroneous R-APS PDUs	0	0
Received R-APS PDUs with our own node ID	0	0
Received R-APS PDUs during guard timer	0	0
Received R-APS PDUs causing FOP-PM	0	0
Received NR R-APS PDUs	0	0
Received NR, RB R-APS PDUs	0	0
Received SF R-APS PDUs	0	0
Received FS R-APS PDUs	0	0
Received MS R-APS PDUs	0	0
Received Event R-APS PDUs	0	0
Transmitted NR R-APS PDUs	0	0
Transmitted NR, RB R-APS PDUs	0	0
Transmitted SF R-APS PDUs	0	0
Transmitted FS R-APS PDUs	0	0
Transmitted MS R-APS PDUs	0	0
Transmitted Event R-APS PDUs	0	0
Number of local signal fails	0	0
Number of FDB flushes	0	0

**Command**

**Command**

No request

Таблица ниже описывает каждый элемент параметров

Параметр	Описание
Configuration	Отображает информацию о конфигурации текущего экземпляра ERPS. Для описания параметров конфигурации см. главу "Конфигурация ERPS".
Status	Отображает текущую информацию о состоянии экземпляра ERPS. Для описания различных параметров см. главу "Статус ERPS".
Ring port status	Отображает информацию о состоянии текущего порта кольца экземпляра ERPS.
Packet statistics	Отображает количество пакетов R-APS каждого типа, полученных и отправленных текущим портом кольца экземпляра ERPS.
Recount	Вы можете очистить статистику полученных и отправленных пакетов R-APS для текущего порта кольца экземпляра ERPS для повторного подсчета статистики.

Параметр	Описание
Switching command	<p>Текущий экземпляр ERPS поддерживает функцию быстрого переключения. Ниже приведены доступные команды управления переключением:</p> <ul style="list-style-type: none"> <li>• No request: Бездействие. Система не выполняет никаких действий, если не поступает команда переключения.</li> <li>• Force switch to Port0: выполняет команду принудительного переключения (FS) на порту Port0. Трафик немедленно переключается на этот порт.</li> <li>• Force switch to Port1: выполняет команду принудительного переключения (FS) на порту Port1. Трафик немедленно переключается на этот порт.</li> <li>• Manual switch to Port0: выполняет команду ручного переключения (MS) на порту Port0. Система запрашивает подтверждение перед переключением трафика на этот порт.</li> <li>• Manual switch to Port1: выполняет команду ручного переключения (MS) на порту Port1. Система запрашивает подтверждение перед переключением трафика на этот порт.</li> <li>• Clear: очищает текущее состояние быстрого переключения</li> </ul>

## 5.2 Протокол связующего дерева (STP)

Для обеспечения резервного канала и повышения надежности сети Ethernet обычно используются избыточные связи. Однако использование избыточных связей может привести к возникновению петель в коммутационной сети, вызывая широковещательные штормы и нестабильность таблиц MAC-адресов, что приводит к низкому качеству связи для пользователей или даже к прерыванию связи. Для решения проблемы петель в коммутационной сети был предложен протокол связующего дерева STP (Spanning Tree Protocol).

Устройства, работающие с протоколом STP, обнаруживают петли в сети, обмениваясь информацией друг с другом, и выборочно блокируют определенный порт. В результате кольцевая структура сети преобразуется в структуру дерева без петель, тем самым предотвращая передачу пакетов в кольцевой сети. Это позволяет избежать постоянного циклического процесса, который может снизить производительность устройства из-за повторного приема одних и тех же пакетов.

В связи с медленной сходимостью топологии STP IEEE в 2001 году выпустил стандарт 802.1w для определения RSTP (Rapid Spanning Tree Protocol). RSTP улучшает работу STP и

обеспечивает быструю сходимость топологии сети. Однако у RSTP и STP все еще есть один и тот же недостаток: поскольку все VLAN в локальной сети используют одно связующее дерево, не удастся достичь балансировки нагрузки трафика данных между VLAN. При блокировке канала он не будет переносить трафик, что также может привести к тому, что пакеты некоторых VLAN не будут перенаправлены.

Для компенсации недостатков STP и RSTP IEEE в 2002 году опубликовал стандарт 802.1s, который определил MSTP. MSTP совместим с STP и RSTP, обеспечивает быструю сходимость сетевой топологии и предоставляет несколько избыточных путей для пересылки данных, достигая балансировки нагрузки VLAN в процессе пересылки данных. MSTP разделяет коммутационную сеть на несколько областей, в каждой из которых формируются несколько деревьев остовов. Деревья остовов являются независимыми друг от друга. Каждое дерево остова называется экземпляром множественного остова (MSTI), а каждая область - регионом MST (MST Region: Multiple Spanning Tree Region).

Термин "экземпляр дерева остова" представляет собой набор нескольких VLAN. Путем объединения нескольких VLAN в один экземпляр можно сэкономить коммуникационную нагрузку и использование ресурсов. Вычисления топологии каждого экземпляра MSTP независимы друг от друга, и на этих экземплярах можно достичь балансировки нагрузки. Несколько VLAN с одинаковой топологией могут быть сопоставлены с одним экземпляром. Состояние пересылки этих VLAN на порту зависит от состояния порта в соответствующем экземпляре MSTP.

## 5.2.1 STP конфигурация моста

Конфигурация моста протокола Spanning Tree (STP), используется для настройки базовой информации и расширенных параметров конфигурации моста.

**STP Bridge Configuration**

**Basic Settings**

Protocol Version	MSTP
Bridge Priority	32768
Hello Time	2
Forward Delay	15
Max Age	20
Maximum Hop Count	20
Transmit Hold Count	6

**Advanced Settings**

Edge Port BPDU Filtering	<input type="checkbox"/>
Edge Port BPDU Guard	<input type="checkbox"/>
Port Error Recovery	<input type="checkbox"/>
Port Error Recovery Timeout	<input style="width: 100%;" type="text"/>

Таблица ниже описывает каждый элемент параметров:

Параметр	Описание
<b>Basic configuration</b>	<b>Basic configuration</b>
Protocol version	Настройка версии протокола MSTP/RSTP/STP. Допустимые значения: STP, RSTP и MSTP.
Bridge priority	Контроль приоритета моста. Чем ниже значение, тем выше приоритет. Приоритет моста, увеличенный на номер экземпляра MSTI, конкатенируется с 6-байтным MAC-адресом коммутатора, чтобы сформировать идентификатор моста. Для операций MSTP это приоритет CIST. В противном случае это приоритет моста STP/RSTP.
Polling cycle	Интервал отправки STP BPDUs. Допустимые значения в диапазоне от 1 до 10 секунд, значение по умолчанию - 2 секунды.
Forwarding delay	Задержка перевода портов моста в режим пересылки root и designated (при использовании в режиме совместимости с STP). Допустимые значения в диапазоне от 4 до 30 секунд.
Maximum survival time	Время устаревания информации, передаваемой мостом, когда мост является корневым мостом. Допустимые значения в диапазоне от 6 до 40 секунд, время устаревания должно быть $\leq (\text{задержка передачи} - 1) * 2$ .
Maximum number of hops	Определение начального значения оставшегося количества переходов для информации MSTI, генерируемой на границе области MSTI. Определяет, сколько мостов может распространять свою информацию BPDU корневой мост. Допустимые значения в диапазоне от 6 до 40 переходов.
The number of packets that the port can send per second	Количество BPDUs, которые порт моста может отправлять в секунду. При превышении этого значения передача следующего BPDU будет задержана. Допустимые значения в диапазоне от 1 до 10 BPDUs в секунду.
<b>Advanced configuration</b>	<b>Расширенная конфигурация</b>
Edge port BPDU filtering	Выбор, является ли порт краевым портом, который будет отправлять и принимать пакеты BPDU.
Edge port BPDU protection	Управляет тем, будет ли порт, явно настроенный как краевой, отключен при получении пакетов BPDU. Порт перейдет в состояние ошибки и будет исключен из активной топологии.
Port error status self-recovery	Управляет тем, будет ли порт, находящийся в состоянии ошибки, автоматически включен после определенного времени. Если восстановление не включено, порт должен быть отключен и снова включен для нормальной работы STP. Перезапуск системы также может снять это состояние.

Параметр	Описание
Port error status self-recovery timeout	Прошедшее время, прежде чем порт в состоянии ошибки может быть включен. Допустимые значения находятся в диапазоне от 30 секунд до 86400 секунд (24 часа).

## 5.2.2 Отображение экземпляров

Интерфейс конфигурации отображения экземпляров показан на рисунке ниже. По умолчанию все VLAN отображаются в CIST, а при настройке MSTP VLAN можно отобразить на экземпляры MSTI1-7.

**MSTI Configuration**

Add VLANs separated by spaces or comma.

Unmapped VLANs are mapped to the CIST. (The default bridge instance).

**Configuration Identification**

Configuration Name	4c-93-a6-c4-14-c0
Configuration Revision	0

**MSTI Mapping**

MSTI	VLANs Mapped
MSTI1	
MSTI2	
MSTI3	
MSTI4	
MSTI5	
MSTI6	
MSTI7	
TE	

Таблица ниже описывает каждый элемент параметров

Параметр	Описание
<b>Configuration definition</b>	<b>Определение конфигурации</b>
Configuration name	Имя флага конфигурации MST, то есть доменное имя MST, по умолчанию равно MAC-адресу устройства.
Configuration version	Уровень ревизии флага конфигурации MST. Значение по умолчанию - все 0. Рекомендуется использовать разные номера для различных областей, чтобы исключить ошибку, что коммутаторы в разных областях считаются находящимися в одной области из-за одинаковой сводной информации таблицы конфигурации MST.
<b>MSTI mapping</b>	<b>Отображение MSTI</b>
MSTI	Экземпляры связующего дерева включают MSTI1-7 и TE. Экземпляр TE - это особый экземпляр. Все VLAN, отображенные на этот экземпляр, всегда будут находиться в состоянии пересылки.

Параметр	Описание
VLAN mapping	Список VLAN, которые необходимо отобразить на соответствующий экземпляр, может быть одним VLAN или несколькими VLAN. Для разделения VLAN используйте запятые или пробелы. Непрерывные VLAN можно соединять с помощью '-'. Один и тот же VLAN может быть отображен только на один экземпляр. Список VLAN, соответствующий неиспользуемым MSTI, должен оставаться пустым.

### 5.2.3 Приоритет экземпляра

Страница конфигурации приоритета экземпляра.

**MSTI Configuration**

MSTI Priority Configuration

MSTI	Priority
*	<> ▼
CIST	32768 ▼
MSTI1	32768 ▼
MSTI2	32768 ▼
MSTI3	32768 ▼
MSTI4	32768 ▼
MSTI5	32768 ▼
MSTI6	32768 ▼
MSTI7	32768 ▼

Save   Reset

Таблица ниже описывает каждый элемент параметров

Параметр	Описание
MSTI	Примеры деревьев охвата, примеры включают CIST и MSTI1-7.
Priority	Приоритет экземпляра. На первой строке можно настроить приоритет всех экземпляров пакетами.

### 5.2.4 CIST порт

Конфигурация портов в экземпляре CIST.

**STP CIST Port Configuration**

CIST Aggregated Port Configuration

Port	STP Enabled	Path Cost	Priority	Admin Edge	Auto Edge	Restricted Role	TCN	BPDU Guard	Point-to-point
-	<input type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Forced True

CIST Normal Port Configuration

Port	STP Enabled	Path Cost	Priority	Admin Edge	Auto Edge	Restricted Role	TCN	BPDU Guard	Point-to-point
*	<input type="checkbox"/>	<>	<>	<>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<>
1	<input type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
2	<input type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
3	<input type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
4	<input type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
5	<input type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
6	<input type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
7	<input type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
8	<input type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
9	<input type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
10	<input type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto

Таблица ниже описывает каждый элемент параметров

Параметр	Описание
CIST aggregation/common port configuration	Конфигурация агрегации/общего порта CIST.
STP enabled	Настройка включения STP на соответствующем порту. Отметьте, чтобы включить его, и снимите отметку, чтобы отключить.
Path cost	Стоимость пути порта. Выберите "Auto" для использования значения по умолчанию или "Specific", чтобы вручную ввести значение в диапазоне от 1 до 200000000.
Priority	Приоритет порта.
Edge port	Настройка соответствующего порта как краевого порта. "Non-Edge" указывает на не краевой порт, а "Edge" на краевой порт.
Automatic boundary	Автоматическое распознавание порта как краевого и его включение.
Limit	<ul style="list-style-type: none"> <li>Role: Это означает, что защита корня включена. После включения защиты корня порт не будет выбран в качестве корневого порта.</li> <li>TCN: Включена защита от TCN. После включения защиты TCN порт не будет принимать и пересылать сообщения о изменении топологии.</li> </ul>

Параметр	Описание
BPDU protection	После включения защиты от BPDU порт больше не будет принимать сообщения BPDU.
Point-to-point network connection	Конфигурация сетевого соединения точка-точка: <ul style="list-style-type: none"> <li>• Auto: Означает, что порт автоматически определяет, является ли он соединением точка-точка.</li> <li>• Yes: Указывает, что порт насильно настроен как соединение точка-точка.</li> <li>• No: Указывает, что порт принадлежит к общей сети.</li> </ul>

## 5.2.5 Порт экземпляра

Страница выбора экземпляра показана на рисунке ниже.

**MSTI Port Configuration**

Select MSTI

MST1 ▾ Get

Выберите соответствующий экземпляр и нажмите кнопку "Получить", чтобы перейти на страницу конфигурации портов данного экземпляра, как показано на рисунке ниже.

**MST1 MSTI Port Configuration**

**MSTI Aggregated Ports Configuration**

Port	Path Cost	Priority
-	Auto	128

**MSTI Normal Ports Configuration**

Port	Path Cost	Priority
*	<>	<>
1	Auto	128
2	Auto	128
3	Auto	128
4	Auto	128
5	Auto	128
6	Auto	128
7	Auto	128
8	Auto	128
9	Auto	128
10	Auto	128
11	Auto	128
12	Auto	128
13	Auto	128
14	Auto	128

Таблица ниже описывает каждый элемент параметров:

Параметр	Описание
Port	Порт Ethernet устройства.
Path cost	Стоимость пути порта. Выберите "Авто", чтобы использовать значение по умолчанию, или выберите "Специфическое", чтобы вручную ввести значение в диапазоне от 1 до 200000000.
Priority	Приоритет порта.

## 5.2.6 Статус моста

Страница отображения статуса моста выглядит следующим образом, как показано на рисунке ниже. Можно отобразить идентификатор моста, идентификатор корня, корневой порт, стоимость пути до корня, флаг изменения топологии и время последнего изменения топологии для каждого экземпляра.

**STP Bridges** Auto-refresh  Refresh

MSTI	Bridge ID	Root			Topology Flag	Topology Change Last
		ID	Port	Cost		
CIST	32768.4C-93-A6-C4-14-C0	32768.4C-93-A6-C4-14-C0	-	0	Steady	-

Таблица ниже описывает каждый элемент параметров:

Параметр	Описание
MSTI	Экземпляр моста. Это также ссылка на подробный статус моста STP.
Bridge ID	Идентификатор моста этого экземпляра
Root	<ul style="list-style-type: none"> <li>ID: Идентификатор моста текущего выбранного корневого моста.</li> <li>Root port: Порт коммутатора, в настоящее время назначенный ролью корневого порта.</li> <li>Path cost: Внешняя стоимость пути. Для корневого моста она равна нулю. Для всех остальных мостов это сумма стоимостей пути портов по наименьшему стоимостному пути к корневому мосту.</li> </ul>
Topology change flag	Состояние флага изменения топологии для данного экземпляра моста.
Last change time of topology	Время с момента последнего изменения топологии.

Щелкните на соответствующем экземпляре, чтобы просмотреть более подробную информацию о мосте STP, как показано на рисунке ниже.

**STP Detailed Bridge Status** Auto-refresh  Refresh

STP Bridge Status	
Bridge Instance	CIST
Bridge ID	32768.4C-93-A6-C4-14-C0
Root ID	32768.4C-93-A6-C4-14-C0
Root Cost	0
Root Port	-
Regional Root	32768.4C-93-A6-C4-14-C0
Internal Root Cost	0
Topology Flag	Steady
Topology Change Count	0
Topology Change Last	-

**CIST Ports & Aggregations State**

Port	Port ID	Role	State	Path Cost	Edge	Point-to-Point	Uptime
<i>No ports or aggregations active</i>							

Таблица ниже описывает каждый элемент параметров

Параметр	Описание
<b>STP bridge status</b>	<b>Статус моста STP</b>
Bridge instance	Экземпляры моста - CIST, MST1,...
Bridge ID	ID этого экземпляра моста.
Root bridge ID	ID моста выбранного корневого моста.

Параметр	Описание
Root port path cost	Внешняя стоимость пути. Для корневого моста она равна нулю. Для всех остальных мостов это сумма стоимости портов на пути наименьшей стоимости к корневому мосту.
Root port	Порт коммутатора, в настоящее время назначенный ролью корневого порта.
Domain root	ID корневого моста текущего домена выбора находится в области MSTP моста. (Только для экземпляров CIST).
Internal path cost	Стоимость пути к корню зоны. Для корневых мостов доменов это ноль. Это сумма стоимости внутренних портов на пути наименьшей стоимости к внутреннему корневому мосту для всех остальных экземпляров CIST в том же MSTP домене. (Только для экземпляров CIST).
Topology change flag	Текущее состояние флага изменения топологии для этого экземпляра моста.
Number of topology changes	Количество раз (в интервалах одной секунды), когда устанавливается флаг изменения топологии.
Last change time of topology	Время с момента последнего изменения топологии.
<b>CIST port and aggregation status</b>	<b>Статус порта и агрегации CIST</b>
Port	Номер порта коммутатора.
Port ID	ID порта, используемый протоколом STP. Это часть приоритета и логический индекс порта моста.
Role	Текущая роль порта STP. Роль порта может быть одной из следующих значений: порт замещения, резервный порт, корневой порт, определенный порт.
Status	Текущий статус порта STP. Статус порта может быть одним из следующих значений: блокировка, обучение и пересылка.
Path cost	Текущая стоимость пути порта STP. Это либо автоматически вычисленное значение, либо любое явно настроенное значение.
Edge	Текущий флаг краевого порта (операционный) порта STP. Краевой порт - это порт коммутатора, который не является мостом. Этот флаг может быть автоматически вычислен или настроен явно. Каждый крайевой порт напрямую переходит в состояние пересылки, поскольку он не может участвовать в петле.

Параметр	Описание
Peer-to-peer network connection	Текущий флаг соединения точка-точка порта STP. Порты точка-точка подключаются к неделимым средам LAN. Этот флаг может быть автоматически вычислен или настроен явно. Точка-точка характер соединения порта влияет на то, насколько быстро он переходит в состояние STP.
Status update time	Время с момента последней инициализации порта моста.

## 5.2.7 Статус порта

На странице "Статус порта STP", отображенной на рисунке ниже, отображается информация о состоянии каждого порта в экземпляре CIST, включая информацию о роли CIST, статусе CIST и время работы.

**STP Port Status** Auto-refresh  [Refresh](#)

Port	CIST Role	CIST State	Uptime
1	Non-STP	Forwarding	-
2	Non-STP	Forwarding	-
3	Non-STP	Forwarding	-
4	Non-STP	Forwarding	-
5	Non-STP	Forwarding	-
6	Non-STP	Forwarding	-
7	Non-STP	Forwarding	-
8	Non-STP	Forwarding	-
9	Non-STP	Forwarding	-
10	Non-STP	Forwarding	-
11	Non-STP	Forwarding	-
12	Non-STP	Forwarding	-
13	Non-STP	Forwarding	-
14	Non-STP	Forwarding	-
15	Non-STP	Forwarding	-
16	Non-STP	Forwarding	-
17	Non-STP	Forwarding	-
18	Non-STP	Forwarding	-
19	Non-STP	Forwarding	-
20	Non-STP	Forwarding	-
21	Non-STP	Forwarding	-
22	Non-STP	Forwarding	-
23	Non-STP	Forwarding	-
24	Non-STP	Forwarding	-
25	Non-STP	Forwarding	-
26	Non-STP	Forwarding	-
27	Non-STP	Forwarding	-
28	Non-STP	Forwarding	-
29	Non-STP	Forwarding	-
30	Non-STP	Forwarding	-
31	Non-STP	Forwarding	-
32	Non-STP	Forwarding	-
33	Non-STP	Forwarding	-
34	Non-STP	Forwarding	-
35	Non-STP	Forwarding	-
36	Non-STP	Forwarding	-

Таблица ниже описывает каждый элемент параметров

Параметр	Описание
Port	Номер порта коммутатора.
CITS roles	Текущая роль порта CIST в протоколе STP. Роль порта может быть одной из следующих: резервный порт, резервный порт, корневой порт, назначенный порт и отключенный порт.
CITS status	Текущий статус порта CIST в протоколе STP. Статус порта может быть одним из следующих: блокирующий, обучающий и перенаправляющий.
Status update time	Время с момента последней инициализации порта моста.

## 5.2.8 Статистика порта

Показана статистика пакетов STP для портов в таблице ниже. Эта страница используется для отображения количества принятых, отправленных и отброшенных пакетов STP для каждого порта.

STP Statistics										Auto-refresh <input type="checkbox"/>	Refresh	Clear
Port	Transmitted				Received				Discarded			
	MSTP	RSTP	STP	TCN	MSTP	RSTP	STP	TCN	Unknown	Illegal		
<i>No ports enabled</i>												

Таблица ниже описывает каждый элемент параметров

Параметр	Описание
Port	Номер порта коммутатора.
Send/receive	<ul style="list-style-type: none"> <li>MSTP: Количество MSTP BPDUs, полученных/отправленных через порт.</li> <li>RSTP: Количество RSTP BPDUs, полученных/отправленных через порт.</li> <li>STP: Количество BPDUs с настройками стандартного STP, полученных/отправленных через порт.</li> <li>TCN: Количество BPDUs оповещения об изменении топологии (TCN), полученных/отправленных через порт.</li> </ul>
Throw away	<ul style="list-style-type: none"> <li>Unknown packets: Количество неизвестных BPDUs о связующем дереве, полученных (и отброшенных) на порту.</li> <li>Illegal messages: Количество недопустимых BPDUs о связующем дереве, полученных (и отброшенных) на порту.</li> </ul>

## 5.3 Обнаружение петель

Для своевременного обнаружения петель в сети уровня 2 и предотвращения серьезных последствий для всей сети используется технология обнаружения обратных петель. Эта технология позволяет немедленно уведомлять пользователей о необходимости проверки сетевого соединения и конфигурации при возникновении петли в сети, а также выявлять проблему. Интерфейс помещается в определенное управляемое состояние.

Технология обнаружения петель периодически отправляет специальное сообщение обнаружения с интерфейса, а затем проверяет, вернулось ли сообщение обратно на устройство (это не требует, чтобы интерфейсы приема и отправки были одним и тем же интерфейсом), а затем определяет сеть или устройство, подключенное к интерфейсу и устройство. И наличие петли между двойными интерфейсами устройства:

- ◆ Если обнаружено, что обнаруживаемые пакеты получены с исходящего интерфейса, считается, что на интерфейсе произошла собственная петля или есть петля в сети или устройстве, подключенном к интерфейсу.
- ◆ Если обнаружено, что пакет обнаружения получен другими интерфейсами на устройстве, считается, что в сети, где находится интерфейс, есть петля, или устройство самоповторяется.

После обнаружения петли устройство регистрирует журнал и выполняет определенные действия по обработке петли (так называемые действия по обработке петли) на проблемном интерфейсе в соответствии с предварительной конфигурацией пользователя, тем самым удерживая интерфейс под контролем и уменьшая влияние петли на устройство и даже на сеть.

После того как интерфейс будет управляемым, он автоматически вернется в нормальное состояние после установленного времени управления и продолжит отправлять пакеты обнаружения. Когда устройство не получает пакеты обнаружения, отправленные интерфейсом, в течение определенного времени, петля считается устраненной. Этот процесс называется автоматическим восстановлением управляемого интерфейса..

### 5.3.1 Конфигурация обнаружения петель

Общая конфигурация и конфигурация порта обнаружения петель, как показано на рисунке ниже

### Loop Protection Configuration

General Settings

Global Configuration

<b>Enable Loop Protection</b>	Disable ▾	
<b>Transmission Time</b>	5	seconds
<b>Shutdown Time</b>	180	seconds

Port Configuration

Port	Enable	Action	Tx Mode
*	<input checked="" type="checkbox"/>	<> ▾	<> ▾
1	<input checked="" type="checkbox"/>	Shutdown Port ▾	Enable ▾
2	<input checked="" type="checkbox"/>	Shutdown Port ▾	Enable ▾
3	<input checked="" type="checkbox"/>	Shutdown Port ▾	Enable ▾
4	<input checked="" type="checkbox"/>	Shutdown Port ▾	Enable ▾
5	<input checked="" type="checkbox"/>	Shutdown Port ▾	Enable ▾
6	<input checked="" type="checkbox"/>	Shutdown Port ▾	Enable ▾
7	<input checked="" type="checkbox"/>	Shutdown Port ▾	Enable ▾
8	<input checked="" type="checkbox"/>	Shutdown Port ▾	Enable ▾
9	<input checked="" type="checkbox"/>	Shutdown Port ▾	Enable ▾
10	<input checked="" type="checkbox"/>	Shutdown Port ▾	Enable ▾
11	<input checked="" type="checkbox"/>	Shutdown Port ▾	Enable ▾
12	<input checked="" type="checkbox"/>	Shutdown Port ▾	Enable ▾
13	<input checked="" type="checkbox"/>	Shutdown Port ▾	Enable ▾
14	<input checked="" type="checkbox"/>	Shutdown Port ▾	Enable ▾
15	<input checked="" type="checkbox"/>	Shutdown Port ▾	Enable ▾

Таблица ниже описывает каждый элемент параметров

Параметр	Описание
<b>Common configuration</b>	<b>Общая конфигурация</b>
Loopback detection Enabled	Переключатель общего включения обнаружения петель.
Detection interval	Период обнаружения сообщений об обнаружении петель.
Controlled recovery time	Время восстановления для перевода порта в управляемое состояние отключения.
<b>Port configuration</b>	<b>Конфигурация порта</b>
Port	Указывает, что порт нужно настроить.
Enable	Если отмечено, это означает включение функции обнаружения петель на этом порту. Первая строка представляет собой пакетную конфигурацию, выберите все или не выбирайте все.
Controlled state	Действия, выполняемые управляемым портом при обнаружении петли. <ul style="list-style-type: none"> <li>• Закрыть порт: означает закрытие порта.</li> </ul>

Параметр	Описание
	<ul style="list-style-type: none"> <li>Закрыть порт и записать журналы: означает закрытие порта и запись журналов.</li> <li>Только записать журналы: означает, что записываются только журналы.</li> </ul>
Send detection message	Переключатель для разрешения порту отправки пакетов обнаружения обратной петли



Уведомление:

Функция обнаружения обратной петли действует только при включенном общем переключателе обнаружения обратной петли.

Если контролируемое состояние включает запись журнала (Log), при обнаружении портом наличия петли можно посмотреть соответствующий журнал обнаружения обратной петли в информации журнала.

### 5.3.2 Статус обнаружения петли

Используется для просмотра информации о статусе обнаружения петель.

Loop Protection Status							Auto-refresh <input type="checkbox"/>	Refresh
Port	Action	Transmit	Loops	Status	Loop	Time of Last Loop		
No ports enabled								

Таблица ниже описывает каждый элемент параметров

Параметр	Описание
Port	Представьте список портов.
Controlled port	Контролируемые действия для настройки порта: <ul style="list-style-type: none"> <li>Отключение: указывает на закрытие порта</li> <li>Отключение + журнал: означает закрытие порта и запись журнала</li> <li>Только журнал: указывает на запись только в журнал</li> </ul>
Send detection message	Порт включен для отправки пакетов обнаружения обратного петли.
Detect loopback times	Количество обнаруженных петель на порту после включения функции обнаружения обратной петли.

Параметр	Описание
Port status	Текущий статус порта. <ul style="list-style-type: none"> <li>Отключен: означает, что порт закрыт.</li> <li>Вверх: указывает на поднятое соединение порта.</li> <li>Вниз: указывает на отключенное соединение порта.</li> </ul>
Current loopback status	Укажите, обнаружен ли в текущем порту кольцевой обрыв. <ul style="list-style-type: none"> <li>Кольцо: указывает на наличие кольцевого обрыва</li> <li>-: указывает на отсутствие кольца</li> </ul>
The time when the loopback was last detected	Последнее время обнаружения кольцевого обрыва на порту.



**Уведомление:**

Функция обнаружения обратного замыкания представляет собой лишь технологию обнаружения одиночного узлового замыкания и не обладает функцией разрыва замкнутых цепей на сетевом уровне.

Состояние кольца не обновляется до следующего цикла обнаружения после завершения контролируемого состояния.

## 6 Характеристики уровня 3

### 6.1 Управление IP

#### 6.1.1 Конфигурация IP

Функции управления IP включают настройку режима хоста и маршрутизации, управление IP-интерфейсами, статическую маршрутизацию и DNS и т. д.

IP Configuration

Domain Name: [No Domain Name] [v]

Mode: [Host] [v]

DNS Server 0: [No DNS server] [v]

DNS Server 1: [No DNS server] [v]

DNS Server 2: [No DNS server] [v]

DNS Proxy:

IP Interfaces

Delete	IF	Enable	DHCPv4				Hostname	Fallback	Current Lease	IPv4		DHCPv6			IPv6	
			Type	IFMac	Client ID	Client ID				Address	Mask Length	Enable	Rapid Commit	Current Lease	Address	Mask Length
<input type="checkbox"/>	VLAN 1	<input type="checkbox"/>	Auto	[v]	Port 1	[v]		0		192.168.16.253	24	<input type="checkbox"/>	<input type="checkbox"/>			

Add Interface

IP Routes

Delete	Network	Mask Length	Gateway	Next Hop VLAN (IPv6)	Distance
<input type="checkbox"/>					

Add Route

Save Reset

Таблица ниже описывает каждый элемент параметров:

Параметр	Описание
<b>IP configuration</b>	<b>IP конфигурация</b>
Domain name	<p>Настройте локальное доменное имя, включая следующие режимы:</p> <ul style="list-style-type: none"> <li>Без доменного имени: Не использовать доменное имя, режим по умолчанию.</li> <li>Настроенное доменное имя: Настройте указанное доменное имя. Убедитесь, что настроенное доменное имя соответствует предоставленному доменному имени вашей организации.</li> <li>С любых интерфейсов DHCPv4: Используйте первое предоставленное доменное имя из аренды DHCPv4 для интерфейса, включенного в DHCPv4.</li> <li>С этого интерфейса DHCPv4: Укажите, с какого интерфейса DHCPv4 предпочтительно использовать предоставленное доменное имя.</li> <li>С любых интерфейсов DHCPv6: Используйте первое предоставленное доменное имя из аренды DHCPv6 для интерфейса, включенного в DHCPv6.</li> </ul>

Параметр	Описание
	<ul style="list-style-type: none"> <li>С этого интерфейса DHCPv6: Укажите, с какого интерфейса DHCPv6 предпочтительно использовать предоставленное доменное имя.</li> </ul>
Mode	<p>Настройте устройство на работу в режиме "Хост" или "Маршрутизатор".</p> <ul style="list-style-type: none"> <li>Хост: В режиме хоста IP-трафик между интерфейсами не будет маршрутизироваться.</li> <li>Маршрутизатор: В режиме маршрутизатора трафик маршрутизируется и пересылается между всеми интерфейсами.</li> </ul>
DNS server 0-2	<p>Настройте сервер доменных имен (DNS), включая следующие режимы:</p> <ul style="list-style-type: none"> <li>Без сервера доменных имен: Не использовать сервер доменных имен.</li> <li>Настроенный IPv4 или IPv6: Настройте сервер доменных имен IPv4 или IPv6.</li> <li>С любых интерфейсов DHCPv4: Используйте первый сервер доменных имен, предоставленный с арендой DHCPv4 для интерфейса, включенного в DHCPv4.</li> <li>С этого интерфейса DHCPv4: Укажите, с какого интерфейса DHCPv4 предпочтительно использовать предоставленный сервер доменных имен</li> <li>С любых интерфейсов DHCPv6: Используйте первый сервер доменных имен, предоставленный с арендой DHCPv6 для интерфейса, включенного в DHCPv6.</li> <li>С этого интерфейса DHCPv6: Укажите, с какого интерфейса DHCPv6 предпочтительно использовать предоставленный сервер доменных имен.</li> </ul>
DNS proxy	<p>После включения функции прокси-сервера DNS система будет перенаправлять запросы DNS на текущий настроенный DNS-сервер и отвечать клиентским устройствам в сети как резолвер DNS.</p> <p>Примечание: В настоящее время поддерживаются только прокси-серверы DNS IPv4.</p>
IP interface	<b>IP-интерфейс</b>
Delete	Удалить выбранный IP-интерфейс.

Параметр	Описание
Interface	VLAN, связанный с IP-интерфейсом. Только порты в этом VLAN могут получать доступ к этому IP-интерфейсу. Это поле доступно только при создании нового интерфейса. Формат ввода должен быть "VLAN 2".
<b>DHCPv4</b>	<b>Настроить DHCPv4 на интерфейсе.</b>
Enable	Включить DHCPv4.
Client ID	<p>Выберите тип клиентского IP, включая режимы IfMac, ASCII и HEX.</p> <ul style="list-style-type: none"> <li>IfMac: Используя имя интерфейса в качестве идентификатора, поле DHCP option61 будет использовать аппаратный MAC-адрес интерфейса.</li> <li>ASCII: Используйте ASCII-код в качестве идентификатора, и поле DHCP option61 будет использовать ASCII-строку.</li> <li>HEX: Используйте шестнадцатеричное число в качестве идентификатора, и поле DHCP option61 будет использовать шестнадцатеричную строку.</li> </ul>
Host name	Имя хоста DHCP-клиента. Если DHCPv4-клиент включен, поле DHCP option12 будет использовать настроенное имя хоста. Когда значение является пустой строкой, это поле использует настроенное системное имя плюс последние 3 байта MAC-адреса системы в качестве имени хоста.
Fallback time	Время (в секундах) для получения аренды DHCP. После истечения времени ожидания настроенный IPv4-адрес будет использоваться в качестве IPv4-адреса интерфейса. Значение 0 отключает механизм возврата, чтобы DHCP продолжал повторять попытки до получения действительной аренды. Допустимый диапазон значений: от 0 до 4294967295 секунд.
Current rental address	Отображает адрес интерфейса, предоставленный DHCPv4-сервером.
<b>IPv4</b>	<b>Настройка статического IPv4-адреса на интерфейсе.</b>
Address	Настройка IPv4-адреса интерфейса в десятичной точечной нотации. Если включен DHCP, настройте резервный адрес в этом поле.
Mask length	Настройка маски сети IPv4 интерфейса, выраженной в битах (длине префикса). Если включен DHCP, это поле настраивает маску сети резервного адреса.
<b>DHCPv6</b>	<b>Настройте DHCPv6 на интерфейсе.</b>
Enable	Включите DHCPv6.
Quick allocation	Включите механизм быстрого выделения DHCPv6. После его включения клиент DHCPv6 немедленно завершит процесс ожидания после получения сообщения Reply с опцией быстрого выделения.

Параметр	Описание
Current rental address	Отображает адрес интерфейса, предоставленный DHCPv6-сервером.
<b>IPv6</b>	<b>Настройка статического IPv6-адреса на интерфейсе.</b>
Address	Настройка IPv6-адреса интерфейса.
Mask length	Настройка маски сети IPv6 интерфейса, выраженной в битах (длине префикса).
Add interface	Щелкните кнопку "Добавить интерфейс", чтобы создать IP-интерфейс.
<b>IP routing</b>	<b>Статическая IP-маршрутизация</b>
Delete	Удалить указанную запись статического маршрута.
Network	Адрес сети или хоста маршрута назначения IP. Допустимые форматы - десятичная точечная или допустимая запись IPv6. Маршрут по умолчанию может быть представлен как 0.0.0.0 или IPv6::.
Mask length	Маска сети или хоста маршрута назначения IP, выраженная в битах (длине префикса).
Gateway	Адрес шлюза, допустимый формат - десятичная точечная или допустимая запись IPv6.
Next hop VLAN (IPv6)	Идентификатор VLAN (VID) IPv6-интерфейса, связанного с шлюзом. Диапазон значений VID составляет от 1 до 4095 и действителен только при наличии соответствующего IPv6-интерфейса. Если IPv6-адрес шлюза - локальный для сети, необходимо указать VLAN следующего перехода для шлюза. Если IPv6-адрес шлюза не локальный для сети, VLAN следующего перехода для этого шлюза игнорируется.
Distance	Используется для предоставления информации о приоритете маршрутизационного протокола маршрутизаторам. При участии двух или более различных протоколов маршрутизации и при совпадении пункта назначения можно использовать значение расстояния для выбора наилучшего пути.
Add route	Нажмите кнопку "Добавить маршрут", чтобы создать запись статического маршрута.

## 6.1.2 IP информация

Страница информации об IP в основном используется для отображения настроенной информации об IP-интерфейсах, информации о маршрутизации IP, информации о соседях и т.д.

**IP Interfaces** Auto-refresh

Interface	Type	Address	Status
VLAN 1	LINK	4c-93-a6-c4-14-c0	<UP BROADCAST MULTICAST>
VLAN 1	IPv4	192.168.16.253/24	
VLAN 1	IPv6	fe80::4e93:a6ff:fec4:14c0/64	

**IP Routes**

IPv4

Network	Gateway	Status
192.168.16.0/24	VLAN 1	<UP>

IPv6

Network	Gateway	Status
fe80::/64	VLAN 1	<UP>

**Neighbor cache**

IPv4

IP Address	Link Address
192.168.16.250	VLAN 1:a8-5e-45-18-09-e2

IPv6

IP Address	Link Address
------------	--------------

Таблица ниже описывает каждый элемент параметров

Параметр	Описание
<b>IP interface</b>	<b>Отобразить информацию о конфигурации и статусе IP-интерфейса:</b>
Interface	Имя интерфейса.
Type	Тип адреса интерфейса, включая LINK, IPv4 и IPv6.
Address	Текущий адрес интерфейса.
Status	Текущий статус интерфейса.
<b>IP routing</b>	<b>Отобразить информацию о маршрутизации IPv4 и IPv6:</b>
Website address	Назначенный IPv4/IPv6 сетевой адрес или адрес хоста маршрута.
Gateway address	Адрес шлюза маршрута.
Status	Текущий статус маршрута.
<b>Neighbor information</b>	<b>Отобразить информацию о соседях IPv4 и IPv6:</b>
IP address	IP-адрес соседа.
Neighbor address	MAC-адрес, соответствующий IP-адресу соседа.

### 6.1.3 Таблица маршрутизации IPv4

Эта страница в основном отображает записи таблицы маршрутизации IPv4 устройства.

**Routing Information Base** 1 - 1 of 1 entry Auto-refresh  Refresh << << >> >>

Start from Network  /  Protocol  NextHop  with  entries per page.

Codes: C - connected, S - static, O - OSPF, R - RIP, \* - selected route, D - DHCP installed route

Protocol	Network/Prefix	NextHop	Distance	Metric	Interface	Uptime (hh:mm:ss)	State
C *	192.168.16.0/24	-	-	-	VLAN 1	00:41:05	Active

Таблица ниже описывает каждый элемент параметров:

Параметр	Описание
Protocol	Тип протокола маршрутизации, включая Connected, Static, RIP, DHCP, OSPF и *.
Network address/prefix	Назначенный IPv4/IPv6 сетевой адрес или адрес хоста и длина маски маршрута.
Next hop	Адрес следующего перехода.
Distance	Расстояние маршрутизации.
Hops	Количество переходов маршрута.
Interface	VLAN маршрутизируемого интерфейса.
Operation hours	Продолжительность после установления маршрута.
Status	Статус маршрутизации.
Refresh	Выберите начальный адрес маршрутизации/длину маски, тип протокола, адрес следующего перехода, количество записей, отображаемых на каждой странице, и другие правила, и нажмите "Обновить", чтобы отобразить соответствующие записи.

### 6.1.4 Таблица маршрутизации IPv6

Эта страница в основном отображает записи таблицы маршрутизации IPv6 устройства, как показано на рисунке ниже.

**Routing Information Base** 1 - 1 of 1 entry Auto-refresh  Refresh << << >> >>

Start from Network  /  Protocol  NextHop  with  entries per page.

Codes: C - connected, S - static, O - OSPF, R - RIP, \* - selected route, D - DHCP installed route

Protocol	Network/Prefix	NextHop	Distance	Metric	Interface	Uptime (hh:mm:ss)	State
C *	fe80::/64	-	-	-	VLAN 1	00:47:39	Active

Таблица ниже описывает каждый элемент параметров:

Параметр	Описание
Protocol	Тип протокола маршрутизации, включая Connected, Static, RIP, DHCP, OSPF и *.
Network address/prefix	Назначенный IPv4/IPv6 сетевой адрес или адрес хоста и длина маски маршрута.
Next hop	Адрес следующего перехода.
Distance	Расстояние маршрутизации.
Hops	Количество переходов маршрута.
Interface	VLAN маршрутизируемого интерфейса.
Operation hours	Продолжительность после установления маршрута.
State	Статус маршрутизации.
Refresh	Выберите начальный адрес маршрутизации/длину маски, тип протокола, адрес следующего перехода, количество записей, отображаемых на каждой странице, и другие правила, и нажмите "Обновить", чтобы отобразить соответствующие записи.

## 6.2 RIP

RIP (Routing Information Protocol) - это относительно простой внутренний протокол шлюза. Он основан на алгоритме Distance-Vector, который использует количество прыжков (Hop Count) в качестве метрики для измерения расстояния до сети назначения.

### 6.2.1 Глобальная конфигурация

Эта страница настраивает глобальные параметры протокола RIP, как показано на рисунке ниже.

### RIP Global Configuration Clear RIP Process

RIP Router Mode		Disable
Version		Default
Timers	Update	30
	Invalid	180
	Garbage-Collection	120
Redistribute	Static	Mode: Disable
		Metric Value: <input checked="" type="radio"/> Auto <input type="radio"/> Specific <input type="text" value="1"/>
	Connected	Mode: Disable
		Metric Value: <input checked="" type="radio"/> Auto <input type="radio"/> Specific <input type="text" value="1"/>
	OSPF	Mode: Disable
		Metric Value: <input checked="" type="radio"/> Auto <input type="radio"/> Specific <input type="text" value="1"/>
Default Metric Value		1
Default Route		Disable
Default Passive Mode		Disable
Administrative Distance		120

Таблица ниже описывает каждый элемент параметров:

Параметр	Описание
RIP mode	Включить или отключить функцию маршрутизации RIP. По умолчанию она отключена.
Version	<p>Настройте версию протокола RIP, включая Default, RIPv1 и RIPv2. По умолчанию установлено значение Default. Методы обработки для каждой версии, следующие:</p> <ul style="list-style-type: none"> <li>• Версия 1: Основана на версии V1, только принимает и отправляет сообщения RIPv1.</li> <li>• Версия 2: Основана на версии V2, только принимает и отправляет сообщения RIPv2.</li> <li>• Default: Основана на версии по умолчанию, маршрутизатор отправляет сообщения RIPv2 и одновременно принимает сообщения RIPv1 и RIPv2. Когда маршрутизатор получает запрос или обновление триггера для любой версии, он отвечает соответствующей версией.</li> </ul>
Timer	<p>Настройка различных таймеров включает:</p> <ul style="list-style-type: none"> <li>• Таймер обновления (Update timer): интервал таймера (в секундах) для отправки полной таблицы маршрутизации всем смежным устройствам RIP. Диапазон от 5 до 2147483 секунд, по умолчанию 30 секунд.</li> </ul>

Параметр	Описание
	<ul style="list-style-type: none"> <li>• Таймер старения (Aging timer): если устройство RIP не получает сообщение об обновлении маршрута от соседа в течение времени старения, оно будет считать маршрут недоступным. Диапазон от 5 до 2147483 секунд, по умолчанию 180 секунд.</li> <li>• Таймер сбора мусора (Garbage collection timer): если недоступный маршрут не получает сообщение об обновлении от того же соседа до окончания таймера сбора мусора, маршрут будет полностью удален из таблицы маршрутизации RIP. Диапазон от 5 до 2147483 секунд, по умолчанию 120 секунд.</li> </ul>
Route introduction	<p>RIP может внедрять информацию о маршрутизации, полученную от других протоколов, для обогащения записей в таблице маршрутизации, включая прямые маршруты, статические маршруты и протокол OSPF.</p> <ul style="list-style-type: none"> <li>• Статическая маршрутизация: Настройте протокол RIP для внедрения записей статической маршрутизации.             <ol style="list-style-type: none"> <li>1. Режим: Включение или отключение внедрения записей статических маршрутов.</li> <li>2. Значение метрики: Настройка значения метрики для внедряемых статических маршрутов. Режим "Auto" использует значение метрики по умолчанию, а режим "Specific" использует указанное значение метрики. Диапазон значений от 1 до 16, по умолчанию 1.</li> </ol> </li> <li>• Прямая маршрутизация: Настройте протокол RIP для внедрения записей прямой маршрутизации.             <ol style="list-style-type: none"> <li>1. Режим: Включение или отключение внедрения записей прямых маршрутов.</li> <li>2. Значение метрики: Настройка значения метрики для внедряемых прямых маршрутов. Режим "Auto" использует значение метрики по умолчанию, а режим "Specific" использует указанное значение метрики. Диапазон значений от 1 до 16, по умолчанию 1.</li> </ol> </li> <li>• Маршрутизация OSPF: Настройте протокол RIP для внедрения записей маршрутизации OSPF.             <ol style="list-style-type: none"> <li>1. Режим: Включение или отключение внедрения записей маршрутизации OSPF.</li> <li>2. Значение метрики: Настройка значения метрики для внедряемых маршрутов OSPF. Режим "Auto" использует значение метрики по умолчанию, а режим "Specific"</li> </ol> </li> </ul>

Параметр	Описание
	использует указанное значение метрики. Диапазон значений от 1 до 16, по умолчанию 1. <ul style="list-style-type: none"> <li>Значение метрики по умолчанию: если не указано конкретное значение для типа внедряемого маршрута, это значение по умолчанию используется в качестве метрики внедряемого маршрута. Диапазон значений от 1 до 16, по умолчанию 1.</li> <li>Реклама маршрута по умолчанию: Включение или отключение рекламы маршрутов по умолчанию RIP.</li> </ul>
Default passive mode	По умолчанию все интерфейсы настроены как пассивные интерфейсы.
administrative distance	Дистанция управления RIP. Допустимый диапазон - от 1 до 255.
Clear RIP process	Нажмите кнопку "Очистить процесс RIP", чтобы очистить статистику счетчиков, поддерживаемую процессом RIP.

## 6.2.2 Конфигурация сети

На этой странице настройки сети RIP используются для указания интерфейса, на котором включен RIP. Когда RIP включен на определенных интерфейсах, информация о маршрутизации может быть отправлена другим устройствам RIP через эти интерфейсы.

**RIP Network Configuration**

Delete	Network Address	Mask Length
*	*	
No entry exists		

Таблица ниже описывает каждый элемент параметров:

Параметр	Описание
Delete	Удалить запись.
Website address	Адрес интерфейса, на котором включен RIP.
Mask length	Длина маски адреса интерфейса, включенного для RIP

### 6.2.3 Конфигурация соседей

На этой странице настраиваются соседи RIP. Если RIP работает на канале, который не поддерживает широковещательные или многоадресные пакеты, необходимо вручную указать соседей RIP. По истечении времени таймера обновления указанный сосед будет отправлен на указанный канал через одноадресную передачу, широковещательную передачу или сетевой адрес. Соседи отправляют сообщения об обновлении RIP.

**RIP Neighbor Configuration**

Delete	Neighbor Address
*	
No entry exists	

Таблица ниже описывает каждый элемент параметров:

Параметр	Описание
Delete	Удалить запись.
Neighbor address	IP-адрес интерфейса соседа, который может быть одноадресным (за исключением петлевого), широковещательным или сетевым IP-адресом.

### 6.2.4 Пассивный интерфейс

Это таблица конфигурации интерфейса маршрутизатора RIP.

**RIP Passive Interface Configuration**

Interface	Passive Interface
*	
No entry exists	

Таблица ниже описывает каждый элемент параметров:

Параметр	Описание
Interface	Имя интерфейса
Passive interface	Настройка интерфейса в пассивном режиме.

## 6.2.5 Конфигурация интерфейса

This page configures the RIP features of the interface, including packet sending and receiving types, split horizon, poison reversal, packet authentication, etc.

RIP Interface Configuration						
Interface	Send Version	Receive Version	Split Horizon Mode	Auth. Type	Change Simple Password / Key-Chain Name	
*	<>	<>	<>	<>	*	*
VLAN 1	Not Specified	Not Specified	Split Horizon	Null Authentication	<input type="checkbox"/>	

Save Reset

Таблица ниже описывает каждый элемент параметров:

Параметр	Описание
Interface	Имя интерфейса
Send message version	Версия пакетов RIP, отправляемых интерфейсом, включает: <ul style="list-style-type: none"> <li>Версия 1: RIPv1</li> <li>Версия 2: RIPv2</li> <li>Версия 1 и 2: RIPv1 и RIPv2</li> <li>Не указано: Не указано</li> </ul>
Receive message version	Версия пакетов RIP, принимаемых интерфейсом, включает: <ul style="list-style-type: none"> <li>Версия 1: RIPv1</li> <li>Версия 2: RIPv2</li> <li>Версия 1 и 2: RIPv1 и RIPv2</li> <li>Не указано: Не указано</li> <li>Нет: Не принимать</li> </ul>
Split Horizontally	Настройте интерфейс для включения или отключения функций "горизонтального разделения" и "отравленного обратного хода", включая: <ul style="list-style-type: none"> <li>Split Horizon: включить горизонтальное разделение</li> <li>Poisoned Reverse: включить отмену отравления</li> <li>Disable: ни одна функция не включена</li> </ul>
Certification type	Настройте, аутентифицирует ли интерфейс пакеты RIP и тип аутентификации, включая: <ul style="list-style-type: none"> <li>Simple Password: Простая аутентификация по паролю, используя аутентификацию в виде обычного текста, необходимо</li> </ul>

Параметр	Описание
	<p>настроить пароль, но пароль можно прочитать, перехватив пакеты.</p> <ul style="list-style-type: none"> <li>Message Digest: Аутентификация с использованием хэш-функции MD5, необходимо настроить ключевую цепочку, это более безопасный метод.</li> <li>Null Authentication: Нет аутентификации.</li> </ul>
Simple Password/Key-Chain	<p>Настройте пароль проверки, соответствующий типу аутентификации. Простой пароль заполняется обычным текстом, а допустимая длина ввода составляет от 1 до 15 печатных символов (за исключением пробельных символов). Допустимая длина ввода имени ключевой цепочки составляет от 1 до 31 печатного символа (за исключением пробельных символов). Пустая строка указывает на то, что на интерфейсе не настроен простой пароль или имя ключевой цепочки.</p> <p>Важно: Простой пароль и имя ключевой цепочки не могут быть настроены одновременно.</p>

## 6.2.6 Привязка значения метрики и фильтрация сообщений

На этой странице настраиваются функции смещения значения метрики и фильтрации пакетов при приеме и рекламе маршрутов RIP через интерфейс.

**RIP Offset-List Configuration**

Delete	VLAN ID	Direction	Access List Name	Offset Metric
*	*	*	*	*
No entry exists				

Таблица ниже описывает каждый элемент параметров:

Параметр	Описание
Delete	Удалить запись.
VLAN ID	Настроить идентификатор VLAN интерфейса. Диапазон значений идентификатора VLAN составляет от 0 до 4095, где 0 означает, что это применяется ко всем интерфейсам.

Параметр	Описание
Direction	Настроить направление, в котором выполняются операции смещения значения метрики маршрута и фильтрации пакетов на интерфейсе, включая входящий и исходящий трафик.
Access control list	Настроить списки управления доступом для фильтрации маршрутов.
Metric value append	Смещение значения метрики входящего или исходящего маршрута. Диапазон значений составляет от 0 до 16.

## 6.2.7 Глобальный статус

Эта страница отображает текущую информацию о глобальных параметрах протокола RIP.

**RIP Global Status** Clear RIP Process  Auto-refresh  Refresh

Status Information
RIP Router Mode Disabled

Таблица ниже описывает каждый элемент параметров:

Параметр	Описание
Version	<p>Настройте версию протокола RIP, включая Default, RIPv1 и RIPv2. По умолчанию установлено значение Default. Методы обработки для каждой версии следующие:</p> <ul style="list-style-type: none"> <li>RIPv1: Основан на версии V1, он принимает и отправляет только сообщения RIPv1.</li> <li>RIPv2: Основан на версии V2, он принимает и отправляет только сообщения RIPv2.</li> <li>Default: Основан на версии по умолчанию, маршрутизатор отправляет сообщения RIPv2 и одновременно принимает сообщения RIPv1 и RIPv2. Когда маршрутизатор получает запрос или обновление триггера для любой версии, он отвечает соответствующей версией.</li> </ul>
Update timer	Интервал таймера (в секундах) для отправки полной таблицы маршрутизации всем смежным устройствам RIP. Диапазон от 5 до 2147483 секунд, по умолчанию 30 секунд.
Aging timer	Если устройство RIP не получает сообщение об обновлении маршрута от соседа в течение времени старения, оно считает маршрут недоступным. Диапазон от 5 до 2147483 секунд, по умолчанию 180 секунд.
Garbage collection timer	Если недоступный маршрут не получает сообщение об обновлении от того же соседа до истечения времени сбора

Параметр	Описание
	мусора, маршрут будет полностью удален из таблицы маршрутизации RIP. Диапазон от 5 до 2147483 секунд, по умолчанию 120 секунд.
The next time to send an update	Оставшееся время до отправки следующего сообщения обновления устройством.
Route import default metric value	Если для типа внедряемого маршрута не указано конкретное значение, это значение по умолчанию используется в качестве метрики внедряемого маршрута. Диапазон значений от 1 до 16, по умолчанию 1.
Introducing direct routes	Протокол RIP внедряет прямые маршруты.
Introduce static routes	Протокол RIP внедряет статические маршруты.
Import OSPF routes	Протокол RIP внедряет маршруты OSPF.
Administrative distance	Это представляет собой значение административного расстояния.

## 6.2.8 Статус интерфейса

Эта страница отображает информацию об интерфейсе протокола RIP.

RIP Interface Status							Auto-refresh <input type="checkbox"/>	Refresh
Interface	Send Version	Receive Version	Triggered Update	Passive	Auth. Type	Key-Chain Name		
No entry exists								

Таблица ниже описывает каждый элемент параметров:

Параметр	Описание
Interface	Имя интерфейса.
Send message version	Версия пакетов RIP, отправляемых интерфейсом, включая: RIPv1, RIPv2, RIPv1 и RIPv2, не указано.
Receive message version	Версия пакетов RIP, принимаемых интерфейсом, включая: RIPv1, RIPv2, RIPv1 и RIPv2, не указано, не получено.
Trigger update	Триггер обновлений интерфейса.
Passive mode	Активен ли пассивный интерфейс.
Certification type	Настройте, аутентифицирует ли интерфейс пакеты RIP и тип аутентификации, включая: <ul style="list-style-type: none"> <li>Аутентификация по простому паролю: Использование аутентификации в виде обычного текста, необходимо настроить пароль, но пароль можно прочитать, перехватив пакеты.</li> </ul>

Параметр	Описание
	<ul style="list-style-type: none"> <li>Аутентификация с использованием хэш-функции: Аутентификация по алгоритму хэширования MD5, необходимо настроить ключевую цепочку, это более безопасный метод.</li> <li>Не сертифицировано.</li> </ul>
Key-Chain	Configure the Key-Chain name when the authentication type is digest authentication.

## 6.2.9 Информация о соседях

На этой странице отображается информация о соседях протокола RIP. Показываемые элементы следующие:

**RIP Peer Information** 0 - 0 of 0 entry    Auto-refresh     Refresh    <<    <<    >>    >>|

Start from Address  with  entries per page.

Gateway	Last Update Time	Version	Received Bad Packets	Received Bad Routes
No entry exists				

Таблица ниже описывает каждый элемент параметров:

Параметр	Описание
Gateway	IP-адрес интерфейса соседа, который может быть одноадресным (исключая петлевой), широковещательным или сетевым IP-адресом.
Last updated	Интервал времени (в секундах) с момента последнего полученного RIP-сообщения соседа до настоящего момента.
Version	Номер версии RIP в последнем заголовке RIP-пакета, полученного от соседа.
Number of error messages	Количество недопустимых RIP-ответных пакетов, отброшенных соседями.
Number of invalid routes	Количество недопустимых маршрутов от соседей, которые были проигнорированы.

## 6.2.10 Таблица маршрутизации

На этой странице отображается база данных с маршрутной информацией протокола RIP.

**RIP Database Information**      0 - 0 of 0 entry    Auto-refresh     Refresh    <<<    <<    >>    >>>

Start from Network  /  , Next Hop  with  entries per page.

Type	Sub-Type	Network	Next Hop	Metric	From	External Metric	Tag	Uptime
No entry exists								

Таблица ниже описывает каждый элемент параметров:

Параметр	Описание
Route type	Тип протокола маршрутизации.
Subtype	Подтип протокола маршрутизации.
Destination address	Адрес маршрута назначения и маска подсети.
Next hop	Адрес следующего перехода.
Metric	Метрика маршрута.
Source	Идентифицирует источник маршрута, который изучен или создан с локального интерфейса.
External measure	Представляет значения метрик из исходного протокола.
Mark	Метка маршрута. Используется для разделения "внутренних" маршрутов RIP, которые могут быть импортированы из EGP (Exterior Gateway Protocol) или другого IGP (Interior Gateway Protocol). Например, маршрут, импортированный из OSPF, может иметь значение метки маршрута, которое может использоваться другими протоколами маршрутизации для предотвращения повторной рекламы этого же маршрута обратно в исходный домен маршрутизации протокола.
Operation hours	Поле времени имеет смысл только в том случае, если маршрут изучен от соседей. Когда маршрут назначения доступен (его значение метрики меньше 16), это указывает на оставшееся время действительности маршрута. Когда маршрут назначения недоступен (его значение метрики больше 16), это указывает на оставшееся время сбора мусора маршрута.

## 6.3 OSPF

### 6.3.1 Глобальная конфигурация

Это таблица конфигурации маршрутизатора OSPF. Это общая группа для настройки общедоступных параметров маршрутизатора OSPF.

**OSPF Global Configuration** Clear OSPF Process

OSPF Router Mode Disable

Save Reset

Настройте режим OSPF и выберите "Включить", затем нажмите "Сохранить", и ниже появится глобальная конфигурация:

**OSPF Global Configuration** Clear OSPF Process

OSPF Router Mode		Enable
Router ID		<input checked="" type="radio"/> Auto <input type="text" value="192.168.16.253"/> <input type="radio"/> Specific <input type="text" value="0.0.0.1"/>
Default Passive Mode		False
Default Metric		<input checked="" type="radio"/> Auto <input type="radio"/> Specific <input type="text" value="0"/>
Redistribute	Static	Metric Type: None
		Metric Value: <input type="radio"/> Auto <input type="radio"/> Specific <input type="text" value="0"/>
	Connected	Metric Type: None
		Metric Value: <input type="radio"/> Auto <input type="radio"/> Specific <input type="text" value="0"/>
	RIP	Metric Type: None
		Metric Value: <input type="radio"/> Auto <input type="radio"/> Specific <input type="text" value="0"/>
Stub Router	On Startup	Mode: Disable
		Interval: <input type="text" value="5"/>
	On Shutdown	Mode: Disable
		Interval: <input type="text" value="5"/>
	Administrative Mode: Disable	
	Default Route Redistribution	Metric Type: None
Metric Value: <input type="radio"/> Auto <input type="radio"/> Specific <input type="text" value="0"/>		
Always: Disable		
Administrative Distance		<input type="text" value="110"/>

Save Reset

Таблица ниже описывает каждый элемент параметров:

Параметр	Описание
OSPF mode	Включить/отключить режим маршрутизатора OSPF
Router ID	Идентификатор маршрутизатора OSPF в формате IPv4-адреса (A.B.C.D). Когда идентификатор маршрутизатора OSPF изменяется, если в текущей области OSPF есть один или несколько полностью смежных соседей, новый идентификатор маршрутизатора вступит в силу после перезапуска процесса OSPF. Пожалуйста, обратите внимание, что идентификатор маршрутизатора должен быть уникальным в пределах автономной системы, значение "0.0.0.0" недопустимо, поскольку оно зарезервировано для алгоритма по умолчанию. <ul style="list-style-type: none"> <li>• Auto: Алгоритм по умолчанию выберет наибольший IP-адрес, назначенный маршрутизатору.</li> </ul>

Параметр	Описание
	<ul style="list-style-type: none"> <li>Specific: Идентификатор маршрутизатора, указанный пользователем. Допустимый диапазон составляет от 0.0.0.1 до 255.255.255.254.</li> </ul>
Default passive mode	<p>По умолчанию все интерфейсы настроены как пассивные интерфейсы. Когда интерфейс настроен как пассивный интерфейс, отправка обновлений маршрутизации OSPF подавляется, так что на интерфейсе не устанавливаются смежности (нет OSPF Hello). Подсети для всех интерфейсов (пассивных и активных) объявляются маршрутизаторами OSPF.</p>
Default metric	<p>Пользовательский указанный метрический параметр по умолчанию для протокола маршрутизации OSPF.</p> <ul style="list-style-type: none"> <li>Auto: Автоматически рассчитывает метрический параметр по умолчанию на основе протокола маршрутизации.</li> <li>Specific: Пользовательский указанный метрический параметр по умолчанию. Допустимый диапазон от 0 до 16777214.</li> </ul>
Route introduction-Static routing	<ul style="list-style-type: none"> <li>Тип: Тип статического маршрута, введенного OSPF. <ul style="list-style-type: none"> <li>None: Не вводить статические маршруты.</li> <li>External Type1: Статические маршруты вводятся как внешний тип 1.</li> <li>External Type2: Статические маршруты вводятся как внешний тип 2.</li> </ul> </li> <li>Значение метрики: Метрическое значение, указанное пользователем для статического маршрута. Допустимый диапазон от 0 до 16777214. <ul style="list-style-type: none"> <li>Auto: Метрическое значение импортированного статического маршрута совпадает с исходным метрическим значением.</li> <li>Specific: Метрика, указанная пользователем для статического маршрута.</li> </ul> </li> </ul>
Route introduction-Direct routing	<ul style="list-style-type: none"> <li>Тип: Тип прямого подключения к маршруту, введенного OSPF. <ul style="list-style-type: none"> <li>None: Не вводить прямые маршруты.</li> <li>External Type 1: Прямые подключенные маршруты импортируются как внешний тип 1.</li> </ul> </li> </ul>

Параметр	Описание
	<ul style="list-style-type: none"> <li>External Type 2: Прямые подключенные маршруты импортируются как внешний тип 2.</li> <li>Метрика: Пользовательский заданный параметр метрики для подключенного интерфейса. Допустимый диапазон от 0 до 16777214.</li> <li>Auto: Метрическое значение импортированного прямого маршрута совпадает с исходным метрическим значением.</li> <li>Specific: Метрика, указанная пользователем для подключенного маршрута.</li> </ul>
Stub Router-Boot process	<ul style="list-style-type: none"> <li>Режим: Настройте, действует ли устройство как маршрутизатор Stub и рекламирует ли его во время фазы запуска.</li> <li>Интервал: Пользователь указывает интервал времени (в секундах) для рекламирования себя как устройства Stub во время процесса запуска. Это действительно только тогда, когда режим процесса запуска настроен как включенный. Допустимый диапазон составляет от 5 до 86400 секунд.</li> </ul>
Stub Router-Shutdown process	<ul style="list-style-type: none"> <li>Mode: Настройте, действует ли устройство как маршрутизатор Stub и рекламирует ли его во время фазы отключения.</li> <li>Interval: Пользователь указывает интервал времени (в секундах) для рекламирования себя как устройства Stub во время процесса отключения. Это действительно только тогда, когда режим процесса отключения настроен как включенный. Допустимый диапазон составляет от 5 до 100 секунд.</li> </ul>
Stub Router-Unlimited mode	Рекламировать себя как устройство Stub на протяжении всего времени работы.
Default route import	<ul style="list-style-type: none"> <li>Тип: Тип маршрута по умолчанию, импортированный OSPF. <ul style="list-style-type: none"> <li>None: Не импортировать маршрут по умолчанию.</li> <li>External Type 1: Маршрут по умолчанию импортируется как внешний тип 1.</li> <li>External Type 2: Маршрут по умолчанию импортируется как внешний тип 2.</li> </ul> </li> <li>Значение метрики: Метрическое значение, указанное пользователем для маршрута по умолчанию. Допустимый диапазон от 0 до 16777214.</li> </ul>

Параметр	Описание
	<ul style="list-style-type: none"> <li>• Auto: Метрическое значение импортированного маршрута по умолчанию совпадает с исходным метрическим значением.</li> <li>• Specific: Метрика, указанная пользователем для маршрута по умолчанию.</li> <li>• Always: Указывает, что маршрут по умолчанию всегда рекламируется во все области, поддерживающие внешнюю маршрутизацию. В противном случае маршрутизатор будет рекламировать маршрут по умолчанию только в том случае, если рекламирующий маршрутизатор уже имеет маршрут по умолчанию.</li> </ul>
Administrative distance	Административное расстояние OSPF.
Clear OSPF process	Нажмите кнопку "Очистить процесс OSPF", чтобы очистить базу данных OSPF и перезапустить процесс маршрутизации OSPF.

### 6.3.2 Конфигурация сети

Когда OSPF включен на конкретных интерфейсах, маршрутизатор может предоставлять информацию о сети другим маршрутизаторам OSPF через эти интерфейсы..

**OSPF Network Area Configuration**

Delete	Network Address	Mask Length	Area ID
*	*	*	*
No entry exists			

Таблица ниже описывает каждый элемент параметров:

Параметр	Описание
Delete	Проверьте запись, и она будет удалена при следующем сохранении.
Website address	IPv4 адрес сети.
Mask length	Длина маски подсети IPv4.
Area ID	ID области OSPF.

### 6.3.3 Пассивный интерфейс

Когда интерфейс настроен как пассивный, отправка обновлений маршрутизации OSPF подавляется, поэтому на интерфейсе не устанавливаются смежности (нет OSPF Hellos). Подсети для всех интерфейсов (пассивных и активных) рекламируются маршрутизаторами OSPF.

**OSPF Passive Interface Configuration**

Interface	Passive Interface
*	<input type="checkbox"/>
VLAN 1	<input type="checkbox"/>

Таблица ниже описывает каждый элемент параметров:

Параметр	Описание
Interface	Идентификатор интерфейса.
Passive interface	Сделать этот интерфейс пассивным для OSPF.

### 6.3.4 Конфигурация зоны

Это таблица конфигурации области Stub. Эта конфигурация используется для уменьшения размера базы данных состояния связи (LSA), отключая определенные LSA, тем самым снижая требования к памяти и процессору.

**OSPF Area Stub Configuration**

Delete	Area ID	Stub Type	No Summary	Translator Role
*	No entry exists			

Таблица ниже описывает каждый элемент параметров:

Параметр	Описание
Delete	Проверьте запись, и она будет удалена при следующем сохранении.
Area ID	ID области OSPF.
Area type	Тип конфигурации области OSPF Stub.

Параметр	Описание
	<ul style="list-style-type: none"> <li>Stub Area: Настройка этой области как области Stub.</li> <li>NSSA: Настройка этой области как области NSSA.</li> </ul>
Totally mode	Настройте, является ли устройство полностью областью Stub (Totally Stub) или полностью областью NSSA (Totally NSSA)
LSA conversion	<p>Перевод LSA для области NSSA OSPF.</p> <ul style="list-style-type: none"> <li>Candidate: Маршрутизатор NSSA-ABR выполняет преобразование LSA после выборов.</li> <li>Never: Маршрутизатор NSSA-ABR никогда не выполняет преобразование LSA.</li> <li>Always: Маршрутизатор NSSA-ABR всегда выполняет преобразование LSA.</li> </ul>

### 6.3.5 Региональная сертификация

Это таблица конфигурации аутентификации области OSPF. Она используется для применения аутентификации ко всем интерфейсам, принадлежащим этой зоне.

**OSPF Area Authentication Configuration**

Delete	Area ID	Auth. Type
*		
No entry exists		

Таблица ниже описывает каждый элемент параметров:

Параметр	Описание
Delete	Проверьте запись, и она будет удалена при следующем сохранении.
Area ID	ID области OSPF
Certification type	Тип аутентификации в зоне применяется ко всем интерфейсам, принадлежащим этой зоне. Тип аутентификации на IP-интерфейсе или виртуальном канале заменяет тип аутентификации в зоне, что полезно, если различные интерфейсы в одной и той же зоне

Параметр	Описание
	используют разные типы аутентификации. Укажите тип аутентификации. <ul style="list-style-type: none"> <li>• Простой пароль: Простая проверка пароля.</li> <li>• Хеш-код сообщения: Аутентификация хеш-кодом MD5.</li> </ul>

### 6.3.6 Региональный охват

Область действия OSPF в основном используется для агрегации маршрутов и подавления их рекламы. Она агрегирует некоторые непрерывные сегменты сети в области и публикует их в других областях через Summary LSA (тип 3) или настраивает статус на "не рекламировать" для подавления Summary LSA (тип 3). Применяется к маршрутизатору границы области (ABR), где могут быть агрегированы только LSA маршрутизатора (тип 1) и LSA сети (тип 2). Поскольку область действия LSA внешних маршрутов AS (тип 5) - это автономная система OSPF, ее нельзя агрегировать. LSA внешних маршрутов NSSA (тип 7) не могут быть агрегированы, потому что эта функция в настоящее время не поддерживается.

**OSPF Area Range Configuration**

Delete	Area ID	Network Address	Mask Length	Advertise	Cost
	*	*	*		
No entry exists					

Таблица ниже описывает каждый элемент параметров:

Параметр	Описание
Delete	Проверьте запись, и она будет удалена при следующем сохранении.
Area ID	ID области OSPF.
Website address	IPv4 сетевой адрес.
Mask length	Длина маски IPv4 подсети.
Notice	После проверки маршрут будет агрегирован и опубликован в других областях. В противном случае он будет подавлен, и LSA не будет отправлен в другие области.
Overhead	Специфицированная пользователем стоимость агрегированного маршрута.

### 6.3.7 Конфигурация интерфейса

Это таблица параметров конфигурации интерфейса.

OSPF Interface Configuration										
Interface	Priority	Cost	FastHelloPackets	Interval			Auth. Type	Change Simple Password	MD Key	
				Hello	Dead	Retransmit				
*	1	<>	<input type="checkbox"/>	2	10	40	5	<>	*	*
VLAN 1	1	Auto	<input type="checkbox"/>	2	10	40	5	Area Configuration	<input type="checkbox"/>	

Save Reset

Таблица ниже описывает каждый элемент параметров:

Параметр	Описание
Interface	Идентификатор интерфейса.
Priority	Приоритет, назначенный пользователем для интерфейса маршрутизатора. Допустимый диапазон значений: от 0 до 255, значение по умолчанию — 1.
overhead	Заданная пользователем стоимость для этого интерфейса. Допустимый диапазон значений: от 1 до 65535, значение по умолчанию — режим "авто" стоимости.
FastHello message	Включить ли механизм FastHello и настроить количество пакетов Hello, отправляемых в секунду. Допустимый диапазон значений: от 1 до 10, значение по умолчанию — отключено.
Timing period	<ul style="list-style-type: none"> <li>• Hello: Цикл отправки сообщений Hello. Допустимый диапазон значений: от 1 до 65535, значение по умолчанию — 10 (секунд).</li> <li>• Neighbor failure: Период отказа соседа. Если в течение этого периода не получается сообщение Hello, сосед считается недоступным. Допустимый диапазон значений: от 1 до 65535, значение по умолчанию — 40 (секунд).</li> <li>• LSA retransmission: Интервал переотправки LSA (в секундах). Допустимый диапазон значений: от 3 до 65535, значение по умолчанию — 5 (секунд).</li> </ul>
Certification type	<p>Тип аутентификации.</p> <ul style="list-style-type: none"> <li>• Простой пароль: использует аутентификацию в виде обычного текста. Пароль должен быть настроен, но его можно прочитать, перехватывая пакеты.</li> <li>• Хэш-код сообщения (MD5): используется алгоритм аутентификации хэш-кода сообщения 5 (MD5). Также необходимо настроить ключ. Этот метод является самым безопасным.</li> <li>• Отсутствует аутентификация: отсутствует аутентификация.</li> </ul>

Параметр	Описание
	<ul style="list-style-type: none"> <li>Конфигурация области: См. настройки аутентификации области.</li> </ul>
Simple password	Для изменения простого пароля (укажите в виде обычного текста). Разрешенная длина ввода составляет от 1 до 8 символов.
MD Key	Нажмите на иконку  для редактирования ключа аутентификации по хэш-коду сообщения данной записи.

Элементы перечислены в порядке приоритета ключа суммарного сообщения.

OSPF Interface Message Digest Configuration VLAN ID

Interface: VLAN 1

Delete	Interface	MD Key ID	Password
*	*	*	*
No entry exists			

Таблица ниже описывает каждый элемент параметров:

Параметр	Описание
Delete	Выберите запись, и она будет удалена при следующем сохранении.
Interface	Идентификатор интерфейса.
MD Key ID	Идентификатор ключа для аутентификации по хэш-коду сообщения. Разрешенный диапазон значений составляет от 1 до 255.
Password	Пароль для аутентификации по хэш-коду сообщения. Разрешенная длина ввода составляет от 1 до 16 символов.

### 6.3.8 Конфигурация виртуального соединения

Это таблица конфигурации виртуальных связей OSPF. Виртуальная связь устанавливается между двумя ABR (Area Border Router) для решения проблемы, когда все области должны быть напрямую подключены к основной (backbone) области.

OSPF Virtual Link Configuration

Delete	Area ID	Router ID	Interval			Auth. Type	Change Simple Password	MD Key
			Hello	Dead	Retransmit			
*	*	*	*	*	*	*	*	*
No entry exists								

Таблица ниже описывает каждый элемент параметров:

Параметр	Описание
Delete	Проверьте запись, и она будет удалена при следующем сохранении.
Area ID	Область OSPF (ID области OSPF).
Router ID	ID маршрутизатора OSPF
Timing period	<ul style="list-style-type: none"> <li>• Hello: период отправки приветственного сообщения. Допустимый диапазон составляет от 1 до 65535 секунд, значение по умолчанию - 10 секунд.</li> <li>• Neighbor failure: период отказа соседа. Если в течение этого периода не получено приветственное сообщение, сосед считается недоступным. Допустимый диапазон составляет от 1 до 65535 секунд, значение по умолчанию - 40 секунд.</li> <li>• LSA retransmission: интервал переотправки LSA (в секундах). Допустимый диапазон составляет от 3 до 65535 секунд, значение по умолчанию - 5 секунд.</li> </ul>
Certification type	<p>Тип аутентификации.</p> <ul style="list-style-type: none"> <li>• Простой пароль: использует аутентификацию в виде обычного текста. Необходимо настроить пароль, который, однако, может быть прочитан при прослушивании пакетов.</li> <li>• MD5-хэш: использует аутентификацию по алгоритму MD5. Требуется также настройка ключа. Это самый безопасный метод.</li> <li>• Без аутентификации: аутентификация отсутствует.</li> <li>• Настройки области: относятся к настройкам аутентификации области.</li> </ul>
Simple password	Для изменения простого пароля (введите обычный текст). Допустимая длина ввода составляет от 1 до 8 символов.
MD Key	Щелкните на значке, чтобы изменить ключ аутентификации по методу Digest

### 6.3.9 Глобальный статус

Это таблица состояний маршрутизатора OSPF. Она используется для предоставления информации о состоянии маршрутизатора OSPF..

OSPF Global Status	
<input type="button" value="Clear OSPF Process"/> <input type="checkbox"/> Auto-refresh <input type="button" value="Refresh"/>	
Status Information	
Router ID	192.168.16.253
SPF Delay	200 msec
SPF Hold Time	400 msec
SPF Max. Wait Time	10000 msec
Last Executed SPF Time Stamp	0 msec
Min. LSA Interval	5 sec
Min. LSA Arrival	1000 msec
External LSA Count	0
External LSA Checksum	0x0
Attached Area Count	0

Таблица ниже описывает каждый элемент параметров:

Параметр	Описание
Router ID	OSPF идентификатор маршрутизатора.
SPF delay time	Время задержки вычисления SPF (в секундах).
SPF minimum interval	Минимальное время удержания (в миллисекундах) между последовательными вычислениями SPF.
SPF maximum interval	Максимальное время ожидания (в миллисекундах) между последовательными вычислениями SPF.
SFP run time	Время, прошедшее (в миллисекундах) с момента начала выполнения алгоритма SPF до текущего времени.
LSA minimum interval	Минимальный интервал для рекламы статуса связи (в секундах).
LAS maximum arrival time	Максимальное время прибытия для рекламы статуса связи в миллисекундах.
Number of External LSAs	Количество полученных внешних LSA.
External LSA checksum	Контрольная сумма внешних LSA.
Number of connected areas	Количество зон, к которым подключен маршрутизатор.

### 6.3.10 Area статус

Эта таблица отображает состояние областей сети OSPF (Open Shortest Path First). Она используется для предоставления информации о состоянии различных областей сети, которые используют протокол маршрутизации OSPF..

OSPF Area Status												
Area ID	Backbone	Area Type	NSSA translator State	Active Interfaces	Auth. Type	SPF Executed Times	LSA Count	Router LSA Count	Network LSA Count	Summary LSA Count	ASBR Summary LSA Count	NSSA LSA Count
No entry exists												

Таблица ниже описывает каждый элемент параметров:

Параметр	Описание
Area ID	ID области
Backbone area	Указывает, является ли она магистральной областью.
Area type	Тип области.

Параметр	Описание
NSSA LSA conversion	Указывает текущий статус NSSA-ABR и происходит ли преобразование LSA типа 7 в LSA типа 5 в магистральной области.
Number of active interfaces	Количество активных интерфейсов, подключенных в области.
Certification type	Тип аутентификации в области.
SPF execution times	Количество выполнений алгоритма SPF в области.
Number of LSAs	Общее количество LSA в области.
Router LSA	<ul style="list-style-type: none"> <li>• Количество: количество LSA маршрутизатора (Тип 1) данного типа в области.</li> <li>• Контрольная сумма: контрольная сумма LSA маршрутизатора (Тип 1).</li> </ul>
Network LSA	<ul style="list-style-type: none"> <li>• Количество: количество LSA сети (Тип 2) данного типа в области.</li> <li>• Контрольная сумма: контрольная сумма LSA сети (Тип 2).</li> </ul>
SummaryLSAs	<ul style="list-style-type: none"> <li>• Количество: количество суммарных LSA (Тип 3) данного типа в области.</li> <li>• Контрольная сумма: контрольная сумма суммарного LSA (Тип 3)</li> </ul>
ASBR Summary LSA	<ul style="list-style-type: none"> <li>• Количество: количество ASBR Summary LSA (Тип 4) данного типа в области.</li> <li>• Контрольная сумма: контрольная сумма ASBR Summary LSA (Тип 4).</li> </ul>
NSSA LSA	<ul style="list-style-type: none"> <li>• Количество: количество NSSA LSAs данного типа в области.</li> <li>• Контрольная сумма: контрольная сумма NSSA LSA.</li> </ul>

### 6.3.11 Таблица статуса соседей

Это таблица статуса соседей OSPF IPv4. Она предоставляет информацию о состоянии соседей OSPF IPv4.

OSPF Neighbor Status						Auto-refresh <input type="checkbox"/>	Refresh
Neighbor ID	Priority	State	Dead Time	Interface Address	Interface		
No entry exists							

Таблица ниже описывает каждый элемент параметров:

Параметр	Описание
Neighbor ID	Идентификатор соседа OSPF.
Priority	Приоритет соседа OSPF. Он определяет приоритет соседних маршрутизаторов. Этот параметр используется при выборе DR для сети. Маршрутизатор с наивысшим приоритетом становится DR.
State	Статус соседа OSPF. Он указывает на функциональный статус соседнего маршрутизатора.
Remaining expiry time	Показывает оставшееся время ожидания маршрутизатором получения OSPF приветственных пакетов от соседа перед объявлением соседа отключенным.
Interface address	IP-адрес.
Interface	Сетевой интерфейс.

### 6.3.12 Статус интерфейса

Это таблица статуса интерфейса OSPF. Она используется для предоставления информации о состоянии интерфейсов OSPF.

OSPF Interface Status														Auto-refresh <input type="checkbox"/>	Refresh				
Interface	Interface Address	Area ID	Router ID	State	DR		BDR		Pri	Cost	Interval Configuration(sec)				Hello Timer	Nbr Count	Adjacent Nbr Count	Passive	Transmit Delay
					ID	Address	ID	Address			Hello	Dead	Wait	Retransmit					
No entry exists																			

Таблица ниже описывает каждый элемент параметров:

Параметр	Описание
Interface	Идентификатор интерфейса.
Interface address	IPv4 сетевой адрес.
Area ID	ID области OSPF.
Router ID	ID маршрутизатора OSPF.
State	Статус соединения.
DR	<ul style="list-style-type: none"> <li>ID: Идентификатор маршрутизатора DR.</li> <li>Address: IP-адрес DR.</li> </ul>
BDR	<ul style="list-style-type: none"> <li>ID: Идентификатор маршрутизатора BDR.</li> <li>Address: IP-адрес BDR.</li> </ul>

Параметр	Описание
Priority	Приоритет OSPF. Он помогает определить маршрутизатор DR и BDR в сети, к которой подключен интерфейс.
overhead	Стоимость интерфейса.
Timing period (seconds)	<ul style="list-style-type: none"> <li>• Hello: цикл отправки приветственного сообщения. Допустимый диапазон составляет от 1 до 65535, значение по умолчанию - 10 секунд.</li> <li>• Neighbor failure: период отказа соседа. Если в течение этого периода не получено приветственное сообщение, сосед считается отключенным. Допустимый диапазон составляет от 1 до 65535, значение по умолчанию - 40 секунд.</li> <li>• Waiting: перед тем как устройство примет участие в выборах DR и BDR, на интерфейсе запускается таймер ожидания. Перед истечением этого таймера приветственное сообщение, отправленное устройством, не содержит информации о DR и BDR, и устройство не может быть выбрано в качестве DR или BDR. Время ожидания такое же, как время истечения соседа.</li> <li>• LSA retransmission: интервал повторной отправки LSA (в секундах). Допустимый диапазон составляет от 3 до 65535, значение по умолчанию - 5 секунд.</li> </ul>
Hello timer	Таймер Hello: после истечения времени этот интерфейс отправит пакет OSPF Hello.
Number of neighbors	Количество соседей: это количество обнаруженных соседей OSPF на этом интерфейсе.
Number of adjacencies	Количество смежностей: это количество обнаруженных смежностей OSPF на этом интерфейсе.
Passive mode	Пассивный интерфейс: указывает, является ли интерфейс пассивным.
Send delay	Задержка передачи LSA для интерфейса.

### 6.3.13 Статус маршрутизации

Это таблица состояния маршрутизации OSPF. Она используется для предоставления информации о состоянии маршрутизации OSPF.

Максимальное количество записей в таблице, отображаемых на одной странице, составляет 999, выбирается через поле ввода "записей на странице". При первом доступе веб-страница отобразит начальную запись таблицы. Поле ввода "Начать с" позволяет пользователю изменить начальную точку в этой таблице. Нажатие кнопки "Обновить" обновит отображаемую таблицу, начиная с этого совпадения или следующего ближайшего

совпадения. Кроме того, эти поля ввода будут принимать значение первой отображаемой записи при нажатии кнопки "Обновить", что позволяет последовательно обновлять с использованием одного и того же начального поля ввода.

OSPF Routing Status 0 - 0 of 0 entry Auto-refresh  Refresh << << >> >>

Start from Route Type Intra Area Destination 0.0.0.0 / 0 Area 0.0.0.0 NextHop 0.0.0.0 with 20 entries per page.

Codes: i - Intra-area Router Path, I - Inter-area Router Path

Route Type	Destination	Area	NextHop	Cost	AS Cost	Border Router Type	Interface	IsConnected
No entry exists								

Таблица ниже описывает каждый элемент параметров:

Параметр	Описание
Route type	<p>Тип маршрута OSPF.</p> <ul style="list-style-type: none"> <li>Внутриобластной: местоположение назначения - маршрут OSPF, находящийся внутри области.</li> <li>Межобластной: местоположение назначения - маршрут OSPF, находящийся между областями.</li> <li>Граничный маршрутизатор: местоположение назначения - граничный маршрутизатор.</li> <li>Внешний тип 1: местоположение назначения - внешний маршрут типа 1.</li> <li>Внешний тип 2: местоположение назначения - внешний маршрут типа 2.</li> </ul>
Destination address	Сеть и префикс данной записи маршрутизации (например, 10.0.0.0/16).
Area	Это указывает, в какую область может попасть/достигнуть маршрут или маршрутизатор.
Next hop	IPv4-адрес, закодированный как "a.b.c.d", где a-d - это читаемое целое число в десятичной системе счисления в диапазоне [0-255].
Служебный трафик	Служебный трафик маршрутизации
AS overhead	Стоимость маршрутизации в сети OSPF. Для внешних маршрутов типа 2 всегда равна "0", а для других типов маршрутов она не учитывается.
BR type	<p>Тип маршрутизатора-границы (BR type) для записи маршрутизации OSPF.</p> <ul style="list-style-type: none"> <li>i-ABR: Маршрутизатор-граница является ABR.</li> </ul>

Параметр	Описание
	<ul style="list-style-type: none"> <li>i-ASBR: Маршрутизатор-граница является ASBR, находящимся внутри области.</li> <li>i-ASBR: Маршрутизатор-граница является ASBR, находящимся между областями.</li> <li>i-ABR/ASBR: Маршрутизатор-граница является ASBR, который соединяет как минимум две области.</li> </ul>
Interface	Интерфейс, через который отправляются IP-пакеты.
Is it directly connected?	Является ли пункт назначения непосредственно подключенным.

## 6.3.14 LSDB

### 6.3.14.1 LSDB

База данных состояния связи OSPF (LSDB). Каждый маршрутизатор OSPF собирает LSA, рекламируемые другими маршрутизаторами, и все LSA собираются вместе, формируя LSDB (базу данных состояния связи). LSA представляет собой описание топологии сети вокруг маршрутизатора, а LSDB - описание топологии сети всей автономной системы.

Максимум 999 записей таблицы могут быть отображены на странице, выбирается через поле ввода "\_\_\_ записей на страницу". При первом доступе веб-страница будет отображать начальную запись таблицы. Поле ввода "Начать с \_\_\_" позволяет пользователю изменить начальную точку в этой таблице. Щелчок по кнопке "Обновить" обновит отображаемую таблицу, начиная с этого совпадения или следующего наиболее близкого совпадения. Кроме того, эти поля ввода будут принимать значение первой отображаемой записи при нажатии кнопки "Обновить", что позволяет последовательно обновлять, используя то же начальное поле ввода.

OSPF Link State Database 0 - 0 of 0 entry    Auto-refresh     Refresh    <<    >>

Start from Area ID  , Link State Type  , Link State ID  , Advertising Router  with  entries per page.

Area ID	Link State Type	Link State ID	Advertising Router	Age (in seconds)	Sequence	Checksum	Router Link Count
No entry exists							

Таблица ниже описывает каждый элемент параметров:

Параметр	Описание
Area ID	Идентификатор области OSPF.
LAS type	Тип объявления статуса связи.

Параметр	Описание
Link status ID	Идентификатор состояния связи OSPF. Он идентифицирует часть домена маршрутизации, описанную LSA.
LSA publishing equipment	Идентификатор рекламирующего маршрутизатора, который сформировал LSA.
Aging time	Время (в секундах) с момента инициации LSA.
Serial number	Последовательный номер LS LSA.
Checksum	Контрольная сумма содержимого LSA.
Number of links	Количество ссылок в LSA. Это поле имеет смысл только когда тип состояния связи - это Router-LSA (Тип1).

### 6.3.14.2 Маршрутизация LSDB

Отображение информации о маршрутах типа OSPF в базе данных состояний связи (LSDB).

Максимальное количество записей в таблице: 999 записей на страницу, выбирается через поле ввода "\_\_\_ записей на страницу". При первом доступе веб-страница отобразит начальную запись таблицы. Поле ввода "Начать с\_\_\_" позволяет пользователю изменить начальную точку в этой таблице. Нажатие кнопки "Обновить" обновит отображаемую таблицу, начиная с указанного совпадения или следующего ближайшего совпадения. Кроме того, эти поля ввода будут принимать значение первой отображаемой записи при щелчке кнопки "Обновить", что позволяет последовательным обновлениям использовать то же самое начальное поле ввода..

OSPF Router Link State Database 0 - 0 of 0 entry Auto-refresh  Refresh |<< << >> >>|

Start from Area ID  , Link State Type  , Link State ID  , Advertising Router  with  entries per page.

Area ID	Link State Type	Link State ID	Advertising Router	Age (in seconds)	Options	Sequence	Checksum	Length	Router Link Count
No entry exists									

Таблица ниже описывает каждый элемент параметров:

Параметр	Описание
Area ID	ID области OSPF для объявлений о состоянии связи
LSA type	Тип объявления о состоянии связи.
Link status ID	Идентификатор состояния связи OSPF. Он идентифицирует часть домена маршрутизации, описанную LSA.
LSA publishing Equipment	ID рекламного маршрутизатора, который сформировал LSA.
Aging time	Время (в секундах) с момента инициации LSA.
Options	Поле опций OSPF в пакете приветствия OSPF позволяет маршрутизатору OSPF поддерживать (или не поддерживать) дополнительные функции и информировать другие маршрутизаторы OSPF о своем уровне функциональности.

Параметр	Описание
Serial number	Последовательный номер LS LSA.
Checksum	Контрольная сумма содержимого LSA.
Length	Длина LSA, выраженная в байтах.
Number of links	Количество ссылок в LSA. Это поле имеет смысл только тогда, когда тип состояния связи - это Router-LSA (Type1).

### 6.3.14.3 Сеть LSDB

Отображение информации о сетевом типе OSPF LSDB.

На одной странице можно отобразить максимум 999 записей таблицы, выбрав соответствующее количество через поле ввода "\_\_\_ записей на страницу". При первом доступе веб-страница отобразит начальную запись таблицы. Поле ввода "Начиная с \_\_\_" позволяет пользователю изменить стартовую точку в этой таблице. Нажатие кнопки "Обновить" обновит отображаемую таблицу, начиная с этого совпадения или следующего ближайшего совпадения. Кроме того, эти поля ввода будут принимать значение первой отображаемой записи при нажатии кнопки "Обновить", что позволяет последовательно обновлять с использованием того же стартового поля ввода.

OSPF Network Link State Database 0 - 0 of 0 entry    Auto-refresh  Refresh    <<< << >> >>>

Start from Area ID  , Link State Type  , Link State ID  , Advertising Router  with  entries per page.

Area ID	Link State Type	Link State ID	Advertising Router	Age (in seconds)	Options	Sequence	Checksum	Length	Network Mask
No entry exists									

Таблица ниже описывает каждый элемент параметров:

Параметр	Описание
Area ID	ID области OSPF для объявлений о состоянии связи.
LSA type	Тип объявления о состоянии связи.
Link status ID	Идентификатор состояния связи OSPF. Он определяет часть области маршрутизации, описанной LSA.
LSA publishing equipment	Идентификатор рекламного маршрутизатора, который создал LSA.
Aging time	Время (в секундах) с момента начала LSA.
Options	Поле опций OSPF в пакете приветствия OSPF позволяет маршрутизатору OSPF поддерживать (или не поддерживать) необязательные функции и информировать другие маршрутизаторы OSPF о своем уровне функций.
Serial number	Последовательный номер LS LSA.
Checksum	Контрольная сумма содержимого LSA.
Length	Длина LSA, выраженная в байтах.

Параметр	Описание
Netmask	Длина маски подсети. Это поле имеет смысл только при типе статуса связи Network-LSA (Type2).

### 6.3.14.4 Суммарная информация LSDB

Отобразить информацию о типе суммарного OSPF LSDB.

Максимальное количество записей в таблице может быть отображено на одной странице, выбрано через поле ввода "\_\_\_ записей на страницу". При первом доступе веб-страница отобразит начальную запись таблицы. Поле ввода "Начать с \_\_\_" позволяет пользователю изменить начальную точку в этой таблице. Нажатие кнопки "Обновить" обновит отображаемую таблицу, начиная с этого совпадения или следующего ближайшего совпадения. Кроме того, эти поля ввода примут значение первой отображаемой записи при нажатии кнопки "Обновить", позволяя последовательные обновления с использованием того же начального поля ввода..

OSPF Summary Link State Database 0 - 0 of 0 entry    Auto-refresh  Refresh    << << >> >>

Start from Area ID  , Link State Type Network , Link State ID  , Advertising Router  with  entries per page.

Area ID	Link State Type	Link State ID	Advertising Router	Age (in seconds)	Options	Sequence	Checksum	Length	Network Mask	Metric
No entry exists										

Таблица ниже описывает каждый элемент параметров:

Параметр	Описание
Area ID	OSPF идентификатор области для объявлений о состоянии связи
LSA type	Тип объявления о состоянии связи.
Link status ID	Идентификатор состояния связи OSPF. Он идентифицирует часть домена маршрутизации, описанную в LSA.
LSA publishing equipment	Идентификатор рекламирующего маршрутизатора, который инициировал LSA.
Aging time	Время (в секундах) с момента инициации LSA.
Options	Поле опций OSPF в пакете приветствия OSPF позволяет маршрутизатору OSPF поддерживать (или не поддерживать) дополнительные функции и информировать другие маршрутизаторы OSPF о его уровне функционирования.
Serial number	Последовательный номер LS LSA.
Checksum	Контрольная сумма содержимого LSA.
Length	Длина LSA, выраженная в байтах.
Netmask	Длина маски подсети. Это поле имеет смысл только в том случае, если тип состояния связи - Summary-LSA (Type3) или ASBR-summary-LSA (Type4).

Параметр	Описание
Metric	Пользовательская метрика для этого сводного маршрута. Это поле имеет смысл только в том случае, если тип состояния связи - Summary-LSA (Type3) или ASBR-summary-LSA (Type4).

### 6.3.14.5 ASBR LSDB

Отобразить информацию о базе данных состояния связи OSPF типа ASBR Summary. Максимальное количество записей в таблице - 999 записей на страницу, которое можно выбрать через поле ввода "\_\_\_ записей на страницу". При первом доступе веб-страница отобразит начальную запись таблицы. Поле ввода "Начать с \_\_\_" позволяет пользователю изменить начальную точку в этой таблице. Нажатие кнопки "Обновить" обновит отображаемую таблицу, начиная с указанной или ближайшей к ней записи. Кроме того, эти поля ввода будут принимать значение первой отображаемой записи при нажатии кнопки "Обновить", что позволяет последовательно обновлять данные, используя то же самое начальное поле ввода.

OSPF ASBR Summary Link State Database 0 - 0 of 0 entry    Auto-refresh     Refresh    <<    <<    >>    >>

Start from Area ID  , Link State Type  , Link State ID  , Advertising Router  with  entries per page.

Area ID	Link State Type	Link State ID	Advertising Router	Age (in seconds)	Options	Sequence	Checksum	Length	Network Mask	Metric
No entry exists										

Таблица ниже описывает каждый элемент параметров:

Параметр	Описание
Area ID	ID области OSPF для объявлений о статусе связи.
LSA type	Тип объявления о статусе связи.
Link status ID	ID состояния связи OSPF. Он идентифицирует часть области маршрутизации, описанной LSA.
LSA publishing equipment	ID рекламирующего маршрутизатора, который сформировал LSA.
Aging time	Время (в секундах) с момента инициации LSA.
Options	Поле опций OSPF в пакете hello OSPF позволяет маршрутизатору OSPF поддерживать (или не поддерживать) необязательные функции и информировать другие маршрутизаторы OSPF о своем уровне функциональности.
Serial number	Последовательный номер LS LSA.
Checksum	Контрольная сумма содержимого LSA.
Length	Длина LSA, выраженная в байтах.

Параметр	Описание
Netmask	Длина маски подсети. Это поле имеет значение только при типе статуса связи Summary-LSA (Type3) или ASBR-summary-LSA (Type4).
Metric	Пользовательское заданная метрика для этого сводного маршрута. Это поле имеет значение только при типе статуса связи Summary-LSA (Type3) или ASBR-summary-LSA (Type4).

### 6.3.14.6 Внешняя информация LSDB

Отображение информации о базе данных состояния связи OSPF типа External.

Максимальное количество записей в таблице, отображаемых на одной странице, можно выбрать с помощью поля ввода " \_\_\_ записей на странице". При первом доступе веб-страница будет отображать начальную запись таблицы. Поле ввода "Начать с \_\_\_" позволяет пользователю изменить начальную точку в этой таблице. Нажатие кнопки "Обновить" обновит отображаемую таблицу, начиная с указанной записи или следующей ближайшей записи. Кроме того, эти поля ввода будут принимать значение первой отображаемой записи при нажатии кнопки "Обновить", что позволяет последовательно обновлять с использованием того же начального поля ввода.

Link State Type	Link State ID	Advertising Router	Age (in seconds)	Options	Sequence	Checksum	Length	Network Mask	Metric Type	Metric	Forward Address
No entry exists											

Таблица ниже описывает каждый элемент параметров:

Параметр	Описание
LSA type	Тип объявления о состоянии связи.
Link status ID	Идентификатор состояния связи OSPF. Он определяет часть домена маршрутизации, описанную в LSA.
LSA publishing equipment	Идентификатор рекламного маршрутизатора, который создал LSA.
Aging time	Время (в секундах) с момента инициации LSA.
Options	Поле опций OSPF в пакете приветствия OSPF позволяет маршрутизатору OSPF поддерживать (или не поддерживать) дополнительные функции и информировать другие маршрутизаторы OSPF о его уровне функциональности.
Serial number	Последовательный номер LS LSA.
Checksum	Контрольная сумма содержимого LSA.
Length	Длина LSA, выраженная в байтах.
Netmask	Длина маски подсети. Это поле имеет смысл только, когда тип состояния связи - "Внешний/ИССА внешний статус связи" (типы 5, 7).

Параметр	Описание
Measure type	Внешний тип LSA. Это поле имеет смысл только, когда тип состояния связи - "Внешний/НССА внешний статус связи" (типы 5, 7).
Metric	Пользовательский указанный метрический путь для этого сводного маршрута. Это поле имеет смысл только, когда тип состояния связи - External-LSA (Тип5) или NSSA LSA (Тип7).
Forwarding address	IP-адрес адреса пересылки. Это поле имеет смысл только, когда тип состояния связи - External-LSA (Тип5) или NSSA LSA (Тип7).

### 6.3.14.7 NSSA внешнего типа LSDB

Отображение информации о типе NSSA OSPF LSDB.

На страницу можно отображать максимум 999 записей в таблице, выбирая через поле ввода "\_\_\_записей на страницу". При первом доступе веб-страница отобразит начальную запись таблицы. Поле ввода "Начать с \_\_\_" позволяет пользователю изменить начальную точку в этой таблице. Нажатие кнопки "Обновить" обновит отображаемую таблицу, начиная с этого совпадения или ближайшего к нему. Кроме того, эти поля ввода будут принимать значение первой отображаемой записи при нажатии кнопки обновления, что позволяет последовательно обновлять, используя то же самое начальное поле ввода.

Link State Type	Link State ID	Advertising Router	Age (in seconds)	Options	Sequence	Checksum	Length	Network Mask	Metric Type	Metric	Forward Address
No entry exists											

Таблица ниже описывает каждый элемент параметров:

Параметр	Описание
LSA type	Тип объявления о состоянии соединения.
Link status ID	Идентификатор состояния связи OSPF. Он определяет часть области маршрутизации, описанную LSA.
LSA publishing equipment	ID рекламирующего маршрутизатора, который сформировал LSA.
Aging time	Время (в секундах) с момента инициации LSA.
Options	Поле опций OSPF в пакете приветствия OSPF позволяет маршрутизатору OSPF поддерживать (или не поддерживать) дополнительные функции и информировать другие маршрутизаторы OSPF о своем уровне функциональности.
Serial number	Последовательный номер LS LSA.
Checksum	Контрольная сумма содержимого LSA.

Параметр	Описание
Length	Длина LSA, выраженная в байтах.
Netmask	Длина маски подсети. Это поле имеет смысл только в том случае, когда тип состояния связи является внешним LSA (тип 5) или NSSA LSA (тип 7).
Measure type	Внешний тип LSA. Это поле имеет смысл только в том случае, когда тип состояния связи является внешним LSA (тип 5) или NSSA LSA (тип 7).
Metric	Пользовательский метрический параметр для этого сводного маршрута. Это поле имеет смысл только в том случае, когда тип состояния связи является внешним LSA (тип 5) или NSSA LSA (тип 7).
Forwarding address	IP-адрес адреса пересылки. Это поле имеет смысл только в том случае, когда тип состояния связи является внешним LSA (тип 5) или NSSA LSA (тип 7).

## 7 Управление безопасностью

### 7.1 Уровни доступа

Устройство предоставляет настройки уровней доступа для каждой группы уровней привилегий. Уровни привилегий могут варьироваться от 0 до 15, где 0 является самым низким уровнем, а 15 - самым высоким. Каждая группа имеет следующие подгруппы авторизованных уровней привилегий:

- Конфигурация может быть только прочитана
- Настройка/выполнение чтения и записи
- Информация о состоянии/статистике доступна только для чтения
- Чтение и запись информации о состоянии/статистике (например, очистка статистической информации)

Уровень привилегий пользователя должен быть больше или равен уровню авторизации привилегий, чтобы получить доступ к группе. В большинстве случаев группа уровней привилегий состоит из одного модуля (например, LACP, RSTP или QOS), но некоторые из этих групп содержат более одного модуля. В следующем описании подробно описаны эти группы уровней привилегий:

- Система: Контакт, имя, местоположение, часовой пояс, летнее время, журнал.
- Безопасность: Аутентификация, управление доступом к системе, порты (включая порты DOT1X, основанные на MAC-адресах и ограничениях MAC-адресов), ACL, HTTPS, SSH, проверка ARP, охрана источника IP.
- IP: Все, кроме "ping".
- Порт: Все, кроме "Veriphy".
- Диагностика: "ping" и "Veriphy".
- Обслуживание: В CLI: перезапуск системы, восстановление значений по умолчанию, пароль системы, сохранение конфигурации, загрузка конфигурации и загрузка прошивки. На веб-странице: пользователи, уровни привилегий и обслуживание.
- Отладка: Только в CLI..

**Privilege Level Configuration**

Group Name	Privilege Levels			
	Configuration Read-only	Configuration/Execute Read/write	Status/Statistics Read-only	Status/Statistics Read/write
Aggregation	5 ▾	10 ▾	5 ▾	10 ▾
Alarm	5 ▾	10 ▾	5 ▾	10 ▾
APS	5 ▾	10 ▾	5 ▾	10 ▾
CFM	5 ▾	10 ▾	5 ▾	10 ▾
DDMI	5 ▾	10 ▾	5 ▾	10 ▾
Debug	15 ▾	15 ▾	15 ▾	15 ▾
DHCP	5 ▾	10 ▾	5 ▾	10 ▾
DHCPv6_Client	5 ▾	10 ▾	5 ▾	10 ▾
Diagnostics	5 ▾	10 ▾	5 ▾	10 ▾
ERPS	5 ▾	10 ▾	5 ▾	10 ▾
ETH_LINK_OAM	5 ▾	10 ▾	5 ▾	10 ▾
Firmware	5 ▾	10 ▾	5 ▾	10 ▾
Green_Ethernet	5 ▾	10 ▾	5 ▾	10 ▾
IP	5 ▾	10 ▾	5 ▾	10 ▾
IPMC_Snooping	5 ▾	10 ▾	5 ▾	10 ▾
LACP	5 ▾	10 ▾	5 ▾	10 ▾
LLDP	5 ▾	10 ▾	5 ▾	10 ▾
Loop_Protect	5 ▾	10 ▾	5 ▾	10 ▾
MAC_Table	5 ▾	10 ▾	5 ▾	10 ▾
Mirroring	5 ▾	10 ▾	5 ▾	10 ▾
Miscellaneous	15 ▾	15 ▾	15 ▾	15 ▾
MRP	5 ▾	10 ▾	5 ▾	10 ▾
MVR	5 ▾	10 ▾	5 ▾	10 ▾
NTP	5 ▾	10 ▾	5 ▾	10 ▾
Ports	5 ▾	10 ▾	1 ▾	10 ▾
Private_VLANs	5 ▾	10 ▾	5 ▾	10 ▾
PTP	5 ▾	10 ▾	5 ▾	10 ▾
QoS	5 ▾	10 ▾	5 ▾	10 ▾
Security(access)	10 ▾	10 ▾	5 ▾	10 ▾
Security(network)	5 ▾	10 ▾	5 ▾	10 ▾
sFlow	5 ▾	10 ▾	5 ▾	10 ▾
Spanning_Tree	5 ▾	10 ▾	5 ▾	10 ▾
System	5 ▾	10 ▾	1 ▾	10 ▾
UDLD	5 ▾	10 ▾	5 ▾	10 ▾
uFDMA_AIL	5 ▾	10 ▾	5 ▾	10 ▾
uFDMA_CIL	5 ▾	10 ▾	5 ▾	10 ▾
UPnP	5 ▾	10 ▾	5 ▾	10 ▾
VCL	5 ▾	10 ▾	5 ▾	10 ▾
VLAN_Translation	5 ▾	10 ▾	5 ▾	10 ▾
VLANs	5 ▾	10 ▾	5 ▾	10 ▾
Voice_VLAN	5 ▾	10 ▾	5 ▾	10 ▾
XXRP	5 ▾	10 ▾	5 ▾	10 ▾

Save Reset

Имя сообщества является названием группы, которое идентифицирует каждую группу уровней привилегий. Каждая группа имеет следующие подгруппы уровней авторизации

привилегий: только чтение конфигурации; чтение и запись конфигурации/выполнение; только чтение статуса/статистики; чтение и запись статуса/статистики (например, очистка статистики). Уровни привилегий могут варьироваться от 0 до 15, где 0 является самым низким уровнем, а 15 - самым высоким уровнем. Уровень привилегий пользователя должен быть больше или равен уровню авторизации привилегий, чтобы предоставить доступ к группе.

## 7.2 SSH

Устройство предоставляет функцию конфигурации SSH, которая может включать или отключать службу SSH.

**SSH Configuration**  
**Mode**  

Описание каждого параметра представлено в следующей таблице:

Параметр	Описание
Mode	Указывает режим работы SSH. Возможные режимы: <ul style="list-style-type: none"><li>• Включено: Включить режим работы SSH.</li><li>• Отключено: Отключить режим работы SSH..</li></ul>

## 7.3 HTTPS

Устройство предоставляет функцию конфигурации HTTPS, которая позволяет включать или отключать службу HTTPS и сохранять текущий сертификат на коммутаторе. HTTPS представляет собой канал HTTP, направленный на обеспечение безопасности. Основываясь на HTTP, он обеспечивает безопасность процесса передачи через шифрование передачи и аутентификацию личности. HTTPS добавляет SSL-слой к основе HTTP. Безопасность HTTPS основана на SSL, поэтому детали шифрования требуют SSL. У HTTPS есть другой порт по умолчанию, чем HTTP, а также слой шифрования/аутентификации (между HTTP и TCP).

### HTTPS Configuration Refresh

<b>Mode</b>	Disabled ▼
<b>Automatic Redirect</b>	Disabled ▼
<b>Certificate Maintain</b>	None ▼
<b>Certificate Status</b>	Switch secure HTTP certificate is presented

Описание каждого параметра представлено в следующей таблице:

Параметр	Описание
Mode	Включить или отключить службу HTTPS.
Automatic redirect	Функция автоматического перенаправления будет включена или выключена только после включения HTTPS. При включенном режиме перенаправления HTTP-соединения автоматически перенаправляются на HTTPS-соединения.
Certificate maintenance	<p>Операции по обслуживанию сертификата. Возможные действия:</p> <ul style="list-style-type: none"> <li>None: Нет операции.</li> <li>Delete: Удалить текущий сертификат.</li> <li>Upload: Загрузить файл PEM-сертификата. Возможные методы: веб-браузер или URL.</li> <li>Generate: Сгенерировать новый самоподписанный RSA-сертификат.</li> </ul>
Certificate pass phrase	При выборе загрузки сертификата введите пароль в это поле, если ваш загруженный сертификат защищен определенным паролем.
Certificate upload	<p>Загрузите файл PEM-сертификата на коммутатор. Этот файл должен содержать сертификат и закрытый ключ. Если у вас есть два отдельных файла для сохранения сертификата и закрытого ключа, используйте команду cat в Linux для объединения их в один файл PEM. Возможные методы:</p> <ul style="list-style-type: none"> <li>Загрузка файла: Загрузите сертификат через веб-браузер.</li> <li>URL: Загрузите сертификат через URL, протоколы - HTTP, HTTPS, TFTP и FTP. Формат URL:  <code>&lt;protocol&gt;://[&lt;username&gt;[:&lt;password&gt;]@]&lt;host&gt;[:&lt;port&gt;][/&lt;path&gt;]/&lt;file_name&gt;</code>. Допустимые имена файлов состоят из букв (A-Z), цифр (0-9), точек (.), дефисов (-) и подчеркиваний (_). Максимальная длина - 63 символа, имя файла не может начинаться с дефиса, и не может использовать '.' в качестве имени файла (имя файла только '.').</li> </ul>

Параметр	Описание
Certificate status	Отобразить текущий статус сертификата на коммутаторе. Возможные состояния: <ul style="list-style-type: none"><li>• Предоставлен HTTPS-сертификат</li><li>• Нет HTTPS-сертификата</li><li>• Генерируется HTTPS-сертификат...</li></ul>



#### Примечание:

Обратите внимание, что из-за проблем безопасности браузеры могут не разрешать перенаправления, если браузер не доверяет сертификату коммутатора. В этом случае вам потребуется вручную инициализировать HTTPS-соединение.

Пожалуйста, обратите внимание, что рекомендуется использовать RSA-сертификаты, так как большинство новых версий браузеров прекратили поддержку сертификатов DSA.

## 7.4 Методы аутентификации

Устройство предоставляет функциональность AAA. AAA - это сокращение от Authentication (аутентификация), Authorization (авторизация) и Accounting (учет). Он предоставляет структуру управления для настройки контроля доступа на устройствах NAS (серверах доступа к сети). Контроль доступа используется для управления тем, какие пользователи могут получить доступ к сети и к каким сетевым ресурсам они могут получить доступ..

### Authentication Method Configuration

Client	Methods		
console	local ▼	no ▼	no ▼
telnet	local ▼	no ▼	no ▼
ssh	local ▼	no ▼	no ▼
http	local ▼	no ▼	no ▼

### Command Authorization Method Configuration

Client	Method	Cmd Lvl	Cfg Cmd
console	no ▼	0	<input type="checkbox"/>
telnet	no ▼	0	<input type="checkbox"/>
ssh	no ▼	0	<input type="checkbox"/>

### Accounting Method Configuration

Client	Method	Cmd Lvl	Exec
console	no ▼		<input type="checkbox"/>
telnet	no ▼		<input type="checkbox"/>
ssh	no ▼		<input type="checkbox"/>

Описание каждого параметра представлено в следующей таблице:

Параметр	Описание
<b>Authentication method configuration</b>	<b>Конфигурация метода аутентификации:</b>
Client	Устройство поддерживает четыре метода входа: консольный, telnet, ssh и http.
Method	<p>Вот 4 метода аутентификации для каждого способа входа. Каждый способ входа может быть настроен с использованием до 3 методов аутентификации. Когда первый метод не удастся, используется второй метод. Когда второй метод не удастся, используется третий метод. Попробуйте каждый метод слева направо до получения успешных или неудачных результатов. Настоятельно рекомендуется настроить последний метод как local, чтобы всегда можно было войти через аутентификацию в локальной базе данных, когда серверы аутентификации недоступны.</p> <ul style="list-style-type: none"> <li>no: Отключить аутентификацию, то есть аутентификация входа не может быть выполнена через этот метод.</li> </ul>

Параметр	Описание
	<ul style="list-style-type: none"> <li>local: Использовать локально хранимую базу данных на устройстве для аутентификации входа</li> <li>radius: Аутентификация входа через удаленный сервер RADIUS</li> <li>tacacs: Аутентификация входа через удаленный сервер TACACS+</li> </ul>
<b>Command authorization mode Configuration</b>	<b>Конфигурация режима авторизации команд</b>
Client	Среди трех методов входа: консоль, telnet и ssh, команды конфигурации могут быть авторизованы через сервер TACACS+.
Method	<p>Доступные опции: no/tacacs.</p> <ul style="list-style-type: none"> <li>No: Указывает, что авторизация команд отключена, и команды, которые пользователи могут использовать, назначаются в соответствии с уровнем пользователя.</li> <li>Tacacs: Указывает использовать удаленный сервер TACACS+ для авторизации команд, которые могут использовать пользователи.</li> </ul>
Command level	Диапазон от 0 до 15. Команды, уровень которых выше или равен этому уровню, будут запрашивать авторизацию на сервере TACACS+, где 0 - самый низкий уровень, а 15 - самый высокий уровень.
Configuration commands	После проверки команды конфигурации также требуют авторизации на сервере.
Billing method configuration	Конфигурация метода выставления счетов.
Client	Среди трех методов входа: консоль, telnet и ssh, входящие пользователи могут выставляться в счет через сервер TACACS+..
Method	<p>Доступные опции: no/tacacs.</p> <ul style="list-style-type: none"> <li>No: Указывает, что учет отключен.</li> <li>Tacacs: Указывает использовать удаленный сервер TACACS+ для выставления счетов пользователям.</li> </ul>

Параметр	Описание
Command level	Диапазон от 0 до 15, команды с уровнем выше или равным этому уровню будут выставляться в счет; пустое значение означает отключение выставления счетов.
Implement	После проверки вход в режим exes будет выставляться в счет.

## 7.5 Управление доступом

Устройство предоставляет функцию конфигурации управления доступом, которая может включать или отключать функцию управления доступом. Функция управления доступом требует настройки таблицы записей управления доступом. Максимальное количество записей - 16. Если тип приложения соответствует какой-либо записи управления доступом, доступ к коммутатору разрешен.

**Access Management Configuration**

Mode

Delete	VLAN ID	Start IP Address	End IP Address	HTTP/HTTPS	SNMP	TELNET/SSH
Add New Entry						

Save    Reset

Описание каждого параметра представлено в следующей таблице:

Параметр	Описание
Mode	Включить или отключить функцию управления доступом.
Delete	Удалить запись: при выборе данной опции она будет удалена во время следующего сохранения.
VLAN ID	ID VLAN этой записи управления доступом.
Starting IP address	Начальный IP-адрес для этой записи управления доступом.
End IP address	Конечный IP-адрес для этой записи управления доступом.
HTTP/HTTPS	При установке этого флажка разрешается доступ к коммутатору через интерфейс http/https, если IP-адрес хоста соответствует диапазону IP-адресов, указанному в записи.
SNMP	При установке этого флажка разрешается доступ к коммутатору через интерфейс snmp, если IP-адрес хоста соответствует диапазону IP-адресов, указанному в записи.

Параметр	Описание
TELNET/SSH	При установке этого флажка разрешается доступ к коммутатору через интерфейс telnet/ssh, если IP-адрес хоста соответствует диапазону IP-адресов, указанному в записи.

## 7.6 SNMP

Простой протокол управления сетью (SNMP) определен Интернет-инженерной рабочей группой и является частью протоколов Интернета. Под определенным условием внимания к определенному сетевому устройству используется SNMP для мониторинга сетевого устройства через систему управления сетью. Протокол SNMP состоит из серии стандартных протоколов управления сетью, протоколов прикладного уровня, баз данных и объектов данных. Протокол SNMP может отображать данные управления, такие как описание конфигурации системы, через форму системы управления. Эти описания конфигурации могут быть запрошены или установлены через приложение управления, поддерживающее SNMP. Протокол SNMP основан на протоколе TCP/IP. SNMP обычно использует UDP-порты 161 (SNMP) и 162 (SNMP-Trap). Агент протокола SNMP (SNMP Agent) существует в сетевом устройстве и использует стандартные MIB (информация, специфичная для устройства) в качестве интерфейсов устройства, через которые эти сетевые устройства могут быть мониторингом или управляться. Когда происходит событие Trap, сообщение передается с помощью SNMP Trap. В этот момент доступный приемник Trap может получить сообщение Trap.

SNMP v1 и SNMP v2c используют аутентификацию по имени сообщества. Сообщество SNMP названо строкой символов, называемой именем сообщества или названием сообщества. Имя сообщества SNMP используется для определения отношений между менеджером SNMP и агентом SNMP. Имя сообщества играет роль, аналогичную паролю, и может ограничивать доступ менеджера SNMP к агенту SNMP на коммутаторе Ethernet. SNMP V3 использует настроенных пользователей для аутентификации. Он также настраивает уровень безопасности, алгоритм аутентификации и пароль, алгоритм шифрования и пароль. Для ловушек SNMP V3 также необходимо настроиться в соответствии с именем пользователя и паролем алгоритма, настроенными на стороне управления. Идентификатор движка также должен быть согласован с конфигурацией на стороне управления.

Технология RMON является расширением функционала SNMP. Это набор переменных MIB, который в основном предназначен для устранения недостатков в SNMP, связанных с отсутствием реального времени в коммуникации между процессом управления и агентом, а также с избыточной нагрузкой при опросе. Этот набор переменных MIB генерируется через

непрерывное, реальное мониторинга сети. RMON является приложением SNMP, следующим структуре SNMP и расширяющим функции и применение SNMP.

## 7.6.1 SNMP настройки

Страница настройки SNMP показана на рисунке ниже.

**SNMP System Configuration**

<b>Mode</b>	Enabled
<b>Engine ID</b>	800019cb034c93a6c414c0

Описание каждого параметра представлено в следующей таблице:

Параметр	Описание
Mode	Включить и отключить функциональность SNMP.
Engine ID	ID движка SNMPv3. Строка должна содержать четное количество цифр (в шестнадцатеричном формате) от 10 до 64, но не допускаются все нули и все F. Доступ к устройству (локальным пользователям) разрешен только для пользователей с этим идентификатором движка, поэтому изменение идентификатора движка отменит доступ для всех текущих локальных пользователей.

## 7.6.2 SNMPv1/v2c сообщество

Страница сообщества SNMPv1/v2c, как показано на рисунке ниже.

**SNMPv3 Community Configuration**

Delete	Community name	Community secret	Source IP	Source Prefix
--------	----------------	------------------	-----------	---------------

Описание каждого параметра представлено в следующей таблице:

Параметр	Описание
Delete	Удалить запись: при выборе запись будет удалена при следующем сохранении.
Group name	Указывает, что имя сообщества сопоставлено с настроенным именем безопасности группы SNMP. Допустимая длина строки составляет от 1 до 32 символов ASCII, а допустимое содержимое - от 33 до 126 символов ASCII.

Параметр	Описание
Community key	Указывает, что ключ сообщества (строка доступа community name) позволяет доступ к агенту SNMP с использованием SNMPv1 и SNMPv2c. Допустимая длина строки составляет от 1 до 32 символов ASCII, а допустимое содержимое - от 33 до 126 символов ASCII.
Source IP address	Указывает исходный адрес доступа SNMP. При использовании вместе с префиксами источника подсети источников можно ограничить с помощью определенных диапазонов адресов источника.
Source address prefix	Указывает префикс исходного адреса доступа SNMP.

### 7.6.3 SNMPv3 пользователи

Страница пользователя SNMPv3, как показано на рисунке ниже.

**SNMPv3 User Configuration**

Delete	Engine ID	User Name	Security Level	Authentication Protocol	Authentication Password	Privacy Protocol	Privacy Password
<input type="button" value="Add New Entry"/> <input type="button" value="Save"/> <input type="button" value="Reset"/>							

Описание каждого параметра представлено в следующей таблице:

Параметр	Описание
Delete	Удалить запись: при выборе запись будет удалена при следующем сохранении.
Engine ID	Восьмибитная строка, указывающая идентификатор движка, к которому должна принадлежать эта запись. Строка должна содержать четное количество цифр (в шестнадцатеричном формате) от 10 до 64, но не допускаются все нули и все F. Архитектура SNMPv3 использует режим безопасности на основе пользователей (USM) для обработки безопасности сообщений и режим контроля доступа на основе представления (VACM) для контроля доступа. Для записей USM usmUserEngineID и usmUserName являются ключами записи. В простом прокси usmUserEngineID всегда равен значению snmpEngineID самого прокси. Это значение также может принимать значение snmpEngineID удаленного SNMP-движка, с которым может взаимодействовать этот пользователь. Другими словами, если идентификатор движка пользователя и идентификатор системы равны, это локальный пользователь; в противном случае это удаленный пользователь.
Username	Строка, указывающая имя безопасности, к которому должна принадлежать эта запись. Допустимая длина строки составляет от 1 до 32 символов ASCII, а допустимое содержимое - от 33 до 126 символов ASCII.

Параметр	Описание
Security Level	<p>Укажите уровень безопасности, к которому должна относиться эта запись. Возможные уровни безопасности:</p> <ul style="list-style-type: none"> <li>NoAuth, NoPriv: Без аутентификации и без шифрования.</li> <li>Auth, NoPriv: Только аутентификация и без шифрования.</li> <li>Auth, Priv: Аутентификация и шифрование.</li> </ul>
Authentication protocol	<p>Укажите протокол аутентификации, к которому должна относиться эта запись. Возможные протоколы аутентификации:</p> <ul style="list-style-type: none"> <li>None: Нет протокола аутентификации.</li> <li>MD5: Инструктирует этого пользователя использовать протокол аутентификации MD5.</li> <li>SHA: Инструктирует этого пользователя использовать протокол аутентификации SHA.</li> </ul>
Authentication password	<p>Строка, идентифицирующая пароль аутентификации. Для протокола аутентификации MD5 допустимая длина строки составляет от 8 до 32 символов. Для протокола аутентификации SHA допустимая длина строки составляет от 8 до 40 символов. Допустимое содержимое - символы ASCII с 33 по 126.</p>
Encryption protocol	<p>Укажите протокол шифрования, к которому должна относиться эта запись. Возможные протоколы шифрования:</p> <ul style="list-style-type: none"> <li>None: Отсутствие протокола шифрования.</li> <li>DES: Инструктирует пользователя использовать протокол шифрования DES.</li> <li>AES: Инструктирует этого пользователя использовать протокол шифрования AES.</li> </ul>
Encrypted password	<p>Строка, идентифицирующая пароль шифрования. Допустимая длина строки составляет от 8 до 32 символов, а допустимое содержимое - символы ASCII с 33 по 126.</p>

## 7.6.4 SNMP группа

Страница конфигурации группы SNMP изображена на рисунке ниже.

SNMPv3 Group Configuration			
Delete	Security Model	Security Name	Group Name
<input type="checkbox"/>	v1	public	default_ro_group
<input type="checkbox"/>	v1	private	default_rw_group
<input type="checkbox"/>	v2c	public	default_ro_group
<input type="checkbox"/>	v2c	private	default_rw_group

Описание каждого параметра представлено в следующей таблице:

Параметр	Описание
Delete	Удалить выбранную запись, она будет удалена при следующем сохранении
Security mode	<p>Укажите режим безопасности, к которому должна принадлежать эта запись. Возможные режимы безопасности:</p> <ul style="list-style-type: none"> <li>v1: Зарезервировано для SNMPv1.</li> <li>v2c: Зарезервировано для SNMPv2c.</li> <li>usm: SNMPv3, режим безопасности на основе пользователя (USM).</li> </ul>
Security name	<p>Строка, указывающая имя безопасности, которому должна принадлежать эта запись. Допустимая длина строки - от 1 до 32 символов, а допустимое содержимое - символы ASCII с 33 по 126. Для SNMPv3 это относится к имени пользователя, а для SNMPv1 и SNMPv2c - к имени сообщества.</p>
Group name	<p>Здесь относится к имени группы, строке, указывающей имя группы, которой должна принадлежать эта запись. Допустимая длина строки - от 1 до 32 символов, а допустимое содержимое - символы ASCII с 33 по 126.</p>

### 7.6.5 SNMP вид

Страница просмотра SNMP, как показано на рисунке ниже.

**SNMPv3 View Configuration**

Delete	View Name	View Type	OID Subtree
<input type="checkbox"/>	default_view	included ▼	.1

Описание каждого параметра представлено в следующей таблице:

Параметр	Описание
Delete	Удалите запись при выборе, и она будет удалена при следующем сохранении.
View name	Строка, указывающая имя представления, к которому должна принадлежать эта запись. Разрешенная длина строки составляет от 1 до 32 символов, а допустимое содержание - от 33 до 126 символов ASCII.
View type	<p>Укажите тип представления, к которому должна принадлежать эта запись. Возможные типы представлений:</p> <ul style="list-style-type: none"> <li>включено: указывает, что это поддерево представления должно быть включено.</li> <li>исключено: указывает, что это поддерево представления должно быть исключено.</li> </ul> <p>Пример: В общем случае, если тип представления записи - "исключено", должна существовать другая запись представления с типом "включено", и ее поддерево OID должно превышать "исключенную запись представления".</p>
SubtreeOID	Определите OID корня поддерева, добавленного к именованному представлению. Разрешенная длина OID составляет от 1 до 128. Разрешенное содержимое строки - числа или звездочки (*).

## 7.6.6 SNMP аутентификация

Страница аутентификации SNMP, как показано на рисунке ниже

**SNMPv3 Access Configuration**

Delete	Group Name	Security Model	Security Level	Read View Name	Write View Name
<input type="checkbox"/>	default_ro_group	any	NoAuth, NoPriv	default_view ▼	None ▼
<input type="checkbox"/>	default_rw_group	any	NoAuth, NoPriv	default_view ▼	default_view ▼

Описание каждого параметра представлено в следующей таблице:

Параметр	Описание
Delete	Удалить запись при выборе, и она будет удалена во время следующего сохранения.
Group name	Здесь указывается имя группы, строка, указывающая имя группы, к которой должна принадлежать эта запись. Разрешенная длина строки составляет от 1 до 32 символов, разрешенное содержимое - от 33 до 126 символов ASCII.
Security mode	Укажите режим безопасности, к которому должна принадлежать эта запись. Возможные режимы безопасности: <ul style="list-style-type: none"> <li>любой: принимает любой режим безопасности (V1   V2C   USM).</li> <li>v1: Зарезервировано для SNMPV1.</li> <li>v2c: Зарезервировано для SNMPV2C.</li> <li>usm: SNMPV3, режим безопасности на основе пользователей (USM).</li> </ul>
Security Level	Укажите уровень безопасности, к которому должна принадлежать эта запись. Возможные уровни безопасности: <ul style="list-style-type: none"> <li>NoAuth,NoPriv: Нет аутентификации и нет шифрования.</li> <li>Auth,NoPriv: Только аутентификация и нет шифрования.</li> <li>Auth,Priv: Аутентификация и шифрование.</li> </ul>
Read view name	Имя представления MIB, которое определяет объект MIB, для которого можно запросить текущее значение. Разрешенная длина строки составляет от 1 до 32 символов, а разрешенное содержимое - от 33 до 126 символов ASCII.
Write view name	Имя представления MIB, которое определяет объекты MIB, для которых можно установить новые значения. Разрешенная длина строки составляет от 1 до 32 символов, а разрешенное содержимое - от 33 до 126 символов ASCII.

## 7.6.7 SNMP Ловушка

### 7.6.7.1 Хост назначения

Страница конфигурации хоста назначения, как показано на рисунке ниже.

### Trap Configuration

#### Trap Destination Configurations

Delete	Name	Enable	Version	Destination Address	Destination Port
<input type="button" value="Add New Entry"/>					
<input type="button" value="Save"/> <input type="button" value="Reset"/>					

Щелкните кнопку "Добавить запись", чтобы войти на страницу конфигурации SNMP-ловушек, как показано на рисунке ниже.

### SNMP Trap Configuration

Trap Config Name	<input type="text"/>
Trap Mode	Disabled <input type="button" value="v"/>
Trap Version	SNMP v2c <input type="button" value="v"/>
Trap Community	public
Trap Destination Address	<input type="text"/>
Trap Destination Port	162
Trap Inform Mode	Disabled <input type="button" value="v"/>
Trap Inform Timeout (seconds)	3
Trap Inform Retry Times	5
Trap Security Engine ID	800019cb034c93a6c414c0
Trap Security Name	None <input type="button" value="v"/>

Описание каждого параметра представлено в следующей таблице:

Параметр	Описание
Trap name	Указывает имя ловушки для конфигурации. Разрешенная длина строки составляет от 1 до 32 символов, а разрешенное содержимое - от 33 до 126 символов ASCII.
Trap mode	Укажите режим работы SNMP. Возможные варианты: <ul style="list-style-type: none"> <li>• Включить: включить режим работы SNMP.</li> <li>• Отключить: отключить режим работы SNMP.</li> </ul>

Параметр	Описание
Trap version	<p>Укажите поддерживаемую версию SNMP. Возможные варианты:</p> <ul style="list-style-type: none"> <li>• SNMP v1: Установить поддержку SNMP версии 1.</li> <li>• SNMP v2c: Установить поддержку версии 2C SNMP.</li> <li>• SNMP v3: Установить поддержку SNMP версии 3.</li> </ul>
Trap groups	<p>Укажите строку доступа к сообществу при отправке пакетов SNMP Trap. Разрешенная длина строки составляет от 0 до 63 символов, а разрешенное содержимое - от 33 до 126 символов ASCII.</p>
Trap destination address	<p>Адрес назначения SNMP Trap:</p> <ul style="list-style-type: none"> <li>• Указывает IPv4-адрес цели SNMP Trap. Допускается действительный IP-адрес в десятичной точечной нотации ('x.y.z.w'). Также допускаются действительные имена хостов. Действительное имя хоста - это строка, состоящая из букв (A-Z), цифр (0-9), точки (.) и дефиса (-). Пробелы не допускаются, первый символ должен быть буквой, а первый и последний символы не должны быть точками или дефисами.</li> <li>• Указывает IPv6-адрес цели SNMP Trap. IPv6-адрес состоит из 128 бит и представлен в виде восьми полей, каждое из которых содержит до четырех шестнадцатеричных цифр, разделенных двоеточием. Например, 'fe80::215:c5ff:fe03:4dc7'. Обозначение '::' является специальным синтаксическим средством, которое может использоваться в качестве краткой записи для представления нескольких 16-битных полей последовательных нулей, но оно может появляться только один раз. Оно также может представлять собой законный и действительный IPv4-адрес. Например, '::192.1.2.34'.</li> </ul>
Trap destination port	<p>Укажите порт цели SNMP Trap. Агент SNMP будет отправлять сообщения SNMP Trap на этот порт, и диапазон портов составляет от 1 до 65535. Значение по умолчанию - 162.</p>
Trap notification mode	<p>Укажите режим работы уведомлений SNMP Trap. Возможные варианты:</p> <ul style="list-style-type: none"> <li>• Включить: включить режим работы уведомлений SNMP Trap.</li> <li>• Отключить: отключить режим работы уведомлений SNMP Trap.</li> </ul>
Trap notification timeout (seconds)	<p>Укажите время ожидания для уведомлений SNMP Trap. Допустимый диапазон составляет от 0 до 2147.</p>
Trap Inform Retry Times	<p>Укажите количество повторных передач уведомлений SNMP Trap. Допустимый диапазон составляет от 0 до 255.</p>

Параметр	Описание
Trap security engine ID	Укажите идентификатор безопасности SNMP Trap. SNMPv3 отправляет Ловушки и Уведомления с использованием USM для аутентификации и шифрования. Для этих ловушек и уведомлений требуется уникальный идентификатор движка. Строка должна содержать четное количество цифр (в шестнадцатеричном формате) от 10 до 64, но недопустимы все нули и все F.
Trap safe name	Укажите имя безопасности SNMP Trap, которое является именем пользователя. SNMPv3 отправляет Ловушки и Уведомления с использованием USM для аутентификации и шифрования. Уникальное имя безопасности требуется при включении Ловушки и Уведомления.

### 7.6.7.2 Настройки источника

Страница настроек источника, как показано ниже.

**Trap Configuration**

**Trap Source Configurations**

Delete	Name	Type	Subset OID
No entry exists			

Нажмите кнопку "Добавить запись", чтобы перейти на страницу конфигурации источника ловушек, как показано на рисунке ниже..

**Trap Configuration**

**Trap Source Configurations**

Delete	Name	Type	Subset OID
Delete	coldStart	included	

Описание каждого параметра представлено в следующей таблице:

Параметр	Описание
Delete	Удалите запись после выбора, и она будет удалена при следующем сохранении.
Name	Укажите имя записи.

Параметр	Описание
Type	<p>Тип фильтра для записи. Возможные типы:</p> <ul style="list-style-type: none"> <li>Включено: указывает, что Ловушка будет отправлена, когда указанный источник Ловушки соответствует.</li> <li>Исключено: указывает, что когда указанный источник Ловушки соответствует, Ловушка не будет отправлена.</li> </ul>
SubtreeOID	<p>Подмножество OID для этой записи. Значение зависит от имени ловушки. Например, ifIndex является подмножеством OID linkUp и linkDown (то есть порт, который должен отправлять статус ссылки). Если поле не заполнено, это означает, что используются все порты по умолчанию. В противном случае будут отправлены только заполненные порты, если они соответствуют. Допустимые подмножества OID - одно или более чисел или звездочек ( ) разделенных точками (.). Первый символ не должен начинаться с звездочки (*), а максимальное количество OID не должно превышать 128.</p>
Add entry	<p>Щелкните, чтобы добавить новую запись конфигурации источника ловушки. Можно добавить до 32 записей.</p>

## 7.6.8 RMON

### 7.6.8.1 Конфигурация группы статистики

Страница конфигурации группы статистики, как показано на рисунке ниже.

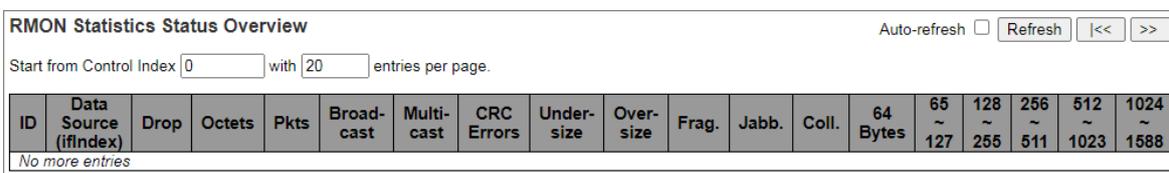
**RMON Statistics Configuration**

Описание каждого параметра представлено в следующей таблице:

Параметр	Описание
Delete	Удалить выбранную запись, и она будет удалена при следующем сохранении.
ID	Укажите индекс записи. Диапазон от 1 до 65535.
Data source	Укажите идентификатор порта для мониторинга. Если это стековый коммутатор, значение должно быть увеличено на 1000000* (ID коммутатора - 1). Например, если порт находится на коммутаторе 3, порт 5, то значение будет 2000005.

### 7.6.8.2 Информация о статистической группе

Страница информации о группе статистики выглядит как показано на рисунке ниже. На этой странице предоставляется обзор записей статистики RMON. Максимум 99 записей может быть отображено на одной странице, по умолчанию 20, управляемое через поле ввода " \_\_\_ записей на странице". При первом посещении веб-страницы будут отображены первые 20 записей, начиная с начальной записи таблицы статистики. Первая отображаемая запись будет той, у которой наименьший идентификатор в таблице статистики. "Контрольный индекс начиная с \_\_\_" позволяет пользователю выбрать начальную точку в таблице статистики. Щелчок по кнопке "Обновить" отобразит запись для "Индексация начинается с \_\_\_".



Описание каждого параметра представлено в следующей таблице:

Параметр	Описание
ID	Укажите индекс записи в группе статистики.
Data source (port index)	Укажите идентификатор мониторируемого порта.
Drop frame	Проанализируйте общее количество событий, в которых пакеты были отброшены из-за нехватки ресурсов.
Byte	Общее количество принятых байтов данных в сети (включая ошибочные пакеты).
Bag	Общее количество принятых пакетов (включая ошибочные пакеты, широковещательные пакеты и многоадресные пакеты).
Broadcast packet	Общее количество корректных пакетов, принятых на широковещательный адрес.
Multicast packet	Общее количество корректных пакетов, принятых на многоадресный адрес.
CRC error frame	Общее количество фреймов с ошибкой проверки цикла CRC.
Ultra short frame	Общее количество принятых фреймов, которые меньше 64 байт.
jumbo frame	Общее количество принятых пакетов, которые больше 1518 байт.
Ultra short FCS error frame	Общее количество принятых фреймов, которые меньше 64 байт и имеют ошибки проверки цикла CRC.
Very long FCS error frame	Общее количество принятых фреймов, которые больше 1518 байт и имеют ошибки проверки цикла CRC.
Conflict frame	Общее количество отправленных фреймов из-за коллизий.
64 bytes	Общее количество принятых пакетов с длиной 64 байта (включая ошибочные пакеты).

Параметр	Описание
65~127	Общее количество принятых пакетов (включая ошибочные пакеты) с длиной от 65 до 127 байт.
128~255	Общее количество принятых пакетов (включая ошибочные пакеты) с длиной от 128 до 255 байт.
256~511	Общее количество принятых пакетов (включая ошибочные пакеты) с длиной от 256 до 511 байт.
512~1023	Общее количество принятых пакетов (включая ошибочные пакеты) с длиной от 512 до 1023 байт.
1024~1588	Общее количество принятых пакетов (включая ошибочные пакеты) с длиной от 1024 до 1588 байт.

### 7.6.8.3 Конфигурация группы истории

Страница конфигурации группы истории выглядит как показано на рисунке ниже.

**RMON History Configuration**

Delete	ID	Data Source	Interval	Buckets	Buckets Granted

Описание каждого параметра представлено в следующей таблице:

Параметр	Описание
Delete	Удалите запись после выбора, и она будет удалена при следующем сохранении.
ID	Укажите индекс записи. Диапазон от 1 до 65535.
Data source	Укажите идентификатор порта для мониторинга. Если это стековый коммутатор, к значению необходимо добавить 1000000 * (ID коммутатора - 1). Например, если порт находится на коммутаторе 3, порт 5, то значение будет 2000005.
Sample interval	Укажите интервал в секундах для выборки исторической статистики. Диапазон от 1 до 3600 секунд, значение по умолчанию - 1800 секунд.
Maximum number of samples	Укажите максимальное количество выбираемых данных, связанных с этой записью управления историей, хранящихся в RMON. Диапазон от 1 до 65535, значение по умолчанию - 50.
Actual number of samples	Фактическое количество данных, хранящихся в RMON.

### 7.6.8.4 Информация о группе истории

Страница информации о группе истории выглядит как показано на рисунке ниже. На этой странице предоставляется обзор записей истории RMON. Максимум 99 записей может быть

отображено на одной странице, значение по умолчанию - 20, управляется через поле ввода "\_\_\_ записей на странице". При первом посещении веб-страницы будут отображены первые 20 записей, начиная с начала таблицы истории. Первая отображаемая запись будет той, у которой наименьший индекс истории и индекс выборки в таблице истории. Контрольный индекс и индекс выборки "Начиная с \_\_\_" позволяют пользователю выбрать начальную точку в таблице истории. Щелчок по кнопке "Обновить" отобразит записи для контрольного индекса и индекса выборки "Начиная с \_\_\_".

**RMON History Overview** Auto-refresh  Refresh |<< >>

Start from Control Index  and Sample Index  with  entries per page.

History Index	Sample Index	Sample Start	Drop	Octets	Pkts	Broad-cast	Multi-cast	CRC Errors	Under-size	Over-size	Frag.	Jabb.	Coll.	Utilization
No more entries														

Описание каждого параметра представлено в следующей таблице:

Параметр	Описание
Index	Укажите индекс записи управления историей.
Sample index	Укажите индекс записи выборки данных, связанной с записью управления.
Start sample	Значение sysUpTime (время работы системы) в начале интервала выборки.
Drop frame	Общее количество обнаруженных событий, в которых пакеты были отброшены из-за нехватки ресурсов.
Byte	Общее количество принятых байтов данных в сети (включая ошибочные пакеты).
Bag	Общее количество принятых пакетов (включая ошибочные пакеты, широковещательные пакеты и многоадресные пакеты).
Broadcast packet	Общее количество корректных пакетов, принятых на широковещательный адрес.
Multicast packet	Общее количество корректных пакетов, принятых на многоадресный адрес.
CRC error frame	Общее количество фреймов с ошибкой проверки цикла CRC.
Ultra short frame	Общее количество принятых фреймов, которые меньше 64 байт.
Jumbo frame	Общее количество принятых фреймов, которые больше 1518 байт.
Ultra short FCS error frame	Общее количество принятых фреймов, которые меньше 64 байт и имеют ошибки проверки цикла CRC.
Very long FCS error frame	Общее количество принятых фреймов, которые больше 1518 байт и имеют ошибки проверки цикла CRC.
Conflicting packages	Общее количество отправленных фреймов из-за коллизий.
Utilization	Наилучшая оценка средней использованности физического уровня сети на этом интерфейсе в течение этого интервала выборки, выраженная в процентах.

### 7.6.8.5 Конфигурация группы оповещений

Страница конфигурации группы сигнализации выглядит как показано на рисунке ниже.

**RMON Alarm Configuration**

Delete	ID	Interval	Variable	Sample Type	Value	Startup Alarm	Rising Threshold	Rising Index	Falling Threshold	Falling Index
<div style="display: flex; justify-content: space-around; align-items: center;"> <input type="button" value="Add New Entry"/> <input type="button" value="Save"/> <input type="button" value="Reset"/> </div>										

Описание каждого параметра представлено в следующей таблице:

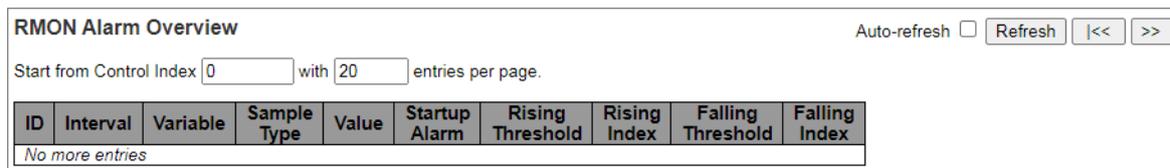
Параметр	Описание
Delete	Удалить выбранную запись, и она будет удалена при следующем сохранении.
ID	Укажите индекс записи. Диапазон от 1 до 65535.
Sample interval	Укажите интервал в секундах для выборки и сравнения верхних и нижних порогов. Диапазон от 1 до 2 <sup>31</sup> -1.

Параметр	Описание
Sample variable	<p>Укажите конкретную переменную для выборки. Возможные переменные:</p> <ul style="list-style-type: none"> <li>• InOctets: Общее количество байтов, полученных на интерфейсе, включая преамбулу фрейма.</li> <li>• InUcastPkts: Количество полученных уникальных пакетов.</li> <li>• InNUcastPkts: Количество полученных широковещательных и многоадресных пакетов.</li> <li>• InDiscards: Количество отброшенных пакетов на входе, даже если они являются нормальными пакетами.</li> <li>• InErrors: Количество входящих пакетов, содержащих ошибки.</li> <li>• InUnknownProtos: Количество входящих пакетов, которые были отброшены из-за неизвестных или не поддерживаемых протоколов.</li> <li>• OutOctets: Общее количество байтов, отправленных на интерфейсе, включая преамбулу фрейма.</li> <li>• OutUcastPkts: Количество отправленных уникальных пакетов.</li> <li>• OutNUcastPkts: Количество отправленных широковещательных и многоадресных пакетов.</li> <li>• OutDiscards: Количество исходящих пакетов, отброшенных, даже если они являются нормальными пакетами.</li> <li>• OutErrors: Количество исходящих пакетов, которые не могли быть переданы из-за ошибок.</li> <li>• OutQLen: Длина очереди исходящих пакетов (в пакетах).</li> </ul>
Sample type	<p>Метод выборки выбранной переменной и расчет значения, которое будет сравниваться с порогом. Возможные типы выборки:</p> <ul style="list-style-type: none"> <li>• Абсолютный: Получить выборку напрямую.</li> <li>• Дельта: рассчитать разницу между выборками (по умолчанию).</li> </ul>
Sample value	Значение статистики за предыдущий период выборки.

Параметр	Описание
Start alarm	Как активировать сигнализацию. Возможные типы сигнализации: <ul style="list-style-type: none"> <li>• Повышение: Сигнализация активируется, когда первое значение превышает верхний порог.</li> <li>• Понижение: Сигнализация активируется, когда первое значение меньше нижнего порога.</li> <li>• Повышение или понижение: Сигнализация активируется, когда первое значение превышает верхний порог или меньше нижнего порога (по умолчанию).</li> </ul>
Upper limit	Верхний порог (-2147483648 - 2147483647).
Upper bound index	Индекс ограниченного события (0-65535). Если это значение равно нулю, связанное событие не будет сгенерировано, потому что ноль не является допустимым индексом события.
Lower limit	Нижний порог (-2147483648 - 2147483647).
Lower bound index	Индекс нижней границы события (0-65535). Если это значение равно нулю, связанное событие не будет сгенерировано, потому что ноль не является допустимым индексом события.

### 7.6.8.6 Информация о группе сигнализации

Страница информации о группе сигнализации выглядит как показано на рисунке ниже. На этой странице предоставляется обзор записей сигнализации RMON. Максимум 99 записей может быть отображено на одной странице, значение по умолчанию - 20, управляется через поле ввода "\_\_\_ записей на странице". При первом посещении веб-страницы будут отображены первые 20 записей, начиная с начала таблицы сигнализации. Первая отображаемая запись будет той, у которой наименьший идентификатор в таблице сигнализации. "Контрольный индекс начиная с \_\_\_" позволяет пользователю выбрать начальную точку для записей в таблице сигнализации. Щелчок по кнопке "Обновить" отобразит запись для "Контрольный индекс начиная с \_\_\_".



Описание каждого параметра представлено в следующей таблице:

Параметр	Описание
ID	Укажите индекс записи. Диапазон от 1 до 65535.

Параметр	Описание
Sampling interval	Укажите интервал в секундах для выборки и сравнения верхних и нижних порогов. Диапазон от 1 до 2 <sup>31</sup> -1.
Sample variable	<p>Укажите конкретную переменную для выборки. Возможные переменные:</p> <ul style="list-style-type: none"> <li>• InOctets: Общее количество байтов, полученных на интерфейсе, включая преамбулу фрейма.</li> <li>• InUcastPkts: Количество полученных уникальных пакетов.</li> <li>• InNUcastPkts: Количество полученных широковещательных и многоадресных пакетов.</li> <li>• InDiscards: Количество отброшенных пакетов на входе, даже если они являются нормальными пакетами.</li> <li>• InErrors: Количество входящих пакетов, содержащих ошибки.</li> <li>• InUnknownProtos: Количество входящих пакетов, которые были отброшены из-за неизвестных или не поддерживаемых протоколов.</li> <li>• OutOctets: Общее количество байтов, отправленных на интерфейсе, включая преамбулу фрейма.</li> <li>• OutUcastPkts: Количество отправленных уникальных пакетов.</li> <li>• OutNUcastPkts: Количество отправленных широковещательных и многоадресных пакетов.</li> <li>• OutDiscards: Количество исходящих пакетов, отброшенных, даже если они являются нормальными пакетами.</li> <li>• OutErrors: Количество исходящих пакетов, которые не могли быть переданы из-за ошибок.</li> <li>• OutQLen: Длина очереди исходящих пакетов (в пакетах).</li> </ul>
Sample type	<p>Тип выборки: Метод выборки выбранной переменной и расчет значения, которое будет сравниваться с порогом. Возможные типы выборки:</p> <ul style="list-style-type: none"> <li>• Абсолютный: Получить выборку напрямую.</li> <li>• Дельта: рассчитать разницу между выборками (по умолчанию).</li> </ul>
Sample value	Значение статистики за последний период выборки.

Параметр	Описание
Start alarm	Как активировать сигнализацию. Возможные типы сигнализации: <ul style="list-style-type: none"> <li>• Повышение: Сигнализация активируется, когда первое значение превышает верхний порог.</li> <li>• Понижение: Сигнализация активируется, когда первое значение меньше нижнего порога.</li> <li>• Повышение или понижение: Сигнализация активируется, когда первое значение превышает верхний порог или меньше нижнего порога (по умолчанию).</li> </ul>
Upper limit	Верхний порог (-2147483648 - 2147483647).
Upper bound index	Индекс ограниченного события (0-65535). Если это значение равно нулю, связанное событие не будет генерироваться, потому что ноль не является допустимым индексом события.
Lower limit	Нижний порог (-2147483648 - 2147483647).
Lower bound index	Индекс нижней границы события (0-65535). Если это значение равно нулю, связанное событие не будет генерироваться, потому что ноль не является допустимым индексом события.

### 7.6.8.7 Конфигурация группы событий

На странице конфигурации группы событий, как показано на рисунке ниже.

**RMON Event Configuration**

Delete	ID	Desc	Type	Event Last Time
<input type="button" value="Add New Entry"/> <input type="button" value="Save"/> <input type="button" value="Reset"/>				

Описание каждого параметра представлено в следующей таблице:

Параметр	Описание
Delete	Удалите выбранную запись, и она будет удалена при следующем сохранении.
ID	Укажите индекс записи. Диапазон от 1 до 65535.
Describe	Опишите это событие. Длина строки от 0 до 127 символов. Значение по умолчанию - пустая строка.

Параметр	Описание
Type	Уведомление о событии, возможные типы: <ul style="list-style-type: none"> <li>none: Нет создания SNMP-логов и нет отправки SNMP-ловушек.</li> <li>log: Создает запись SNMP-лога при срабатывании события.</li> <li>snmptrap: Отправляет SNMP-ловушку при срабатывании события.</li> <li>logandtrap: Создает записи SNMP-лога и отправляет SNMP-ловушки при срабатывании событий.</li> </ul>
The time of the most recent incident	Значение sysUpTime, когда данная запись события последний раз генерировала событие.

### 7.6.8.8 Информация о группе событий

Страница информации о группе событий отображается на рисунке ниже. Эта страница предоставляет обзор записей таблицы событий RMON. Максимум 99 записей может быть отображено на одной странице, значение по умолчанию - 20, управляется через поле ввода "\_\_\_ записей на странице". При первом доступе к веб-странице будут отображены первые 20 записей, начиная с начала таблицы событий. Первая отображаемая запись будет той, у которой наименьший индекс события и индекс лога в таблице событий. "Контрольный индекс начиная с \_\_\_" позволяет пользователю выбрать начальную точку в таблице событий. Щелчок по кнопке "Обновить" отобразит запись для "Контрольный индекс начиная с \_\_\_".

**RMON Event Overview** Auto-refresh  Refresh |<< >>

Start from Control Index  and Sample Index  with  entries per page.

Event Index	LogIndex	LogTime	LogDescription
No more entries			

Описание каждого параметра представлено в следующей таблице:

Параметр	Описание
Event index	Укажите индекс записи события.
Log index	Укажите индекс записи журнала.
Log time	Укажите время записи события.
Log description	Укажите описание события.

## 7.7 Порт безопасности

Port Security повышает безопасность устройства путем преобразования динамического MAC-адреса, изученного интерфейсом, в безопасный MAC-адрес (включая безопасный динамический MAC, безопасный статический MAC и прилипший MAC), чтобы предотвратить связь нелегальных пользователей с коммутатором через этот интерфейс. После включения функции безопасности порта, когда обнаруживается нелегальное сообщение, система запускает соответствующие функции и обрабатывает его заранее определенным образом, что упрощает управление пользователями и повышает безопасность системы. Нелегальные пакеты здесь относятся к пользовательским пакетам, MAC-адрес которых не был изучен портом.

### Классификация безопасных MAC-адресов

Безопасные MAC-адреса разделяются на: безопасный динамический MAC, безопасный статический MAC и липкий MAC.

Тип	Определение	Характеристики
Secure dynamic MAC	MAC-адрес, преобразованный при включенной функции безопасности порта, но при этом функция "липкий MAC" не включена.	После перезапуска устройства записи в таблице будут утеряны и должны будут быть заново изучены. По умолчанию, они не будут подвержены старению. Старение может быть включено только после включения соответствующей функции. Правила старения следующие: когда MAC-адрес преобразуется в безопасный динамический MAC, запускается таймер старения. По истечении времени таймера MAC-адрес проверяется на наличие трафика. Если в следующем цикле старения трафика нет, MAC-адрес подвергается старению для освобождения ресурсов.
Secure static MAC	Статический MAC-адрес, вручную настроенный после включения безопасности порта.	После сохранения конфигурации вручную и перезапуска устройства записи в таблице не будут устаревать и не будут потеряны.
Sticky MAC	MAC-адрес, преобразованный после включения безопасности порта и одновременного включения функции "липкий".	После сохранения конфигурации вручную и перезапуска устройства записи в таблице не будут устаревать и не будут потеряны.

### Port Security Protection Mode

После того как количество безопасных MAC-адресов на интерфейсе достигнет предела (лимита), если коммутатор получит пакет с несуществующим исходным MAC-адресом,

независимо от того, существует ли целевой MAC-адрес, коммутатор считает, что происходит атака от несанкционированного пользователя и будет защищать интерфейс в соответствии с настроенными действиями.

Режим нарушения	Описание
Restrict	MAC-адреса, превышающие лимит, будут изучены и помечены как нарушающие, пока не достигнут предел нарушений. По истечении времени удержания эти MAC-адреса будут удалены. Пакеты с несуществующими исходными MAC-адресами будут отбрасываться.
Protect	MAC-адреса, превышающие лимит, не будут изучаться, и будут отбрасываться только пакеты с несуществующими исходными MAC-адресами.
Shutdown	Максимальное количество изучаемых MAC-адресов ограничено лимитом, и еще один MAC-адрес вызовет отключение порта. Существует три метода восстановления порта: <ul style="list-style-type: none"> <li>• Отключить, а затем снова включить порт в представлении конфигурации порта.</li> <li>• Изменить конфигурацию безопасности порта этого порта.</li> <li>• Перезагрузить устройство.</li> </ul>



Примечание:

MAC-адреса, помеченные как нарушающие, не являются безопасными MAC-адресами. Это означает, что пакеты с исходными MAC-адресами, отмеченными как нарушающие, не будут перенаправляться.

### Sticky MAC (клейкий MAC)

После настройки функции безопасности порта MAC-адреса, изученные интерфейсом, будут преобразованы в безопасные MAC-адреса. После того как максимальное количество изученных интерфейсом MAC-адресов достигнет верхнего предела, он перестанет изучать новые MAC-адреса, и только эти MAC-адреса будут разрешены для общения с коммутатором. Если пользователь доступа изменится, вы можете обновить запись в таблице MAC-адресов, перезагрузив устройство или настроив время устаревания безопасного MAC-адреса. Для относительно стабильных пользователей сети, если вы не хотите последующих изменений, вы можете дополнительно включить функцию клейкого MAC-адреса на интерфейсе, чтобы записи в таблице MAC-адресов не обновлялись или не терялись после

сохранения конфигурации. Функция Sticky MAC обычно используется в сетях с небольшим числом изменений конечных пользователей. Sticky MAC не будет устаревать при изменении связи порта.

## 7.7.1 Конфигурация порта

На веб-странице конфигурации порта, изображенной на рисунке ниже, можно настроить глобальные параметры, такие как функция устаревания, период устаревания и время удержания.

**Port Security Configuration** Refresh

**Global Configuration**

Aging Enabled	<input type="checkbox"/>	
Aging Period	<input type="text" value="3600"/>	seconds
Hold Time	<input type="text" value="300"/>	seconds

**Port Configuration**

Port	Mode	Limit	Violation Mode	Violation Limit	Sticky	State
*	<>	4	<>	4	<input type="checkbox"/>	
1	Disabled	4	Protect	4	<input type="checkbox"/>	Disabled
2	Disabled	4	Protect	4	<input type="checkbox"/>	Disabled
3	Disabled	4	Protect	4	<input type="checkbox"/>	Disabled
4	Disabled	4	Protect	4	<input type="checkbox"/>	Disabled
5	Disabled	4	Protect	4	<input type="checkbox"/>	Disabled
6	Disabled	4	Protect	4	<input type="checkbox"/>	Disabled
7	Disabled	4	Protect	4	<input type="checkbox"/>	Disabled
8	Disabled	4	Protect	4	<input type="checkbox"/>	Disabled
9	Disabled	4	Protect	4	<input type="checkbox"/>	Disabled
10	Disabled	4	Protect	4	<input type="checkbox"/>	Disabled
11	Disabled	4	Protect	4	<input type="checkbox"/>	Disabled
12	Disabled	4	Protect	4	<input type="checkbox"/>	Disabled

Описание каждого параметра представлено в следующей таблице:

Параметр	Описание
<b>Global configuration</b>	<b>Глобальная конфигурация</b>
Aging enabled	При включении безопасный динамический MAC-адрес будет периодически устаревать для освобождения ресурсов.
Aging cycle	Диапазон составляет от 10 до 10000000 секунд, а значение по умолчанию - 3600 секунд.
Hold time	Диапазон составляет от 10 до 10000000 секунд, а значение по умолчанию - 300 секунд. Нарушающие MAC-адреса будут удалены после времени удержания. Причина сохранения нарушающих MAC-адресов в таблице адресов заключается в том, чтобы предотвратить появление одного и того же MAC-адреса непрерывно, что может вызвать продолжение связанных с этим информации об ошибках.

Параметр	Описание
<b>Port configuration</b>	<b>Конфигурация порта</b>
Mode	Включение/отключение по выбору, можно установить, включить ли безопасность порта.
Limit	Диапазон составляет от 0 до 1023, а значение по умолчанию - 4. Установите предел безопасных MAC-адресов.
Violation pattern	<p>Опционально Защита/Ограничение/Отключение.</p> <ul style="list-style-type: none"> <li>Защита: MAC-адреса, превышающие предел, не будут изучаться, и только пакеты с несуществующими исходными MAC-адресами будут отбрасываться.</li> <li>Ограничение: MAC-адреса, превышающие предел, будут изучены и помечены как нарушающие. Максимум нарушающих пределов будет изучено. По истечении времени удержания эти MAC-адреса будут удалены. Пакеты с несуществующими исходными MAC-адресами будут отбрасываться.</li> <li>Отключение: Максимум Limit MAC-адресов может быть изучено, и еще один MAC-адрес вызовет отключение порта.</li> </ul>
Violation restrictions	Диапазон составляет от 0 до 1023, а значение по умолчанию - 4. Установите максимальное количество MAC-адресов, которые могут быть помечены как нарушающие. Это влияет только в том случае, когда режим нарушения установлен как Ограничение.
Sticky	Установите, включить ли функцию Sticky. Sticky MAC не будет устаревать при изменении состояния порта.
State	<p>Есть 4 состояния: Отключено/Готово/Достигнут предел/Отключение, отображающие текущий статус безопасности порта.</p> <ul style="list-style-type: none"> <li>Отключено: указывает, что безопасность порта отключена.</li> <li>Готово: указывает, что количество безопасных MAC-адресов еще не достигло максимального предела.</li> <li>Достигнут предел: указывает, что количество безопасных MAC-адресов достигло максимального предела.</li> <li>Отключение: указывает, что порт отключен функцией безопасности порта.</li> </ul>

## 7.7.2 MAC конфигурация

Страница конфигурации MAC-адресов показана на рисунке ниже, где вы можете добавить статический MAC-адрес или Sticky MAC-адрес. Щелкните кнопку "Добавить новую запись MAC-адреса", чтобы добавить новый MAC-адрес, который вступит в силу после нажатия кнопки "Сохранить".

Port Security Static and Sticky MAC Addresses Refresh

Delete	Port	VLAN ID	MAC Address	Type
Add New MAC Entry				

Save Reset



Примечание:

Когда количество безопасных MAC-адресов (включая динамические и статические адреса) достигает максимального предела, больше нельзя добавлять статические безопасные MAC-адреса.

## 7.7.3 Глобальный статус

Эта страница отображает информацию о безопасности портов. Функция безопасности портов может быть настроена напрямую или косвенно через другие функциональные модули, такие как 802.1X и Voice VLAN. В таблице состояния портов столбец "Пользователь" указывает на настроившего безопасность портов и идентифицируется с помощью

аббревиатур. Для значений аббревиатур обратитесь к " User Module Legend".

**Port Security Switch Status** Auto-refresh  Refresh

**User Module Legend**

User Module Name	Abbr
Port Security (Admin)	P
802.1X	8
Voice VLAN	V

**Port Status**

Clear	Port	Users	Violation Mode	State	MAC Count		
					Current	Violating	Limit
Clear	1	---	Disabled	Disabled	-	-	-
Clear	2	---	Disabled	Disabled	-	-	-
Clear	3	---	Disabled	Disabled	-	-	-
Clear	4	---	Disabled	Disabled	-	-	-
Clear	5	---	Disabled	Disabled	-	-	-
Clear	6	---	Disabled	Disabled	-	-	-
Clear	7	---	Disabled	Disabled	-	-	-
Clear	8	---	Disabled	Disabled	-	-	-
Clear	9	---	Disabled	Disabled	-	-	-
Clear	10	---	Disabled	Disabled	-	-	-
Clear	11	---	Disabled	Disabled	-	-	-

Описание каждого параметра представлено в следующей таблице:

Параметр	Описание
User module legend	Легенда модуля пользователя
Full name of user module	Полное название модуля, который может запрашивать услуги безопасности портов.
abbreviation	Аббревиатура модуля пользователя. Используется в столбце "Пользователь" таблицы состояния портов.
port status	Состояние порта
Clear	Щелкните, чтобы удалить все динамические MAC-адреса для всех VLAN на этом порту. Эта кнопка доступна для нажатия только в случае, если количество безопасных MAC-адресов ненулевое.
port	Номер порта состояния приложения. Щелкните на номер порта, чтобы просмотреть состояние этого конкретного порта.
user	У модулей пользователя есть столбец, который показывает, включена ли для них функция безопасности портов. "-" указывает на то, что соответствующий модуль пользователя не включен, в то время как буква указывает, что модуль пользователя, сокращенный этой буквой (см. Аббревиатуру), имеет включенную функцию безопасности портов.

Параметр	Описание
Violation pattern	<p>Отображается режим нарушения конфигурации порта. Принимает одно из следующих четырех значений:</p> <ul style="list-style-type: none"> <li>Отключено: На этом порту нет административно включенной безопасности порта.</li> <li>Защита: Безопасность порта административно включена в режиме защиты.</li> <li>Ограничено: Безопасность порта административно включена в режиме ограничения.</li> <li>Выключено: Безопасность порта административно включена в режиме отключения.</li> </ul>
state	<p>Отображается текущий статус порта. Принимает одно из следующих четырех значений:</p> <ul style="list-style-type: none"> <li>Отключено: На данный момент ни один модуль пользователя не использует сервис безопасности порта.</li> <li>Готово: Сервис безопасности порта используется как минимум одним модулем пользователя и ожидает появления кадров с неизвестными MAC-адресами.</li> <li>Достигнут лимит: Сервис безопасности порта включен как минимум модулем управления лимитом, что указывает на то, что лимит достигнут, и больше MAC-адресов приниматься не должно.</li> <li>Отключение: Сервис безопасности порта включен как минимум модулем управления лимитом, который указал, что лимит превышен. MAC-адрес не может быть изучен на порте до тех пор, пока не будет повторно открыта страница веб-конфигурации контроля ограничения на управлении портами.</li> </ul>
MAC address statistics	<p>Эти два столбца представляют текущее количество изученных MAC-адресов (пересылка и блокировка) и максимальное количество MAC-адресов, которые можно изучить на порту, соответственно.</p> <ul style="list-style-type: none"> <li>Если на порту не включен ни один пользовательский модуль, то текущий столбец будет отображать тире (-).</li> <li>Если модуль управления пределом не включен на порту, то столбец предела будет отображать тире (-).</li> </ul>

## 7.7.4 Статус порта

Эта страница отображает таблицу защищенных MAC-адресов, которую можно фильтровать и просматривать по портам, а также можно непосредственно удалять защищенные MAC-адреса..

**Port Security Port Status All Ports** All  Auto-refresh

Delete	Port	VLAN ID	MAC Address	Type	State	Age/Hold
No MAC addresses attached						

Описание каждого параметра представлено в следующей таблице:

Параметр	Описание
Delete	Нажмите, чтобы удалить этот конкретный MAC-адрес из таблицы MAC-адресов. Эта кнопка доступна только если тип записи - Dynamic.
port	Если показано "Все порты" (выбирается через выпадающий список в верхней части), это покажет порт, к которому привязан MAC-адрес.
VLAN ID	ID VLAN, отображаемый на этом порту.
MAC address	MAC-адрес, отображаемый на этом порту. Если MAC-адрес не известен, будет отображена строка "MAC-адрес не указан".
Type	<p>Укажите тип записи. Принимает одно из трех значений:</p> <ul style="list-style-type: none"> <li>• Динамический: когда порт не находится в режиме "Sticky", записи изучаются через прибывающие фреймы обучения в модуле безопасности порта.</li> <li>• Статический: запись вводится конечным пользователем через административный доступ. Записи не подвержены ограничениям по сроку службы.</li> <li>• Sticky: когда порт находится в режиме "Sticky", все записи, которые в противном случае будут изучены как динамические, будут изучены как "Sticky".</li> </ul> <p>Иллюстрация: Записи Sticky являются частью текущей конфигурации и, следовательно, могут быть сохранены в запускающейся конфигурации. Важным аспектом стикеров MAC-адресов является то, что они выживают при изменении соединения (в отличие от динамических, которые требуют повторного изучения). Если текущая конфигурация сохраняется в запускающуюся конфигурацию, они также могут выжить после перезагрузок.</p>
State	Укажите, находится ли соответствующий MAC-адрес в нарушении (пользователь управления настроил интерфейс в режиме "restricted" и MAC-адрес заблокирован), заблокирован или перенаправлен

Параметр	Описание
Aging/holding time	<ul style="list-style-type: none"> <li>• Если хотя бы один модуль пользователя решит заблокировать этот MAC-адрес, он останется заблокированным до истечения времени удержания (в секундах).</li> <li>• Если все модули пользователя решат разрешить этот MAC-адрес для пересылки, и функция старения включена, модуль безопасности порта периодически будет проверять, пересылает ли этот MAC-адрес еще трафик.</li> <li>• Если истекло время старения (в секундах), и фреймы не обнаружены, MAC-адрес удаляется из таблицы MAC. В противном случае начнется новый период старения.</li> <li>• Если старение отключено или модуль пользователя решает сохранять MAC-адрес бессрочно, отображается тире (-).</li> </ul>

## 7.8 802.1X порт аутентификация

### 7.8.1 Протокол 802.1X

#### 7.8.1.1 802.1X

Протокол 802.1X представляет собой протокол управления доступом к сети на основе портов (Port-based Network Access Control, Port-Based NAC) и является протоколом уровня 2 (Data Link Layer). Он используется для взаимодействия между пользователями и устройствами доступа с целью обеспечения установки безопасного и стабильного соединения между ними.

#### 7.8.1.2 802.1X Принцип работы

#### 802.1X Система аутентификации

Система 802.1X имеет типичную структуру Клиент/Сервер, включающую три сущности: клиент, устройство доступа и аутентификационный сервер.

- ◆ Клиент: обычно это устройство конечного пользователя, пользователь может инициировать аутентификацию 802.1X, запустив клиентское программное обеспечение. Клиент должен поддерживать протокол расширяемой аутентификации по сети LAN (EAPoL).

- ◆ Устройство доступа: обычно это сетевое устройство, поддерживающее протокол 802.1X. Оно предоставляет клиенту порт для доступа к локальной сети. Порт может быть физическим или логическим.
- ◆ Аутентификационный сервер: используется для осуществления аутентификации, авторизации и учета пользователей, обычно это сервер RADIUS.

### 802.1X протокол аутентификации

Система аутентификации 802.1X использует протокол расширяемой аутентификации (EAP) для обмена информацией между клиентом, устройством и сервером аутентификации. Протокол EAP может работать на различных нижних уровнях, включая уровень канала передачи данных и протоколы верхних уровней (например, UDP, TCP и т. д.), не требуя IP-адреса. Поэтому аутентификация 802.1X с использованием протокола EAP обладает хорошей гибкостью.

- ◆ Между клиентом и устройством сообщения протокола EAP используют формат инкапсуляции EAPoL (EAP over LANs) и непосредственно передаются в среде LAN.
- ◆ Между устройством и сервером аутентификации пользователи могут выбирать метод аутентификации на основе поддержки клиента и требований к безопасности сети.

### EAP инкапсуляция

EAPoL (EAP over LAN) - это формат инкапсуляции сообщений (определенный в RFC3784), используемый протоколом 802.1X. Он в основном используется для передачи сообщений протокола EAP между клиентами и устройствами, чтобы позволить передавать сообщения протокола EAP по LAN. Тип Ethernet для протокола PAE: 0x888E. Структура сообщения следующая:

Тип Ethernet PAE	Версия протокола	Тип	Длина	Тело пакета
------------------	------------------	-----	-------	-------------

EAPoR (EAP over RADIUS) добавляет два атрибута к протоколу RADIUS: EAP-Message (сообщение EAP) и Message-Authenticator (код аутентификации сообщения). Среди них, атрибут EAP-Message используется для инкапсуляции сообщений EAP, а атрибут Message-Authenticator используется для аутентификации и проверки аутентификационных сообщений для предотвращения незаконного подделывания сообщений. Структура сообщения следующая:

Код	Идентификатор	Длина	Аутентификатор ответа	Атрибуты
-----	---------------	-------	-----------------------	----------

Тип	Длина	Значение
-----	-------	----------

## EAP метод аутентификации

Обмен сообщениями EAP между устройством и сервером RADIUS выполняется двумя механизмами обработки: пробросом EAP и завершением EAP. В этом продукте используется механизм проброса EAP для аутентификации.

- ◆ Метод завершения EAP: Сообщения EAP завершаются на устройстве и повторно инкапсулируются в сообщения RADIUS, используя стандартный протокол RADIUS для завершения аутентификации, авторизации и учета. При этом механизме обработки, поскольку существующие серверы RADIUS в основном поддерживают аутентификацию PAP и CHAP, для сервера нет особых требований, но обработка на стороне устройства более сложная. Устройство должно действовать в качестве сервера EAP для разбора и обработки сообщений EAP клиента.
- ◆ Режим проброса EAP: Пакеты EAP непосредственно инкапсулируются в пакеты RADIUS (EAP через RADIUS, называемые EAPoR), чтобы пройти через сложные сети и достичь сервера аутентификации. При этом механизме обработки аутентификация EAP выполняется между клиентом и сервером RADIUS. Сервер RADIUS выступает в качестве сервера EAP для обработки запроса аутентификации EAP клиента. Устройство действует как реле и только пересылает сообщения EAP. Поэтому обработка на устройстве проста, и оно может поддерживать различные методы аутентификации EAP, но требуется, чтобы сервер RADIUS поддерживал соответствующие методы аутентификации EAP.

## 802.1X режим аутентификации

На основе порта этот продукт поддерживает следующие режимы аутентификации:

- ◆ Принудительно недопущенные (Force Unauthorized): Устройство отправит сообщение об ошибке EAPoL программе клиента, когда порт будет подключен. Все пользователи на порте не смогут получить доступ к сети.
- ◆ На основе порта 802.1X (Port-based 802.1X): Этот метод контроля доступа основан на портах. После успешной аутентификации первого пользователя на порту другие пользователи могут использовать сетевые ресурсы без аутентификации. Однако, когда первый пользователь отключается, другим пользователям также будет отказан

доступ к сети.

- ◆ **Одиночная аутентификация 802.1X (Single 802.1X):** подобно на основе порта 802.1X, но порт позволяет использовать сеть только одному успешно аутентифицированному пользователю. Первый успешно аутентифицированный пользователь, кто бы это ни был, может использовать сеть, и его MAC-адрес будет установлен как безопасный MAC-адрес благодаря модулю безопасности порта.
- ◆ **Множественная аутентификация 802.1X (Multi 802.1X):** Один порт позволяет множеству успешно аутентифицированных пользователей использовать сеть, и количество пользователей может быть ограничено с помощью функции безопасности порта. Когда на порту нет аутентификации пользователей, устройство использует многоадресный адрес для отправки сообщений EAPoL. В противном случае устройство анализирует MAC-адрес пользователя на основе полученного сообщения EAPoL, а затем использует MAC-адрес для отправки EAPoL для аутентификации каждого пользователя отдельно.
- ◆ **Аутентификация на основе MAC-адреса (MAC-based Auth):** Пользователям не требуется программа клиента 802.1X. Устройство завершает функции программы клиента 802.1X и взаимодействует с сервером RADIUS. Устройство будет перехватывать любой пакет, отправленный пользователем, получать его MAC-адрес, использовать его в качестве имени пользователя и пароля (в формате "xx-xx-xx-xx-xx-xx") и аутентифицироваться на сервере RADIUS. Метод аутентификации поддерживает только вызовы MD5. Поэтому сервер RADIUS должен быть настроен заранее при использовании этого метода. Количество пользователей может быть ограничено с помощью функции безопасности порта.

### 7.8.1.3 802.1X аутентификация

#### QoS and VLAN авторизация

Аутентификация используется для подтверждения легитимности идентификации пользователя, пытающегося получить доступ к сети, в то время как авторизация используется для определения прав доступа к сети, которые могут иметь легитимные пользователи, то есть, к каким ресурсам пользователь может получить доступ. Самыми базовыми и наиболее часто используемыми параметрами авторизации для определения прав доступа являются VLAN, QoS и т. д.

Этот продукт поддерживает авторизацию по VLAN и авторизацию по QoS, которые действительны только в режимах аутентификации на основе портов 802.1X и одиночной аутентификации 802.1X.:

Авторизация	RADIUS атрибут	Описание
QoS	User-Priority-Table (Таблица Приоритетов Пользователя) (RFC4675): Значения от "0" до "7"	Устройство применит приоритет обслуживания QoS, авторизованный RADIUS, к порту, но не изменит исходную конфигурацию QoS порта. После отключения пользователя вступит в силу исходная конфигурация QoS порта.
VLAN	Tunnel-Medium-Type (Тип Туннеля): "IEEE-802" Tunnel-Type (Тип Туннеля): "VLAN" Tunnel-Private-Group-ID (Идентификатор Приватной Группы Туннеля): Значения от "1" до "4095"	Устройство применит VLAN, авторизованный RADIUS, к порту, но не изменит исходную конфигурацию VLAN порта. После отключения пользователя вступит в силу исходная конфигурация VLAN порта. Вы можете проверить, какие модули покрывают текущую конфигурацию VLAN порта на странице VLAN.

### Гостевой VLAN

Гостевая VLAN позволяет пользователям получать доступ к ресурсам в определенной VLAN без аутентификации. Обычно эта VLAN содержит некоторые серверы, с помощью которых пользователи могут скачивать клиентское программное обеспечение или другие программы обновлений. Гостевая VLAN действует только в режимах аутентификации на основе портов 802.1X, одиночной аутентификации 802.1X и множественной аутентификации 802.1X.

Порт устройства будет записывать, получал ли порт сообщение EAPOL (эта запись будет очищаться при отключении порта или изменении режима аутентификации порта). После включения гостевой VLAN на порту устройства и доступа пользовательского терминала к порту, устройство отправит сообщение EAPOL Request Identity на пользовательский терминал с интервалом таймаута EAPOL. Если не получен ответ от пользовательского терминала после превышения количества отправленных запросов максимального числа повторных аутентификаций, устройство готово войти в гостевую VLAN. Если включена опция "Разрешить вход в гостевую VLAN при получении EAPOL", даже если порт записывает, что он получил сообщения EAPOL, ему будет разрешен вход в гостевую VLAN; если опция "Разрешить вход в гостевую VLAN при получении EAPOL" отключена, устройство сначала проверит, получал ли порт сообщение EAPOL. Если он его не получал, он сразу войдет в гостевую VLAN. В противном случае устройство не войдет в гостевую VLAN, а продолжит отправлять сообщения EAPOL Request Identity и ожидать аутентификации.

В гостевой VLAN устройство все равно будет контролировать сообщения EAPOL. Если оно получит запрос на аутентификацию, оно сразу выйдет из гостевой VLAN и выполнит процесс аутентификации.

## 7.8.2 Конфигурация порта

802.1X конфигурация делится на системную (глобальную) конфигурацию и конфигурацию портов, как показано на следующей схеме:

**Network Access Server Configuration** Refresh

**System Configuration**

Mode	Disabled
Reauthentication Enabled	<input type="checkbox"/>
Reauthentication Period	3600 seconds
EAPOL Timeout	30 seconds
Aging Period	300 seconds
Hold Time	10 seconds
RADIUS-Assigned QoS Enabled	<input type="checkbox"/>
RADIUS-Assigned VLAN Enabled	<input type="checkbox"/>
Guest VLAN Enabled	<input type="checkbox"/>
Guest VLAN ID	1
Max. Reauth. Count	2
Allow Guest VLAN if EAPOL Seen	<input type="checkbox"/>

**Port Configuration**

Port	Admin State	RADIUS-Assigned QoS Enabled	RADIUS-Assigned VLAN Enabled	Guest VLAN Enabled	Port State	Restart
*	<>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		
1	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate Reinitialize
2	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate Reinitialize
3	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate Reinitialize
4	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate Reinitialize
5	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate Reinitialize
6	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate Reinitialize
7	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate Reinitialize
8	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate Reinitialize
9	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate Reinitialize
10	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate Reinitialize
11	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate Reinitialize
12	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate Reinitialize
13	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate Reinitialize

Описание каждого параметра представлено в следующей таблице:

Параметр	Описание
<b>System Configuration</b>	<b>Конфигурация системы</b>
Mode	Дополнительно разрешить/запретить, по умолчанию отключено, глобально настроить, включена ли функция 802.1X.
Re-authentication enabled	Когда установлен флажок, успешно аутентифицированным пользователям потребуется повторная аутентификация после завершения цикла повторной аутентификации..
Recertification cycle	Диапазон составляет от 1 до 3600 секунд, а значение по умолчанию составляет 3600 секунд. Если установлена повторная аутентификация, пользователи, успешно

Параметр	Описание
	прошедшие аутентификацию, должны будут повторно аутентифицироваться после завершения цикла повторной аутентификации.
EAPOL timeout	Диапазон составляет от 1 до 65535 секунд, а значение по умолчанию составляет 30 секунд. Настроить интервал времени для повторной передачи сообщений EAPOL Request Identity.
Aging cycle	Диапазон составляет от 10 до 1000000 секунд, а значение по умолчанию составляет 300 секунд. Эта конфигурация вступает в силу в режимах аутентификации Single 802.1X, Multi 82.1X и MAC-Based Auth. Эти три режима аутентификации связаны с безопасностью порта. MAC-адрес безопасного пользователя устаревает в течение периода устаревания.
Hold time	Диапазон составляет от 10 до 1000000 секунд, а значение по умолчанию составляет 10 секунд. Эта конфигурация вступает в силу в режимах аутентификации Single 802.1X, Multi 802.1X и MAC-Based Auth. При отклонении аутентификации пользователя останется в недопущенном состоянии в течение этого времени конфигурации.
RADIUS authorization QoS enablement	Поставьте флажок, чтобы включить глобальную конфигурацию авторизации QoS. Устройство будет применять приоритет обслуживания QoS, авторизованный RADIUS, к порту, но не изменит исходную конфигурацию QoS порта. После отключения пользователя исходная конфигурация QoS порта вступит в силу.
RADIUS authorization VLAN enabled	Поставьте флажок, чтобы включить глобальную конфигурацию авторизации VLAN. Устройство будет применять VLAN, авторизованный RADIUS, к порту, но не изменит исходную конфигурацию VLAN порта. После отключения пользователя исходная конфигурация VLAN порта вступит в силу. Вы можете проверить, какие модули покрывают текущую конфигурацию VLAN порта на странице VLAN.
Guest VLAN enabled	Включите глобальную конфигурацию гостевой VLAN. Гостевая VLAN действует только в режимах аутентификации на основе портов 802.1X, одиночной аутентификации 802.1X и множественной аутентификации 802.1X, позволяя пользователям получать доступ к ресурсам в определенной VLAN без аутентификации.
Guest VLAN ID	Диапазон составляет от 1 до 4095, значение по умолчанию - 1. Настройте идентификатор VLAN гостевой сети.
Maximum number of re-authentication	Диапазон составляет от 1 до 255, значение по умолчанию - 2. Настройте количество попыток повторной отправки сообщения EAPOL Request Identity.

Параметр	Описание
Allow entry to guest VLAN when receiving EAPOL	Если включено, даже если порт записывает, что он получил сообщения EAPOL, ему будет разрешен вход в гостевую VLAN; если не включено, устройство сначала проверит, получал ли порт сообщения EAPOL, и если нет, оно сразу войдет в гостевую VLAN. В противном случае устройство не войдет в гостевую VLAN, а будет продолжать отправлять сообщения EAPOL Request Identity и ожидать аутентификации.
<b>Port configuration</b>	<b>Конфигурация порта</b>
Authentication mode	<p>Опции режима аутентификации следующие:</p> <ul style="list-style-type: none"> <li>• Force Authorized: Устройство отправляет сообщение EAPoL об успешной аутентификации программе клиента, когда порт подключен. Любой пользователь на порту может получить доступ к сети без аутентификации.</li> <li>• Force Unauthorized: Устройство отправляет сообщение EAPoL о неудачной аутентификации программе клиента, когда порт подключен. Все пользователи на порту не смогут получить доступ к сети.</li> <li>• Port-based 802.1X: Метод управления доступом на основе портов 802.1X. Пока первый пользователь на порту успешно проходит аутентификацию, другие пользователи могут использовать сетевые ресурсы без аутентификации. Однако, когда первый пользователь отключается, другим пользователям также будет отказан доступ к сети.</li> <li>• Single 802.1X: Похоже на режим Port-based 802.1X, но порт позволяет использовать сеть только одному успешно аутентифицированному пользователю. Первый успешно аутентифицированный пользователь, кто бы это ни был, может использовать сеть, и его MAC-адрес будет установлен как безопасный MAC-адрес модулем безопасности порта.</li> <li>• Multi 802.1X: Один порт позволяет нескольким успешно аутентифицированным пользователям использовать сеть, и количество пользователей может быть ограничено через безопасность порта. Когда на порту нет аутентификации пользователей, устройство использует многоадресный адрес для отправки сообщений EAPoL. В противном случае, устройство анализирует MAC-адрес пользователя на основе полученного сообщения EAPoL, а затем использует его для отправки сообщений EAPoL для аутентификации каждого пользователя отдельно.</li> </ul>

Параметр	Описание
	<ul style="list-style-type: none"> <li>MAC-based Auth: Пользователям не требуется программа клиента 802.1X. Устройство завершает функции программы клиента 802.1X и взаимодействует с сервером RADIUS. Устройство перехватывает любой пакет, отправленный пользователем, получает его MAC-адрес, использует его в качестве имени пользователя и пароля (в формате "xx-xx-xx-xx-xx-xx"), и аутентифицируется с сервером RADIUS. Метод аутентификации поддерживает только вызовы MD5. Поэтому, сервер RADIUS должен быть настроен заранее при использовании этого метода. Количество пользователей может быть ограничено через безопасность порта.</li> </ul>
RADIUS authorization QoS enablement	Авторизованный QoS будет включен на соответствующем порту только после того, как будет отмечена опция "RADIUS Authorized QoS Enable" в "System Configuration" и эта конфигурация.
RADIUS authorization VLAN enabled	Авторизация VLAN будет включена на соответствующем порту только после того, как будет отмечена опция "RADIUS Authorization QoS Enable" в "System Configuration" и эта конфигурация.
Guest VLAN enabled	После того как обе опции "Enable Guest VLAN" в "System Configuration" и эта конфигурация будут отмечены, гостевая VLAN будет включена на соответствующем порту.
Port status	<p>Есть 5 типов статуса порта:</p> <ul style="list-style-type: none"> <li>Глобально Отключен: указывает на то, что 802.1X глобально отключен.</li> <li>Соединение Отключено: указывает на то, что 802.1X глобально включен, но соединение порта отключено.</li> <li>Авторизован: указывает на то, что режим аутентификации порта - Force Authorized, или режим аутентификации порта - Single 802.1X и аутентификация пользователя пройдена.</li> <li>Неавторизован: указывает на то, что режим аутентификации порта - Force Unauthorized, или режим аутентификации порта - Single 802.1X и аутентификация пользователя не удалась.</li> <li>X Auth/Y Unauth означает, что режим аутентификации порта - Multi 802.1X, и X пользователей прошли</li> </ul>

Параметр	Описание
	аутентификацию, а Y пользователей не прошли аутентификацию.
Restart	<p>Операция перезапуска аутентификации порта имеет следующие варианты:</p> <ul style="list-style-type: none"> <li>• "Re-authentication" (Повторная аутентификация) - выполнит повторную аутентификацию. Эта конфигурация предназначена только для пользователей, которые успешно прошли аутентификацию, и не прервет текущий процесс аутентификации пользователя.</li> <li>• "Reinitialize" (Повторная инициализация) - означает, что этот порт будет немедленно инициализирован для пользователя на порту, текущий процесс аутентификации пользователя будет завершен, и будет запущен новый процесс аутентификации.</li> </ul>

### 7.8.3 Статус устройства

Вы можете посмотреть статус 802.1X на странице состояния устройства, как показано на рисунке ниже

Network Access Server Switch Status						
Port	Admin State	Port State	Last Source	Last ID	QoS Class	Port VLAN ID
1	Force Authorized	Globally Disabled			-	
2	Force Authorized	Globally Disabled			-	
3	Force Authorized	Globally Disabled			-	
4	Force Authorized	Globally Disabled			-	
5	Force Authorized	Globally Disabled			-	
6	Force Authorized	Globally Disabled			-	
7	Force Authorized	Globally Disabled			-	
8	Force Authorized	Globally Disabled			-	
9	Force Authorized	Globally Disabled			-	
10	Force Authorized	Globally Disabled			-	
11	Force Authorized	Globally Disabled			-	
12	Force Authorized	Globally Disabled			-	
13	Force Authorized	Globally Disabled			-	
14	Force Authorized	Globally Disabled			-	
15	Force Authorized	Globally Disabled			-	
16	Force Authorized	Globally Disabled			-	
17	Force Authorized	Globally Disabled			-	
18	Force Authorized	Globally Disabled			-	
19	Force Authorized	Globally Disabled			-	
20	Force Authorized	Globally Disabled			-	
21	Force Authorized	Globally Disabled			-	
22	Force Authorized	Globally Disabled			-	
23	Force Authorized	Globally Disabled			-	
24	Force Authorized	Globally Disabled			-	
25	Force Authorized	Globally Disabled			-	
26	Force Authorized	Globally Disabled			-	
27	Force Authorized	Globally Disabled			-	
28	Force Authorized	Globally Disabled			-	
29	Force Authorized	Globally Disabled			-	
30	Force Authorized	Globally Disabled			-	
31	Force Authorized	Globally Disabled			-	
32	Force Authorized	Globally Disabled			-	
33	Force Authorized	Globally Disabled			-	
34	Force Authorized	Globally Disabled			-	
35	Force Authorized	Globally Disabled			-	
36	Force Authorized	Globally Disabled			-	

Описание каждого параметра представлено в следующей таблице:

Параметр	Описание
Port	Номер порта устройства. Щелкните по ссылке порта, чтобы просмотреть информацию о состоянии порта
Authentication mode	<p>Отобразить режим аутентификации порта, который может быть отображен следующим образом:</p> <ul style="list-style-type: none"> <li>Force Authorized: Устройство отправит сообщение об успешной аутентификации EAPoL в программу клиента, когда порт подключен. Любой пользователь на порту может получить доступ к сети без аутентификации.</li> <li>Force Unauthorized: Устройство отправит сообщение о неудачной аутентификации EAPoL в программу клиента, когда порт подключен. Все пользователи на порту не смогут получить доступ к сети.</li> <li>Port-based 802.1X: Метод управления доступом на основе</li> </ul>

Параметр	Описание
	<p>портов 802.1X. Пока первый пользователь на порту успешно проходит аутентификацию, другие пользователи могут использовать сетевые ресурсы без аутентификации. Однако, когда первый пользователь отключается, другим пользователям также будет отказан доступ к сети.</p> <ul style="list-style-type: none"> <li>• Single 802.1X: Похож на метод управления доступом на основе портов 802.1X, но порт позволяет использовать сеть только одному успешно аутентифицированному пользователю. Первый, кто успешно пройдет аутентификацию, может использовать сеть, и его MAC-адрес будет установлен как безопасный MAC-адрес модулем безопасности порта.</li> <li>• Multi 802.1X: Один порт позволяет использовать сеть нескольким успешно аутентифицированным пользователям, и количество пользователей может быть ограничено через безопасность порта. Когда на порту нет аутентификации пользователей, устройство использует многоадресный адрес для отправки сообщений EAPoL. В противном случае, устройство анализирует MAC-адрес пользователя на основе полученного сообщения EAPoL, а затем использует его для отправки сообщений EAPoL для аутентификации каждого пользователя отдельно.</li> <li>• MAC-based Auth: Пользователям не требуется программа клиента 802.1X. Устройство выполняет функции программы клиента 802.1X и взаимодействует с сервером RADIUS. Устройство перехватывает любой пакет, отправленный пользователем, получает его MAC-адрес, использует его в качестве имени пользователя и пароля (в формате "xx-xx-xx-xx-xx-xx"), и аутентифицируется с сервером RADIUS. Метод аутентификации поддерживает только вызовы MD5. Поэтому сервер RADIUS должен быть настроен заранее при использовании этого метода. Количество пользователей может быть ограничено через безопасность порта..</li> </ul>
Port status	<p>Отображение статуса порта может быть следующим:</p> <ul style="list-style-type: none"> <li>• Глобально Отключен: указывает на то, что 802.1X глобально отключен.</li> <li>• Соединение Отключено: указывает на то, что 802.1X глобально включен, но соединение порта отключено.</li> <li>• Авторизован: указывает на то, что режим аутентификации порта - Force Authorized, или режим аутентификации порта - Single 802.1X и аутентификация пользователя пройдена.</li> </ul>

Параметр	Описание
	<ul style="list-style-type: none"> <li>Не авторизован: указывает на то, что режим аутентификации порта - Force Unauthorized, или режим аутентификации порта - Single 802.1X и аутентификация пользователя не удалась.</li> <li>X Auth/Y Unauth: означает, что режим аутентификации порта - Multi 802.1X, и X пользователей прошли аутентификацию, а Y пользователей не прошли аутентификацию.</li> </ul>
Recent certification source	Отобразить исходный MAC-адрес последнего полученного пакета EAPOL.
Most recent authentication ID	Отобразить идентификатор пользователя последнего полученного сообщения EAPOL. Для режима аутентификации на основе MAC отображается исходный MAC-адрес нового пользователя.
QoS categories	Отобразить тип QoS для авторизации RADIUS.
Port VLAN ID	Отобразить идентификатор VLAN, авторизованный RADIUS, или идентификатор VLAN гостевой сети.

### 7.8.4 Статус порта

На странице статуса порта вы можете просмотреть информацию, связанную с 802.1X, включая статус порта, статистику пакетов EAPOL, статистику сервера и недавнюю статистику пользователей.

**NAS Statistics Port 1** Port 1 ▼ Auto-refresh  Refresh

**Port State**

Admin State	Force Authorized
Port State	Globally Disabled

Описание параметров статистики сообщений EAPOL

RX/TX	Имя	IEEE имя	Утверждение
Rx	Total	dot1xAuthEapolFramesRx	Количество действительных кадров EAPOL любого типа, полученных коммутатором.
Rx	Response ID	dot1xAuthEapolRespIdFramesRx	Количество действительных кадров EAPOL ответа на запрос идентификации (EAPOL Response Identity), полученных коммутатором.

RX/TX	Имя	IEEE имя	Утверждение
Rx	Responses	dot1xAuthEapolRespFramesRx	Количество действительных кадров EAPOL ответа (кроме кадров ответа на запрос идентификации), полученных коммутатором.
Rx	Start	dot1xAuthEapolStartFramesRx	Количество кадров EAPOL начала аутентификации (EAPOL Start), полученных коммутатором.
Rx	Logoff	dot1xAuthEapolLogoffFramesRx	Количество действительных кадров EAPOL выхода (EAPOL Logoff), полученных коммутатором.
Rx	Invalid Type	dot1xAuthInvalidEapolFramesRx	Количество кадров EAPOL, полученных коммутатором, в которых тип кадра не распознан.
Rx	Invalid Length	dot1xAuthEapLengthErrorFramesRx	Количество кадров EAPOL, полученных коммутатором, в которых поле длины тела пакета (Packet Body Length) является недопустимым.
Tx	Total	dot1xAuthEapolFramesTx	Количество кадров EAPOL любого типа, переданных коммутатором.
Tx	Request ID	dot1xAuthEapolReqIdFramesTx	Количество кадров EAPOL запроса идентификации (EAPOL Request Identity), переданных коммутатором.
Tx	Requests	dot1xAuthEapolReqFramesTx	Количество действительных кадров EAPOL запроса (кроме кадров запроса идентификации), переданных коммутатором.

Backend server statistical parameter description:

RX/TX	Имя	IEEE имя	Утверждение
Rx	Access Challenges	dot1xAuthBackendAccessChallenges	<ul style="list-style-type: none"> <li>Основываясь на 802.1X: количество первых запросов, полученных от сервера;</li> <li>Основываясь на MAC-адресе: количество полученных вызовов доступа.</li> </ul>
Rx	Other Requests	dot1xAuthBackendOtherRequestsToSupplicant	Основываясь на 802.1X: количество запросов EAP, отправленных устройством;
Rx	Auth. Successes	dot1xAuthBackendAuthSuccesses	Количество успешных аутентификаций, полученных устройством;
Rx	Auth. Failures	dot1xAuthBackendAuthFails	Количество неудачных аутентификаций, полученных устройством.
Tx	Responses	dot1xAuthBackendResponses	<ul style="list-style-type: none"> <li>Основываясь на 802.1X: количество пакетов первого ответа пользователя, отправленных на сервер;</li> <li>Основываясь на MAC-адресе: количество всех пакетов, отправленных на сервер.</li> </ul>

Описание параметров статистики последних пользователей:

Имя	IEEE имя	Утверждение
MAC Address	dot1xAuthLastEapolFrameSource	MAC-адрес источника пользователя
VLAN ID	-	ID VLAN последнего пакета, полученного предыдущим клиентом
Version	dot1xAuthLastEapolFrameVersion	Версия протокола полученного сообщения EAPOL
Identity	-	Имя пользователя в сообщении EAPOL Response Identity

## 7.9 AAA Сертификация

### 7.9.1 AAA

#### 7.9.1.2 AAA протокол

AAA - это сокращение от аутентификации (Authentication), авторизации (Authorization) и учета (Accounting). Он предоставляет фреймворк управления для настройки контроля доступа на устройствах NAS (Network Access Server). Контроль доступа используется для управления тем, какие пользователи могут получить доступ к сети и к каким сетевым ресурсам они могут получить доступ.

- Аутентификация: Подтверждение личности пользователя, получающего доступ к сети, и определение, является ли посетитель законным пользователем сети.
- Авторизация: Предоставление различных разрешений различным пользователям и ограничение услуг, которые пользователи могут использовать.
- Учет: Запись всех операций, выполняемых пользователями при использовании сетевых услуг, включая используемые типы услуг, время начала, трафик данных и т. д. Он используется для сбора и записи использования пользователями сетевых ресурсов и может реализовать учет на основе времени и трафика. Требования к выставлению счетов также играют роль мониторинга в сети.

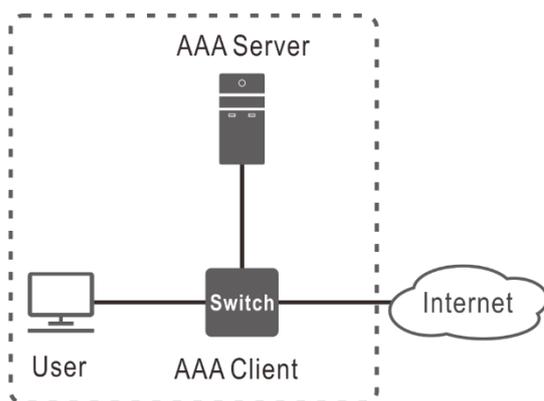
#### 7.9.1.2 AAA принцип работы

##### Базовая топология

AAA использует структуру клиент-сервер. AAA-клиент работает на устройстве доступа, обычно называемом устройством NAS, и отвечает за аутентификацию и управление доступом пользователей;

Сервер AAA - это общее название для сервера аутентификации, сервера авторизации и сервера учета, и отвечает за централизованное управление информацией о пользователях.

Базовая архитектура аутентификации AAA показана на рисунке ниже..



AAA может быть реализован с использованием нескольких протоколов. В настоящее время устройство поддерживает AAA на основе протокола RADIUS или TACACS+.

### Введение в протокол RADIUS

Протокол RADIUS (Remote Authentication Dial-In User Service) является распределенным, структурированным на клиент-серверной основе протоколом обмена информацией, который может защитить сеть от несанкционированного доступа и часто используется в приложениях с повышенными требованиями. В различных сетевых средах с высоким уровнем безопасности и разрешающих удаленный доступ пользователей. Протокол RADIUS объединяет процессы аутентификации и авторизации. Он определяет формат сообщений RADIUS и механизм передачи сообщений, и устанавливает, что для инкапсуляции сообщений RADIUS используется протокол транспортного уровня UDP, а порты UDP 1812 и 1813 используются соответственно, как порты аутентификации/авторизации и учета.

### Введение в протокол TACACS+

TACACS+ (Terminal Access Controller Access Control System) - это протокол безопасности с расширенными функциями на основе протокола TACACS. Этот протокол имеет аналогичные функции с протоколом RADIUS и использует режим клиент-сервер для обмена данными между устройством доступа NAS и сервером TACACS+. Протокол TACACS+ в основном используется для AAA для пользователей доступа PPP и VPDN (Virtual Private Dial-up Network) и конечных пользователей.

### Comparison of RADIUS and TACACS+

RADIUS	TACACS+
Используя UDP, сетевая передача более эффективна, и только поле пароля в сообщении проверки аутентификации зашифровано.	Используя TCP, сетевая передача более надежна. За исключением заголовка сообщения TACACS+, все субъекты сообщений зашифрованы.

RADIUS	TACACS+
<p>Протокольное сообщение относительно просто, и аутентификация и авторизация объединены и сложно разделить.</p>	<p>Протокольные сообщения относительно сложны, и аутентификация и авторизация разделены, так что аутентификационные и авторизационные службы могут быть реализованы отдельно на разных серверах безопасности. Например, вы можете использовать один сервер TACACS+ для аутентификации и другой сервер TACACS+ для авторизации.</p>
<p>Авторизация команд конфигурации устройства не поддерживается. Строки команд, которые пользователь может использовать после входа в устройство, определяются уровнем пользователя. Пользователи могут использовать только строки команд с уровнем по умолчанию, равным или ниже уровня пользователя.</p>	<p>Поддерживается авторизованное использование команд конфигурации устройства. Строки команд, которые пользователи могут использовать, подвергаются двойным ограничениям на уровень пользователя и авторизацию AAA. Каждая команда, введенная пользователем на определенном уровне, должна быть авторизована сервером TACACS+. Если авторизация проходит успешно, команда может быть выполнена.</p>

### Аутентификация и авторизация AAA на локальном уровне

Вход на устройство поддерживает локальную аутентификацию и авторизацию. При локальной аутентификации и авторизации информация о пользователе (включая имя пользователя, пароль и различные атрибуты локального пользователя) настраивается на самом устройстве. Преимущество локальной аутентификации и авторизации заключается в том, что она быстрая и может снизить операционные расходы. Недостатком является то, что объем информации, хранимой на устройстве, ограничен аппаратными условиями устройства.

## 7.9.2 RADIUS

### 7.9.2.1 RADIUS конфигурация

Страница конфигурации сервера RADIUS отображается на рисунке ниже. Во время процесса аутентификации пользователя устройство отправляет сообщение запроса аутентификации на сервер RADIUS. Чтобы избежать ситуации, когда устройство не может получить ответное сообщение от сервера из-за сбоя в сети, задержек и т. д., устройство имеет механизм повторной отправки с таймаутом при отправке сообщения запроса аутентификации на сервер, который контролируется количеством повторных отправок и периодом таймаута.

### RADIUS Server Configuration

#### Global Configuration

Timeout	5	seconds
Retransmit	3	times
Deadtime	0	minutes
Change Secret Key	No <span style="float: right;">▼</span>	
NAS-IP-Address	<input type="text"/>	
NAS-IPv6-Address	<input type="text"/>	
NAS-Identifier	<input type="text"/>	

#### Server Configuration

Delete	Hostname	Auth Port	Acct Port	Timeout	Retransmit	Change Secret Key
<input type="button" value="Add New Server"/>						
<input type="button" value="Save"/> <input type="button" value="Reset"/>						

Описание каждого параметра представлено в следующей таблице:

Параметр	Описание
<b>Global configuration</b>	<b>Глобальная конфигурация</b>
Overtime time	Диапазон составляет от 1 до 1000 секунд, а значение по умолчанию - 5 секунд. Этот таймер запускается, когда устройство отправляет сообщение запроса аутентификации на сервер RADIUS. Если устройство не получает ответное сообщение от сервера RADIUS после истечения времени ожидания, оно повторно отправит сообщение запроса аутентификации.
Number of resends	Диапазон составляет от 1 до 1000 раз, а значение по умолчанию - 3 раза. После достижения максимального числа повторных отправок, если устройство по-прежнему не получает ответное сообщение от сервера RADIUS, сервер считается недоступным.
Dead time	Диапазон составляет от 0 до 1440 минут, а значение по умолчанию - 0. Чтобы предотвратить устройство от постоянных попыток связаться с сервером RADIUS, который был признан недоступным, можно установить время простоя. В течение этого периода устройство не будет пытаться снова связаться с сервером RADIUS, а будет пытаться повторно подключиться к нему после истечения времени ожидания. Эта конфигурация начнет действовать только после добавления как минимум 2 серверов.
Change key	Опционально Да/Нет, выберите, хотите ли вы изменить общий ключ между устройством и сервером RADIUS. После выбора "Да" необходимо указать измененный общий ключ. Общий ключ представляет собой строку из 1-63 символов; если не задан, ключ будет пустым.

Параметр	Описание
NAS-IP-Address	Настройте стандартный атрибут RADIUS 4, который по умолчанию равен IP-адресу исходящего интерфейса устройства. Сервер RADIUS идентифицирует различных клиентов по разным IP-адресам. Обычно клиент использует IP-адрес локального интерфейса для уникальной идентификации себя. Это NAS-IP-адрес.
NAS-IPv6-Address	Настройте стандартный атрибут RADIUS 95, который по умолчанию равен IPv6-адресу исходящего интерфейса устройства.
NAS-Identifier	Имя, используемое устройством для идентификации перед сервером RADIUS, представляет собой строку из 1-253 символов. Если оно пустое, этот атрибут не будет включен в пакет.
<b>Server configuration</b>	<b>Настройки сервера</b>
Delete	Удалить эту конфигурацию сервера.
Host name	IPv4/IPv6-адрес или имя хоста сервера RADIUS.
Authentication port number	Значение по умолчанию - 1812. Номер UDP-порта, используемый для служб аутентификации на сервере RADIUS. Установите значение 0, чтобы отключить аутентификацию.
Accounting port number	Значение по умолчанию - 1813. Номер UDP-порта, используемый для служб учета на сервере RADIUS. Установите значение 0, чтобы отключить учет.
Overtime time	Эта конфигурация переопределяет конфигурацию тайм-аута в глобальной конфигурации. Если не задано, будет использоваться глобально настроенный тайм-аут.
Number of resends	Эта конфигурация переопределяет конфигурацию количества повторных передач в глобальной конфигурации. Если не задано, будет использоваться количество повторных передач из глобальной конфигурации.
Change key	Эта конфигурация переопределяет конфигурацию изменения ключа в глобальной конфигурации. Если не задано, будет использоваться глобально настроенный ключ.



Уведомление:

После настройки ключа он не будет отображаться на веб-странице, но можно просмотреть его в командной строке (ключ будет отображаться в зашифрованном виде).

### 7.9.2.2 RADIUS статус

Страница статуса RADIUS, как показано ниже:

RADIUS Server Status Overview					Auto-refresh <input type="checkbox"/>	Refresh
#	IP Address	Authentication Port	Authentication Status	Accounting Port	Accounting Status	
1			Disabled		Disabled	
2			Disabled		Disabled	
3			Disabled		Disabled	
4			Disabled		Disabled	
5			Disabled		Disabled	

Вы можете просмотреть статус сервера RADIUS на странице мониторинга RADIUS, которая отображает IP-адрес сервера, номер порта аутентификации, статус аутентификации, номер порта учета и статус учета. Статус аутентификации и статус учета имеют четыре состояния:

- Отключено: Этот сервер RADIUS отключен.
- Не готов: Этот сервер RADIUS включен, но еще не была установлена IP-связь.
- Готов: Этот сервер RADIUS включен и может выполнять IP-связь и принимать запросы на доступ.
- Мертвый (осталось N секунд): Устройство пыталось отправить запрос аутентификации на сервер RADIUS, но не получило ответ. В этот момент сервер RADIUS будет временно отключен. По истечении времени ожидания мертвой зоны сервер RADIUS будет вновь включен, и оставшееся время будет отображено.

### 7.9.2.3 RADIUS данные

Эта страница может отображать статистику полученных пакетов и другую информацию о сервере RADIUS. В правом верхнем углу вы можете выбрать, какой сервер отображать.

RADIUS Authentication Statistics for Server #1				Server #1	Auto-refresh <input type="checkbox"/>	Refresh	Clear
Receive Packets		Transmit Packets					
Access Accepts	0	Access Requests	0				
Access Rejects	0	Access Retransmissions	0				
Access Challenges	0	Pending Requests	0				
Malformed Access Responses	0	Timeouts	0				
Bad Authenticators	0						
Unknown Types	0						
Packets Dropped	0						
Other Info							
IP Address							
State				Disabled			
Round-Trip Time				0 ms			
RADIUS Accounting Statistics for Server #1							
Receive Packets		Transmit Packets					
Responses	0	Requests	0				
Malformed Responses	0	Retransmissions	0				
Bad Authenticators	0	Pending Requests	0				
Unknown Types	0	Timeouts	0				
Packets Dropped	0						
Other Info							
IP Address							
State				Disabled			
Round-Trip Time				0 ms			

#### Данные аутентификации RADIUS сервера

Часть данных аутентификации RADIUS взята из RFC4668-RADIUS Authentication Client MIB, включая 7 статистических данных о приеме пакетов и 4 статистических данных о передаче пакетов, как показано в следующей таблице:

Имя	RFC4668 имя	Утверждение
Access consent message	radiusAuthClientExtAccessAccepts	Количество полученных сообщений RADIUS Access-Accept (включая легальные и нелегальные)
Access rejection message	radiusAuthClientExtAccessRejects	Количество полученных сообщений RADIUS Access-Reject (включая легальные и нелегальные)
Access challenge message	radiusAuthClientExtAccessChallenges	Количество полученных сообщений RADIUS Access-Challenge (включая легальные и нелегальные)
Malformed access response message	radiusAuthClientExtMalformedAccessResponses	Количество искаженных сообщений RADIUS Access-Response, таких как нелегальная длина самого сообщения.
Illegal authentication message	radiusAuthClientExtBadAuthenticators	Количество полученных сообщений RADIUS Access-Response, содержащих нелегальную информацию об аутентификаторе.
Unknown type of message	radiusAuthClientExtUnknownTypes	Количество полученных пакетов RADIUS неизвестного типа.
discard message	radiusAuthClientExtPacketsDropped	Количество отброшенных пакетов RADIUS.
Access request message	radiusAuthClientExtAccessRequests	Количество отправленных сообщений RADIUS Access-Request.
Access retransmission message	radiusAuthClientExtAccessRetransmissions	Количество повторно отправленных сообщений RADIUS Access-Request.
Pending request	radiusAuthClientExtPendingRequests	Количество отправленных сообщений RADIUS Access-Request, на которые не получен ответ и которые не истекли по времени.
Number of timeouts	radiusAuthClientExtTimeouts	Количество тайм-аутов аутентификации.

Имя	RFC4668 имя	Утверждение
IP address	-	IP-адрес сервера RADIUS и UDP-порт.
Certification status	-	Подробности о введении TACACS+ см. в следующем разделе.
Round trip time	radiusAuthClientExtRoundTripTime	Интервал времени между последними сообщениями Access-Reply/Access-Challenge и Access-Request в миллисекундах, с шагом 100 миллисекунд.

### Данные учета RADIUS сервера

Данные учета RADIUS сервера представлены в RFC4670 - RADIUS Accounting Client MIB, включая 5 статистических показателей приема пакетов и 4 статистических показателя передачи пакетов, как показано в следующей таблице:

Имя	RFC4670 имя	Утверждение
Response message	radiusAccClientExtResponses	Количество полученных пакетов RADIUS (включая легальные и нелегальные)
Malformed response message	radiusAccClientExtMalformedResponses	Количество некорректных сообщений RADIUS Access-Response, таких как некорректная длина самого сообщения.
Illegal authentication message	radiusAcctClientExtBadAuthenticators	Количество полученных сообщений RADIUS Access-Response, содержащих нелегальную аутентификационную информацию.
Unknown type of message	radiusAccClientExtUnknownTypes	Количество пакетов RADIUS неизвестного типа, полученных.
Discard message	radiusAccClientExtPacketsDropped	Количество отброшенных пакетов RADIUS.
Request message	radiusAccClientExtRequests	Количество пакетов RADIUS, отправленных на сервер, исключая повторные отправки.
Resend message	radiusAccClientExtRetransmissions	Количество повторно отправленных пакетов RADIUS на сервер учета.
Pending request	radiusAccClientExtPendingRequests	Количество сообщений RADIUS Access-Request, отправленных, но не получивших ответа и не достигших тайм-аута.

Имя	RFC4670 имя	Утверждение
Number of timeouts	radiusAccClientExtTimeouts	Количество истекших сроков аутентификации.
IP address	-	IP-адрес сервера RADIUS и UDP-порт.
Billing status	-	См. следующий раздел для подробностей о введении TACACS+.
Round trip time	radiusAccClientExtRoundTripTime	Интервал времени между самым последним Access-Reply/Access-Challenge и Access-Request, в миллисекундах, с шагом в 100 миллисекунд.

## 7.9.3 TACACS+

### 7.9.3.1 TACACS+ конфигурация

TACACS+ страница конфигурации сервера, как показано на рисунке ниже.

**TACACS+ Server Configuration**

**Global Configuration**

<b>Timeout</b>	<input type="text" value="5"/>	seconds
<b>Deadtime</b>	<input type="text" value="0"/>	minutes
<b>Change Secret Key</b>	<input type="text" value="No"/>	

**Server Configuration**

Delete	Hostname	Port	Timeout	Change Secret Key
<input type="button" value="Add New Server"/>				
<input type="button" value="Save"/> <input type="button" value="Reset"/>				

Описание каждого параметра представлено в следующей таблице:

Параметр	Описание
<b>Global configuration</b>	<b>Глобальная конфигурация</b>
Overtime time	Диапазон составляет от 1 до 1000 секунд, а значение по умолчанию - 5 секунд. Этот таймер запускается, когда устройство отправляет сообщение с запросом аутентификации на сервер TACACS+. Если устройство не получает ответное сообщение от сервера TACACS+ после истечения времени ожидания, оно повторно отправляет запрос аутентификации.
Dead time	Диапазон составляет от 0 до 1440 минут, а значение по умолчанию - 0. Чтобы предотвратить постоянные попытки связи устройства с сервером TACACS+, который был признан

Параметр	Описание
	недоступным, можно установить время ожидания. В течение этого периода устройство больше не будет пытаться связаться с сервером TACACS+, который был признан недоступным, и будет пытаться повторно подключиться к нему только после истечения времени ожидания. Эта конфигурация не будет применяться, пока не будет добавлено как минимум 2 сервера.
Change key	Опционально Да/Нет, выберите, хотите ли вы изменить общий ключ между устройством и сервером TACACS+. После выбора "Да" вам нужно будет указать измененный общий ключ. Общий ключ представляет собой строку от 1 до 63 символов.
<b>Server configuration</b>	<b>Конфигурация сервера</b>
Delete	Удалить эту конфигурацию сервера.
Host name	IPv4/IPv6-адрес или имя хоста сервера TACACS+.
The port number	Номер TCP-порта, используемого для аутентификационных служб на сервере TACACS+. Установите значение 0, чтобы отключить аутентификацию.
Overtime time	Установите значение переопределения глобального таймаута. Оставьте его пустым, чтобы использовать глобальное значение таймаута.
Change key	Эта конфигурация переопределит конфигурацию изменения ключа в глобальной конфигурации. Если не установлено, будет использоваться измененный ключ глобальной конфигурации.

## 7.10 ACL конфигурация

ACL (Access Control List) реализует фильтрацию пакетов путем настройки правил сопоставления и операций обработки для пакетов. Среди правил сопоставления включаются исходный адрес, адрес назначения, номер порта и т. д. данных пакета.

ACL состоит из серии записей, называемых элементами управления доступом (Access Control Entry, ACE). Каждая запись списка управления доступом определяет условия сопоставления и поведение, удовлетворяющее этой записи.

### 7.10.1 Управление портом

Контроль порта применяет соответствующую функцию ACL (списка управления доступом) на порт. Как показано ниже.

ACL Ports Configuration									
Port	Policy ID	Action	Rate Limiter ID	Port Redirect	Mirror	Logging	Shutdown	State	Counter
*	0	<>	<>	Disabled Port 1 Port 2	<>	<>	<>	<>	*
1	0	Permit	Disabled	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	740866
2	0	Permit	Disabled	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	0
3	0	Permit	Disabled	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	0
4	0	Permit	Disabled	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	0
5	0	Permit	Disabled	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	0
6	0	Permit	Disabled	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	0
7	0	Permit	Disabled	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	0

Описание каждого параметра представлено в следующей таблице:

Параметр	Описание
Port	Номер порта.
Policy ID	Представляет собой идентификатор шаблона политики, который может содержать соответствия и определенные действия. Подробности о создании шаблонов политики см. в Списке управления доступом. Идентификатор шаблона политики по умолчанию - 0.
Action	Выберите одно из действий: deny (запретить) или allow (разрешить). По умолчанию разрешено.
Rate limiter ID	Идентификатор ограничителя скорости применения интерфейса. Подробности о модификации шаблона ограничителя скорости см. в Ограничении скорости. По умолчанию эта функция отключена.
Port redirection	После получения текущим интерфейсом пакета его можно перенаправить на указанный интерфейс. Примечание: Если включена функция перенаправления порта, действие интерфейса должно быть настроено как deny. По умолчанию эта функция отключена.
Mirror	Указывает, считаются ли пакеты, полученные этим интерфейсом, отраженными пакетами. По умолчанию эта функция отключена.
Log	Указывает, будут ли зарегистрированы пакеты, полученные этим интерфейсом. По умолчанию эта функция отключена.
Closure	Если включено, интерфейс будет выключен после получения кадра с длиной менее 1518 байт. По умолчанию эта функция отключена.
State	Если отключено, интерфейс будет выключен немедленно. По умолчанию эта функция включена.
Counter	Количество отправленных и полученных пакетов интерфейсом.

## 7.10.2 Ограничение скорости

Настройте шаблон ограничителя скорости. Как показано ниже.

**ACL Rate Limiter Configuration**

Rate Limiter ID	Rate	Unit
*	10	<> ▾
1	10	pps ▾
2	10	pps ▾
3	10	pps ▾
4	10	pps ▾
5	10	pps ▾
6	10	pps ▾
7	10	pps ▾
8	10	pps ▾
9	10	pps ▾
10	10	pps ▾
11	10	pps ▾
12	10	pps ▾
13	10	pps ▾
14	10	pps ▾
15	10	pps ▾
16	10	pps ▾

Save Reset

Описание каждого параметра представлено в следующей таблице:

Параметр	Описание
Rate limiter ID	Укажите идентификатор шаблона ограничителя скорости.
Rate	Для пакетов в секунду (pps) шаг составляет 10, а возможный диапазон - от 0 до 5000000; для килобитов в секунду (kbps) шаг составляет 25, а возможный диапазон - от 0 до 10000000.
Unit	Выберите одно из значений: пакетов в секунду (pps) или килобитов в секунду (kbps).



Уведомление:

Изменение значения шаблона ограничителя скорости повлияет на все функции, к которым был применен данный шаблон.

### 7.10.3 Контроль доступа

Настроить список контроля доступа. Как показано ниже:

ACE	Ingress Port	Policy / Bitmask	Frame Type	Action	Rate Limiter	Port Redirect	Mirror	Counter
Auto-refresh <input type="checkbox"/> Refresh Clear Remove All								
+								

Создайте ACE, нажмите на синюю иконку +, и появится следующая страница.

#### ACE Configuration

<b>Ingress Port</b>	All Port 1 Port 2 Port 3 Port 4	<b>Action</b>	Permit
<b>Policy Filter</b>	Any	<b>Rate Limiter</b>	Disabled
<b>Frame Type</b>	Any	<b>Mirror</b>	Disabled
		<b>Logging</b>	Disabled
		<b>Shutdown</b>	Disabled
		<b>Counter</b>	0

#### VLAN Parameters

<b>802.1Q Tagged</b>	Any
<b>VLAN ID Filter</b>	Any
<b>Tag Priority</b>	Any

Save Reset Cancel

Различные типы кадров имеют разные страницы конфигурации, и поддерживаются следующие типы кадров.

- Any

#### ACE Configuration

<b>Ingress Port</b>	All Port 1 Port 2 Port 3 Port 4	<b>Action</b>	Permit
<b>Policy Filter</b>	Any	<b>Rate Limiter</b>	Disabled
<b>Frame Type</b>	Any	<b>Mirror</b>	Disabled
		<b>Logging</b>	Disabled
		<b>Shutdown</b>	Disabled
		<b>Counter</b>	0

#### VLAN Parameters

<b>802.1Q Tagged</b>	Any
<b>VLAN ID Filter</b>	Any
<b>Tag Priority</b>	Any

Save Reset Cancel

- Ethernet Type

**ACE Configuration**

Ingress Port	All Port 1 Port 2 Port 3 Port 4
Policy Filter	Any
Frame Type	Ethernet Type

Action	Permit
Rate Limiter	Disabled
Mirror	Disabled
Logging	Disabled
Shutdown	Disabled
Counter	0

**MAC Parameters**

SMAC Filter	Any
DMAC Filter	Any

**VLAN Parameters**

802.1Q Tagged	Any
VLAN ID Filter	Any
Tag Priority	Any

**Ethernet Type Parameters**

EtherType Filter	Any
------------------	-----

Save Reset Cancel

- ARP

**ACE Configuration**

Ingress Port	All Port 1 Port 2 Port 3 Port 4
Policy Filter	Any
Frame Type	ARP

Action	Permit
Rate Limiter	Disabled
Mirror	Disabled
Logging	Disabled
Shutdown	Disabled
Counter	0

**MAC Parameters**

SMAC Filter	Any
DMAC Filter	Any

**VLAN Parameters**

802.1Q Tagged	Any
VLAN ID Filter	Any
Tag Priority	Any

**ARP Parameters**

ARP/RARP	Any
Request/Reply	Any
Sender IP Filter	Any
Target IP Filter	Any

ARP Sender MAC Match	Any
RARP Target MAC Match	Any
IP/Ethernet Length	Any
IP	Any
Ethernet	Any

Save Reset Cancel

- IPv4

**ACE Configuration**

Ingress Port	All
	Port 1
	Port 2
	Port 3
	Port 4
Policy Filter	Any
Frame Type	IPv4

Action	Permit
Rate Limiter	Disabled
Mirror	Disabled
Logging	Disabled
Shutdown	Disabled
Counter	0

**MAC Parameters**

DMAC Filter	Any
-------------	-----

**VLAN Parameters**

802.1Q Tagged	Any
VLAN ID Filter	Any
Tag Priority	Any

**IP Parameters**

IP Protocol Filter	Any
IP TTL	Any
IP Fragment	Any
IP Option	Any
SIP Filter	Any
DIP Filter	Any

Save Reset Cancel

- IPv6

**ACE Configuration**

Ingress Port	All
	Port 1
	Port 2
	Port 3
	Port 4
Policy Filter	Any
Frame Type	IPv6

Action	Permit
Rate Limiter	Disabled
Mirror	Disabled
Logging	Disabled
Shutdown	Disabled
Counter	0

**MAC Parameters**

DMAC Filter	Any
-------------	-----

**VLAN Parameters**

802.1Q Tagged	Any
VLAN ID Filter	Any
Tag Priority	Any

**IPv6 Parameters**

Next Header Filter	Any
SIP Filter	Any
Hop Limit	Any

Save Reset Cancel

Описание каждого параметра представлено в следующей таблице:

Параметр	Описание
Ingress port	Укажите номер порта для сопоставления. "All" означает сопоставление всех портов.
Policy filter	Если этот элемент равен любому, это означает, что это ACL; наоборот, если этот элемент принимает любое значение от 0

Параметр	Описание
	до 255, это означает, что данная политика конфигурации ACL является шаблоном фильтра, влияющим на все функции, к которым был применен этот идентификатор политики.
Frame type	<p>Тип кадра Ethernet имеет следующие варианты:</p> <ul style="list-style-type: none"> <li>Любой</li> <li>Ethernet Type: По умолчанию сопоставляет ether-типы, отличные от 0x0806/0x0800/0x86DD.</li> <li>ARP: По умолчанию сопоставляет ether-тип 0x0806.</li> <li>IPv4: По умолчанию сопоставляет ether-тип 0x0800.</li> <li>IPv6: По умолчанию сопоставляет ether-тип 0x86DD.</li> </ul>
Action	Отбросить/разрешить/фильтровать. Для фильтрации необходимо указать один или несколько интерфейсов, что означает, что пакеты, соответствующие правилу, могут выходить через отфильтрованный интерфейс.
Rate limiter	Применение шаблона ограничителя скорости на ACL.
Mirror	Соответствует ли пакет, попавший под это ACL, зеркальному пакету.
Log	Требуется ли регистрация пакетов, соответствующих этому ACL.
Closure	<p>Если включено, и длина пакета, соответствующего этому ACL, меньше 1518 байт, интерфейс, соответствующий этому ACL, будет отключен.</p> <p>Примечание: Если в данный момент ACL активировал механизм отключения порта, кроме удаления или изменения правила, также необходимо выполнить включение статуса порта на соответствующем интерфейсе.</p>
Counter	Статистика пакетов, соответствующих этому ACL.
<b>VLAN parameters</b>	<b>Параметры VLAN</b>
802.1Q tag	Настроить совпадение пакетов без тегов/с тегами/любые пакеты.
VLAN ID filtering	Можно настроить совпадение vlan-id или любого.
Tag priority	Можно настроить значение приоритета vlan. В настоящее время поддерживаются следующие значения совпадения: <0-7>/0-1/2-3/4-5/6-7/0-3/4-7/любой.
<b>MAC parameters</b>	<b>Параметры MAC</b>
SMAC filtering	Если тип кадра - Etype, совпадает с MAC-адресом отправителя в заголовке Ethernet; если тип кадра - arp, совпадает с MAC-адресом отправителя в заголовке arp.

Параметр	Описание
DMAC filtering	Если тип кадра - Etype, совпадает с MAC-адресом получателя в заголовке Ethernet; если тип кадра - arp, совпадает с MAC-адресом назначения в заголовке arp.
<b>ARP parameters</b>	<b>Параметры ARP</b>
ARP/RARP	Совпадение пакетов arp/rarp.
Request/Reply	Совпадение типа пакета запроса arp или ответа.
Sender IP filter	Совпадение поля отправителя IP в заголовке arp.
Destination IP filter	Совпадение поля назначения IP в заголовке arp.
Match ARP sender MAC	Чтобы гарантировать, что MAC-адрес отправителя ARP соответствует SMAC заголовка Ethernet.
Match RARP destination MAC	Чтобы гарантировать, что MAC-адрес получателя RARP соответствует DMAC заголовка Ethernet.
IP/Ethernet length	Если значение равно 1, сообщение считается совпавшим, когда размер аппаратного адреса в заголовке arp равен 6, а размер адреса протокола равен 4; если значение равно 0, сообщение считается совпавшим, когда размер аппаратного адреса в заголовке arp не равен 6 или размер адреса протокола не равен 4.
IP	Если значение равно 1, сообщение считается совпавшим, когда тип протокола в заголовке arp равен 0x0800; если значение равно 0, сообщение считается совпавшим, когда тип протокола в заголовке arp не равен 0x0800.
Ethernet	Если значение равно 1, сообщение считается совпавшим, когда тип аппаратного адреса в заголовке arp равен 1; если значение равно 0, сообщение считается совпавшим, когда тип аппаратного адреса в заголовке arp не равен 1.
<b>IP parameters</b>	<b>Параметры IP</b>
IP protocol filtering	Выполнение специального сопоставления с сообщениями ICMP/TCP/UDP.
IP TTL	Сопоставление характеристик пакетов с TTL равным 0/не равным 0.
IP fragmentation	Сопоставление характеристик пакетов с фрагментацией IP.
IP options	Если значение равно 1, сообщение считается совпавшим, когда параметр Option вставлен в поле Header Option заголовка IPv4; если значение равно 0, сообщение считается совпавшим, когда параметр Option не вставлен в поле Header Option заголовка IPv4.
Source IP filtering	Указание SIP для сопоставления IPv4-пакетов. Фиксированный маскирующий хост - 255.255.255.255, или маска подсети настраивается (для обеспечения непрерывности маски).
Destination IP filtering	Указание DIP для сопоставления IPv4-пакетов. Фиксированный маскирующий хост - 255.255.255.255, или маска подсети настраивается (для обеспечения непрерывности маски).
<b>ICMP parameters</b>	<b>Параметры ICMP</b>

Параметр	Описание
ICMP type filtering	Сопоставление типа ICMP. Диапазон настраивается <0-255>.
ICMP Code filtering	Сопоставление кода ICMP. Диапазон настраивается <0-255>.
<b>TCP/UDP parameters</b>	<b>Параметры TCP/UDP</b>
Source port filtering	Сопоставление исходного порта TCP/UDP IPv4.
Destination port filtering	Сопоставление порта назначения TCP/UDP IPv4.
TCP FIN	Если значение равно 1, и флаг Fin в поле Flags заголовка TCP равен 1, сообщение считается совпавшим; если значение равно 0, и флаг Fin в поле Flags заголовка TCP равен 0, сообщение считается совпавшим.
TCP SYN	Если значение равно 1, и флаг Syn в поле Flags заголовка TCP равен 1, сообщение считается совпавшим; если значение равно 0, и флаг Syn в поле Flags заголовка TCP равен 0, сообщение считается совпавшим.
TCP RST	Если значение равно 1, и флаг Reset в поле Flags заголовка TCP равен 1, сообщение считается совпавшим; если значение равно 0, и флаг Reset в поле Flags заголовка TCP равен 0, сообщение считается совпавшим.
TCP PSH	Если значение равно 1, и флаг Push в поле Flags заголовка TCP равен 1, сообщение считается совпавшим; если значение равно 0, и флаг Push в поле Flags заголовка TCP равен 0, сообщение считается совпавшим.
TCP ACK	Если значение равно 1, и флаг Acknowledgment в поле Flags заголовка TCP равен 1, сообщение считается совпавшим; если значение равно 0, и флаг Acknowledgment в поле Flags заголовка TCP равен 0, сообщение считается совпавшим.
TCP URG	Если значение равно 1, и флаг Urgent в поле Flags заголовка TCP равен 1, сообщение считается совпавшим; если значение равно 0, и флаг Urgent в поле Flags заголовка TCP равен 0, сообщение считается совпавшим.
<b>IPv6 parameters</b>	<b>IPv6 параметр</b>
Hop limit	Если значение равно 1, и Hop Limit в заголовке IPv6 не равен 0, то пакет считается совпавшим; если значение равно 0, и Hop Limit в заголовке IPv6 равен 0, то пакет считается совпавшим.
Next header filter	Соответствие конкретным значениям Next Header. Диапазон значений: <0-5>, <7-16>, <18-57>, <59-255>.
Source IP filtering	Указание SIP для сопоставления IPv6. Маска представляет собой последние 32 бита SIP.

## 7.10.4 ACL статус

Проверить статус настроенного ACL

ACL Status		combined		Auto-refresh <input type="checkbox"/>		Refresh		
User	ACE	Frame Type	Action	Rate Limiter	Mirror	CPU	Counter	Conflict
IP	1	IPv4 DIP:224.0.0.1/32	Permit	Disabled	Disabled	Yes	0	No

Описание каждого параметра представлено в следующей таблице:

Параметр	Описание
user	Указать модуль, к которому применяется текущий ACE.
ACE ID	Запись списка контроля доступа.
Frame type	Информация о типе совпадающего кадра.
action	Выполняемая функция.
rate limiter	Идентификатор применяемого лимитера скорости.
mirror	Включена ли функция отражения.
CPU	Отправляется ли пакет на CPU.
counter	Текущая статистика полученных пакетов ACE.
conflict	<p>Отображает аппаратный статус конкретного ACE. Из-за аппаратных ограничений определенные ACE не должны использоваться на аппаратном уровне.</p> <p>Пример:                      Настроена запись ACL, но из-за недостаточных ресурсов ACL приостановлен и не передается на чип. После освобождения других ресурсов, использующих модуль ACL, модуль ACL повторно проверяет ресурсы, и конфликтующие ACL могут быть повторно переданы на чип.</p>

## 7.11 Защита источника IPv4

Защита источника IPv4 (Source IPv4 protection) - это технология фильтрации трафика порта на основе IP/MAC, которая может предотвращать атаки подделки IP-адресов в локальной сети. IPSG (IP Source Guard) может гарантировать, что IP-адреса конечных устройств в сети второго уровня не будут перехвачены, и также может обеспечить, что несанкционированные устройства не смогут получить доступ к сети, указывая свои собственные IP-адреса, или атаковать сеть, вызывая ее сбой или паралич.

### 7.11.1 Конфигурация порта

Страница конфигурации порта показана на рисунке ниже.

**IP Source Guard Configuration**

Mode

Translate dynamic to static

**Port Mode Configuration**

Port	Mode	Max Dynamic Clients
*	<>	<>
1	Disabled	Unlimited
2	Disabled	Unlimited
3	Disabled	Unlimited
4	Disabled	Unlimited
5	Disabled	Unlimited
6	Disabled	Unlimited
7	Disabled	Unlimited
8	Disabled	Unlimited
9	Disabled	Unlimited
10	Disabled	Unlimited
11	Disabled	Unlimited
12	Disabled	Unlimited
13	Disabled	Unlimited
14	Disabled	Unlimited

Описание каждого параметра представлено в следующей таблице:

Параметр	Описание
Mode	Настройте глобальный порт для включения/отключения функции защиты источника IP.
Convert dynamic to static	Преобразуйте всю динамическую информацию DHCP, полученную на устройстве, в статические конфигурации.
<b>Port mode configuration</b>	<b>Конфигурация режима порта</b>
Port	Номер порта устройства.
Mode	Настройте порт для включения/отключения функции защиты источника IP.
Max Dynamic Client	<p>Настройте максимальное количество динамических клиентов на указанном порту. Варианты следующие:</p> <ul style="list-style-type: none"> <li>• 0</li> <li>• 1</li> <li>• 2</li> <li>• No limit</li> </ul>

### 7.11.2 Статические таблицы

Интерфейс для настройки статической таблицы привязки источников IPSG показан на рисунке ниже.

**Static IP Source Guard Table**

Delete	Port	VLAN ID	IP Address	MAC address
Add New Entry				
Save    Reset				

Описание каждого параметра представлено в следующей таблице:

Параметр	Описание
Delete	Включить удаление статической таблицы защиты IP.
Port	Указать порт этой статической таблицы защиты IP.
VLAN ID	Указать VLAN этой статической таблицы защиты IP.
IPv4 address	Указать IPv4-адрес этой статической таблицы защиты IP.
MAC address	Указать физический адрес этой статической таблицы защиты IP.

### 7.11.3 Статус

Проверьте динамически изученную таблицу защиты IP-источника, как показано на рисунке ниже.

**Dynamic IP Source Guard Table** Auto-refresh  Refresh |<< >>

Start from Port 1 , VLAN 1 and IP address 0.0.0.0 with 20 entries per page.

Port	VLAN ID	IP Address	MAC Address
No more entries			

## 7.12 Защита источника IPv6

IPv6 Source Guard (IPSG) - это технология фильтрации трафика на порту, основанная на IPv6/MAC, которая предотвращает атаки подделки IPv6-адресов в локальной сети. IPSG гарантирует, что IPv6-адреса конечных устройств в сети второго уровня не будут подменены, а также предотвращает несанкционированным устройствам доступ к сети или атаки на сеть с использованием собственных IPv6-адресов, что может привести к сбою или параличу сети.

## 7.12.1 Конфигурация порта

Страница конфигурации порта показана на рисунке ниже.

### IPv6 Source Guard Configuration

Mode Disabled ▾

Translate dynamic to static

Port	Mode	Max Dynamic Clients
*	<> ▾	<> ▾
Gi 1/1	Disabled ▾	Unlimited ▾
Gi 1/2	Disabled ▾	Unlimited ▾
Gi 1/3	Disabled ▾	Unlimited ▾
Gi 1/4	Disabled ▾	Unlimited ▾
Gi 1/5	Disabled ▾	Unlimited ▾
Gi 1/6	Disabled ▾	Unlimited ▾
Gi 1/7	Disabled ▾	Unlimited ▾
Gi 1/8	Disabled ▾	Unlimited ▾
Gi 1/9	Disabled ▾	Unlimited ▾
Gi 1/10	Disabled ▾	Unlimited ▾
Gi 1/11	Disabled ▾	Unlimited ▾
Gi 1/12	Disabled ▾	Unlimited ▾
Gi 1/13	Disabled ▾	Unlimited ▾
Gi 1/14	Disabled ▾	Unlimited ▾
Gi 1/15	Disabled ▾	Unlimited ▾
Gi 1/16	Disabled ▾	Unlimited ▾
Gi 1/17	Disabled ▾	Unlimited ▾
Gi 1/18	Disabled ▾	Unlimited ▾

Описание каждого параметра представлено в следующей таблице:

Параметр	Описание
Mode	Настройте глобальный порт для включения/отключения функции защиты источника IPv6.
Convert dynamic to static	Преобразуйте все динамические данные IPv6 DHCP, которые были получены на устройстве, в статическую конфигурацию.
<b>Port mode configuration</b>	Настройка режима порта
Port	Номер устройства порта.
Mode	Настройте порт для включения/отключения функции защиты источника IPv6.
Max Dynamic Client	Настройте максимальное количество динамических клиентов на указанном порту. Варианты следующие: <ul style="list-style-type: none"> <li>• 0</li> <li>• 1</li> </ul>

Параметр	Описание
	<ul style="list-style-type: none"> <li>• 2</li> <li>• No limit</li> </ul>

### 7.12.2 Статические таблицы

Интерфейс для настройки статической таблицы привязки источника IPSG показан на рисунке ниже.

**IPv6 Source Guard Static Table** Auto-refresh

Port  VLAN ID  IP Address  MAC Address

Port	VLAN ID	IPv6 Address	MAC Address

Описание каждого параметра представлено в следующей таблице:

Параметр	Описание
Delete	Включите удаление статической таблицы защиты IPv6.
Port	Укажите порт этой статической таблицы защиты IPv6.
VLAN ID	Укажите VLAN этой статической таблицы защиты IPv6.
IPv6 address	Укажите IPv6-адрес этой статической таблицы защиты IPv6.
MAC address	Укажите физический адрес этой статической таблицы защиты IPv6.

### 7.12.3 Информация

Просмотрите динамически изученную таблицу защиты источника IPv6, как показано на следующем рисунке.

**IPv6 Source Guard Dynamic Table** Auto-refresh

Port	VLAN ID	IPv6 Address	MAC Address

## 7.13 ARP защита

Протокол ARP (Протокол разрешения адресов) обладает преимуществами простоты и удобства использования, однако из-за отсутствия любого механизма безопасности его легко эксплуатировать злоумышленниками. В сети распространены следующие основные методы атак ARP:

- ◆ Атака затопления ARP, также называемая атакой отказа в обслуживании DoS (Denial of Service);
- ◆ Атака подмены ARP заключается в том, что злоумышленник злонамеренно изменяет записи ARP устройства или других хостов пользователей в сети, отправляя поддельные ARP-пакеты, что приводит к нарушению нормальной передачи пакетов для пользователей или сети.

ARP-защита предназначена главным образом для предотвращения этих атак и избегания различных вредоносных последствий, вызванных атаками ARP.

### ARP Инспекция

Это устройство поддерживает функцию инспекции ARP, которая нормально передает ARP-пакеты от законных пользователей, в противном случае непосредственно отбрасывает их, тем самым предотвращая атаки от фальшивых пользователей и фальшивых шлюзов. После включения этой функции устройство сравнивает информацию об источнике IP, источнике MAC, интерфейсе и VLAN в ARP-пакете с информацией в таблице привязки. Если информация совпадает, это означает, что пользователь, отправивший ARP-пакет, является законным пользователем. Пакет ARP этого пользователя пропускается, в противном случае он считается атакой, пакет ARP отбрасывается, и может быть сгенерирована информация в журнале.

Для доверенных интерфейсов ARP проверка законности пользователя не выполняется; для недоверенных интерфейсов ARP проверка законности пользователя требуется для предотвращения атак путем подделки пользователей. Проверка законности пользователя основана на исходном IP-адресе и исходном MAC-адресе в ARP-сообщении, чтобы проверить, является ли пользователь законным пользователем на интерфейсе, к которому принадлежит VLAN, включая проверку на основе статических записей привязки ARP и динамических записей безопасности ARP на основе проверки DHCP Snooping. При совпадении любой из них ARP-сообщение считается законным и передается. Если ни в одной из проверок не найдена соответствующая запись, пакет считается незаконным и отбрасывается, а также может быть сгенерирована информация в журнале.

### 7.13.1 Конфигурация порта

Веб-страница конфигурации порта показана на рисунке ниже.

#### ARP Inspection Configuration

Mode

#### Port Mode Configuration

Port	Mode	Check VLAN	Log Type
*	<>	<>	<>
1	Disabled	Disabled	None
2	Disabled	Disabled	None
3	Disabled	Disabled	None
4	Disabled	Disabled	None
5	Disabled	Disabled	None
6	Disabled	Disabled	None
7	Disabled	Disabled	None
8	Disabled	Disabled	None
9	Disabled	Disabled	None
10	Disabled	Disabled	None
11	Disabled	Disabled	None
12	Disabled	Disabled	None
13	Disabled	Disabled	None
14	Disabled	Disabled	None

Описание каждого параметра представлено в следующей таблице:

Параметр	Описание
Mode	ARP detection global configuration позволяет включить функцию обнаружения ARP.
<b>Port mode configuration</b>	<b>Конфигурация режима порта</b>
Port	Номер устройства порта
Mode	Дополнительные параметры включения/отключения: <ul style="list-style-type: none"> <li>Включить: указывает, что функция обнаружения ARP на порту включена. В этом случае порт является недоверенным портом ARP.</li> <li>Отключить: указывает, что функция обнаружения ARP на порту отключена. В этом случае порт является доверенным портом ARP..</li> </ul>

Параметр	Описание
Check VLAN	<p>Дополнительные параметры включения/отключения:</p> <ul style="list-style-type: none"> <li>Включить: указывает на то, что будет проверяться действительность ARP-пакетов в указанной VLAN (настроенной на странице конфигурации VLAN, описанной в следующем разделе).</li> <li>Отключить: указывает на проверку действительности всех ARP-пакетов, полученных на этом порту.</li> </ul>
Log type	<p>Дополнительные параметры: Нет/Запретить/Разрешить/Все:</p> <ul style="list-style-type: none"> <li>Нет: означает, что записи журнала обнаружения ARP не ведутся.</li> <li>Запретить: означает, что в журнале записываются только отклоненные записи ARP.</li> <li>Разрешить: означает, что в журнале записываются только разрешенные записи ARP.</li> <li>Все: означает, что в журнале записываются все записи ARP.</li> </ul>

## 7.13.2 VLAN конфигурация

Выбор VLAN, на которых действует функция обнаружения ARP и тип журнала для каждого VLAN представлен на веб-странице конфигурации VLAN, как показано на рисунке ниже..

**VLAN Mode Configuration** Refresh | << >>

Start from VLAN  with  entries per page.

Delete	VLAN ID	Log Type
<input type="button" value="Add New Entry"/>		
<input type="button" value="Save"/> <input type="button" value="Reset"/>		

### 7.13.3 Статические таблицы

Настройка статического обнаружения ARP показана на рисунке ниже. После включения функции обнаружения ARP, соответствующие пакеты ARP, настроенные в таблице статического обнаружения ARP, могут быть перенаправлены нормально.

**Static ARP Inspection Table**

Delete	Port	VLAN ID	MAC Address	IP Address
Add New Entry				
Save		Reset		

Описание каждого параметра представлено в следующей таблице:

Параметр	Описание
Delete	После проверки нажмите кнопку "Сохранить", чтобы удалить существующие элементы конфигурации ARP.
Port	Настройте порт, на котором действует статический ARP.
VLAN ID	Настройте VLAN, к которой относятся разрешенные для прохода пакеты ARP.
MAC address	Настройте исходный MAC-адрес пакетов ARP, которым разрешен проход.
IP address	Настройте исходный IP-адрес пакетов ARP, которым разрешен проход.

### 7.13.4 Динамическая таблица

Конфигурация динамического обнаружения ARP показана на рисунке ниже..

**Dynamic ARP Inspection Table** Auto-refresh  Refresh << >>

Start from Port 1 , VLAN 1 , MAC address 00-00-00-00-00-00 and IP address 0.0.0.0 with 20 entries per page.

Port	VLAN ID	MAC Address	IP Address	Translate to static
No more entries				

Save    Reset

Динамическое обнаружение ARP зависит от функции DHCP Snooping. После включения функции DHCP Snooping на устройстве, когда DHCP-пользователь выходит в сеть, устройство автоматически создает таблицу привязки DHCP Snooping. Динамическое обнаружение ARP использует эту таблицу для проверки, является ли пакет ARP допустимым. Установите флажок "Преобразовать в статический" и нажмите кнопку "Сохранить", чтобы преобразовать динамический ARP в статический ARP. Соответствующие

записи динамического ARP исчезнут, а преобразованные записи ARP будут отображены в таблице статического обнаружения ARP.

### 7.13.5 Информация о фильтрации ARP

Эта страница будет отображать все динамические записи ARP.

**Dynamic ARP Inspection Table** Auto-refresh  Refresh |<< >>

Start from Port 1 , VLAN 1 , MAC address 00-00-00-00-00-00 and IP address 0.0.0.0 with 20 entries per page.

Port	VLAN ID	MAC Address	IP Address
No more entries			

## 8 Продвинутые функции

### 8.1 QoS

QoS (Quality of Service) используется для оценки способности поставщика услуг удовлетворить потребности клиентов. В Интернете для улучшения качества сетевого обслуживания введен механизм QoS, и QoS используется для оценки способности сети доставлять пакеты. То, что мы обычно называем QoS, - это оценка возможности сервиса поддерживать основные требования, такие как задержка, джиттер и потеря пакетов в процессе доставки пакетов.

#### 8.1.1 Классификация портов

Настройка страницы с информацией о классификации портов.

### QoS Port Classification

Port	Ingress								Egress
	CoS	DPL	PCP	DEI	CoS ID	Tag Class.	DSCP Based	Map	Map
*	<>	<>	<>	<>	<>		<input type="checkbox"/>		
1	0	0	0	0	0	Disabled	<input type="checkbox"/>		
2	0	0	0	0	0	Disabled	<input type="checkbox"/>		
3	0	0	0	0	0	Disabled	<input type="checkbox"/>		
4	0	0	0	0	0	Disabled	<input type="checkbox"/>		
5	0	0	0	0	0	Disabled	<input type="checkbox"/>		
6	0	0	0	0	0	Disabled	<input type="checkbox"/>		
7	0	0	0	0	0	Disabled	<input type="checkbox"/>		
8	0	0	0	0	0	Disabled	<input type="checkbox"/>		
9	0	0	0	0	0	Disabled	<input type="checkbox"/>		
10	0	0	0	0	0	Disabled	<input type="checkbox"/>		
11	0	0	0	0	0	Disabled	<input type="checkbox"/>		
12	0	0	0	0	0	Disabled	<input type="checkbox"/>		
13	0	0	0	0	0	Disabled	<input type="checkbox"/>		
14	0	0	0	0	0	Disabled	<input type="checkbox"/>		
15	0	0	0	0	0	Disabled	<input type="checkbox"/>		
16	0	0	0	0	0	Disabled	<input type="checkbox"/>		
17	0	0	0	0	0	Disabled	<input type="checkbox"/>		
18	0	0	0	0	0	Disabled	<input type="checkbox"/>		
19	0	0	0	0	0	Disabled	<input type="checkbox"/>		
20	0	0	0	0	0	Disabled	<input type="checkbox"/>		
21	0	0	0	0	0	Disabled	<input type="checkbox"/>		
22	0	0	0	0	0	Disabled	<input type="checkbox"/>		
23	0	0	0	0	0	Disabled	<input type="checkbox"/>		
24	0	0	0	0	0	Disabled	<input type="checkbox"/>		
25	0	0	0	0	0	Disabled	<input type="checkbox"/>		
26	0	0	0	0	0	Disabled	<input type="checkbox"/>		
27	0	0	0	0	0	Disabled	<input type="checkbox"/>		
28	0	0	0	0	0	Disabled	<input type="checkbox"/>		
29	0	0	0	0	0	Disabled	<input type="checkbox"/>		
30	0	0	0	0	0	Disabled	<input type="checkbox"/>		
31	0	0	0	0	0	Disabled	<input type="checkbox"/>		
32	0	0	0	0	0	Disabled	<input type="checkbox"/>		
33	0	0	0	0	0	Disabled	<input type="checkbox"/>		
34	0	0	0	0	0	Disabled	<input type="checkbox"/>		
35	0	0	0	0	0	Disabled	<input type="checkbox"/>		
36	0	0	0	0	0	Disabled	<input type="checkbox"/>		

Save Reset

Описание каждого параметра представлено в следующей таблице

Параметр	Описание
Port	Номер порта устройства
Entrance direction	Метка данных направления входа: <ul style="list-style-type: none"> <li>CoS: Отображение значения CoS. Значение CoS имеет взаимно-однозначное соответствие с QueueId.</li> </ul>

Параметр	Описание
	<ul style="list-style-type: none"> <li>• DPL: Отображение значения DPL. Это значение DPL используется для Remark/Classification/Remap.</li> <li>• PCP: Это значение 802.1P.</li> <li>• DEI: Это значение CFI.</li> <li>• CoS ID: Отображается в CoS_ID. Это значение используется для сопоставления egress_map.</li> <li>• Классификация тега: Включена ли функция доверия к тегу на интерфейсе.</li> <li>• Основано на DSCP: Включена ли функция доверия к DSCP на интерфейсе. Соответствующая запись в таблице - dscp-cos.</li> <li>• Отображение: Этот интерфейс использует запись ingress_map.</li> </ul>
Exit direction	MAP: На этом интерфейсе применяются записи egress_map.



Уведомление:

Если функции доверия к DSCP и доверия к тегу включены одновременно, и настроена запись dscp-cos, то доверие к DSCP имеет более высокий приоритет, чем доверие к тегу; в противном случае, доверие к тегу имеет более высокий приоритет, чем доверие к DSCP.

Приоритет ingress\_map выше, чем функции доверия к тегу и доверия к DSCP.

## 8.1.2 Политика порта

Настройка входной политики порта для QoS.

**QoS Ingress Port Policers**

Port	Enable	Rate	Unit
*	<input type="checkbox"/>	500	<> ▾
1	<input type="checkbox"/>	500	kbps ▾
2	<input type="checkbox"/>	500	kbps ▾
3	<input type="checkbox"/>	500	kbps ▾
4	<input type="checkbox"/>	500	kbps ▾
5	<input type="checkbox"/>	500	kbps ▾
6	<input type="checkbox"/>	500	kbps ▾
7	<input type="checkbox"/>	500	kbps ▾
8	<input type="checkbox"/>	500	kbps ▾
9	<input type="checkbox"/>	500	kbps ▾
10	<input type="checkbox"/>	500	kbps ▾
11	<input type="checkbox"/>	500	kbps ▾
12	<input type="checkbox"/>	500	kbps ▾
13	<input type="checkbox"/>	500	kbps ▾
14	<input type="checkbox"/>	500	kbps ▾
15	<input type="checkbox"/>	500	kbps ▾
16	<input type="checkbox"/>	500	kbps ▾
17	<input type="checkbox"/>	500	kbps ▾
18	<input type="checkbox"/>	500	kbps ▾
19	<input type="checkbox"/>	500	kbps ▾
20	<input type="checkbox"/>	500	kbps ▾
21	<input type="checkbox"/>	500	kbps ▾
22	<input type="checkbox"/>	500	kbps ▾
23	<input type="checkbox"/>	500	kbps ▾
24	<input type="checkbox"/>	500	kbps ▾
25	<input type="checkbox"/>	500	kbps ▾
26	<input type="checkbox"/>	500	kbps ▾
27	<input type="checkbox"/>	500	kbps ▾
28	<input type="checkbox"/>	500	kbps ▾
29	<input type="checkbox"/>	500	kbps ▾
30	<input type="checkbox"/>	500	kbps ▾
31	<input type="checkbox"/>	500	kbps ▾
32	<input type="checkbox"/>	500	kbps ▾
33	<input type="checkbox"/>	500	kbps ▾
34	<input type="checkbox"/>	500	kbps ▾
35	<input type="checkbox"/>	500	kbps ▾
36	<input type="checkbox"/>	500	kbps ▾

Save Reset

Описание каждого параметра представлено в следующей таблице

Параметр	Описание
Enable	Включить входное ограничение скорости на указанном интерфейсе.
Rate	Настроить значение ограничения скорости входящего трафика на указанном интерфейсе. Диапазон ограничения скорости составляет <1-13128147>.
Unit	Настроить единицу измерения ограничения скорости. Допустимые единицы измерения: kbps/Mbps/fps/kfps. По умолчанию используется kbps.

### 8.1.3 Стратегия очереди

Настройте портовую команду для включения в интерфейс политики направления.

### QoS Ingress Queue Policers

Port	Queue 0	Queue 1	Queue 2	Queue 3	Queue 4	Queue 5	Queue 6	Queue 7
	Enable							
*	<input type="checkbox"/>							
1	<input type="checkbox"/>							
2	<input type="checkbox"/>							
3	<input type="checkbox"/>							
4	<input type="checkbox"/>							
5	<input type="checkbox"/>							
6	<input type="checkbox"/>							
7	<input type="checkbox"/>							
8	<input type="checkbox"/>							
9	<input type="checkbox"/>							
10	<input type="checkbox"/>							
11	<input type="checkbox"/>							
12	<input type="checkbox"/>							
13	<input type="checkbox"/>							
14	<input type="checkbox"/>							
15	<input type="checkbox"/>							
16	<input type="checkbox"/>							
17	<input type="checkbox"/>							
18	<input type="checkbox"/>							
19	<input type="checkbox"/>							
20	<input type="checkbox"/>							
21	<input type="checkbox"/>							
22	<input type="checkbox"/>							
23	<input type="checkbox"/>							
24	<input type="checkbox"/>							
25	<input type="checkbox"/>							
26	<input type="checkbox"/>							
27	<input type="checkbox"/>							
28	<input type="checkbox"/>							
29	<input type="checkbox"/>							
30	<input type="checkbox"/>							
31	<input type="checkbox"/>							
32	<input type="checkbox"/>							
33	<input type="checkbox"/>							
34	<input type="checkbox"/>							
35	<input type="checkbox"/>							
36	<input type="checkbox"/>							

Описание каждого параметра представлено в следующей таблице

Параметр	Описание
Port	Номер порта устройства
Queue 0-7	<ul style="list-style-type: none"> <li>Включить: включить функцию ограничения входящей скорости на указанном интерфейсе.</li> <li>Скорость: настроить значение ограничения входящей скорости на указанном интерфейсе. Диапазон ограничения скорости составляет &lt;1-13128147&gt;.</li> </ul>

Параметр	Описание
	<ul style="list-style-type: none"> <li>Единица: настроить единицу измерения ограничения скорости, допустимые единицы измерения: kbps/Mbps. По умолчанию используется kbps.</li> </ul>

### 8.1.4 Расписание портов

Настройка расписания очереди и формирования интерфейса порта.

**QoS Egress Port Schedulers**

Port	Mode	Weight							
		Q0	Q1	Q2	Q3	Q4	Q5	Q6	Q7
1	Strict Priority	-	-	-	-	-	-	-	-
2	Strict Priority	-	-	-	-	-	-	-	-
3	Strict Priority	-	-	-	-	-	-	-	-
4	Strict Priority	-	-	-	-	-	-	-	-
5	Strict Priority	-	-	-	-	-	-	-	-
6	Strict Priority	-	-	-	-	-	-	-	-
7	Strict Priority	-	-	-	-	-	-	-	-
8	Strict Priority	-	-	-	-	-	-	-	-
9	Strict Priority	-	-	-	-	-	-	-	-
10	Strict Priority	-	-	-	-	-	-	-	-
11	Strict Priority	-	-	-	-	-	-	-	-
12	Strict Priority	-	-	-	-	-	-	-	-
13	Strict Priority	-	-	-	-	-	-	-	-
14	Strict Priority	-	-	-	-	-	-	-	-
15	Strict Priority	-	-	-	-	-	-	-	-
16	Strict Priority	-	-	-	-	-	-	-	-
17	Strict Priority	-	-	-	-	-	-	-	-
18	Strict Priority	-	-	-	-	-	-	-	-
19	Strict Priority	-	-	-	-	-	-	-	-
20	Strict Priority	-	-	-	-	-	-	-	-
21	Strict Priority	-	-	-	-	-	-	-	-
22	Strict Priority	-	-	-	-	-	-	-	-
23	Strict Priority	-	-	-	-	-	-	-	-
24	Strict Priority	-	-	-	-	-	-	-	-
25	Strict Priority	-	-	-	-	-	-	-	-
26	Strict Priority	-	-	-	-	-	-	-	-
27	Strict Priority	-	-	-	-	-	-	-	-
28	Strict Priority	-	-	-	-	-	-	-	-
29	Strict Priority	-	-	-	-	-	-	-	-
30	Strict Priority	-	-	-	-	-	-	-	-
31	Strict Priority	-	-	-	-	-	-	-	-
32	Strict Priority	-	-	-	-	-	-	-	-
33	Strict Priority	-	-	-	-	-	-	-	-
34	Strict Priority	-	-	-	-	-	-	-	-
35	Strict Priority	-	-	-	-	-	-	-	-
36	Strict Priority	-	-	-	-	-	-	-	-

Описание каждого параметра представлено в следующей таблице

Параметр	Описание
Port	Номер порта коммутатора. Щелкните по номеру порта, чтобы настроить планировщик.
Mode	Отображает режим планирования этого порта.
Weight	Отображает вес этой очереди и порта.

Щелкните на ссылке порта, чтобы войти в конфигурацию расписания и формирования исходящего трафика QoS на указанном порту.

QoS Egress Port Scheduler and Shapers Port 1 Port 1 ▾

Scheduler Mode: Strict Priority ▾

Queue Shaper					Queue Scheduler	Port Shaper			
Enable	Rate	Unit	Rate-type	Credit	Cut-through	Enable	Rate	Unit	Rate-type
<input type="checkbox"/>	500	kbps ▾	Line ▾	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	500	kbps ▾	Line ▾
<input type="checkbox"/>	500	kbps ▾	Line ▾	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	500	kbps ▾	Line ▾
<input type="checkbox"/>	500	kbps ▾	Line ▾	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	500	kbps ▾	Line ▾
<input type="checkbox"/>	500	kbps ▾	Line ▾	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	500	kbps ▾	Line ▾
<input type="checkbox"/>	500	kbps ▾	Line ▾	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	500	kbps ▾	Line ▾
<input type="checkbox"/>	500	kbps ▾	Line ▾	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	500	kbps ▾	Line ▾
<input type="checkbox"/>	500	kbps ▾	Line ▾	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	500	kbps ▾	Line ▾
<input type="checkbox"/>	500	kbps ▾	Line ▾	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	500	kbps ▾	Line ▾

S  
T  
R  
I  
C  
T

Save Reset Back

Описание каждого параметра представлено в следующей таблице

Параметр	Описание
Scheduling mode	<p>Необязательный режим планирования, диапазон конфигурации веса составляет от 1 до 100:</p> <ul style="list-style-type: none"> <li>• Строгий приоритет: Очереди 0–7 планируются с полным строгим приоритетом.</li> <li>• 2 веса очереди: Очереди 0–1 планируются по методу взвешенного кругового расписания, очереди 2–7 планируются с полным строгим приоритетом.</li> <li>• 3 веса очереди: Очереди 0–2 планируются по методу взвешенного кругового расписания, а очереди 3–7 планируются с полным строгим приоритетом.</li> <li>• 4 веса очереди: Очереди 0–3 планируются по методу взвешенного кругового расписания, а очереди 4–7 планируются с полным строгим приоритетом.</li> </ul>

Параметр	Описание
	<ul style="list-style-type: none"> <li>• 5 весов очереди: Очереди 0–4 планируются по методу взвешенного кругового расписания, а очереди 5-7 планируются с полным строгим приоритетом.</li> <li>• 6 весов очереди: Очереди 0–5 планируются по методу взвешенного кругового расписания, а очереди 6–7 планируются с полным строгим приоритетом.</li> <li>• 7 весов очереди: Очереди 0–6 планируются по методу взвешенного кругового расписания, а 7-я очередь планируется с полным строгим приоритетом.</li> <li>• 8 весов очереди: Очереди 0–7 планируются по методу взвешенного кругового расписания.</li> </ul>
Queue shaping	<ul style="list-style-type: none"> <li>• Включить: включить функцию ограничения входящей скорости на указанном интерфейсе.</li> <li>• Скорость: настроить значение ограничения входящей скорости на указанном интерфейсе. Диапазон ограничения скорости составляет &lt;1-13128147&gt;.</li> <li>• Единица: настроить единицу измерения ограничения скорости. Допустимые единицы измерения: kbps/Mbps//fps/kfps. По умолчанию используется kbps.</li> <li>• Режим скорости: настроить тип скорости ограничения скорости, который можно настроить как линия/данные/кадр. Единица измерения линии/данных - kbps/Mbps, а единица измерения кадра - fps/kfps. По умолчанию используется линия.</li> <li>• Доверие: Параметры конфигурации TSN.</li> </ul>
Queue scheduler	Cut-through: Включить ли режим обмена данными в режиме Cut-through.
Port shaping	<ul style="list-style-type: none"> <li>• Включить: Управляет включением формирования порта для порта коммутатора. Показываются только несервисные конфигурации.</li> <li>• Скорость: Управляет скоростью формирования порта. При "Единице" kbps значение ограничено от 100 до 3281943, а при "Единице" Mbps значение ограничено от 1 до 3281. Показываются только несервисные конфигурации. Скорость внутренне округляется до ближайшего значения, поддерживаемого формированием порта.</li> <li>• Единица: Единица измерения, используемая для управления скоростью формирования порта, такая как kbps/Mbps/fps/kfps. Показываются только несервисные конфигурации.</li> </ul>

Параметр	Описание
	<ul style="list-style-type: none"> <li>Режим скорости: Настроить тип скорости ограничения скорости, line/data/frame. Единица измерения line/data - kbps/Mbps, а единица измерения frame - fps/kfps. По умолчанию используется line.</li> </ul>

 Уведомление:

Line представляет собой скорость первого уровня (за исключением IPG); data - скорость второго уровня (включая IPG).

Cut-through Этот метод заменяет метод store-and-forward. Он не обеспечивает возможности обнаружения ошибок в пакетах и подвержен потере пакетов, но обладает низкой задержкой и высокой скоростью коммутации.

### 8.1.5 Формирование порта

Посмотрите страницу планирования портов

**QoS Egress Port Shapers**

Port	Shapers								Port
	Q0	Q1	Q2	Q3	Q4	Q5	Q6	Q7	
1	-	-	-	-	-	-	-	-	-
2	-	-	-	-	-	-	-	-	-
3	-	-	-	-	-	-	-	-	-
4	-	-	-	-	-	-	-	-	-
5	-	-	-	-	-	-	-	-	-
6	-	-	-	-	-	-	-	-	-
7	-	-	-	-	-	-	-	-	-
8	-	-	-	-	-	-	-	-	-
9	-	-	-	-	-	-	-	-	-
10	-	-	-	-	-	-	-	-	-
11	-	-	-	-	-	-	-	-	-
12	-	-	-	-	-	-	-	-	-
13	-	-	-	-	-	-	-	-	-
14	-	-	-	-	-	-	-	-	-
15	-	-	-	-	-	-	-	-	-
16	-	-	-	-	-	-	-	-	-
17	-	-	-	-	-	-	-	-	-
18	-	-	-	-	-	-	-	-	-
19	-	-	-	-	-	-	-	-	-
20	-	-	-	-	-	-	-	-	-
21	-	-	-	-	-	-	-	-	-
22	-	-	-	-	-	-	-	-	-
23	-	-	-	-	-	-	-	-	-
24	-	-	-	-	-	-	-	-	-
25	-	-	-	-	-	-	-	-	-
26	-	-	-	-	-	-	-	-	-
27	-	-	-	-	-	-	-	-	-
28	-	-	-	-	-	-	-	-	-
29	-	-	-	-	-	-	-	-	-
30	-	-	-	-	-	-	-	-	-
31	-	-	-	-	-	-	-	-	-
32	-	-	-	-	-	-	-	-	-
33	-	-	-	-	-	-	-	-	-
34	-	-	-	-	-	-	-	-	-
35	-	-	-	-	-	-	-	-	-
36	-	-	-	-	-	-	-	-	-

## 8.1.6 Маркировка портов

Страница установки меток на исходящих портах.

Port	Mode
<a href="#">1</a>	Classified
<a href="#">2</a>	Classified
<a href="#">3</a>	Classified
<a href="#">4</a>	Classified
<a href="#">5</a>	Classified
<a href="#">6</a>	Classified
<a href="#">7</a>	Classified
<a href="#">8</a>	Classified
<a href="#">9</a>	Classified
<a href="#">10</a>	Classified
<a href="#">11</a>	Classified
<a href="#">12</a>	Classified
<a href="#">13</a>	Classified
<a href="#">14</a>	Classified
<a href="#">15</a>	Classified
<a href="#">16</a>	Classified
<a href="#">17</a>	Classified
<a href="#">18</a>	Classified
<a href="#">19</a>	Classified
<a href="#">20</a>	Classified
<a href="#">21</a>	Classified
<a href="#">22</a>	Classified
<a href="#">23</a>	Classified
<a href="#">24</a>	Classified
<a href="#">25</a>	Classified
<a href="#">26</a>	Classified
<a href="#">27</a>	Classified
<a href="#">28</a>	Classified
<a href="#">29</a>	Classified
<a href="#">30</a>	Classified
<a href="#">31</a>	Classified
<a href="#">32</a>	Classified
<a href="#">33</a>	Classified
<a href="#">34</a>	Classified
<a href="#">35</a>	Classified
<a href="#">36</a>	Classified

Щелкните на ссылке порта, чтобы войти на страницу конфигурации маркировки исходящего порта, как показано на рисунке ниже.

QoS Egress Port Tag Remarking Port 1 Port 1 ▾

Tag Remarking Mode Mapped ▾

(CoS, DPL) to (PCP, DEI) Mapping

CoS	DPL	PCP	DEI
*	*	<> ▾	<> ▾
0	0	1 ▾	0 ▾
0	1	1 ▾	1 ▾
1	0	0 ▾	0 ▾
1	1	0 ▾	1 ▾
2	0	2 ▾	0 ▾
2	1	2 ▾	1 ▾
3	0	3 ▾	0 ▾
3	1	3 ▾	1 ▾
4	0	4 ▾	0 ▾
4	1	4 ▾	1 ▾
5	0	5 ▾	0 ▾
5	1	5 ▾	1 ▾
6	0	6 ▾	0 ▾
6	1	6 ▾	1 ▾
7	0	7 ▾	0 ▾
7	1	7 ▾	1 ▾

Save
Reset
Cancel

Описание каждого параметра представлено в следующей таблице

Параметр	Описание
Label relabeling mode	Режим переосмысления меток, варианты, следующие: <ul style="list-style-type: none"> <li>• Классификация: означает, что функция переустановки меток не активирована.</li> <li>• По умолчанию: означает, что все CoS и DPL отображаются на один и тот же PCP и DEI.</li> <li>• Сопоставление: означает сопоставление в соответствии с записью cos-tag.</li> </ul>
CoS	Отображение значения CoS входящего направления.
DPL	Отображение значения DPL входящего направления.
PCP	Перемеченное значение 802.1P.
DEI	Перемеченное значение CFI.

### 8.1.7 Порт DSCP

Страница настройки DSCP порта.

QoS Port DSCP Configuration

Port	Ingress		Egress
	Translate	Classify	Rewrite
*	<input type="checkbox"/>	<> ▾	<> ▾
1	<input type="checkbox"/>	Disable ▾	Disable ▾
2	<input type="checkbox"/>	Disable ▾	Disable ▾
3	<input type="checkbox"/>	Disable ▾	Disable ▾
4	<input type="checkbox"/>	Disable ▾	Disable ▾
5	<input type="checkbox"/>	Disable ▾	Disable ▾
6	<input type="checkbox"/>	Disable ▾	Disable ▾
7	<input type="checkbox"/>	Disable ▾	Disable ▾
8	<input type="checkbox"/>	Disable ▾	Disable ▾
9	<input type="checkbox"/>	Disable ▾	Disable ▾
10	<input type="checkbox"/>	Disable ▾	Disable ▾
11	<input type="checkbox"/>	Disable ▾	Disable ▾
12	<input type="checkbox"/>	Disable ▾	Disable ▾
13	<input type="checkbox"/>	Disable ▾	Disable ▾
14	<input type="checkbox"/>	Disable ▾	Disable ▾
15	<input type="checkbox"/>	Disable ▾	Disable ▾
16	<input type="checkbox"/>	Disable ▾	Disable ▾
17	<input type="checkbox"/>	Disable ▾	Disable ▾
18	<input type="checkbox"/>	Disable ▾	Disable ▾
19	<input type="checkbox"/>	Disable ▾	Disable ▾
20	<input type="checkbox"/>	Disable ▾	Disable ▾
21	<input type="checkbox"/>	Disable ▾	Disable ▾
22	<input type="checkbox"/>	Disable ▾	Disable ▾
23	<input type="checkbox"/>	Disable ▾	Disable ▾
24	<input type="checkbox"/>	Disable ▾	Disable ▾
25	<input type="checkbox"/>	Disable ▾	Disable ▾
26	<input type="checkbox"/>	Disable ▾	Disable ▾
27	<input type="checkbox"/>	Disable ▾	Disable ▾
28	<input type="checkbox"/>	Disable ▾	Disable ▾
29	<input type="checkbox"/>	Disable ▾	Disable ▾
30	<input type="checkbox"/>	Disable ▾	Disable ▾
31	<input type="checkbox"/>	Disable ▾	Disable ▾
32	<input type="checkbox"/>	Disable ▾	Disable ▾
33	<input type="checkbox"/>	Disable ▾	Disable ▾
34	<input type="checkbox"/>	Disable ▾	Disable ▾
35	<input type="checkbox"/>	Disable ▾	Disable ▾
36	<input type="checkbox"/>	Disable ▾	Disable ▾

Save Reset

Описание каждого параметра представлено в следующей таблице

Параметр	Описание
Convert	Включить/отключить функцию преобразования входящего DSCP. После включения функции преобразования на интерфейсе выполняется отображение в соответствии с опцией "Translate" в записи отображения DSCP во входящем направлении. Преобразование имеет более низкий приоритет, чем классификация.

Параметр	Описание
Classification	<p>Настройка вариантов классификации входящего DSCP. Варианты, следующие:</p> <ul style="list-style-type: none"><li>• Отключить</li><li>• DSCP=0: Указывает, что обрабатываются только пакеты с значением DSCP равным 0, и пакеты обрабатываются в соответствии с таблицей классификации DSCP.</li><li>• Выбранный: указывает, что обрабатываются только пакеты DSCP с включенной классификацией во входящем направлении в записи отображения DSCP, и пакеты обрабатываются в соответствии с записью классификации DSCP.</li><li>• Все: Все пакеты обрабатываются в соответствии с записями классификации DSCP. Для пакетов, совпадающих с записями таблицы классификации, необходимо включить функцию перезаписи на исходящем порту (Включить).</li></ul>
Rewrite	<p>Настройка опций перезаписи в исходящем направлении порта. Варианты следующие:</p> <ul style="list-style-type: none"><li>• Отключить</li><li>• Включить: Для пакетов, классифицированных по DSCP во входящем направлении, необходимо выбрать Включить для исходящего порта этого типа пакета.</li><li>• Перемапировать: Перемапировать в соответствии с конфигурацией перемапирования в исходящем направлении в записи таблицы отображения DSCP.</li></ul>

## 8.1.8 DSCP-QoS

Страница настройки записи DSCP-CoS.

**DSCP-Based QoS Ingress Classification**

DSCP	Trust	CoS	DPL
*	<input type="checkbox"/>	<> ▾	<> ▾
0 (BE)	<input type="checkbox"/>	0 ▾	0 ▾
1	<input type="checkbox"/>	0 ▾	0 ▾
2	<input type="checkbox"/>	0 ▾	0 ▾
3	<input type="checkbox"/>	0 ▾	0 ▾
4	<input type="checkbox"/>	0 ▾	0 ▾
5	<input type="checkbox"/>	0 ▾	0 ▾
6	<input type="checkbox"/>	0 ▾	0 ▾
7	<input type="checkbox"/>	0 ▾	0 ▾
8 (CS1)	<input type="checkbox"/>	0 ▾	0 ▾
9	<input type="checkbox"/>	0 ▾	0 ▾
10 (AF11)	<input type="checkbox"/>	0 ▾	0 ▾
11	<input type="checkbox"/>	0 ▾	0 ▾
12 (AF12)	<input type="checkbox"/>	0 ▾	0 ▾
13	<input type="checkbox"/>	0 ▾	0 ▾
14 (AF13)	<input type="checkbox"/>	0 ▾	0 ▾
15	<input type="checkbox"/>	0 ▾	0 ▾
16 (CS2)	<input type="checkbox"/>	0 ▾	0 ▾
17	<input type="checkbox"/>	0 ▾	0 ▾
18 (AF21)	<input type="checkbox"/>	0 ▾	0 ▾
19	<input type="checkbox"/>	0 ▾	0 ▾
20 (AF22)	<input type="checkbox"/>	0 ▾	0 ▾
21	<input type="checkbox"/>	0 ▾	0 ▾

Описание каждого параметра представлено в следующей таблице

Параметр	Описание
Trust	Включить функцию отображения DSCP на CoS.
CoS	Отобразить значение CoS.
DPL	Отобразить значения DPL.

### 8.1.9 Отображение DSCP

Страница записи отображения DSCP.

**DSCP Translation**

DSCP	Ingress		Egress Remap
	Translate	Classify	
*	<> ▾	<input type="checkbox"/>	<> ▾
0 (BE)	0 (BE) ▾	<input type="checkbox"/>	0 (BE) ▾
1	1 ▾	<input type="checkbox"/>	1 ▾
2	2 ▾	<input type="checkbox"/>	2 ▾
3	3 ▾	<input type="checkbox"/>	3 ▾
4	4 ▾	<input type="checkbox"/>	4 ▾
5	5 ▾	<input type="checkbox"/>	5 ▾
6	6 ▾	<input type="checkbox"/>	6 ▾
7	7 ▾	<input type="checkbox"/>	7 ▾
8 (CS1)	8 (CS1) ▾	<input type="checkbox"/>	8 (CS1) ▾
9	9 ▾	<input type="checkbox"/>	9 ▾
10 (AF11)	10 (AF11) ▾	<input type="checkbox"/>	10 (AF11) ▾
11	11 ▾	<input type="checkbox"/>	11 ▾
12 (AF12)	12 (AF12) ▾	<input type="checkbox"/>	12 (AF12) ▾
13	13 ▾	<input type="checkbox"/>	13 ▾
14 (AF13)	14 (AF13) ▾	<input type="checkbox"/>	14 (AF13) ▾
15	15 ▾	<input type="checkbox"/>	15 ▾
16 (CS2)	16 (CS2) ▾	<input type="checkbox"/>	16 (CS2) ▾
17	17 ▾	<input type="checkbox"/>	17 ▾
18 (AF21)	18 (AF21) ▾	<input type="checkbox"/>	18 (AF21) ▾
19	19 ▾	<input type="checkbox"/>	19 ▾
20 (AF22)	20 (AF22) ▾	<input type="checkbox"/>	20 (AF22) ▾
21	21 ▾	<input type="checkbox"/>	21 ▾
22 (AF23)	22 (AF23) ▾	<input type="checkbox"/>	22 (AF23) ▾
23	23 ▾	<input type="checkbox"/>	23 ▾

Описание каждого параметра представлено в следующей таблице

Параметр	Описание
Convert	Настройка отображения DSCP входящего направления на DSCP.
Classification	Включить/отключить указанную функцию классификации DSCP.
Remap	Настройка отображения DSCP исходящего направления на DSCP.

### 8.1.10 DSCP классификация

Настройка записей таблицы классификации DSCP.

**DSCP Classification**

CoS	DSCP DP0	DSCP DP1	DSCP DP2	DSCP DP3
*	<> ▾	<> ▾	<> ▾	<> ▾
0	0 (BE) ▾	0 (BE) ▾	0 (BE) ▾	0 (BE) ▾
1	0 (BE) ▾	0 (BE) ▾	0 (BE) ▾	0 (BE) ▾
2	0 (BE) ▾	0 (BE) ▾	0 (BE) ▾	0 (BE) ▾
3	0 (BE) ▾	0 (BE) ▾	0 (BE) ▾	0 (BE) ▾
4	0 (BE) ▾	0 (BE) ▾	0 (BE) ▾	0 (BE) ▾
5	0 (BE) ▾	0 (BE) ▾	0 (BE) ▾	0 (BE) ▾
6	0 (BE) ▾	0 (BE) ▾	0 (BE) ▾	0 (BE) ▾
7	0 (BE) ▾	0 (BE) ▾	0 (BE) ▾	0 (BE) ▾

Save Reset

Описание каждого параметра представлено в следующей таблице

Параметр	Описание
QoS classification	Фактический класс QoS.
DSCP DP0	Выберите значение DSCP (0-63) для классификации для уровня приоритета сброса 0.
DSCP DP1	Выберите значение DSCP (0-63) для классификации для уровня приоритета сброса 1.
DSCP DP2	Выберите значение DSCP (0-63) для классификации для уровня приоритета сброса 2.
DSCP DP3	Выберите значение DSCP (0-63) для классификации для уровня приоритета сброса 3.

### 8.1.11 Сопоставление записей

Настройка записей таблицы сопоставления..

**QoS Ingress Map Configuration** Auto-refresh

Map ID	Key-Type	Action-Type					CoS ID
		CoS	DPL	PCP	DEI	DSCP	
							+

Страница создания/изменения экземпляра сопоставления входящего направления.

**Ingress Map Configuration**

**Ingress Map ID**

MAP ID

**Ingress Map Key**

Map Key

**Ingress Map Action**

CoS	Disabled ▾
DPL	Disabled ▾
PCP	Disabled ▾
DEI	Disabled ▾
DSCP	Disabled ▾
CoS ID	Disabled ▾

Описание каждого параметра представлено в следующей таблице

Параметр	Описание
Mapping ID	Идентификатор экземпляра сопоставления входящего направления. Диапазон <0-255>.
Mapping key	Тип ключа сопоставления входящего направления. Дополнительные опции: PCP/PCP-DEI/DSCP/DSCP-PCP-DEI.
CoS	Включить или настроить значение CoS.
DPL	Включить или настроить значение DPL.
PCP	Включить или настроить сопоставление значений PCP или отображение значений PCP.
DEI	Включить или настроить сопоставление значений DEI или отображение значений DEI.
DSCP	Включить или настроить сопоставление значений DSCP или отображение значений DSCP.
CoS ID	Включить или настроить значение CoS ID.

### 8.1.12 Экспорт сопоставления

Настройка записей сопоставления экспорта.

**QoS Egress Map Configuration** Auto-refresh  Refresh Remove All

Map ID	Key-Type	Action-Type		
		PCP	DEI	DSCP

+

Описание каждого параметра представлено в следующей таблице

Параметр	Описание
Mapping ID	Идентификатор экземпляра сопоставления исходящего направления. Диапазон <0-511>.
Key type	Тип ключа сопоставления исходящего направления. Опционально: CoS ID/CoS ID-DPL/DSCP/DSCP-DPL.
Function type	<p>Укажите тип операции, который будет использоваться для фильтрации правил сопоставления при применении сопоставления. Возможные типы операций:</p> <ul style="list-style-type: none"> <li>PCP: Приоритетный кодовый пункт.</li> <li>DEI: Индикатор пригодности для удаления.</li> <li>DSCP: Кодовая точка подсервиса.</li> </ul>

### 8.1.13 QoS список управления

Настройка списка управления QoS.

**QoS Control List Configuration**

QCE	Port	DMAC	SMAC	Tag	VID	PCP	DEI	Frame	Action					
									CoS	DPL	DSCP	PCP	DEI	Policy

+

Щелкните кнопку "Добавить значок", чтобы войти на страницу конфигурации QCE, как показано на рисунке ниже..

### QCE Configuration

Port Members																																				
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	
<input checked="" type="checkbox"/>																																				

#### Key Parameters

DMAC	Any
SMAC	Any
Tag	Any
VID	Any
PCP	Any
DEI	Any
Inner Tag	Any
Inner VID	Any
Inner PCP	Any
Inner DEI	Any
Frame Type	Any

#### Action Parameters

CoS	0
DPL	Default
DSCP	Default
PCP	Default
DEI	Default
Policy	
Ingress Map ID	

Save
Reset
Cancel

Описание каждого параметра представлено в следующей таблице

Параметр	Описание
Port member	Укажите порт, для которого применяется эта QCE.
<b>Key parameter</b>	<b>Ключевой параметр.</b>
Destination MAC	Настройте соответствие информации DMAC.
Source MAC	Настройте соответствие информации SMAC.
Label	Настройте параметры соответствия тегов. Варианты: Не помечен/Помечен/S-Помечен/C-Помечен.
VID	Настройте соответствие VID.
PCP	Настройте соответствие или переопределение значений 802.1P.
DEI	Настройте соответствие или переопределение значений CFI.
Inner label	Настройте параметры соответствия внутреннему тегу. Варианты: Не помечен/Помечен/S-Помечен/C-Помечен.
Inner VID	Настройте соответствие внутреннему VID.
Inner PCP	Настройте значения, соответствующие внутреннему 802.1P.
Medial DEI	Настройте значение, соответствующее внутреннему CFI.
Frame type	Настройте параметры соответствия типу кадра. Возможные значения: EtherType/LLC/SNAP/IPv4/IPv6.
<b>Function parameter</b>	<b>Параметр функции.</b>
CoS	Сопоставленное значение CoS.
DPL	Сопоставленное значение DPL.

Параметр	Описание
DSCP	Сопоставленное значение DSCP.
Strategy	Применить экземпляр политики. Для этой информации о политике необходимо проверить информацию о конфигурации ACL.
Ingress Map ID	Применить пример входящего сопоставления.
<b>EtherType parameters</b>	<b>Параметры EtherType.</b>
EtherType	Когда тип кадра - "EtherType", диапазон настраиваемых значений составляет <0x600-0x7ff, 0x801-0x86dc, 0x86de-0xffff>

## 8.1.14 Стратегия управления бурей

Страница настройки политики бурь.

**Global Storm Policer Configuration**

Frame Type	Enable	Rate	Unit
Unicast	<input type="checkbox"/>	10	fps
Multicast	<input type="checkbox"/>	10	fps
Broadcast	<input type="checkbox"/>	10	fps

**Port Storm Policer Configuration**

Port	Unicast Frames			Broadcast Frames			Unknown Frames		
	Enable	Rate	Unit	Enable	Rate	Unit	Enable	Rate	Unit
*	<input type="checkbox"/>	500	<>	<input type="checkbox"/>	500	<>	<input type="checkbox"/>	500	<>
1	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	500	kbps
2	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	500	kbps
3	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	500	kbps
4	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	500	kbps
5	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	500	kbps
6	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	500	kbps
7	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	500	kbps
8	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	500	kbps
9	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	500	kbps
10	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	500	kbps
11	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	500	kbps
12	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	500	kbps
13	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	500	kbps
14	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	500	kbps
15	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	500	kbps
16	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	500	kbps
17	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	500	kbps
18	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	500	kbps
19	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	500	kbps
20	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	500	kbps
21	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	500	kbps

Описание каждого параметра представлено в следующей таблице

Параметр	Описание
Enable	Включить/отключить функцию политики бурь для одиночных/широковещательных/многоадресных/неизвестных кадров.
Rate	Настроить значение ограничения скорости политики бурь для указанного интерфейса. Диапазон ограничения скорости составляет <1-13128147>.

Параметр	Описание
Unit	Настроить единицу измерения скорости ограничения. Допустимые единицы измерения: kbps/Mbps/fps/kfps. По умолчанию используется kbps.

 Уведомление:

Режим ограничения скорости - это скорость на уровне кадра (за исключением IPG).

В глобальной конфигурации бури: Одиночные кадры - это неизвестные одиночные кадры; Многоадресные - это неизвестные многоадресные кадры; Широковещательные - это неизвестные широковещательные кадры.

В конфигурации бури на интерфейсе: Одиночные кадры - это известные одиночные кадры + неизвестные одиночные кадры; Неизвестные - это неизвестные одиночные кадры + неизвестные многоадресные кадры + широковещательные.

### 8.1.15 Статистика QoS

Просмотр статистики отправки и приема пакетов в очередях QoS.

Queuing Counters		Auto-refresh <input type="checkbox"/> Refresh Clear														
Port	Q0		Q1		Q2		Q3		Q4		Q5		Q6		Q7	
	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx
1	796547	11234	0	0	0	0	0	0	0	0	0	0	0	0	0	7
2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
11	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
12	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
13	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
14	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
15	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
17	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
18	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
19	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
20	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
21	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
22	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
23	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
24	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
25	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
26	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
27	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
28	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
29	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
30	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
31	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
32	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
33	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
34	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
35	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
36	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Описание каждого параметра представлено в следующей таблице

Параметр	Описание
Port	Номер порта коммутатора
Queue 1-7	Каждый порт имеет 8 очередей QoS. Очередь 0 является очередью с наименьшим приоритетом. <ul style="list-style-type: none"> <li>• TX: Количество пакетов, отправленных каждой очередью.</li> <li>• RX: Количество пакетов, принятых каждой очередью.</li> </ul>

### 8.1.16 QCL статус

Проверьте состояние списка управления QoS.

**QoS Control List Status** 

 Auto-refresh

User	QCE	Port	Frame	Action						Conflict
				CoS	DPL	DSCP	PCP	DEI	Policy	
No entries										

Описание каждого параметра представлено в следующей таблице

Параметр	Описание
user	Укажите пользователей QCL.
QoS control ID	Укажите идентификатор QCE.
Port	Укажите список портов, настроенных с использованием QCE.
Frame type	Укажите тип кадра. Возможные значения: <ul style="list-style-type: none"> <li>• Любой (Any): Соответствует любому типу кадра.</li> <li>• Ethernet: Соответствует кадрам типа Ethernet.</li> <li>• LLC: Соответствует кадрам LLC (Logical Link Control).</li> <li>• SNAP: Соответствует кадрам SNAP (Subnetwork Access Protocol).</li> <li>• IPv4: Соответствует кадрам IPv4.</li> <li>• IPv6: Соответствует кадрам IPv6.</li> </ul>
Action	Укажите действие классификации, которое должно быть выполнено над входящим кадром, если настроенные параметры соответствуют содержимому кадра. Возможные действия: <ul style="list-style-type: none"> <li>• CoS: Классификация услуг.</li> <li>• DPL: Классификация приоритетов сброса.</li> <li>• DSCP: Классификация значений DSCP.</li> </ul>

Параметр	Описание
	<ul style="list-style-type: none"> <li>PCP: Классификация значений PCP.</li> <li>DEI: Классификация значений DEI.</li> <li>Policy: Содержание шаблона политики (совпадающие элементы и элементы функции), созданного с использованием модуля ACL.</li> <li>Входящее направление сопоставления.</li> </ul>
Conflict	<p>Отображает статус конфликта записей QCL. Поскольку аппаратные ресурсы используются несколькими приложениями, может возникнуть ситуация, когда ресурсы, необходимые для добавления записи QCE, недоступны. В этом случае статус конфликта будет показан как "Да" (Yes), в противном случае всегда будет "Нет" (No). Обратите внимание, что нажатие кнопки "Разрешить конфликт" освобождает ресурсы, используемые аппаратным обеспечением, для добавления записи QCL и разрешает конфликт.</p>

## 8.2 DDM

DDM (Digital Diagnostic Monitoring) - это эффективный метод мониторинга важных параметров работы оптических модулей. Он включает в себя мониторинг таких рабочих параметров, как температура, рабочее напряжение, ток смещения, оптическая мощность передачи, оптическая мощность приема, а также информацию об их аварийных ситуациях и т. д. Через цифровую диагностическую функцию оптического модуля коммутатор может мониторить вышеуказанные пять рабочих параметров модуля в реальном времени, быстро находить конкретное место ошибки в оптическом кабеле, упрощать работу по обслуживанию и повышать надежность системы.

Все оптические порты этого коммутатора являются интерфейсами цифрового мониторинга диагностики (DDMI), которые могут обеспечивать расширенные функции диагностики оптических модулей и в реальном времени запрашивать информацию о передатчике, информацию о рабочих параметрах и различные предупреждения о различных оптических модулях, вставленных в интерфейс, а также информацию об авариях и т. д., таким образом, пользователи могут быстро локализовать неисправности оптического модуля, предотвратить проблемы с оптическим модулем заранее и решать их своевременно.

### 8.2.1 DDM конфигурация

Страница конфигурации DDMI используется для настройки глобального состояния коммутатора функции цифрового диагностического мониторинга для всех оптических портов на коммутаторе, как показано на рисунке ниже.

**DDMI Configuration**

Mode

Save

Описание каждого параметра представлено в следующей таблице

Параметр	Описание
Mode	Настройка статуса включения глобального переключателя DDMI. <ul style="list-style-type: none"> <li>Включить: Включить функцию DDMI.</li> <li>Отключить: Отключить функцию DDMI.</li> </ul>

## 8.2.2 DDM обзор

На странице сводки DDMI отображается список информации об оптических трансиверах SFP всех оптических портов на коммутаторе, как показано на рисунке ниже.

**DDMI Overview** Auto-refresh  [Refresh](#)

Port	Vendor	Part Number	Serial Number	Revision	Date Code	Transceiver
9	-	-	-	-	-	-
10	-	-	-	-	-	-
11	-	-	-	-	-	-
12	-	-	-	-	-	-
13	-	-	-	-	-	-
14	-	-	-	-	-	-
15	-	-	-	-	-	-
16	-	-	-	-	-	-
17	-	-	-	-	-	-
18	-	-	-	-	-	-
19	-	-	-	-	-	-
20	-	-	-	-	-	-
21	-	-	-	-	-	-
22	-	-	-	-	-	-
23	-	-	-	-	-	-
24	-	-	-	-	-	-
25	-	-	-	-	-	-
26	-	-	-	-	-	-
27	-	-	-	-	-	-
28	-	-	-	-	-	-
29	-	-	-	-	-	-
30	-	-	-	-	-	-
31	-	-	-	-	-	-
32	-	-	-	-	-	-
33	-	-	-	-	-	-
34	-	-	-	-	-	-
35	-	-	-	-	-	-
36	-	-	-	-	-	-

Описание каждого параметра представлено в следующей таблице

Параметр	Описание
Port	Порт DDMI. Щелкните ссылку порта, чтобы просмотреть подробную информацию о модуле SFP указанного порта.
Manufacturer	Наименование производителя SFP.
Part code	Компонентный код PN, предоставленный производителем SFP.
Serial number	Серийный номер SN, предоставленный производителем SFP.
Revision	Ревизия части SFP.
Production Date	Дата производства SFP.
Transceiver	Тип оптического трансивера SFP.

### 8.2.3 DDM детали

На странице с подробной информацией DDMI выбирается номер порта первого оптического порта из выпадающего списка портов в правом верхнем углу страницы. Подробная информация о модуле SFP на оптическом порту отображается в нижней части страницы, включая две таблицы: информацию о трансивере и информацию о цифровом диагностическом мониторинге DDMI.

**Transceiver Information** Port 9 ▾ Auto-refresh  Refresh

Vendor	-
Part Number	-
Serial Number	-
Revision	-
Date Code	-
Transceiver	-

**DDMI Information**

Type	Current	Alarm/Warning	Low Warning Threshold	High Warning Threshold	Low Alarm Threshold	High Alarm Threshold
Temperature [C]	-	-	-	-	-	-
Voltage [V]	-	-	-	-	-	-
Tx Bias [mA]	-	-	-	-	-	-
Tx Power [mW]	-	-	-	-	-	-
Rx Power [mW]	-	-	-	-	-	-

Описание каждого параметра представлено в следующей таблице

Параметр	Описание
<b>Transceiver information</b>	<b>Информация о трансивере</b>
Manufacturer	Наименование поставщика SFP.
Mode	Компонентный номер PN, предоставленный поставщиком SFP.
Serial number	Серийный номер SN, предоставленный поставщиком.
Revision	Ревизия части SFP.
Production Date	Код даты изготовления SFP.
Transceiver	Тип оптического трансивера SFP.
<b>Optical module information</b>	<b>Информация об оптическом модуле</b>
The current value	Текущие значения температуры, напряжения, тока смещения, передаваемой оптической мощности и принимаемой оптической мощности.
Alarm/Early Warning	Индикация наличия предупреждений или предупреждений о ранних сигналах для температуры, напряжения, тока смещения, передаваемой оптической мощности и принимаемой оптической мощности.
Lower warning limit	Нижние пороги предупреждения для температуры, напряжения, тока смещения, передаваемой оптической мощности и принимаемой оптической мощности.
Early warning upper limit	Верхние пороги предупреждения для температуры, напряжения, тока смещения, передаваемой оптической мощности и принимаемой оптической мощности.

Параметр	Описание
Alarm lower limit	Нижние пороги аварийного сигнала для температуры, напряжения, тока смещения, передаваемой оптической мощности и принимаемой оптической мощности.
Alarm upper limit	Верхние пороги аварийного сигнала для температуры, напряжения, тока смещения, передаваемой оптической мощности и принимаемой оптической мощности.

## 8.3 Ping

Ping (Packet Internet Groper, поиск пакетов в интернете) - это инструмент для исследования сетевых пакетов, программа, используемая для тестирования уровня сетевых соединений. В интернете для упрощения проверки состояния сети между устройством и целевым хостом был введен механизм Ping. Ping используется для определения доступности целевой станции и понимания соответствующего состояния.

### 8.3.1 Ping (IPv4)

Страница конфигурации Ping (IPv4).

**Ping (IPv4)**

Fill in the parameters as needed and press "Start" to initiate the Ping session.

Hostname or IP Address	<input type="text"/>	
Payload Size	<input type="text" value="56"/>	bytes
Payload Data Pattern	<input type="text" value="0"/>	(single byte value; integer or hex with prefix '0x')
Packet Count	<input type="text" value="5"/>	packets
TTL Value	<input type="text" value="64"/>	
VID for Source Interface	<input type="text"/>	
Source Port Number	<input type="text"/>	
IP Address for Source Interface	<input type="text"/>	
Quiet (only print result)	<input type="checkbox"/>	

Описание каждого параметра представлено в следующей таблице

Параметр	Описание
IP or domain name	Имя или IP-адрес целевого хоста.
Message size	Размер полезной нагрузки ICMP-сообщения, также может быть понят как размер пакета PING, размер сообщения, отправляемого на целевой адрес. Диапазон от 2 до 1452 байт, значение по умолчанию - 56 байт.
Data input	Режим данных полезной нагрузки ICMP-сообщения. Значение в один байт - это целое число или шестнадцатеричное число, предваренное "0x". Диапазон от 0 до 255. Значение по умолчанию - 0.
Number of messages	Количество сообщений, количество отправляемых сообщений, в диапазоне от 1 до 60, значение по умолчанию - 5.
TTL value	Время жизни (TTL), значение TTL уменьшается на 1 при прохождении через маршрутизатор. Когда оно уменьшается

Параметр	Описание
	до 0, пакет отбрасывается. Диапазон от 0 до 255, значение по умолчанию - 64.
Source port VLAN ID	VID идентификатор источника порта и VLAN ID источника порта, в диапазоне от 1 до 4095.
Source port number	Номер источника порта.
Source IP	IP-адрес источника порта.
Simple mode (only output results)	После проверки будут напечатаны только результаты, подробные данные процесса пинга не будут напечатаны.

 **Примечание:**

Обязательно заполните информацию об IP-адресе или доменном имени, размере пакета, заполнении данных, количестве пакетов и значении TTL.

Необходимо настроить только одно из значений VLAN ID или IP-адреса источника порта.

Необходимо настроить только одно из значений номера порта источника или IP-адреса порта источника.

### 8.3.2 Ping (IPv6)

Страница конфигурации Ping (IPv6).

**Ping (IPv6)**

Fill in the parameters as needed and press "Start" to initiate the Ping session.

Hostname or IP Address	<input type="text"/>	
Payload Size	<input type="text" value="56"/>	bytes
Payload Data Pattern	<input type="text" value="0"/>	(single byte value; integer or hex with prefix '0x')
Packet Count	<input type="text" value="5"/>	packets
VID for Source Interface	<input type="text"/>	
Source Port Number	<input type="text"/>	
IP Address for Source Interface	<input type="text"/>	
Quiet (only print result)	<input type="checkbox"/>	

Описание каждого параметра представлено в следующей таблице

Параметр	Описание
IP or domain name	Направление имя хоста или IP-адрес.
Message size	Размер полезной нагрузки ICMP-сообщения также можно понимать как размер пакета PING, размер сообщения, отправленного на целевой адрес. Диапазон составляет от 2 до 1452 байт, а значение по умолчанию составляет 56 байт.
Data input	Режим данных полезной нагрузки ICMP-сообщения. Однобайтное значение представляет собой целое число или шестнадцатеричное число с префиксом "0x". Диапазон составляет от 0 до 255, а значение по умолчанию - 0.

Параметр	Описание
Number of messages	Количество сообщений, количество отправленных сообщений, варьируется от 1 до 60, а значение по умолчанию - 5.
Source port VLAN ID	VID источника порта и VLAN ID источника порта, варьирующиеся от 1 до 4095.
Source port number	Номер порта источника.
Source IP	IP-адрес порта источника.
Simple mode (only output results)	После проверки будут напечатаны только результаты, а подробные данные процесса пинга не будут напечатаны.

 **Примечание:**

Обязательно заполните информацию об IP-адресе или доменном имени, размере пакета, заполнении данных и количестве пакетов.

Необходимо настроить только одно из значений VLAN ID или IP-адреса источника порта.

Необходимо настроить только одно из значений номера порта источника или IP-адреса порта источника.

## 8.4 Traceroute

Traceroute - это важный инструмент для определения маршрута между исходным хостом и целевым хостом. Это также самый удобный инструмент. Хотя инструмент Ping также может обнаружить маршрут, преимущество Traceroute заключается в том, что он может записывать пройденные маршрутизаторы.

Traceroute использует протокол ICMP для определения всех маршрутизаторов между исходным хостом и целевым хостом, отображает количество маршрутизаторов или шлюзов, через которые проходит сообщение, с помощью TTL, управляет значением TTL независимых ICMP-сообщений и наблюдает за возвращаемой информацией, когда сообщение отбрасывается.

### 8.4.1 Traceroute (IPv4)

Настройка страницы информации Traceroute (IPv4).

**Traceroute (IPv4)**

Fill in the parameters as needed and press "Start" to initiate the Traceroute session.

Hostname or IP Address	<input type="text"/>	
DSCP Value	<input type="text" value="0"/>	
Number of Probes Per Hop	<input type="text" value="3"/>	packets
Response Timeout	<input type="text" value="3"/>	seconds
First TTL Value	<input type="text" value="1"/>	
Max TTL Value	<input type="text" value="30"/>	
VID for Source Interface	<input type="text"/>	
IP Address for Source Interface	<input type="text"/>	
Use ICMP instead of UDP	<input type="checkbox"/>	
Print Numeric Addresses	<input type="checkbox"/>	

Описание каждого параметра представлено в следующей таблице

Параметр	Описание
IP or domain name	Имя хоста или IP-адрес.
DSCP value	DSCP - это кодовая точка проверки оценки службы, которая является полем в пакете данных IP и может назначать различные уровни обслуживания для сетевых коммуникаций. Чем выше значение, тем выше приоритет, варьируется от 0 до 63.
Number of attempts per hop	Определите количество проб (пакетов), отправляемых на каждом хопе. Значение по умолчанию - 3. Допустимый диапазон - от 1 до 60.
Response timeout	Определяет количество секунд ожидания ответа на отправленный запрос, варьируется от 1 до 86400.
First hop TTL value	Определите значение поля "время жизни" (TTL) в заголовке IPv4 в первом отправленном пакете. Число по умолчанию - 1. Допустимый диапазон - от 1 до 30.
TTL maximum value	Определяет максимальное значение поля "время жизни" (TTL) в заголовке IPv4. Тестирование прекращается, если указанный удаленный хост достигнут до достижения этого значения. Число по умолчанию - 30. Допустимый диапазон - от 1 до 255.
Source port VLAN ID	Идентификатор VLAN исходного порта. Это поле может использоваться для принудительного использования теста определенного интерфейса с нативным VLAN в качестве исходного интерфейса. Оставьте это поле пустым для автоматического выбора на основе конфигурации маршрутизации. Диапазон - от 1 до 4095.
Source IP	IP-адрес исходного порта.
Use ICMP instead of UDP	Использовать сообщения ICMP вместо сообщений UDP.
Output IP address	По умолчанию команда traceroute будет выводить информацию о ХОП для полученного IP-адреса хоста, используя обратный DNS-поиск. Если DNS-информация недоступна, это может замедлить отображение. Выбор этой опции предотвратит обратный DNS-поиск и принудит команду traceroute выводить числовые IP-адреса.

 Примечание:

Требуемая информация включает IP- или доменное имя, значение DSCP, количество попыток для каждого хопа, тайм-аут ответа, значение TTL для первого хопа и максимальное значение TTL.

Значение TTL для первого хопа должно быть меньше максимального значения TTL.

### 8.4.2 Traceroute (IPv6)

Настройка страницы информации Traceroute (IPv6).

### Traceroute (IPv6)

Fill in the parameters as needed and press "Start" to initiate the Traceroute session.

Hostname or IP Address	<input type="text"/>	
DSCP Value	<input type="text" value="0"/>	
Number of Probes Per Hop	<input type="text" value="3"/>	packets
Response Timeout	<input type="text" value="3"/>	seconds
Max TTL Value	<input type="text" value="30"/>	
VID for Source Interface	<input type="text"/>	
IP Address for Source Interface	<input type="text"/>	
Print Numeric Addresses	<input type="checkbox"/>	

Описание каждого параметра представлено в следующей таблице

Параметр	Описание
IP or domain name	Имя хоста или IP-адрес.
DSCP value	DSCP (Differentiated Services Code Point) - это поле в пакете данных IP, которое может назначать различные уровни обслуживания для сетевых коммуникаций. Чем выше значение, тем выше приоритет, варьируется от 0 до 63.
Number of attempts per hop	Определите количество проб (пакетов), отправляемых на каждом хопе. Значение по умолчанию - 3. Допустимый диапазон - от 1 до 60.
Response timeout	Определяет количество секунд ожидания ответа на отправленный запрос, варьируется от 1 до 86400.
TTL maximum value	Определяет максимальное значение для поля "время использования" (TTL) в заголовке IPv4. Тестирование прекращается, если указанный удаленный хост достигнут до достижения этого значения. Число по умолчанию - 30. Допустимый диапазон - от 1 до 255.
Source port VLAN ID	Идентификатор VLAN исходного порта. Это поле может использоваться для принудительного использования теста определенного интерфейса с нативным VLAN в качестве исходного интерфейса. Оставьте это поле пустым для автоматического выбора на основе конфигурации маршрутизации. Диапазон - от 1 до 4095.
Source IP	IP-адрес исходного порта.
Output IP address	По умолчанию команда traceroute будет выводить информацию о ХОП для полученного IP-адреса хоста с использованием обратного DNS-поиска. Если информация DNS недоступна, это может замедлить отображение. Выбор этой опции предотвратит обратные DNS-поиски и принудит команду traceroute выводить числовые IP-адреса.

**Примечание:**

Требуемая информация включает IP-адрес или доменное имя, значение DSCP, количество попыток для каждого хопа, тайм-аут ответа и максимальное значение TTL.

## 8.5 PTP (Precision Time Protocol) синхронизация времени

### Определение

При настройке PTP для достижения синхронизации времени, сначала необходимо обеспечить синхронизацию частоты по всей сети. Синхронизацию частоты можно достичь, настроив функцию синхронизации Ethernet-часов. В этой главе конфигурация сосредоточена исключительно на синхронизации времени PTP. По умолчанию пакет PTP является многоадресным пакетом уровня 2, который обладает характеристиками многоадресных пакетов. Если он настроен неправильно, это может вызвать петли или штормы, серьезно влияя на нижестоящие устройства. Перед настройкой и включением порта PTP настройте VLAN или STP, чтобы предотвратить штормы или петли.

По умолчанию метод синхронизации устройства следующий: получение частотного сигнала через синхронный Ethernet и получение временного сигнала через PTP..

### ВМС алгоритм

В домене PTP выбор оптимальных часов и установление мастер-слейв отношений между портами осуществляется с помощью алгоритма ВМС оптимальных часов.

Алгоритм ВМС сравнивает наборы данных, передаваемые в сообщениях Announce между узлами синхронизации, чтобы выбрать оптимальные часы и определить состояние каждого порта PTP.

Набор данных, используемый алгоритмом ВМС для выбора оптимальных часов и определения статуса порта PTP, включает следующую информацию:

- ◆ **Приоритет1:** Приоритет часов 1, поддерживает пользовательскую конфигурацию, диапазон значений от 0 до 255, чем меньше значение, тем выше приоритет.
- ◆ **КлассЧасов:** Уровень часов, который определяет способность к отслеживанию времени или частоты по международному атомному времени (TAI).
- ◆ **ТочностьЧасов:** Точность часов. Чем ниже значение, тем выше точность.
- ◆ **ОтклонениеШкалированнаяЛогВариация:** Стабильность часов.
- ◆ **Приоритет2:** Приоритет часов 2, поддерживает пользовательскую конфигурацию, диапазон значений от 0 до 255, чем меньше значение, тем выше приоритет.

Когда устройство PTP выполняет динамический алгоритм выбора источника ВМС, порядок приоритетного выбора определяется следующим образом:  $\text{Приоритет1} > \text{КлассЧасов} > \text{ТочностьЧасов} > \text{ОтклонениеШкалированнаяЛогВариация} > \text{Приоритет2}$ , то есть сначала сравнивается приоритет1 выбранного источника времени, и если приоритет1 одинаков, сравнивается класс часов, и так далее. Часы с высоким приоритетом, высоким уровнем и хорошей точностью становятся оптимальными часами.

Изменяя приоритет, уровень и другие атрибуты часов, пользователи могут влиять на выбор основных часов системы PTP, тем самым выбирая часовой сигнал, который они хотят синхронизировать. Алгоритм ВМС позволяет реализовать распределение и защиту синхронизации часов PTP.

### Синхронизация частоты PTP:

После установления мастер-слейв отношений можно выполнять синхронизацию частоты и времени. PTP изначально предназначен только для высокоточной синхронизации времени между устройствами пользователей, но также может быть использован для синхронизации частоты между устройствами.

PTP записывает отметки времени, генерируемые при обмене сообщениями событий между устройствами-мастером и устройствами-слейвами, вычисляет задержку пути и временное смещение между устройствами-мастером и устройствами-слейвами, и достигает синхронизации

времени и частоты между ними. Устройство поддерживает два режима передачи отметок времени, которые представлены:

- Режим одношаговых часов (Onestep) означает, что сообщения событий Sync и Pdelay\_Resp содержат отметку времени отправки этого сообщения. Оповещение о временной информации также завершается при отправке и получении сообщения.
- 
- Режим двухшаговых часов (Twostep) означает, что сообщения событий Sync и Pdelay\_Resp не содержат отметку времени отправки этого сообщения, но последующие общие сообщения Follow\_Up и Pdelay\_Resp\_Follow\_Up содержат информацию о времени отправки сообщений Sync и Pdelay\_Resp соответственно. В режиме двухшаговых часов генерация и оповещение временной информации завершаются в два этапа, что может быть совместимо с некоторыми устройствами, которые не поддерживают отметки времени для пакетов событий.

### Синхронизация времени:

Синхронизация времени PTP имеет два различных метода синхронизации: режим задержки и режим Pdelay. Это разделение в основном обусловлено тем, что у PTP есть два механизма расчета задержки пути.

- Механизм запроса-ответа с задержкой E2E (EndtoEnd): рассчитывает разницу во времени на основе общего времени задержки пути между часами мастера и часами слейва. Соответствует методу синхронизации времени Delay.
- Механизм пиринговой задержки P2P (PeertoPeer): рассчитывает разницу во времени на основе времени задержки каждого звена между часами мастера и часами слейва. Соответствует методу синхронизации времени PDelay.

## 8.5.1 Руководство по настройке PTP



Примечание:

Для настройки функции синхронизации времени PTP в веб-интерфейсе вам нужно будет настроить только необходимые параметры в соответствии со следующими шагами. Другие конфигурации не требуется изменять. Большинство настроек по умолчанию выполняется при выборе файла предварительной настройки в веб-интерфейсе.

Добавьте источник времени PTP. Тип устройства можно выбрать субъективно: мастер-часы или слейв-часы, или выбрать общие часы и выбрать мастер-часы и слейв-часы с помощью алгоритма VMC (уровень часов, точность, приоритет и т. д.).

### 8.5.1.1 Конфигурация внешнего источника синхронизации

Интерфейс отображения режима внешнего источника синхронизации.

**PTP External Clock Mode**

<b>One_PPS_Mode</b>	Output <span style="float: right;">▼</span>
<b>Adjust Method</b>	Auto <span style="float: right;">▼</span>

Описание каждого параметра представлено в следующей таблице

Параметр	Описание
1PPS mode	Режим ввода и вывода сигнала импульса 1PPS.
Calibration method	Режим калибровки: АВТО или LTC (локальный подсчет времени).

### 8.5.1.2 Настройка часов PTP

1. В интерфейсе отображения конфигурации часов PTP, добавьте новые часы PTP и нажмите кнопку "Добавить часы PTP", чтобы завершить настройку часов PTP.

**PTP Clock Configuration**

Delete	Clock Instance	HW Domain	VID	Device Type	Profile
	No Clock				
	Instances				
	Present				

Интерфейс отображения создания часов PTP:

**PTP Clock Configuration**

Delete	Clock Instance	HW Domain	VID	Device Type	Profile
<input checked="" type="checkbox"/>	0	0	1	Ord-Bound	802.1AS

Описание каждого параметра представлено в следующей таблице

Параметр	Описание
Delete	Под созданными часами PTP установите флажок "Удалить" и нажмите "Сохранить", чтобы удалить текущие часы PTP.
Clock instance	Экземпляр часов, диапазон 02, значение по умолчанию 0.
Hardware clock domain	Домен часов PTP, диапазон 02, значение по умолчанию 0.
Vlan ID	ID VLAN, диапазон 0~4095. Параметр 0 будет автоматически адаптирован.
Equipment type	Тип устройства, Ord-Bound/E2eTransp/P2pTransp/mastronly/slaveonly.
Profile	Предустановленные файлы включают 1588 и 802.1AS. Параметры по умолчанию каждого предустановленного файла различаются. Выберите предустановленный файл в соответствии с фактическим применением.

2. На интерфейсе отображения настройки часов PTP щелкните по номеру экземпляра часов, чтобы войти в интерфейс настройки часов.

**PTP Clock's Configuration and Status**

**Clock Type and Profile**

Clock Instance	HW Domain	Device Type	Profile	Apply Profile Defaults	Filter Type
0	0	Ord-Bound	802.1AS	<input type="button" value="Apply"/>	BASIC

**Port Enable and Configuration**

Port Enable																																				Configuration	
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	<b>Ports</b>	
<input type="checkbox"/>	<b>Configuration</b>																																				

Описание каждого параметра представлено в следующей таблице:

Параметр	Описание
Filter type	Тип фильтра: ACI_BASIC_PHASE, ACI_BASIC_PHASE_LOW, BASIC. Дополнительные сведения см. в приложении А.
Port enable	Порт часов включен, выбраны порты мастера и слейва PTP

3. Интерфейс таблицы данных часов по умолчанию выглядит следующим образом:

**Clock Default DataSet**

Device Type	One-Way	2 Step Flag	Ports	Clock Identity	Dom	Clock Quality
Ord-Bound	False	True	36	20:c7:92:ff:fe:a0:02:2b	0	Cl:248 Ac:Unknwn Va:17258
Pri1	Pri2	Local Prio	Protocol		PCP	DSCP
246	248	128	Ethernet		0	0

Описание каждого параметра представлено в следующей таблице

Параметр	Описание
One Way	Выберите значение true, если текущий режим - односторонний; выберите значение false, если текущий режим - двусторонний, и сообщения с задержкой не отправляются в одностороннем режиме.
Two Step	Условия для непосылки сообщений с задержкой: 1. Односторонний, 2. Не E2E, 3. Не BC, только слейв.
Clock domain	Выберите значение true, если текущий режим - двухшаговый; выберите значение false, если текущий режим - одношаговый.
Priority 1	Домен часов, диапазон 0127.
Priority 2	Приоритет 1, участвует в выборах мастера и слейва, диапазон 0-255.
Local priority	Приоритет 2, участвует в выборах мастера и слейва, диапазон 0-255.
Agreement type	Локальный приоритет, участвует в выборах мастера и слейва, диапазон 0-255.
PCP	Протокол сетевого транспорта, Ethernet/EthnertMixed/IPV4Multi/IPv4Mixed/IPv4Uni/onePPS/EthIPv4IPV6combo.
DSCP	Приоритет PCP, диапазон от 0 до 7.

 **Примечание:**  
802.1AS не поддерживает режим TC, только мастер, только режим слейва.

802.1AS не поддерживает режим одношаговой синхронизации.

802.1AS поддерживает только передачу Ethernet.

Включение порта PTP, порт физического уровня не поддерживается для не-0 домена часов.

4. Интерфейс локальной синхронизации времени выглядит следующим образом:

Local Clock Current Time		
PTP Time	Clock Adjustment method	
2023-12-12T10:11:07+08:00 752,643,390	Internal Timer	Synchronize to System Clock

Описание каждого параметра представлено в следующей таблице:

Параметр	Описание
Synchronize system time	Synchronize system time to PTP time
Synchronize to system time	Synchronize PTP time to system time. Only time synchronization of clock instance 0 is supported.

5. Интерфейс текущего набора данных часов выглядит следующим образом:

Clock Current DataSet		
stpRm	Offset From Master	Mean Path Delay
1	0.000,000,000,000	0.000,000,000,000

Clock Parent DataSet								
Parent Port ID	Port	PStat	Var	Rate	GrandMaster ID	GrandMaster Clock Quality	Pri1	Pri2
20:c7:92:ff:fe:a0:01:bc	7	False	0	0	20:c7:92:ff:fe:a0:01:bc	Cl:248 Ac:Unknwn Va:17258	200	248

Описание каждого параметра представлено в следующей таблице

Параметр	Описание
Master clock bias	Значение смещения основных часов
Average path delay	Задержка пути
Parent clock ID	Идентификатор родительского узла (предыдущий узел)
Ancestor clock ID	Идентификатор предка часов
Ancestral clock quality	Качество предка часов (ранг, точность, вариация)

6. Интерфейс отображения конфигурации порта часов PTP:

PTP Clock's Port Data Set Configuration																	
Port	Stat	MDR	PeerMeanPathDel	Anv	Ato	Syv	Dlm	MPR	Delay Asymmetry	Ingress Latency	Egress Latency	Version	Mcast Addr	Not Slave	Local Prio	2 Step Flag	Not Master
7	slve	0	0.000,000,003,632	0	3	-3	p2p	0	0	0	0	2	Link-local	False	128	Clock Def	False

Описание каждого параметра представлено в следующей таблице

Параметр	Описание
Announce interval	Интервал объявлений, время $t$ , 2 в степени $t$ , например, $t=1$ , то это 2 секунды, $t=-1$ , то это 0.5 секунды, диапазон $t$ от -3 до 5.
Announce timeout	Время ожидания объявлений, время $t$ , 2 в степени $t$ , например, $t=1$ , то это 2 секунды, $t=-1$ , то это 0.5 секунды, диапазон $t$ от 1 до 10.
Sync interval	Интервал синхронизации, время $t$ , 2 в степени $t$ , например, $t=1$ , то это 2 секунды, $t=-1$ , то это 0.5 секунды, диапазон $t$ от -7 до 4.

Параметр	Описание
Delay mechanism	Настройка механизма задержки, p2p, e2e.
Request message interval	Интервал запроса задержки/задержки, время t, 2 в степени t, например, t=1, то это 2 секунды, t=-1, то это 0.5 секунды, диапазон t от -7 до 5.
Delay asymmetry	Асимметричное время задержки порта, единица измерения нс, диапазон -100000100000.
Entrance delay	Значение компенсации задержки на входе порта, единица измерения нс, диапазон -100000100000.
Exit delay	Значение компенсации задержки на выходе порта, единица измерения нс, диапазон -100000100000.
Multicast address	Многоадресный адрес, значение по умолчанию.
Non-slave clock	Не слейв-часы, значение по умолчанию false.
Local priority	Локальный приоритет, диапазон 0255, значение по умолчанию 128.
Two steps	Двухшаговая синхронизация, значение по умолчанию часы def.
Non-master clock	Не основные часы, значение по умолчанию false.
MDR	Среднее время задержки запросов.

### 7. Конфигурация фильтра BASIC

**Basic Filter Parameters**

Delay Filter	Period	Dist
6	1	2

**Basic Servo Parameters**

Display	P-enable	I-enable	D-enable	'P' constant	'I' constant	'D' constant	Gain constant
False	True	True	True	3	30	40	1

Описание каждого параметра представлено в следующей таблице

Параметр	Описание
Delayed filtering	Параметры фильтра задержки, диапазон 0-6.
Cycle	Период фильтра, диапазон 1-10000.
Hop count	Расстояние, диапазон 0-10.
Show	В отладочном терминале отображаются offsetFromMaster, meanPathDelay и clockAdjust.
P-enable	Включение пропорциональной составляющей, true/false, см. алгоритм сервопривода PID.
I-enable	Включение дифференциальной составляющей, true/false, см. алгоритм сервопривода PID.
D-enable	Включение интегральной составляющей, true/false, см. алгоритм сервопривода PID.
P-constant	Пропорциональная константа, диапазон 1-1000, см. алгоритм сервопривода PID.
I-constant	Дифференциальная константа, диапазон 1-10000, см. алгоритм сервопривода PID.
D-constant	Интегральная константа, диапазон 1-10000, см. алгоритм сервопривода PID.

Параметр	Описание
Gain constant	Константа коэффициента усиления, диапазон 1-10000, см. алгоритм сервопривода PID.

### 8. Конфигурация набора данных порта 802.1AS

802.1AS Port Data Set Configuration														
Port	Port Role	IsMeasDelay	As Capable	Neighbor rate ratio	CAnv	CSyv	SyncTimeIntrvl	CMPR	AMTE	Version Number	NPDT	SRT	ALR	AFs
7	Slave	True	True	-21221917	0	-3	0.375,000,000,000	0	FALSE	2	800	3	9	9

Port	useMgmtSync	SyncIntrvl	useMgmtAnnounce	AnnounceIntrvl	useMgmtPdelay	PdelayIntrvl	uMSCNRR	MSCNRR	uMSCMLD	MSCMLD
7	<input type="checkbox"/>	-3	<input type="checkbox"/>	0	<input type="checkbox"/>	0	<input type="checkbox"/>	True	<input type="checkbox"/>	True

Port	useMgmtGtpCapIntrvl	MgmtGtpCapIntrvl	GtpCapableReceiptTimeout	initialLogGtpCapableMessageInterval
7	<input type="checkbox"/>	3	3	3

Описание каждого параметра представлено в следующей таблице

Параметр	Описание
NPDT	Средний порог задержки, диапазон 0-4000000000 нс.
Sync receive timeout	Диапазон 1-255.
Number of lost responses allowed	Диапазон 0-10.
Number of faults allowed	Диапазон 1-255.
Sync interval	Диапазон -74.
Announce interval	Диапазон -34.
Pdelay interval	Диапазон -75.
Gtp interval	Диапазон -2424.
Gtp receive timeout	Диапазон 1~255.
Initialize Gtp interval	Не поддерживается.

### 9. Конфигурация специфического порта обслуживания общей задержки 802.1AS

802.1AS Common Link Delay Services Specific Port Data Configuration													
Port	MLDT	DA	iLPDRv	uMSLPDRv	MSLPDRv	iCNRR	cm_uMSCNRR	cm_MSCNRR	iCMLD	cm_uMSCMLD	cm_MSCMLD	cm_ALR	cm_Afs
7	800	0	0	<input type="checkbox"/>	0	True	<input type="checkbox"/>	True	True	<input type="checkbox"/>	True	9	9

Описание каждого параметра представлено в следующей таблице

Параметр	Описание
Average delay threshold	Средний порог задержки, диапазон 0-4000000000 нс.
Delay asymmetry	Диапазон -100000100000.
Delay request interval	Диапазон -75.
Number of lost responses allowed	Диапазон 010.
Number of faults allowed	Диапазон 1255.

#### 8.5.1.3 PTP статус

Интерфейс отображения статуса PTP:

PTP Clock's Configuration															
Clock Type and Profile															
Clock Instance	HW Domain	Device Type	Profile	Filter Type		Filter Mode									
0	0	Ord-Bound	802.1AS	BASIC		PACKET									
Local Clock Current Time															
PTP Time		Clock Adjustment method		Ports Monitor Page											
2023-12-12T10:19:37+08:00		116,065,645		Internal Timer		Ports Monitor									
Clock Default DataSet															
Device Type	One-Way	2 Step Flag	Ports	Clock Identity	Dom	Clock Quality	Pri1	Pri2	Local Prio	Protocol	VID	PCP	DSCP	GM Capable	sdold
Ord-Bound	False	True	36	20:c7:92:ff:fe:a0:02:2b	0	Cl:248 Ac:Unknwn Va:17258	246	248	128	Ethernet	1	0	0	True	0x100
Clock Current DataSet															
stpRm	Offset From Master	Mean Path Delay	Last GM Ph Change	Last GM FR Change	GM time base	GM change count	Last GM Change Event	Last GM Phase Change Event	Last GM Freq Change Event	Slave Port	Slave State	Holdover(ppb)			
1	-0.000,045,490,619	0.000,000,000,000	0.000,000,000	1.000000	0	1	418001	418001	418013	7	PHASE_LOCKING	N.A.			
Clock Parent DataSet															
Parent Port ID	port	PStat	Var	Rate	GrandMaster ID	GrandMaster Clock Quality	Pri1	Pri2	CRR						
20:c7:92:ff:fe:a0:01:bc	7	False	0	-8435	20:c7:92:ff:fe:a0:01:bc	Cl:248 Ac:Unknwn Va:17258	200	248	7761682						

Описание каждого параметра представлено в следующей таблице

Параметр	Описание
Clock instance	Экземпляр часов.
Hardware clock domain	Область аппаратных часов.
Equipment type	Тип устройства, включая мастер-часы, слейв-часы, граничные часы, прозрачные часы и т. д.
Profile	Предустановленные файлы, параметры по умолчанию каждого предустановленного файла отличаются, выберите предустановленный файл в соответствии с фактическим применением.
Filter type	Тип фильтра, ACI_BASIC_PHASE, ACI_BASIC_PHASE_LOW, BASIC.
Filter mode	Режим фильтрации.
PTP time	Время PTP.
Time calibration method	Метод калибровки времени.
One way	Односторонняя синхронизация.
Two steps	Двухшаговая синхронизация.
Clock ID	Идентификатор часов.
Clock domain	Домен часов.
Clock quality	Качество часов.
Priority 1	Приоритет 1.
Priority 2	Приоритет 2.
Local priority	Локальный приоритет.
Agreement type	Тип соглашения.
PCP	Приоритет PCP.
DSCP	Приоритет DSCP.
GM capable	Способность к GM (главному мастеру).
Sdold	Sdold.
Wxya	Удаление шагов.

Параметр	Описание
Offset From Master	Смещение.
Mean Path Delay	E2E задержка, PTP равна 0.
Last GM ph change	Последнее изменение фазы GM (главного мастера).
GM time Base	Базовое время GM (главного мастера).
GM change count	Счетчик изменений GM (главного мастера).
Last GM change event	Время изменения GM (главного мастера).
Last GM phase change event	Время изменения фазы GM (главного мастера).
Last GM freq change event	Время изменения частоты GM (главного мастера).
Slave state	Статус слейв-часов.
Hold over	Резервирование.
Parent clock ID	Идентификатор родительского часов.
Pstat	Статус родительского часов.
Variance	Дисперсия.
Rate	Скорость.
Ancestor clock ID	Идентификатор предка часов.
Ancestral clock quality	Качество предка часов.
CRR	Скорость накопления.

### 8.5.1.4 802.1AS статистика

Интерфейс отображения статистики 802.1AS:

802.1AS Clock Instance Specific Statistics																	Clock Instance 0	Auto-refresh	Refresh	Delete
Port	Sync Count		FollowUp Count		Pdelay Request Count		Pdelay Response Count		Pdelay Response FollowUp Count		Announce Count		PTP Packet Discard Count	Sync Receipt Timeout	Announce Receipt Timeout	Pdelay Allowed Lost Responses Exceeded Count				
	Rx	TX	Rx	TX	Rx	TX	Rx	TX	Rx	TX	Rx	TX		Count	Count					
	1	0	0	0	0	0	0	0	0	0	0	0		0	0		0	0	0	
2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0				
3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0				
4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0				
5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0				
6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0				
7	28222	0	28222	0	3516	3516	3237	3239	3236	3236	3754	0	0	0	0	0				
8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0				
9	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0				
10	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0				
11	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0				
12	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0				

Описание каждого параметра представлено в следующей таблице

Параметр	Описание
SyncCount	Количество пакетов Sync
FollowUpCount	Количество пакетов FollowUp
PdelayRequestCount	Количество сообщений PdelayRequest

Параметр	Описание
PdelayResponseCount	Количество сообщений PdelayResponse
PdelayResponseFollowUpCount	Количество сообщений PdelayResponseFollowUp
AnnounceCount	Количество сообщений Announce
PTPPacketDiscardCount	Количество отброшенных пакетов PTP
syncReceiptTimeoutCount	Количество таймаутов приема синхронизации
announceReceiptTimeoutCount	Количество таймаутов приема объявлений
pdelayAllowedLostResponsesExceededCount	Количество превышений допустимого количества потерянных ответов на Pdelay

### 8.5.2 Пример конфигурации PTP

#### 8.5.2.1 Конфигурация предустановленного файла 1588

1. Конфигурация внешнего источника синхронизации: Внешний источник может быть настроен с использованием 1pps, локальных часов и других настроек.

**PTP External Clock Mode**

**One\_PPS\_Mode**

**Adjust Method**

- Добавьте источник часов PTP, выберите "Mastronly" в качестве типа устройства и установите предустановленный файл на "1588".

**PTP Clock Configuration**

Delete	Clock Instance	HW Domain	VID	Device Type	Profile
<input type="checkbox"/>	0	0	1	Ord-Bound	802.1AS

- Настройте экземпляр часов:
  - a. Выберите тип фильтра ACI\_BASIC\_PHASE\_LOW, и в зависимости от ваших потребностей вы можете выбрать другие параметры.

**Clock Type and Profile**

Clock Instance	HW Domain	Device Type	Profile	Apply Profile Defaults	Filter Type
0	0	Ord-Bound	802.1AS	<input type="button" value="Apply"/>	BASIC

- b. Выберите порт, соединяющий устройства мастер-часов и слейв-часов.

Port Enable and Configuration																																					
Port Enable																																			Configuration		
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	<b>Ports</b>	
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<b>Configuration</b>																													

2. Конфигурация часов-слейв

- Настройте внешние часы: Режим One\_PPS установлен на Выход.

### PTP External Clock Mode

<b>One_PPS_Mode</b>	Output <span style="float: right;">▼</span>
<b>Adjust Method</b>	Auto <span style="float: right;">▼</span>

- Добавьте источник часов PTP, выберите "slaveonly" или "Ord-Bound" в качестве типа устройства и установите предустановленный файл на "1588".

### PTP Clock Configuration

Delete	Clock Instance	HW Domain	VID	Device Type	Profile
<input type="checkbox"/>	0	0	1	Ord-Bound	802.1AS

Add New PTP Clock Save Reset

- Настройте экземпляр часов:
  - a. Выберите тип фильтра ACI\_BASIC\_PHASE\_LOW. Вы можете выбрать другие параметры в соответствии с вашими потребностями. Основные часы остаются неизменными.

### Clock Type and Profile

Clock Instance	HW Domain	Device Type	Profile	Apply Profile Defaults	Filter Type
0	0	Ord-Bound	802.1AS	<span>Apply</span>	BASIC <span style="float: right;">▼</span>

- b. Выберите порт, соединяющий устройства мастер-часов и слейв-часов.

Port Enable and Configuration																																				
Port Enable																																			Configuration	
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	<b>Ports</b>
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<b>Configuration</b>																												

3. Проверьте результат синхронизации часов-слейв по протоколу PTP:

- Состояние слейв отображается как PHASE\_LOCKED или FREQ\_LOCKED.
- offset from master отображает коррекцию значения частотной синхронизации.
- Mean path delay отображает задержку пути.
- Идентификатор родительского часов отображается как ID верхнего уровня.
- Идентификатор предка часов отображается как идентификатор предка.

PTP Clock's Configuration Auto-refresh  Refresh

**Clock Type and Profile**

Clock Instance	HW Domain	Device Type	Profile	Filter Type	Filter Mode
0	0	Ord-Bound	802.1AS	BASIC	PACKET

**Local Clock Current Time**

PTP Time	Clock Adjustment method	Ports Monitor Page
2023-12-12T10:24:26+08:00 285,287,674	Internal Timer	<a href="#">Ports Monitor</a>

**Clock Default DataSet**

Device Type	One-Way	2 Step Flag	Ports	Clock Identity	Dom	Clock Quality	Pri1	Pri2	Local Prio	Protocol	VID	PCP	DSCP	GM Capable	sdold
Ord-Bound	False	True	36	20:c7:92:ff:fea0:02:2b	0	Cl:248 Ac:Unknwn Va:17258	246	248	128	Ethernet	1	0	0	True	0x100

**Clock Current DataSet**

stpRm	Offset From Master	Mean Path Delay	Last GM Ph Change	Last GM FR Change	GM time base	GM change count	Last GM Change Event	Last GM Phase Change Event	Last GM Freq Change Event	Slave Port	Slave State	Holdover(ppb)
1	-0.026,280,722,126	0.000,000,000,000	0.000,000,000	1.000000	0	1	418001	418001	418013	7	PHASE_LOCKING	N.A.

**Clock Parent DataSet**

Parent Port ID	port	PStat	Var	Rate	GrandMaster ID	GrandMaster Clock Quality	Pri1	Pri2	CRR
20:c7:92:ff:fea0:01:bc	7	False	0	3470	20:c7:92:ff:fea0:01:bc	Cl:248 Ac:Unknwn Va:17258	200	248	-13115514

### 8.5.2.2 Конфигурация предустановленного файла 802.1AS

#### 1. Конфигурация основных часов:

- Настройте внешние часы: Режим One\_PPS установлен на Выход.

**PTP External Clock Mode**

**One\_PPS\_Mode**

**Adjust Method**

- обавьте источник часов PTP, выберите "Ord-Bound" в качестве типа устройства и установите предустановленный файл на "802.1AS"

**PTP Clock Configuration**

Delete	Clock Instance	HW Domain	VID	Device Type	Profile
<input type="checkbox"/>	0	0	1	Ord-Bound	802.1AS

- Настройте экземпляр часов:

#### a. Выберите тип фильтра BASIC.

**Clock Type and Profile**

Clock Instance	HW Domain	Device Type	Profile	Apply Profile Defaults	Filter Type
0	0	Ord-Bound	802.1AS	<input type="button" value="Apply"/>	BASIC <input type="text"/>

#### b. Выберите порт, соединяющий устройства мастер-часов и слейв-часов

**Port Enable and Configuration**

Port Enable																																				Configuration
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	<b>Ports</b>
<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<b>Configuration</b>																																	

с. Конфигурация приоритета: обычно приоритет мастер-часов меньше 128, а приоритет слейв-часов больше 128.

Clock Default DataSet						
Device Type	One-Way	2 Step Flag	Ports	Clock Identity	Dom	Clock Quality
Ord-Bound	False	True	36	20:c7:92:ff:fe:a0:02:2b	0	Cl:248 Ac:Unknwn Va:17258
Pri1	Pri2	Local Prio	Protocol	PCP	DSCP	
246	248	128	Ethernet	0	0	

д. Другие конфигурации не требуют изменений. Большая часть конфигурации по умолчанию выполнена при выборе предустановленного файла через веб-интерфейс.

2. Конфигурация часов-слейва

◆ Настройка внешнего источника времени: режим One\_PPS установлен на Выход.

PTP External Clock Mode	
One_PPS_Mode	Output
Adjust Method	Auto

◆ Добавьте источник часов PTP, выберите тип устройства "Ord-Bound" и установите предустановленный файл на "802.1AS".

PTP Clock Configuration					
Delete	Clock Instance	HW Domain	VID	Device Type	Profile
<input type="checkbox"/>	0	0	1	Ord-Bound	802.1AS

Add New PTP Clock Save Reset

◆ Настройте экземпляр часов:

а. Выберите тип фильтра BASIC.

Clock Type and Profile					
Clock Instance	HW Domain	Device Type	Profile	Apply Profile Defaults	Filter Type
0	0	Ord-Bound	802.1AS	Apply	BASIC

б. Выберите порт, соединяющий устройства мастер-часов и слейв-часов.

Port Enable and Configuration																																					
Port Enable																																				Configuration	
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	<b>Ports</b>	
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<b>Configuration</b>																													

с. Другие конфигурации не требуют изменений. Большая часть работы по настройке по умолчанию была выполнена при выборе предустановленного файла через веб-интерфейс.

3. Проверьте результат синхронизации часов-слейва по протоколу PTP:

- ◆ Состояние слейва отображается как PHASE\_LOCKED.
- ◆ Смещение от мастера отображается в значениях ns.
- ◆ Идентификатор родительского часов отображается как ID верхнего уровня.
- ◆ Идентификатор предка часов отображается как идентификатор предка.

## 8.6 TSN

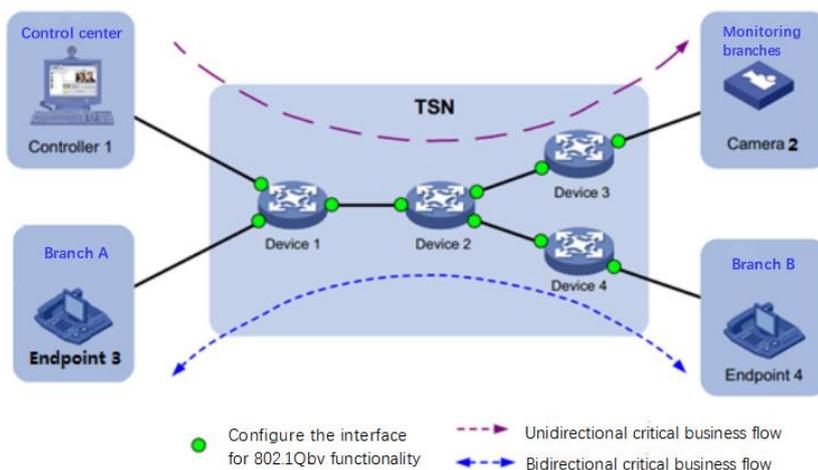
### 8.6.1 Определение

TSN (Time Sensitive Networking) - это стандарт сети нового поколения, основанный на Ethernet. Он предоставляет универсальный механизм, чувствительный к времени, для уровня MAC протокола Ethernet с целью достижения низкой задержки, высокой надежности и детерминированной передачи ключевых данных, таких как голос, видео и инструкции промышленной автоматизации в сети Ethernet. Стандарт TSN включает в себя в основном синхронизацию часов, контроль потока, надежность, безопасность и другие компоненты.

Основываясь на ключевых сервисах, работающих в сети, пользователь анализирует характеристики потока и время выполнения этих ключевых сервисов, использует функцию 802.1Qbv для разрешения определенных ключевых сервисов входить в определенную очередь передачи интерфейса, а затем гибко и периодически планирует эти очереди для реализации пересылки устройства. Для этих бизнес-критичных трафиков отсутствует перегрузка и потеря пакетов. Развертывание функции 802.1Qbv по всей сети TSN для контроля задержки пересылки ключевого бизнес-трафика на уровне микросекунд при прохождении через сеть TSN.

### 8.6.2 802.1Qbv

Как показано на рисунке ниже, Контроллер 1 должен отправить инструкции к Камере2 для управления параметрами включения и выключения Камеры2. Инструкции, выданные Контроллером 1, должны проходить через Ethernet, чтобы достичь Камеры2; важная видеоконференция проводится между Конечной точкой 3 и Конечной точкой 4, двусторонние видеопотоки имеют высокие требования к задержке сети и джиттеру задержки. Ethernet имеет риск неопределенности задержки и даже перегрузки и потери пакетов. Функция 802.1Qbv развернута на Устройстве 1, Устройстве 2, Устройстве 3 и Устройстве 4, где потоки сопоставляются по входному интерфейсу, а планирование очередей и пересылка пакетов выполняются на исходящем интерфейсе. Она может контролировать задержку ключевых бизнес-потоков от отправителя к получателю в пределах микросекундного уровня, обеспечивая важную гарантию для реального времени передачи между точками на сети.



### 1. Очередь пересылки

Для предотвращения потери пакетов, вызванной перегрузкой сети, интерфейсный чип использует очередь пересылки для отправки пакетов. Каждый интерфейс имеет 8 очередей пересылки, с номерами очередей от 0 до 7. Когда интерфейсу нужно отправить пакет, он сначала попадает в соответствующую очередь в соответствии с определенными правилами. Для пакетов в одной и той же очереди сначала отправляется тот пакет, который пришел первым.

### 2. Поток TSN

Потоки TSN (Time-Sensitive Networking) - это ключевые бизнес-потоки, требующие детерминированной передачи в сети TSN. После получения пакета интерфейс определяет, является ли трафик потоком TSN на основе характеристик потока. Параметры характеристик потока включают в себя исходный MAC-адрес, MAC-адрес назначения, идентификатор VLAN и т. д. в пакете. Чем больше параметров указано, тем более точное совпадение.

### 3. Список управления 802.1Qbv

Список управления расписанием пересылки потоков TSN используется для реализации планирования очереди пересылки интерфейса и пересылки пакетов.

Список управления 802.1Qbv содержит до 256 узлов. Узел - это логическое понятие. Каждый узел определяет три атрибута. Через эти три атрибута выполняется операция выполнения узла:

- Номер узла: В контрольном связанном списке может быть определено до 256 узлов, и соответствующие номера узлов - от 0 до 255. Планирование 802.1Qbv выполняется в порядке номеров узлов от меньшего к большему.
- Статус переключения очереди: Состояние переключения очереди пересылки интерфейса представлено в виде 8-битной двоичной строки (XXXXXXXX). Справа налево, первая цифра справа представляет состояние переключения очереди 0, вторая цифра справа представляет состояние переключения очереди 1 и так далее. Когда бит имеет значение 0, это означает отключено, то есть сообщения в очереди не могут быть отправлены; когда бит имеет значение 1, это означает включено, то есть сообщения в очереди могут быть отправлены.

Q0	Q1	Q2	Q3	Q4	Q5	Q6	Q7
0/1	0/1	0/1	0/1	0/1	0/1	0/1	0/1

Queue0 Queue1 Queue2 Queue3 Queue4 Queue5 Queue6 Queue7

0:Indicates that it is enabled and allows the queue to send messages

1:Indicates that the queue is closed and not allowed to send messages

- Продолжительность состояния переключения: это время, в течение которого интерфейсная очередь пересылки находится в состоянии переключения в данном узле. По истечении этого времени выполнение переходит к следующему узлу и переходит к состоянию переключения очереди следующего узла.

#### 4. Зона защиты

Защитная полоса 802.1Qbv - это буферная полоса между двумя узлами в контрольном списке планирования пересылки потоков TSN. Каждые 8 бит составляют 1 байт. Несколько байт формируют кадр данных. Ethernet передает данные в кадрах. Защитная полоса используется для обеспечения того, что устройство может полностью передать текущий кадр данных в момент планирования очереди пересылки 802.1Qbv. Например, когда интерфейс передает характеристический поток 802.1Qbv, передается половина кадра данных, и достигается продолжительность состояния переключения очереди. В этот момент:

- Если функция защитной полосы 802.1Qbv выключена, то 802.1Qbv немедленно выполнит следующий узел. Содержимое текущего кадра данных будет усечено, и оставшееся содержимое может быть отброшено или может потребоваться ожидание до следующего цикла опроса, прежде чем оно сможет быть отправлено.
- Если функция защитной полосы 802.1Qbv включена, то 802.1Qbv отправит оставшуюся часть кадра данных перед выполнением следующего узла.

#### 5. Время цикла

802.1Qbv выполняет связанный список управления периодически, и время цикла - это длительность времени, необходимая системе для выполнения связанного списка управления один раз. Когда 802.1Qbv начинает выполнение первого узла, начинается отсчет времени и выполняется список управления по порядку. По достижении времени цикла список управления автоматически выполняется снова с первого узла.

#### 6. Базовое время

Время, когда интерфейс начинает выполнение политики планирования очереди пересылки 802.1Qbv.

Базовое время используется для вычисления времени выполнения алгоритма планирования устройством. Например, если пользователь планирует начать выполнение алгоритма планирования 802.1Qbv в 12:00:00 18 марта 2020 года, ему необходимо сначала вычислить разницу времени между этим временем и 00:00:00 1 января 1970 года и преобразовать ее в формат времени PTP (секунды в ганские секунды), настроив с использованием преобразованных секунд и наносекунд.

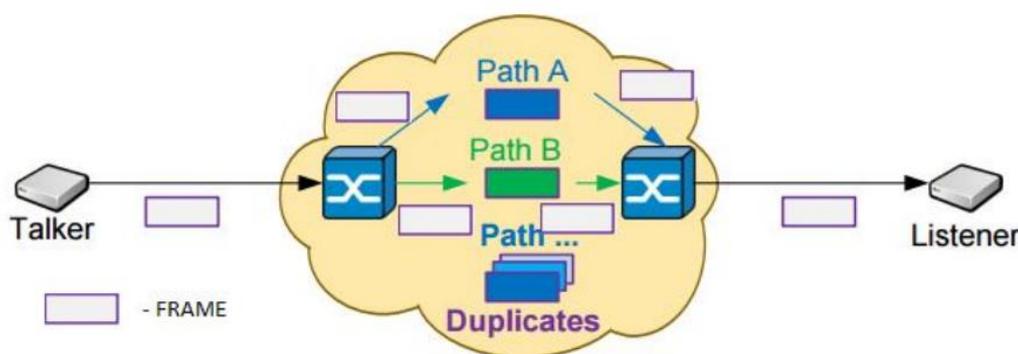
Для достижения детерминированной передачи потоков TSN все устройства TSN в сети TSN должны работать вместе, то есть каждое устройство TSN разрешает проход потока TSN в одинаковый момент времени (соответствующий базовому времени), а продолжительность времени, разрешенная для прохода (соответствующая продолжительности состояния переключения), одинакова, требуется точность времени до наносекундного уровня. Исходя из этого требования, все устройства TSN должны использовать технологию PTP для достижения

временной синхронизации перед передачей потоков TSN. Существует несколько протоколов, которые могут обеспечить синхронизацию времени по протоколу PTP. В среде сетевой организации TSN рекомендуется использовать протокол IEEE 802.1AS.

### 8.6.3 802.1CB

Для очень важных данных 802.1CB отправит дополнительное резервное копирование данных, которое будет передаваться по пути, наиболее удаленному от пересечения основных путей данных. Если обе копии данных получены, лишний кадр удаляется на приемном конце. Если получена только одна копия данных, то включается режим резервного копирования. В стандарте ISO/IEC 62439-3 определены два типа избыточности, PRP и HSR. Этот тип избыточности является глобальным и имеет высокую стоимость. 802.1CB обеспечивает избыточность только для ключевых кадров, что позволяет снизить затраты.

802.1CB также может быть сокращено как FRER. Ниже приведена основная топологическая диаграмма дублирования и исключения кадров.



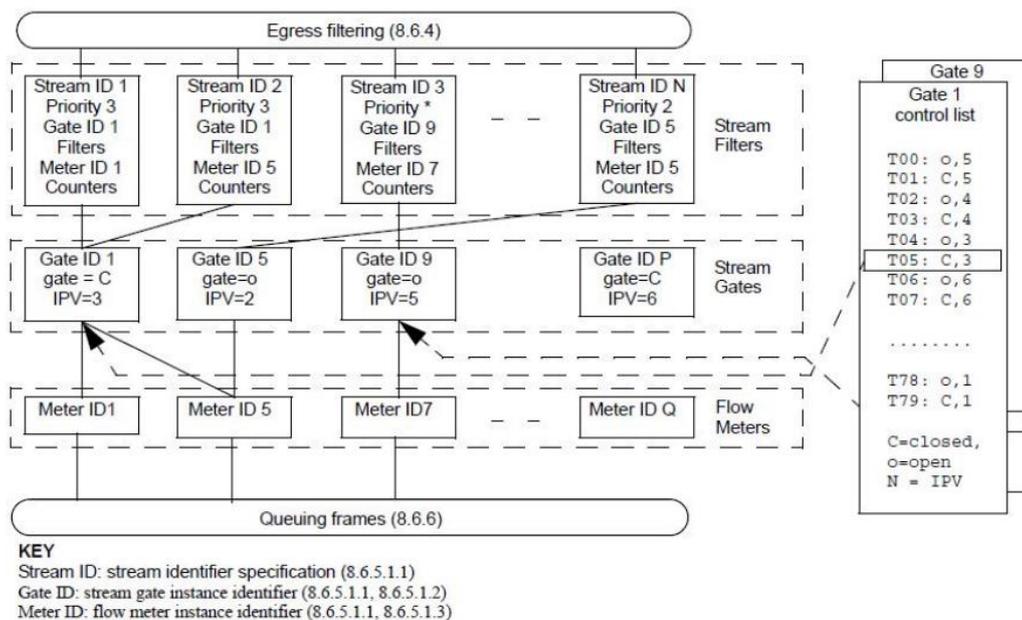
### 8.6.4 802.1Qbu

В механизме TAS возникают две проблемы: ① Расход защитной полосы ширины определенного интервала выборки; ② Риск инверсии низкого приоритета. Поэтому рабочие группы 802.1Qbu и IEEE 802.3 TSN совместно разработали IEEE 802.3br - механизм преемтивного MAC. Механизм передачи на основе преемтивного MAC [19] показан на рисунке 11. Он использует механизм предварительного прерывания кадра в 802.3TG и делит заданный выход на два MAC-сервисных интерфейса, которые называются прерываемым MAC (pMAC-Preemptible MAC) и быстрым MAC (eMAC-express MAC). pMAC может быть прерван eMAC. После входа в стек данных он ожидает завершения передачи данных eMAC, прежде чем передавать снова.

Благодаря прерыванию ширина защитной полосы может быть сведена к минимальному сегменту кадра низкого приоритета. Однако в худшем случае фрагмент низкого приоритета может завершиться до следующего фрагмента высокого приоритета. Конечно, процесс передачи с преемтивным MAC происходит только на интерфейсе уровня соединения, то есть для преемтивного MAC коммутатору требуется поддержка специализированного аппаратного уровня MAC.

### 8.6.5 802.1Qci

Полное название IEEE802.1 Qci - это Фильтрация и Контроль для Каждого Потока (далее в документе PSFP), то есть применяются стратегии фильтрации и контроля для каждого потока данных, чтобы обеспечить соответствие входящего трафика спецификациям и тем самым избежать проблем с аномальным трафиком, вызванным сбоями или злонамеренными атаками (например, атаками типа DoS).



PSFP осуществляется с помощью трех таблиц: Stream Filters, Stream Gates и Flow Meters на рисунке:

Stream Filters, то есть таблица фильтрации потоков. Каждая запись представляет собой фильтр, соответствующий определенному потоку, и связана с определенным шлюзом (Gate) и измерителем потока (Meter);

Stream Gates, то есть таблица управления потоком. Каждая запись представляет собой меру управления для определенного потока (например, если статус шлюза выключен, это означает, что соответствующий трафик запрещен к передаче);

Flow Meters - таблица счетчиков потока. Каждый элемент таблицы представляет статистику трафика определенного потока. При превышении потоком ограниченной пропускной способности применяется ограничение или блокировка потока. Для трафика из неизвестных источников PSFP закрывается путем установки шлюзов для предотвращения проникновения подозрительного трафика; для аномального трафика от известных источников. Аномальные характеристики здесь не ограничиваются пропускной способностью (превышение зарезервированной пропускной способности), но также включают: превышение максимальной длины служебных данных (SDU) по требованиям и т. д. PSFP может выбирать блокировку или ограничение потока.

## 8.6.6 TSN Руководство по конфигурации

### 8.6.6.1 TSN конфигурация

#### TSN Configuration

<b>Procedure</b>	Time only <input type="button" value="v"/>
<b>Timeout</b>	<input type="text" value="20"/>
<b>PTP Port</b>	<input type="text" value="0"/>

Описание каждого параметра представлено в следующей таблице

Параметр	Описание
Delayed start	Отложенный запуск TSN. Параметры, следующие: <ul style="list-style-type: none"><li>• Нет: запустить немедленно</li><li>• Время и РТР: запустится, когда статус РТР заблокирован или зафиксирован. Если время превысит установленное, а статус РТР не заблокирован или не зафиксирован, также будет запущен.</li><li>• Только время: запустить после превышения времени</li><li>• Значение по умолчанию. Только время</li></ul>
Timeout mode	Время ожидания, диапазон 10200 секунд, значение по умолчанию 20.
PTP port	Экземпляр РТР, диапазон 02, значение по умолчанию 0.

#### 8.6.6.2 Конфигурация предварительного прерывания кадра

Конфигурация предварительного прерывания кадра.

Frame Preemption Configuration

Port	Frame Preemption TX	Start Without LLDP	Verify Disable TX	Preemptable Queues TX								
				Q0	Q1	Q2	Q3	Q4	Q5	Q6	Q7	
*	<input type="checkbox"/>											
1	<input type="checkbox"/>											
2	<input type="checkbox"/>											
3	<input type="checkbox"/>											
4	<input type="checkbox"/>											
5	<input type="checkbox"/>											
6	<input type="checkbox"/>											
7	<input type="checkbox"/>											
8	<input type="checkbox"/>											
9	<input type="checkbox"/>											
10	<input type="checkbox"/>											
11	<input type="checkbox"/>											
12	<input type="checkbox"/>											
13	<input type="checkbox"/>											
14	<input type="checkbox"/>											
15	<input type="checkbox"/>											
16	<input type="checkbox"/>											
17	<input type="checkbox"/>											
18	<input type="checkbox"/>											
19	<input type="checkbox"/>											

Описание каждого параметра представлено в следующей таблице

Параметр	Описание
Port	Список портов
TX frame preemption	Разрешено предварительное прерывание кадра на выходе
Non-waiting LLDP	Не ожидать LLDP, включить функцию предварительного прерывания кадра
Check disabled	Не проверять предварительное прерывание кадра у партнера
TX queue frame preemption	Очередь предварительного прерывания кадра

8.6.6.3 Статус предварительного прерывания кадра

TSN Egress Port Frame Preemption Status

Port	Hold Advance	Release Advance	Preemption Active	Hold Request	Status Verify	Loc Preempt Support	Loc Preempt Enabled	Loc Preempt Active	Loc Add Frag Size
1	0	0	✗	✗	indeterminate	✓	✗	✓	0
2	0	0	✗	✗	indeterminate	✓	✗	✓	0
3	0	0	✗	✗	indeterminate	✓	✗	✓	0
4	0	0	✗	✗	indeterminate	✓	✗	✓	0
5	0	0	✗	✗	indeterminate	✓	✗	✓	0
6	0	0	✗	✗	indeterminate	✓	✗	✓	0
7	0	0	✗	✗	indeterminate	✓	✗	✓	0
8	0	0	✗	✗	disabled	✓	✗	✓	0

Описание каждого параметра представлено в следующей таблице

Параметр	Описание
Port	Список портов
Hold Advance	Максимальное количество наносекунд, которое Mac отправляет для остановки передачи, время ожидания
Release Advance	Освобождение заранее
Preemption Active	поддерживается и активно - true
Hold Request	Действует ли задержка или освобождение
Status check	Проверить статус партнера
Preemption support	Поддерживается ли предварительное прерывание
Preemption enabled	Включено ли предварительное прерывание?
Loc Preempt Active	Действует ли предварительное прерывание
Extra fragment length	Дополнительная длина фрагмента предварительного прерывания кадра

### 8.6.6.4 TAS конфигурация

TAS Configuration Parameters

Always Guard Band Option

Описание каждого параметра представлено в следующей таблице

Параметр	Описание
Always Guard Band Option	Опция всегда стража полосы. Включить и выключить защитный ремень.

#### 1. TAS конфигурация порта

TAS Port Configuration Parameters

Port	Gate								GCL Length	GCL	Cycle Time			Base Time	Config Change	
	Enabled	State									Value	Unit	Extension, ns			
		Q0	Q1	Q2	Q3	Q4	Q5	Q6	Q7							
*	<input type="checkbox"/>	<input checked="" type="checkbox"/>	0		100	<>	256	0	<input type="checkbox"/>							
1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	0	Configuration	100	MilliSeconds	256	0	<input type="checkbox"/>							
2	<input type="checkbox"/>	<input checked="" type="checkbox"/>	0	Configuration	100	MilliSeconds	256	0	<input type="checkbox"/>							
3	<input type="checkbox"/>	<input checked="" type="checkbox"/>	0	Configuration	100	MilliSeconds	256	0	<input type="checkbox"/>							
4	<input type="checkbox"/>	<input checked="" type="checkbox"/>	0	Configuration	100	MilliSeconds	256	0	<input type="checkbox"/>							
5	<input type="checkbox"/>	<input checked="" type="checkbox"/>	0	Configuration	100	MilliSeconds	256	0	<input type="checkbox"/>							
6	<input type="checkbox"/>	<input checked="" type="checkbox"/>	0	Configuration	100	MilliSeconds	256	0	<input type="checkbox"/>							
7	<input type="checkbox"/>	<input checked="" type="checkbox"/>	0	Configuration	100	MilliSeconds	256	0	<input type="checkbox"/>							
8	<input type="checkbox"/>	<input checked="" type="checkbox"/>	0	Configuration	100	MilliSeconds	256	0	<input type="checkbox"/>							
9	<input type="checkbox"/>	<input checked="" type="checkbox"/>	0	Configuration	100	MilliSeconds	256	0	<input type="checkbox"/>							
10	<input type="checkbox"/>	<input checked="" type="checkbox"/>	0	Configuration	100	MilliSeconds	256	0	<input type="checkbox"/>							
11	<input type="checkbox"/>	<input checked="" type="checkbox"/>	0	Configuration	100	MilliSeconds	256	0	<input type="checkbox"/>							
12	<input type="checkbox"/>	<input checked="" type="checkbox"/>	0	Configuration	100	MilliSeconds	256	0	<input type="checkbox"/>							
13	<input type="checkbox"/>	<input checked="" type="checkbox"/>	0	Configuration	100	MilliSeconds	256	0	<input type="checkbox"/>							
14	<input type="checkbox"/>	<input checked="" type="checkbox"/>	0	Configuration	100	MilliSeconds	256	0	<input type="checkbox"/>							
15	<input type="checkbox"/>	<input checked="" type="checkbox"/>	0	Configuration	100	MilliSeconds	256	0	<input type="checkbox"/>							
16	<input type="checkbox"/>	<input checked="" type="checkbox"/>	0	Configuration	100	MilliSeconds	256	0	<input type="checkbox"/>							

Описание каждого параметра представлено в следующей таблице

Параметр	Описание
Gating	Gated queue Enable: При включении, когда длина GCL не равна 0, управление воротами GCL действительно. Когда длина GCL равна 0, управление воротами осуществляется внешним образом. Когда Отключено включено, управление воротами GCL отключено, а внешнее управление воротами включено.
GCL length	Длина ворот GCL, диапазон 0256
GCL	Конфигурация ворот, каждая очередь должна быть проверена один раз за цикл
Time period	Значение времени, диапазон: 1999999999 Преобразованное время меньше 1000 мс Единица измерения: мс, мкс, нс Расширение: задержка, нс, значение по умолчанию 0
Base time	Базовое время, диапазон: Секунды: 04294967295 Наносекунды: 0999999999 Значение по умолчанию 0
Configuration changes	Изменения конфигурации, связанные с очередью, применяются только после завершения изменений, включения и проверки изменения конфигурации одновременно, конфигурация вступает в силу

2. GCL конфигурация

### GCL Configuration

GCE ID	Gate State							Time Interval	
	Q0	Q1	Q2	Q3	Q4	Q5	Q6	Q7	NanoSeconds
*									

Save Reset Back

Описание каждого параметра представлено в следующей таблице

Параметр	Описание
Gated state	Состояние ворот: очередь включена или выключена
Time interval	Диапазон: 1~999999999, сумма всех временных интервалов должна быть меньше или равна значению периода времени

### 3. Max SDU конфигурация

#### TAS SDU Configuration

Port	Max SDU Size							
	Q0	Q1	Q2	Q3	Q4	Q5	Q6	Q7
*	1536	1536	1536	1536	1536	1536	1536	1536
1	1536	1536	1536	1536	1536	1536	1536	1536
2	1536	1536	1536	1536	1536	1536	1536	1536
3	1536	1536	1536	1536	1536	1536	1536	1536
4	1536	1536	1536	1536	1536	1536	1536	1536
5	1536	1536	1536	1536	1536	1536	1536	1536
6	1536	1536	1536	1536	1536	1536	1536	1536
7	1536	1536	1536	1536	1536	1536	1536	1536
8	1536	1536	1536	1536	1536	1536	1536	1536
9	1536	1536	1536	1536	1536	1536	1536	1536
10	1536	1536	1536	1536	1536	1536	1536	1536
11	1536	1536	1536	1536	1536	1536	1536	1536
12	1536	1536	1536	1536	1536	1536	1536	1536
13	1536	1536	1536	1536	1536	1536	1536	1536
14	1536	1536	1536	1536	1536	1536	1536	1536
15	1536	1536	1536	1536	1536	1536	1536	1536
16	1536	1536	1536	1536	1536	1536	1536	1536
17	1536	1536	1536	1536	1536	1536	1536	1536
18	1536	1536	1536	1536	1536	1536	1536	1536

Описание каждого параметра представлено в следующей таблице

Параметр	Описание
Maximum SDU size	Максимальная единица обслуживания, диапазон: 0, 64~10240

### 8.6.6.5 TAS статус

TAS Status Parameters

Port	Operation Gate							Cycle Time			Time		Config Change		Tick Granularity	Config Pending	Time			
	Enabled	Q0	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Value	Unit	Extension, ns	Base	Current			Time	Error	Length	GCL
1	✗	✓	✓	✓	✓	✓	✓	✓	✓	100	MilliSeconds	256	0	798	0	0	1	false	0	Status
2	✗	✓	✓	✓	✓	✓	✓	✓	✓	100	MilliSeconds	256	0	798	0	0	1	false	0	Status
3	✗	✓	✓	✓	✓	✓	✓	✓	✓	100	MilliSeconds	256	0	798	0	0	1	false	0	Status
4	✗	✓	✓	✓	✓	✓	✓	✓	✓	100	MilliSeconds	256	0	798	0	0	1	false	0	Status
5	✗	✓	✓	✓	✓	✓	✓	✓	✓	100	MilliSeconds	256	0	798	0	0	1	false	0	Status
6	✗	✓	✓	✓	✓	✓	✓	✓	✓	100	MilliSeconds	256	0	798	0	0	1	false	0	Status
7	✗	✓	✓	✓	✓	✓	✓	✓	✓	100	MilliSeconds	256	0	798	0	0	1	false	0	Status
8	✗	✓	✓	✓	✓	✓	✓	✓	✓	100	MilliSeconds	256	0	798	0	0	1	false	0	Status

Описание каждого параметра представлено в следующей таблице

Параметр	Описание
Port	Список портов
Gating	Включение/отключение ограждения, включение/отключение очереди
Time period	Время цикла GCL
Time	Базовое время и текущее время
Configuration changes	Время изменения конфигурации, количество ошибок изменения
Interval	Количество тактов между интервалами
Configuration hangs	Висячая конфигурация
GCL length	Длина списка управления ограждением

### 8.6.6.6 PSFP конфигурация

4. Конфигурация измерения потока:

#### PSFP Flow Meter Configuration

Delete	FMI ID	CIR	CBS	EIR	EBS	CF	CM	Drop On Yellow	Mark Red

Add Entry

Save    Reset

Описание каждого параметра представлено в следующей таблице

Параметр	Описание
Delete	Удалить
FMI ID	Идентификатор измерения потока, диапазон 01022, значение по умолчанию 0.
CIR	Скорость отправки, диапазон: 04294967295 кбит/с, значение по умолчанию 10000.
CBS	Размер пакета, диапазон: 04294967295 байт, значение по умолчанию 2048.
EIR	Суперскорость, диапазон: 04294967295 кбит/с, значение по умолчанию 0.
EBS	Суперразмер пакета, диапазон: 04294967295 байт, значение по умолчанию 0.
CF	Флаг связывания, диапазон 01, значение по умолчанию 0.
Color mode	Метод обработки цветowych сообщений:
Drop On Yellow	Отбрасывать желтые пакеты
Mark Red	Помечать красные пакеты

 **Примечание:**  
 Настроенный диапазон CIR, EIR, CBS и EBS не является диапазоном, поддерживаемым чипом. При выдаче конфигурации будут выбраны оптимальные параметры на основе поддержки чипа.

### 5. Конфигурация фильтрации потока

PSFP Stream Filter Configuration

Delete	SFI ID	Stream ID	Stream Enable	Priority Spec	SFI ID	SFI Enable	SDU Size	FMI ID	FMI Enable	Oversize Block Enable

Add Entry

Save    Reset

Описание каждого параметра представлено в следующей таблице

Параметр	Описание
SFI ID	Идентификатор фильтра потока, диапазон 01022
Stream ID	Идентификатор потока, диапазон 1127
Stream enable	Включить поток
Priority	Внутренний приоритет, диапазон ни один, 07
SFI ID	Идентификатор SFI, диапазон 01022
SFI enabled	SFI включен
SDU size	Размер SDU, диапазон 065535
FMI ID	Идентификатор FMI, диапазон 01022
FMI enable	FMI включить
Jumbo frame blocking enable	Включить или выключить блокировку кадров большого размера

6. Конфигурация потокового затора

PSFP SGI Configuration

Delete	SGI ID	Gate		Cycle Time			Base Time	Admin IPV	GCL Length	GCL Configuration	Enable Gate-closed-due-to		Config Change
		Enabled	State	Value	Unit	Extension					Invalid-RX	Octets-exceeded	

Add Entry

Save Reset

Описание каждого параметра представлено в следующей таблице

Параметр	Описание
SGI ID	SGI ID, диапазон: 01022, значение по умолчанию 0
Enable	Управление включено
Port status	Статус переключателя управления дверью
Time value	Значение времени, диапазон: 11000000000, не более 1000 мс, значение по умолчанию 0
Unit	мс, мкс, нс
Extension of time	Расширенное время, диапазон: 0-999999999 нс, значение по умолчанию 0
Base time	Базовое время, диапазон: секунды: 04294967295, наносекунды: 0999999999, значение по умолчанию 0
Internal priority	Внутренний приоритет, диапазон: 07, значение по умолчанию 0
GCL length	Длина GCL, диапазон: 04, значение по умолчанию 0
Invalid Rx	Отключение неверного закрытия сигнализации при приеме Rx
Over fixed length	Закрытие сигнализации из-за слишком длинного байта
Configuration changes	Модификация конфигурации, модификация связанная с очередью, после модификации, проверьте изменение конфигурации, конфигурация вступит в силу

7. Конфигурация потокового управления через GCL.

GCL Configuration

SGI ID	GCL ID	GCL Parameters			
		Gate State	IPV	Time Interval (ns)	Octet Max

Save Reset

Cancel

Параметр	Описание
SGI ID	SGI ID

Параметр	Описание
GCL ID	GCL ID
Gated state	Статус переключателя управления дверью
IPV	Внутренний приоритет, диапазон 07, значение по умолчанию 0
Time interval	Время переключения управления шлюзом, сумма интервалов времени в диапазоне меньше или равна времени цикла, значение по умолчанию 1
Maximum bytes	Максимальное количество переданных байтов за один цикл, диапазон 010000, значение по умолчанию 0

### 8.6.6.7 Статус параметров потока PSFP

PSFP Stream Parameter Status

Max Stream Filter Instances	1023
Max Stream Gate Instances	1023
Max Flow Meter Instances	1023
Supported List Max	4

Описание каждого параметра представлено в следующей таблице

Параметр	Описание
Maximum flow filtering example	Пример максимальной фильтрации потока
Maximum flow gating example	Пример максимального управления потоком
Maximum flow meter example	Пример максимального измерения потока
Largest list	Список максимальных GCL с управлением

### 8.6.6.8 Статус фильтрации потока PSFP

PSFP Stream Filter Status

Clear	SFI ID	Blocked Due To Oversize Frame

Описание каждого параметра представлено в следующей таблице

Параметр	Описание
SFI ID	Идентификатор фильтра потока
Due to jumbo frame blocking	Блокируются ли сверхдлинные фреймы

### 8.6.6.9 Статистика фильтрации потока PSFP

PSFP Stream Filter Statistics

Clear	SFI ID	Matching Frame Count	Passing Frame Count	Not Passing Frame Count	Passing SDU Count	Not Passing SDU Count	RED Frames Count

Описание каждого параметра представлено в следующей таблице

Параметр	Описание
SFI ID	Идентификатор фильтра потока
Match frame count	Количество совпадающих фреймов
Forwarded frame count	Количество перенаправленных фреймов
Blocking frame count	Количество заблокированных фреймов
Forwarded SDU count	Количество перенаправленных SDU
Blocking SDU count	Количество заблокированных SDU
RED frame count	Количество фреймов RED

### 8.6.6.10 Статус управления потоком PSFP

PSFP SGI Status

SGI ID	Operation Gate		Cycle Time	Cycle Time Extension	Time		Config Change		Tick Granularity	Config Pending	IPV	Rx	Octets
	Enabled	State			Base	Current	Time	Error					

Описание каждого параметра представлено в следующей таблице

Параметр	Описание
SGI ID	Идентификатор управления доступом
Gating	Включение/отключение управления дверью, статус переключателя управления дверью
Time period	Период времени GCL
Extension of time	Расширение времени
Time	Базовое время и текущее время
Configuration Changes	Время изменения конфигурации
Interval	Количество тактов между интервалами
Configuration hangs	Зависание конфигурации
Internal priority	Внутренний приоритет
Take over	Закрытие управления ворот при приеме недопустимых сообщений
Byte	Закрытие управления воротами при превышении длины байта

### 8.6.6.11 FRER конфигурация

#### FRER конфигурация

FRER Configuration

FRER Configuration

Instance	Mode	Enabled	FRER VLAN	Recovery						Latent Error Detection				
				Algorithm	History Length	Reset Timeout	Take-no-sequence	Individual	Terminate	Enabled	Error Diff	Period	Paths	Reset Period
0	Generation ▾	<input type="checkbox"/>	1	Vector ▾	2	1000	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	100	2000	2	30000

Ingress Streams

Ingress Streams List

Egress Ports

Egress Port List

保存 重置 取消

Описание каждого параметра представлено в следующей таблице

Параметр	Описание
Example	Диапазон: 1127
Operating mode	Генерация: копирование кадра, Восстановление: исключение кадра
Enable	Конфигурация FRER вступает в силу
FRER VLAN	Идентификатор VLAN для FRER
Algorithm	Действительно в режиме восстановления: совпадение, векторный алгоритм
Length of history	В режиме восстановления векторный алгоритм действителен, и длина истории вектора равна
Timeout reset	Действительно в режиме восстановления: функция сброса по таймауту восстановления
Take-no-sequence	Действительно в режиме восстановления: отбрасывание пакетов без метки R
Individual	Действительно в режиме восстановления: одиночный поток
Terminate	Действительно в режиме восстановления: удаление метки R
Potential error Detection	Количество допустимых ошибок: количество допустимых ошибок, диапазон: 0-10000000, значение по умолчанию 100, Период: Диапазон: 1000-86400000, значение по умолчанию 2000 Количество путей (объектов): Диапазон: 2-8, значение по умолчанию 2 Период сброса: Диапазон: 1000-86400000, значение по умолчанию 30000
Inbound flow list	Идентификатор входящего потока, диапазон 1-127, значение по умолчанию отсутствует
Outbound port list	Идентификатор исходящего порта, диапазон 1-36, значение по умолчанию отсутствует

### 8.6.6.12 FRER статус

### FRER Status

Instance	Operation	Warnings	Latent Error	Statistics	Reset	
					Action	Latent Error

Описание каждого параметра представлено в следующей таблице

Параметр	Описание
Example	Диапазон: 1~127
Operate	Индикатор работы
Warn	Индикатор предупреждения
Potential errors	Индикатор потенциальной ошибки
Statistics	Кнопка сброса
Reset	Кнопка сброса

### 8.6.6.13 FRER статистика

FRER Statistics

Clear	Instance	Mode	Egress Ports	Ingress Streams	Out of Order	Rogue	Passed	Discarded	Lost	Tag Less	Recovery Resets	Latent Error Resets	Generation	Generation Resets

Описание каждого параметра представлено в следующей таблице

Параметр	Описание
Example	Диапазон: 1~127
Operating mode	Генерация, Режим восстановления
Egress port	Исходящий порт
Incoming flow	Входящий поток
Out of order	Неверный номер последовательности
Over limit	Превышение лимита
Forward	Количество пересылок
Throw away	Количество отброшенных
Lost	Потерянные счетчики
No label	Количество без метки
RecoveryReset	Сбросы восстановления
Number of potential error resets	Количество сбросов потенциальной ошибки
Generation reset	Количество сбросов генерации

## 9 Управление системой

### 9.1 Пользователь

Эта страница отображает список всех текущих пользователей и предоставляет функции для добавления, удаления и изменения информации об учетной записи каждого пользователя, как показано на рисунке ниже. Список пользователей содержит имя каждого пользователя и информацию о его уровне привилегий.

**Users Configuration**

User Name	Privilege Level
admin	15

Описание каждого параметра представлено в следующей таблице:

Параметр	Описание
Username	Отображается текущее имя пользователя. Щелкните ссылку с именем пользователя, чтобы изменить пароль и разрешения пользователя.
Permission level	Отображает уровень разрешений пользователя. Чем больше значение, тем выше уровень разрешений.

#### Новый пользователь

На странице "Пользователи" нажмите кнопку "Добавить пользователя", чтобы перейти на страницу создания нового пользователя и добавить новых пользователей, как показано на рисунке ниже.

**Add User**

User Settings	
User Name	<input type="text"/>
Password	<input type="password"/>
Password (again)	<input type="password"/>
Privilege Level	0 <input type="button" value="v"/>

Описание каждого параметра представлено в следующей таблице:

Параметр	Описание
Username	Имя пользователя нового пользователя. Допустимая длина строки составляет от 1 до 31 символа, а допустимый диапазон значений - буквы, цифры или подчеркивания.
Password	Добавьте пароль нового пользователя. Допустимая длина строки составляет от 1 до 31 символа, и принимаются любые печатные символы, включая пробелы.
Password (enter again)	Введите пароль еще раз для подтверждения.
Permission level	Уровень привилегий пользователя может быть от 0 до 15. Фактические разрешения пользователя для каждой функции

Параметр	Описание
	согласованы с уровнем привилегий каждой функциональной группы. Только пользователь, уровень привилегий которого больше или равен уровню привилегий группы, может получить доступ к этой группе

### Редактирование/удаление пользователя

На странице "Пользователь" нажмите ссылку, чтобы указать имя пользователя и перейти на страницу редактирования пользователя, как показано на рисунке ниже..

**Edit User**

User Settings	
User Name	admin
Change Password	No ▼
Privilege Level	15 ▼

Описание каждого параметра представлено в следующей таблице:

Параметр	Описание
Username	Отображается имя пользователя для редактирования
Change Password	Изменить пароль пользователя: <ul style="list-style-type: none"> <li>• Да</li> <li>• Нет</li> </ul>
Password	При изменении пароля допустимая длина строки для нового пароля пользователя составляет от 0 до 31 символа, и принимаются любые печатные символы, включая пробелы.
Password (enter again)	Введите пароль еще раз для подтверждения.
Permission level	Уровень привилегий пользователя может быть от 0 до 15. Фактические разрешения пользователя для каждой функции согласованы с уровнем привилегий каждой функциональной группы. Только пользователь, уровень привилегий которого больше или равен уровню привилегий группы, может получить доступ к этой группе.
Delete users	Нажмите кнопку "Удалить пользователя", чтобы удалить пользователя

**Примечания:**

После первого входа на веб-страницу коммутатора в окне браузера, открытие новой вкладки в том же окне для доступа к коммутатору приведет к тому, что диалоговое окно входа больше не будет появляться, и ранее введенное имя пользователя и пароль будут использоваться для входа автоматически по умолчанию. Если вы хотите использовать другую учетную запись

пользователя для входа на веб-страницу коммутатора, вам нужно просто нажать кнопку выхода в правом верхнем углу страницы или снова открыть окно браузера.

Имя пользователя администратора коммутатора по умолчанию - admin, пароль - admin, уровень привилегий - 15, и у него есть все права управления.

Пользователь администратора по умолчанию admin не может быть удален или изменен уровень привилегий, но пароль может быть изменен. Другие добавленные вручную пользователи могут быть удалены и у них может быть изменен уровень привилегий.

После удаления текущего вошедшего в систему пользователя на веб-странице или изменения пароля текущего вошедшего в систему пользователя на веб-странице вам будет предложено войти в систему снова; однако после удаления текущего вошедшего в систему пользователя в командной строке или изменения пароля текущего вошедшего в систему пользователя в командной строке это не повлияет на текущий статус входа в систему, только на текущий статус входа в систему. При повторном входе в систему проверка входа будет осуществляться в соответствии с новыми настройками учетной записи.

Изменения прав доступа текущего вошедшего в систему пользователя на веб-странице вступают в силу немедленно; однако изменения прав доступа текущего вошедшего в систему пользователя в командной строке вступают в силу только после повторного входа в систему.

При добавлении нового пользователя можно настроить только имя пользователя. После успешного добавления рекомендуется изменить пароль и уровень привилегий, нажав на имя пользователя в списке пользователей. В противном случае у пользователя по умолчанию пароль пустой, уровень привилегий равен 0, и у пользователя нет прав доступа к веб-странице и командной строке коммутатора.

На странице редактирования назначенного пользователя можно изменить только пароль пользователя и уровень привилегий, но не имя пользователя.

Пожалуйста, осторожно используйте учетные записи пользователей без пароля.

## 9.2 DHCPv4

### 9.2.1 Служба DHCPv4

DHCP (Dynamic Host Configuration Protocol) - это улучшенная версия протокола BOOTP. Он использует режим клиент-сервер для обмена данными. Все параметры конфигурации IP-сети централизованно управляются DHCP-сервером и отвечают за обработку запросов DHCP клиента. Клиент будет использовать назначенные сервером параметры IP-сети для обмена данными.

В зависимости от различных потребностей клиентов DHCP предоставляет три стратегии выделения IP-адресов:

- Ручное выделение адресов: администратор статически привязывает фиксированные IP-адреса к небольшому числу конкретных клиентов и отправляет настроенные фиксированные IP-адреса клиентам через DHCP.
- Автоматическое выделение адресов: DHCP выделяет IP-адрес с бесконечным сроком аренды клиенту.
- Динамическое выделение адресов: DHCP выделяет IP-адрес с определенным сроком действия для клиента. После истечения срока действия клиенту нужно повторно запросить адрес.

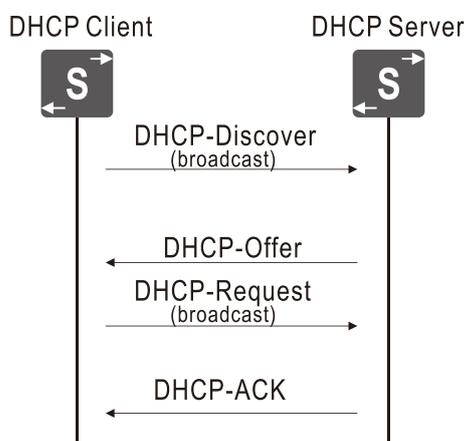
Администраторы могут выбирать, какая политика DHCP будет использоваться на основе конкретной сети или хоста.

Для использования механизма динамического выделения адресов DHCP администратор должен сконфигурировать DHCP-сервер так, чтобы он мог предоставлять группу IP-адресов, называемую адресным пулом. Каждый раз, когда новый компьютер подключается к сети, он связывается с сервером и запрашивает IP-адрес. Сервер выбирает адрес из настроенного адресного пула и назначает его компьютеру.

Для динамического получения и использования допустимого IP-адреса необходимо пройти следующие этапы:

- Фаза обнаружения: это фаза, в которой клиент DHCP ищет DHCP-сервер.
- Этап предоставления: это этап, когда DHCP-сервер предоставляет IP-адрес.
- Фаза выбора: это фаза, в которой клиент DHCP выбирает IP-адрес, предоставленный определенным DHCP-сервером.
- Фаза подтверждения: это фаза, когда DHCP-сервер подтверждает предоставленный IP-адрес.

Процесс динамического получения IP-адреса показан на рисунке ниже.



### 9.2.1.1 Режим обслуживания

Для запуска службы динамического выделения адресов на всей системе необходимо включить DHCP-сервис глобально.

Кроме того, поскольку DHCP-сервер является протоколом на основе IP, необходимо также запустить DHCP-сервис соответствующего интерфейса VLAN. Перед запуском DHCP-сервиса для каждого интерфейса VLAN на веб-странице убедитесь, что интерфейс VLAN уровня 3 был создан, а членские порты VLAN были правильно настроены.

Страница конфигурации режима DHCP-сервера показана на рисунке ниже.

### DHCP Server Mode Configuration

**Global Mode**

Mode

**VLAN Mode**

VLAN	Enabled
1	<input type="checkbox"/>

Описание каждого параметра представлено в следующей таблице:

Параметр	Описание
<b>Global mode</b>	<b>Глобальный режим</b>
Mode	Настройте режим работы DHCP-сервиса для всей системы, включая: <ul style="list-style-type: none"> <li>Включить: включить глобальный DHCP-сервис;</li> <li>Отключить: отключить глобальный DHCP-сервис</li> </ul>
<b>VLAN mode</b>	<b>VLAN режим</b>
VLAN	VLAN идентификатор
Enable	Настройте режим работы DHCP-сервиса для каждого интерфейса VLAN уровня 3, установив или сняв флажок "Включить" напротив каждого интерфейса VLAN: <ul style="list-style-type: none"> <li>Выбрано: включить DHCP-сервис соответствующего интерфейса VLAN;</li> <li>Не выбрано: отключить DHCP-сервис соответствующего интерфейса VLAN</li> </ul>

**Примечание:**

Перед запуском DHCP-сервиса для каждого интерфейса VLAN на веб-странице, пожалуйста, создайте соответствующий интерфейс VLAN уровня 3 на странице "Функции уровня 3 > Управление IP > Конфигурация IP" и создайте соответствующий интерфейс VLAN уровня 3 на странице "Функции уровня 2 > VLAN > Глобальная конфигурация". Завершите конфигурацию атрибутов VLAN, таких как PVID для каждого порта.

Перед использованием службы DHCP-сервера, пожалуйста, включите глобальное маршрутизирование на коммутаторе, чтобы обеспечить доступность маршрутов между клиентами на различных интерфейсах VLAN коммутатора.

### 9.2.1.2 Отсутствие выделения IP-адресов

В любой IP-подсети, чтобы обеспечить IP-связность и услуги, будут настроены некоторые IP-серверы или маршрутизаторы вручную, и их адреса не должны конфликтовать с любым

устройством в той же подсети. По этой причине DHCP-сервер должен исключить эти статические IP-адреса при назначении адресов. Фактически, IP-адрес локального интерфейса устройства по умолчанию исключается DHCP-сервером. Пользователям также следует вручную исключить известные адреса брандмауэров.

Установив диапазон адресов, который не выделяет IP-адреса, на странице настройки зарезервированных IP-адресов DHCP-сервера, DHCP-сервер запретит выделение IP-адресов в этом диапазоне для клиентов DHCP. DHCP-сервер не назначает конфигурацию IP-адреса, как показано на рисунке ниже.

**DHCP Server Excluded IP Configuration**

**Excluded IP Address**

Delete IP Range

Add IP Range

Save Reset

Описание каждого параметра представлено в следующей таблице:

Параметр	Описание
Delete	Отображается поле для удаления или кнопка удаления. Установка флажка удаления означает, что строка записей диапазона исключенных IP-адресов будет удалена после сохранения. Нажатие кнопки удаления означает, что строка записей диапазона исключенных IP-адресов будет немедленно удалена.
IP range	Определите диапазоны IP для исключения. Первый исключенный IP должен быть $\leq$ второго исключенного IP. Однако, если диапазон IP содержит только 1 исключенный IP, вы можете ввести только первый или второй исключенный IP, или тот же IP для обоих
Add IP range	Щелкните, чтобы добавить новую запись диапазона исключенных IP-адресов

 **Примечание:**

Запрещено резервировать IP-адреса, зарезервированные в пуле адресов DHCP

### 9.2.1.3 Пул адресов

После настройки пула адресов DHCP, DHCP-сервер будет выделять IP-адреса на основе конфигурации пула адресов и передавать параметры конфигурации DHCP-клиенту. Страница конфигурации пула адресов DHCP показана на рисунке ниже.

**DHCP Server Pool Configuration**

**Pool Setting**

Delete	Name	Type	IP	Subnet Mask	Reserved only	Lease Time
<input type="button" value="Add New Pool"/>						
<input type="button" value="Save"/> <input type="button" value="Reset"/>						

В верхней части страницы отображается краткая таблица конфигурации пула адресов DHCP, в которой перечислены основные сведения о всех пулах адресов на текущем DHCP-сервере, включая имя, тип, IP-адрес, маску подсети, нераспределение и период аренды.

Описание каждого параметра представлено в следующей таблице:

Параметр	Описание
Delete	Отображается поле для удаления или кнопка удаления. Установка флажка удаления означает, что запись конфигурации пула адресов в этой строке будет удалена после сохранения. Нажатие кнопки удаления означает, что запись конфигурации пула адресов в этой строке будет немедленно удалена.
Name	Имя пула адресов, длина строки составляет от 1 до 32 символов, и его значение может быть любым символом, доступным для печати на английской клавиатуре (включая заглавные и строчные буквы, специальные символы и цифры, но не включая пробелы). После щелчка по имени любого пула адресов в списке конфигурации пула адресов можно просмотреть подробную информацию о конфигурации пула адресов.
Type	Тип пула адресов может принимать следующие два значения: <ul style="list-style-type: none"> <li>• Сеть: Этот пул адресов может обслуживать несколько DHCP-клиентов;</li> <li>• Хост: Этот пул адресов может обслуживать только определенных DHCP-клиентов, идентифицируемых идентификаторами клиентов или аппаратными адресами</li> </ul>
IP	Адреса подсети, которые могут быть выделены из пула адресов.
Subnet mask	Маска подсети пула адресов
Only allocated reserved addresses	Функция выделения адресов только в соответствии с записями зарезервированных IP-адресов в пуле адресов имеет два значения: <ul style="list-style-type: none"> <li>• Включено: Только зарезервированные IP-адреса назначаются на привязанный интерфейс.</li> <li>• Выключено: Назначить зарезервированный IP на привязанный интерфейс, а также назначить другие динамические IP-адреса на другие интерфейсы.</li> </ul>
Lease period	Длительность аренды для адреса.
Add address pool	Нажмите кнопку "Добавить новый пул" в таблице суммарной конфигурации пула адресов DHCP. Пустая запись будет добавлена в

Параметр	Описание
	конец таблицы суммарной конфигурации пула адресов DHCP, как показано на рисунке ниже. Введите допустимое имя пула адресов в соответствующее поле имени, а затем после щелчка по кнопке "Сохранить" будет добавлен пустой пул адресов с этим именем в систему. Все атрибуты пустого пула адресов имеют значения по умолчанию



Утверждение:

"-" во всех списках означает неопределенное значение

### Добавить пул адресов

Щелкните кнопку "Добавить пул адресов" под таблицей суммарной конфигурации пула адресов DHCP. Пустая запись будет добавлена в конец таблицы суммарной конфигурации пула адресов DHCP, как показано на рисунке ниже. Введите допустимое имя пула адресов в соответствующее поле имени. Затем после нажатия кнопки "Сохранить" будет добавлен пустой пул адресов с этим именем в систему. Все атрибуты пустого пула адресов имеют значения по умолчанию.

### Удалить пул адресов

Для пустой записи пула адресов, которая добавляется, но еще не сохранена, вы можете нажать кнопку "Удалить" в первом столбце записи или нажать кнопку "Сбросить" под таблицей суммарной конфигурации пула адресов DHCP, чтобы удалить ее.

Для пула адресов, который был сохранен, вам нужно установить флажок удаления в первом столбце элемента таблицы, а затем нажать кнопку "Сохранить" под таблицей, чтобы удалить его.

### Настройка пула адресов

Страница детальной конфигурации пула адресов DHCP состоит из трех частей. В верхней части страницы находится область выбора имени пула адресов, в которой по умолчанию в списке опций имени пула адресов отображается имя пула адресов, которое пользователь ранее выбрал в таблице суммарной конфигурации пула адресов DHCP. Пользователь может выбрать детальную конфигурацию какого DHCP-пула адресов отобразить на текущей странице из выпадающего списка опций имени.

В левой нижней части страницы находится область конфигурации атрибутов для пула адресов, как показано на рисунке ниже.

### DHCP Pool Configuration

Pool

Name

#### Setting

Pool Name	1	
Type	None	
IP	0.0.0.0	
Subnet Mask	0.0.0.0	
Lease Time	<input type="text" value="1"/>	days (0-365)
	<input type="text" value="0"/>	hours (0-23)
	<input type="text" value="0"/>	minutes (0-59)
Domain Name	<input type="text"/>	
Broadcast Address	0.0.0.0	
Allocate reserved entries only	Off	
Default Router	0.0.0.0	
	0.0.0.0	
	0.0.0.0	
	0.0.0.0	
DNS Server	0.0.0.0	
	0.0.0.0	
	0.0.0.0	
	0.0.0.0	
NTP Server	0.0.0.0	
	0.0.0.0	
	0.0.0.0	
	0.0.0.0	
NetBIOS Node Type	None	
NetBIOS Scope	<input type="text"/>	
NetBIOS Name Server	0.0.0.0	
	0.0.0.0	
	0.0.0.0	
	0.0.0.0	
NIS Domain Name	<input type="text"/>	
NIS Server	0.0.0.0	
	0.0.0.0	
	0.0.0.0	
	0.0.0.0	
Client Identifier	None	<input type="text"/>
Hardware Address	00:00:00:00:00:00	
Client Name	<input type="text"/>	
Vendor 1 Class Identifier	<input type="text"/>	
Vendor 1 Specific Information	<input type="text"/>	
Vendor 2 Class Identifier	<input type="text"/>	
Vendor 2 Specific Information	<input type="text"/>	
Vendor 3 Class Identifier	<input type="text"/>	
Vendor 3 Specific Information	<input type="text"/>	
Vendor 4 Class Identifier	<input type="text"/>	
Vendor 4 Specific Information	<input type="text"/>	

#### Reserved Ip Addresses

Delete	Reserved address	Interface
No entry exists		

Add New Entry

Save

Save Reset Back to pools page

Описание каждого параметра представлено в следующей таблице:

Параметр	Описание
<b>Address pool</b>	<b>Пул адресов</b>
Name	Список выбора имени пула адресов, в котором можно выбрать различные пулы адресов для конфигурации.
<b>Configuration</b>	<b>Конфигурация</b>
Address pool name	Имя пула адресов, доступное только для чтения, соответствует выбору имени пула адресов выше
Type	<p>Тип пула адресов имеет следующие два значения:</p> <ul style="list-style-type: none"> <li>• Сеть: Этот пул адресов может обслуживать несколько DHCP-клиентов, и адрес, который может быть выделен, является сетевым адресом (например, 192.168.1.0/24);</li> <li>• Хост: Этот пул адресов может обслуживать только конкретные DHCP-клиенты, идентифицированные идентификаторами клиентов или аппаратными адресами. Выделяемый адрес является адресом хоста (например, 192.168.1.5/24)</li> </ul>
IP	Адрес подсети, назначенный пулу адресов.
Subnet mask	Маска подсети, назначенная пулу адресов, соответствующая DHCP-опции 1.
Lease period	DHCP-опция 51. Указывает срок действия аренды пула адресов. Если срок аренды адресов в пуле настроен на веб-странице как 0 дней, 0 часов и 0 минут, это означает неограниченный срок аренды.
Domain name	DHCP-опция 15. Указывает доменное имя, которое клиенты должны использовать при разрешении имен хостов через DNS.
Broadcast address	DHCP-опция 28. Указывает широковещательный адрес, используемый в подсети клиента.
Assign reserved entries only	<p>Будет ли выделение адресов происходить только в соответствии с зарезервированными записями IP-адресов в пуле адресов, имеет два значения:</p> <ul style="list-style-type: none"> <li>• Включено: Только зарезервированные IP-адреса выделяются для связанного интерфейса.</li> <li>• Выключено: Выделяется зарезервированный IP-адрес для связанного интерфейса, а также выделяются другие динамические IP-адреса для других интерфейсов.</li> </ul>
Default gateway	DHCP-опция 3. Указывает список IP-адресов маршрутизатора подсети клиента, который является адресом шлюза, назначенным клиенту.
DNS server	DHCP-опция 6. Указывает список IP-адресов серверов DNS, доступных для клиента.
NTP server	DHCP-опция 42. Указывает список IP-адресов серверов NTP, доступных для клиента.

Параметр	Описание
NetBIOS node type	<p>DHCP-опция 46. Когда клиент DHCP использует протокол NetBIOS для связи в сети, ему необходимо установить отображающее отношение между именем хоста и IP-адресом. В зависимости от способов получения отношений отображения, типы узлов NetBIOS разделяются на следующие четыре типа:</p> <ul style="list-style-type: none"> <li>• Узел класса В (B-node): "В" означает широковещательную рассылку, то есть этот тип узла использует широковещательную рассылку для получения отношений отображения. Исходный узел получает IP-адрес целевого узла, отправив широковещательное сообщение с именем хоста целевого узла. После получения широковещательного сообщения целевой узел возвращает свой IP-адрес исходному узлу.</li> <li>• Узел типа Р (P-node): "Р" означает одноранговую связь, то есть этот тип узла получает отношения отображения, отправляя одноадресные сообщения для связи с сервером WINS (Windows Internet Naming Service). Исходный узел отправляет одноадресное сообщение на сервер WINS. После получения одноадресного сообщения сервер WINS возвращает IP-адрес, соответствующий запрошенному имени хоста целевого узла.</li> <li>• Узел типа М (M-node): "М" означает смешанный, это узел типа Р с некоторыми характеристиками широковещательной рассылки. Этот тип узла сначала отправляет широковещательное сообщение для получения отношения отображения. Если отношение отображения не получено, затем отправляется одноадресное сообщение для связи с сервером WINS для получения отношения отображения.</li> <li>• Узел Н (H-node): "Н" означает гибридный, это узел класса В с механизмом "точка-точка" коммуникации. Этот тип узла сначала отправляет одноадресное сообщение для связи с сервером WINS для получения отношения отображения. Если отношение отображения не получено, затем отправляется широковещательное сообщение для получения отношения отображения</li> </ul>
NetBIOS scope	DHCP-опция 47. Указывает NetBIOS согласно параметрам диапазона TCP/IP клиента, указанным в RFC 1001/1002.
NetBIOS name server	DHCP-опция 44. Указывает приоритетный список серверов имен NBNS.
NIS domain name	DHCP-опция 40. Указывает имя домена NIS (Network Information System) клиента.
NIS server	DHCP-опция 41. Указывает список IP-адресов серверов NIS, доступных для клиента.

Параметр	Описание
Client identifier	<p>DHCP-опция 61. Указывает уникальный идентификатор клиента для использования при обмене сообщениями DHCP, когда пул адресов имеет тип "хост". Сначала выберите тип идентификатора клиента из выпадающего списка, а затем заполните соответствующее значение в следующем поле ввода. Доступны следующие типы идентификаторов клиентов:</p> <ul style="list-style-type: none"> <li>• None: Не указывать идентификатор.</li> <li>• Name: Любой идентификатор, не являющийся аппаратным. В этом случае в поле ввода должна быть введена любая строка, не содержащая китайских символов;</li> <li>• MAC: Идентификатор типа аппаратного адреса MAC. В этом случае в поле ввода следует указать MAC-адрес. Формат: XX:XX:XX:XX:XX:XX, где X - шестнадцатеричное целое число.</li> </ul>
Hardware address	<p>адайте аппаратный адрес (MAC) клиента для использования при настройке пула адресов типа "хост". MAC-адрес должен быть уникальным и иметь формат XX:XX:XX:XX:XX:XX, где X - шестнадцатеричное целое число.</p>
CPU name	<p>DHCP-опция 12. Указывает имя хоста клиента для использования при настройке пула адресов типа "хост".</p>
Manufacturer classification mark	<p>DHCP-опция 60. Клиент использует эту опцию для идентификации производителя, к которому он принадлежит; DHCP-сервер может отличить производителя клиента по этой опции и назначить ему определенный диапазон IP-адресов.</p>
Manufacturer feature information	<p>DHCP-опция 43. Указывает конкретную информацию о каждом идентификаторе производителя для обмена информацией между DHCP-сервером и DHCP-клиентом.</p>
<b>Reserve IP address</b>	<b>Зарезервированный IP-адрес</b>
Delete	<p>Отображается флажок удаления или кнопка удаления. При установке флажка удаления этой строки конфигурация зарезервированного IP-адреса будет удалена после сохранения. При нажатии кнопки удаления эта строка конфигурации зарезервированного IP-адреса будет немедленно удалена.</p>
Reserved address	<p>IP-адрес зарезервирован для указанного физического порта уровня 2.</p>
Interface	<p>Имя физического порта уровня 2, привязанного к зарезервированному IP-адресу. Формат записи имени интерфейса должен быть согласован с сокращенным форматом имени интерфейса на странице имени порта. Можно также использовать полное имя, например, "GigabitEthernet 1/32" или "10GigabitEthernet 1/4"</p>

 Уведомление:

Сначала следует настроить тип, IP и маску подсети пула адресов, а затем настраивать записи зарезервированных IP-адресов пула.

Настройка записей зарезервированных IP-адресов допускается только при типе пула адресов "Сеть", и зарезервированный IP-адрес должен находиться в пределах диапазона подсети пула адресов.

После настройки параметра "Только зарезервированные записи" необходимо настроить хотя бы один IP-адрес, иначе DHCP-сервер не будет выделять никаких IP.

Только когда тип пула адресов - "Хост", требуется использовать идентификатор клиента, аппаратный адрес и имя клиента; когда тип пула адресов - "Сеть", эти три атрибута настраивать не нужно.

### 9.2.1.4 Статистика

Страница статистики DHCP-сервера отображает статистику записей базы данных DHCP-сервера, статистику привязки записей и количество отправленных и полученных сообщений DHCP. Страница выглядит как показано на рисунке ниже.

**DHCP Server Statistics** Auto-refresh

**Database Counters**

Pool	Excluded IP Address	Declined IP Address
1	0	0

**Binding Counters**

Automatic Binding	Manual Binding	Expired Binding
0	0	0

**DHCP Message Received Counters**

DISCOVER	REQUEST	DECLINE	RELEASE	INFORM
0	0	0	0	0

**DHCP Message Sent Counters**

OFFER	ACK	NAK
0	0	0

Описание каждого параметра представлено в следующей таблице:

Параметр	Описание
Database statistics	<p>Отображается статистика различных баз данных DHCP-сервера.</p> <ul style="list-style-type: none"> <li>Пул адресов: количество пулов адресов.</li> <li>Не выделять IP: количество исключенных диапазонов IP-адресов.</li> <li>Отклоненные IP: количество отклоненных IP-адресов</li> </ul>
Binding statistics	<p>Отображается статистика количества различных привязок DHCP-сервера.</p> <ul style="list-style-type: none"> <li>Автоматическая привязка: количество автоматически связанных записей адресов в пуле адресов типа Network.</li> <li>Ручная привязка: количество записей привязки адресов, назначенных администратором клиенту в пуле адресов типа Host.</li> </ul>

Параметр	Описание
	<ul style="list-style-type: none"> <li>Срок действия привязки: количество записей привязки адресов, которые истекли срок аренды или были удалены из записей привязки автоматического/ручного типа.</li> </ul>
Received DHCP message statistics	<p>Отображение статистического числа DHCP-сообщений, полученных DHCP-сервером.</p> <ul style="list-style-type: none"> <li>Поиск: количество DHCP-сообщений DHCP-DISCOVER, полученных DHCP-сервером.</li> <li>Запрос: количество DHCP-сообщений DHCP-REQUEST, полученных DHCP-сервером.</li> <li>Отклонение: количество DHCP-сообщений DHCP-DECLINE, полученных DHCP-сервером.</li> <li>Освобождение: количество DHCP-сообщений DHCP-RELEASE, полученных DHCP-сервером.</li> <li>Уведомление: количество DHCP-сообщений DHCP-INFORM, полученных DHCP-сервером.</li> </ul>
Statistics on sending DHCP messages	<p>Отображается статистика количества отправленных DHCP-пакетов DHCP-сервером.</p> <ul style="list-style-type: none"> <li>Предложение: количество сообщений DHCP-OFFER, отправленных DHCP-сервером.</li> <li>Подтверждение: количество сообщений DHCP-ACK, отправленных DHCP-сервером.</li> <li>Не подтверждено: количество сообщений DHCP-NAK, отправленных DHCP-сервером.</li> </ul>

### 9.2.1.5 Привязать IP

Страница "Привязанные IP-адреса DHCP-сервера" отображает все записи о привязанных IP-адресах DHCP-сервера, как показано на рисунке ниже.

**DHCP Server Binding IP**      Auto-refresh     Refresh    Clear Selected    Clear Automatic    Clear Manual    Clear Expired

Binding IP Address

Delete	IP	Type	State	Pool Name	Server/Relay IP

Описание каждого параметра представлено в следующей таблице:

Параметр	Описание
Delete	Отметка в поле "Удалить" означает, что запись о привязанном IP-адресе в этой строке будет удалена.
IP	IP-адрес, назначенный DHCP-клиенту.

Параметр	Описание
Type	Тип привязки адреса. Возможные типы - автоматическая, ручная, просроченная.
State	Статус привязки адреса. Возможные статусы - отправлен, назначен, просрочен.
Address pool name	Имя пула адресов, к которому привязан IP-адрес.
Server/Relay IP	IP-адрес DHCP-сервера или агента ретрансляции, предоставившего IP

**Кнопка Очистить**

- Очистить выбранные: Нажмите, чтобы очистить отмеченную привязанную запись IP-адреса. Если выбранная привязка является автоматической или ручной, она изменится на просроченную. Если выбранная привязка просрочена, она будет освобождена.
- Очистить автоматически: Нажмите, чтобы очистить все автоматически привязанные записи IP-адресов и изменить их на просроченные привязки.
- Очистить ручные: Нажмите, чтобы очистить все ручные привязанные записи IP-адресов и изменить их на просроченные привязки.
- Очистить просроченные: Нажмите, чтобы очистить все просроченные записи IP-адресов и освободить их.

Щелкните любой IP-адрес в списке привязанных IP-адресов, и будет отображена страница данных о привязанных IP-адресах DHCP-сервера, как показано на рисунке ниже.

На верхнем левом углу страницы находится список опций привязки IP. Пользователи могут выбрать привязанный IP-адрес, соответствующий данным IP текущей страницы из выпадающего списка IP. По умолчанию отображается IP-адрес, на который пользователь щелкнул в списке привязанных IP-адресов.

IP 192.168.40.50

**Binding IP Data**

IP	192.168.40.50
Type	Automatic
State	Committed
Pool Name	pool1
Server/Relay IP	192.168.40.73
VLAN	1
Subnet Mask	255.255.255.0
Client ID Type	MAC
Client ID Value	00-02-b3-2e-80-5d
MAC Address	00-02-b3-2e-80-5d
Lease Time	1 minutes 0 seconds
Will Expired in	49 seconds

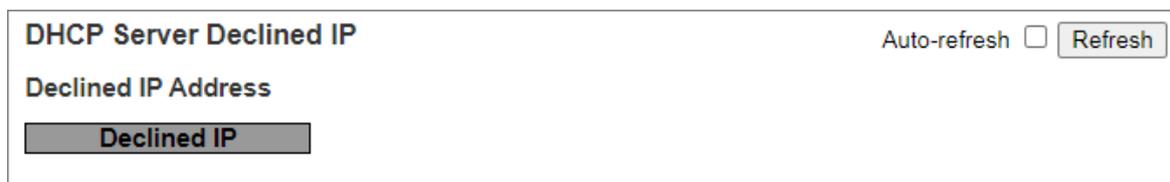
Описание каждого параметра представлено в следующей таблице:

Параметр	Описание
IP	IP-адрес, назначенный клиенту DHCP.
Type	Тип привязки адреса, включая автоматический, ручной и истекший.
State	Статус привязки адреса, включая использованный, выделенный и истекший.
Pool name	Название пула адресов, к которому относится привязанный IP.

Параметр	Описание
Server/relay IP	IP-адрес DHCP-сервера или агента ретрансляции, который предоставил IP.
VLAN	Идентификатор VLAN интерфейса DHCP-клиента.
Subnet mask	Маска подсети, назначенная DHCP-клиенту
Client ID type	Тип идентификатора клиента в опции 61 DHCP-клиента. Возможные типы: имя, MAC и "-". <ul style="list-style-type: none"> <li>"-": указывает на то, что DHCP-клиент не упаковывает опцию 61 в сообщение DHCP.</li> <li>Имя: указывает на то, что идентификатор клиента имеет тип, отличный от аппаратного.</li> <li>MAC: указывает на то, что тип идентификатора клиента - аппаратный MAC-адрес</li> </ul>
Client ID value	Значение идентификатора клиента в опции 61 DHCP-клиента.
MAC address	Аппаратный адрес в поле Chaddr сообщения DHCP клиента.
Lease period	Общее время аренды IP-адреса, привязанного к DHCP-клиенту.
Remaining lease term	Оставшееся время аренды IP-адреса, привязанного к DHCP-клиенту

### 9.2.1.6 Отказ в выделении IP-адреса

Когда клиент обнаруживает, что присвоенный ему сервером IP-адрес конфликтует, он уведомляет сервер, отправляя сообщение DHCP-DECLINE, и повторно запрашивает адрес у сервера. Страница DHCP-сервера "Отказ в выделении IP-адреса" отображает все записи IP-адресов, отклоненные DHCP-клиентом, как показано на рисунке ниже.



Описание каждого параметра представлено в следующей таблице:

Параметр	Описание
Deny IP	IP-адрес, который был отклонен DHCP-клиентом

## 9.2.2 Отслеживание DHCPv4

Протокол DHCP работает на основе протоколов UDP и IP и имеет множество уязвимостей. Более того, в механизме работы DHCP обычно отсутствует механизм аутентификации между сервером и клиентом. Если на сети присутствует несколько DHCP-серверов, это может вызвать путаницу в сети. Например, злоумышленники могут выдавать неправильные IP-адреса, информацию о DNS-сервере или информацию о шлюзе по умолчанию, перехватывая трафик и так далее.

Отслеживание DHCP (DHCP Snooping) - это функция безопасности DHCP, которая обладает следующими функциями:

Основная функция прослушивания DHCP Snooping

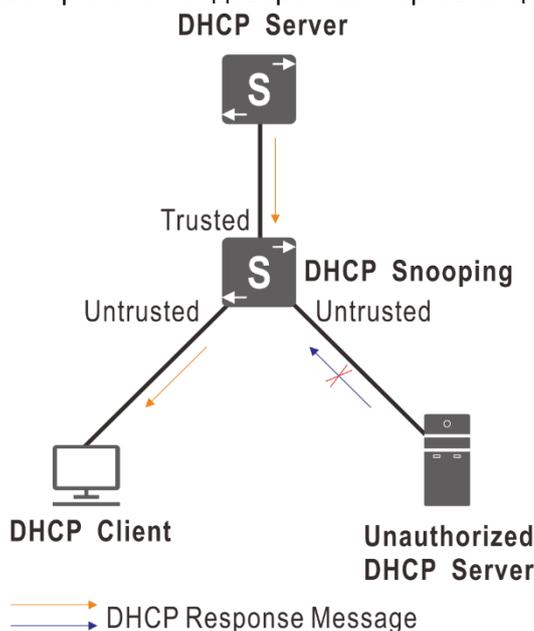
- DHCP Snooping является функцией прослушивания уровня 2 службы DHCP. В целях безопасности отделу безопасности необходимо регистрировать IP-адрес, используемый пользователем при выходе в Интернет, и подтверждать соответствие между IP-адресом, запрошенным пользователем, и MAC-адресом используемого им хоста. В таких случаях можно использовать функцию DHCP Snooping для отслеживания полученных сообщений DHCP-REQUEST и DHCP-ACK, извлечения и записи информации об IP-адресе, полученной пользователем.
- Функция доверия DHCP Snooping

Функция доверия DHCP Snooping может контролировать источник сообщений ответа DHCP-сервера, чтобы предотвратить выдачу IP-адресов и другой конфигурационной информации другим хостам, которые могут существовать в сети, от фальшивых или нелегальных DHCP-серверов.

Функция доверия DHCP Snooping разделяет порты на доверенные и недоверенные порты:

- Доверенный порт: Порт, подключенный напрямую или косвенно к легитимному DHCP-серверу. Доверенный порт пересылает полученные сообщения DHCP нормально, тем самым обеспечивая получение DHCP-клиентом правильного IP-адреса.
- Недоверенный порт: Порт, не подключенный к легитимному DHCP-серверу. Сообщения DHCP-ACK, DHCP-NAK и DHCP-OFFER, полученные с недоверенного порта от ответа DHCP-сервера, будут отброшены, что предотвращает получение DHCP-клиентом неправильного IP-адреса.

Типичные применения доверенных портов следующие:



### 9.2.2.1 Настройка прослушивания

Страница конфигурации DHCP Snooping показана на рисунке ниже..

**DHCP Snooping Configuration**

Snooping Mode

**Port Mode Configuration**

Port	Mode
*	<>
1	Trusted
2	Trusted
3	Trusted
4	Trusted
5	Trusted
6	Trusted
7	Trusted
8	Trusted
9	Trusted
10	Trusted
11	Trusted
12	Trusted
13	Trusted
14	Trusted
15	Trusted
16	Trusted
17	Trusted
18	Trusted

Описание каждого параметра представлено в следующей таблице:

Параметр	Описание
Snooping mode	<p>Выберите режим прослушивания DHCP.</p> <ul style="list-style-type: none"> <li>Включить: включить функцию DHCP Snooping. Когда функция DHCP Snooping включена, сообщения запроса DHCP будут перенаправляться на доверенные порты, и только ответные пакеты с доверенных портов разрешается получать.</li> <li>Отключить: отключить функцию DHCP Snooping.</li> </ul>
<b>Port mode configuration</b>	<b>Конфигурация режима порта.</b>
Port	Номер порта устройства.
Mode	<p>Выберите режим доверия порта DHCP.</p> <ul style="list-style-type: none"> <li>Доверенный: Настройте порт как доверенный источник сообщений DHCP.</li> <li>Недоверенный: Настройте порт как недоверенный источник сообщений DHCP</li> </ul>

**9.2.2.2 Таблица прослушивания**

На странице статуса DHCP Snooping, показанной на рисунке ниже, отображается информация о динамическом выделении IP-адресов, прослушиваемых на устройстве после включения функции DHCP Snooping. Динамическая таблица DHCP Snooping на этой странице будет содержать динамические IP-адреса, полученные всеми клиентами DHCP, подключенными к устройству через доверенный DHCP-сервер через устройство.

**Dynamic DHCP Snooping Table** Auto-refresh  Refresh |<< >>

Start from MAC address  , VLAN  with  entries per page.

MAC Address	VLAN ID	Source Port	IP Address	IP Subnet Mask	DHCP Server
No more entries					

Описание каждого параметра представлено в следующей таблице:

Параметр	Описание
MAC address	MAC-адрес DHCP-клиента.
VLAN ID	Идентификатор VLAN, где находится DHCP-клиент.
Source port	Номер локального порта на устройстве прослушивания DHCP, который принимает сообщения клиента.
IP address	IP-адрес, назначенный клиенту.
IP subnet mask	Маска подсети IP, назначенная клиенту.
DHCP server	Адрес DHCP-сервера, который назначает IP-адрес клиенту

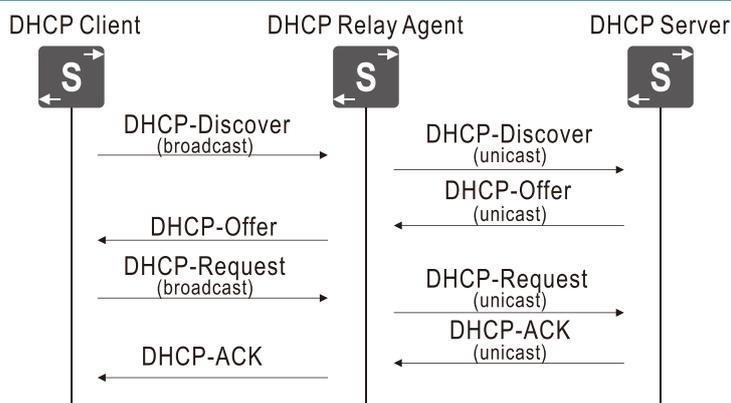
Динамическая таблица DHCP Snooping поддерживает отображение по страницам. Каждая страница может содержать до 99 записей. По умолчанию установлено значение 20. Пользователь может установить количество записей, отображаемых на каждой странице, в поле ввода числа записей на странице. Пользователь также может установить MAC-адрес и идентификатор VLAN, совпадающие с первой записью DHCP Snooping, которая будет отображаться, в соответствующих полях ввода для начального MAC-адреса и начального VLAN, затем щелкнуть кнопку "Обновить", и страница будет отображаться в обратном порядке, начиная с совпадающей записи DHCP Snooping.

**Уведомление:**

Легальный порт DHCP-сервера должен быть установлен как доверенный порт. В противном случае ответное сообщение DHCP не будет проходить через устройство, что приведет к невозможности получить ПК IP-адрес.

### 9.2.3 Перенаправление DHCPv4

Исходный протокол DHCP требует, чтобы клиент и сервер находились только в одной подсети и не могли работать через сегменты сети. Поэтому для динамической конфигурации хостов необходимо настраивать DHCP-сервер на всех сегментах сети, что очевидно нерационально. Введение DHCP Relay (перенаправление DHCP) решает эту проблему. Он предоставляет услуги ретрансляции между DHCP-клиентами и серверами в разных сегментах сети, перенаправляя сообщения протокола DHCP через сегменты сети к целевому DHCP-серверу. DHCP-клиенты могут взаимодействовать с DHCP-сервером.



Процесс работы DHCP Relay показан на рисунке выше. DHCP-клиент отправляет сообщение запроса DHCP-серверу. После того как DHCP Relay получает сообщение и обрабатывает его соответствующим образом, он отправляет его на указанный DHCP-сервер, расположенный на других сегментах сети. Сервер возвращает конфигурационную информацию клиенту через DHCP Relay на основе необходимой информации, предоставленной в запросе, чтобы завершить динамическую конфигурацию клиента.

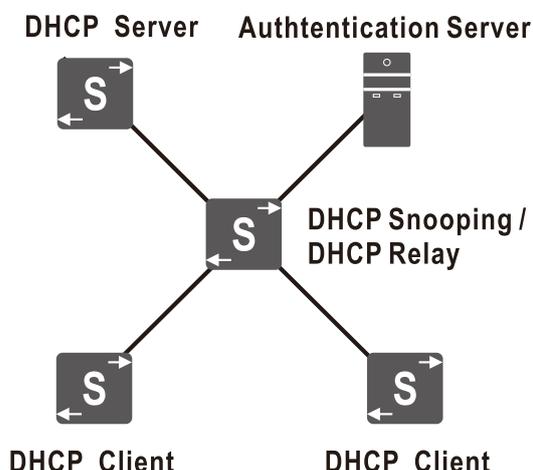
### Опция информации ретранслятора (Option 82)

В традиционном методе DHCP для динамического выделения IP-адресов пользователи в одной и той же VLAN имеют точно такие же права на получение IP-адресов. Сетевым администраторам нельзя эффективно управлять конкретными пользователями в одной и той же VLAN. Обычные агенты ретрансляции DHCP не поддерживают опцию 82 (опция информации ретранслятора DHCP) и не могут различать различных клиентов. Поэтому невозможно сочетать применение DHCP для динамического выделения IP-адресов с контролем доступа клиента к сетевым ресурсам, что представляет собой серьезное вызов для контроля безопасности сети.

RFC 3046 определяет опцию информации ретранслятора DHCP (опцию 82), которая записывает информацию о местоположении DHCP-клиента. Администраторы могут использовать эту опцию для определения местоположения DHCP-клиентов для контроля безопасности и учета клиентов.

Если ретранслятор DHCP поддерживает функцию опции 82, при получении сообщения запроса DHCP ретранслятор DHCP обрабатывает сообщение в соответствии с наличием в сообщении опции 82 и настроенной политикой обработки, а затем пересылает обработанное сообщение DHCP-серверу. Если ответное сообщение, полученное ретранслятором DHCP, содержит опцию 82, он удалит опцию 82 и затем переслестит его DHCP-клиенту.

Опция 82 содержит две подопции: идентификатор цепи (подопция 1) и удаленный идентификатор (подопция 2). Процесс работы показан на рисунке ниже:



1. Перед тем, как пользователь получит динамический IP-адрес, только пакеты DHCP могут проходить через устройство DHCP Snooping / DHCP Relay.
2. После того как сообщение DHCP-DISCOVER, отправленное клиентом, достигает устройства DHCP Snooping / DHCP Relay, устройство DHCP Snooping / DHCP Relay включает информацию о местоположении клиента в опцию 82 и пересылает сообщение DHCP-DISCOVER на сервер.
3. DHCP-сервер, поддерживающий политику выделения адресов DHCP Option 82, выделяет соответствующий IP-адрес пользователю в соответствии с опцией 82 и отвечает сообщением DHCP-OFFER, содержащим исходную информацию опции 82.
4. Устройство DHCP Snooping / DHCP Relay удаляет опцию 82 из ответного сообщения и отправляет ответное сообщение клиенту.
5. После того как сообщение DHCP-REQUEST, отправленное клиентом, достигает устройства DHCP Snooping / DHCP Relay, устройство DHCP Snooping / DHCP Relay включает информацию о местоположении клиента в опцию 82 и пересылает сообщение DHCP-REQUEST на сервер.
6. DHCP-сервер, поддерживающий политику выделения адресов DHCP Option 82, отвечает DHCP-ACK, содержащим исходную информацию опции 82 в сообщении.
7. Устройство DHCP Snooping / DHCP Relay удаляет опцию 82 из сообщения DHCP-ACK и отправляет сообщение DHCP-ACK клиенту.

Сочетая опцию 82 с DHCP-сервером, поддерживающим политику выделения адресов по опции 82, можно использовать подопции Circuit ID и Remote ID опции 82 для выделения разных IP-адресов пользователям на основе разных прав доступа пользователей. С одной стороны, это позволяет более точно управлять IP-адресами; с другой стороны, это позволяет устройству выполнять маршрутизацию по политике "исходного IP-адреса", чтобы пользователи с разными IP-адресами имели разные правила маршрутизации.

### 9.2.3.1 Конфигурация реле

Агенты реле DHCP используются для пересылки и передачи сообщений DHCP между клиентами и серверами в различных подсетевых доменах. Они сохраняют IP-адрес входного интерфейса в поле GIADDR пакета DHCP. DHCP-сервер может использовать значение поля GIADDR для определения назначенной подсети. В этом случае убедитесь, что IP-адрес интерфейса VLAN коммутатора и PVID (идентификатор VLAN по умолчанию для порта) сконфигурированы правильно.

На рисунке ниже показана страница конфигурации реле DHCP.

#### DHCP Relay Configuration

<b>Relay Mode</b>	Disabled ▾
<b>Relay Server</b>	0.0.0.0
<b>Relay Information Mode</b>	Disabled ▾
<b>Relay Information Policy</b>	Keep ▾

Описание каждого параметра представлено в следующей таблице:

Параметр	Описание
Relay mode	Выберите режим включения реле DHCP. По умолчанию функция реле DHCP отключена.

Параметр	Описание
	<ul style="list-style-type: none"> <li>Включить: Включить функцию реле DHCP на коммутаторе. Когда функция реле DHCP включена, коммутатор действует как агент реле DHCP и отвечает за пересылку и передачу сообщений DHCP между клиентами и серверами в различных подсетях. В целях безопасности широковещательные сообщения DHCP не передаются.</li> <li>Отключить: Отключить функцию реле DHCP на коммутаторе</li> </ul>
Relay server	Введите IP-адрес DHCP-сервера реле. По умолчанию этот элемент не указан.
Relay message mode	<p>Выберите, поддерживать ли опцию информации агента реле DHCP Option 82. По умолчанию опция информации агента реле DHCP Option 82 отключена.</p> <ul style="list-style-type: none"> <li>Включить: включить опцию информации агента реле DHCP.</li> <li>Отключить: отключить опцию информации агента реле DHCP.</li> </ul>
Relay message strategy	<p>Выберите политику обработки опции информации агента реле DHCP. По умолчанию политика для опции информации агента реле DHCP сохранена.</p> <ul style="list-style-type: none"> <li>Замена: когда полученное сообщение запроса DHCP содержит опцию 82, исходная информация опции 82 в сообщении заменяется и пересылается.</li> <li>Сохранение: когда полученное сообщение запроса DHCP содержит опцию 82, исходная информация опции 82 в сообщении сохраняется и пересылается без изменений.</li> <li>Отбросить: когда полученное сообщение запроса DHCP содержит опцию 82, отбросить сообщение.</li> </ul>

 **Уведомление:**

Когда DHCP-клиент получает IP-адрес через реле DHCP, DHCP-сервер должен быть сконфигурирован с пулом адресов, который полностью совпадает с сегментом сети (сетевым номером и маской) IP-адреса интерфейса, к которому подключено реле DHCP для соединения с DHCP-клиентом. В противном случае DHCP-клиент не сможет получить правильный IP-адрес.

Опция информации агента реле DHCP может начать действовать только после включения функции реле DHCP.

### 9.2.3.2 Статистика ретрансляции

На странице статистики реле DHCP, показанной на рисунке ниже.

DHCP Relay Statistics								Auto-refresh <input type="checkbox"/>	Refresh	Clear
Server Statistics										
Transmit to Server	Transmit Error	Receive from Server	Receive Missing Agent Option	Receive Missing Circuit ID	Receive Missing Remote ID	Receive Bad Circuit ID	Receive Bad Remote ID			
0	0	0	0	0	0	0	0			
Client Statistics										
Transmit to Client	Transmit Error	Receive from Client	Receive Agent Option	Replace Agent Option	Keep Agent Option	Drop Agent Option				
0	0	0	0	0	0	0				

Описание каждого параметра представлено в следующей таблице:

Параметр	Описание
<b>Server statistics</b>	<b>Статистика сервера:</b>
Send to server	Количество ретранслированных сообщений от клиента к серверу.
Send Error	Количество отправленных сообщений об ошибках клиенту.
Receive from server	Количество сообщений, полученных от сервера.
Receive option missing message	Количество полученных пакетов без опции информации агента реле.
Receive circuit ID missing message	Количество полученных сообщений без опции идентификатора цепи.
Receive Remote ID missing message	Количество полученных пакетов без опции удаленного идентификатора.
Receive Circuit ID error message	Количество полученных пакетов с неизвестной опцией идентификатора цепи.
Receive Remote ID error message	Количество полученных пакетов с неизвестной опцией удаленного идентификатора.
<b>Client statistics</b>	<b>Статистика клиента:</b>
Send to client	Количество ретранслированных сообщений от сервера к клиенту.
Send Error	Количество отправленных сообщений об ошибках серверу.
Receive from client	Количество сообщений, полученных от клиента.
Receive option	Количество полученных сообщений, содержащих опции информации агента реле.
Replace option	Количество полученных пакетов, заменяющих опцию информации агента реле.
Keep option	Количество полученных сообщений, сохраняющих опцию информации агента реле.
Discard option	Количество отброшенных пакетов, содержащих опции информации агента реле.

### 9.2.4 Детализированная статистика DHCP

Страница детальной статистики DHCP отображает подробную информацию о пакетах DHCP, отправленных и полученных каждым портом коммутатора в различных режимах работы DHCP. На странице показано на рисунке ниже.

DHCP Detailed Statistics Port 1			
		Combined	Port 1
		Auto-refresh	Refresh Clear
Receive Packets		Transmit Packets	
Rx Discover	0	Tx Discover	0
Rx Offer	0	Tx Offer	0
Rx Request	0	Tx Request	0
Rx Decline	0	Tx Decline	0
Rx ACK	0	Tx ACK	0
Rx NAK	0	Tx NAK	0
Rx Release	0	Tx Release	0
Rx Inform	0	Tx Inform	0
Rx Lease Query	0	Tx Lease Query	0
Rx Lease Unassigned	0	Tx Lease Unassigned	0
Rx Lease Unknown	0	Tx Lease Unknown	0
Rx Lease Active	0	Tx Lease Active	0
Rx Discarded Checksum Error	0		
Rx Discarded from Untrusted	0		

В верхнем левом углу страницы, за заголовком "DHCP Detailed Statistics", будет отмечен номер порта, соответствующий таблице статистики DHCP-пакетов текущей страницы.

В верхнем правом углу страницы предоставлен ряд элементов управления удалением и операциями с таблицей данных, слева направо:

- Поле выбора режима работы DHCP: Выберите режим работы коммутатора. Доступно несколько типов: смешанный, нормальный режим, серверный, клиентский, прослушивание и реле. По умолчанию выбран смешанный режим, то есть текущая страница отображает статистику пакетов коммутатора во всех режимах работы DHCP.
- Поле выбора номера порта: Выберите номер порта, соответствующий таблице статистики сообщений DHCP на текущей странице. По умолчанию выбран порт 1, то есть в данный момент отображается статистика DHCP-пакетов порта 1..

Внизу страницы отображается отфильтрованная таблица детализированной статистики DHCP, которая содержит следующие типы сообщений DHCP:

Параметр	Описание
RX/TX Discover	Количество полученных/отправленных сообщений DHCP обнаружения (опция 53 имеет значение 1).
RX/TX Offer	Количество полученных/отправленных сообщений DHCP предложения (значение 2 для опции 53).
RX/TX Request	Количество полученных/отправленных сообщений DHCP запроса (опция 53 имеет значение 3).
RX/TX Decline	Количество полученных/отправленных сообщений DHCP отклонения (значение 4 для опции 53).
RX/TX ACK	Количество полученных/отправленных сообщений DHCP подтверждения (опция 53 имеет значение 5).
RX/TX NAK	Количество полученных/отправленных сообщений DHCP без подтверждения (значение 6 для опции 53).
RX/TX Release	Количество полученных/отправленных сообщений DHCP освобождения (опция 53 имеет значение 7).
RX/TX Inform	Количество полученных/отправленных сообщений DHCP уведомления (значение 8 для опции 53).
RX/TX Lease Query	Количество полученных/отправленных сообщений DHCP запроса аренды (опция 53 имеет значение 10).
Rx/TX Lease Unassigned	Количество полученных/отправленных сообщений DHCP отказа аренды (значение 11 для опции 53).

Параметр	Описание
RX/TX Lease Unknown	Количество полученных/отправленных сообщений DHCP неизвестной аренды (значение 12 для опции 53).
RX/TX Lease Active	Количество полученных/отправленных сообщений DHCP активной аренды (значение 13 для опции 53).
RX Discarded Checksum Error	Количество отброшенных входящих пакетов из-за ошибок IP/UDP-контрольной суммы.
RX Discarded from Untrusted	Количество отброшенных входящих пакетов из-за их происхождения из ненадежных портов

 Уведомление:

Отброшенные ненадежные пакеты, отвергнутые RX, действительны только в режиме прослушивания DHCP и смешанном режиме.

Если входящий поток пакетов DHCP осуществляется через механизм L3-пересылки, стандартная статистика TX каждого порта не будет увеличиваться, и очистка статистики определенного порта может не повлиять на общую статистику, поскольку они собирают различные данные уровня.

### 9.3 NTP

Network Time Protocol (NTP) является протоколом прикладного уровня в наборе протоколов TCP/IP. NTP используется для синхронизации часов между рядом распределенных серверов времени и клиентов. Реализация NTP основана на протоколах IP и UDP. Сообщения NTP передаются через UDP, а номер порта составляет 123.

По мере усложнения топологии сети синхронизация часов устройств во всей сети становится очень важной. Если администратору приходится вручную изменять системные часы, то не только рабочая нагрузка огромна, но и точность часов не гарантируется. Возникновение NTP направлено на решение проблемы синхронизации системных часов устройств в сети. NTP в основном используется в ситуациях, когда часы всех устройств в сети должны быть согласованы.

Настройка NTP показана на рисунке ниже.

**NTP Configuration**

<b>Mode</b>	Disabled <span style="float: right;">▼</span>
<b>Server 1</b>	<input type="text"/>
<b>Server 2</b>	<input type="text"/>
<b>Server 3</b>	<input type="text"/>
<b>Server 4</b>	<input type="text"/>
<b>Server 5</b>	<input type="text"/>

Описание каждого параметра представлено в следующей таблице:

Параметр	Описание
Mode	Список раскрывающегося меню "Включить NTP" содержит следующие варианты: <ul style="list-style-type: none"><li>• Включить: Включить функцию NTP;</li><li>• Отключить: Отключить функцию NTP.</li></ul>
Server 1-5	Адреса или доменные имена серверов NTP (1-5)

## 9.4 Время

Разделение часовых поясов мира основано на меридиане. От 7,5° западной долготы до 7,5° восточной долготы (интервал долготы составляет 15°) - это нулевая зона. От двух границ нулевого часового пояса на восток и на запад соответственно каждые 15° долготы делится часовой пояс. В восточном и западном направлениях есть 12 часовых поясов. 12 восточных часовых поясов совпадают с 12 западными часовыми поясами; мир разделен на 24 часовых пояса. В каждом часовом поясе используется местное среднее солнечное время на центральном меридиане как стандартное время пояса. Стандартная разница во времени между двумя соседними часовыми поясами составляет один час. В принципе, границы часовых поясов делятся в соответствии с географическими линиями долготы, но в конкретной реализации они часто определяются на основе административных границ или природных границ каждой страны для удобства использования. Устройство может выбирать соответствующие часовые пояса на основе типичных регионов, и устройство автоматически корректирует внутренний сдвиг времени на основе выбранного часового пояса.

Страница настройки времени показана на рисунке ниже.

### Time Zone Configuration

Time Zone Configuration	
Time Zone	(UTC) Coordinated Universal Time <span style="float: right;">▼</span>
Hours	0 <span style="float: right;">▼</span>
Minutes	0 <span style="float: right;">▼</span>
Acronym	<input type="text"/> ( 0 - 16 characters )

### Daylight Saving Time Configuration

Daylight Saving Time Mode	
Daylight Saving Time	Disabled <span style="float: right;">▼</span>

Start Time settings	
Month	Jan <span style="float: right;">▼</span>
Date	1 <span style="float: right;">▼</span>
Year	2014 <span style="float: right;">▼</span>
Hours	0 <span style="float: right;">▼</span>
Minutes	0 <span style="float: right;">▼</span>

End Time settings	
Month	Jan <span style="float: right;">▼</span>
Date	1 <span style="float: right;">▼</span>
Year	2097 <span style="float: right;">▼</span>
Hours	0 <span style="float: right;">▼</span>
Minutes	0 <span style="float: right;">▼</span>

Offset settings	
Offset	1 <span style="float: right;">( 1 - 1439) Minutes</span>

Описание каждого параметра представлено в следующей таблице:

Параметр	Описание
Time zone configuration	Конфигурация часового пояса.
Time zone	Смещение часового пояса в часах.
Hour	Смещение часового пояса в минутах.
Minute	Наименование по вашему выбору.
Abbreviation	Режим летнего времени
Daylight saving time mode	Конфигурация часового пояса.
Summer time	Летнее время включено, варианты следующие: <ul style="list-style-type: none"> <li>Отключить: Отключить переход на летнее время, следующие настройки не могут быть сконфигурированы при отключенном режиме.</li> <li>Цикл: Период с начала перехода на летнее время до его окончания каждый год.</li> <li>Нециклический: Весь период времени от начала перехода на летнее время до его окончания</li> </ul>
Start/end time settings	Годичный период начала/окончания перехода на летнее время.  Циклическое летнее время:

Параметр	Описание
	<ul style="list-style-type: none"> <li>Неделя: Неделя начала/окончания перехода на летнее время.</li> <li>День: День начала/окончания перехода на летнее время.</li> <li>Месяц: Месяц начала/окончания перехода на летнее время.</li> <li>Час: Время начала/окончания перехода на летнее время (час).</li> <li>Минуты: Время начала/окончания перехода на летнее время (минуты).</li> </ul> <p>Нециклическое летнее время:</p> <ul style="list-style-type: none"> <li>Месяц: Месяц начала/окончания перехода на летнее время.</li> <li>День: День начала/окончания перехода на летнее время.</li> <li>Год: Год начала/окончания перехода на летнее время.</li> <li>Час: Время начала/окончания перехода на летнее время (час).</li> <li>Минуты: Время начала/окончания перехода на летнее время (минуты)</li> </ul>
Bias setting	Смещение: Временное смещение

## 9.5 Журнал

Устройство предоставляет функцию журнала для ссылки пользователей, которые могут столкнуться с проблемами настройки. Журналы разделены на разные уровни: ошибка, предупреждение, уведомление и информация. Записи в журнале можно отображать и очищать по уровням, и уровень можно выбрать для загрузки журналов на сервер журналов.

### 9.5.1 Конфигурация журнала

Страница конфигурации журнала выглядит следующим образом, как показано на рисунке ниже.

**System Log Configuration**

<b>Server Mode</b>	Disabled <span style="float: right;">▼</span>
<b>Server Address</b>	<input type="text"/>
<b>Syslog Level</b>	Informational <span style="float: right;">▼</span>

Описание каждого параметра представлено в следующей таблице:

Параметр	Описание
Server mode	Режим сервера, указывающий режим работы сервера. При включении режима схемы сообщения Syslog отправляются на сервер Syslog. Протокол Syslog основан на UDP-коммуникации и принимается на UDP-порту 514, и сервер Syslog не будет отправлять подтверждение отправителю, потому что UDP является безсоединительным протоколом и не предоставляет подтверждения. Пакеты Syslog всегда будут отправляться, даже если сервер Syslog не существует.
Server address	Адрес сервера, указывающий IPv4-адрес хоста сервера Syslog. Если коммутатор предоставляет функциональность DNS, это также может быть доменное имя
Log level	Уровень Syslog, указывающий, какие сообщения будут отправлены на сервер Syslog. Возможные шаблоны: <ul style="list-style-type: none"> <li>• Ошибка: Отправляет конкретное сообщение с кодом серьезности меньше Ошибка (3).</li> <li>• Предупреждение: Отправляет конкретное сообщение, код серьезности которого меньше или равен Предупреждению (4).</li> <li>• Уведомление: Отправляет конкретное сообщение с кодом серьезности меньше или равным Уведомлению (5).</li> <li>• Информационное: Отправляет конкретное сообщение с кодом серьезности меньше Информационного (6)</li> </ul>

## 9.5.2 Информация о журнале

Страница информации о журнале выглядит следующим образом, как показано на рисунке ниже.

**System Log Information** Auto-refresh  Refresh Clear << >> >>>

Level: All Clear Level: All

The total number of entries is 20 for the given level.

Start from ID  with  entries per page.

ID	Level	Time	Message
1	Informational	2023-06-30T14:49:34+00:00	SYS-BOOTING: Switch just made a cool boot.
2	Notice	2023-06-30T14:49:35+00:00	LINK-UPDOWN: IP Interface VLAN 1 changed state to down.
3	Notice	2023-06-30T14:49:35+00:00	LINK-UPDOWN: IP Interface VLAN 1 changed state to down.
4	Notice	2023-06-30T14:49:39+00:00	LINK-UPDOWN: Interface GigabitEthernet 1/1, changed state to up.
5	Notice	2023-06-30T14:49:40+00:00	LINK-UPDOWN: IP Interface VLAN 1 changed state to up.
6	Notice	2023-06-30T14:55:49+00:00	LINK-UPDOWN: IP Interface VLAN 1 changed state to up.
7	Notice	2023-06-30T16:23:58+00:00	LINK-UPDOWN: Interface GigabitEthernet 1/1, changed state to down.
8	Notice	2023-06-30T16:24:00+00:00	LINK-UPDOWN: IP Interface VLAN 1 changed state to down.
9	Notice	2023-06-30T16:24:03+00:00	LINK-UPDOWN: Interface GigabitEthernet 1/1, changed state to up.
10	Notice	2023-06-30T16:24:04+00:00	LINK-UPDOWN: Interface GigabitEthernet 1/1, changed state to down.
11	Notice	2023-06-30T16:24:10+00:00	LINK-UPDOWN: Interface GigabitEthernet 1/1, changed state to up.
12	Notice	2023-06-30T16:24:15+00:00	LINK-UPDOWN: IP Interface VLAN 1 changed state to up.
13	Notice	2023-06-30T16:24:15+00:00	LINK-UPDOWN: Interface GigabitEthernet 1/1, changed state to down.
14	Notice	2023-06-30T16:24:18+00:00	LINK-UPDOWN: IP Interface VLAN 1 changed state to down.
15	Notice	2023-06-30T16:24:18+00:00	LINK-UPDOWN: Interface GigabitEthernet 1/1, changed state to up.
16	Notice	2023-06-30T16:24:24+00:00	LINK-UPDOWN: IP Interface VLAN 1 changed state to up.
17	Notice	2023-06-30T16:24:40+00:00	LINK-UPDOWN: Interface GigabitEthernet 1/1, changed state to down.
18	Notice	2023-06-30T16:24:42+00:00	LINK-UPDOWN: IP Interface VLAN 1 changed state to down.
19	Notice	2023-06-30T16:24:44+00:00	LINK-UPDOWN: Interface GigabitEthernet 1/1, changed state to up.
20	Notice	2023-06-30T16:24:48+00:00	LINK-UPDOWN: IP Interface VLAN 1 changed state to up.

Описание каждого параметра представлено в следующей таблице:

Параметр	Описание
Grade	Используется для фильтрации отображаемых записей системного журнала.
Clear level	Используется для указания, какие записи системного журнала будут удалены. Чтобы очистить определенный уровень записей системного журнала, выберите уровень для очистки, а затем нажмите кнопку "Очистить".
ID	Идентификатор записи системного журнала.
Grade	Уровень записи системного журнала.
Time	Время возникновения записи системного журнала.
Information	Подробное сообщение записи системного журнала

### Кнопки

- Начальный ID: Поле ввода начального ID позволяет пользователю изменить точку начала отображаемых элементов, то есть с какого элемента начать отображение. Если ID существует, он будет отображаться, начиная с записи с этим ID. Если ID не существует, отображение начнется с ближайшей к нему следующей записи. После ввода нажмите кнопку "Обновить", чтобы изменения вступили в силу.
- Страница: измените количество записей, отображаемых на странице, через поле ввода количества страниц. Можно отображать до 999 записей на странице.
- Автоматическое обновление: когда выбран флажок "Автоматическое обновление", страница будет автоматически обновляться каждые 3 секунды.
- Обновить: Нажмите кнопку "Обновить", чтобы обновить записи таблицы, начиная с текущей записи.
- Очистить: Нажмите кнопку "Очистить", чтобы удалить записи на основе выбранного уровня очистки.
- |<<: Обновить записи таблицы, начиная с первой доступной записи.
- <<: Обновить записи таблицы, с текущей первой отображаемой записи в качестве конечной.
- >>: Обновить записи таблицы, с последней текущей отображаемой записи в качестве начальной.
- >>|: Обновить записи таблицы, с последней доступной записи в качестве конечной.



Уведомление:

Четыре кнопки "|<<, <<, >>, >>|" немного отличаются от обычно мыслимых кнопок "домашняя страница", "предыдущая страница", "следующая страница" и "последняя страница".

### 9.5.3 Подробные журналы

Страница подробного журнала выглядит следующим образом, как показано на рисунке ниже.

**Detailed System Log Information** Refresh | << << >> >>|

ID

**Message**

Level	Informational
Time	2023-06-30T14:49:34+00:00
Message	SYS-BOOTING: Switch just made a cool boot.

Описание каждого параметра представлено в следующей таблице:

Параметр	Описание
ID	Идентификатор записи журнала. Вы можете ввести идентификатор и нажать кнопку "Обновить", чтобы отобразить информацию о конкретной записи.

### Кнопки

- Обновить: обновить запись системного журнала до текущего идентификатора записи.
- |<<: Обновить запись системного журнала до первого доступного идентификатора записи.
- <<: Обновить запись системного журнала до предыдущего доступного идентификатора записи.
- >>: Обновить запись системного журнала до следующего доступного идентификатора записи.
- >>|: Обновить запись системного журнала до последнего доступного идентификатора записи.

## 9.6 Управление файлами конфигурации

Эта серия коммутаторов хранит множество файлов конфигурации в формате CLI. Некоторые из них являются виртуальными файлами (основанными на ОЗУ), а некоторые хранятся во Flash-памяти коммутатора. Эти файлы конфигурации включают:

- Running configuration (running-config): Виртуальный файл, отражающий текущую активную конфигурацию коммутатора. Он хранится в ОЗУ коммутатора в бинарном формате и легко теряется.
- Startup configuration (startup-config): Файл конфигурации, считываемый коммутатором при запуске. Если этот файл не существует при запуске, коммутатор запустится с конфигурацией по умолчанию. Этот файл хранится во Flash-памяти коммутатора.
- Default configuration (default-config): Файл только для чтения, содержащий поставщик-специфическую конфигурацию. Этот файл используется для восстановления системы к заводской конфигурации или когда файл startup-конфигурации отсутствует после запуска системы, он хранится во Flash-памяти коммутатора.
- Пользовательская конфигурация (имя пользовательского файла): Система может сохранять до 31 пользовательского файла конфигурации, которые специально используются для резервного копирования конфигурации или переключения конфигурации и хранятся во Flash-памяти коммутатора.

### 9.6.1 Сохранить как конфигурацию при запуске

На странице "Сохранить конфигурацию при запуске" отображается следующее, как показано на рисунке ниже.

**Save Running Configuration to startup-config**

Please note: The generation of the configuration file may be time consuming, depending on the amount of non-default configuration.

Save Configuration

Описание каждого параметра представлено в следующей таблице:

Параметр	Описание
Save configuration	Сохранить текущую рабочую конфигурацию системы в качестве конфигурации при запуске, чтобы гарантировать использование текущей активной конфигурации при следующем запуске системы

 Уведомление:

Чем больше нетиповых конфигураций, тем больше времени потребуется на создание файла конфигурации.

### 9.6.2 Скачать

Вы можете загрузить любой файл конфигурации на коммутаторе на локальный компьютер через браузер. Страница загрузки конфигурации показана на рисунке ниже.

**Download Configuration**

Select configuration file to save.

Please note: running-config may take a while to prepare for download.

File Name
<input type="radio"/> running-config
<input type="radio"/> default-config
<input type="radio"/> startup-config

Download Configuration

Описание каждого параметра представлено в следующей таблице:

Параметр	Описание
File name	Имя загружаемого файла конфигурации на коммутаторе.
Download configuration	После выбора имени файла из списка имен файлов нажмите кнопку "Загрузить конфигурацию", чтобы загрузить файл конфигурации с соответствующим именем с коммутатора в указанный путь сохранения файла в текущем браузере

 Уведомление:

Перед загрузкой текущей рабочей конфигурации необходимо сгенерировать файл конфигурации, поэтому это потребует дополнительного времени.

### 9.6.3 Загрузка

Вы можете загрузить локальный файл конфигурации на коммутатор через браузер, чтобы обновить текущую рабочую конфигурацию коммутатора или сохранить его как файл конфигурации без установленных по умолчанию на коммутаторе. Страница загрузки конфигурации показана на рисунке ниже.

**Upload Configuration**

**File To Upload**

No file chosen

**Destination File**

File Name	Parameters
<input type="radio"/> running-config	<input checked="" type="radio"/> Replace <input type="radio"/> Merge
<input type="radio"/> startup-config	
<input type="radio"/> Create new file	<input style="width: 100%;" type="text"/>

Описание каждого параметра представлено в следующей таблице:

Параметр	Описание
<b>Uploaded file</b>	<b>Загруженный файл</b>
Select a document	Нажмите кнопку "Выбрать файл", чтобы выбрать локальный файл конфигурации для загрузки. После выбора будет отображено имя выбранного файла за кнопкой.
<b>Destination file</b>	<b>Целевой файл</b>
File name	Имя целевого файла конфигурации, который можно обновить на коммутаторе или создать новое имя файла для сохранения загруженного файла конфигурации.
Parameter	<p>Если выбранное имя целевого файла - это running-config, система предоставляет следующие два варианта для обновления текущей рабочей конфигурации коммутатора:</p> <ul style="list-style-type: none"> <li>Заменить: полностью заменить текущую рабочую конфигурацию загруженной конфигурацией.</li> <li>Объединить: объединить загруженную конфигурацию с текущей рабочей конфигурацией.</li> </ul> <p>Если выбранное имя целевого файла - это Создать новый файл, пользователю необходимо ввести новое имя файла в следующем поле ввода параметра.</p>
Upload configuration	После выбора локального файла конфигурации для загрузки, выбора имени целевого файла для сохранения и выбора метода его обновления, нажмите кнопку "Загрузить конфигурацию", чтобы обновить или заменить выбранный целевой файл выбранным локальным файлом конфигурации..

Уведомление:

Файл конфигурации по умолчанию на коммутаторе доступен только для чтения и не может быть заменен.

## 9.6.4 Активация

Вы можете выбрать активировать любой файл конфигурации, сохраненный во flash-памяти коммутатора. Страница активации конфигурации показана на рисунке ниже.

**Activate Configuration**

Select configuration file to activate. The previous configuration will be completely replaced, potentially leading to loss of management connectivity.

Please note: The activated configuration file will not be saved to startup-config automatically.

**File Name**

default-config

startup-config

Описание каждого параметра представлено в следующей таблице:

Параметр	Описание
File name	Имя существующего файла конфигурации на flash-памяти коммутатора.
Activate configuration	После выбора файла конфигурации, который нужно активировать, из списка имен файлов и нажатия кнопки "Активировать конфигурацию", текущая рабочая конфигурация коммутатора будет полностью заменена выбранным файлом конфигурации

 Уведомление:

После активации конфигурации связь пользователя с управляемым коммутатором может быть потеряна, поэтому действуйте осторожно!

Активированный файл конфигурации не будет автоматически сохранен как конфигурация при запуске. Если активирована конфигурация, которая не является конфигурацией при запуске, конфигурация будет потеряна после перезапуска коммутатора.

## 9.6.5 Удалить

Вы можете выбрать удаление любого записываемого файла конфигурации, хранящегося во flash-памяти коммутатора. Страница удаления показана ниже.

**Delete Configuration File**

Select configuration file to delete.

**File Name**

startup-config

Описание каждого параметра представлено в следующей таблице:

Параметр	Описание
File name	Имя файла конфигурации, который может быть удален из flash-памяти коммутатора.
Delete profile	После выбора файла конфигурации, который нужно удалить из списка имен файлов, нажмите кнопку "Удалить файл конфигурации", чтобы удалить выбранный файл конфигурации из flash-памяти коммутатора

 Уведомление:

Конфигурация коммутатора по умолчанию доступна только для чтения и не может быть удалена.

Если вы удалите конфигурацию запуска коммутатора, а затем перезагрузите коммутатор без сохранения конфигурации, коммутатор будет восстановлен до заводских настроек.

## 9.7 Управление зеркалированием

### 9.7.1 Обновление

Страница обновления образа отображена на рисунке ниже.

**Software Upload**

Select File ... No file selected Start Upgrade

Upload status: Idle

Описание каждого параметра представлено в следующей таблице:

Параметр	Описание
Select a document	Выберите локальный образ файла для обновления. После выбора, соответствующее имя файла образа будет отображено за кнопкой.
Start upgrading	Начните обновление прошивки коммутатора с использованием выбранного файла образа.

 Уведомление:

После успешной загрузки файла образа начнется обновление прошивки. Процесс обновления занимает около одной минуты, после чего коммутатор автоматически перезагрузится, но не будет восстанавливать заводскую конфигурацию.

Пожалуйста, не перезагружайте коммутатор и не отключайте его питание во время процесса обновления, иначе коммутатор может работать неправильно

### 9.7.2 Выбор

Страница переключения образов отображает информацию о текущем активном образе и резервном образе на коммутаторе, включая имя файла образа, версию прошивки и время

компиляции. На этой странице вы можете выбрать, нужно ли откатиться к предыдущему резервному образу, как показано на рисунке ниже.

**Software Image Selection**

Active Image	
Image	MISCOM8036GX-PTP-E-1.0.5b9eb29.230630.img
Date	2023-06-30T14:49:33+08:00

Alternate Image	
Image	MISCOM8036GX-1.0.9fda78b.230522.img
Date	2023-05-22T11:39:12+08:00

Описание каждого параметра представлено в следующей таблице:

Параметр	Описание
Activate backup image	Щелкните, чтобы восстановить системное ПО из резервного образа и перезагрузить систему.
Cancel	Деактивируйте резервный образ и вернитесь на главную страницу

**Уведомление:**

Если есть резервный образ, кнопка "Активировать резервный образ" будет активна; в противном случае кнопка будет отключена.

## 9.8 Перегрузка

Страница перезагрузки устройства показана на рисунке ниже

**Restart Device**

**Are you sure you want to perform a Restart?**

### Кнопки

- Да: Нажмите, чтобы перезагрузить устройство.
- Нет: Нажмите, чтобы вернуться на домашнюю страницу без перезагрузки.

## 9.9 Восстановление заводских настроек

На странице восстановления заводских настроек отображена информация о процессе восстановления заводских настроек устройства.

## Factory Defaults

Are you sure you want to reset the configuration to  
Factory Defaults?

**Кнопки**

- Да: Нажмите, чтобы восстановить заводскую конфигурацию по умолчанию.
- Нет: Нажмите, чтобы вернуться на главную страницу без восстановления заводской конфигурации по умолчанию.



Уведомление:

Восстановление заводской конфигурации через веб-страницу немедленно активирует конфигурацию по умолчанию системы, но сохраняет предыдущую конфигурацию IP-адреса интерфейса VLAN1. Перезагрузка не произойдет автоматически, и конфигурация запуска не будет изменена