



Промышленный коммутатор Ethernet уровня 3

WEB-Руководство пользователя

➤ MISCOM8030PTP-6XGF-16GF-8GC

Номер версии: V1.0

Пожалуйста, внимательно прочтите это руководство пользователя перед использованием данного продукта.

Уведомление о авторском праве

Авторские права © Wuhan Maiwe Communication Co., Ltd.

исключительная торговая марка Wuhan Maiwe Communication Co., Ltd.

Microsoft и Windows являются зарегистрированными товарными знаками корпорации Microsoft Corporation. Все связанные товарные знаки, упомянутые в настоящем руководстве по эксплуатации, принадлежат соответствующим производителям.

Иллюстрация

Это руководство пользователя применимо к модели MISCOM8030PTP-6XGF-16GF-8GC. Перед использованием данного руководства внимательно прочтите следующий отказ от ответственности. Продукция, описанная в этом руководстве, может использоваться только в случае вашего согласия с нижеследующим отказом от ответственности.

Отказ от ответственности

Любая информация, предоставленная нашей компанией в данном руководстве, не означает, что компания предоставила соответствующее разрешение на такую информацию. Компания стремится сделать предоставленную в этом руководстве информацию точной и применимой. Однако компания не несет ответственности за использование данной информации, а также не несет совместной и несовместной ответственности за использование данной информации. Продукция и руководства пользователя могут содержать технические или типографские ошибки.

Наша компания оставляет за собой право изменять все или часть данного руководства без предварительного уведомления

Инструкции по безопасному использованию

Этот продукт обладает хорошей и надежной производительностью в пределах разработанного диапазона использования, однако необходимо избегать повреждения или уничтожения оборудования, вызванного вандальными действиями.

- Внимательно прочтите это руководство и сохраните его для последующего использования.
- Не размещайте устройство рядом с водой или влагой.
- Не помещайте ничего на силовой кабель, держите его в недоступном месте.
- Для предотвращения возгорания не перекручивайте или не обматывайте кабели.
- Силовой разъем и другие соединения оборудования должны быть тщательно закреплены друг за другом, регулярно проверяйте их.
- Обратите внимание на чистоту оборудования и, при необходимости, протрите его мягкой хлопковой тканью.
- Пожалуйста, не пытайтесь самостоятельно ремонтировать оборудование, если в руководстве не указано обратное.

В следующих ситуациях немедленно отключите питание и свяжитесь с нашей компанией.

- Вода попадает в оборудование.
- Оборудование сломано.
- Устройство работает ненормально или проявляет производительность, полностью измененную.
- Оборудование издает запах, дым или шум..



Описание: Необходимая пояснительная информация во время использования этого устройства



Примечание: Вещи, на которые следует обратить особое внимание при использовании этого оборудования

Содержание

1	Веб-интерфейс устройства	13
1.1	Веб-вход	13
1.2	Введение в веб-интерфейс.....	14
1.3	Общие кнопки веб-интерфейса.....	15
1.4	Настройка языка веб-интерфейса	16
1.5	Выйти из веб-интерфейса	16
2	Системное сообщение.....	17
2.1	Системное сообщение	17
2.2	Статус порта.....	19
2.3	Загрузка CPU	21
2.4	Конфигурация системы.....	22
3	Конфигурация порта	23
3.1	Конфигурация порта.....	23
3.2	Ограничение скорости порта.....	26
3.3	Шторм- подавление	27
3.4	Шторм-детектор	29
3.5	Агрегация портов	31
3.5.1	Настройка группы агрегации	31
3.5.2	Режим балансировки нагрузки.....	33
3.5.3	Состояние группы агрегации	34
3.5.4	LACP	35
3.5.4.1	LACP конфигурация	35
3.5.4.2	Статус системы	36
3.5.4.3	Состояние локального порта	37
3.5.4.4	Состояние порта партнера	38
3.5.4.5	Статистика кадров LACP	40
3.6	Зеркалирование портов	40
3.7	Статистика порта	43
3.7.1	Общая статистика.....	43
3.7.2	Подробная статистика.....	44
3.8	DDM.....	47
3.8.1	DDM конфигурация.....	48
3.8.2	DDM обзор.....	48
3.8.3	DDM подробности.....	49

4	Характеристики 2 уровня	51
4.1	VLAN	51
4.1.1	Глобальная конфигурация	51
4.1.2	SVL конфигурация	53
4.1.3	Члены VLAN	54
4.1.4	Статус портов	54
4.2	Расширенные настройки VLAN	56
4.2.1	MAC-VLAN	56
4.2.2	Протокол-VLAN	56
4.2.2.1	Протокол-группа	56
4.2.2.2	Группа-VLAN	57
4.2.3	IP-VLAN.....	58
4.3	PVLAN	58
4.3.1	Конфигурация участников.....	59
4.3.2	Изоляция портов	59
4.4	Перевод VLAN.....	60
4.4.1	Конфигурация групп портов.....	60
4.4.2	Отображение VLAN	61
4.5	Таблица MAC-адресов	62
4.5.1	Конфигурация таблицы адресов	62
4.5.2	Запись в таблице MAC-адресов.....	63
4.6	IGMP отслеживание.....	64
4.6.1	Базовая конфигурация	64
4.6.2	VLAN Конфигурация	66
4.6.3	Статус	67
4.6.4	Информация о группе	68
4.6.5	Настройка фильтрации	69
4.6.6	SFM информация	69
4.7	MLD-отслеживание	70
4.7.1	Базовая конфигурация	70
4.7.2	VLAN конфигурация	72
4.7.3	Статус	74
4.7.4	Групповая информация.....	74
4.7.5	Настройка фильтра	75
4.7.6	SFM информация	76
4.8	Фильтрация многоадресной рассылки	77
4.8.1	Файл конфигурации	77
4.8.2	Записи адресов.....	79

4.9	LLDP.....	80
4.9.1	LLDP конфигурация.....	81
4.9.2	Информация о соседях.....	84
4.9.3	MED конфигурация.....	85
4.9.4	Информация о соседе MED.....	90
4.9.5	Статистика порта.....	91
5	Кольцевая избыточность.....	92
5.1	Быстрая кольцевая сеть.....	92
5.1.1	Конфигурация быстрой кольцевой сети.....	92
5.1.2	Статус быстрой кольцевой сети.....	94
5.2	ERPS.....	95
5.2.1	ERPS конфигурация.....	95
5.2.2	ERPS статус.....	98
5.3	Протокол связующего дерева.....	101
5.3.1	STP конфигурация моста.....	103
5.3.2	Отображение экземпляров.....	104
5.3.3	Приоритет экземпляра.....	106
5.3.4	CIST порт.....	107
5.3.5	Порт экземпляра.....	108
5.3.6	Статус моста.....	109
5.3.7	Статус порта.....	112
5.3.8	Статистика порта.....	113
5.4	Обнаружение петель.....	113
5.4.1	Конфигурация обнаружения петель.....	114
5.4.2	Статус обнаружения петли.....	116
6	Характеристики уровня 3.....	118
6.1	Управление IP.....	118
6.1.1	Конфигурация IP.....	118
6.1.2	IP информация.....	122
6.1.3	Таблица маршрутизации IPv4.....	123
6.1.4	Таблица маршрутизации IPv6.....	124
6.2	Маршрутизация и управление.....	125
6.2.1	Цепочка ключей.....	125
6.2.2	Идентификатор ключа.....	126
6.2.3	Список доступа.....	126
6.3	RIP.....	127
6.3.1	Глобальная конфигурация.....	127

6.3.2	Конфигурация сети	130
6.3.3	Конфигурация соседей.....	131
6.3.4	Пассивный интерфейс	131
6.3.5	Конфигурация интерфейса.....	132
6.3.6	Привязка значения метрики и фильтрация сообщений	134
6.3.7	Глобальный статус	135
6.3.8	Статус интерфейса.....	136
6.3.9	Информация о соседях	137
6.3.10	Таблица маршрутизации.....	138
6.4	OSPF	139
6.4.1	Глобальная конфигурация	139
6.4.2	Конфигурация сети	143
6.4.3	Пассивный интерфейс	143
6.4.4	Конфигурация зоны	144
6.4.5	Региональная сертификация	145
6.4.6	Региональный охват	146
6.4.7	Конфигурация интерфейса.....	147
6.4.8	Конфигурация виртуального соединения.....	149
6.4.9	Глобальный статус	151
6.4.10	Статус области.....	152
6.4.11	Статус соседей	153
6.4.12	Статус интерфейса.....	154
6.4.13	Статус маршрутизации	156
6.4.14	LSDB	158
6.4.14.1	LSDB.....	158
6.4.14.2	Маршрутизация LSDB.....	158
6.4.14.3	Сеть LSDB.....	159
6.4.14.4	Сводная информация LSDB	160
6.4.14.5	ASBR LSDB.....	161
6.4.14.6	Внешняя информация LSDB	162
6.4.14.7	NSSA внешняя LSDB.....	164
6.5	OSPFv3	165
6.5.1	Глобальная конфигурация	165
6.5.2	Включение интерфейса	166
6.5.3	Настройка зоны.....	167
6.5.4	Агрегация маршрутов области	168
6.5.5	Конфигурация интерфейса.....	170
6.5.6	Глобальный статус	171
6.5.7	Статус зоны	172

6.5.8	Статус соседей	173
6.5.9	Статус интерфейса	174
6.5.10	Статус маршрутизации	175
6.5.11	LSDB	176
6.5.11.1	LSDB суммарная информация	176
6.5.11.2	LSD детали	178
7	Управление безопасностью	183
7.1	HTTPS	183
7.2	SSH	185
7.3	SNMP	185
7.3.1	SNMP настройки	186
7.3.2	SNMPv1/v2c сообщество	187
7.3.3	SNMPv3 пользователи	187
7.3.4	SNMP группа	189
7.3.5	SNMP вид	190
7.3.6	SNMP аутентификация	191
7.3.7	SNMP Ловушка	192
7.3.7.1	Хост назначения	192
7.3.7.2	Настройки источника	195
7.4	RMON	196
7.4.1	Конфигурация группы статистики	197
7.4.2	Информация о статистической группе	197
7.4.3	Конфигурация группы истории	200
7.4.4	Информация о группе истории	201
7.4.5	Настройка группы сигнализации	203
7.4.6	Информация о группе сигнализации	205
7.4.7	Конфигурация группы событий	207
7.4.8	Информация о группе событий	207
7.5	Управление доступом	209
7.5.1	Настройка управления доступом	209
7.5.2	Статистика управления доступом	210
7.6	Уровень разрешений	210
7.7	Метод проверки	212
7.8	802.1X порт аутентификация	214
7.8.1	Протокол 802.1X	214
7.8.1.1	802.1X	214
7.8.1.2	802.1X Принцип работы	214
7.8.1.3	802.1X аутентификация	217

7.8.2	Конфигурация порта	218
7.8.3	Статус устройства.....	222
7.8.4	Статус порта	224
7.9	AAA Сертификация.....	227
7.9.1	AAA	227
7.9.1.1	AAA протокол.....	227
7.9.1.2	AAA принцип работы	228
7.9.2	RADIUS	230
7.9.2.1	RADIUS конфигурация	230
7.9.2.2	RADIUS статус	232
7.9.2.3	RADIUS данные	233
7.9.3	TACACS+	234
7.9.3.1	TACACS+ конфигурация	234
7.10	Порт безопасности	236
7.10.1	Конфигурация порта	238
7.10.2	MAC конфигурация	240
7.10.3	Глобальный статус	240
7.10.4	Статус порта	243
7.11	Защита источника IPv4	244
7.11.1	Конфигурация порта	244
7.11.2	Статические таблицы	246
7.11.3	Динамические таблицы	246
7.12	Защита источника IPv6	247
7.12.1	Конфигурация порта	247
7.12.2	Статические таблицы	249
7.12.3	Динамические таблицы	249
7.13	ARP защита	250
7.13.1	Конфигурация порта	251
7.13.2	VLAN конфигурация	252
7.13.3	Статические таблицы	253
7.13.4	Динамическая таблица.....	253
7.13.5	Информация о фильтрации ARP	254
8	Расширенные функции	255
8.1	QoS.....	255
8.1.1	Классификация портов.....	255
8.1.2	Стратегия очереди.....	256
8.1.3	Расписание портов	258
8.1.4	Формирование порта	261

8.1.5	Маркировка портов	262
8.1.6	Порт DSCP	265
8.1.7	DSCP-QoS	267
8.1.8	Отображение DSCP.....	268
8.1.9	DSCP классификация	269
8.1.10	Сопоставление записей	270
8.1.11	Экспорт сопоставления.....	273
8.1.12	QoS список управления	276
8.1.13	Статистика QoS	278
8.1.14	QCL статус.....	279
8.2	ACL конфигурация.....	281
8.2.1	Управление портом	281
8.2.2	Ограничение скорости.....	282
8.2.3	Контроль доступа	283
8.2.4	ACL статус	290
8.3	Link OAM.....	291
8.3.1	Конфигурация порта.....	291
8.3.2	Конфигурация событий	293
8.3.3	Статистика.....	294
8.3.4	Статус порта.....	295
8.3.5	Статус события	297
8.3.6	MIB поиск.....	299
8.4	CFM.....	301
8.4.1	Глобальная конфигурация	301
8.4.2	Конфигурация домена обслуживания	302
8.4.3	Конфигурация служб	303
8.4.4	Конфигурация терминала обслуживания.....	304
8.4.5	Статус терминала обслуживания.....	307
8.4.6	Примеры типичной конфигурации CFM.....	309
8.4.6.1	Конфигурация CFM для прямой связи SW1-SW2	309
8.4.6.2	Конфигурация CFM для связи SW1-SW2-SW3	310
8.5	UDLD	312
8.5.1	UDLD конфигурация	312
8.5.2	UDLD статус	314
8.6	Линейная диагностика	315
8.7	sFlow	317
8.7.1	sFlow конфигурация	317
8.7.1.1	Конфигурация агента	317
8.7.1.2	Конфигурация приемника	318

8.7.1.3	Конфигурация порта	319
8.7.2	sFlow статистика	319
8.8	Ping.....	321
8.8.1	Ping (IPv4).....	321
8.8.2	Ping (IPv6).....	322
8.9	Traceroute	324
8.9.1	Traceroute (IPv4).....	324
8.9.2	Traceroute (IPv6).....	325
8.10	PTP (Precision Time Protocol) синхронизация времени	327
8.10.1	Мастер настройки PTP	329
8.10.1.1	Настройка внешнего источника сигнала времени	329
8.10.1.2	Настройка часов PTP	330
8.10.1.3	PTP статус	337
8.10.1.4	802.1AS статистика	339
8.10.2	Пример конфигурации PTP.....	340
8.10.2.1	Конфигурация предустановленного файла 1588.....	340
8.10.2.2	Конфигурация предустановленного файла 802.1AS	343
9	Управление системой	346
9.1	Пользователь	346
9.2	DHCPv4.....	349
9.2.1	DHCPv4 сервер.....	349
9.2.1.1	Режим обслуживания	350
9.2.1.2	Отсутствие выделения IP-адресов	351
9.2.1.3	Пул адресов.....	352
9.2.1.4	Статистика	359
9.2.1.5	Привязать IP	360
9.2.1.6	Отказ в выделении IP-адреса.....	364
9.2.2	DHCPv4 отслеживание.....	364
9.2.2.1	Настройка прослушивания	366
9.2.2.2	Таблица прослушивания.....	367
9.2.3	Перенаправление DHCPv4	368
9.2.3.1	Конфигурация транка.....	370
9.2.3.2	Статистика ретранслятора	372
9.2.4	Детализированная статистика DHCP	373
9.3	DHCPv6.....	375
9.3.1	DHCPv6 отслеживание.....	375
9.3.1.1	Конфигурация прослушивания.....	375
Listening tableОшибка! Закладка не определена.		

9.3.1.2	Статистика прослушивания	377
9.3.2	Ретрансляция DHCPv6	378
9.3.2.1	Конфигурация транка	378
9.3.2.2	Статистика ретранслятора	379
9.4	Системное время	379
9.4.1	Настройка времени	379
9.5	NTP	381
9.6	Журнал	382
9.6.1	Конфигурация журнала	382
9.6.2	Информация о журнале	383
9.6.3	Подробные журналы	385
9.7	Управление файлами конфигурации	386
9.7.1	Сохранить как конфигурацию при запуске	386
9.7.2	Скачать	387
9.7.3	Загрузка	388
9.7.4	Активация	389
9.7.5	Удалить	390
9.8	Перезагрузка	391
9.9	Восстановление заводских настроек	392
9.10	Управление образом	393
9.10.1	Обновление	393
9.10.2	Образ программного обеспечения	393
10	Ремонт и обслуживание	394
10.1	Интернет-сервисы	395
10.2	Техническая поддержка по телефону	395
10.3	Возврат или замена продукции	395
Приложение А: Список фильтров сервопривода		396

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.



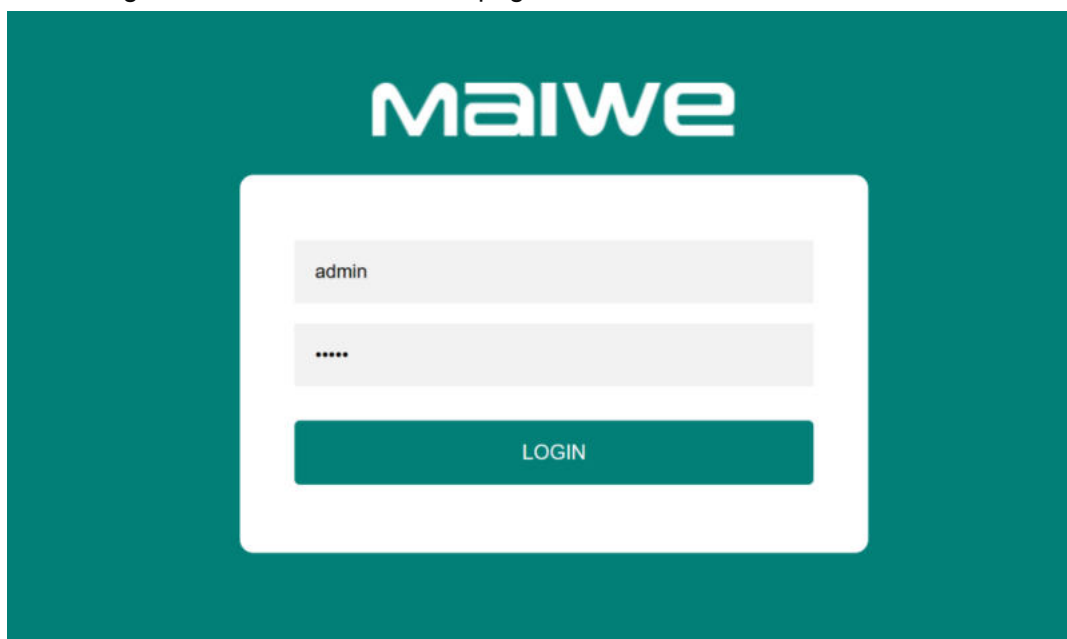
Примечание:

- 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.

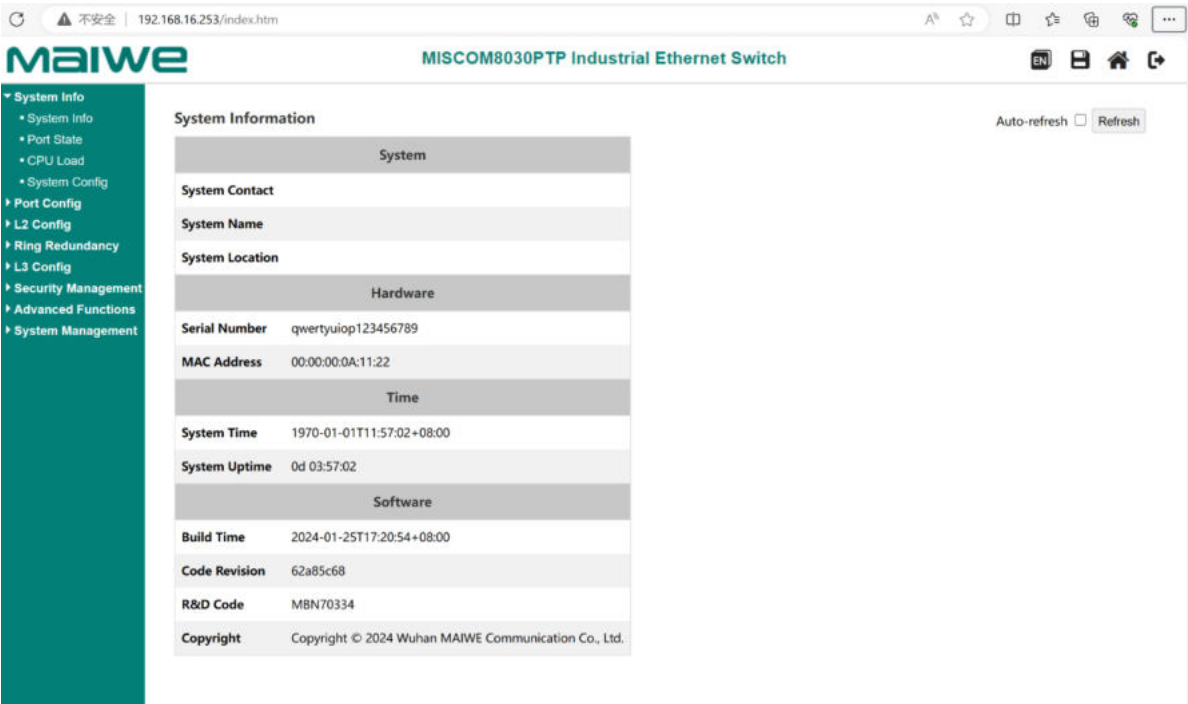
1. Непосредственно соедините ПК и сетевой интерфейс устройства сетевым кабелем.
2. Настройте IP-адрес ПК (например, 192.168.16.100) и маску подсети (например, 255.255.255.0) так, чтобы они находились в том же сетевом сегменте, что и устройство, для обеспечения взаимодействия/
3. Откройте браузер на ПК, 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 пароль устройства — оба «admin»
5. Нажмите кнопку «Войти», чтобы перейти на WEB-страницу.

Click the "Login" button to enter the Web page.



1.2 Введение в веб-интерфейс






После прохождения проверки логина войдите на главную веб-страницу коммутатора. В заголовке отображается модель текущего коммутатора. Веб-страница разделена на три основные области. В верхней части находится область отображения логотипа, типа






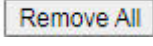
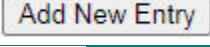











устройства и ярлыков быстрого доступа. Слева находится область меню, а справа - область отображения основных функций.

1.3 Общие кнопки веб-интерфейса

Часто используемые кнопки и значки показаны на рисунке ниже.



Кнопка	Описание
	Отображает текущий язык веб-интерфейса. Нажмите, чтобы переключить язык на английский.
	Отображает текущий язык веб-интерфейса. Нажмите, чтобы переключить язык на китайский.
	Нажмите, чтобы сохранить конфигурацию. Рекомендуется сохранить текущую конфигурацию перед выходом из веб-сетевое управления, чтобы избежать потери несохраненных конфигураций после перезагрузки устройства.
	Нажмите, чтобы вернуться на главную страницу.
	Нажмите, чтобы выйти из текущей учетной записи пользователя.
Auto-refresh <input type="checkbox"/>	Установите флажок "Автообновление", чтобы автоматически обновлять информацию на текущей странице каждые 3 секунды. На некоторых страницах могут быть различия во времени обновления, действует фактическое время обновления страницы.

Кнопка	Описание
	Выбрав порт, вы можете просматривать или настраивать информацию выбранного порта.
	Нажмите, чтобы немедленно обновить текущую страницу.
	Очистить статистику, связанную с текущей страницей.
	Нажмите, чтобы сохранить изменения.
	Нажмите, чтобы отменить любые внесенные локальные изменения и вернуться к ранее сохраненным значениям.
	Нажмите, чтобы удалить все записи конфигурации с текущей страницы.
	Нажмите, чтобы добавить запись конфигурации текущей страницы.
	Нажмите, чтобы просмотреть домашнюю страницу списка.
	Нажмите, чтобы просмотреть предыдущую страницу списка.
	Нажмите, чтобы просмотреть следующую страницу списка.
	Нажмите, чтобы просмотреть последнюю страницу списка.
	Нажмите, чтобы добавить запись конфигурации текущей страницы.
	Нажмите, чтобы отредактировать текущую запись.
	Нажмите, чтобы удалить текущую запись.
	Нажмите, чтобы переместить текущую запись вверх.
	Нажмите, чтобы переместить текущую запись вниз.


1.4 Настройка языка веб-интерфейса

Устройство предоставляет функцию переключения языка веб-интерфейса. На интерфейсе веб-сетевого управления нажмите кнопку языка страницы в правом верхнем углу, чтобы временно переключиться на китайский/английский язык. Эта опция не отображается, когда заводская конфигурация является исключительно английской.

Каждая кнопка показана в следующей таблице:

Кнопка	Описание
	Текущий язык веб-интерфейса — китайский, нажмите, чтобы переключить язык на английский.
	Текущий язык веб-интерфейса — английский, нажмите, чтобы переключить язык на китайский.

1.5 Выйти из веб-интерфейса

На интерфейсе веб-сетевого управления нажмите значок "  " в правом верхнем углу, чтобы выйти из веб-сетевого управления.

Примечание:

- При выходе из веб-сетевого управления система не сохраняет текущую конфигурацию автоматически. Рекомендуется сохранить текущую конфигурацию перед выходом из веб-сетевого управления, чтобы избежать потери несохраненных конфигураций после перезапуска устройства.
- Нажмите кнопку "Сохранить конфигурацию" в разделе "Управление системой > Управление файлами конфигурации > Сохранить как стартовую конфигурацию", чтобы сохранить текущий файл конфигурации.

2 Системное сообщение

2.1 Системное сообщение

Страница информации о системе отображает различную информацию о программном и аппаратном обеспечении, такую как контактное лицо системы коммутатора, название системы, местоположение системы, номер продукта, MAC-адрес, время системы, время запуска системы, время выпуска программного обеспечения, версию кода, наименование

System Information

Auto-refresh ☐ Refresh

System	
System Contact	
System Name	
System Location	
Hardware	
Serial Number	qwertyuiop123456789
MAC Address	00:00:00:0A:11:22
Time	
System Time	1970-01-01T11:57:02+08:00
System Uptime	0d 03:57:02
Software	
Build Time	2024-01-25T17:20:54+08:00
Code Revision	62a85c68
R&D Code	MBN70334
Copyright	Copyright © 2024 Wuhan MAIWE Communication Co., Ltd.

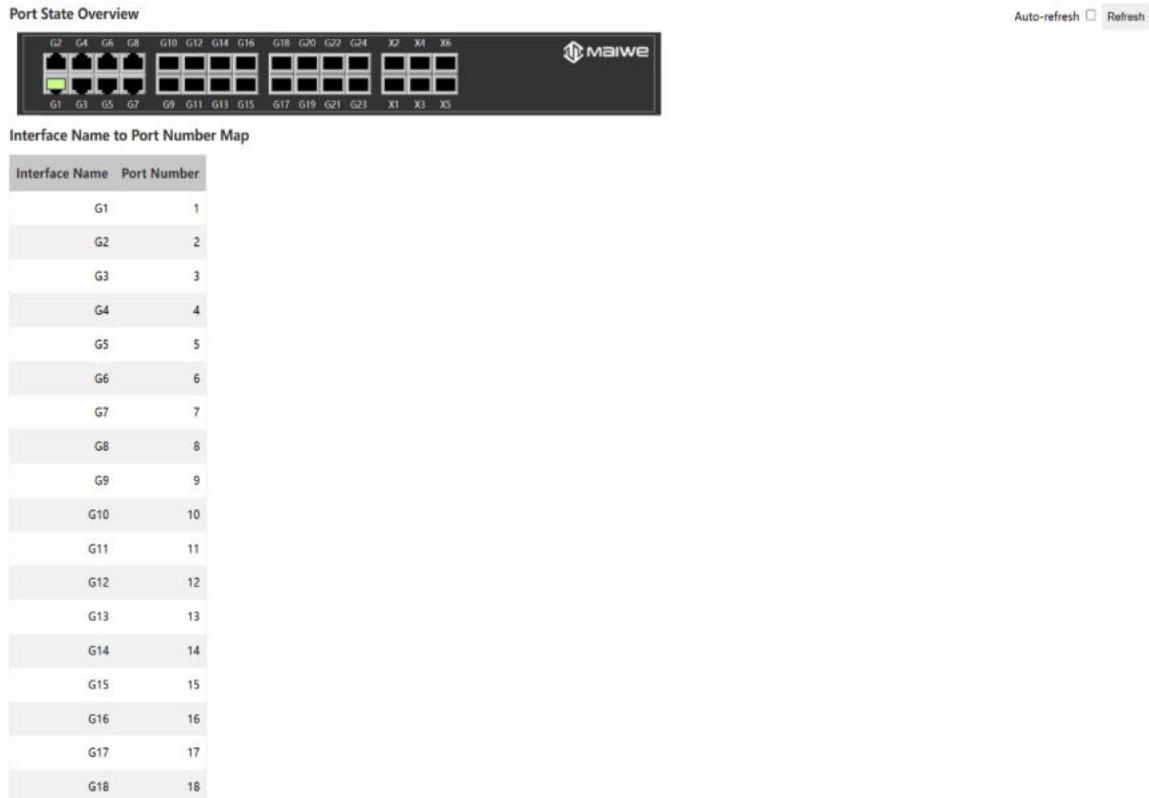
кода для исследований и разработок и т. д., как показано на рисунке ниже.

Описание каждого параметра представлено в следующей таблице:






Параметр	Описание
system	<p>Отображение системной информации коммутатора:</p> <ul style="list-style-type: none"> • Контакт системы: Соответствует информации о контактном лице системы в таблице SNMP MIB по узлу sysContact. • Название системы: Название системы, соответствующее командной строке, а также информация о узле sysName в таблице SNMP MIB. • Местоположение системы: Соответствует информации о местоположении системы в таблице SNMP MIB по узлу sysLocation. <p>Иллюстрация: В разделе "Информация о системе > Конфигурация системы" вы можете настроить информацию о системе.</p>
hardware	<p>Отображение информации об аппаратном обеспечении устройства:</p> <ul style="list-style-type: none"> • Номер продукта: Заводской серийный номер устройства. • MAC-адрес: Заводской MAC-адрес устройства.
time	<p>Отображение информации о времени устройства:</p> <ul style="list-style-type: none"> • Системное время: Текущая системная дата, время, часовой пояс и другая информация. • Время запуска системы: Время работы системы после последнего запуска.
software	<p>Отображение информации о программном обеспечении устройства:</p> <ul style="list-style-type: none"> • Время выпуска: Время выпуска текущего активного образа программного обеспечения на устройстве. • Версия кода: Версия программного обеспечения текущего активного образа. • Имя кодовой базы исследований и разработок (R&D): Кодовое имя платформы, к которой принадлежит текущий активный образ программного обеспечения. • Информация об авторском праве: Отображает авторские права компании и последний год выпуска программного обеспечения





2.2 Статус порта

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



Описание каждого параметра представлено в следующей таблице:

Параметр	Описание
Port status overview	Обзор статуса портов
port mode	<p>Иконка режима оптического/электрического порта имеет следующий вид:</p> <ul style="list-style-type: none">  или : электрический порт. : оптический порт.
port status	<p>Значок состояния порта выглядит следующим образом:</p> <ul style="list-style-type: none"> RJ45 статус порта: <ul style="list-style-type: none"> : Черный указывает на то, что порт не установил действующее соединение. : Зеленый указывает на то, что порт установил

Параметр	Описание
	<p>действующее соединение.</p> <ul style="list-style-type: none"> ♦ : Серый указывает на то, что порт отключен, и соединение невозможно. • SFP статус порта: <ul style="list-style-type: none"> ♦ : Черный указывает на то, что порт не установил действующее соединение ♦ : Зеленый указывает на то, что порт установил действующее соединение. ♦ : Серый указывает на то, что порт отключен, и соединение невозможно.
Port name mapping	Отображение соответствия имён портов
port name	Соответствие программного имени к физическому порту
port number	Номер физического порта

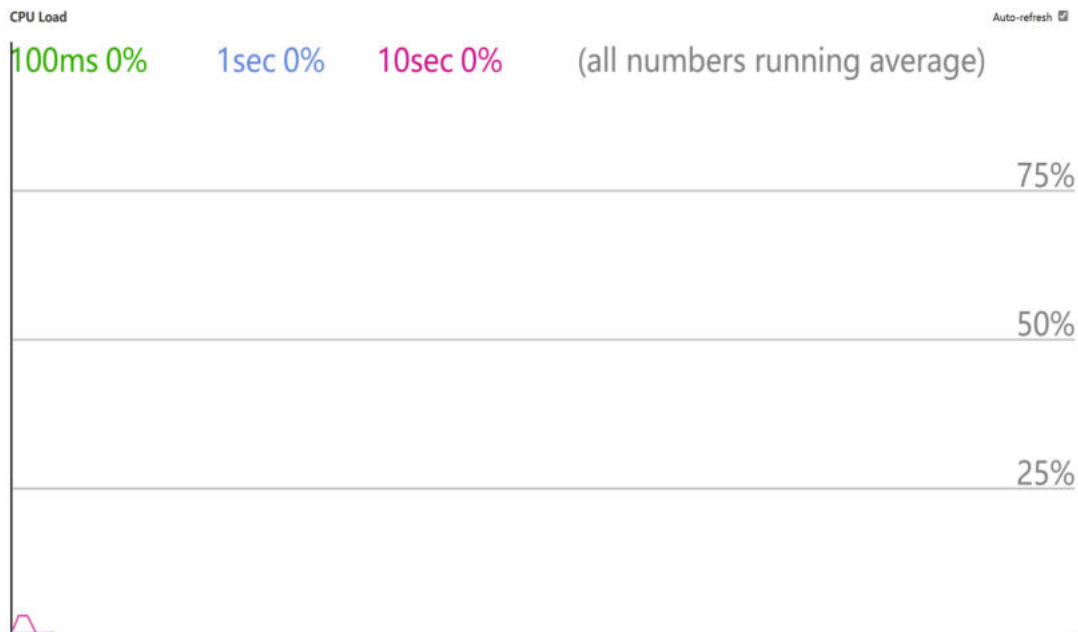
Детальная статистика портов

Щелкните на порту Ethernet, чтобы просмотреть статистику различных типов кадров, полученных и отправленных данным портом, таких как одиночные кадры, кадры многоадресной рассылки, широковещательные кадры, кадры различной длины, кадры различных очередей, кадры с ошибками и т. д. Подробную информацию смотрите в разделе "Конфигурация порта > Статистика порта".

Detailed Port Statistics			
Receive Total		Transmit Total	
Rx Packets	11091	Tx Packets	7509
Rx Octets	1712594	Tx Octets	4176929
Rx Unicast	3633	Tx Unicast	6759
Rx Multicast	1267	Tx Multicast	736
Rx Broadcast	6191	Tx Broadcast	14
Rx Pause	0	Tx Pause	0
Receive Size Counters		Transmit Size Counters	
Rx 64 Bytes	7560	Tx 64 Bytes	2179
Rx 65-127 Bytes	1253	Tx 65-127 Bytes	999
Rx 128-255 Bytes	478	Tx 128-255 Bytes	254
Rx 256-511 Bytes	327	Tx 256-511 Bytes	1690
Rx 512-1023 Bytes	1425	Tx 512-1023 Bytes	290
Rx 1024-1518 Bytes	48	Tx 1024-1518 Bytes	2097
Rx 1519- Bytes	0	Tx 1519- Bytes	0
Receive Queue Counters		Transmit Queue Counters	
Rx Q0	11091	Tx Q0	0
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	7509
Receive Error Counters		Transmit Error Counters	
Rx Drops	0	Tx Drops	0
Rx CRC/Alignment	0	Tx Late/Exc. Coll.	0
Rx Undersize	0		
Rx Oversize	0		
Rx Fragments	0		
Rx Jabber	0		
Rx Filtered	995		

2.3 Загрузка CPU

Эта страница отображает информацию о выборке нагрузки на ЦП коммутатора в форме рисунка SVG. Как показано ниже. Для корректного отображения рендеринга SVG необходимо убедиться, что браузер поддерживает формат SVG. Для конкретных решений обратитесь в Вики-страницу SVG.



2.4 Конфигурация системы

Страница конфигурации информации о системе показана на рисунке ниже. Она используется для настройки контактной информации о системе, названия системы и местоположения системы коммутатора, которые соответственно соответствуют узлам sysContact, sysName и sysLocation в таблице SNMP MIB.

System Information Configuration

SystemContact	<input type="text"/>
SystemName	<input type="text"/>
SystemLocation	<input type="text"/>

Описание каждого параметра представлено в следующей таблице:

Параметр	Описание
system contact	Информация о контакте устройства. Длина строки контактной информации системы составляет от 0 до 255 байтов и может содержать все печатаемые символы клавиатуры с ASCII-кодами от 32 до 126.
system name	Имя хоста устройства. Изменение имени системы также изменит приглашение командной строки. Строка имени системы может содержать заглавные и строчные буквы (AZ, az), цифры (0-9) и дефисы (-). Она не может содержать пробелы. Строка имени системы должна

Параметр	Описание
	начинаться с буквы, и первый и последний символы не могут быть дефисами. Длина строки имени системы составляет от 0 до 255 байтов.
System location	Физическая информация о местоположении устройства. Длина строки местоположения системы составляет от 0 до 255 байтов и может содержать все печатаемые символы клавиатуры с ASCII-кодами от 32 до 126

3 Конфигурация порта

3.1 Конфигурация порта

Функция конфигурации порта используется для настройки и отображения скорости дуплекса порта, управления потоком, jumbo-кадров и т. д. Как показано ниже.

Port Configuration Refresh

Port	Link	Warning	Dual-media	Speed		Flow Control			Maximum	Excessive	Frame
				Current	Configured	Enabled	Curr Rx	Curr Tx	Frame Size	Collision Mode	Length Check
*			<>		<>	<input type="checkbox"/>				<>	<input type="checkbox"/>
G1			Dual	1G FDX	Automatic	<input type="checkbox"/>			10240	Discard	<input type="checkbox"/>
G2			Dual	Down	Automatic	<input type="checkbox"/>			10240	Discard	<input type="checkbox"/>
G3			Dual	Down	Automatic	<input type="checkbox"/>			10240	Discard	<input type="checkbox"/>
G4			Dual	Down	Automatic	<input type="checkbox"/>			10240	Discard	<input type="checkbox"/>
G5			Dual	Down	Automatic	<input type="checkbox"/>			10240	Discard	<input type="checkbox"/>
G6			Dual	Down	Automatic	<input type="checkbox"/>			10240	Discard	<input type="checkbox"/>
G7			Dual	Down	Automatic	<input type="checkbox"/>			10240	Discard	<input type="checkbox"/>
G8			Dual	Down	Automatic	<input type="checkbox"/>			10240	Discard	<input type="checkbox"/>
G9			Fiber	Down	Automatic	<input type="checkbox"/>			10240		<input type="checkbox"/>
G10			Fiber	Down	Automatic	<input type="checkbox"/>			10240		<input type="checkbox"/>

Описание каждого параметра представлено в следующей таблице:

Параметр	Описание
port	Номер порта.
connection status	Зеленый цвет указывает на активное соединение, красный — на отсутствие соединения.
alarm	Сигнал тревоги: <ul style="list-style-type: none"> Серый: нет тревоги для данного порта.

Параметр	Описание
	<ul style="list-style-type: none"> Желтый: на порту есть тревога. Для просмотра информации о тревоге наведите курсор мыши на индикатор.
port type	<p>Индикация типа порта:</p> <ul style="list-style-type: none"> Три режима доступны: мультиплексный порт, электрический порт и оптический порт. Порт RJ45: Порт не настраиваем и представляет собой чисто электрический порт. Оптический порт: Порт не настраиваем и представляет собой чисто оптический порт
rate	<p>Отображение и настройка режима скорости и дуплекса порта.</p> <ul style="list-style-type: none"> Текущая скорость: Отображает текущую скорость подключения порта. Настройка скорости: Предоставляет настраиваемые варианты скорости и дуплекса для порта. Варианты настройки предоставляются только для поддерживаемых портом опций. Значение по умолчанию - автоматическое согласование. <p>Доступные варианты настройки скорости и дуплекса:</p> <ul style="list-style-type: none"> Отключить: Отключает порт коммутатора. Автосогласование: Автоматически согласовывает скорость и дуплекс с портом подключения и выбирает самую высокую совместимую скорость с подключенным партнером. 10Мбит/с полудуплекс: Принудительно устанавливает режим 10Мбит/с полудуплекс. 10Мбит/с полнодуплекс: Принудительно устанавливает режим 10Мбит/с полнодуплекс. 100Мбит/с полудуплекс: Принудительно устанавливает режим 100Мбит/с полудуплекс. 100Мбит/с полнодуплекс: Принудительно устанавливает режим 100Мбит/с полнодуплекс. 1Гбит/с полнодуплекс: Принудительно устанавливает режим 1Гбит/с полнодуплекс. 10Гбит/с полнодуплекс: Принудительно устанавливает режим 10Гбит/с полнодуплекс.

Параметр	Описание
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"> Включить (Enable): отметьте этот флажок, чтобы включить функцию управления потоком на порту. 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. Отправка управляющих кадров (Sending flow control frames): : Порт может отправлять кадры паузы для управления потоком. : Порт не может отправлять кадры паузы для управления потоком.
maximum frame length	<p>Максимальная длина кадров – это максимальный размер блока данных, который порт коммутатора может передать по сети.</p> <p>Значение для данного порта: 1518-10240 байт</p>
excessive conflict handling model	<p>Режим обработки коллизий определяет, как порт коммутатора будет реагировать на возникновение коллизий.</p> <ul style="list-style-type: none"> Отбросить (Discard): (Значение по умолчанию) после 16 попыток передачи с коллизией, порт отбрасывает кадр. Перезапустить (Restart): после 16 попыток передачи с коллизией, порт перезапускает алгоритм отсрочки передачи (backoff algorithm).
frame length detection	<p>Установка этого флажка означает, что функция обнаружения длины кадров настроена; в противном случае функция обнаружения длины кадров не настроена.</p>



Описание:

- После настройки параметров в первом столбце они будут применены ко всем портам.
- После настройки порта необходимо нажать кнопку "Сохранить", чтобы изменения вступили в силу.
- Если после настройки порта вы не нажали "Сохранить", и вы хотите восстановить конфигурацию, нажмите кнопку "Сброс".
- При просмотре текущего статуса порта необходимо нажать кнопку "Обновить", чтобы просмотреть его.
- При использовании мультиплексного порта с оптическим и электрическим соединением рекомендуется настроить режим оптического порта или режим электрического порта для обеспечения надежности соединения.

3.2 Ограничение скорости порта

Страница ограничения скорости порта предоставляет ограничение входящей скорости порта. Пользователи могут ограничить трафик связи каждого порта или отменить ограничение трафика порта. Пользователи могут выбрать фиксированную скорость и использовать различные единицы измерения скорости для ограничения скорости порта, поддерживая кбит/с, Мбит/с, фреймы в секунду (fps) и тысячи фреймов в секунду (kfps). Входящая скорость относится к фактической скорости потока от ПК и других устройств к порту коммутатора. Также поддерживается конфигурация ограничения скорости управления потоком, что удобно для настройки и использования функции управления потоком порта.

Интерфейс настройки ограничения скорости входящего порта.

Global Storm Control Configuration

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

Port Storm Control Configuration

Port	Unicast Frame			Broadcast Frame			Undefined Frame		
	Enable	Rate	Unit	Enable	Rate	Unit	Enable	Rate	Unit
*	<input type="checkbox"/>		<> ▾	<input type="checkbox"/>		<> ▾	<input type="checkbox"/>		<> ▾
G1	<input type="checkbox"/>	500	kbits ▾	<input type="checkbox"/>	500	kbits ▾	<input type="checkbox"/>	500	kbits ▾
G2	<input type="checkbox"/>	500	kbits ▾	<input type="checkbox"/>	500	kbits ▾	<input type="checkbox"/>	500	kbits ▾
G3	<input type="checkbox"/>	500	kbits ▾	<input type="checkbox"/>	500	kbits ▾	<input type="checkbox"/>	500	kbits ▾
G4	<input type="checkbox"/>	500	kbits ▾	<input type="checkbox"/>	500	kbits ▾	<input type="checkbox"/>	500	kbits ▾
G5	<input type="checkbox"/>	500	kbits ▾	<input type="checkbox"/>	500	kbits ▾	<input type="checkbox"/>	500	kbits ▾
G6	<input type="checkbox"/>	500	kbits ▾	<input type="checkbox"/>	500	kbits ▾	<input type="checkbox"/>	500	kbits ▾
G7	<input type="checkbox"/>	500	kbits ▾	<input type="checkbox"/>	500	kbits ▾	<input type="checkbox"/>	500	kbits ▾
G8	<input type="checkbox"/>	500	kbits ▾	<input type="checkbox"/>	500	kbits ▾	<input type="checkbox"/>	500	kbits ▾
G9	<input type="checkbox"/>	500	kbits ▾	<input type="checkbox"/>	500	kbits ▾	<input type="checkbox"/>	500	kbits ▾
G10	<input type="checkbox"/>	500	kbits ▾	<input type="checkbox"/>	500	kbits ▾	<input type="checkbox"/>	500	kbits ▾
G11	<input type="checkbox"/>	500	kbits ▾	<input type="checkbox"/>	500	kbits ▾	<input type="checkbox"/>	500	kbits ▾

Описание каждого параметра представлено в следующей таблице:

Параметр	Описание
enable	Включите ограничение входящей скорости на указанном интерфейсе.
rate	Настройте значение ограничения входящей скорости для указанного интерфейса. Диапазон ограничения скорости составляет <1-13128147>.
unit	Примечание: существует разница в диапазоне скорости для разных единиц измерения; диапазон значений для kbps и fps составляет от 10 до 13128147, а для Mbps и kfps - от 1 до 13128.
flow control	Настройте единицу измерения скорости. Допустимые единицы: kbps/Mbps/fps/kfps. По умолчанию используется kbps.

3.3 Шторм- подавление

Функция шторм-подавления используется для ограничения скорости неизвестных широковещательных, многоадресных и одиночных пакетов. Она ограничивает входящий коммуникационный трафик порта в фиксированном диапазоне, что позволяет эффективно подавлять сетевые штормы.

Global Storm Control Configuration

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

Port Storm Control Configuration

Port	Unicast Frame			Broadcast Frame			Undefined Frame		
	Enable	Rate	Unit	Enable	Rate	Unit	Enable	Rate	Unit
*	<input type="checkbox"/>		<> ▾	<input type="checkbox"/>		<> ▾	<input type="checkbox"/>		<> ▾
G1	<input type="checkbox"/>	500	kbps ▾	<input type="checkbox"/>	500	kbps ▾	<input type="checkbox"/>	500	kbps ▾
G2	<input type="checkbox"/>	500	kbps ▾	<input type="checkbox"/>	500	kbps ▾	<input type="checkbox"/>	500	kbps ▾
G3	<input type="checkbox"/>	500	kbps ▾	<input type="checkbox"/>	500	kbps ▾	<input type="checkbox"/>	500	kbps ▾
G4	<input type="checkbox"/>	500	kbps ▾	<input type="checkbox"/>	500	kbps ▾	<input type="checkbox"/>	500	kbps ▾
G5	<input type="checkbox"/>	500	kbps ▾	<input type="checkbox"/>	500	kbps ▾	<input type="checkbox"/>	500	kbps ▾
G6	<input type="checkbox"/>	500	kbps ▾	<input type="checkbox"/>	500	kbps ▾	<input type="checkbox"/>	500	kbps ▾
G7	<input type="checkbox"/>	500	kbps ▾	<input type="checkbox"/>	500	kbps ▾	<input type="checkbox"/>	500	kbps ▾
G8	<input type="checkbox"/>	500	kbps ▾	<input type="checkbox"/>	500	kbps ▾	<input type="checkbox"/>	500	kbps ▾
G9	<input type="checkbox"/>	500	kbps ▾	<input type="checkbox"/>	500	kbps ▾	<input type="checkbox"/>	500	kbps ▾
G10	<input type="checkbox"/>	500	kbps ▾	<input type="checkbox"/>	500	kbps ▾	<input type="checkbox"/>	500	kbps ▾
G11	<input type="checkbox"/>	500	kbps ▾	<input type="checkbox"/>	500	kbps ▾	<input type="checkbox"/>	500	kbps ▾

Описание каждого параметра представлено в следующей таблице:

Параметр	Описание
Global storm suppression	Глобальное подавление шторма
enable	Включить/отключить функцию глобальной политики шторма для неизвестных одиночных/многоадресных/широковещательных пакетов.
rate	Настроить значение ограничения скорости политики шторма для указанного интерфейса. Диапазон ограничения скорости составляет <1-13128147>.
unit	Примечание: существует разница в диапазоне скорости для разных единиц измерения; диапазон значений для kbps и fps составляет от 10 до 13128147, а для Mbps и kfps - от 1 до 13128.
Port storm suppression	Подавление шторма на порту
enable	Включить/отключить функцию политики шторма порта для одиночных кадров/многоадресных кадров/неизвестных кадров.

Параметр	Описание
rate	Настроить значение ограничения скорости политики шторма для указанного интерфейса. Диапазон ограничения скорости составляет <1-13128147>.
unit	Примечание: существует разница в диапазоне скорости для разных единиц измерения; диапазон значений для kbps и fps составляет от 10 до 13128147, а для Mbps и kfps - от 1 до 13128.



Примечания:

- Режим ограничения скорости является слоем скорости (включая IPG).
- Глобальная конфигурация шторма: подавление неизвестных одиночных, неизвестных многоадресных и неизвестных широковещательных пакетов.
- Конфигурация шторма порта: подавление одиночных кадров включает подавление известных одиночных + неизвестных одиночных + известных широковещательных; подавление широковещательных кадров включает подавление известных широковещательных и неизвестных широковещательных; подавление неизвестных кадров включает подавление неизвестных одиночных + неизвестных многоадресных + широковещательных.
- Когда одновременно включены как одиночные кадры, так и неизвестные кадры, подавление неизвестных одиночных подчиняется минимальному порогу.
- Когда одновременно включены как широковещательные кадры, так и неизвестные кадры, подавление неизвестных широковещательных основано на минимальном пороге.
- Поскольку известные широковещательные пакеты отправляются на процессор, они подвержены воздействию одиночных кадров, широковещательных кадров и неизвестных кадров. Когда все три включены одновременно, известные широковещательные пакеты подавляются на основе минимального порога.

3.4 Шторм-детектор

Функция обнаружения шторма используется для настройки порогового значения разрешенного для прохождения широковещательного и многоадресного трафика через каждый порт. Когда широковещательный и многоадресный трафик на порте превышает пороговое значение, срабатывают тревоги и активируются действия реагирования, а порт закрывается или блокируется для предотвращения сетевых штормов и обеспечения нормальной работы сети.

Страница обнаружения шторма показана на рисунке ниже.

Storm Detect Configuration

Storm Detect

Disabled

Auto-refresh ☐ Refresh

Storm Detect Configuration

Port	Broadcast Statistic(pps)	Multicast Statistic(pps)	Triggered Action	Recovery Time(s)	Current Broadcast Flow(pps)	Current Multicast Flow(pps)	Current Port Status	Residual Recovery Time(s)
*			<>		*	*	*	*
G1	0	0	Down	60	0	0	forward	0
G2	0	0	Down	60	0	0	down	0
G3	0	0	Down	60	0	0	down	0
G4	0	0	Down	60	0	0	down	0
G5	0	0	Down	60	0	0	down	0
G6	0	0	Down	60	0	0	down	0
G7	0	0	Down	60	0	0	down	0
G8	0	0	Down	60	0	0	down	0
G9	0	0	Down	60	0	0	down	0
G10	0	0	Down	60	0	0	down	0
G11	0	0	Down	60	0	0	down	0
G12	0	0	Down	60	0	0	down	0
G13	0	0	Down	60	0	0	down	0
G14	0	0	Down	60	0	0	down	0

Описание каждого параметра представлено в следующей таблице:

Параметр	Описание
storm detection	Включить или отключить функцию обнаружения шторма. После отключения функции обнаружения шторма будет отображаться только текущее состояние LINK порта, а реальный трафик порта не будет отображаться.
broadcast packet	Настроить порог для реального трафика на порте. После превышения порога состояние порта будет изменено. Порог связан с пропускной способностью, которая составляет 1.4881*пропускная способность.
multicast packet	Действия триггера разделяются на блокировку (блокировка порта) и отключение (отключение порта).
trigger action	Время, необходимое для изменения состояния порта и возврата к нормальному режиму пересылки.
recovery time	Отображает реальный широковещательный трафик после настройки порта с функцией обнаружения широковещательного или многоадресного шторма.
live broadcast traffic	После настройки порта с функцией обнаружения широковещательного или многоадресного шторма отображается реальный многоадресный трафик.
real-time multicast traffic	Когда порт находится в нормальном режиме пересылки, он отображается как forward, когда порт заблокирован, он отображается

Параметр	Описание
	как block, и когда порт отключен, он отображается как down.
real-time port status	После того как порт вызывает действие триггера, время восстановления отсчитывается, и состояние порта восстанавливается, когда оставшееся время восстановления равно 0
remaining recovery time	Включить или отключить функцию обнаружения шторма. После отключения функции обнаружения шторма будет отображаться только текущее состояние LINK порта, а реальный трафик порта не будет отображаться.

3.5 Агрегация портов

Основная функция агрегации портов заключается в объединении нескольких физических каналов связи для создания логического канала с большей пропускной способностью. Агрегация портов может обеспечить большую пропускную способность без обновления оборудования, а также резервирование каналов связи.

3.5.1 Настройка группы агрегации

Конфигурационная страница группы агрегации. Как показано ниже.

Aggregation Group Configuration

	Port Members																				Group Configuration													
Group ID	G1	G2	G3	G4	G5	G6	G7	G8	G9	G10	G11	G12	G13	G14	G15	G16	G17	G18	G19	G20	G21	G22	G23	G24	X1	X2	X3	X4	X5	X6	Mode	Revertive	Max Bundle	
Normal	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		
1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Disabled	<input type="checkbox"/>	16
2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Disabled	<input type="checkbox"/>	16
3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Disabled	<input checked="" type="checkbox"/>	16
4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Disabled	<input checked="" type="checkbox"/>	16
5	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Disabled	<input checked="" type="checkbox"/>	16
6	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Disabled	<input checked="" type="checkbox"/>	16
7	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Disabled	<input checked="" type="checkbox"/>	16
8	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Disabled	<input checked="" type="checkbox"/>	16
9	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Disabled	<input checked="" type="checkbox"/>	16
10	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Disabled	<input checked="" type="checkbox"/>	16
11	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Disabled	<input checked="" type="checkbox"/>	16
12	<input type="checkbox"/>	<input type="checkbox"/>																																

Описание каждого параметра представлено в следующей таблице:

Параметр	Описание
group ID	Номер группы агрегации указывает идентификатор группы агрегации для настроек, содержащихся в той же строке. Групповой идентификатор "non-aggregation port" (неагрегированный порт) означает, что порт не входит ни в какую группу. Для каждого порта может быть назначена только одна группа. Всего можно настроить 8 групп.
member port	<p>Все порты коммутатора перечислены по идентификаторам групп. Выберите переключатель, чтобы добавить порт в агрегацию или удалить порт из агрегации, сделав его неагрегированным. По умолчанию ни один порт не принадлежит какой-либо группе агрегации. Чтобы конфигурация агрегации вступила в силу, порт необходимо добавить в группу агрегации и настроить режим агрегации для этой группы.</p> <p>Примечание:</p> <p>Порты в одной группе агрегации должны иметь одинаковые характеристики.</p>
aggregation group configuration-mode	<p>Установите режим агрегации для группы агрегации.</p> <ul style="list-style-type: none"> Отключено: Группа отключена. Статический: Группа работает в режиме статической агрегации. LACP (активный): В этом режиме порт активно отправляет

Параметр	Описание
	<p>сообщения LACPDU партнеру для выполнения вычислений протокола LACP.</p> <ul style="list-style-type: none"> LACP (пассивный): В этом режиме порт не активно отправляет сообщения LACPDU. После получения сообщения LACP, отправленного партнером, порт переходит в состояние вычислений протокола.
aggregation group configuration-failback mode	Этот параметр применяется только к группам агрегации, поддерживающим протокол LACP. Включение режима автоматического возврата (switchback) позволяет сохранить активный порт с более высоким приоритетом порта. Например: когда порт с высоким приоритетом переходит в неактивное состояние из-за сбоя, а затем восстанавливается, если режим автоматического возврата включен, порт с высоким приоритетом будет пересмотрен для того, чтобы снова стать активным портом; в противном случае порт не сможет стать активным после восстановления.
aggregation group configuration-maximum number of active ports	Этот параметр применяется только к группам, поддерживающим протокол LACP. Он определяет максимальное количество активных сгруппированных портов LACP, разрешенных в агрегации.

3.5.2 Режим балансировки нагрузки

Страница конфигурации режима балансировки нагрузки. Как показано ниже.

Common Aggregation Configuration

Hash Code Contributors

Source MAC Address ☒

Destination MAC Address ☐

IP Address ☒

TCP/UDP Port Number ☒

Save

Reset

Описание каждого параметра представлено в следующей таблице:

Параметр	Описание
source MAC address	Исходный MAC-адрес может использоваться для расчета исходного MAC-адреса кадра. Установите флажок для включения его; снимите флажок для отключения. По умолчанию исходный MAC-адрес включен.
destination MAC address	Направленный MAC-адрес может использоваться для расчета направленного MAC-адреса кадра. По умолчанию направленный MAC-адрес отключен.
IP address	IP-адрес может использоваться для расчета исходного и направленного IP-адресов кадра. По умолчанию IP-адреса включены.
TCP/UDP port number	Номер порта TCP/UDP может использоваться для расчета номеров исходного TCP/UDP и направленного TCP/UDP портов кадра. По умолчанию номера портов TCP/UDP включены

3.5.3 Состояние группы агрегации

Эта страница используется для просмотра состояния портов группы агрегации. Как показано ниже.

Aggregation Status

Aggr ID	Name	Type	Speed	Configured Ports	Aggregated Ports
No aggregation groups					

Описание каждого параметра представлено в следующей таблице:

Параметр	Описание
group ID	Агрегированный идентификатор, связанный с этим экземпляром агрегата.
group name	Название идентификатора группы агрегации.
type	Тип группы агрегации (статическая или LACP).
rate	Скорость портов-членов агрегации.
configure member ports	Порты-члены, настроенные в группе агрегации.
aggregate member port	Группа агрегации выбирает порты-члены агрегации

3.5.4 LACP

3.5.4.1 LACP конфигурация

Эта страница позволяет пользователям просматривать и изменять текущий приоритет системы LACP и конфигурацию порта, как показано на рисунке ниже.

LACP System Configuration

System Priority	32768	(0~65535)
-----------------	-------	-----------

LACP Port Configuration

Port	LACP	Timeout	Piro
*		<> ▾	
G1	Disabled	Fast ▾	32768
G2	Disabled	Fast ▾	32768
G3	Disabled	Fast ▾	32768
G4	Disabled	Fast ▾	32768
G5	Disabled	Fast ▾	32768
G6	Disabled	Fast ▾	32768
G7	Disabled	Fast ▾	32768
G8	Disabled	Fast ▾	32768
G9	Disabled	Fast ▾	32768
G10	Disabled	Fast ▾	32768
G11	Disabled	Fast ▾	32768
G12	Disabled	Fast ▾	32768

Описание каждого параметра представлено в следующей таблице:

Параметр	Описание
LACP system configuration	Конфигурация системы LACP
System priority	Для различения приоритета устройств на обоих концах агрегации портов, устройство с более высоким приоритетом служит активным концом LACP. Чем меньше значение, тем выше приоритет. По умолчанию приоритет системы составляет 32768; если приоритеты системы одинаковы, выбирается конец с меньшим MAC-адресом в качестве активного конца.
LACP port configuration	Конфигурация порта LACP

Параметр	Описание
port	Номер порта устройства.
LACP	Отображает, включен ли в данный момент LACP на порту устройства.
timeout mode	<p>Настройка периода времени ожидания для порта приема сообщений LACP. Если локальный активный порт не получает сообщение протокола LACP, отправленное партнером, в течение установленного периода времени ожидания, партнер считается недоступным, и активный порт выходит из работы.</p> <ul style="list-style-type: none"> Быстрый: Локальный порт получает пакеты LACP каждую секунду, а таймаут составляет 3 секунды. Медленный: Локальный порт получает пакеты LACP каждые 30 секунд, а таймаут составляет 90 секунд
port priority	Приоритет порта используется для различения приоритетов различных портов при выборе их в качестве активных портов. Чем меньше значение, тем выше приоритет. По умолчанию приоритет порта составляет 32768.

3.5.4.2 Статус системы

Эта страница предоставляет обзор состояния информации о LACP на уровне системы. Как показано ниже.

LACP System Status		Auto-refresh <input type="checkbox"/> Refresh
IDLocal System ID		
Priority	MAC Address	
32768	00:00:00:0A:11:22	
Partner System Status		
Aggr ID	PartnerSystem ID	Partner Prio
		Partner Key
		Last Changed
		Local Ports
No ports enabled or no existing partners		

Описание каждого параметра представлено в следующей таблице:

Параметр	Описание
Local system ID	Локальный идентификатор системы
priority	Приоритет локальной системы.
MAC address	MAC-адрес локальной системы.
Peer system status	Статус системы партнера
Group ID	Идентификатор агрегата, связанный с этим экземпляром агрегата.

Параметр	Описание
Peer system ID	Идентификатор (MAC-адрес) устройства-партнера.
peer priority	Приоритет системы устройства-партнера.
peer Key	Ключ устройства-партнера соответствует идентификатору агрегата.
last change time	Время с момента последнего изменения этой агрегации.
local port number	Отображает, какие порты являются частью агрегации этого устройства

3.5.4.3 Состояние локального порта

Эта страница предоставляет обзор состояния внутреннего (т.е. локальной системы) статуса всех портов LACP. Отображаются только порты, которые являются частью группы LACP. Как показано ниже.

LACP Internal Port Status

Auto-refresh☐ Refresh

Port	State	Key	Priority	Activity	Timeout	Aggregation	Synchronization	Collecting	Distributing	Defaulted	Expired
No LACP ports enabled											

Описание каждого параметра представлено в следующей таблице:

Параметр	Описание
port	Номер порта
port status	Текущее состояние порта. <ul style="list-style-type: none"> Не выбран: указывает на неактивный порт. Выбран: указывает на активный порт. Резервный: указывает на порт в резервном состоянии.
key	Идентификатор агрегации этого порта. Только порты с тем же ключом на одном устройстве могут участвовать в агрегации.
priority	Приоритет порта.
negotiation mode	Режим согласования порта в статусе соединения, 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"> Да: указывает, что соединение может быть объединено. Нет: указывает, что соединение является независимым и не

Параметр	Описание
	может быть объединено.
aggregation synchronization	<p>Указывает, завершена ли текущая агрегация порта.</p> <ul style="list-style-type: none"> Да: указывает на то, что отправляющее соединение находится в состоянии IN_SYNC, то есть порт был назначен правильной группе агрегации. Нет: указывает на то, что соединение находится в состоянии OUT_OF_SYNC, то есть порт не выбрал правильную группу агрегации.
package receiving status	"Yes" указывает на то, что включен текущий сбор пакетов на соединении, в противном случае "Нет".
contract delivery status	"Yes" указывает на то, что отправка пакетов включена на текущем соединении, в противном случае "Нет".
default state	"Yes" означает, что информация о партнере, используемая этим концом, поступает из значения по умолчанию, настроенного администратором. "No" указывает на то, что информация о партнере, используемая локальным концом, поступает из полученного LACPDU.
packet receiving timeout	"Yes" означает, что локальная машина приема пакетов находится в состоянии тайм-аута, "No" означает, что она не находится в состоянии тайм-аута

3.5.4.4 Состояние порта партнера

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☐ Refresh

Port	State	Group ID	Partner Key	Partner Port	Partner Port Priority	Activity	Timeout	Aggregation	Synchronization	Collecting	Distributing	Defaulted	Expired
No LACP neighbor status available													

Описание каждого параметра представлено в следующей таблице:

Параметр	Описание
port	Номер порта.
state	Текущее состояние порта.

Параметр	Описание
	<ul style="list-style-type: none"> Неактивный: указывает, что порт неактивен. Активный: указывает, что порт активен. Резервный: указывает, что порт находится в режиме ожидания
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.
negotiation mode	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	<p>Указывает на возможность агрегации порта партнера.</p> <ul style="list-style-type: none"> Да: указывает на возможность агрегации соединения. Нет: указывает на то, что соединение является независимым и не может быть агрегировано.
aggregation synchronization	<p>Указывает, завершена ли текущая агрегация порта партнера.</p> <ul style="list-style-type: none"> Да: указывает, что отправляемое соединение находится в состоянии IN_SYNC, то есть порт был назначен правильной группе агрегации. Нет: указывает, что соединение находится в состоянии OUT_OF_SYNC, то есть порт не выбран в правильную группу агрегации.
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.
packet receiving timeout	"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.

3.5.4.5 Статистика кадров LACP

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

LACP Statistics Auto-refresh ☐ Refresh Clear

Port	LACP Received	LACP Transmitted	Discarded	
			Unknown	Illegal
No ports enabled				

Описание каждого параметра представлено в следующей таблице:

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 LACP frames dropped	Показывает, сколько неизвестных или недопустимых LACP-кадров было отброшено на каждом порту.

3.6 Зеркалирование портов

Это используется для просмотра и настройки функции зеркалирования портов.

Функция зеркалирования портов. Как показано ниже.

Mirror Configuration Table Auto-refresh ☐ Refresh

Session ID	Mode	Type
1	Disabled	Mirror

Описание каждого параметра представлено в следующей таблице:

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

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	Mirror ▾

Source VLAN(s) Configuration

VLAN ID	<input type="text"/>
---------	----------------------

Port Configuration

Port	Source	Destination
*	<> ▾	<input type="checkbox"/>
G1	Disabled ▾	<input type="checkbox"/>
G2	Disabled ▾	<input type="checkbox"/>
G3	Disabled ▾	<input type="checkbox"/>
G4	Disabled ▾	<input type="checkbox"/>
G5	Disabled ▾	<input type="checkbox"/>
G6	Disabled ▾	<input type="checkbox"/>
G7	Disabled ▾	<input type="checkbox"/>
G8	Disabled ▾	<input type="checkbox"/>
G9	Disabled ▾	<input type="checkbox"/>
G10	Disabled ▾	<input type="checkbox"/>

Описание каждого параметра представлено в следующей таблице:

Параметр	Описание
Global configuration	Глобальная конфигурация
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.

Параметр	Описание
	<ul style="list-style-type: none"> Локальное зеркалирование: Исходный порт и порт назначения этой функции находятся на этом устройстве.
Source VLAN configuration	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.
Port configuration	Конфигурация портов
Port	Установите логический порт.
Source port mirroring mode	<p>Выберите режим зеркалирования исходного порта.</p> <ul style="list-style-type: none"> Отключено: не используется в качестве порта источника зеркалирования. Двунаправленное зеркалирование: как передаваемые, так и принимаемые кадры зеркалируются на порт назначения. Зеркалирование входящего трафика: принимаемые кадры этого порта зеркалируются на порт назначения. Передаваемые кадры не зеркалируются. Зеркалирование исходящего трафика: передаваемые кадры этого порта зеркалируются на порт назначения. Принимаемые кадры не зеркалируются.
Destination port	Выберите целевой порт.



Примечания:

В режиме зеркалирования можно выбрать только один порт назначения.

3.7 Статистика порта

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

3.7.1 Общая статистика

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			
G1	13	11	2241	2563	0	0	0	0	3			
G2	0	0	0	0	0	0	0	0	0			
G3	0	0	0	0	0	0	0	0	0			
G4	0	0	0	0	0	0	0	0	0			
G5	0	0	0	0	0	0	0	0	0			
G6	0	0	0	0	0	0	0	0	0			
G7	0	0	0	0	0	0	0	0	0			
G8	0	0	0	0	0	0	0	0	0			
G9	0	0	0	0	0	0	0	0	0			
G10	0	0	0	0	0	0	0	0	0			
G11	0	0	0	0	0	0	0	0	0			
G12	0	0	0	0	0	0	0	0	0			
G13	0	0	0	0	0	0	0	0	0			
G14	0	0	0	0	0	0	0	0	0			
G15	0	0	0	0	0	0	0	0	0			
G16	0	0	0	0	0	0	0	0	0			
G17	0	0	0	0	0	0	0	0	0			
G18	0	0	0	0	0	0	0	0	0			

Описание каждого параметра представлено в следующей таблице:

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.

3.7.2 Подробная статистика

Функция подробной статистики отображается ниже.

Detailed Port Statistics

G1

Auto-refresh

Refresh

Clear

Receive Total		Transmit Total	
Rx Packets	97	Tx Packets	60
Rx Octets	12662	Tx Octets	18684
Rx Unicast	29	Tx Unicast	53
Rx Multicast	4	Tx Multicast	7
Rx Broadcast	64	Tx Broadcast	0
Rx Pause	0	Tx Pause	0
Receive Size Counters		Transmit Size Counters	
Rx 64 Bytes	76	Tx 64 Bytes	23
Rx 65-127 Bytes	5	Tx 65-127 Bytes	13
Rx 128-255 Bytes	4	Tx 128-255 Bytes	2
Rx 256-511 Bytes	2	Tx 256-511 Bytes	12
Rx 512-1023 Bytes	10	Tx 512-1023 Bytes	4
Rx 1024-1518 Bytes	0	Tx 1024-1518 Bytes	6
Rx 1519- Bytes	0	Tx 1519- Bytes	0

Receive Queue Counters		Transmit Queue Counters	
Rx Q0	97	Tx Q0	0
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	60
Receive Error Counters		Transmit Error Counters	
Rx Drops	0	Tx Drops	0
Rx CRC/Alignment	0	Tx Late/Exc. Coll.	0
Rx Undersize	0		
Rx Oversize	0		
Rx Fragments	0		
Rx Jabber	0		
Rx Filtered	4		

Описание каждого параметра представлено в следующей таблице:

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"> • Количество принятых/отправленных кадров: подсчитывает количество кадров, принятых/отправленных портом. • Количество принятых/отправленных байт: подсчитывает количество байт, принятых/отправленных портом. • Количество принятых/отправленных одноадресных кадров: подсчитывает количество принятых/отправленных одноадресных кадров портом. • Количество принятых/отправленных кадров многоадресной рассылки: подсчитывает количество принятых/отправленных кадров многоадресной рассылки портом. • Количество принятых/отправленных широковещательных кадров: подсчитывает количество принятых/отправленных широковещательных кадров портом. • Количество принятых/отправленных кадров приостановки: подсчитывает количество принятых/отправленных кадров приостановки портом.
Receive/send frame length statistics	<p>Подсчитайте количество длин кадров, принятых/отправленных портом.</p> <ul style="list-style-type: none"> • Количество принятых/отправленных кадров размером 64 байта: подсчитывает количество пакетов данных размером 64 байта, принятых/отправленных портом. • Количество принятых/отправленных кадров размером от 65 до 127 байт: подсчитывает количество кадров размером от 65 до 127 байт, принятых/отправленных портом. • Количество принятых/отправленных кадров размером от 128 до 255 байт: подсчитывает количество кадров размером от 128 до 255 байт, принятых/отправленных портом. • Количество принятых/отправленных кадров размером от 256 до 511 байт: подсчитывает количество кадров размером от 256 до 511 байт, принятых/отправленных портом. • Количество принятых/отправленных кадров размером от 512 до 1023 байт: подсчитывает количество кадров размером от 512 до 1023 байт, принятых/отправленных портом.

Параметр	Описание
	<ul style="list-style-type: none"> Количество принятых/отправленных кадров размером от 1024 до 1518 байт: подсчитывает количество кадров размером от 1024 до 1518 байт, принятых/отправленных портом. Количество принятых/отправленных кадров размером 1519 байт и более: подсчитывает количество кадров размером 1519 байт и более, принятых/отправленных портом.
Receive/send queue statistics	<p>Подсчитайте количество кадров в очереди, принятых/отправленных портом.</p> <ul style="list-style-type: none"> Принять/отправить Q0: подсчитывает количество кадров, принятых/отправленных портом в очереди Q0. Принять/отправить Q1: подсчитывает количество кадров, принятых/отправленных портом в очереди Q1. Принять/отправить Q2: подсчитывает количество кадров, принятых/отправленных портом в очереди Q2. Принять/отправить Q3: подсчитывает количество кадров, принятых/отправленных портом в очереди Q3. Принять/отправить Q4: подсчитывает количество кадров, принятых/отправленных портом в очереди Q4. Принять/отправить Q5: подсчитывает количество кадров, принятых/отправленных портом в очереди Q5. Принять/отправить Q6: подсчитывает количество кадров, принятых/отправленных портом в очереди Q6. Принять/отправить Q7: подсчитывает количество кадров, принятых/отправленных портом в очереди Q7.
Receive error frame statistics	<p>Подсчитайте количество ошибочных кадров, полученных портом.</p> <ul style="list-style-type: none"> Количество принятых отброшенных кадров: подсчитывает количество отброшенных кадров, полученных портом. Количество принятых кадров с ошибкой проверки/выравнивания: подсчитывает количество кадров с ошибкой CRC или выравнивания данных, полученных портом. Количество принятых ультракоротких кадров: подсчитывает количество ультракоротких кадров, полученных портом.

Параметр	Описание
	<ul style="list-style-type: none"> Количество принятых кадров джамбо: подсчитывает количество кадров джамбо, полученных портом. Количество принятых недопустимых фрагментов кадров: подсчитывает количество недопустимых ультракоротких кадров, полученных портом. Количество принятых недопустимых кадров джамбо: подсчитывает количество недопустимых кадров джамбо, полученных портом. Количество принятых отфильтрованных кадров: подсчитывает количество отфильтрованных кадров, полученных портом.
Send error frame statistics	<p>Подсчитайте количество ошибочных кадров данных, отправленных портом.</p> <ul style="list-style-type: none"> Количество отправленных отброшенных кадров: подсчитывает количество отброшенных кадров, отправленных портом. Количество отправленных конфликтных кадров: подсчитывает количество конфликтных кадров, отправленных портом.

3.8 DDM

DDM (цифровое диагностическое мониторингирование) – это эффективный метод для контроля важных параметров производительности оптических модулей. Он отслеживает следующие рабочие параметры: температуру, рабочее напряжение, ток смещения, оптическую мощность передачи, оптическую мощность приема, а также их информацию о тревогах и т. д. Через цифровую диагностическую функцию оптического модуля коммутатор может в реальном времени отслеживать вышеуказанные пять рабочих параметров модуля, быстро находить конкретное местоположение ошибки в оптическом кабеле, упрощать обслуживание и повышать надежность системы.

Все оптические порты этого коммутатора поддерживают DDMI (Интерфейс цифрового диагностического мониторинга), который может обеспечить расширенные диагностические функции оптического модуля и запрос в реальном времени информации о передатчике, информации о рабочих параметрах и различных предупреждениях о различных оптических модулях, вставленных в интерфейс, а также информацию о тревогах и т. д., таким образом, пользователи могут быстро локализовать неисправности оптических модулей,

предотвращать проблемы с оптическим модулем заранее и своевременно их решать.

3.8.1 DDM конфигурация

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

DDM Configuration

Mode

Disabled ▾

Save

Reset

Описание каждого параметра представлено в следующей таблице:

Параметр	Описание
model	<p>Настройка статуса активации глобального переключателя DDM.</p> <ul style="list-style-type: none"> Включить: Включить функцию DDM. Отключить: Отключить функцию DDM

3.8.2 DDM обзор

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

DDM Overview

Auto-refresh ☐ Refresh

Port	Vendor	Part Pumber	Serial Number	Revision	Date Code	Transceiver
G1	-	-	-	-	-	-
G2	-	-	-	-	-	-
G3	-	-	-	-	-	-
G4	-	-	-	-	-	-
G5	-	-	-	-	-	-
G6	-	-	-	-	-	-
G7	-	-	-	-	-	-
G8	-	-	-	-	-	-
G9	-	-	-	-	-	-
G10	-	-	-	-	-	-
G11	-	-	-	-	-	-
G12	-	-	-	-	-	-
G13	-	-	-	-	-	-
G14	-	-	-	-	-	-
G15	-	-	-	-	-	-

Описание каждого параметра представлено в следующей таблице:

Параметр	Описание
port	Порт DDM. Щелкните по ссылке порта, чтобы просмотреть подробную информацию о модуле SFP указанного порта.
manufacturer	Название производителя SFP.
part code	Компонентный код PN, предоставленный производителем SFP.
serial number	Серийный номер SN, предоставленный производителем SFP.
revision	Ревизия части модуля SFP.
production date	Дата производства модуля SFP.
transceiver	Тип трансивера SFP

3.8.3 DDM подробности

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

Как показано ниже.

Transceiver Information

G1 ☐ Auto-refresh ☐ Refresh

Vendor	-
Part Pumber	-
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
Transceiver information	Информация о трансивере:
manufacturer	Название производителя SFP.
part code	Компонентный код PN, предоставленный производителем SFP.
serial number	Серийный номер SN, предоставленный производителем SFP.
revision	Ревизия части модуля SFP.
production date	Дата производства модуля SFP.
transceiver	Тип трансивера SFP.
Optical module information	Информация об оптическом модуле:
the current value	Текущие значения температуры, напряжения, тока смещения, передаваемой оптической мощности и принимаемой оптической мощности.
alarm/early warning	Указывает, есть ли тревоги или предупреждения о температуре, напряжении, токе смещения, передаваемой оптической мощности и принимаемой оптической мощности.
lower warning limit	Нижние пороговые значения для предупреждений о температуре, напряжении, токе смещения, передаваемой оптической мощности и принимаемой оптической мощности.
early warning	Верхние пороговые значения для предупреждений о температуре,

Параметр	Описание
upper limit	напряжении, токе смещения, передаваемой оптической мощности и принимаемой оптической мощности.
alarm lower limit	Нижние пороговые значения для тревог о температуре, напряжении, токе смещения, передаваемой оптической мощности и принимаемой оптической мощности.
alarm upper limit	Верхние пороговые значения для тревог о температуре, напряжении, токе смещения, передаваемой оптической мощности и принимаемой оптической мощности.

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	
G1	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag All	1	
G2	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag All	1	
G3	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag All	1	
G4	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag All	1	
G5	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag All	1	
G6	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag All	1	
G7	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag All	1	
G8	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag All	1	
G9	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag All	1	
G10	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag All	1	
G11	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag All	1	

Описание каждого параметра представлено в следующей таблице:

Параметр	Описание
VLAN global configuration	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.
Port VLAN configuration	Конфигурация VLAN порта
Port	Логический номер порта.
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

Параметр	Описание
	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.



Примечания:

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

Описание каждого параметра представлено в следующей таблице:

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 1 with 20 entries per page. << >>

Port Members																														
VLAN ID	G1	G2	G3	G4	G5	G6	G7	G8	G9	G10	G11	G12	G13	G14	G15	G16	G17	G18	G19	G20	G21	G22	G23	G24	X1	X2	X3	X4	X5	X6
1	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

Описание каждого параметра представлено в следующей таблице:

Параметр	Описание
VLAN ID	Отобразить идентификатор VLAN порта-участника.
member port	Отобразить каждый порт-участник, соответствующий идентификатору VLAN.
combined	Переключение статуса участника VLAN, настроенного в различных модулях и представлениях пользователя, включая статус участника VLAN, настроенный в комбинированном представлении, представлении администратора и других модулях

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
G1	C-Port	<input checked="" type="checkbox"/>	All	1	Untag All		No
G2	C-Port	<input checked="" type="checkbox"/>	All	1	Untag All		No
G3	C-Port	<input checked="" type="checkbox"/>	All	1	Untag All		No
G4	C-Port	<input checked="" type="checkbox"/>	All	1	Untag All		No
G5	C-Port	<input checked="" type="checkbox"/>	All	1	Untag All		No
G6	C-Port	<input checked="" type="checkbox"/>	All	1	Untag All		No
G7	C-Port	<input checked="" type="checkbox"/>	All	1	Untag All		No
G8	C-Port	<input checked="" type="checkbox"/>	All	1	Untag All		No
G9	C-Port	<input checked="" type="checkbox"/>	All	1	Untag All		No
G10	C-Port	<input checked="" type="checkbox"/>	All	1	Untag All		No
G11	C-Port	<input checked="" type="checkbox"/>	All	1	Untag All		No
G12	C-Port	<input checked="" type="checkbox"/>	All	1	Untag All		No
G13	C-Port	<input checked="" type="checkbox"/>	All	1	Untag All		No
G14	C-Port	<input checked="" type="checkbox"/>	All	1	Untag All		No
G15	C-Port	<input checked="" type="checkbox"/>	All	1	Untag All		No
G16	C-Port	<input checked="" type="checkbox"/>	All	1	Untag All		No

Описание каждого параметра представлено в следующей таблице:

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.
conflict	Показать, есть ли у двух пользователей конфликты в конфигурации VLAN порта.
combined	Переключение статуса порта VLAN, настроенного в различных модулях и представлениях пользователя, включая статус порта VLAN, настроенный в комбинированном представлении, представлении администратора и других модулях.

4.2 Расширенные настройки VLAN

4.2.1 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.

MAC-based VLAN Membership Configuration Auto-refresh ☐ Refresh

			Port Members																													
Delete	MAC Address	VLAN ID	G1	G2	G3	G4	G5	G6	G7	G8	G9	G10	G11	G12	G13	G14	G15	G16	G17	G18	G19	G20	G21	G22	G23	G24	X1	X2	X3	X4	X5	X6
Currently no entries present																																

Add New Entry

Save Reset

Описание каждого параметра представлено в следующей таблице:

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

4.2.2 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.

4.2.2.1 Протокол-группа

Как показано ниже.

Protocol to Group Mapping Table

Auto-refresh ☐ Refresh

Delete	Frame Type	Value	Group Name
Currently no entries present			

Add New Entry

Save Reset

Описание каждого параметра представлено в следующей таблице:

Параметр	Описание
delete	Удалить соответствующую запись.
frame type	Тип кадра, доступны три типа кадров: Ethernet, SNAP и LLC.
value	<p>Для трех типов кадров действуют различные диапазоны значений.</p> <ul style="list-style-type: none"> Ethernet: 0x0600-0xFFFF. SNAP: OUI, PID. <ul style="list-style-type: none"> Диапазон конфигурации OUI: xx-xx-xx, диапазон каждого xx составляет от 0x00 до 0xff. Диапазон конфигурации PID: Если OUI равен 00, диапазон PID равен (0x0600-0xffff). В противном случае диапазон равен 0x0000-0xffff. LLC: DSAP, SSAP. <ul style="list-style-type: none"> Диапазон конфигурации DSAP: 0x00-0xff. Диапазон конфигурации SSAP: 0x00-0xff.
group name	Название созданной протокольной группы.

4.2.2.2 Группа-VLAN

Как показано ниже:

Group Name to VLAN mapping Table

Auto-refresh ☐ Refresh

			Port Members																													
Delete	Group Name	VLAN ID	G1	G2	G3	G4	G5	G6	G7	G8	G9	G10	G11	G12	G13	G14	G15	G16	G17	G18	G19	G20	G21	G22	G23	G24	X1	X2	X3	X4	X5	X6
Currently no entries present																																

Add New Entry

Save Reset

Описание каждого параметра представлено в следующей таблице:

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.

4.2.3 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.

IP Subnet-based VLAN Membership Configuration Auto-refresh ☐ Refresh

				Port Members																													
Delete	IP Address	Mask Length	VLAN ID	G1	G2	G3	G4	G5	G6	G7	G8	G9	G10	G11	G12	G13	G14	G15	G16	G17	G18	G19	G20	G21	G22	G23	G24	X1	X2	X3	X4	X5	X6
Currently no entries present																																	

Add New Entry

Save Reset

Описание каждого параметра представлено в следующей таблице:

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.

4.3 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.

4.3.1 Конфигурация участников

Как показано ниже..

Private VLAN Membership Configuration Auto-refresh ☐ Refresh

		Port Members																													
Delete	PVLAN ID	G1	G2	G3	G4	G5	G6	G7	G8	G9	G10	G11	G12	G13	G14	G15	G16	G17	G18	G19	G20	G21	G22	G23	G24	X1	X2	X3	X4	X5	X6
<input type="checkbox"/>	1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	

Add New Private VLAN

Save Reset

Описание каждого параметра представлено в следующей таблице:

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

4.3.2 Изоляция портов

Конфигурация изоляции портов.

Port Isolation Configuration Auto-refresh ☐ Refresh

		Port Members																													
		G1	G2	G3	G4	G5	G6	G7	G8	G9	G10	G11	G12	G13	G14	G15	G16	G17	G18	G19	G20	G21	G22	G23	G24	X1	X2	X3	X4	X5	X6
		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	

Save Reset

Описание каждого параметра представлено в следующей таблице:

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



Примечания:

- Поддерживается несколько групп частных VLAN, но поддерживается только одна группа изоляции портов.
- Группа изоляции разделяет только отмеченные порты друг от друга.

4.4 Перевод VLAN

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

4.4.1 Конфигурация групп портов

The port group configuration page is shown in the figure below.

VLAN Translation Port Configuration Auto-refresh ☐ Refresh

Port	Group Configuration	
	Default	Group ID
*	<input type="checkbox"/>	<> ▾
G1	<input type="checkbox"/>	1 ▾
G2	<input type="checkbox"/>	2 ▾
G3	<input type="checkbox"/>	3 ▾
G4	<input type="checkbox"/>	4 ▾
G5	<input type="checkbox"/>	5 ▾
G6	<input type="checkbox"/>	6 ▾
G7	<input type="checkbox"/>	7 ▾
G8	<input type="checkbox"/>	8 ▾
G9	<input type="checkbox"/>	9 ▾
G10	<input type="checkbox"/>	10 ▾
G11	<input type="checkbox"/>	11 ▾
G12	<input type="checkbox"/>	12 ▾
G13	<input type="checkbox"/>	13 ▾
G14	<input type="checkbox"/>	14 ▾

Описание каждого параметра представлено в следующей таблице:

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



Примечания:

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

4.4.2 Отображение VLAN

Страница отображения VLAN, показанная на рисунке ниже.

VLAN Translation Mapping Table

Auto-refresh ☐ Refresh Remove All

Group ID	Direction	VID	TVID

Описание каждого параметра представлено в следующей таблице:

Параметр	Описание
Group ID	Отображение перевода VLAN разделено на группы, определяемые идентификатором группы.
Direction	<p>Выберите направление входа, направление выхода или выберите все.</p> <ul style="list-style-type: none"> Двунаправленный: направление входа, направление выхода. Вход: направление входа. Выход: направление выхода.
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.



Примечания:

При применении перевода VLAN для входного идентификатора VLAN (VID) на входном порту, порт должен добавить TVID; при применении перевода VLAN для исходного идентификатора VLAN (VID) на выходном порту, порт должен добавить VID; при применении перевода VLAN для обоих идентификаторов VLAN (VID:TVID) на порту, порт должен добавить TVID.

4.5 Таблица MAC-адресов

Таблица MAC-адресов является таблицей маршрутизации на основе портов уровня 2 и является основой для быстрого пересылки пакетов. В таблице MAC-адресов содержится несколько записей маршрутизации, и каждая запись маршрутизации имеет соответствующий MAC-адрес назначения, порт VID и порт пересылки.

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																													
	G1	G2	G3	G4	G5	G6	G7	G8	G9	G10	G11	G12	G13	G14	G15	G16	G17	G18	G19	G20	G21	G22	G23	G24	X1	X2	X3	X4	X5	X6
Auto	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	
Disable	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	
Secure	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<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	G1	G2	G3	G4	G5	G6	G7	G8	G9	G10	G11	G12	G13	G14	G15	G16	G17	G18	G19	G20	G21	G22	G23	G24	X1	X2	X3	X4	X5	X6
Add New Static Entry																																

Save Reset

Описание каждого параметра представлено в следующей таблице:

Параметр	Описание
Aging time configuration	Информация о конфигурации времени устаревания
disable automatic aging	Поставьте отметку, чтобы отключить функцию автоматического устаревания MAC-адресов.
MAC address aging time	Время устаревания адресов настраивается, значение по умолчанию составляет 300 секунд, а диапазон настроек составляет от 10 до 1000000 секунд.

Параметр	Описание
MAC address table learning	Информация о изучении таблицы MAC-адресов
automatic	Автоматическое изучение MAC-адресов.
closure	Не изучать MAC-адреса.
safety	Можно настроить только статические записи MAC-адресов.
VLAN learning configuration	Информация о конфигурации изучения VLAN
list of VLANs prohibited from learning	Идентификаторы VLAN в списке не будут изучать MAC-адреса.
Static MAC address table configuration	Конфигурация статической таблицы MAC-адресов
delete	Удалить текущую запись.
VLAN ID	Идентификатор VLAN, связанный со статическим MAC-адресом.
MAC address	Статический MAC-адрес.
member port	Порт, связанный со статическим MAC-адресом.
add new static entry	Добавить новую запись в статическую таблицу MAC-адресов и указать идентификатор VLAN, MAC-адрес и принадлежность порту для новой записи.

4.5.2 Запись в таблице MAC-адресов

На этой странице отображается таблица MAC-адресов. Каждая запись пересылки имеет соответствующий адрес MAC назначения, VID порта и порт пересылки.

MAC Address Table

Auto-refresh ☐

Refresh

Clear

<<

>>

Start from VLAN and MAC address , with entries per page.

			Port Members																														
Type	VLAN	MAC Address	CPU	G1	G2	G3	G4	G5	G6	G7	G8	G9	G10	G11	G12	G13	G14	G15	G16	G17	G18	G19	G20	G21	G22	G23	G24	X1	X2	X3	X4	X5	X6
Static	1	00:00:00:0A:11:22	✓																														
Static	1	33:33:00:00:00:01	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Static	1	33:33:00:00:00:02	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Static	1	33:33:FF:00:00:00	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Static	1	33:33:FF:0A:11:22	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Dynamic	1	FC:45:96:4F:BE:9A	✓																														
Static	1	FF:FF:FF:FF:FF:FF	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

Описание каждого параметра представлено в следующей таблице:

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

4.6 IGMP отслеживание

4.6.1 Базовая конфигурация

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

Как показано ниже.

IGMP Snooping Configuration

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"/>	<> ▾
G1	<input type="checkbox"/>	<input type="checkbox"/>	unlimited ▾
G2	<input type="checkbox"/>	<input type="checkbox"/>	unlimited ▾
G3	<input type="checkbox"/>	<input type="checkbox"/>	unlimited ▾
G4	<input type="checkbox"/>	<input type="checkbox"/>	unlimited ▾
G5	<input type="checkbox"/>	<input type="checkbox"/>	unlimited ▾
G6	<input type="checkbox"/>	<input type="checkbox"/>	unlimited ▾
G7	<input type="checkbox"/>	<input type="checkbox"/>	unlimited ▾
G8	<input type="checkbox"/>	<input type="checkbox"/>	unlimited ▾
G9	<input type="checkbox"/>	<input type="checkbox"/>	unlimited ▾
G10	<input type="checkbox"/>	<input type="checkbox"/>	unlimited ▾

Описание каждого параметра представлено в следующей таблице:

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

Параметр	Описание
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.
Port configuration	Конфигурация портов
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

Это устройство поддерживает независимую настройку функции IGMP-Snooping в пределах VLAN. Настройка VLAN используется для конфигурации связанных параметров в определенном VLAN, как показано на следующей иллюстрации:

IGMP Snooping VLAN Configuration

Start from VLAN 1, with 20 entries per page.

Refresh << >>

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

Save Reset

Описание каждого параметра представлено в следующей таблице:

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 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.

Параметр	Описание
Protocol version	<p>Настройка версии протокола.</p> <ul style="list-style-type: none"> Автоматическое распознавание IGMP: автоматическое адаптирование версии IGMP. IGMPv1: принудительное использование IGMPv1. IGMPv2: принудительное использование IGMPv2. IGMPv3: принудительное использование IGMPv3.
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.

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.

IGMP Snooping Status Auto-refresh ☐ Refresh Clear

Statistics

VLAN	Querier	Host	Querier	Queries	Queries	V1 Reports	V2 Reports	V3 Reports	V2 Leaves
ID	Version	Version	Status	Transmitted	Received	Received	Received	Received	Received

Router Port

Port	Status
G1	-
G2	-
G3	-
G4	-
G5	-
G6	-
G7	-
G8	-
G9	-
G10	-
G11	-
G12	-
G13	-

Содержание таблицы статистики состояния IGMP-Snooping слева направо следующее: идентификатор VLAN, версия IGMP опросника, версия IGMP хоста, подключенного к порту-участнику, статус опросника, количество отправленных опросных сообщений опросником, количество полученных опросных сообщений опросником, количество полученных сообщений о присоединении IGMPv1, количество полученных сообщений о присоединении IGMPv2, количество полученных сообщений о присоединении IGMPv3, количество полученных сообщений об уходе IGMPv2.

В таблице портов маршрутизатора отображается режим конфигурации порта маршрутизатора, динамическое обучение или статическая конфигурация.

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 1 and group address 224.0.0.0 with 20 entries per page.

		Port Members																													
VLAN ID	Groups	G1	G2	G3	G4	G5	G6	G7	G8	G9	G10	G11	G12	G13	G14	G15	G16	G17	G18	G19	G20	G21	G22	G23	G24	X1	X2	X3	X4	X5	X6
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 определяет конфигурационный файл фильтрации для определенного порта. Для этой конфигурации необходимо предварительно настроить конфигурационный файл фильтрации многоадресных передач. Если на системе отсутствует такой файл конфигурации фильтрации многоадресных передач, то конфигурационный файл не может быть указан для данного порта. Как показано ниже:

IGMP Snooping Port Filtering Profile Configuration

Port	Filtering Profile
G1	-
G2	-
G3	-
G4	-
G5	-
G6	-
G7	-
G8	-
G9	-
G10	-
G11	-
G12	-
G13	-
G14	-
G15	-
G16	-
G17	-
G18	-

Выберите конфигурационный файл фильтрации для соответствующего порта и нажмите "Сохранить".

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 1 and group address 224.0.0.0 with 20 entries per page.

VLAN ID	Groups	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 MLD-отслеживание

4.7.1 Базовая конфигурация

Страница базовой конфигурации веб-интерфейса включает две части: "Глобальная конфигурация" и "Конфигурация портов". Как показано ниже.

MLD Snooping Configuration

Global Configuration	
Snooping Enabled	<input checked="" type="checkbox"/>
Unregistered IPMCv6 Flooding Enabled	<input checked="" type="checkbox"/>
MLD SSM Range	ff3e:: / 32
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"/>	<> ▾
G1	<input type="checkbox"/>	<input type="checkbox"/>	Unlimited ▾
G2	<input type="checkbox"/>	<input type="checkbox"/>	Unlimited ▾
G3	<input type="checkbox"/>	<input type="checkbox"/>	Unlimited ▾
G4	<input type="checkbox"/>	<input type="checkbox"/>	Unlimited ▾
G5	<input type="checkbox"/>	<input type="checkbox"/>	Unlimited ▾
G6	<input type="checkbox"/>	<input type="checkbox"/>	Unlimited ▾
G7	<input type="checkbox"/>	<input type="checkbox"/>	Unlimited ▾
G8	<input type="checkbox"/>	<input type="checkbox"/>	Unlimited ▾

Описание каждого параметра представлено в следующей таблице:

Параметр	Описание
Global configuration	Глобальная конфигурация
snooping enabled	Глобальный переключатель включения функции MLD-Snooping. Предпосылкой для включения функции MLD-Snooping в VLAN является включение этого переключателя на этом коммутаторе.
unknown IPv6 multicast flooding enabled	Включить переключатель рассылки неизвестных IPv6 многоадресных пакетов
MLD SSM range	Диапазон многоадресных адресов IPv6 SSM, формат адреса - IPv6. По умолчанию диапазон адресов групповой рассылки - FF3x::/32, где x представляет собой любой допустимый диапазон, не равный 1 или 2 (область - это поле в формате адреса IPv6).

Параметр	Описание
	Значение по умолчанию - ff3e::/32.
done message proxy enable	Включить прокси-сервер сообщений Done MLD. После включения можно сократить пересылку ненужных сообщений Done верхнему потоку сети.
agent enabled	Включить прокси-сервер MLD. После включения устройство может проксировать запрос квивера для отправки запросов вниз по потоку к узлам-членам, а также проксировать пакеты отчета о членстве от узлов вниз по потоку к устройству вверх по потоку.
Port configuration	Конфигурация портов
port	Номер порта устройства.
router port	Настроить статические порты маршрутизаторов.
quickly leave the group	Включить функцию быстрого отсоединения для определенного порта.
entry restrictions	Ограничение на количество записей адресов. После установки максимальное количество записей, которое может изучить определенный порт

4.7.2 VLAN конфигурация

Это устройство поддерживает независимую конфигурацию функции MLD-Snooping в пределах VLAN. Конфигурация VLAN используется для настройки связанных параметров в пределах конкретного VLAN, как показано на следующей иллюстрации:

MLD Snooping VLAN Configuration Refresh |<< >>

VLAN Start from VLAN 1 with 20 entries per page.

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

Save Reset

Описание каждого параметра представлено в следующей таблице:

Параметр	Описание
VLAN ID	Номер идентификатора VLAN.
snooping enabled	Переключатель активации функции MLD-Snooping в конкретном VLAN.
querier election	Переключатель активации выбора запроса.
protocol version	Настройка версии протокола. <ul style="list-style-type: none"> MLD-Auto: Автоматический выбор версии протокола MLD. Когда коммутатор работает в этой версии протокола, хост

Параметр	Описание
	<p>может свободно выбирать одну из всех версий протокола, таких как MLDv1 и MLDv2.</p> <ul style="list-style-type: none"> • MLDv1: Принудительное использование MLDv1. • MLDv2: Принудительное использование MLDv2
priority	Приоритет, диапазон значений от 0 до 7, где 7 - наивысший приоритет, а значение по умолчанию - 0. Этот приоритет используется для конфигурации поля приоритета метки VLAN в различных протокольных пакетах.
robustness factor	Коэффициент надежности, диапазон значений от 1 до 255, значение по умолчанию - 2.
query interval (seconds)	Интервал запроса, временной интервал для отправки общих запросов группы запросов. Диапазон значений от 1 до 31744, значение по умолчанию - 125.
maximum query response time (0.1 seconds)	Максимальное время ответа на запрос группы общих запросов, диапазон значений от 0 до 65535, значение по умолчанию - 100.
specific (source) group query message interval (0.1 seconds)	Для отправки конкретных (исходных) запросов группы. Диапазон значений от 0 до 31744. Значение по умолчанию - 10

4.7.3 Статус

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

MLD Snooping Status

Auto-refresh ☐ Refresh Clear

Statistics

VLAN IDQuerier VersionHost VersionQuerier StatusQueries TransmittedQueries ReceivedV1 Reports ReceivedV2 Reports ReceivedV1 Leaves Received

Router Port

Port	Status
G1	-
G2	-
G3	-
G4	-
G5	-
G6	-
G7	-
G8	-
G9	-
G10	-
G11	-
G12	-

Таблица статистики состояния MLD-Snooping слева направо включает следующие параметры:

Идентификатор VLAN, версия протокола запросчика (querier), версия протокола хоста, подключенного к порту-члену (member port), состояние запросчика, количество отправленных запросов запросчиком (querier), количество полученных запросов запросчиком (querier), количество полученных сообщений MLD v1 отчетов, количество полученных сообщений MLD v2 отчетов и количество полученных сообщений MLD v1 о покидании группы.

Таблица портов маршрутизатора показывает режим конфигурации порта маршрутизатора, динамическое обучение или статическую конфигурацию.

4.7.4 Групповая информация

Эта веб-страница отображает все изученные записи IPv6 многоадресной группы, как показано на следующем рисунке..:

MLD Snooping Group Information

Auto-refresh ☐ Refresh << >>

Start from VLAN 1 and group address #00: with 20 entries per page.

Port Members																															
VLAN ID	Groups	G1	G2	G3	G4	G5	G6	G7	G8	G9	G10	G11	G12	G13	G14	G15	G16	G17	G18	G19	G20	G21	G22	G23	G24	X1	X2	X3	X4	X5	X6
No More Entries																															

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

4.7.5 Настройка фильтра

Эта веб-страница указывает конфигурационный файл фильтрации для определенного порта. Файл конфигурации фильтрации многоадресных пакетов должен быть предварительно сконфигурирован перед этой настройкой. Если в системе нет конфигурационного файла фильтрации многоадресных пакетов, то нельзя указать файл конфигурации для порта. Как показано ниже:

MLD Snooping Port Filtering Profile Configuration

Port	Filtering Profile
G1	-
G2	-
G3	-
G4	-
G5	-
G6	-
G7	-
G8	-
G9	-
G10	-
G11	-
G12	-
G13	-
G14	-
G15	-
G16	-
G17	-
G18	-

Выберите конфигурационный файл фильтрации для соответствующего порта и нажмите кнопку "Сохранить".

4.7.6 SFM информация

SFM (Source Filtering Multicast) - Фильтрация по источнику мультикаста. Эта веб-страница отображает всю информацию о записях SFM, как показано на следующем рисунке:

MLD SFM Information

Auto-refresh ☐ Refresh << >>

VLAN Start from VLAN 1 and Group #00: with 20 entries per page.

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

Информация, содержащаяся в записи информации о SFM, расположена слева направо::

VLAN ID, IPv6-адрес группы, номер порта, режим фильтрации (ВКЛЮЧИТЬ/ИСКЛЮЧИТЬ), адрес источника, тип (Разрешить/Запретить), аппаратное коммутаторное устройство.

4.8 Фильтрация многоадресной рассылки

4.8.1 Файл конфигурации

Фильтрация многоадресных передач используется для развертывания контроля доступа к IP-многоадресным потокам. Эта веб-страница позволяет создавать файлы конфигурации фильтрации многоадресных передач и ассоциировать правила для этих файлов конфигурации. Как показано ниже:

IPMC Profile Configurations

Global Profile Mode Disabled ▾

IPMC Profile Table Setting





Delete	Profile Name	Profile Description	Rule
Delete			

Add New IPMC Profile

Save Reset

Описание каждого параметра представлено в следующей таблице:

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.
Multicast filtering configuration file table	Таблица файла конфигурации фильтрации многоадресной рассылки:
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




Параметр	Описание
	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">  Перечисляет правила, связанные с указанным подмножеством.  Регулирует правила, связанные с указанным подмножеством.

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

Эта страница предоставляет настройки правил фильтрации для определенного профиля. Она отображает настроенные записи правил в порядке приоритета. Первая запись правила имеет наивысший приоритет при поиске, а последняя запись правила имеет наименьший приоритет при поиске.





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

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

Описание каждого параметра представлено в следующей таблице:

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	Опишем действие обучения, когда получен кадр

Параметр	Описание
	<p>присоединения/отчета с групповым адресом, совпадающим с диапазоном адресов, заданным в правиле.</p> <ul style="list-style-type: none"> Запретить (Deny): удалить групповые адреса, совпадающие с указанным диапазоном в правиле. Разрешить (Allow): обучиться групповым адресам, совпадающим с указанным диапазоном в правиле.
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"> Включено (Enabled): регистрировать соответствующую информацию для групповых адресов, совпадающих с диапазоном, указанным в правиле. Отключено (Disabled): не регистрировать соответствующую информацию для групповых адресов, совпадающих с диапазоном, указанным в правиле.
Rule management button	<p>Вы можете управлять правилами и соответствующими приоритетами с помощью следующих кнопок:</p> <ul style="list-style-type: none"> : Добавляет новое правило перед текущей записью правила. : Удаляет текущую запись правила. : Перемещает текущую запись правила вверх по списку. : Перемещает текущую запись правила вниз по списку.

4.8.2 Записи адресов

Эта страница предоставляет настройки диапазона адресов, которые должен использовать профиль фильтрации многоадресной рассылки. Записи адресов используются для указания диапазона адресов, который будет связан с профилем.

IPMC Profile Address Configuration

Refresh |<< >>

Navigate Address Entry Setting in IPMC Profile by 20 entries per page.

Delete	Entry Name	Start Address	End Address
Delete			

Add New Address(Range) Entry

Save Reset

Описание каждого параметра представлено в следующей таблице:

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.

4.9 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.

4.9.1 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

Interface Configuration

Interface	Mode	CDP aware	Trap	Optional TLVs				
				Port Descr	Sys Name	Sys Descr	Sys Capa	Mgmt Addr
*	<> v	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
G1	Disabled v	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
G2	Disabled v	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
G3	Disabled v	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
G4	Disabled v	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
G5	Disabled v	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
G6	Disabled v	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
G7	Disabled v	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
G8	Disabled v	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
G9	Disabled v	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
G10	Disabled v	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Описание каждого параметра представлено в следующей таблице:

Параметр	Описание
LLDP parameters	Конфигурация параметров LLDP

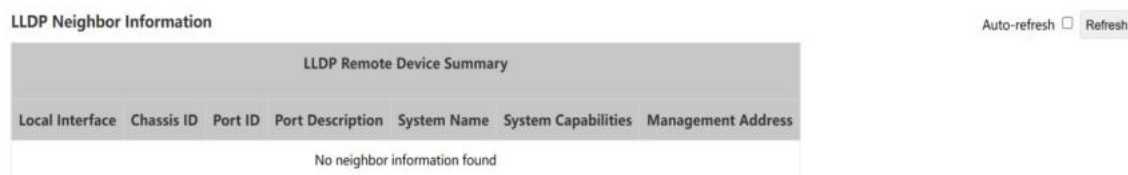
Параметр	Описание
Sending interval	Интервал отправки кадров LLDP: Переключатель периодически отправляет LLDP-кадры своим соседям для обновления информации о сети. Интервал отправки между LLDP-кадрами определяется этим значением. Значение по умолчанию для интервала отправки составляет 30 секунд, и значение 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 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.
LLDP interface configuration	Конфигурация интерфейса LLDP
Interface	Логическое имя интерфейса коммутатора.
Operating mode	<ul style="list-style-type: none"> Выберите режим работы интерфейса LLDP. Режимы следующие: Только прием: принимать только кадры LLDP и не отправлять кадры LLDP. Только отправка: отправлять только кадры LLDP и не принимать кадры LLDP. Не отправлять/не принимать: не отправлять и не принимать кадры LLDP. Отправка/прием: и отправлять, и принимать кадры LLDP.
CDP discovery	Когда выбрано, это используется для декодирования кадров CDP. Коммутатор не будет отправлять кадры CDP. Кадры CDP будут

Параметр	Описание
	<p>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"> • Поле "Device ID" CDP TLV сопоставляется с полем "Chassis ID" LLDP; • 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; • Поле "Port ID" CDP TLV сопоставляется с полем "Port ID" LLDP; • Поле "Version and Platform" CDP TLV сопоставляется с полем "System Description" LLDP; • Поле "Port ID" CDP TLV сопоставляется с полем "Port ID" LLDP; • Поле "Port ID" CDP TLV сопоставляется с полем "Port ID" LLDP; • Поле "Port ID" CDP TLV сопоставляется с полем "Port ID" LLDP; • Поле "Port ID" CDP TLV сопоставляется с полем "Port ID" LLDP. <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. Примечание: Когда "CDP discovery" отключено на интерфейсе, информация CDP не будет немедленно удалена, но будет удалена по истечении времени удержания.</p>
Trap	При выборе этой опции будут отправляться SNMP-трапы при изменении таблицы информации о соседних устройствах на интерфейсе.
Optional TLVs	<ul style="list-style-type: none"> • Описание порта: Дополнительный TLV. При выборе этой опции в LLDP передается информация об описании порта.

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

4.9.2 Информация о соседях

Страница с информацией о соседях отображена на рисунке ниже.



Описание каждого параметра представлено в следующей таблице:

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"> Others Repeater (Репитер) Bridge (Мост)

Параметр	Описание
	<ul style="list-style-type: none"> WLAN access point (Точка доступа WLAN) Router (Маршрутизатор) Telephone (Телефон) Cable equipment (Кабельное оборудование) Site only (client) (Только клиент на сайте) Reserved (Зарезервировано)
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.

4.9.3 MED конфигурация

Страница конфигурации MED показана на рисунке ниже.

LLDP_MED Configuration

Fast Start Repeat Count

Fast Start Repeat Count 4

LLDP MED Interface Configuration

Interface	Transmit TLVs			Device Type
	Capabilities	Policies	Location	
*	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<> ▾
G1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Connectivity ▾
G2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Connectivity ▾
G3	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Connectivity ▾
G4	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Connectivity ▾
G5	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Connectivity ▾
G6	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Connectivity ▾
G7	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Connectivity ▾
G8	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Connectivity ▾

Coordinates Location

Latitude 0 ° North ▾ Longitude 0 ° East ▾ Altitude 0 Meters ▾ Map Datum WGS84 ▾

Civic Address Location

Country Code		State		County	
City		City District		Block (Neighborhood)	
Street		Leading Street Direction		Trailing Street Suffix	
Street Suffix		House No.		House No.Suffix	
Landmark		Additional Location Info		Name	
Zip Code		Building		Apartment	
Floor		Room No.		Place Type	
Postal Community Name		P.O.Box		Addition Code	

Emergency Call Service

ELIN

Policies

Delete	Policy ID	Application Type	Tag	VLAN ID	L2 Priority	DSCP
No Policies						

Add New Policy

Policies Interface Configuration

Save Reset

Описание каждого параметра представлено в следующей таблице:

Параметр	Описание
number of messages sent quickly	Количество пакетов быстрого ответа, которые отправляет подключенное устройство после получения нового LLDP_MED. Значение по умолчанию - 4, а диапазон значений может быть любым от 1 до 10.
LLDP MED interface configuration	Конфигурация интерфейса LLDP MED
interface	Логическое имя интерфейса коммутатора
TLVs to send	<ul style="list-style-type: none"> • Функция: Дополнительный TLV. При выборе этой опции информация о передаче LLDP_MED содержит информацию о функции. • Политика: Дополнительный TLV. При выборе этой опции информация о передаче LLDP_MED содержит информацию о политике. • Местоположение: Дополнительный TLV. При выборе этой опции информация о передаче LLDP_MED содержит информацию о местоположении..
equipment type	<ul style="list-style-type: none"> • TLV LLDP_MED не будет инициироваться до тех пор, пока устройство-конечная точка не будет обнаружено в качестве партнера по ссылке. После обнаружения партнера по ссылке (то есть получения пакета LLDP, содержащего информацию о MED), начните отправку пакетов LLDP, содержащих информацию о MED (включите состояние отправки), только когда изменится состояние ссылки порта или изменится режим работы LLDP (TX ONLY, TXRX меняется на RX ONLY, DISABLE), состояние отправки будет инициализировано, и LLDP_MED сообщения больше не будут активно отправляться. После инициализации состояния отправки, если обнаружен партнер по ссылке, начинается отправка пакетов LLDP, содержащих информацию о MED. • Конечное устройство: Начните передачу TLV LLDP_MED немедленно
coordinate location	<p>Установите координатное местоположение устройства:</p> <ul style="list-style-type: none"> • Широта: Широта устройства, разделенная на южную и северную широту, диапазон от 0 до 90°. • Долгота: Долгота, где расположено устройство, разделена на восточную и западную долготу, диапазон от 0 до 180°. • Высота: высота устройства, тип высоты метры, этажи, диапазон -2097151.9-2097151.9.

Параметр	Описание
	<ul style="list-style-type: none"> Система координат: Укажите геодезическую систему для использования: WGS84, NAD83/NAVD88, NAD83/MLLW
location information	<p>Установите информацию о местоположении устройства следующим образом:</p> <ul style="list-style-type: none"> Код страны, поддерживает только две заглавные буквы. Провинция Административный район (Муниципалитет) Город Район (округ) Коммуна (сельсовет) Улица Основная улица Подробности о районе Подробности о улице Место (номер дома) Подробности о месте (номер счета) Ориентир Информация о прикреплении адреса Имя Почтовый индекс Здание Блок Этаж

Параметр	Описание
	<ul style="list-style-type: none"> • Номер комнаты • Тип места • Название почтового сообщества • Почтовый ящик • Информация о прикреплении
Emergency call service	Настройка служб экстренного вызова
ELIN	Идентификатор ELIN службы экстренного вызова, используемый во время установки экстренного вызова к старой аналоговой сети CAMA или ISDN транк к центру обработки экстренных вызовов PSAP.
Strategy	Настройка сетевой политики, поддерживаемой LLDP_MED.
delete	Удаление выбранной сетевой политики.
policy ID	Идентификатор политики, диапазон от 0 до 31
app types	<p>Специализированный тип приложения, который условно поддерживает отдельные сетевые политики для следующих типов медиа:</p> <ul style="list-style-type: none"> • Аудио • Аудиосигнал • Аудио клиента • Аудиосигнал клиента • Аудио для программного телефона • Видеоконференция • Видеопоток • Видеосигнал
tag	Метка, указывающая, использует ли указанный тип приложения "тегированные" или "нетегированные" VLAN.
VLAN ID	Идентификатор VLAN (VID) порта, определенный в стандарте IEEE 802.1Q, действителен только при использовании политики "тегированных" VLAN.
L2 priority	Значение 802.1p CoS, используемое для приоритизации определенного приложения.
DSCP	Значение DSCP, используемое для обеспечения поведения

Параметр	Описание
	узла Diffserv для конкретных приложений.
add new strategy	Добавить новую сетевую политику.
Policy interface configuration	Конфигурация интерфейса политики.
interface	Логическое имя интерфейса коммутатора.
policy ID	Идентификатор политики, выберите, поддерживает ли интерфейс устройства сетевую политику

4.9.4 Информация о соседи MED

Информация о соседи MED (Media Endpoint Discovery) представлена на странице, показанной на рисунке ниже.

LLDP MED Peer information	
G5	
Device Type	Functions
Endpoint Class 1	LLDP-MED Capabilities, Network Policy, Location Identification
Locations	
Latitude:0.0000 North, Longitude:0.0000 East, Altitude:0.0 meter(s), Map datum:WGS84	
Emergency Call Service:	
Automatic	Automatic Status
Supported	Enabled
Automatic Function	
MAU Type	
100BASE-T full duplex mode, 100BASE-TX full duplex mode, 100BASE-TX half duplex mode, 100BASE-T full duplex mode, 10BASE-T half duplex mode 100BaseTXFD - 2 pair category 5 UTP, full duplex mode	

Описание каждого параметра представлено в следующей таблице:

Параметр	Описание
local interface	Интерфейс, на котором был получен кадр LLDP_MED.
equipment type	Тип устройства интерфейса, подключенного устройства или терминального устройства.
function	Передаваемая информация LLDP_MED включает в себя функции, политики и местоположения.
app types	Отдельные сетевые политики для поддерживаемых типов средств передачи.
strategy	Соответствие сетевой политике.
tag	Метка, указывающая, использует ли указанный тип приложения «тегированные» или «нетегированные» VLAN.
VLAN ID	Идентификатор VLAN (VID) порта, определенный в IEEE 802.1Q, действителен только при использовании политики «тегированные» VLAN.
priority	Значение CoS 802.1p, используемое для приоритизации определенного приложения.
DSCP	Значение DSCP, используемое для определения поведения

Параметр	Описание
	узла Diffserv для конкретных приложений.
place	Местоположение оборудования.
auto-negotiation	Поддержка ли автоматического согласования.
auto-negotiation status	Состояние автоматического согласования.
auto-negotiation function	Состояние автоматического согласования.
MAU type	Тип MAU

4.9.5 Статистика порта

Статистические значения делятся на глобальные счетчики и локальные счетчики.

Глобальные относятся к статистике всего коммутатора, а локальные - к статистике порта.

LLDP 总体统计值

自动刷新 ☐

刷新清除

总体统计值	
清除总体统计值	<input checked="" type="checkbox"/>
邻居信息最后更新时间	1970-01-01T08:00:00+08:00 (3819 secs. ago)
所有添加的邻居信息数目	0
所有删除的邻居信息数目	0
所有丢弃的邻居信息数目	0
所有过期的邻居信息	0

LLDP 统计本地计数器

本地接口	报文发送总数	报文接收总数	接收的错误报文数	丢弃的报文数	丢弃的TLVs总数	未知的TLVs总数	丢弃的不支持的TLV数目	过期的邻居数目	清除
*	*	*	*	*	*	*	*	*	<input checked="" type="checkbox"/>
G1	0	0	0	0	0	0	0	0	<input checked="" type="checkbox"/>
G2	0	0	0	0	0	0	0	0	<input checked="" type="checkbox"/>
G3	0	0	0	0	0	0	0	0	<input checked="" type="checkbox"/>
G4	0	0	0	0	0	0	0	0	<input checked="" type="checkbox"/>
G5	0	0	0	0	0	0	0	0	<input checked="" type="checkbox"/>
G6	0	0	0	0	0	0	0	0	<input checked="" type="checkbox"/>
G7	0	0	0	0	0	0	0	0	<input checked="" type="checkbox"/>
G8	0	0	0	0	0	0	0	0	<input checked="" type="checkbox"/>

Описание каждого параметра представлено в следующей таблице:

Параметр	Описание
LLDP overall statistical value	Общее статистическое значение LLDP.

Параметр	Описание
clear overall statistics	После проверки нажмите кнопку "Очистить", чтобы сбросить глобальный счетчик.
neighbor information last updated time	Показывает, когда была добавлена или удалена последняя запись. Также отображает время, прошедшее с момента последнего обнаружения изменений.
the number of all neighbor information added	Показывает количество новых записей, добавленных с момента последней перезагрузки коммутатора.
the number of deleted neighbor information	Показывает количество новых записей, которые были удалены с момента последней перезагрузки коммутатора.
the number of discarded neighbor information	Отображает количество кадров LLDP, отброшенных из-за заполнения таблицы входящего потока

5 Кольцевая избыточность

5.1 Быстрая кольцевая сеть

Технология быстрой кольцевой сети - это протокол частной кольцевой сети, разработанный и спроектированный нашей компанией специально для высоконадежных промышленных сетей управления. Он позволяет соединять коммутаторы с избыточными связями. Если одна из них отключается, другая связь может быть быстро и автоматически восстановлена. При прерывании сети или отказе сети у нее есть избыточность каналов и быстрые возможности самовосстановления. Технология быстрой кольцевой сети позволяет пользователям назначать некоторые порты коммутатора в качестве избыточных портов кольцевой сети для подключения к другим коммутаторам. Когда одно из сетевых соединений прерывается, механизм избыточности быстрой кольцевой сети позволяет резервному каналу быстро восстановить сетевые коммуникации.

5.1.1 Конфигурация быстрой кольцевой сети

На странице отображается информация о конфигурации быстрой кольцевой сети, как показано на рисунке ниже. Вся настроенная информация о группах кольцевой сети будет отображаться на этой странице.

Ring Configuration Auto-refresh ☐ Refresh

Ring Number	Ring ID	Primary Port	Secondary Port	Hello-time	Fail-time	Priority	Ring Enable
<div>+</div>							

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

Ring Number	Ring ID	Primary Port	Secondary Port	Hello-time	Fail-time	Priority	Ring Enable
<input type="text"/>	<input type="text"/>	G1 <input type="button" value="v"/>	G1 <input type="button" value="v"/>	<input type="text" value="1"/>	<input type="text" value="3"/>	<input type="text" value="100"/>	<input type="checkbox"/>

Save Reset Cancel

Описание каждого параметра представлено в следующей таблице:

Параметр	Описание
ring network number	Номер группы кольцевой сети, используемый этим устройством для различения разных групп кольцевой сети, диапазон от 1 до 32.
ring ID	Идентификатор кольцевой сети, единственный идентификатор кольца в той же группе кольцевой сети, диапазон от 1 до 255.
main port	Порт кольцевой сети группы. Когда кольцевая сеть формирует кольцо, ссылка, где находится основной порт главного узла, является основной ссылкой. Вы можете выбрать любой порт из списка портов устройства в качестве основного порта.
slave port	Порт кольцевой сети группы. Когда кольцевая сеть формирует кольцо, ссылка, где находится резервный порт главного узла, является резервной ссылкой. Вы можете выбрать любой порт из списка портов устройства в качестве резервного порта.
hello-time	Период обнаружения кольцевой сети, диапазон от 1 до 21845, единица измерения - секунда. Условие 3Hello-time <= Fail-time должно быть выполнено.
fail-time	Время ожидания кольцевого тайм-аута, диапазон от 3 до 65535, единица измерения - секунда. Условие 3Hello-time <= Fail-time должно быть выполнено.
priority	Приоритет узла кольцевой сети, используемый для выбора между узлами. Чем меньше значение, тем выше приоритет. Диапазон от 1 до 254.
ring network enabled	Переключатель включения группы кольцевой сети

Нажмите на значок редактирования, чтобы перейти на страницу редактирования группы кольцевой сети, как показано:

Ring Number	Ring ID	Primary Port	Secondary Port	Hello-time	Fail-time	Priority	Ring Enable
1	2	G1	G1	1	3	100	<input type="checkbox"/>

Save Reset Cancel

Пожалуйста, обратите внимание на следующее при редактировании:

- Номер кольца и идентификатор кольца не могут быть изменены.
- При включенной группе кольцевой сети параметры кольцевой сети не могут быть изменены. Группа кольцевой сети должна быть отключена сначала, а затем изменена.



Примечания:

- При настройке порта быстрой кольцевой сети необходимо отключить функцию покрывающего дерева на порту.
- При настройке порта кольцевой сети быстрой передачи необходимо отключить функцию обнаружения обратной петли на порту.
- Порт быстрой кольцевой сети не может быть портом кольцевой сети ERPS.

5.1.2 Статус быстрой кольцевой сети

Вы можете просмотреть текущий статус быстрой кольцевой сети на странице информации о статусе быстрой кольцевой сети, как показано на следующем рисунке:

Ring Status												Auto-refresh <input type="checkbox"/> Refresh
Ring Number	Ring ID	Primary Port	Secondary Port	Hello-time	Fail-time	Priority	Ring Enable	Ring Status	Node Type	Node ID	Master ID	
1	2	G1	Forwarding	G2	Forwarding	1	3	100	Disabled	Idle	Master	00:00:00:0A:11:22 00:00:00:0A:11:22

Описание каждого параметра представлено в следующей таблице:

Параметр	Описание
ring network number	Отображает информацию о текущем номере группы кольцевой сети, а конфигурационные параметры описаны в разделе "Настройка быстрой кольцевой сети".
ring ID	Отображает информацию о текущем идентификаторе группы кольцевой сети. Для описания различных параметров обратитесь к разделу "Конфигурация быстрой кольцевой сети".
main port	Показывает информацию о текущем статусе пересылки основного порта кольцевой сети в реальном времени, включая Пересылка,

Параметр	Описание
	Отбрасывание и Блокировка.
slave port	Отображает информацию о текущем статусе пересылки резервного порта кольцевой сети в реальном времени, включая Пересылка, Отбрасывание и Блокировка.
hello-time	Отображает информацию о Hello-time текущей группы кольцевой сети.
fail-time	Отображает информацию о Fail-time текущей группы кольцевой сети.
priority	Отображает информацию о приоритете этого узла в текущей группе кольцевой сети.
ring network enabled	Отображает информацию о текущем статусе включения группы кольцевой сети, Включено или Отключено.
ring network status	Отображает информацию о статусе кольца текущей кольцевой сети, включая Простой, Инициализация, Ошибка и Завершение.
node type	Отображает тип узла этого узла в текущей группе кольцевой сети, Мастер, Транзит.
node ID	Отображает информацию об идентификаторе этого узла.
master node ID	Отображает информацию об идентификаторе мастер-узла текущей группы кольцевой сети

5.2 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.

5.2.1 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	RingId	NodeId	Level	Control	Rev	Guard	WTR	Hold Off	Enable	Oper	Warning
	Mode	Port			Instance	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-#	Ver	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"/>	0	<input type="checkbox"/>	G1	G1	1	00:00:00:00:00:00	0	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

Описание каждого параметра представлено в следующей таблице:

Параметр	Описание
Configuration	Конфигурация
ERPS example	ID экземпляра кольца ERPS.
version	Версия протокола ERPS, опционально V1 или V2.
ring network type	Тип кольцевой сети ERPS: Major представляет основное кольцо, Sub - дополнительное кольцо, а InterSub - дополнительное кольцо на межсоединенном узле.
virtual channel	Виртуальный канал: отмечено означает включено, неотмечено - выключено.
main ring to which it belongs	ID основного кольца, к которому относится дополнительное кольцо на межсоединенном узле.
topology change notification	Состояние объявления обнаружения топологии. Отметьте, чтобы включить эту функцию.
port0	Порт кольца: Port0 представляет восточный порт, в режиме InterSub действует только Port0.
port1	Групповой кольцевой порт: Port1 представляет западный порт.
ring ID	Идентификатор кольца используется для уникальной идентификации кольца ERPS. Тот же идентификатор кольца должен быть сконфигурирован на всех узлах в одном кольце ERPS.
node ID	Идентификатор узла кольца.
MD/MEG level	Уровень сообщения R-APS.
VLAN	Управляющая VLAN, то есть протокольная VLAN, это VLAN, передаваемый в протокольных пакетах ERPS.
PCP	Приоритет PCP протокольных пакетов ERPS.
switchback	Revertive устанавливает режим реверсии кольцевой сети. Если

Параметр	Описание
mode	отмечено, это означает реверсию, а если не отмечено, это означает отсутствие реверсии.
guard	Таймер Guard-time запускается, когда порт обнаруживает восстановление связи, и используется для предотвращения появления излишних остаточных сообщений R-APS из-за задержки онлайн-пересылки, что может вызвать ненужные вибрации в сети. До истечения этого таймера интерфейс больше не обрабатывает все пакеты R-APS. Этот таймер влияет на производительность восстановления связи при возникновении нескольких точек отказа.
WTR	Таймер WTR. В режиме реверсии этот таймер запускается, когда узел-владелец получает сообщение NR в состоянии MS или FS. Он используется для предотвращения блокировки и повторного разблокирования порта RPL на кольцевой сети из-за мерцания сети. Перед истечением этого таймера RPL продолжает пересылать, и неполадочный узел отправляет сообщения NR. В течение этого периода, если узел-владелец снова получает сообщение SF, это означает, что в кольцевой сети все еще есть неисправный канал. Таймер отключается напрямую, и RPL продолжает пересылать. В противном случае, после истечения таймера узел-владелец блокирует RPL, отправляет сообщение (NR, RB) для оповещения временной точки блокировки о разблокировке и одновременно обновляет запись MAC-адреса.
hold off	Таймер Hold-off запускается, когда порт обнаруживает отказ связи, задерживая скорость сообщения о неисправности. При отказе связи ожидайте истечения таймера Hold-off и повторного сообщения, если неисправность еще существует. Это дает слою обслуживания возможность восстановить связь и избежать излишнего сообщения о неисправности. Длина этого таймера влияет на скорость сообщения о неисправности канала и производительность переключения канала при возникновении неисправности.
enable	Переключатель включения кольца, отмеченный означает включено, неотмеченный - отключено.
SF trigger	Конфигурация механизма срабатывания сигнала SF
type	Режим срабатывания сигнала SF: Link означает срабатывание на основе состояния связи порта, а MEP означает срабатывание на основе MEP, установленного портом.
maintenance domain	Действительно в режиме MEP: доменное имя MEP, настроенное на порте.
serve	Действительно в режиме MEP: имя службы MEP, настроенное на порте.
MEPID	Действительно в режиме MEP: идентификатор MEP, настроенный на порте.
Protect VLAN	Защитная VLAN.
VLAN ID	Список защитных VLAN. Та же защитная VLAN должна быть сконфигурирована на всех узлах в том же экземпляре кольца ERPS.

Параметр	Описание
RPL configuration	Конфигурация RPL.
node type	Роль узла ERPS: <ul style="list-style-type: none"> None представляет обычный узел; Owner представляет узел-владелец; Neighbor представляет соседний узел.
RPL port	Порт RPL узла ERPS



Примечания:

- Управляющая VLAN ERPS действует на протокольные пакеты ERPS. Не рекомендуется смешивать эту VLAN с другими служебными VLAN для предотвращения вмешательства в кольцевую сеть ERPS и влияния на стабильность кольцевой сети.
- При настройке механизма срабатывания информации о сигнале SF порта ERPS на MEP, необходимо убедиться, что конфигурация MEP порта корректна.

5.2.2 ERPS статус

Интерфейс отображения состояния ERPS.

ERPS Status Auto-refresh ☐ Refresh

ERPS-#	Oper	Warning	State	TxRapsActive	cFOPTo	Tx Info							
						UpdateTimeSecs	Request	Version	Rb	Dnf	Bpr	Node Id	SMAC

Описание каждого параметра представлено в следующей таблице:

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.

Параметр	Описание
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"> • Время обновления: Время последнего обновления статуса узла ERPS. Это время относительно времени запуска устройства. • Запрос: Тип сообщения. • Версия: Версия протокола ERPS, 0 представляет V1, 1 представляет V2. • Rb: Статус RPL-связи, × указывает, что связь RPL не заблокирована, и √ указывает, что связь RPL заблокирована. • Dnf: Уведомляет, следует ли обновить таблицу MAC-адресов, × означает, что таблица MAC-адресов не обновляется, × означает, что таблица MAC-адресов обновляется. • Vpr: Порт RPL. • Идентификатор узла: Идентификатор узла, переданный в сообщении R-APS, связан с конфигурацией. По умолчанию это MAC-адрес порта. • SMAC: MAC-адрес источника, используемый пакетами R-APS. По умолчанию это MAC-адрес порта.



Примечания:

- При настройке порта кольца ERPS необходимо отключить функцию покрывающего дерева на порту.
- Порт кольца ERPS не может одновременно быть портом кольца быстрой кольцевой сети.

Информация о состоянии ERPS

Нажмите на соответствующий экземпляр ERPS на странице конфигурации ERPS и странице состояния ERPS, чтобы перейти на страницу отображения информации о состоянии ERPS.

ERPS Status

Auto-refresh ☐ Refresh

Configuration

ERPS #	Ver	Type	VC	Prop	Port0	Port1	RingId	NodeId	Level	VLAN	PCP	Rev	Guard	WTR	HoldOff	Enable
1	v2	Major	×	×	G1	G2	1	00:00:00:00:00:00	0	1	7	✓	500	300	0	✓

Status

Oper	Warning	State	TxRapsActive	cFOPTo	UpdateTimeSecs	Request	Version	Rb	Dnf	Bpr	Node Id	SMAC
●	●	Protection	✓	✓	27185	Signal Failed	1	×	✓		RingPort1 00:00:00:0A:11:22 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	

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	3	0
Transmitted NR, RB R-APS PDUs	0	0
Transmitted SF R-APS PDUs	45	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	1

Описание каждого параметра представлено в следующей таблице:

Параметр	Описание
configuration	Отображает информацию о конфигурации текущего экземпляра ERPS. Для описания параметров конфигурации обратитесь к разделу конфигурации ERPS.
state	Отображает информацию о текущем состоянии экземпляра ERPS. Для описания различных параметров обратитесь к разделу статуса ERPS.
ring port status	Отображает информацию о текущем состоянии в реальном времени порта кольца текущего экземпляра ERPS. × означает, что статус не соответствует, √ означает, что статус соответствует.
packet statistics	Отображает количество полученных и отправленных пакетов R-APS каждого типа портом кольца текущего экземпляра ERPS.
recount	Вы можете очистить статистику пакетов R-APS, полученных и отправленных портом кольца текущего экземпляра ERPS, для повторного подсчета статистики
switching command	Текущий экземпляр ERPS поддерживает быстрое переключение. Команды переключения следующие: <ul style="list-style-type: none"> • No request: Без операции. • Принудительное переключение на порт0: Выполнить команду FS на порту 0. • Принудительное переключение на порт1: Выполнить команду FS на порту 1. • Ручное переключение на порт0: Выполнить команду MS на порту 0. • Ручное переключение на порт1: Выполнить команду MS на порту 1. • Очистить: Очистить статус переключения

5.3 Протокол связующего дерева

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 широковебательные 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.

5.3.1 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

☐

Edge Port BPDU Guard

☐

Port Error Recovery

☐

Port Error Recovery Timeout

Save

Reset

Описание каждого параметра представлено в следующей таблице:

Параметр	Описание
Basic configuration	Basic configuration
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

Параметр	Описание
	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 $\leq (\text{задержка передачи} - 1) \times 2$.
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.
Advanced configuration	Расширенная конфигурация
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.
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).

5.3.2 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

Configuration Revision

MSTI Mapping

MSTI	VLANs Mapped
MSTI1	<input type="text"/>
MSTI2	<input type="text"/>
MSTI3	<input type="text"/>
MSTI4	<input type="text"/>
MSTI5	<input type="text"/>
MSTI6	<input type="text"/>
MSTI7	<input type="text"/>
TE	<input type="text"/>

Save

Reset

Описание каждого параметра представлено в следующей таблице:

Параметр	Описание
Configuration definition	Определение конфигурации
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.
MSTI mapping	Отображение MSTI
MSTI	Экземпляры связующего дерева включают MSTI1-7 и TE. Экземпляр TE - это особый экземпляр. Все VLAN, отображенные на этот экземпляр,

Параметр	Описание
	всегда будут находиться в состоянии пересылки.
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.

5.3.3 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

Описание каждого параметра представлено в следующей таблице:

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

5.3.4 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		BPDU Guard	Point-to-point
						Role	TCN		
-	<input type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Force True

CIST Normal Port Configuration

Port	STP Enabled	Path Cost	Priority	Admin Edge	Auto Edge	Restricted		BPDU Guard	Point-to-point
						Role	TCN		
*	<input type="checkbox"/>	<>	<>	<>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<>
G1	<input type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
G2	<input type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
G3	<input type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
G4	<input type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
G5	<input type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
G6	<input type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
G7	<input type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
G8	<input type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
G9	<input type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
G10	<input type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto

Описание каждого параметра представлено в следующей таблице:

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.

Параметр	Описание
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"> Role: Это означает, что защита корня включена. После включения защиты корня порт не будет выбран в качестве корневого порта. TCN: Включена защита от TCN. После включения защиты TCN порт не будет принимать и пересылать сообщения о изменении топологии.
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"> Auto: Означает, что порт автоматически определяет, является ли он соединением точка-точка. Yes: Указывает, что порт насильно настроен как соединение точка-точка. No: Указывает, что порт принадлежит к общей сети.

5.3.5 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.

STP CIST Port Configuration

CIST Aggregated Port Configuration

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

CIST Normal Port Configuration

Port	STP Enabled	Path Cost	Priority	Admin Edge	Auto Edge	Restricted		BPDU Guard	Point-to-point
						Role	TCN		
*	<input type="checkbox"/>	<>	<>	<>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<>
G1	<input type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
G2	<input type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
G3	<input type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
G4	<input type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
G5	<input type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
G6	<input type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
G7	<input type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
G8	<input type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
G9	<input type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto

Описание каждого параметра представлено в следующей таблице:

Параметр	Описание
port	Порт Ethernet и порт агрегации.
path cost	Стоимость пути порта. Выберите значение по умолчанию для автоматического расчета. Выберите конкретное значение для вручную заполненного значения, в диапазоне от 1 до 200000000. Значение по умолчанию для порта 10 Гигабит составляет 2000, для порта Gigabit - 20000, для порта 100 Мбит - 200000, а для порта 10 Мбит - 2000000. Порт агрегации рассчитывается на основе накопленной пропускной способности соединенных портов и затем сопоставляется соответствующему значению стоимости пути или вручную заданному значению. Формула расчета (20000000/ширина полосы пропускания М).
priority	Приоритет порта

5.3.6 Статус моста

Страница отображения состояния моста выглядит следующим образом, как показано на рисунке ниже. Для каждого экземпляра можно отображать идентификатор моста, идентификатор корня, порт корня, стоимость пути к корню, флаг изменения топологии и время последнего изменения топологии.

STP Bridges

Auto-refresh ☐ Refresh

MSTI	Bridge ID	Root			Topology Flag	Topology Change Last
		ID	Port	Path Cost		
CIST	32768.00:00:00:0A:11:22	32768.00:00:00:0A:11:22	-	0	Steady	-

Описание каждого параметра представлено в следующей таблице:

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"> ID: Идентификатор моста текущего выбранного корневого моста. Root port: Порт коммутатора, в настоящее время назначенный ролью корневого порта. 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.
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	32768.00:00:00:0A:11:22
ID	32768.00:00:00:0A:11:22
Cost	0
Port	-
Regional Root	32768.00:00:00:0A:11:22
Internal Root Cost	0
Topology Flag	Steady
Topology Change Count	0
Topology Change Last	-

CIST Port & Aggregations State

Port	Port ID	Role	State	Path Cost	Admin Edge	Point-to-point	Uptime
No ports or aggregations active							

Описание каждого параметра представлено в следующей таблице:

Параметр	Описание
STP bridge status	Статус моста STP
Bridge instance	Экземпляры моста - CIST, MST1,...
Bridge ID	ID этого экземпляра моста.
Root bridge ID	ID моста выбранного корневого моста.
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.
CIST port and aggregation status	Статус порта и агрегации CIST
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.
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-

Параметр	Описание
	точка характер соединения порта влияет на то, насколько быстро он переходит в состояние STP.
Status update time	Время с момента последней инициализации порта моста.

5.3.7 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
G1	Non-STP	Forwarding	-
G2	Non-STP	Forwarding	-
G3	Non-STP	Forwarding	-
G4	Non-STP	Forwarding	-
G5	Non-STP	Forwarding	-
G6	Non-STP	Forwarding	-
G7	Non-STP	Forwarding	-
G8	Non-STP	Forwarding	-
G9	Non-STP	Forwarding	-
G10	Non-STP	Forwarding	-
G11	Non-STP	Forwarding	-
G12	Non-STP	Forwarding	-
G13	Non-STP	Forwarding	-
G14	Non-STP	Forwarding	-
G15	Non-STP	Forwarding	-
G16	Non-STP	Forwarding	-
G17	Non-STP	Forwarding	-

Описание каждого параметра представлено в следующей таблице:

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.

5.3.8 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 ☐ Refresh Clear

Port	Transmitted				Received				Discarded	
	MSTP	RSTP	STP	TCN	MSTP	RSTP	STP	TCN	Unknown	Illegal
No ports enabled										

Описание каждого параметра представлено в следующей таблице:

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

5.4 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.

5.4.1 Конфигурация обнаружения петель

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

Loop Protection Configuration

General Settings

Global Configuration

Enable Loop Protection

Disabled ▾

Transmission Time

5

Seconds

Shutdown Time

180

Seconds

Port Configuration

Port	Enable	Action	Tx Mode
*	<input type="checkbox"/>	<> ▾	<> ▾
G1	<input type="checkbox"/>	Shutdown Port ▾	Enabled ▾
G2	<input type="checkbox"/>	Shutdown Port ▾	Enabled ▾
G3	<input type="checkbox"/>	Shutdown Port ▾	Enabled ▾
G4	<input type="checkbox"/>	Shutdown Port ▾	Enabled ▾
G5	<input type="checkbox"/>	Shutdown Port ▾	Enabled ▾
G6	<input type="checkbox"/>	Shutdown Port ▾	Enabled ▾
G7	<input type="checkbox"/>	Shutdown Port ▾	Enabled ▾
G8	<input type="checkbox"/>	Shutdown Port ▾	Enabled ▾
G9	<input type="checkbox"/>	Shutdown Port ▾	Enabled ▾
G10	<input type="checkbox"/>	Shutdown Port ▾	Enabled ▾
G11	<input type="checkbox"/>	Shutdown Port ▾	Enabled ▾

Описание каждого параметра представлено в следующей таблице:

Параметр	Описание
Common configuration	Общая конфигурация
loopback detection enabled	<p>Общий переключатель включения обнаружения обратной петли.</p> <ul style="list-style-type: none"> Включить: Включить общий переключатель включения обнаружения обратной петли. Отключить: Отключить общий переключатель включения обнаружения обратной петли. (по умолчанию)
detection interval	Период обнаружения сообщений об обратной петле. Разрешенный диапазон настраиваемых значений составляет от 1 до 10 секунд. Значение по умолчанию - 5 секунд.
controlled recovery time	Время восстановления для перехода порта в контролируемое состояние. Разрешенный диапазон настраиваемых значений составляет от 1 до 604800 секунд. Значение по умолчанию - 180 секунд
Port configuration	Конфигурация порта
port	Представляет список портов.
enable	Когда отмечено, означает включение функции обнаружения обратной петли на этом порту. Первая строка представляет собой

Параметр	Описание
	пакетную конфигурацию, выберите все или не выбирайте все. По умолчанию отключено
controlled state	<p>Действия, выполняемые управляемым портом при обнаружении петли.</p> <ul style="list-style-type: none"> Закрыть порт: означает закрытие порта. Закрыть порт и записать журналы: означает закрытие порта и запись журналов. Только записать журналы: означает, что записываются только журналы.
send detection message	<p>Переключатель включения отправки портом пакетов обнаружения обратной петли.</p> <ul style="list-style-type: none"> Включить: Включить порт для отправки пакетов обнаружения обратной петли. (по умолчанию) Отключить: Отключить переключатель включения порта для отправки пакетов обнаружения обратной петли



Примечания:

- Функция обнаружения обратной петли действует только в случае, если общий переключатель включения обнаружения обратной петли находится в состоянии включения.
- Когда состояние включает в себя "Log", при обнаружении портом наличия петли можно просматривать соответствующий журнал обнаружения обратной петли в информации журнала.

5.4.2 Статус обнаружения петли

Используется для просмотра информации о статусе обнаружения петель.

Loop Protection Status

Auto-refresh ☐

Refresh

Port	Action	Tx Mode	Loops	Status	Loop	Time of Last Loop
Not ports enabled						

Описание каждого параметра представлено в следующей таблице:

Параметр	Описание
Port	Представьте список портов.
Controlled port	<p>Контролируемые действия для настройки порта:</p> <ul style="list-style-type: none"> Отключение: указывает на закрытие порта Отключение + журнал: означает закрытие порта и запись журнала Только журнал: указывает на запись только в журнал
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.
Port status	<p>Текущий статус порта.</p> <ul style="list-style-type: none"> Отключен: означает, что порт закрыт. Вверх: указывает на поднятое соединение порта. Вниз: указывает на отключенное соединение порта.
Current loopback status	<p>Укажите, обнаружен ли в текущем порту кольцевой обрыв.</p> <ul style="list-style-type: none"> Кольцо: указывает на наличие кольцевого обрыва -: указывает на отсутствие кольца
The time when the loopback was last detected	Последнее время обнаружения кольцевого обрыва на порту.


Примечания:

- Функция обнаружения обратной петли представляет собой только технологию обнаружения петель на одиночных узлах и не имеет функции разрыва петель на уровне сети.
- Состояние кольца обновляется в следующем цикле 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

Mode: Router

DNS Server 0: No DNS server

DNS Server 1: No DNS server

DNS Server 2: No DNS server

DNS Proxy: ☐

IP Interfaces

Delete	VLAN ID	Enabled	Type	IF_MAC	DHCPv4			Current Lease	IPv4		DHCPv6		
					Client ID	Hostname	Fallback		Address	Mask Length	Enabled	Rapid Commit	Current Lease
<input type="checkbox"/>	1	<input type="checkbox"/>	Auto	G1				0	192.168.16.253	24	<input type="checkbox"/>	<input type="checkbox"/>	128

Add Interface

IP Routes

Delete	Network	Mask Length	Gateway	Next Hop VLAN(IPv6)	Distance
--------	---------	-------------	---------	---------------------	----------

Add Route

Save Reset

Описание каждого параметра представлено в следующей таблице:

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

Параметр	Описание
	<ul style="list-style-type: none"> С этого интерфейса DHCPv4: Укажите, с какого интерфейса DHCPv4 предпочтительно использовать предоставленное доменное имя. С любых интерфейсов DHCPv6: Используйте первое предоставленное доменное имя из аренды DHCPv6 для интерфейса, включенного в DHCPv6. С этого интерфейса DHCPv6: Укажите, с какого интерфейса DHCPv6 предпочтительно использовать предоставленное доменное имя.
model	<p>Настройте устройство на работу в режиме "Хост" или "Маршрутизатор".</p> <ul style="list-style-type: none"> Хост: В режиме хоста IP-трафик между интерфейсами не будет маршрутизироваться. Маршрутизатор: В режиме маршрутизатора трафик маршрутизируется и пересылается между всеми интерфейсами.
DNS server 0-2	<p>Настройте сервер доменных имен (DNS), включая следующие режимы:</p> <ul style="list-style-type: none"> Без сервера доменных имен: Не использовать сервер доменных имен. Настроенный IPv4 или IPv6: Настройте сервер доменных имен IPv4 или IPv6. С любых интерфейсов DHCPv4: Используйте первый сервер доменных имен, предоставленный с арендой DHCPv4 для интерфейса, включенного в DHCPv4. С этого интерфейса DHCPv4: Укажите, с какого интерфейса DHCPv4 предпочтительно использовать предоставленный сервер доменных имен С любых интерфейсов DHCPv6: Используйте первый сервер доменных имен, предоставленный с арендой DHCPv6 для интерфейса, включенного в DHCPv6. С этого интерфейса DHCPv6: Укажите, с какого интерфейса DHCPv6 предпочтительно использовать предоставленный сервер доменных имен.
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>

Параметр	Описание
	<p>Примечание:</p> <p>В настоящее время поддерживаются только прокси-серверы DNS IPv4.</p>
IP interface	IP-интерфейс
delete	Удалить выбранный IP-интерфейс.
VLAN ID	VID (идентификатор VLAN) VLAN, связанный с IP-интерфейсом. Только порты внутри этой VLAN могут получить доступ к этому IP-интерфейсу. Это поле доступно только при создании нового интерфейса. Введите соответствующий идентификатор VLAN, диапазон от 1 до 4095.
DHCPv4	Настройте DHCPv4 на интерфейсе для получения адреса.
enable	При включенном DHCPv4 интерфейс действует как клиент DHCP и динамически получает IP-адрес от сервера
client ID	<p>Содержание поля option61 в DHCP-пакете, отправленном клиентом. Выберите тип IP-адреса клиента, включая режимы Auto, IF_MAC, ASCII и HEX.</p> <ul style="list-style-type: none"> • Auto: Автоматически генерирует идентификатор клиента согласно определенным правилам. • IF_MAC: Использует MAC-адрес соответствующего порта в качестве идентификатора клиента. • ASCII: Использует введенное содержимое в коде ASCII в качестве идентификатора клиента. • HEX: Вводит содержимое в шестнадцатеричном формате в качестве идентификатора клиента
host name	Hostname: Имя хоста DHCP-клиента. Если клиент DHCPv4 включен, настроенное имя хоста будет использоваться в поле option12 сообщения DHCP. Ввод должен соответствовать спецификациям доменного имени, и его длина не должна превышать 63 символа. Когда значение является пустой строкой, имя хоста будет автоматически сгенерировано согласно определенным правилам и заполнено в соответствующем поле сообщения.
fallback time	Таймаут ожидания предложения: После отправки клиентом сообщения Discover он ожидает ответа от сервера с действительным предложением. По истечении тайм-аута будет использоваться настроенный IPv4-адрес в качестве IPv4-адреса интерфейса. Это значение равно 0 для отключения механизма автоматической настройки. В этом случае, если действительное предложение не получено, DHCP будет повторно отправлять сообщения Discover для попытки получения адреса до получения действительного арендного соглашения. Допустимый диапазон

Параметр	Описание
	значений: 0 - 4294967295 секунд.
current rental address	Адрес интерфейса, предоставленный DHCPv4-сервером.
IPv4	Настройка статического IPv4-адреса на интерфейсе.
address	Настройка IPv4-адреса интерфейса в десятичном формате с точками. Если включен DHCP, в этом поле настраивается резервный адрес.
mask length	Настройка сетевой маски IPv4 интерфейса, выраженной в цифрах (длина префикса), и диапазон настройки составляет 1-30. Если включен DHCP, это поле настраивает резервную маску сети
DHCPv6	Включите DHCPv6 на интерфейсе.
enable	Включив механизм быстрого выделения DHCPv6, клиент DHCPv6 будет включать опцию Rapid Commit в сообщении Solicit; если сервер DHCPv6 также поддерживает эту функцию, он немедленно ответит сообщением Reply, содержащим адрес и другие параметры, назначенные клиенту, пропуская ответ сервера. Процесс взаимодействия между Advertise и запросом клиента.
quick allocation	Включите DHCPv6 на интерфейсе.
current rental address	Отображает адрес интерфейса, предоставленный сервером DHCPv6.
mask length	Установите длину маски для получения адреса клиентом DHCPv6, значение по умолчанию - 128;
IPv6	Настройте статический IPv6-адрес на интерфейсе.
address	Настройте IPv6-адрес интерфейса, допустимый одноадресный адрес, выраженный в шестнадцатеричном формате.
mask length	Настройте сетевую маску IPv6 интерфейса, выраженную в битах (длина префикса), и диапазон настройки составляет 1-128.
add interface	Щелкните кнопку "Добавить интерфейс", чтобы создать IP-интерфейс.
IP routing	Статическая IP-маршрутизация
delete	Удалите указанную запись статического маршрута.
network	IP-адрес сети или хоста маршрута. Допустимый формат - одноадресный адрес, выраженный в десятичном формате с точками (IPv4) или шестнадцатеричном формате (IPv6). Маршрут по умолчанию может быть представлен как 0.0.0.0 (IPv4) или :: (IPv6).
mask length	Длина сети или хоста маршрута, выраженная в битах (длина префикса). Диапазон длины IPv4 составляет 1-32, диапазон длины IPv6 составляет 1-128, и длина маршрута по умолчанию устанавливается на 0.
gateway	IP-адрес шлюза, допустимый формат - одноадресный адрес, выраженный в десятичном формате с точками (IPv4) или шестнадцатеричном формате (IPv6).
next hop VLAN (IPv6)	Идентификатор VLAN (VID) интерфейса IPv6, связанного с шлюзом. Диапазон значений VID составляет 1 ~ 4095. Этот параметр

Параметр	Описание
	требуется только в статической маршрутизации IPv6: если IPv6-адрес шлюза является локальным для сегмента, необходимо указать VLAN следующего перехода шлюза. Если IPv6-адрес шлюза не является локальным для сегмента, это значение следует установить равным 0.
distance	Используется для предоставления информации о приоритете маршрутизации маршрутизатору. Диапазон настроек - 1-255. При вовлечении двух или более разных протоколов маршрутизации и одинаковом назначении можно выбрать лучший путь на основе значения расстояния. Чем меньше значение, тем выше приоритет.
add route	Кнопка "Добавить маршрут" для создания записи статического маршрута.
save	Сохраните и примените текущую конфигурацию страницы.
reset	Отмените все изменения на этой странице перед щелчком по кнопке "Сохранить"

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 <input type="checkbox"/> Refresh
IF	Type	Address	Status	
VLAN 1	LINK	00:00:00:0A:11:22	<UP BROADCAST MULTICAST>	
VLAN 1	IPv4	192.168.16.253/24		
VLAN 1	IPv6	fe80::200:ff:fe0a:1122/64		
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			
192.168.16.200	VLAN 1:FC45:96:4F:BE:9A			
192.168.16.251	VLAN 1:00:02:B3:46:31:A1			
IPv6				
IP Address	Link Address			

Описание каждого параметра представлено в следующей таблице:

Параметр	Описание
IP interface	Отобразить информацию о конфигурации и статусе IP-

Параметр	Описание
	интерфейса:
Interface	Имя интерфейса.
Type	Тип адреса интерфейса, включая LINK, IPv4 и IPv6.
Address	Текущий адрес интерфейса.
Status	Текущий статус интерфейса.
IP routing	Отобразить информацию о маршрутизации IPv4 и IPv6:
Website address	Назначенный IPv4/IPv6 сетевой адрес или адрес хоста маршрута.
Gateway address	Адрес шлюза маршрута.
Status	Текущий статус маршрута.
Neighbor information	Отобразить информацию о соседях IPv4 и IPv6:
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.

IPv4 Routing Information Base 1 - 1 of 1 entry Auto-refresh ☐ Refresh << < > >>

Start from Network 192.168.16.0 / 24 Protocol Connected NextHop 0.0.0.0 with 20 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)	Status
C *	192.168.16.0/24	-	-	-	VLAN 1	03:04:11	Active

Описание каждого параметра представлено в следующей таблице:

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.

Параметр	Описание
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.

IPv6 Routing Information Base

1 - 1 of 1 entry

Auto-refresh ☐

Refresh

<<

<

>

>>

Start from Network fe80:: / 64 Protocol Connected NextHop :: with 20 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)	Status
C *	fe80::/64	-	-	-	VLAN 1	03:04:27	Active

Описание каждого параметра представлено в следующей таблице:

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 Маршрутизация и управление

6.2.1 Цепочка ключей

Эта страница настраивает цепочку ключей. Цепочка ключей в основном используется для аутентификации с помощью дайджеста MD5 в функции маршрутизации.

Router Key-Chain Configuration

Delete	Key Chain Name	Key ID
	*	*

Add Entry

Save Reset

Описание каждого параметра представлено в следующей таблице:

Параметр	Описание
delete	Щелкните "Сохранить" после проверки для удаления текущей выбранной записи.
add entry	Щелкните для создания цепочки ключей.
keychain name	Имя цепочки ключей, включая заглавные и строчные буквы, цифры и специальные символы, с максимальной длиной 31 символ.
key ID	Идентификатор ключа, значение от 1 до 255

После создания цепочки ключей и ее сохранения, после идентификатора ключа появится специальная иконка. Щелкните на этой иконке, чтобы перейти в интерфейс конфигурации идентификатора ключа. Пожалуйста, обратитесь к следующей главе для описания интерфейса.



Примечания:

Перед созданием цепочки ключей, пожалуйста, запустите протоколы динамической маршрутизации, такие как RIP, OSPF и т. д.

6.2.2 Идентификатор ключа

Эта страница используется для настройки ключей в цепочке ключей.

Описание каждого параметра представлено в следующей таблице:

Параметр	Описание
delete	Щелкните "Сохранить" после проверки, чтобы удалить текущую выбранную запись.
add entry	Щелкните, чтобы создать цепочку ключей.
keychain name	Имя цепочки ключей, состоящее из заглавных и строчных букв, цифр или специальных символов, с максимальной длиной 31 символ.
key ID	Идентификатор ключа, значение от 1 до 255.
key string	Символы шифрования ключа, состоящие из заглавных и строчных букв, цифр или специальных символов, с максимальной длиной 63 символа



Примечания:

В верхнем правом углу вы можете выбрать предварительно настроенную цепочку ключей, а по умолчанию отображаются все цепочки ключей.

6.2.3 Список доступа

Эта страница используется для списков доступа маршрутизации. Другие протоколы маршрутизации могут использовать этот список доступа для сопоставления записей таблицы маршрутизации и выполнения соответствующих контрольных действий.

Router Access-List Configuration

Delete	Name	Mode	Network Address	Mask Length
	*	*	*	*

Add Entry

Save Reset

Описание каждого параметра представлено в следующей таблице:

Параметр	Описание
delete	Щелкните "Сохранить" после отметки, чтобы удалить текущую выбранную запись.
add entry	Щелкните, чтобы создать список доступа.
entry name	Имя списка доступа, состоящее из заглавных и строчных букв, цифр или специальных символов, с максимальной длиной 31 символ.
model	Режим сопоставления записи таблицы, включая разрешение и блокировку.
website address	IP-адрес сопоставляемой сети.
mask length	Длина маски сопоставляемого IP-адреса сети

6.3 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.

6.3.1 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 Timer	30
	Invalid Timer	180
	Garbage-Collection	120
Redistribute	Static Mode	Disable
	Static Metric Value	<input checked="" type="radio"/> Auto <input type="radio"/> Specific 1
	Connected Mode	Disable
	Connected Metric Value	<input checked="" type="radio"/> Auto <input type="radio"/> Specific 1
	OSPF Mode	Disable
	OSPF Metric Value	<input checked="" type="radio"/> Auto <input type="radio"/> Specific 1
Default Metric Value		1
Default Route		Disable
Default Passive Mode		Disable
Administrative Distance		120

Save Reset

Описание каждого параметра представлено в следующей таблице:

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"> Версия 1: Основана на версии V1, только принимает и отправляет сообщения RIPv1. Версия 2: Основана на версии V2, только принимает и отправляет сообщения RIPv2. 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.
Timer	<p>Настройка различных таймеров включает:</p> <ul style="list-style-type: none"> 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.

Параметр	Описание
	<ul style="list-style-type: none"> 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. 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.
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"> Статическая маршрутизация: Настройте протокол RIP для внедрения записей статической маршрутизации. <ol style="list-style-type: none"> Режим: Включение или отключение внедрения записей статических маршрутов. 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. Прямая маршрутизация: Настройте протокол RIP для внедрения записей прямой маршрутизации. <ol style="list-style-type: none"> Режим: Включение или отключение внедрения записей прямых маршрутов. 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. Маршрутизация OSPF: Настройте протокол RIP для внедрения записей маршрутизации OSPF. <ol style="list-style-type: none"> Режим: Включение или отключение внедрения записей маршрутизации OSPF.

Параметр	Описание
	<p>2. Значение метрики: Настройка значения метрики для внедряемых маршрутов OSPF. Режим "Auto" использует значение метрики по умолчанию, а режим "Specific" использует указанное значение метрики. Диапазон значений от 1 до 16, по умолчанию 1.</p> <ul style="list-style-type: none"> 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. Реклама маршрута по умолчанию: Включение или отключение рекламы маршрутов по умолчанию RIP.
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.

6.3.2 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
	*	*

Add Entry

Save Reset

Описание каждого параметра представлено в следующей таблице:

Параметр	Описание
Delete	Delete
Website address	Website address
Mask length	Длина маски адреса интерфейса RIP, диапазон значений от 0 до 32.

6.3.3 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
	*

Add Entry

Save Reset

Описание каждого параметра представлено в следующей таблице:

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

6.3.4 Пассивный интерфейс

Это таблица конфигурации пассивных интерфейсов маршрутизатора RIP. Когда порт настроен в пассивном режиме, он не активно отправляет сообщения об обновлении RIP, а только пассивно принимает такие сообщения.

RIP Passive Interface Configuration

Interface	Passive Interface
*	

Описание каждого параметра представлено в следующей таблице:

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

6.3.5 Конфигурация интерфейса

Эта страница предназначена для настройки функций RIP интерфейса, включая типы отправки и приема пакетов, split horizon, poison reversal, аутентификацию пакетов и т. д.

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"/> <input type="text"/> <input type="text"/>

Описание каждого параметра представлено в следующей таблице:

Параметр	Описание
Interface	Имя интерфейса
Send message version	Версия пакетов RIP, отправляемых интерфейсом, включает: <ul style="list-style-type: none"> Версия 1: RIPv1 Версия 2: RIPv2

Параметр	Описание
	<ul style="list-style-type: none"> Версия 1 и 2: RIPv1 и RIPv2 Не указано: Не указано
Receive message version	<p>Версия пакетов RIP, принимаемых интерфейсом, включает:</p> <ul style="list-style-type: none"> Версия 1: RIPv1 Версия 2: RIPv2 Версия 1 и 2: RIPv1 и RIPv2 Не указано: Не указано Нет: Не принимать
Split Horizontally	<p>Настройте интерфейс для включения или отключения функций "горизонтального разделения" и "отравленного обратного хода", включая:</p> <ul style="list-style-type: none"> Split Horizon: включить горизонтальное разделение Poisoned Reverse: включить отмену отравления Disable: ни одна функция не включена
Certification type	<p>Настройте, аутентифицирует ли интерфейс пакеты RIP и тип аутентификации, включая:</p> <ul style="list-style-type: none"> Simple Password: Простая аутентификация по паролю, используя аутентификацию в виде обычного текста, необходимо настроить пароль, но пароль можно прочитать, перехватив пакеты. Message Digest: Аутентификация с использованием хэш-функции MD5, необходимо настроить ключевую цепочку, это более безопасный метод. Null Authentication: Нет аутентификации.
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:</p>

Параметр	Описание
	Простой пароль и имя ключевой цепочки не могут быть настроены одновременно.



Примечания:

При настройке аутентификации MD5 ключи, идентификаторы ключей и строки, настроенные на обеих сторонах интерфейса, должны быть согласованными. Рекомендуется настроить только один набор ключей в одной цепочке ключей.

6.3.6 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
	*	*	*	*

Add Entry

Save

Reset

Описание каждого параметра представлено в следующей таблице:

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.
Direction	Настроить направление, в котором выполняются операции смещения значения метрики маршрута и фильтрации пакетов на интерфейсе, включая входящий и исходящий трафик.

Параметр	Описание
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.



Примечания:

Списки контроля доступа настраиваются в модуле управления маршрутизацией.

6.3.7 Глобальный статус

Эта страница отображает текущую информацию о глобальных параметрах протокола RIP.

RIP Global Status		Clear RIP Process	Auto-refresh <input type="checkbox"/>	Refresh
Status Information				
Version	Default			
Update Timer	30 secs			
Invalid Timer	180 secs			
Garbage-Collection Timer	120 secs			
Next Update Time	25 secs			
Redistribute Default Metric	1			
Redistribute Connected	Disable			
Redistribute Static	Disable			
Redistribute OSPF	Disable			
Administrative Distance	120			

Описание каждого параметра представлено в следующей таблице:

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"> RIPv1: Основан на версии V1, он принимает и отправляет только сообщения RIPv1. RIPv2: Основан на версии V2, он принимает и отправляет только сообщения RIPv2. 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.

Параметр	Описание
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 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.

6.3.8 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	

Описание каждого параметра представлено в следующей таблице:

Параметр	Описание
Interface	Имя интерфейса.
Send message version	Версия пакетов RIP, отправляемых интерфейсом, включая: RIPv1, RIPv2, RIPv1 и RIPv2, не указано.

Параметр	Описание
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	<p>Настройте, аутентифицирует ли интерфейс пакеты RIP и тип аутентификации, включая:</p> <ul style="list-style-type: none"> Аутентификация по простому паролю: Использование аутентификации в виде обычного текста, необходимо настроить пароль, но пароль можно прочитать, перехватив пакеты. Аутентификация с использованием хэш-функции: Аутентификация по алгоритму хэширования MD5, необходимо настроить ключевую цепочку, это более безопасный метод. Не сертифицировано.
Key-Chain	Configure the Key-Chain name when the authentication type is digest authentication.

6.3.9 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 Network 0.0.0.0 with 20 entries per page.

Gateway	Last Update Time	Version	Received Bad Packets	Received Bad Routes

Описание каждого параметра представлено в следующей таблице:

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	Количество недопустимых RIP-ответных пакетов, отброшенных

Параметр	Описание
messages	соседями.
Number of invalid routes	Количество недопустимых маршрутов от соседей, которые были проигнорированы.

6.3.10 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 0.0.0.0 / 0 , Next Hop 0.0.0.0 with 20 entries per page.

Type	Sub-Type	Network	Next Hop	Metric	From	External Metric	Tag	Uptime
------	----------	---------	----------	--------	------	-----------------	-----	--------

Описание каждого параметра представлено в следующей таблице:

Параметр	Описание
route type	Тип протокола маршрутизации.
subtype	Подтип протокола маршрутизации. <ul style="list-style-type: none"> Обычный: Маршруты, изученные из других устройств через RIP. Интерфейс: маршрут интерфейса этого устройства. По умолчанию: маршрут по умолчанию. Распределение: внесение внешних маршрутов
destination address	Адрес маршрута назначения и маска подсети.
next hop	Адрес следующего перехода.
metric	Метрика маршрута.
source	Идентифицирует источник маршрута, который изучен или сгенерирован с локального интерфейса. <ul style="list-style-type: none"> self: Маршрут, изученный локальным интерфейсом. Если отображается как IPv4-адрес, это указывает на маршруты, изученные от других устройств
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

Параметр	Описание
	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.

6.4 OSPF

6.4.1 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 Disabled ▾

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

Save Reset

Описание каждого параметра представлено в следующей таблице:

Параметр	Описание
OSPF mode	Включить/отключить режим маршрутизатора OSPF
Router ID	<p>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.</p> <ul style="list-style-type: none"> • Auto: Алгоритм по умолчанию выберет наибольший IP-адрес, назначенный маршрутизатору. • Specific: Идентификатор маршрутизатора, указанный пользователем. Допустимый диапазон составляет от 0.0.0.1 до 255.255.255.254.
Default passive mode	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.
Default metric	<p>Пользовательский указанный метрический параметр по умолчанию для протокола маршрутизации OSPF.</p> <ul style="list-style-type: none"> • Auto: Автоматически рассчитывает метрический параметр по умолчанию на основе протокола маршрутизации. • Specific: Пользовательский указанный метрический параметр по умолчанию. Допустимый диапазон от 0 до 16777214.
Route introduction-Static routing	<ul style="list-style-type: none"> • Тип: Тип статического маршрута, введенного OSPF. <ul style="list-style-type: none"> • None: Не вводить статические маршруты. • External Type1: Статические маршруты вводятся как внешний тип 1. • External Type2: Статические маршруты вводятся как внешний тип 2. • Значение метрики: Метрическое значение, указанное пользователем для статического маршрута. Допустимый диапазон от 0 до 16777214.

Параметр	Описание
	<ul style="list-style-type: none"> Auto: Метрическое значение импортированного статического маршрута совпадает с исходным метрическим значением. Specific: Метрика, указанная пользователем для статического маршрута.
Route introduction-Direct routing	<ul style="list-style-type: none"> Тип: Тип прямого подключения к маршруту, введенного OSPF. <ul style="list-style-type: none"> None: Не вводить прямые маршруты. External Type 1: Прямые подключенные маршруты импортируются как внешний тип 1. External Type 2: Прямые подключенные маршруты импортируются как внешний тип 2. Метрика: Пользовательский заданный параметр метрики для подключенного интерфейса. Допустимый диапазон от 0 до 16777214. <ul style="list-style-type: none"> Auto: Метрическое значение импортированного прямого маршрута совпадает с исходным метрическим значением. Specific: Метрика, указанная пользователем для подключенного маршрута.
Stub Router-Boot process	<ul style="list-style-type: none"> Режим: Настройте, действует ли устройство как маршрутизатор Stub и рекламирует ли его во время фазы запуска. 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.
Stub Router-Shutdown process	<ul style="list-style-type: none"> Mode: Настройте, действует ли устройство как маршрутизатор Stub и рекламирует ли его во время фазы отключения. 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.
Stub Router-Unlimited mode	Рекламировать себя как устройство Stub на протяжении всего времени работы.

Параметр	Описание
Default route import	<ul style="list-style-type: none"> Тип: Тип маршрута по умолчанию, импортированный OSPF. <ul style="list-style-type: none"> None: Не импортировать маршрут по умолчанию. External Type 1: Маршрут по умолчанию импортируется как внешний тип 1. External Type 2: Маршрут по умолчанию импортируется как внешний тип 2. Значение метрики: Метрическое значение, указанное пользователем для маршрута по умолчанию. Допустимый диапазон от 0 до 16777214. Auto: Метрическое значение импортированного маршрута по умолчанию совпадает с исходным метрическим значением. Specific: Метрика, указанная пользователем для маршрута по умолчанию. 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.
Administrative distance	Административное расстояние OSPF.
Clear OSPF process	Нажмите кнопку "Очистить процесс OSPF", чтобы очистить базу данных OSPF и перезапустить процесс маршрутизации OSPF.
OSPF mode	Включить/отключить режим маршрутизатора OSPF



Примечания:

- Идентификатор маршрутизатора должен быть уникальным в пределах автономной системы, значение "0.0.0.0" не допустимо, так как оно зарезервировано для алгоритма по умолчанию.
- Когда идентификатор маршрутизатора OSPF меняется, если в текущей области OSPF есть один или несколько полностью смежных соседей, новый идентификатор маршрутизатора вступит в силу после перезапуска процесса OSPF.

6.4.2 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
	*	*	*

Add Entry

Save Reset

Описание каждого параметра представлено в следующей таблице:

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.

6.4.3 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"/>

Описание каждого параметра представлено в следующей таблице:

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

6.4.4 Конфигурация зоны

Протокол OSPF делит автономные системы на различные области и ограничивает распространение LSA в пределах области, тем самым улучшая использование сети и скорость сходимости маршрутизации. Области логически разделяют маршрутизаторы на различные группы, и каждая группа идентифицируется уникальным идентификатором области. Границами областей являются маршрутизаторы, а не соединения.

OSPF Area Stub Configuration

Delete	Area ID	Stub Type	No Summary	Translator Role
	*			

Описание каждого параметра представлено в следующей таблице:

Параметр	Описание
delete	Поставьте отметку напротив записи, и она будет удалена при следующем сохранении.

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

6.4.5 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	Stub Type
	*	

Add Entry

Save Reset

Описание каждого параметра представлено в следующей таблице:

Параметр	Описание
delete	Поставьте отметку напротив записи, и она будет удалена при

Параметр	Описание
	следующем сохранении.
area ID	Идентификатор области OSPF.
certification type	Настройка типа аутентификации в области. <ul style="list-style-type: none"> Простая аутентификация по паролю Аутентификация по MD5-дайджесту

6.4.6 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 Authentication Configuration

Delete	Area ID	Stub Type
	*	

Add Entry

Save

Reset

Описание каждого параметра представлено в следующей таблице:

Параметр	Описание
delete	Поставьте отметку напротив записи, и она будет удалена при следующем сохранении.
area ID	Идентификатор области OSPF.

Параметр	Описание
website address	IPv4 сетевой адрес.
mask length	Длина маски IPv4 сети, диапазон значений 0-32.
notice	После установки отметки маршрут будет агрегирован и опубликован в других областях. В противном случае он будет подавлен, и LSA не будет отправлен в другие области.
overhead	Пользовательский заданный стоимость агрегированного маршрута. Диапазон конфигурации составляет от 0 до 16777215. По умолчанию стоимость - это максимальная стоимость среди детализированных агрегированных маршрутов

6.4.7 Конфигурация интерфейса

Это таблица параметров конфигурации интерфейса.


OSPF Interface Configuration

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

Save Reset

Описание каждого параметра представлено в следующей таблице:

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"> Hello: Цикл отправки сообщений Hello. Допустимый диапазон значений: от 1 до 65535, значение по умолчанию — 10 (секунд). Neighbor failure: Период отказа соседа. Если в течение этого периода не получается сообщение Hello, сосед считается

Параметр	Описание
	<p>недоступным. Допустимый диапазон значений: от 1 до 65535, значение по умолчанию — 40 (секунд).</p> <ul style="list-style-type: none"> LSA retransmission: Интервал переотправки LSA (в секундах). Допустимый диапазон значений: от 3 до 65535, значение по умолчанию — 5 (секунд).
Certification type	<p>Тип аутентификации.</p> <ul style="list-style-type: none"> Простой пароль: использует аутентификацию в виде обычного текста. Пароль должен быть настроен, но его можно прочитать, перехватывая пакеты. Хэш-код сообщения (MD5): используется алгоритм аутентификации хэш-кода сообщения 5 (MD5). Также необходимо настроить ключ. Этот метод является самым безопасным. Отсутствует аутентификация: отсутствует аутентификация. Конфигурация области: См. настройки аутентификации области.
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.

Нажмите на значок , чтобы изменить ключ аутентификации Digest записи.

OSPF Interface Message Digest Configuration

VLAN ID VLAN 1

Interface: VLAN 1

Delete	Interface	MD Key ID	Password
	*	*	*

Add Entry

Save Reset

Описание каждого параметра представлено в следующей таблице:

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.



Примечания:

При настройке аутентификации MD5 ключи, цепочки ключей, и идентификаторы ключей, а также строки, настроенные на обеих сторонах интерфейса, должны быть согласованными. Рекомендуется настраивать только один набор ключей в рамках одной цепочки ключей.

6.4.8 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 Configuration(sec)			Auth. Type	Change Simple Password	MD Key
			Hello	Dead	Retransmit			
	*	*					*	*


Add Entry

Save

Reset

Описание каждого параметра представлено в следующей таблице:

Параметр	Описание
Delete	Проверьте запись, и она будет удалена при следующем сохранении.
Area ID	Область OSPF (ID области OSPF).
Router ID	ID маршрутизатора OSPF

Параметр	Описание
Timing period	<ul style="list-style-type: none"> Hello: период отправки приветственного сообщения. Допустимый диапазон составляет от 1 до 65535 секунд, значение по умолчанию - 10 секунд. 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. LSA retransmission: интервал переотправки LSA (в секундах). Допустимый диапазон составляет от 3 до 65535 секунд, значение по умолчанию - 5 секунд.
Certification type	<p>Тип аутентификации.</p> <ul style="list-style-type: none"> Простой пароль: использует аутентификацию в виде обычного текста. Необходимо настроить пароль, который, однако, может быть прочитан при прослушивании пакетов. MD5-хэш: использует аутентификацию по алгоритму MD5. Требуется также настройка ключа. Это самый безопасный метод. Без аутентификации: аутентификация отсутствует. Настройки области: относятся к настройкам аутентификации области.
Simple password	Для изменения простого пароля (введите обычный текст). Допустимая длина ввода составляет от 1 до 8 символов.
MD Key	Выберите тип аутентификации как MD5, сохраните изменения, затем щёлкните по значку  , чтобы изменить ключ аутентификации дайджеста записи

Нажмите на значок , чтобы изменить ключ аутентификации Digest записи.

OSPF Virtual Link Message Digest Configuration

Area ID: 192.168.16.253

Delete	Area ID	Router ID	MD Key ID	Password
	*	*	*	*

Add Entry

Save

Reset

Описание каждого параметра представлено в следующей таблице:

Параметр	Описание
delete	Проверьте запись, и она будет удалена при следующем сохранении.
area ID	OSPF area ID.
router ID	OSPF router ID.
MD key ID	Идентификатор ключа для аутентификации дайджеста. Допустимый диапазон - от 1 до 255.
password	Пароль в открытом тексте для аутентификации дайджеста. Допустимая длина ввода - от 1 до 16 символов.



Примечания:

При настройке аутентификации MD5 необходимо, чтобы цепочки ключей, идентификаторы ключей и строки, настроенные на обеих сторонах интерфейса, были согласованными. Рекомендуется настраивать только один набор ключей в рамках одной цепочки ключей.

6.4.9 Глобальный статус

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

OSPF Global Status

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 msec
External LSA Checksum	0x0
Attached Area Count	2

Clear OSPF Process Auto-refresh ☐ Refresh

Описание каждого параметра представлено в следующей таблице:

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	Максимальное время ожидания (в миллисекундах) между

Параметр	Описание
interval	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.

6.4.10 Статус области

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 Auto-refresh ☐ Refresh

Area ID	Backbone	Area Type	NSSA translator State	Active Interfaces	Auth. Type	SPF Executed Times	LSA Count	Router LSA		Network LSA		Summary LSA		ASBR Summary LSA		NSSA LSA	
								Count	Checksum	Count	Checksum	Count	Checksum	Count	Checksum	Count	Checksum
0.0.0.0	Yes	Normal	disabled	0	None	0	0	0	0x0	0	0x0	0	0x0	0	0x0	0	0x0
192.168.16.253	No	Normal	disabled	0	None	0	0	0	0x0	0	0x0	0	0x0	0	0x0	0	0x0

Описание каждого параметра представлено в следующей таблице:

Параметр	Описание
area ID	ID области
backbone area	Указывает, является ли она магистральной областью.
area type	<p>Тип области.</p> <ul style="list-style-type: none"> Обычная: Обычная область. Заглушка: Область заглушка. Полностью заглушка: Полностью заглушенная область. NSSA: Область NSSA. Полностью NSSA: Полностью область NSSA.

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 зоне. <ul style="list-style-type: none"> Нет: Аутентификация не требуется. Простой пароль: Аутентификация с помощью простого пароля. Сообщение с хэш-функцией: Аутентификация MD5
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"> Количество: количество LSA маршрутизатора (Тип 1) данного типа в области. Контрольная сумма: контрольная сумма LSA маршрутизатора (Тип 1).
Network LSA	<ul style="list-style-type: none"> Количество: количество LSA сети (Тип 2) данного типа в области. Контрольная сумма: контрольная сумма LSA сети (Тип 2).
SummaryLSAs	<ul style="list-style-type: none"> Количество: количество суммарных LSA (Тип 3) данного типа в области. Контрольная сумма: контрольная сумма суммарного LSA (Тип 3)
ASBR Summary LSA	<ul style="list-style-type: none"> Количество: количество ASBR Summary LSA (Тип 4) данного типа в области. Контрольная сумма: контрольная сумма ASBR Summary LSA (Тип 4).
NSSA LSA	<ul style="list-style-type: none"> Количество: количество NSSA LSAs данного типа в области. Контрольная сумма: контрольная сумма NSSA LSA.

6.4.11 Статус соседей

Это таблица статуса соседей OSPF IPv4. Она используется для предоставления

информации о статусе соседей OSPF.

OSPF Neighbor Status

Auto-refresh ☐ Refresh

Neighbor ID	Pri	State	Dead Time	Interface Address	Interface

Описание каждого параметра представлено в следующей таблице:

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	<p>Статус соседа OSPF. Он указывает на функциональный статус соседнего маршрутизатора.</p> <ul style="list-style-type: none"> FULL: Установлено смежное соединение. INIT: Начальное состояние. 2WAY: Установка соседства. EXSTART: Согласование отношения мастер-слэйв. EXCHANGE: Обмен сообщениями DD. LOADING: Синхронизация LSDB. DR: Сосед является маршрутизатором DR. BDR: Сосед является маршрутизатором BDR. DROTHER: Сосед не участвует в выборе маршрутизатора DR
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.

6.4.12 Статус интерфейса

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

OSPF Interface Status Auto-refresh ☐ 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
OSPF-VLINK 1	0.0.0.0/0	0.0.0.0	192.168.16.253	DOWN	ID	Address	ID	Address			Hello	Dead	Wait	Retransmit					
					0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	1	1	10	40	40	5	00:00:00	0	0	false	1 sec

Описание каждого параметра представлено в следующей таблице:

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"> ID: Идентификатор маршрутизатора DR. Address: IP-адрес DR.
BDR	<ul style="list-style-type: none"> ID: Идентификатор маршрутизатора BDR. Address: IP-адрес BDR.
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"> Hello: цикл отправки приветственного сообщения. Допустимый диапазон составляет от 1 до 65535, значение по умолчанию - 10 секунд. 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. 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.

Параметр	Описание
	<ul style="list-style-type: none"> LSA retransmission: интервал повторной отправки LSA (в секундах). Допустимый диапазон составляет от 3 до 65535, значение по умолчанию - 5 секунд.
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.

6.4.13 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

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.

Route Type	Destination	Area	NextHop	Cost	AS Cost	Border Router Type	Interface	IsConnected
------------	-------------	------	---------	------	---------	--------------------	-----------	-------------

Описание каждого параметра представлено в следующей таблице:

Параметр	Описание
Route type	<p>Тип маршрута OSPF.</p> <ul style="list-style-type: none"> Внутриобластной: местоположение назначения - маршрут OSPF, находящийся внутри области.

Параметр	Описание
	<ul style="list-style-type: none"> Межобластной: местоположение назначения - маршрут OSPF, находящийся между областями. Граничный маршрутизатор: местоположение назначения - граничный маршрутизатор. Внешний тип 1: местоположение назначения - внешний маршрут типа 1. Внешний тип 2: местоположение назначения - внешний маршрут типа 2.
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"> i-ABR: Маршрутизатор-граница является ABR. i-ASBR: Маршрутизатор-граница является ASBR, находящимся внутри области. i-ASBR: Маршрутизатор-граница является ASBR, находящимся между областями. i-ABR/ASBR: Маршрутизатор-граница является ASBR, который соединяет как минимум две области.
Interface	Интерфейс, через который отправляются IP-пакеты.
Is it directly connected?	Является ли пункт назначения непосредственно подключенным.

6.4.14 LSDB

6.4.14.1 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 LSDB 0 - 0 of 0 entry Auto-refresh ☐ Refresh << < > >>

Start from Area ID 0.0.0.0, Link State Type Network, Link State ID 0.0.0.0, Advertising Router 0.0.0.0 with 20 entries per page.

Area ID	Link State Type	Link State ID	Advertising Router	Age (in seconds)	Sequence	Checksum	Router Link Count

Описание каждого параметра представлено в следующей таблице:

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

6.4.14.2 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 LSDB 0 - 0 of 0 entry Auto-refresh ☐ Refresh << < > >>

Start from Area ID 0.0.0.0, Link State Type Network, Link State ID 0.0.0.0, Advertising Router 0.0.0.0, with 20 entries per page.

Area ID	Link State Type	Link State ID	Advertising Router	Age (in seconds)	Options	Sequence	Checksum	Length	Router Link Count

Описание каждого параметра представлено в следующей таблице:

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.
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).

6.4.14.3 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 LSDB 0 - 0 of 0 entry Auto-refresh ☐ Refresh [<< < > >>]

Start from Area ID 0.0.0.0 , Link State Type Network , Link State ID 0.0.0.0 , Advertising Router 0.0.0.0 , with 20 entries per page.

Area ID	Link State Type	Link State ID	Advertising Router	Age (in seconds)	Options	Sequence	Checksum	Length	Network Mask

Описание каждого параметра представлено в следующей таблице:

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

6.4.14.4 Сводная информация LSDB

Отображает сводную информацию о типе OSPF LSDB. Максимальное количество записей в таблице, которое может быть отображено на одной странице, составляет 999 и выбирается через поле 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 этого совпадения или ближайшего следующего совпадения. Кроме того, эти поля ввода примут значение первой отображаемой записи при

нажатии кнопки "Обновить", что позволит последовательные обновления с использованием того же начального поля ввода.

OSPF Summary LSDB 0 - 0 of 0 entry Auto-refresh ☐ Refresh << < > >>

Start from Area ID 0.0.0.0, Link State Type Network, Link State ID 0.0.0.0, Advertising Router 0.0.0.0, with 20 entries per page.

Area ID	Link State Type	Link State ID	Advertising Router	Age (in seconds)	Options	Sequence	Checksum	Length	Network Mask	Metric Value

Описание каждого параметра представлено в следующей таблице:

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).
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).

6.4.14.5 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 LSDB 0 - 0 of 0 entry Auto-refresh ☐ Refresh << << >> >>

Start from Area ID 0.0.0.0, Link State Type Network, Link State ID 0.0.0.0, Advertising Router 0.0.0.0, with 20 entries per page.

Area ID	Link State Type	Link State ID	Advertising Router	Age (in seconds)	Options	Sequence	Checksum	Length	Network Mask	Metric Value

Описание каждого параметра представлено в следующей таблице:

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.
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).

6.4.14.6 Внешняя информация LSDB

Отображает информацию OSPF LSDB типа External.

Максимальное количество записей в таблице, которое может быть отображено на одной странице, составляет 999 и выбирается через поле ввода "___записей на странице". При первом доступе веб-страница будет отображать начальную запись таблицы. Поле ввода "Начать с ___" позволяет пользователю изменить начальную точку в таблице. Нажатие кнопки "Обновить" обновит отображаемую таблицу, начиная с этого совпадения или ближайшего следующего совпадения. Кроме того, эти поля ввода примут значение первой отображаемой записи при нажатии кнопки "Обновить", что позволит последовательные обновления с использованием того же начального поля ввода.

OSPF External LSDB 0 - 0 of 0 entry Auto-refresh ☐ Refresh << < > >>

Start from Link State Type Network, Link State ID 0.0.0.0, Advertising Router 0.0.0.0, with 20 entries per page.

Link State Type	Link State ID	Advertising Router	Age (in seconds)	Options	Sequence	Checksum	Length	Network Mask	Metric Type	Metric Value	Forward Address

Описание каждого параметра представлено в следующей таблице:

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/HCCA внешний статус связи" (типы 5, 7).
Measure type	Внешний тип LSA. Это поле имеет смысл только, когда тип состояния связи - "Внешний/HCCA 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).

6.4.14.7 NSSA внешняя 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.

OSPF NSSA External LSDB 0 - 0 of 0 entry Auto-refresh ☐ Refresh << << >> >>

Start from Link State Type Network, Link State ID 0.0.0.0, Advertising Router 0.0.0.0, with 20 entries per page.

Link State Type	Link State ID	Advertising Router	Age (in seconds)	Options	Sequence	Checksum	Length	Network Mask	Metric Type	Metric Value	Forward Address

Описание каждого параметра представлено в следующей таблице:

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.
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

Параметр	Описание
	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).

6.5 OSPFv3

6.5.1 Глобальная конфигурация

Страница глобальной конфигурации OSPFv3 в основном настраивает активацию, деактивацию и глобальные параметры OSPFv3. Перед включением OSPFv3 отображается конфигурация режима OSPFv3.

Выберите "Включить", чтобы настроить режим OSPFv3, а затем нажмите "Сохранить", чтобы отобразить форму глобальной конфигурации.

Описание каждого параметра представлено в следующей таблице:

Параметр	Описание
OSPFv3 mode	Включение или отключение функции OSPFv3.
router ID	Идентификатор маршрутизатора (Router ID) уникально идентифицирует маршрутизатор в автономной системе и может быть настроен вручную или сгенерирован автоматически: <ul style="list-style-type: none"> По умолчанию: Выбирается максимальный IPv4-адрес, назначенный маршрутизатору, по умолчанию.

Параметр	Описание
	<ul style="list-style-type: none"> Указанное значение: Идентификатор маршрутизатора, указанный пользователем; допустимый диапазон составляет от 0.0.0.1 до 255.255.255.254
route introduction-static routing	<ul style="list-style-type: none"> Включить: Статические маршруты импортируются как второй тип внешних маршрутов. Отключить: Отменить введение статического маршрута.
route import - direct route	<ul style="list-style-type: none"> Включить: Маршруты, прямо подключенные к сети, импортируются как второй тип внешних маршрутов. Отключить: Отменить введение прямого маршрута
route introduction - RIPng routing	<ul style="list-style-type: none"> Включить: Маршруты RIP ng импортируются как второй тип внешних маршрутов. Отключить: Отменить импорт маршрутов RIPng
administrative distance	Приоритет протокола OSPFv3, диапазон значений от 1 до 255, по умолчанию 110.
clear OSPF v3 process	Нажмите кнопку "Очистить процесс OSPF v3", чтобы перезапустить процесс маршрутизации OSPF v3



Примечания:

- Идентификатор маршрутизатора должен быть уникальным в пределах автономной системы; значение "0.0.0.0" недопустимо, так как оно зарезервировано для используемого по умолчанию алгоритма.
- Если идентификатор маршрутизатора изменяется, и в текущей области OSPFv3 есть один или несколько полностью смежных соседей, новый идентификатор маршрутизатора вступит в силу после перезапуска процесса OSPFv3.
- При изменении административной дистанции существующая административная дистанция маршрута не будет обновлена, а новая административная дистанция маршрута будет обновлена до текущего значения конфигурации.

6.5.2 Включение интерфейса

Когда OSPFv3 включен на конкретных интерфейсах, маршрутизатор может устанавливать соседство с другими маршрутизаторами через эти интерфейсы и обмениваться информацией о маршрутизации.

Выберите соответствующий интерфейс, выберите "Включить", затем введите идентификатор зоны и нажмите "Сохранить".

OSPFv3 Interface Enable

Interface	Area ID
VLAN 1 <input type="button" value="Enable"/>	<input type="text" value="0.0.0.1"/>
VLAN 10 <input type="button" value="Disable"/>	<input type="text" value="0.0.0.0"/>
VLAN 20 <input type="button" value="Disable"/>	<input type="text" value="0.0.0.0"/>
VLAN 30 <input type="button" value="Disable"/>	<input type="text" value="0.0.0.0"/>

Описание каждого параметра представлено в следующей таблице:

Параметр	Описание
interface	<p>Интерфейсы OSPFv3 могут быть включены.</p> <ul style="list-style-type: none"> Включить: Включить OSPFv3 на указанном интерфейсе, и соответствующий интерфейс начнет отправлять приветственные сообщения Hello. Отключить: Отключить OSPFv3 на указанном интерфейсе. Соответствующий интерфейс перестанет отправлять приветственные сообщения Hello и очистит информацию о соседях
area ID	Идентификатор области OSPFv3.

6.5.3 Настройка зоны

Протокол OSPF v3 разделяет автономные системы на различные области и ограничивает распространение LSA внутри области, тем самым повышая использование сети и скорость сходимости маршрутизации. Области логически разделяют маршрутизаторы на различные группы, и каждая группа идентифицируется идентификатором области (Area ID). Границы областей определяются маршрутизаторами, а не соединениями.

В настоящее время OSPFv3 поддерживает только настройку областей как стабильных (Stub areas).

OSPFv3 Area Stub Configuration

Delete	Area ID	No Summary
	*	

Add Entry

Save

Reset

Нажмите "Добавить запись", и будет создан элемент конфигурационной таблицы. Затем введите идентификатор области. В зависимости от конкретной ситуации, вы можете отметить "Полностью режим" (Totally Mode). Нажмите "Сохранить", чтобы настроить текущую область как стабильную (Stub area).

OSPFv3 Area Stub Configuration

Delete	Area ID	No Summary
	*	
Delete	0.0.0.1	<input checked="" type="checkbox"/>
Delete	0.0.0.2	<input checked="" type="checkbox"/>

Add Entry

Save

Reset

Описание каждого параметра представлено в следующей таблице:

Параметр	Описание
delete	Проверьте запись, и она будет удалена при следующем сохранении.
area ID	Идентификатор области OSPFv3. При настройке стабильной области идентификатор области не может быть идентификатором области основной области.
totally mode	Настройте устройство как полностью стабильную область

6.5.4 Агрегация маршрутов области

Агрегация маршрутов между областями выполняется на маршрутизаторе ABR и в основном используется для объединения маршрутов между областями в пределах автономной системы (AS). Когда ABR отправляет информацию о маршрутизации в другие области, он создает LSA типа 3 по сегментам сети. Если в области есть непрерывные сегменты сети, вы можете использовать команды для агрегации этих непрерывных сегментов сети в один сегмент сети. Таким образом, ABR отправляет только один агрегированный LSA, и все LSA, принадлежащие к агрегированному сегменту сети, указанному в команде, не будут отправляться отдельно.

OSPFv3 Area Range Configuration

Delete	Area ID	Network Address	Mask Length	Advertise	Cost
	*	*	*		
<input type="button" value="Add Entry"/>					
<input type="button" value="Save"/> <input type="button" value="Reset"/>					

Нажмите "Добавить запись", и будет создана таблица конфигурации. Затем введите идентификатор области, сетевой адрес, длину маски, отметьте или снимите отметку уведомления, укажите стоимость или оставьте стоимость по умолчанию. Нажмите "Сохранить", чтобы настроить запись агрегации маршрута области.

OSPFv3 Area Range Configuration

Delete	Area ID	Network Address	Mask Length	Advertise	Cost
	*	*	*		
<input type="button" value="Delete"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="0::0"/>	<input type="text" value="96"/>	<input checked="" type="checkbox"/> Specific <input type="button" value="v"/>	<input type="text" value="0"/>
<input type="button" value="Add Entry"/>					
<input type="button" value="Save"/> <input type="button" value="Reset"/>					

Описание каждого параметра представлено в следующей таблице:

Параметр	Описание
delete	Проверьте запись, и она будет удалена при следующем сохранении.
area ID	Идентификатор области OSPFv3.
website address	Префикс сетевого адреса IPv6. Он может быть только глобальным одноадресным адресом, а не адресом all-0, локальным адресом

Параметр	Описание
	связи, адресом обратной петли или многоадресным адресом.
mask length	Длина маски сетевого адреса IPv6, диапазон значений от 1 до 128.
notice	Когда отмечено, маршрут будет агрегирован и опубликован в другие области. В противном случае он будет подавлен, и LSA не будет отправлен в другие области
overhead	<ul style="list-style-type: none"> Указанное значение: Пользовательская стоимость агрегированного маршрута, диапазон от 0 до 16777215. Значение по умолчанию: Значение стоимости опубликованного агрегированного маршрута равно максимальному значению стоимости в подробном маршруте..



Примечания:

При настройке отсутствия объявлений агрегированных маршрутов значение стоимости не может быть указано.

6.5.5 Конфигурация интерфейса

Конфигурация интерфейса в основном предназначена для настройки соответствующих параметров интерфейса с учетом реальных сетевых условий.

OSPFv3 Interface Configuration

Interface	Priority	Passive Interface	Cost	Interval		
				Hello	Dead	Retransmit
*	<input type="text"/>	<input type="checkbox"/>	<input type="text"/> <input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
VLAN 1	<input type="text"/>	<input type="checkbox"/>	Auto <input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
VLAN 10	<input type="text"/>	<input type="checkbox"/>	Auto <input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
VLAN 20	<input type="text"/>	<input type="checkbox"/>	Auto <input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
VLAN 30	<input type="text"/>	<input type="checkbox"/>	Auto <input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

Save Reset

Описание каждого параметра представлено в следующей таблице:

Параметр	Описание
interface	Идентификатор интерфейса.
priority	Пользовательский приоритет маршрутизатора для интерфейса. Допустимый диапазон составляет от 0 до 255, значение по умолчанию - 1.
passive interface	Пользователь настраивает данный интерфейс на прекращение установки смежности
overhead	<p>Пользовательская стоимость для этого интерфейса.</p> <ul style="list-style-type: none"> Указанное значение: Пользовательская стоимость интерфейса, диапазон от 1 до 65535. Значение по умолчанию: Стоимость интерфейса по умолчанию равна 1
timing period	<ul style="list-style-type: none"> Приветствие: Цикл отправки приветственного сообщения. Допустимый диапазон составляет от 1 до 65535, значение по умолчанию - 10 (секунд). Отказ соседа: Период отказа соседа. Если в течение этого периода не получено ни одного приветственного сообщения, сосед считается отказавшим. Допустимый диапазон составляет от 1 до 65535, значение по умолчанию - 40 (секунд). Переотправка LSA: Интервал повторной отправки LSA (в секундах). Допустимый диапазон составляет от 3 до 65535, значение по умолчанию - 5 (секунд)

6.5.6 Глобальный статус

Отображение таблицы глобального статуса маршрутизации OSPFv3. Она используется для предоставления информации о глобальном статусе маршрутизации OSPFv3.

OSPFv3 Global Status		Clear OSPFv3 Process	Auto-refresh <input type="checkbox"/>	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	1527366 msec			
Attached Area Count	2			

Описание каждого параметра представлено в следующей таблице:

Параметр	Описание
router ID	Идентификатор маршрутизатора OSPFv3.
SPF delay time	Время задержки вычисления SPF в миллисекундах.
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	Прошедшее время (в миллисекундах) между началом выполнения алгоритма SPF и текущим временем.
number of connected areas	Количество областей, к которым подключен маршрутизатор.
clear OSPF v3 process	Нажмите кнопку "Очистить процесс OSPF v3", чтобы перезапустить процесс маршрутизации OSPF v3.
refresh	Нажмите "Обновить", чтобы обновить информацию о глобальном статусе OSPFv3

6.5.7 Статус зоны

Таблица статуса областей OSPFv3. Она используется для предоставления информации о состоянии областей сети OSPFv3.

OSPFv3 Area Status

Auto-refresh ☐ Refresh

Area ID	Backbone	Area Type	Active Interfaces	SPF Executed Times	LSA Count
0.0.0.0	Yes	Normal	1	1	1
0.0.0.1	No	Normal	0	3	1

Описание каждого параметра представлено в следующей таблице:

Параметр	Описание
area ID	Идентификатор области
backbone area	Указывает, является ли это магистральной областью.
area type	Тип области. "Normal" указывает на обычную область, "Stub" указывает на область Stub, "Totally Stub" указывает на полностью Stub область.
number of active interfaces	Количество интерфейсов, включенных в OSPFv3 в данной области.
SPF execution times	Количество выполнений алгоритма SPF в области.
number of LSAs	Общее количество LSAs в области.
refresh	Нажмите "Обновить", чтобы обновить информацию о статусе областей OSPFv3

6.5.8 Статус соседей

Таблица статуса соседей OSPFv3. Она используется для предоставления информации о статусе соседей OSPFv3.

OSPFv3 Neighbor Status

Auto-refresh ☐ Refresh

Neighbor ID	Priority	State	Dead Time	Interface Address	Interface

Описание каждого параметра представлено в следующей таблице:

Параметр	Описание
neighbor ID	Идентификатор маршрутизатора соседа.
priority	Приоритет соседа OSPFv3. Представляет собой приоритет, объявленный соседними маршрутизаторами. Этот параметр используется при выборе DR для сети.
state	Статус соседа OSPFv3.
remaining expiry	Указывает оставшееся время, в течение которого маршрутизатор

Параметр	Описание
time	ожидает получения приветственных пакетов Hello от соседа, прежде чем объявить соседа отключенным.
interface address	Локальный адрес соседа.
interface	Сетевой интерфейс.
refresh	Нажмите "Обновить", чтобы обновить информацию о статусе соседей OSPFv3

6.5.9 Статус интерфейса

Таблица статуса интерфейсов OSPFv3. Она используется для предоставления информации о статусе интерфейсов OSPFv3.

OSPFv3 Interface Status													Auto-refresh <input type="checkbox"/> Refresh
Interface	Interface Address	Area ID	Router ID	State	DR	BDR	Pri	Cost	Interval Configuration(sec)			Passive	Transmit Delay
					ID	ID			Hello	Dead	Retransmit		
VLAN 1	fe80::200:ff:fe0a:1122/64	0.0.0.1	192.168.16.253	DR	192.168.16.253	0.0.0.0	10	1	10	40	5	false	1 sec

Описание каждого параметра представлено в следующей таблице:

Параметр	Описание
interface	Идентификатор интерфейса.
interface address	Соответствует глобальному unicast-адресу ipv6 или локальному адресу интерфейса.
area ID	Идентификатор области OSPFv3.
router ID	Идентификатор маршрутизатора OSPFv3.
state	Статус интерфейса.
DRID	Идентификатор маршрутизатора, выбранный в качестве DR на этом соединении.
BDR ID	Идентификатор маршрутизатора, выбранный в качестве BDR на этом соединении.
priority	Приоритет OSPFv3. Используется для выбора DR и BDR на сети, подключенной к этому интерфейсу.
overhead	Значение стоимости интерфейса
timing period (seconds)	<ul style="list-style-type: none"> Приветствие: Цикл отправки приветственного сообщения. Допустимый диапазон составляет от 1 до 65535, значение по умолчанию - 10 (секунд). Отказ соседа: Период отказа соседа. Если в течение этого периода не получено ни одного приветственного сообщения, сосед считается отказавшим. Допустимый диапазон

Параметр	Описание
	<p>составляет от 1 до 65535, значение по умолчанию - 40 (секунд).</p> <ul style="list-style-type: none"> Переотправка LSA: Интервал повторной отправки LSA (в секундах). Допустимый диапазон составляет от 3 до 65535, значение по умолчанию - 5 (секунд)
passive mode	Указывает, является ли интерфейс пассивным.
send delay	Время задержки для интерфейса передачи LSA.
refresh	Нажмите "Обновить", чтобы обновить информацию о статусе интерфейса OSPFv3

6.5.10 Статус маршрутизации

Это таблица состояния маршрутизации OSPFv3. Она используется для предоставления информации о состоянии маршрутизации OSPFv3.

На одной странице может быть отображено максимум 999 записей таблицы, выбранных через поле ввода "___ записей на странице". При первом доступе к веб-странице будет отображаться начальная 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 позволит последовательные обновления с использованием того же начального поля ввода.

OSPFv3 Routing Status 0 - 0 of 0 entry Auto-refresh ☐

Start from Route Type Destination / Area NextHop

with entries per page.

Route Type	Destination	Area	NextHop	Cost	AS Cost	Border Router Type	Interface	IsConnected

Описание каждого параметра представлено в следующей таблице:

Параметр	Описание
route type	Тип маршрута OSPFv3. <ul style="list-style-type: none">Внутриобластной: Маршрутизация внутри области.

Параметр	Описание
	<ul style="list-style-type: none"> Межобластной: Маршрутизация между областями. Граничный маршрутизатор: Граничная маршрутизация. Внешний тип - 1: Первый тип внешней маршрутизации. Внешний тип - 2: Второй тип внешней маршрутизации.
destination address	Адрес и длина маски назначения маршрута.
area	Он указывает, через какую область должен проходить маршрут, чтобы достичь своего назначения.
next hop	Адрес следующего перехода маршрута. Следующий переход - это локальный адрес связи. Если следующего перехода нет, то назначение находится непосредственно.
overhead	Накладные расходы на маршрутизацию.
AS overhead	Стоимость достижения OSPFv3 до других доменов AS. Это действительно для маршрутов внешнего типа 2 и всегда "0" для других типов маршрутов
BR type	Тип граничного маршрутизатора для OSPFv3: <ul style="list-style-type: none"> i-ABR: Граничный маршрутизатор является ABR. i-ASBR: Граничный маршрутизатор - ASBR, расположенный внутри области. I-ASBR: Граничный маршрутизатор - ASBR, расположенный между областями. i-ABR/ASBR: Граничный маршрутизатор - это ASBR, который соединяет как минимум две области
interface	Интерфейс следующего перехода.
Is it directly connected?	Является ли назначение прямым подключением

6.5.11 LSDB

6.5.11.1 LSDB суммарная информация

База данных состояний соединений (LSDB) OSPFv3. Маршрутизаторы OSPF v3 на каждом устройстве собирают LSA, объявленные другими маршрутизаторами, и все LSA собираются вместе, формируя базу данных состояний соединений (LSDB). LSA - это описание топологии сети вокруг маршрутизатора, а LSDB - это описание топологии сети всей автономной

системы.

На одной странице может быть отображено максимум 999 записей таблицы, выбранных через поле ввода "___ записей на странице". При первом доступе к веб-странице будет отображаться начальная 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 позволит последовательные обновления с использованием того же начального поля ввода.

OSPFv3 Link State Database

1 - 3 of 3 entries Auto-refresh ☐ Refresh

Start from Area ID 0.0.0.1, Link State Type Link, Link State ID 0.0.0.4, Advertising Router 11.11.11.173 with 20 entries per page.

Area ID	Link State Type	Link State ID	Advertising Router	Age (in seconds)	Sequence
0.0.0.1	Link	0.0.0.4	11.11.11.173	1468	0x80000002
0.0.0.1	Router	0.0.0.0	11.11.11.173	1468	0x80000002
0.0.0.2	Router	0.0.0.0	11.11.11.173	155	0x80000001

Описание каждого параметра представлено в следующей таблице:

Параметр	Описание
area ID	Идентификатор области OSPFv3
LSA type	<p>Тип объявления статуса связи.</p> <ul style="list-style-type: none"> Маршрутизатор: LSA типа 1 Сеть: LSA типа 2 Межобластной префикс: LSA типа 3 Межобластной маршрутизатор: LSA типа 4 Внутриобластной префикс: LSA типа 9 Связь: LSA типа 8 Внешний: LSA типа 5
link status ID	Идентификатор состояния связи OSPFv3. Он идентифицирует

Параметр	Описание
	часть области маршрутизации, описанную LSA.
LSA publishing equipment	ID рекламирующего маршрутизатора, который сформировал LSA.
aging time	Время (в секундах) с момента инициации LSA.
serial number	Порядковый номер LSA

6.5.11.2 LSD детали

Маршрутизация

Эта страница отображает информацию о LSA типа маршрутизатора OSPFv3.

OSPFv3 Router Link State Database 1 - 2 of 2 entries Auto-refresh ☐ Refresh First Page Previous Page Next Page Last Page

Start from Area ID 0.0.0.1, Link State Type Router, Link State ID 0.0.0.0, Advertising Router 11.11.11.173 with 20 entries per page.

Area ID	Link State Type	Link State ID	Advertising Router	Age (in seconds)	Options	Sequence	Checksum	Length	Router Link Count
0.0.0.1	Router	0.0.0.0	11.11.11.173	1520	0x17	0x80000002	0x55F	24	0
0.0.0.2	Router	0.0.0.0	11.11.11.173	207	0x17	0x80000001	0x75E	24	0

Описание каждого параметра представлено в следующей таблице:

Параметр	Описание
area ID	Идентификатор области OSPFv3 для объявлений статуса связи.
LSA type	Тип LSA. Фиксирован как Маршрутизатор.
link status ID	Идентификатор состояния связи OSPFv3. Он идентифицирует 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 в LSA.
serial number	Порядковый номер LSA.
checksum	Контрольная сумма содержимого LSA.
length	Длина LSA, выраженная в байтах.
number of connected routers	Количество связей в LSA. Указывает количество маршрутизаторов, подключенных к этому LSA

Сеть

Отображает информацию о базе данных состояний соединений OSPFv3 типа сети.

OSPFv3 Network Link State Database

0 - 0 of 0 entry Auto-refresh ☐ Refresh First Page Previous Page Next Page Last Page

Start from Area ID 0.0.0.0 , Link State Type Network , Link State ID 0.0.0.0 , Advertising Router 0.0.0.0 with 20 entries per page.

Area ID	Link State Type	Link State ID	Advertising Router	Age (in seconds)	Options	Sequence	Checksum	Length
---------	-----------------	---------------	--------------------	------------------	---------	----------	----------	--------

Описание каждого параметра представлено в следующей таблице:

Параметр	Описание
area ID	Идентификатор области OSPFv3 для объявлений статуса связи.
LSA type	Тип объявления статуса связи. Фиксирован как Сеть.
link status ID	Идентификатор состояния связи OSPFv3. Он идентифицирует часть описания области маршрутизации LSA.
LSA publishing equipment	ID рекламирующего маршрутизатора, который сформировал LSA.
aging time	Время (в секундах) с момента инициации LSA.
options	Поле опций в LSA.
serial number	Порядковый номер LSA.
checksum	Контрольная сумма содержимого LSA.
length	Длина LSA, выраженная в байтах

Link

Каждое устройство будет генерировать LSA типа "Link Type" для каждого соединения, описывая локальный адрес связи и адрес префикса IPv6 на этой связи, а также предоставляя опции связи, которые будут установлены в LSA типа "Network". Оно используется только на этой связи. Отображает информацию о базе данных состояний соединений OSPFv3 типа "Link".

OSPFv3 Link Link State Database

1 - 1 of 1 entry Auto-refresh ☐ 刷新 First Page Previous Page Next Page Last Page

Start from Area ID 0.0.0.1 , Link State Type Link , Link State ID 0.0.0.4 , Advertising Router 11.11.11.173 with 20 entries per page.

Area ID	Link State Type	Link State ID	Advertising Router	Age (in seconds)	Options	Sequence	Checksum	Length	Number of Links
0.0.0.1	Link	0.0.0.4	11.11.11.173	1593	0x17	0x80000002	0xC8D4	44	0

Описание каждого параметра представлено в следующей таблице:

Параметр	Описание
area ID	Идентификатор области OSPFv3 для объявлений статуса связи.
LSA type	Тип объявления статуса связи. Фиксирован как Ссылка.
link status ID	Идентификатор состояния связи OSPFv3. Он идентифицирует

Параметр	Описание
	часть описания области маршрутизации LSA.
LSA publishing equipment	ID рекламирующего маршрутизатора, который сформировал LSA.
aging time	Время (в секундах) с момента инициации LSA.
options	Поле опций в LSA.
serial number	Порядковый номер LSA.
checksum	Контрольная сумма содержимого LSA.
length	Длина LSA, выраженная в байтах.
number of links	Количество префиксов IPv6 маршрутизации, передаваемых LSA

Внутриобластной префикс

Каждое устройство и DR будет генерировать один или несколько таких LSAs и распространять их в пределах области, к которой они принадлежат. Этот тип LSA, сгенерированный устройством, описывает адрес префикса IPv6, связанный с LSA маршрутизатора. Этот тип LSA, сгенерированный DR, описывается сетью. Адрес префикса IPv6, связанный с LSA. Информация о LSDB OSPFv3 типа IntraAreaPrefix.

OSPFv3 IntraArea Prefix Link State Database							0 - 0 of 0 entry		Auto-refresh <input type="checkbox"/>	Refresh	First Page	Previous Page	Next Page	Last Page
Start from Area ID 0.0.0.0		Link State Type IntraAreaPrefix		Link State ID 0.0.0.0		Advertising Router 0.0.0.0		with 20		entries per page.				
Area ID	Link State Type	Link State ID	Advertising Router	Age (in seconds)	Sequence	Checksum	Length	Number of Links						

Описание каждого параметра представлено в следующей таблице:

Параметр	Описание
area ID	Идентификатор области OSPFv3 для объявлений статуса связи.
LSA type	Тип объявления статуса связи. Фиксирован как Внутриобластной префикс.
link status ID	Идентификатор состояния связи OSPFv3. Он идентифицирует часть описания области маршрутизации LSA.
LSA publishing equipment	ID рекламирующего маршрутизатора, который сформировал LSA.
aging time	Время (в секундах) с момента инициации LSA.
serial number	Порядковый номер LSA.
checksum	Контрольная сумма содержимого LSA.
length	Длина LSA, выраженная в байтах.
number of links	Количество префиксов IPv6 маршрутизации, передаваемых LSA

Межобластной префикс

Этот тип LSA генерируется ABR и описывает маршрут определенного сегмента сети в области, после чего рекламируется в другие связанные области. Информация о LSDB OSPFv3 типа InterAreaPrefix

OSPFv3 InterArea Prefix Link State Database

0 - 0 of 0 entry Auto-refresh ☐ Refresh First Page Previous Page Next Page Last Page

Start from Area ID 0.0.0.0 , Link State Type InterAreaPrefix , Link State ID 0.0.0.0 , Advertising Router 0.0.0.0 with 20 entries per page.

Area ID	Link State Type	Link State ID	Advertising Router	Age (in seconds)	Options	Sequence	Checksum	Length	Prefix	Prefix Length	Metric

Описание каждого параметра представлено в следующей таблице:

Параметр	Описание
area ID	Идентификатор области OSPFv3 для объявлений статуса связи.
LSA type	Тип объявления статуса связи. Фиксирован как Межобластной префикс.
link status ID	Идентификатор состояния связи OSPFv3. Он идентифицирует часть описания области маршрутизации LSA.
LSA publishing equipment	ID рекламирующего маршрутизатора, который сформировал LSA.
aging time	Время (в секундах) с момента инициации LSA.
options	Поле опций в LSA.
serial number	Порядковый номер LSA.
checksum	Контрольная сумма содержимого LSA.
length	Длина LSA, выраженная в байтах.
prefix	Префикс маршрута, передаваемый LSA для рекламы.
prefix length	Длина маски маршрута, передаваемая LSA для рекламы.
metric	Значение стоимости маршрутного префикса

Межобластной маршрутизатор

Отображает информацию о базе данных состояний соединений OSPFv3 типа "Межобластной маршрутизатор"

OSPFv3 InterArea Router Link State Database

0 - 0 of 0 entry Auto-refresh ☐ Refresh First Page Previous Page Next Page Last Page

Start from Area ID 0.0.0.0, Link State Type InterAreaRouter, Link State ID 0.0.0.0, Advertising Router 0.0.0.0 with 20 entries per page.

Area ID	Link State Type	Link State ID	Advertising Router	Age (in seconds)	Options	Sequence	Checksum	Length	Metric

Описание каждого параметра представлено в следующей таблице:

Параметр	Описание
area ID	Идентификатор области OSPFv3 для объявлений статуса связи.
LSA type	Тип объявления статуса связи.
link status ID	Идентификатор состояния связи OSPFv3. Он идентифицирует часть описания области маршрутизации LSA.
LSA publishing equipment	ID рекламирующего маршрутизатора, который сформировал LSA.
aging time	Время (в секундах) с момента инициации LSA.
options	Поле опций в LSA.
serial number	Порядковый номер LSA.
checksum	Контрольная сумма содержимого LSA.
length	Длина LSA, выраженная в байтах.
metric	Значение стоимости маршрутного префикса

Внешний

Отображает информацию о базе данных состояний соединений OSPFv3 типа "Внешний"..

OSPFv3 External Link State Database

0 - 0 of 0 entry Auto-refresh ☐ Refresh First Page Previous Page Next Page Last Page

Start from Link State Type External, Link State ID 0.0.0.0, Advertising Router 0.0.0.0 with 20 entries per page.

Link State Type	Link State ID	Advertising Router	Age (in seconds)	Options	Sequence	Checksum	Length	Prefix	Prefix Length	Metric Type	Metric	Forward Address

Описание каждого параметра представлено в следующей таблице:

Параметр	Описание
LSA type	Тип объявления статуса связи. Фиксирован как Внешний.
link status ID	Идентификатор состояния связи OSPFv3. Он идентифицирует часть описания области маршрутизации LSA.

Параметр	Описание
LSA publishing equipment	ID рекламирующего маршрутизатора, который сформировал LSA.
aging time	Время (в секундах) с момента инициации LSA.
options	Поле опций в LSA.
serial number	Порядковый номер LSA.
checksum	Контрольная сумма содержимого LSA.
length	Длина LSA, выраженная в байтах.
prefix	Префикс маршрута, передаваемый LSA для рекламы.
prefix length	Длина маски маршрута, передаваемая LSA для рекламы.
measurement type	Тип метрики для внешних маршрутов. Первый тип внешнего маршрута отображается как 1, а второй тип внешнего маршрута отображается как 2.
metric	Значение стоимости маршрутного префикса.
forwarding address	Адрес пересылки внешнего маршрута, передаваемый в LSA

7 Управление безопасностью

7.1 HTTPS

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

HTTPS Configuration

Mode

Disabled

Automatic Redirect

Disabled

Certificate Maintain

None

Certificate Status

Switch secure HTTP certificate is presented

Save

Reset

Refresh

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	Операции по обслуживанию сертификата. Возможные действия: <ul style="list-style-type: none"> • None: Нет операции. • Delete: Удалить текущий сертификат. • Upload: Загрузить файл PEM-сертификата. Возможные методы: веб-браузер или URL. • Generate: Сгенерировать новый самоподписанный RSA-сертификат.
Certificate pass phrase	При выборе загрузки сертификата введите пароль в это поле, если ваш загруженный сертификат защищен определенным паролем.
Certificate upload	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: <ul style="list-style-type: none"> • Загрузка файла: Загрузите сертификат через веб-браузер. • URL: Загрузите сертификат через URL, протоколы - HTTP, HTTPS, TFTP и FTP. Формат URL: <code><protocol>://[<username>[:<password>]@]<host>[:<port>][/<path>]/<file_name></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 '.').
Certificate status	Отобразить текущий статус сертификата на коммутаторе. Возможные состояния: <ul style="list-style-type: none"> • Предоставлен HTTPS-сертификат • Нет HTTPS-сертификата • Генерируется HTTPS-сертификат...



Примечания:

- 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 сертификаты RSA, так как большинство новых версий браузеров прекратили поддержку сертификатов DSA.

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
model	Включите или отключите службу SSH. После выбора нажмите кнопку "Сохранить", чтобы изменения вступили в силу.

7.3 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.

7.3.1 SNMP настройки

Страница настройки SNMP показана на рисунке ниже.

SNMP System Configuration

Mode	Enabled
Engine ID	8000e7c8030000000a1122

Save Reset

Описание каждого параметра представлено в следующей таблице:

Параметр	Описание
model	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

Параметр	Описание
	движка отменит доступ для всех текущих локальных пользователей.

7.3.2 SNMPv1/v2c сообщество

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

SNMPv1/v2 Community Configuration

Delete	Community Name	Community Secret	Source IP	Source Prefix
<div> <input type="button" value="Add Entry"/> <input type="button" value="Save"/> <input type="button" value="Reset"/> </div>				

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.
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. Допустимые символы - числа от 0 до 32.

7.3.3 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
Add Entry	Save	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.
security level	<p>Укажите уровень безопасности, к которому должна относиться эта запись. Возможные уровни безопасности:</p> <ul style="list-style-type: none"> NoAuth, NoPriv: Без аутентификации и без шифрования. Auth, NoPriv: Только аутентификация и без шифрования. Auth, Priv: Аутентификация и шифрование..
authentication protocol	<p>Укажите протокол аутентификации, к которому должна относиться эта запись. Возможные протоколы аутентификации:</p> <ul style="list-style-type: none"> None: Нет протокола аутентификации. MD5: Инструктирует этого пользователя использовать протокол аутентификации MD5.

Параметр	Описание
	<ul style="list-style-type: none"> SHA: Инструктирует этого пользователя использовать протокол аутентификации SHA.
authentication password	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.
encryption protocol	<p>Укажите протокол шифрования, к которому должна относиться эта запись. Возможные протоколы шифрования:</p> <ul style="list-style-type: none"> None: Отсутствие протокола шифрования. DES: Инструктирует пользователя использовать протокол шифрования DES. AES: Инструктирует этого пользователя использовать протокол шифрования AES.
encrypted password	Строка, идентифицирующая пароль шифрования. Допустимая длина строки составляет от 8 до 32 символов, а допустимое содержимое - символы ASCII с 33 по 126.

7.3.4 SNMP группа

Страница конфигурации группы SNMP изображена на рисунке ниже.

SNMP Group Configuration

Delete	Security Model	Security Name	Group Name
<div> <input type="button" value="Add 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, она будет удалена при следующем сохранении

Параметр	Описание
Security mode	Укажите режим безопасности, к которому должна принадлежать эта запись. Возможные режимы безопасности: <ul style="list-style-type: none"> v1: Зарезервировано для SNMPv1. v2c: Зарезервировано для SNMPv2c. usm: SNMPv3, режим безопасности на основе пользователя (USM).
Security name	Строка, указывающая имя безопасности, к 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.
Group name	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.

7.3.5 SNMP вид

Страница просмотра SNMP, как показано на рисунке ниже.

SNMP 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.

Параметр	Описание
View type	<p>Укажите тип представления, к которому должна принадлежать эта запись. Возможные типы представлений:</p> <ul style="list-style-type: none"> включено: указывает, что это поддерево представления должно быть включено. исключено: указывает, что это поддерево представления должно быть исключено. <p>Пример:</p> <p>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	<p>Определите OID корня поддерева, добавленного к именованному представлению. Разрешенная длина OID составляет от 1 до 128. Разрешенное содержимое строки - числа или звездочки (*).</p>

7.3.6 SNMP аутентификация

Страница аутентификации SNMP, как показано на рисунке ниже.

SNMP Access Configuration

Delete	Group Name	Security Model	Security Level	Read View Name	Write View Name
Add Entry	Save	Reset			

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:

Параметр	Описание
	<ul style="list-style-type: none"> любой: принимает любой режим безопасности (V1 V2C USM). v1: Зарезервировано для SNMPV1. v2c: Зарезервировано для SNMPV2C. usm: SNMPV3, режим безопасности на основе пользователей (USM).
Security Level	<p>Укажите уровень безопасности, к которому должна принадлежать эта запись. Возможные уровни безопасности:</p> <ul style="list-style-type: none"> NoAuth,NoPriv: Нет аутентификации и нет шифрования. Auth,NoPriv: Только аутентификация и нет шифрования. Auth,Priv: Аутентификация и шифрование.
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.

7.3.7 SNMP Ловушка

7.3.7.1 Хост назначения

Страница конфигурации хоста назначения, как показано на рисунке ниже.

Trap Configuration

Trap Destination Configurations

Delete	Name	Enabled	Version	Destination Address	Destination Port
Add Entry					
Save 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 ▾
Trap Version	SNMP v2c ▾
Trap Community	<input type="text"/>
Trap Destination Address	<input type="text"/>
Trap Destination Port	162
Trap Inform Mode	Disabled ▾
Trap Inform Timeout (seconds)	3
Trap Inform Retry Times	5
Trap Security Engine ID	8000e7c8030000000a1122
Trap Security Name	<input type="text"/>

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	<p>Укажите режим работы SNMP. Возможные варианты:</p> <ul style="list-style-type: none"> Включить: включить режим работы SNMP. Отключить: отключить режим работы SNMP.
Trap version	<p>Укажите поддерживаемую версию SNMP. Возможные варианты:</p> <ul style="list-style-type: none"> SNMP v1: Установить поддержку SNMP версии 1. SNMP v2c: Установить поддержку версии 2C SNMP. SNMP v3: Установить поддержку SNMP версии 3.

Параметр	Описание
Trap groups	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.
Trap destination address	<p>Адрес назначения SNMP Trap:</p> <ul style="list-style-type: none"> 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. 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'.
Trap destination port	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.
Trap notification mode	<p>Укажите режим работы уведомлений SNMP Trap. Возможные варианты:</p> <ul style="list-style-type: none"> Включить: включить режим работы уведомлений SNMP Trap. Отключить: отключить режим работы уведомлений SNMP Trap.
Trap notification timeout (seconds)	Укажите время ожидания для уведомлений SNMP Trap. Допустимый диапазон составляет от 0 до 2147.
Trap Inform Retry Times	Укажите количество повторных передач уведомлений SNMP Trap. Допустимый диапазон составляет от 0 до 255.

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.

7.3.7.2 Настройки источника

Страница настроек источника, как показано ниже.

Trap Configuration

Trap Source Configurations

Delete	Name	Type	Subset OID

Add Entry

Save

Reset

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	

Add Entry

Save Reset

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.
Type	Тип фильтра для записи. Возможные типы: <ul style="list-style-type: none"> Включено: указывает, что Ловушка будет отправлена, когда указанный источник Ловушки соответствует. Исключено: указывает, что когда указанный источник Ловушки соответствует, Ловушка не будет отправлена.
SubtreeOID	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.
Add entry	Щелкните, чтобы добавить новую запись конфигурации источника ловушки. Можно добавить до 32 записей.

7.4 RMON

Технология RMON (Remote Monitoring) является расширением функционала SNMP (Simple Network Management Protocol). Это набор переменных MIB (Management Information Base), который в основном предназначен для устранения недостатков SNMP, таких как отсутствие реального времени в обмене данными между процессом управления и агентом, а также

избыточная нагрузка при опросе. Этот набор переменных MIB генерируется путем непрерывного реального мониторинга сети. RMON является приложением SNMP, которое следует структуре SNMP и расширяет функции и применение SNMP.

7.4.1 Конфигурация группы статистики

Страница конфигурации группы статистики, как показано на рисунке ниже.

RMON Statistics Configuration

Delete	ID	Data Source
<div>Add Entry</div> <div>Save</div> <div>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.
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.

7.4.1 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 ___".

RMON Statistics Status Overview

Auto-refresh ☐ Refresh << >>

Start from Control Index 0 with 20 entries per page.

ID	Data Source	Drop	Octets	Pkts	Broadcast Pkts	Multicast Pkts	CRC Errors	Under-size	Over-size	Frag	Jabb	Coll	64 Bytes	65	128	256	512	1024
	(ifIndex)													~	~	~	~	~
														127	255	511	1023	1518

No More Entries

Описание каждого параметра представлено в следующей таблице:

Параметр	Описание
ID	Индекс записи статистики группы.
data source (port index)	Идентификатор мониторируемого порта.
drop frames	Общее количество событий, когда пакеты были отброшены из-за нехватки ресурсов.
byte	Общее количество байтов данных, полученных в сети (включая пакеты с ошибками).
bag	Общее количество полученных пакетов (включая пакеты с ошибками, широковещательные и многоадресные пакеты).
broadcast packet	Общее количество правильно полученных пакетов на широковещательный адрес.
multicast packet	Общее количество правильно полученных пакетов на многоадресный адрес.
CRC error frame	Общее количество кадров с ошибкой проверки цикла CRC.
ultra short frame	Общее количество полученных кадров, размер которых меньше 64 байт
jumbo frame	Общее количество полученных кадров, больших чем 1518 байт. Пояснение: Размер этого байта определяется настройками порта. Текущая максимальная длина кадра по умолчанию для порта составляет 10240 байтов, а 1518 байтов - максимальная длина кадра стандарта Ethernet. Конечное значение все равно зависит от настроек порта
ultra short FCS error frame	Общее количество кадров, полученных с размером меньше 64 байт и с ошибками проверки цикла CRC

Параметр	Описание
long FCS error frame	<p>Общее количество кадров, полученных с размером больше 1518 байт и с ошибками проверки цикла CRC.</p> <p>Пояснение: Размер этого байта определяется настройками порта. Текущая максимальная длина кадра по умолчанию для порта составляет 10240 байтов, а 1518 байтов - максимальная длина кадра стандарта Ethernet. Конечное значение все равно зависит от настроек порта.</p>
conflict frame	Общее количество отправленных кадров из-за коллизий столкновения.
64 bytes	Общее количество принятых пакетов с длиной 64 байта (включая ошибочные пакеты).
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.
1024~1518	Общее количество принятых пакетов (включая ошибочные пакеты) с длиной от 1024 до 1588 байт.

Нажмите на номер ID на странице информации о статистической группе, чтобы перейти на страницу с подробной статистикой.

Detailed RMON Statistics ID 1

ID 1 ▾ 自动刷新 ☐ 刷新

Receive Total	
PortIndex	1000001
Drops	0
Octets	4147844
Pkts	12151
Broadcast Pkts	2253
Multicast Pkts	968
CRC/Alignment	0
Under-size	0
Over-size	0
Fragments	0
Jabber	0
Collisions	0
64 Bytes	5601
65-127 Bytes	1238
128-255 Bytes	486
256-511 Bytes	1941

7.4.2 Конфигурация группы истории

The history group configuration page is as shown in the figure below.

RMON History Configuration

Delete	ID	Data Source	Interval	Buckets	Buckets Granted
<div> <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	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.

Параметр	Описание
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.

7.4.3 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 0 and Sample Index 0 with 20 entries per page.

History Index	Sample Index	Sample Start	Drop	Octets	Pkts	Broadcast Pkts	Multicast Pkts	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.
starting sample	Значение sysUpTime (время работы системы) в начале интервала выборки.
drop frames	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.

Параметр	Описание
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 кадров, принятых с размером более 1518 байтов. Пояснение: Размер этого байта зависит от настроек порта. Текущая максимальная длина кадра по умолчанию для порта составляет 10240 байтов, а 1518 байтов - максимальная длина кадра стандарта Ethernet. Конечное значение все равно зависит от настроек порта
ultra short FCS error frame	Общее количество принятых фреймов, которые меньше 64 байт и имеют ошибки проверки цикла CRC.
long FCS error frame	Общее количество кадров, принятых с размером более 1518 байтов и имеющих ошибки проверки цикла CRC. Пояснение: Размер этого байта зависит от настроек порта. Текущая максимальная длина кадра по умолчанию для порта составляет 10240 байтов, а 1518 байтов - максимальная длина кадра стандарта Ethernet. Конечное значение все равно зависит от настроек порта.
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.

Нажмите на номер индекса на странице информации о исторической группе, чтобы перейти на страницу с подробностями истории.

Detailed RMON Statistics ID 1

ID 1 ▾ 自动刷新 ☐ 刷新

Receive Total	
PortIndex	1000001
Drops	0
Octets	27671249
Pkts	89667
Broadcast Pkts	21236
Multicast Pkts	7975
CRC/Alignment	0
Under-size	0
Over-size	0
Fragments	0
Jabber	0
Collisions	0
64 Bytes	44970
65-127 Bytes	10197
128-255 Bytes	3090

7.4.5 Настройка группы сигнализации

Страница настройки 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
--------	----	----------	----------	-------------	-------	---------------	------------------	--------------	-------------------	---------------

Add Entry Save Reset

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 $2^{31}-1$.

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

Параметр	Описание
Start alarm	Как активировать сигнализацию. Возможные типы сигнализации: <ul style="list-style-type: none"> Повышение: Сигнализация активируется, когда первое значение превышает верхний порог. Понижение: Сигнализация активируется, когда первое значение меньше нижнего порога. Повышение или понижение: Сигнализация активируется, когда первое значение превышает верхний порог или меньше нижнего порога (по умолчанию).
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.

7.4.6 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 ___".

RMON Alarm Overview Auto-refresh ☐ Refresh << >>

Start from Control Index 0 with 20 entries per page.

ID	Interval	Variable	Sample Type	Value	Startup Alarm	Rising Threshold	Rising Index	Falling Threshold	Falling Index
No More Entries									

Описание каждого параметра представлено в следующей таблице:

Параметр	Описание
ID	Укажите индекс записи. Диапазон от 1 до 65535.
Sampling interval	Укажите интервал в секундах для выборки и сравнения верхних и нижних порогов. Диапазон от 1 до $2^{31}-1$.
Sample variable	<p>Укажите конкретную переменную для выборки. Возможные переменные:</p> <ul style="list-style-type: none"> InOctets: Общее количество байтов, полученных на интерфейсе, включая преамбулу фрейма. InUcastPkts: Количество полученных уникальных пакетов. InNUcastPkts: Количество полученных широковещательных и многоадресных пакетов. InDiscards: Количество отброшенных пакетов на входе, даже если они являются нормальными пакетами. InErrors: Количество входящих пакетов, содержащих ошибки. InUnknownProtos: Количество входящих пакетов, которые были отброшены из-за неизвестных или не поддерживаемых протоколов. OutOctets: Общее количество байтов, отправленных на интерфейсе, включая преамбулу фрейма. OutUcastPkts: Количество отправленных уникальных пакетов. OutNUcastPkts: Количество отправленных широковещательных и многоадресных пакетов. OutDiscards: Количество исходящих пакетов, отброшенных, даже если они являются нормальными пакетами. OutErrors: Количество исходящих пакетов, которые не могли быть переданы из-за ошибок. OutQLen: Длина очереди исходящих пакетов (в пакетах).
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"> Абсолютный: Получить выборку напрямую. Дельта: рассчитать разницу между выборками (по умолчанию).
Sample value	Значение статистики за последний период выборки.

Параметр	Описание
Start alarm	Как активировать сигнализацию. Возможные типы сигнализации: <ul style="list-style-type: none"> Повышение: Сигнализация активируется, когда первое значение превышает верхний порог. Понижение: Сигнализация активируется, когда первое значение меньше нижнего порога. Повышение или понижение: Сигнализация активируется, когда первое значение превышает верхний порог или меньше нижнего порога (по умолчанию).
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.

7.4.7 Конфигурация группы событий

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

RMON Event Configuration

Delete	ID	Desc	Type	Event Last Time
--------	----	------	------	-----------------

Add Entry

Save

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.

Параметр	Описание
Describe	Опишите это событие. Длина строки от 0 до 127 символов. Значение по умолчанию - пустая строка.
Type	Уведомление о событии, возможные типы: <ul style="list-style-type: none"> • none: Нет создания SNMP-логов и нет отправки SNMP-ловушек. • log: Создает запись SNMP-лога при срабатывании события. • trap: Отправляет SNMP-ловушку при срабатывании события. • Log and trap: Создает записи SNMP-лога и отправляет SNMP-ловушки при срабатывании событий.
The time of the most recent incident	Значение sysUpTime, когда данная запись события последний раз генерировала событие.

7.4.8 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 0 and Sample Index 0 with 20 entries per page.

Event Index	Log Index	Log Time	Log Description
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.

7.5 Управление доступом

7.5.1 Настройка управления 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
<div>Add Entry</div> <div> <div>Save</div> <div>Reset</div> </div>						

Описание каждого параметра представлено в следующей таблице:

Параметр	Описание
model	Включить или отключить функцию управления доступом.
delete	Удалить запись. При выборе этой опции запись будет удалена при следующем сохранении.
VLAN ID	Идентификатор VLAN для этой записи управления доступом.
starting IP address	Начальный IP-адрес уникаста для этой записи управления доступом.
end IP address	Конечный IP-адрес уникаста 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-

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

7.5.2 Статистика управления доступом

Функции статистики управления доступом. Как показано ниже.

Access Management Statistics				Auto-refresh <input type="checkbox"/> Refresh Clear	
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		

Описание каждого параметра представлено в следующей таблице:

Параметр	Описание
Protocol interface	Тип протокола для доступа к устройству. Доступ к устройству поддерживается через протоколы HTTP, HTTPS, SNMP, TELNET и SSH.
Number of frames received	Подсчет количества принятых кадров.
Number of frames allowed	Подсчет количества разрешенных кадров.
Number of dropped frames	Подсчет количества отброшенных кадров

7.6 Уровень разрешений

Устройство предоставляет настройки уровня разрешений для каждой группы привилегий. Уровни привилегий могут варьироваться от 0 до 15, где 0 - самый низкий уровень, а 15 - самый высокий уровень. Каждая группа имеет следующие подгруппы авторизованных

уровней привилегий:

- Только чтение конфигурации
- Настройка/выполнение чтения и записи
- Только чтение статуса/статистики
- Чтение и запись статуса/статистики (например, очистка статистики)

Уровень привилегий пользователя должен быть больше или равен уровню привилегий авторизации для доступа к группе. В большинстве случаев группа привилегий состоит из одного модуля (например, LACP, RSTP или QOS), но некоторые из этих групп содержат более одного модуля.

Privilege Level Configuration

Groups Name	Privilege Levels			
	Configuration	Configuration/Execute	Status/Statistics	Status/Statistics
	Read-only	Read/write	Read-only	Read/write
Aggregation	5	10	5	10
CFM	5	10	5	10
DDM	5	10	5	10
DHCP	5	10	5	10
DHCPv6_Snooping	5	10	5	10
DHCPv6Relay	5	10	5	10
Diagnostics	5	10	5	10
ERPS	5	10	5	10
Firmware	5	10	5	10
FRR	5	10	5	10
IP	5	10	5	10
IPMC_LIB	5	10	5	10
IPMC_Snooping	5	10	5	10
IPv6_Source_Guard	5	10	5	10

Описание каждого параметра представлено в следующей таблице:

Параметр	Описание
group name	Идентифицирует название группы привилегий. В большинстве случаев группа уровней привилегий состоит из одного модуля (например, LACP, RSTP или QOS), но некоторые из этих групп содержат более одного модуля
Privilege level	Для каждой группы привилегий существуют уровни доступа к следующим подгруппам: Только чтение конфигурации; Настройка/выполнение чтения и записи; Только чтение статуса/статистики; Чтение и запись статуса/статистики (например, очистка статистики). Уровни привилегий могут варьироваться от 0 до 15, где 0 - самый низкий уровень, а 15 - самый высокий уровень. Уровень привилегий пользователя должен быть больше или равен уровню привилегий авторизации для доступа к группе.

Параметр	Описание
	<p>Иллюстрация:</p> <p>Некоторые функции веб-страницы будут применяться для доступа к ресурсам из других модулей и требуют соответствующей проверки разрешений. Например, при доступе к ERPS будет проверяться разрешение только на чтение статуса портов</p>

7.7 Метод проверки

Устройство предоставляет функциональность AAA. AAA - это сокращение от Authentication (аутентификация), Authorization (авторизация) и Accounting (учет). Он предоставляет систему управления для настройки контроля доступа на устройствах NAS (сервера 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	Methods	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	Methods	Cmd Lvl	Exec
console	no ▾		<input type="checkbox"/>
telnet	no ▾		<input type="checkbox"/>
ssh	no ▾		<input type="checkbox"/>

Save Reset

Описание каждого параметра представлено в следующей таблице:

Параметр	Описание
Authentication method configuration	Настройка метода аутентификации
client	Устройство поддерживает четыре метода входа: консольный, Telnet, SSH и HTTP
method	<p>Для каждого метода входа доступны 4 метода аутентификации. Каждый метод входа может быть настроен с использованием до 3 методов аутентификации. Когда первый метод неудачен, используется второй метод. Когда второй метод неудачен, используется третий метод. Пробуйте каждый метод слева направо до получения успешного или неудачного результата. Настоятельно рекомендуется настроить последний метод как local, чтобы всегда можно было выполнять вход через аутентификацию в локальной базе данных, когда серверы аутентификации недоступны.</p> <ul style="list-style-type: none"> no: Отключить аутентификацию, то есть аутентификация входа не будет производиться через данный метод. local: Использовать базу данных, хранящуюся локально на устройстве, для аутентификации входа. radius: Аутентификация входа через удаленный сервер RADIUS. tacacs: Аутентификация входа через удаленный сервер TACACS+
Command authorization mode configuration	Команда конфигурации режима авторизации
client	Среди трех методов входа: консоль, telnet и ssh, настройка команд может быть авторизована через сервер TACACS+
method	<p>Опционально no/tacacs.</p> <ul style="list-style-type: none"> No: указывает, что авторизация команд отключена, и команды, которые пользователи могут использовать, назначаются в соответствии с уровнем пользователя. Tacacs: указывает на использование удаленного сервера TACACS+ для авторизации команд, которые пользователи могут использовать
command level	Диапазон значений - от 0 до 15. Команды с уровнем, равным или выше этого уровня, будут запрашивать авторизацию на сервере TACACS+, где 0 - самый низкий уровень, а 15 - самый высокий уровень.

Параметр	Описание
Configuration commands	После установки флажка, команды конфигурации также требуют авторизации на сервере
Billing method configuration	Конфигурация метода тарификации
client	Среди трех методов входа: консольного, telnet и ssh, пользователи могут быть тарифицированы через сервер TACACS+
method	Дополнительно можно выбрать опцию no/tacacs. <ul style="list-style-type: none"> No: Указывает на отключение учета. Tacacs: Указывает на использование удаленного сервера TACACS+ для тарификации пользователей
command level	Диапазон от 0 до 15. Команды, превышающие или равные этому уровню, будут тарифицированы; пустое значение означает отключение тарификации.
login for billing	После проверки входа в режим выполнения команды будут тарифицированы

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:



ЕАР метод аутентификации

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

- Метод завершения ЕАР: Сообщения ЕАР 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 ЕАР для разбора и обработки сообщений ЕАР клиента.
- Режим проброса ЕАР: Пакеты ЕАР непосредственно инкапсулируются в пакеты RADIUS (ЕАР через RADIUS, называемые ЕАРoR), чтобы пройти через сложные сети и достичь сервера аутентификации. При этом механизме обработки аутентификация ЕАР выполняется между клиентом и сервером RADIUS. Сервер RADIUS выступает в качестве сервера ЕАР для обработки запроса аутентификации ЕАР клиента. Устройство действует как реле и только пересылает сообщения ЕАР. Поэтому обработка на устройстве проста, и оно может поддерживать различные методы аутентификации ЕАР, но требуется, чтобы сервер RADIUS поддерживал соответствующие методы аутентификации ЕАР.

802.1X режим аутентификации

На основе порта этот продукт поддерживает следующие режимы аутентификации:

- Принудительная авторизация: Устройство отправляет сообщение об успешной аутентификации ЕАРoL программе клиента, когда порт подключается. Любой пользователь на порту может получить доступ к сети без аутентификации.
- Принудительный запрет: Устройство отправляет сообщение об ошибке аутентификации ЕАРoL программе клиента, когда порт подключается. Все

пользователи на порту не могут получить доступ к сети.

- Управление доступом на основе порта 802.1X: После успешной аутентификации первого пользователя под портом, другие пользователи могут использовать сетевые ресурсы без аутентификации. Однако, если первый пользователь выходит из сети, доступ к сети будет отказан и другим пользователям.
- Одиночная аутентификация 802.1X: Аналогично управлению доступом на основе порта 802.1X, но порт разрешает использование сети только одному успешно аутентифицированному пользователю. Первый успешно аутентифицировавшийся пользователь получает доступ к сети, и его MAC-адрес устанавливается как безопасный MAC адрес модулем безопасности порта.
- Множественная аутентификация 802.1X: Один порт позволяет нескольким успешно аутентифицированным пользователям использовать сеть, и количество пользователей может быть ограничено с помощью безопасности порта. Когда на порту нет аутентификации пользователя, 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 отдельных сообщений EAPoL для аутентификации каждого пользователя отдельно.
- Аутентификация на основе MAC-адреса: Пользователям не требуется клиентская программа 802.1X. Устройство выполняет функции клиентской программы 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"), а затем аутентифицируется с сервером RADIUS. Метод аутентификации поддерживает только вызовы MD5. Следовательно, серверу RADIUS необходима предварительная настройка при использовании этого метода. Количество пользователей может быть ограничено с помощью безопасности порта.

7.8.1.3 802.1X аутентификация

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
Reauthentication Period 3600 seconds
EAPOL Timeout 30 seconds
Aging Period 300 seconds
Hold Time 10 seconds
Guest VLAN Enabled
Guest VLAN ID 1
Max. Reauth. Count 2
Allow Guest VLAN if EAPOL Seen

Port Configuration

Port	Admin State	Guest VLAN Enabled	Port State	Restart
*	<>			
G1	Force Authorized		Globally Disabled	Reauthenticate Reinitialize
G2	Force Authorized		Globally Disabled	Reauthenticate Reinitialize

Описание каждого параметра представлено в следующей таблице:

Параметр	Описание
System Configuration	Конфигурация системы
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 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

Параметр	Описание
	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.
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.
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.
Port configuration	Конфигурация порта
Authentication mode	<p>Опции режима аутентификации следующие:</p> <ul style="list-style-type: none"> 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. Force Unauthorized: Устройство отправляет сообщение EAPoL о неудачной аутентификации программе клиента, когда порт подключен. Все пользователи на порту не смогут получить доступ к сети. 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. 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,

Параметр	Описание
	<p>может использовать сеть, и его MAC-адрес будет установлен как безопасный MAC-адрес модулем безопасности порта.</p> <ul style="list-style-type: none"> 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. 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.
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"> Глобально Отключен: указывает на то, что 802.1X глобально отключен. Соединение Отключено: указывает на то, что 802.1X глобально включен, но соединение порта отключено. Авторизован: указывает на то, что режим аутентификации порта - Force Authorized, или режим аутентификации порта - Single 802.1X и аутентификация пользователя пройдена. Неавторизован: указывает на то, что режим аутентификации порта - Force Unauthorized, или режим аутентификации порта - Single 802.1X и аутентификация пользователя не удалась. X Auth/Y Unauth означает, что режим аутентификации порта - Multi 802.1X, и X пользователей прошли аутентификацию, а Y пользователей не прошли аутентификацию.

Параметр	Описание
Restart	<p>Операция перезапуска аутентификации порта имеет следующие варианты:</p> <ul style="list-style-type: none"> "Re-authentication" (Повторная аутентификация) - выполнит повторную аутентификацию. Эта конфигурация предназначена только для пользователей, которые успешно прошли аутентификацию, и не прервет текущий процесс аутентификации пользователя. "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.

7.8.3 Статус устройства

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

Network Access Server Switch Status Auto-refresh ☐ Refresh

Port	Admin State	Port State	Last Source	Last ID	Port VLAN ID
G1	Force Authorized	Globally Disabled			
G2	Force Authorized	Globally Disabled			
G3	Force Authorized	Globally Disabled			
G4	Force Authorized	Globally Disabled			
G5	Force Authorized	Globally Disabled			
G6	Force Authorized	Globally Disabled			
G7	Force Authorized	Globally Disabled			
G8	Force Authorized	Globally Disabled			
G9	Force Authorized	Globally Disabled			
G10	Force Authorized	Globally Disabled			
G11	Force Authorized	Globally Disabled			
G12	Force Authorized	Globally Disabled			
G13	Force Authorized	Globally Disabled			
G14	Force Authorized	Globally Disabled			
G15	Force Authorized	Globally Disabled			
G16	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	Отобразить режим аутентификации порта, который может быть отображен следующим образом:

Параметр	Описание
	<ul style="list-style-type: none"> 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. 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. 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. 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. 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. 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..

Параметр	Описание
Port status	<p>Отображение статуса порта может быть следующим:</p> <ul style="list-style-type: none"> Глобально Отключен: указывает на то, что 802.1X глобально отключен. Соединение Отключено: указывает на то, что 802.1X глобально включен, но соединение порта отключено. Авторизован: указывает на то, что режим аутентификации порта - Force Authorized, или режим аутентификации порта - Single 802.1X и аутентификация пользователя пройдена. Не авторизован: указывает на то, что режим аутентификации порта - Force Unauthorized, или режим аутентификации порта - Single 802.1X и аутентификация пользователя не удалась. X Auth/Y Unauth: означает, что режим аутентификации порта - Multi 802.1X, и X пользователей прошли аутентификацию, а Y пользователей не прошли аутентификацию.
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.
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 G1

G1 Auto-refresh Refresh Clear

Port State

Admin State	Force Authorized
Port State	Authorized

Port Counters

Receive EAPOL Counters	Transmit EAPOL Counters
Total	0
Response ID	0
Responses	0
Start	0
Logoff	0
Invalid Type	0
Invalid Length	0

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	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/TX	Имя	IEEE имя	Утверждение
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.

Описание статистических параметров сервера бэкэнда

RX/TX	Имя	IEEE имя	Утверждение
Rx	Access Challenges	dot1xAuthBackendAccessChallenges	<ul style="list-style-type: none"> Основываясь на 802.1X: количество первых запросов, полученных от сервера; Основываясь на MAC-адресе: количество полученных вызовов доступа.
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.

RX/TX	Имя	IEEE имя	Утверждение
Tx	Responses	dot1xAuthBackendResponses	<ul style="list-style-type: none"> Основываясь на 802.1X: количество пакетов первого ответа пользователя, отправленных на сервер; Основываясь на MAC-адресе: количество всех пакетов, отправленных на сервер.

Описание последних пользовательских статистических параметров

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

7.9.1.1 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.

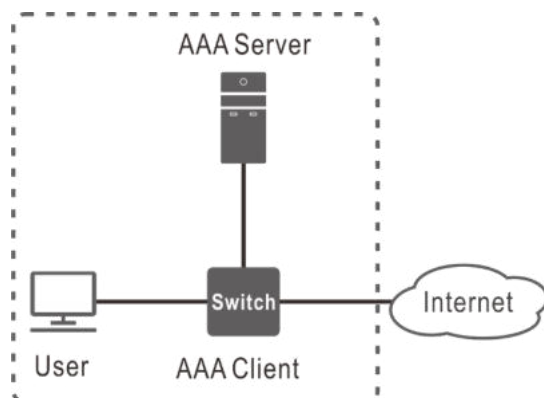
7.9.1.2 AAA принцип работы

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.
Протокольное сообщение относительно просто, и аутентификация и авторизация объединены и сложно разделить.	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.
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.	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.

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	▼
NAS-IP-Address		
NAS-IPv6-Address		
NAS-Identifier		

Server Configuration

Delete	Hostname	Auth Port	Timeout	Retransmit	Change Secret Key
Add New Server					
Save Reset					

Описание каждого параметра представлено в следующей таблице:

Параметр	Описание
Global configuration	Глобальная конфигурация
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

Параметр	Описание
	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.
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.
Server configuration	Настройки сервера
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 переопределит конфигурацию тайм-аута в глобальной конфигурации. Если не задано, будет

Параметр	Описание
	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.



Примечания:

После настройки ключа он не будет отображаться на веб-странице, однако его можно просмотреть в командной строке (ключ отображается в зашифрованной форме).

7.9.2.2 RADIUS статус

RADIUS статус

Страница статуса RADIUS, как показано ниже.

RADIUS Server Status Overview

Auto-refresh ☐ Refresh

#	IP Address	Authentication Port	Authentication Status
1			Disabled
2			Disabled
3			Disabled
4			Disabled
5			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.
- Dead (осталось N секунд): Устройство пыталось отправить запрос на аутентификацию на сервер RADIUS, но не получило ответа. В этот момент сервер RADIUS будет временно отключен. По истечении времени ожидания dead time сервер RADIUS снова будет включен, и будет отображено количество оставшихся секунд до истечения тайм-

аута.

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.

#1RADIUS Authentication Statistics for Server

Server #1 Auto-refresh 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

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 некорректных сообщений RADIUS Access-Response, таких как неправильная длина самого сообщения.

Имя	RFC4668 имя	Утверждение
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 messages	radiusAuthClientExtAccessRetransmissions	Количество переотправленных сообщений RADIUS Access-Request.
Pending request	radiusAuthClientExtPendingRequests	Количество сообщений RADIUS Access-Request, отправленных, но не получивших ответ и не завершившихся таймаутом.
Number of timeouts	radiusAuthClientExtTimeouts	Количество таймаутов аутентификации.
IP address	-	IP-адрес и UDP-порт сервера RADIUS.
Certification status	-	Для получения подробной информации смотрите описание статуса RADIUS.
Round trip time	radiusAuthClientExtRoundTripTime	Интервал времени между самым недавним Access-Reply/Access-Challenge и Access-Request, в миллисекундах, с шагом 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

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

Server Configuration

Delete	Hostname	Port	Timeout	Change Secret Key
--------	----------	------	---------	-------------------

Add New Server

Save Reset

Описание каждого параметра представлено в следующей таблице:

Параметр	Описание
Global configuration	Глобальная конфигурация
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 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.
Server configuration	Конфигурация сервера
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

Параметр	Описание
	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 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.

Тип	Определение	Характеристики
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"> Отключить, а затем снова включить порт в представлении конфигурации порта. Изменить конфигурацию безопасности порта этого порта. Перезагрузить устройство.



Примечания:

Помечены как нарушающие безопасные MAC-адреса. Другими словами, пакеты, у которых исходные MAC-адреса помечены как нарушающие, не будут пересылаться.

Sticky MAC (клеякий 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.

7.10.1 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

☐

Aging Period

3600

seconds

Hold Time

300

seconds

Port Configuration

Port	Mode	Limit	Violation Mode	Violation Limit	Sticky	State
*	<>		<>		<input type="checkbox"/>	
G1	Disabled	4	Protect	4	<input type="checkbox"/>	Disabled
G2	Disabled	4	Protect	4	<input type="checkbox"/>	Disabled
G3	Disabled	4	Protect	4	<input type="checkbox"/>	Disabled
G4	Disabled	4	Protect	4	<input type="checkbox"/>	Disabled
G5	Disabled	4	Protect	4	<input type="checkbox"/>	Disabled
G6	Disabled	4	Protect	4	<input type="checkbox"/>	Disabled
G7	Disabled	4	Protect	4	<input type="checkbox"/>	Disabled
G8	Disabled	4	Protect	4	<input type="checkbox"/>	Disabled
G9	Disabled	4	Protect	4	<input type="checkbox"/>	Disabled
G10	Disabled	4	Protect	4	<input type="checkbox"/>	Disabled

Описание каждого параметра представлено в следующей таблице:

Параметр	Описание
Global configuration	Глобальная конфигурация
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.
Port configuration	Конфигурация порта
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"> Защита: MAC-адреса, превышающие предел, не будут изучаться, и только пакеты с несуществующими исходными MAC-адресами будут отбрасываться. 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. Отключение: Максимум Limit MAC-адресов может быть изучено, и еще один MAC-адрес вызовет отключение порта.
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.

Параметр	Описание
State	<p>Есть 4 состояния: Отключено/Готово/Достигнут предел/Отключение, отображающие текущий статус безопасности порта.</p> <ul style="list-style-type: none"> Отключено: указывает, что безопасность порта отключена. Готово: указывает, что количество безопасных MAC-адресов еще не достигло максимального предела. Достигнут предел: указывает, что количество безопасных MAC-адресов достигло максимального предела. Отключение: указывает, что порт отключен функцией безопасности порта.

7.10.2 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



Примечания:

Когда безопасный MAC-адрес (включая динамические и статические адреса) достигает максимального предела, больше статических безопасных MAC-адресов не могут быть добавлены.

7.10.3 Глобальный статус

Эта страница отображает информацию о безопасности порта. Функция безопасности порта может быть настроена непосредственно или косвенно другими функциональными модулями, такими как 802.1X. В таблице состояния порта столбец "Пользователь" указывает конфигуратор безопасности порта и идентифицируется с помощью аббревиатур. Для

значений аббревиатур смотрите "Легенду модулей пользователя".

Port Security Switch Status

Auto-refresh ☐ Refresh

User Module Legend

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

Port Status

Clear	Port	Users	Violation Mode	State	MAC Count		
					Current	Violating	Limit
Clear	G1	--	Disabled	Disabled	-	-	-
Clear	G2	--	Disabled	Disabled	-	-	-
Clear	G3	--	Disabled	Disabled	-	-	-
Clear	G4	--	Disabled	Disabled	-	-	-
Clear	G5	--	Disabled	Disabled	-	-	-
Clear	G6	--	Disabled	Disabled	-	-	-
Clear	G7	--	Disabled	Disabled	-	-	-
Clear	G8	--	Disabled	Disabled	-	-	-
Clear	G9	--	Disabled	Disabled	-	-	-
Clear	G10	--	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"> Отключено: На этом порту нет административно включенной безопасности порта. Защита: Безопасность порта административно включена в режиме защиты. Ограничено: Безопасность порта административно включена в режиме ограничения. Выключено: Безопасность порта административно включена в режиме отключения.
state	<p>Отображается текущий статус порта. Принимает одно из следующих четырех значений:</p> <ul style="list-style-type: none"> Отключено: На данный момент ни один модуль пользователя не использует сервис безопасности порта. Готово: Сервис безопасности порта используется как минимум одним модулем пользователя и ожидает появления кадров с неизвестными MAC-адресами. 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. 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.
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"> Если на порту не включен ни один пользовательский модуль, то текущий столбец будет отображать тире (-). Если модуль управления пределом не включен на порту, то столбец предела будет отображать тире (-).

7.10.4 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 Port All All ▾ Auto-refresh ☐ 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"> Динамический: когда порт не находится в режиме "Sticky", записи изучаются через прибывающие фреймы обучения в модуле безопасности порта. Статический: запись вводится конечным пользователем через административный доступ. Записи не подвержены ограничениям по сроку службы. Sticky: когда порт находится в режиме "Sticky", все записи, которые в противном случае будут изучены как динамические, будут изучены как "Sticky". <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>

Параметр	Описание
State	Укажите, находится ли соответствующий MAC-адрес в нарушении (пользователь управления настроил интерфейс в режиме "restricted" и MAC-адрес заблокирован), заблокирован или перенаправлен
Aging/holding time	<ul style="list-style-type: none"> Если хотя бы один модуль пользователя решит заблокировать этот MAC-адрес, он останется заблокированным до истечения времени удержания (в секундах). 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. Если истекло время старения (в секундах), и фреймы не обнаружены, MAC-адрес удаляется из таблицы MAC. В противном случае начнется новый период старения. Если старение отключено или модуль пользователя решает сохранять MAC-адрес бессрочно, отображается тире (-).

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 Disabled ▾

Translate dynamic to static

Port Mode Configuration

Port	Mode	Max Dynamic Clients
*	<> ▾	<> ▾
G1	Disabled ▾	Unlimited ▾
G2	Disabled ▾	Unlimited ▾
G3	Disabled ▾	Unlimited ▾
G4	Disabled ▾	Unlimited ▾
G5	Disabled ▾	Unlimited ▾
G6	Disabled ▾	Unlimited ▾
G7	Disabled ▾	Unlimited ▾
G8	Disabled ▾	Unlimited ▾
G9	Disabled ▾	Unlimited ▾
G10	Disabled ▾	Unlimited ▾
G11	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.
Port mode configuration	Конфигурация режима порта
Port	Номер порта устройства.
Mode	Настройте порт для включения/отключения функции защиты источника IP.
Max Dynamic Client	Настройте максимальное количество динамических клиентов на указанном порту. Варианты следующие: <ul style="list-style-type: none"> 0

Параметр	Описание
	<ul style="list-style-type: none"> 1 2 No limit

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 Динамические таблицы

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

Dynamic IP Source Guard Table

start from , VLAN and IP address with entries per page.

Auto-refresh ☐ Refresh

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
*	<> ▾	<> ▾
G1	Disabled ▾	Unlimited ▾
G2	Disabled ▾	Unlimited ▾
G3	Disabled ▾	Unlimited ▾
G4	Disabled ▾	Unlimited ▾
G5	Disabled ▾	Unlimited ▾
G6	Disabled ▾	Unlimited ▾
G7	Disabled ▾	Unlimited ▾
G8	Disabled ▾	Unlimited ▾
G9	Disabled ▾	Unlimited ▾
G10	Disabled ▾	Unlimited ▾
G11	Disabled ▾	Unlimited ▾
G12	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.
Port mode configuration	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:

Параметр	Описание
	<ul style="list-style-type: none"> 0 1 2 No limit

7.12.2 Статические таблицы

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

IPv6 Source Guard Static Table Auto-refresh ☐ Refresh

Port G1 VLAN ID IPv6 Address MAC Address Add Entry

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 Динамические таблицы

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

IPv6 Source Guard Dynamic Table Auto-refresh ☐ 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

Disabled ▾

Translate dynamic to static

Port Mode Configuration

Port	Mode	Check VLAN	Log Type
*	<> ▾	<> ▾	<> ▾
G1	Disabled ▾	Disabled ▾	None ▾
G2	Disabled ▾	Disabled ▾	None ▾
G3	Disabled ▾	Disabled ▾	None ▾
G4	Disabled ▾	Disabled ▾	None ▾
G5	Disabled ▾	Disabled ▾	None ▾
G6	Disabled ▾	Disabled ▾	None ▾
G7	Disabled ▾	Disabled ▾	None ▾
G8	Disabled ▾	Disabled ▾	None ▾
G9	Disabled ▾	Disabled ▾	None ▾
G10	Disabled ▾	Disabled ▾	None ▾
G11	Disabled ▾	Disabled ▾	None ▾

Описание каждого параметра представлено в следующей таблице:

Параметр	Описание
Mode	ARP detection global configuration позволяет включить функцию обнаружения ARP.
convert dynamic entries to static entries	Преобразовать все текущие динамические записи защиты ARP в статические записи.
Port mode	Конфигурация режима порта

Параметр	Описание
configuration	
Port	Номер устройства порта
Mode	Дополнительные параметры включения/отключения: <ul style="list-style-type: none"> Включить: указывает, что функция обнаружения ARP на порту включена. В этом случае порт является недоверенным портом ARP. Отключить: указывает, что функция обнаружения ARP на порту отключена. В этом случае порт является доверенным портом ARP..
Check VLAN	Дополнительные параметры включения/отключения: <ul style="list-style-type: none"> Включить: указывает на то, что будет проверяться действительность ARP-пакетов в указанной VLAN (настроенной на странице конфигурации VLAN, описанной в следующем разделе). Отключить: указывает на проверку действительности всех ARP-пакетов, полученных на этом порту.
Log type	Дополнительные параметры: Нет/Запретить/Разрешить/Все: <ul style="list-style-type: none"> Нет: означает, что записи журнала обнаружения ARP не ведутся. Запретить: означает, что в журнале записываются только отклоненные записи ARP. Разрешить: означает, что в журнале записываются только разрешенные записи ARP. Все: означает, что в журнале записываются все записи ARP.

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

Start from VLAN 1 with 20 entries per page.

Refresh |<< >>

Delete	VLAN ID	Log Type
Add New Entry		
Save	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: G1, 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: G1, 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 Расширенный функции

8.1 QoS

QoS (Qualify 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"/>		
G1	0 ▾	0 ▾	0 ▾	0 ▾	0 ▾	Disabled	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>
G2	0 ▾	0 ▾	0 ▾	0 ▾	0 ▾	Disabled	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>
G3	0 ▾	0 ▾	0 ▾	0 ▾	0 ▾	Disabled	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>
G4	0 ▾	0 ▾	0 ▾	0 ▾	0 ▾	Disabled	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>
G5	0 ▾	0 ▾	0 ▾	0 ▾	0 ▾	Disabled	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>
G6	0 ▾	0 ▾	0 ▾	0 ▾	0 ▾	Disabled	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>
G7	0 ▾	0 ▾	0 ▾	0 ▾	0 ▾	Disabled	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>
G8	0 ▾	0 ▾	0 ▾	0 ▾	0 ▾	Disabled	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>
G9	0 ▾	0 ▾	0 ▾	0 ▾	0 ▾	Disabled	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>
G10	0 ▾	0 ▾	0 ▾	0 ▾	0 ▾	Disabled	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>
G11	0 ▾	0 ▾	0 ▾	0 ▾	0 ▾	Disabled	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>
G12	0 ▾	0 ▾	0 ▾	0 ▾	0 ▾	Disabled	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>
G13	0 ▾	0 ▾	0 ▾	0 ▾	0 ▾	Disabled	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>

Описание каждого параметра представлено в следующей таблице:

Параметр	Описание
Port	Номер порта устройства
Entrance direction	Метка данных направления входа:

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



Примечания:

- Если одновременно включены функции trust dscp и trust tag, а также настроен dscp-cos entry, то trust dscp имеет более высокий приоритет, чем trust tag; в противном случае, trust tag имеет более высокий приоритет, чем trust dscp.
- Приоритет записи в таблице отображения выше, чем функции trust tag и trust dscp.

8.1.2 Стратегия очереди

Настройте портовую команду для включения в интерфейс политики направления.

QoS Ingress Queue Policers

Port	Q0	Q1	Q2	Q3	Q4	Q5	Q6	Q7
	Enabled	Enabled	Enabled	Enabled	Enabled	Enabled	Enabled	Enabled
*	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
G1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
G2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
G3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
G4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
G5	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
G6	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
G7	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
G8	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
G9	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
G10	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
G11	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
G12	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
G13	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Описание каждого параметра представлено в следующей таблице:

Параметр	Описание
port	Device port number.
queue 0-7	<ul style="list-style-type: none"> Включить: Включить функцию ограничения скорости входящего трафика на указанном интерфейсе. Скорость: Настроить значение ограничения скорости входящего трафика на указанном интерфейсе. Диапазон ограничения скорости составляет <1-13128147>. Единица измерения: Настроить единицу измерения скорости. Возможные единицы измерения - кбит/с или Мбит/с. По умолчанию используется кбит/с. <p>Примечание: Существуют различия в диапазоне скоростей для разных единиц измерения; когда выбрана единица кбит/с, диапазон ограничения скорости составляет от 25 до 13128147 кбит/с; когда выбрана единица Мбит/с, диапазон ограничения скорости составляет от 1 до 13128 Мбит/с</p>

8.1.3 Расписание портов

Настройка расписания очереди и формирования интерфейса порта.

QoS Egress Port Schedulers

Port	Mode	Weight							
		Q0	Q1	Q2	Q3	Q4	Q5	Q6	Q7
G1	Strict Priority	-	-	-	-	-	-	-	-
G2	Strict Priority	-	-	-	-	-	-	-	-
G3	Strict Priority	-	-	-	-	-	-	-	-
G4	Strict Priority	-	-	-	-	-	-	-	-
G5	Strict Priority	-	-	-	-	-	-	-	-
G6	Strict Priority	-	-	-	-	-	-	-	-
G7	Strict Priority	-	-	-	-	-	-	-	-
G8	Strict Priority	-	-	-	-	-	-	-	-
G9	Strict Priority	-	-	-	-	-	-	-	-
G10	Strict Priority	-	-	-	-	-	-	-	-
G11	Strict Priority	-	-	-	-	-	-	-	-
G12	Strict Priority	-	-	-	-	-	-	-	-
G13	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.

G1 QoS Egress Port Scheduler and Shapers Port 1

G1

Scheduler Mode: Strict Priority

Queue Shaper					Queue Scheduler		Port Shaper			
Enabled	Rate	Unit	Rate-Type	Cred	Cut-through	Enabled	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"/>	<input type="checkbox"/>					
<input type="checkbox"/>	500	kbps	Line	<input type="checkbox"/>	<input type="checkbox"/>					
<input type="checkbox"/>	500	kbps	Line	<input type="checkbox"/>	<input type="checkbox"/>					
<input type="checkbox"/>	500	kbps	Line	<input type="checkbox"/>	<input type="checkbox"/>					
<input type="checkbox"/>	500	kbps	Line	<input type="checkbox"/>	<input type="checkbox"/>					
<input type="checkbox"/>	500	kbps	Line	<input type="checkbox"/>	<input type="checkbox"/>					
<input type="checkbox"/>	500	kbps	Line	<input type="checkbox"/>	<input type="checkbox"/>					
<input type="checkbox"/>	500	kbps	Line	<input type="checkbox"/>	<input type="checkbox"/>					
<input type="checkbox"/>	500	kbps	Line	<input type="checkbox"/>	<input type="checkbox"/>					

STRICT

500 kbps Line

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"> Строгий приоритет: Очереди 0–7 планируются с полным строгим приоритетом. 2 веса очереди: Очереди 0–1 планируются по методу взвешенного кругового расписания, очереди 2–7 планируются с полным строгим приоритетом. 3 веса очереди: Очереди 0–2 планируются по методу взвешенного кругового расписания, а очереди 3–7 планируются с полным строгим приоритетом. 4 веса очереди: Очереди 0–3 планируются по методу взвешенного кругового расписания, а очереди 4–7 планируются с полным строгим приоритетом. 5 весов очереди: Очереди 0–4 планируются по методу взвешенного кругового расписания, а очереди 5–7 планируются с полным строгим приоритетом. 6 весов очереди: Очереди 0–5 планируются по методу взвешенного кругового расписания, а очереди 6–7 планируются с полным строгим приоритетом.

Параметр	Описание
	<p>приоритетом.</p> <ul style="list-style-type: none"> 7 весов очереди: Очереди 0–6 планируются по методу взвешенного кругового расписания, а 7-я очередь планируется с полным строгим приоритетом. 8 весов очереди: Очереди 0–7 планируются по методу взвешенного кругового расписания.
queue shaping	<ul style="list-style-type: none"> Включить: Включить функцию ограничения скорости входящего трафика на указанном порту. Скорость: Настроить значение ограничения скорости передачи данных для каждого направления на порту. Диапазон ограничения скорости составляет <1-13107100>. Единица измерения: Настроить единицу измерения ограничения скорости. Возможные единицы измерения - кбит/с или Мбит/с. По умолчанию используется кбит/с. <p>Примечание: Когда выбрана единица кбит/с, диапазон ограничения скорости составляет от 100 до 13107100 кбит/с; когда выбрана единица Мбит/с, диапазон ограничения скорости составляет от 1 до 13107 Мбит/с.</p> <ul style="list-style-type: none"> Режим скорости: Настроить тип скорости ограничения, который можно настроить как скорость линии/данные (line/data). Единицы измерения скорости - кбит/с или Мбит/с. По умолчанию используется скорость линии. Доверие: Параметры конфигурации TSN (Time-Sensitive Networking). Если TSN не включен, рекомендуется не включать опцию доверия
queue scheduler	Cut-through: Включить ли режим обмена данными в режиме Cut-through.
port shaping	<ul style="list-style-type: none"> Включить: Управляет включением формирования порта для порта коммутатора. Показываются только несервисные конфигурации. 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.

Параметр	Описание
	<ul style="list-style-type: none"> Единица: Единица измерения, используемая для управления скоростью формирования порта, такая как kbps/Mbps/fps/kfps. Показываются только несервисные конфигурации. 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.



Примечания:

- Скорость линии (line) - это скорость передачи данных на первом уровне (включая IPG); данные (data) - это скорость передачи данных на втором уровне (исключая IPG).
- Прямая передача (cut-through forwarding) заменяет метод "хранить и передавать" (store-and-forward). Он не обеспечивает возможности обнаружения ошибок пакетов и подвержен потере пакетов, но имеет низкую задержку и высокую скорость коммутации.

8.1.4 Формирование порта

Просмотрите страницу планирования портов.

QoS Egress Port Shapers

Port	Shapers								Port
	Q0	Q1	Q2	Q3	Q4	Q5	Q6	Q7	
<u>G1</u>	-	-	-	-	-	-	-	-	-
<u>G2</u>	-	-	-	-	-	-	-	-	-
<u>G3</u>	-	-	-	-	-	-	-	-	-
<u>G4</u>	-	-	-	-	-	-	-	-	-
<u>G5</u>	-	-	-	-	-	-	-	-	-
<u>G6</u>	-	-	-	-	-	-	-	-	-
<u>G7</u>	-	-	-	-	-	-	-	-	-
<u>G8</u>	-	-	-	-	-	-	-	-	-
<u>G9</u>	-	-	-	-	-	-	-	-	-
<u>G10</u>	-	-	-	-	-	-	-	-	-
<u>G11</u>	-	-	-	-	-	-	-	-	-
<u>G12</u>	-	-	-	-	-	-	-	-	-
<u>G13</u>	-	-	-	-	-	-	-	-	-
<u>G14</u>	-	-	-	-	-	-	-	-	-

Для получения подробной информации о конфигурации и отображении формирования порта, пожалуйста, обратитесь к странице "Планирование портов". Эти две функции тесно связаны между собой.

8.1.5 Маркировка портов

Страница установки меток на исходящих портах.

QoS Egress Port Tag Remarking

Port	Mode
G1	Classified
G2	Classified
G3	Classified
G4	Classified
G5	Classified
G6	Classified
G7	Classified
G8	Classified
G9	Classified
G10	Classified

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

G1QoS Egress Port Tag Remarking

Tag Remarking Mode

Classified ▾

Save

Reset

Cancel

G1QoS Egress Port Tag Remarking

Tag Remarking Mode Default ▾

PCP/DEI Configuration

Default PCP 0 ▾

Default DEI 0 ▾

Save Reset Cancel

G1QoS Egress Port Tag Remarking

Tag Remarking Mode Map ▾

(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 ▾

Описание каждого параметра представлено в следующей таблице:

Параметр	Описание
Label relabeling	Режим переосмысления меток, варианты, следующие:

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

8.1.6 Порт DSCP

Страница настройки DSCP порта..

QoS Port DSCP Configuration

Port	In		Out
	Translate	Classified	Rewrite
*	<input type="checkbox"/>	<> ▾	<> ▾
G1	<input type="checkbox"/>	Disabled ▾	Disabled ▾
G2	<input type="checkbox"/>	Disabled ▾	Disabled ▾
G3	<input type="checkbox"/>	Disabled ▾	Disabled ▾
G4	<input type="checkbox"/>	Disabled ▾	Disabled ▾
G5	<input type="checkbox"/>	Disabled ▾	Disabled ▾
G6	<input type="checkbox"/>	Disabled ▾	Disabled ▾
G7	<input type="checkbox"/>	Disabled ▾	Disabled ▾
G8	<input type="checkbox"/>	Disabled ▾	Disabled ▾
G9	<input type="checkbox"/>	Disabled ▾	Disabled ▾
G10	<input type="checkbox"/>	Disabled ▾	Disabled ▾
G11	<input type="checkbox"/>	Disabled ▾	Disabled ▾
G12	<input type="checkbox"/>	Disabled ▾	Disabled ▾
G13	<input type="checkbox"/>	Disabled ▾	Disabled ▾
G14	<input type="checkbox"/>	Disabled ▾	Disabled ▾

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.
Classification	Настройка вариантов классификации входящего DSCP. Варианты, следующие: <ul style="list-style-type: none"> Отключить

Параметр	Описание
	<ul style="list-style-type: none"> DSCP=0: Указывает, что обрабатываются только пакеты с значением DSCP равным 0, и пакеты обрабатываются в соответствии с таблицей классификации DSCP. 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. 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).
Rewrite	<p>Настройка опций перезаписи в исходящем направлении порта. Варианты следующие:</p> <ul style="list-style-type: none"> Отключить Включить: Для пакетов, классифицированных по DSCP во входящем направлении, необходимо выбрать Включить для исходящего порта этого типа пакета. Перемапировать: Перемапировать в соответствии с конфигурацией перемапирования в исходящем направлении в записи таблицы отображения DSCP.

8.1.7 DSCP-QoS

Страница настройки записи DSCP-CoS.

DSCP-Based QoS Ingress Classification

DSCP	Trust	CoS	DPL
*	<input type="checkbox"/>	<> v	<> v
0 (BE)	<input type="checkbox"/>	0 v	0 v
1	<input type="checkbox"/>	0 v	0 v
2	<input type="checkbox"/>	0 v	0 v
3	<input type="checkbox"/>	0 v	0 v
4	<input type="checkbox"/>	0 v	0 v
5	<input type="checkbox"/>	0 v	0 v
6	<input type="checkbox"/>	0 v	0 v
7	<input type="checkbox"/>	0 v	0 v
8 (CS1)	<input type="checkbox"/>	0 v	0 v
9	<input type="checkbox"/>	0 v	0 v
10 (AF11)	<input type="checkbox"/>	0 v	0 v
11	<input type="checkbox"/>	0 v	0 v
12 (AF12)	<input type="checkbox"/>	0 v	0 v
13	<input type="checkbox"/>	0 v	0 v
14 (AF13)	<input type="checkbox"/>	0 v	0 v

Описание каждого параметра представлено в следующей таблице:

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

8.1.8 Отображение DSCP

Страница записи отображения DSCP.

DSCP Translation

DSCP Translation	In		Out
	Translate	Classified	Remap
*	<> ▾	<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 ▾

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.

8.1.9 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.

8.1.10 Сопоставление записей

Настройка записей таблицы сопоставления.

QoSIngress Port Tag Classification Port

Auto-refresh ☐ Refresh Batch Delete

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

+

Нажмите на значок добавления, чтобы перейти на страницу создания/изменения экземпляра сопоставления входящего потока.

Ingress Port Tag Classification Port

Ingress MAC ID

Map ID

Ingress Map Key

Map Key

Ingress Map Action

CoS	<input type="text" value="Disabled"/>
DPL	<input type="text" value="Disabled"/>
PCP	<input type="text" value="Disabled"/>
DEI	<input type="text" value="Disabled"/>
DSCP	<input type="text" value="Disabled"/>
CoS ID	<input type="text" value="Disabled"/>

трагца конфигурации и изменения ключевых правил для входящего направления DSCP-PCP-DEI:

QoS Map Rules Ingress Map 0

Rules with Key PCP-DEI

Key		Action					
PCP	DEI	CoS	DPL	PCP	DEI	DSCP	CoS ID

☐ Auto-refresh

QoS Map Rules Ingress Map 0

Rules with Key DSCP

Key		Action					
DSCP	CoS	DPL	PCP	DEI	DSCP	CoS ID	

☐ Auto-refresh

IngressMap 0 Rule Configuration

IngressRule Key

PCP	0 ▾
DEI	0 ▾

Ingress Rule Action

CoS	0 ▾
DPL	0 ▾
PCP	0 ▾
DEI	0 ▾
DSCP	0 (BE) ▾
CoS ID	0 ▾

Save	Reset	Cancel
------	-------	--------

IngressMap 0 Rule Configuration

IngressRule Key

DSCP	0 (BE) ▾
------	----------

Ingress Rule Action

CoS	0 ▾
DPL	0 ▾
PCP	0 ▾
DEI	0 ▾
DSCP	0 (BE) ▾
CoS ID	0 ▾

Save	Reset	Cancel
------	-------	--------

Описание каждого параметра представлено в следующей таблице:

Параметр	Описание
Mapping ID	Идентификатор экземпляра сопоставления входящего направления. Диапазон <0-255>.

Параметр	Описание
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.



Примечания:

- Для сопоставления портала можно использовать 512 ресурсов, а максимальный конфигурируемый идентификатор экземпляра - 255.
- Экземпляры сопоставления потребляют разные ресурсы в зависимости от типов ключей. PCP занимает 1, PCP-DEI занимает 2, DSCP занимает 8, а DSCP-PCP-DEI занимает 10. Поэтому конкретное количество экземпляров, которые можно настроить, зависит не только от верхнего предела конфигурации идентификатора экземпляра, но и от связанных с ним ресурсов.

8.1.11 Экспорт сопоставления

Настройка записей сопоставления экспорта.

QoS Egress Port Tag Classification Port

Auto-refresh ☐ Refresh Batch Delete

Map ID	Key-Type	Action-Type		
		PCP	DEI	DSCP

Страница создания/изменения экземпляра сопоставления исходящего потока.

QoS Egress Map Configuration

Egress Map ID

Map ID

Egress Map Key

Map Key

Egress Map Action

PCP

DEI

DSCP

Страница настройки и изменения правил ключа для сопоставления исходящего направления Cos ID-DPL

QoS Egress Port Tag Classification Port

Auto-refresh ☐

Map ID	Key-Type	Action-Type		
		PCP	DEI	DSCP

EgressMap 0 Rule Configuration

EgressRule Key

CoS ID

DPL

Egress Rule Action

PCP

DEI

DSCP

Страница настройки и изменения правил ключа для исходящего направления DSCP-DPL.

QoS Egress Port Tag Classification Port Auto-refresh ☐ Refresh Batch Delete

Map ID	Key-Type	Action-Type		
		PCP	DEI	DSCP

+

EgressMap 0 Rule Configuration

EgressRule Key

DSCP	0 (BE)	▼
DPL	0	▼


Egress Rule Action

PCP	0	▼
DEI	0	▼
DSCP	0 (BE)	▼

Save Reset Cancel

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	Указывает тип операции, который будет использоваться для фильтрации правил сопоставления при применении сопоставления. Возможные типы операций: <ul style="list-style-type: none"> PCP: указывает на 802.1P. DEI: указывает на Discard Eligibility Indicator (индикатор пригодности для удаления). DSCP: указывает на Differentiated Services Code Point (точку кода дифференцированных служб)

 Примечания:

- Для экспорта сопоставления можно использовать 4096 ресурсов, а максимальный конфигурируемый экземпляр составляет 512.
- Экземпляры сопоставления потребляют разные ресурсы в зависимости от типов ключей. CoS ID занимает 8, CoS ID-DPL занимает 32, DSCP занимает 64, а DSCP-DPL занимает 256. Поэтому конкретное количество экземпляров, которые можно настроить, зависит не только от верхнего предела конфигурации идентификатора экземпляра, но и от ресурсов, связанных с их использованием.

8.1.12 QoS список управления

Настройка списка управления QoS.

QoS 控制列表配置

QoS 控制 ID	端口	目的 MAC	源 MAC	标签类型	VID	PCP	DEI	帧类型	功能参数							
									CoS	DPL	DSCP	PCP	DEI	策略	入方向映射	
<div style="text-align: right;">+</div>																

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

QCE Configuration

Port Members																													
G1	G2	G3	G4	G5	G6	G7	G8	G9	G10	G11	G12	G13	G14	G15	G16	G17	G18	G19	G20	G21	G22	G23	G24	X1	X2	X3	X4	X5	X6
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	

Key Parameters

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

Action Parameters

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

Описание каждого параметра представлено в следующей таблице:

Параметр	Описание
Port member	Укажите порт, для которого применяется эта QCE.
Key parameter	Ключевой параметр.
Destination	Настройте соответствие информации DMAC.

Параметр	Описание
MAC	
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.
Function Parameter	Параметры функции:
CoS	Значение сопоставленного CoS.
DPL	Значение сопоставленного DPL.
DSCP	Значение сопоставленного DSCP.
PCP	Значение сопоставленного PCP.
DEI	Значение сопоставленного DEI
Strategy	Применить экземпляр политики. Для этой информации о политике необходимо проверить информацию о конфигурации ACL.
Ingress Map ID	Применить пример входящего сопоставления.
Ethernet Parameters	Параметры Ethernet:
Ethernet	Когда тип кадра "EtherType", диапазон конфигурации составляет <0x600-0x7ff, 0x801-0x86dc, 0x86de-0xffff>.
LLC Parameters	Параметры LLC:
SSAP address	Исходный адрес точки доступа к сервису (Source Service Access Point), также называемый адресом исходной точки доступа к сервису LLC, варьируется от 0X00 до 0XFF.
DSAP address	Адрес точки доступа к сервису назначения (Destination Service Access Point), также называемый адресом точки доступа к сервису LLC назначения, варьируется от 0X00 до 0XFF.
control	Контроль (Control), диапазон составляет от 0X00 до 0XFF.
SNAP Parameters	Параметры SNAP:
PID	Значение типа Ether, варьируется от 0x0000 до 0xFFFF.
IPv4 Parameters	Параметры IPv4:

Параметр	Описание
protocol	Соответствует типу протокола IPv4, такому как TCP/UDP или другим, и диапазон значений составляет 0-255.
SIP	Настройка информации об исходном IP, которая соответствует параметрам IPv4.
DIP	Настройка информации о целевом IP, которая соответствует параметрам IPv4.
IP fragmentation	Настройка информации о фрагментации IP, которая соответствует параметрам IPv4.
DSCP	Настройка значения DSCP, соответствующего параметрам IPv4.
source port	Настройка номера порта источника TCP/UDP, диапазон значений составляет 0-65535.
destination port	Настройка номера порта назначения TCP/UDP, диапазон значений составляет 0-65535.
IPv6 Parameters	Параметры IPv6:
protocol	Настройка типа протокола IPv6, такого как TCP/UDP или других, и диапазон значений составляет 0-255.
SIP	Настройка информации об исходном IP (32 младших бита), соответствующей параметрам IPv6.
DIP	Настройка информации о целевом IP (32 младших бита), соответствующей параметрам IPv6.
DSCP	Настройка значения DSCP, соответствующего параметрам IPv6.
source port	Настройка номера порта источника TCP/UDP, диапазон значений составляет 0-65535.
destination port	Настройка номера порта назначения TCP/UDP, диапазон значений составляет 0-65535.



Примечания:

- При настройке диапазонов значений для DSCP, SPORT, DPORT и VID, если значение диапазона нельзя преобразовать в форму значения/маски, будет применяться хранилище ресурсов. Для параметров диапазона разрешается использовать только 8 ресурсов. Недостаточное количество ресурсов приведет к конфликтам правил.
- Диапазон внутренней конфигурации VID не поддерживает применение ресурсов, поэтому он должен быть в форме, которая может быть преобразована в значение/маску.
- Преобразование в режим значения/маски: ((нижний & ~маска) == нижний) && ((верхний & маска) == маска)

8.1.13 Статистика QoS

Просмотр статистики отправки и приема пакетов в очередях QoS.

Queueing Counters

Auto-refresh ☐ 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
G1	15617	0	0	0	0	0	0	0	0	0	0	0	0	0	0	16286
G2	3543	0	0	0	0	0	0	0	0	0	0	0	0	0	0	3603
G3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
G4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
G5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
G6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
G7	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
G8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
G9	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
G10	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
G11	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
G12	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
G13	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
G14	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
G15	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	<p>Каждый порт имеет 8 очередей QoS. Очередь 0 является очередью с наименьшим приоритетом.</p> <ul style="list-style-type: none"> TX: Количество пакетов, отправленных каждой очередью. RX: Количество пакетов, принятых каждой очередью.

8.1.14 QCL статус

Проверьте состояние списка управления QoS.

QoS Control List Status

Combined ☐ Auto-refresh ☐ Resolve Conflict Refresh

User	QCE	Port	Frame Type	Action							conflict
				CoS	DPL	DSCP	PCP	DEI	Policy	Ingress Map	
No more 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	<p>Укажите тип кадра. Возможные значения:</p> <ul style="list-style-type: none"> Любой (Any): Соответствует любому типу кадра. Ethernet: Соответствует кадрам типа Ethernet. LLC: Соответствует кадрам LLC (Logical Link Control). SNAP: Соответствует кадрам SNAP (Subnetwork Access Protocol). IPv4: Соответствует кадрам IPv4. IPv6: Соответствует кадрам IPv6.
Action	<p>Укажите действие классификации, которое должно быть выполнено над входящим кадром, если настроенные параметры соответствуют содержимому кадра.</p> <p>Возможные действия:</p> <ul style="list-style-type: none"> CoS: Классификация услуг. DPL: Классификация приоритетов сброса. DSCP: Классификация значений DSCP. PCP: Классификация значений PCP. DEI: Классификация значений DEI. Policy: Содержание шаблона политики (совпадающие элементы и элементы функции), созданного с использованием модуля ACL. Входящее направление сопоставления.
Conflict	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

Параметр	Описание
	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.

8.2 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.

8.2.1 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
*		<>	<>	Disabled G1 G2 G3	<>	<>	<>	<>	*
G1	0	Permit	Disabled	Disabled G1 G2 G3 G4	Disabled	Disabled	Disabled	Enabled	15419
G2	0	Permit	Disabled	Disabled G1 G2 G3 G4	Disabled	Disabled	Disabled	Enabled	3515
G3	0	Permit	Disabled	Disabled G1 G2 G3 G4	Disabled	Disabled	Disabled	Enabled	0
G4	0	Permit	Disabled	Disabled G1 G2 G3 G4	Disabled	Disabled	Disabled	Enabled	0
G5	0	Permit	Disabled	Disabled G1 G2 G3 G4	Disabled	Disabled	Disabled	Enabled	0
G6	0	Permit	Disabled	Disabled G1 G2 G3 G4	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, будет ли записываться информация о пакетах, полученных данным интерфейсом (кадры с длиной кадра менее 1526 байт). По умолчанию эта опция отключена. Примечание: Длина сообщения в журнале не включает 4-байтовую контрольную сумму кадра (FCS)
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.

8.2.2 Ограничение скорости

Настройте шаблон ограничителя скорости. Как показано ниже.

ACL Rate Limiter Configuration

Rate Limiter ID	Rate	Unit
*	<input type="text"/>	<input type="text"/>
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

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).



Примечания:


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

8.2.3 Контроль доступа

Настроить список контроля доступа. Как показано ниже:

Access Control List Configuration Auto-refresh ☐ Refresh Clear Remove All

ACL ID	Ingress Port	Policy/Bitmask	Frame Type	Action	Rate Limiter ID	Port Redirect	Mirror	Counter
+								

Создайте ACE, нажмите на синюю иконку , и появится следующая страница. Различные типы кадров имеют разные страницы конфигурации, и поддерживаются следующие типы кадров.

- Arbitrary

ACE Configuration

Ingress Port	All
	G1
	G2
	G3
	G4
Policy Filter	Any
Frame Type	Any

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

VLAN Parameters

802.1Q Tagged	Any
VLAN ID Filter	Any
Tag Priority	Any

Save Reset Cancel

- Ether type

ACE Configuration

Ingress Port	All G1 G2 G3 G4
Policy Filter	Specific
Policy Value	0
Policy Bitmask	0xff
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 G1 G2 G3 G4
Policy Filter	Specific
Policy Value	0
Policy Bitmask	0xff
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

Sender MAC Match SMAC	Any
Target MAC Match SMAC	Any
IP/Ethernet Length	Any
IP	Any
Ethernet	Any

Save Reset Cancel

• IPv4

ACE Configuration

Ingress Port	All G1 G2 G3 G4
Policy Filter	Specific
Policy Value	0
Policy Bitmask	0xff
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 G1 G2 G3 G4
Policy Filter	Specific
Policy Value	0
Policy Bitmask	0xff
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.

Параметр	Описание
policy filter	<p>Если данное значение - any, это указывает на то, что это ACL; наоборот, если это значение находится в диапазоне от 0 до 255, это указывает на то, что данная политика конфигурации ACL является шаблоном фильтрации, влияющим на все функции, к которым был применен данный идентификатор политики.</p> <p>Примечание: Когда идентификатор политики применяется к порту, его входная конфигурация порта также используется в качестве ключа для участия в сопоставлении. Попадание произойдет только в том случае, если порт, к которому применен этот идентификатор политики, и входной порт, настроенный с этим идентификатором политики, также совпадают.</p>
frame type	<p>Тип кадра Ethernet имеет следующие варианты:</p> <ul style="list-style-type: none"> Любой Ethernet Type: По умолчанию сопоставляет ether-типы, отличные от 0x0806/0x0800/0x86DD. ARP: По умолчанию сопоставляет ether-тип 0x0806. IPv4: По умолчанию сопоставляет ether-тип 0x0800. IPv6: По умолчанию сопоставляет ether-тип 0x86DD.
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:</p> <p>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.
VLAN Parameters	Параметры VLAN

Параметр	Описание
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.
MAC Parameters	Параметры MAC
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.
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.
Ether type Parameters	Параметры типа Ether:
ether type filtering	<p>Сопоставляет пакеты с указанными значениями EtherType, отличными от (0x0806/0x0800/0x86DD).</p> <p>Примечание: При сопоставлении значения EtherType 0x8100/0x88a8 необходимо сопоставить параметр VLAN, а фильтрация EtherType должна быть установлена на "Any", чтобы это сработало.</p>
ARP Parameters	Параметры ARP
ARP/RARP	Сопоставление пакетов arp/rarp.
request/Reply	Сопоставление типа пакета arp запроса или ответа.
sender IP filter	Сопоставление поля отправителя IP в заголовке arp.
target IP filter	Сопоставление поля целевого IP в заголовке arp.
sender MAC matches SMAC	Учитывать соответствие MAC-адреса отправителя ARP и SMAC в заголовке Ethernet. Значение 0 означает отсутствие совпадения, а 1 - совпадение (равенство).
destination MAC matches SMAC	Учитывать соответствие MAC-адреса назначения RARP и SMAC в заголовке Ethernet. Значение 0 означает отсутствие совпадения, а 1 - совпадение (равенство)
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

Параметр	Описание
	в заголовке arp не равен 1.
IP parameters	Параметры IP
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).
ICMP parameters	Параметры ICMP
ICMP type filtering	Сопоставление типа ICMP. Диапазон настраивается <0-255>.
ICMP Code filtering	Сопоставление кода ICMP. Диапазон настраивается <0-255>.
TCP/UDP parameters	Параметры TCP/UDP
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

Параметр	Описание
	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.
IPv6 parameters	IPv6 параметр
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.

8.2.4 ACL статус

Проверить статус настроенного ACL.

ACL Status combined ☐ Auto-refresh

User	ACE ID	Frame Type	Action	Rate Limiter	Mirror	CPU	Counter	conflict
CST	1	Ethernet Type	Deny	Disabled	Disabled	Yes	0	No
CST	2	Ethernet Type	Deny	Disabled	Disabled	Yes	0	No
CST	3	IPv4/UDP 57050	Filter	Disabled	Disabled	Yes	0	No
CST	4	IPv4/UDP 57051	Filter	Disabled	Disabled	Yes	0	No
IP	1	IPv4 DIP:224.0.0.1/32	Permit	Disabled	Disabled	Yes	0	No
IP	2	IPv4 DIP:224.0.0.188/32	Permit	Disabled	Disabled	Yes	0	No
static	1	Any	Permit	Disabled	Disabled	No	394	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.

Параметр	Описание
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>

8.3 Link OAM

OAM (Operations, Administration, and Maintenance) - это инструмент для мониторинга сетевых сбоев и качества связи. Link OAM - это функция уровня канала связи OAM, которая соответствует стандарту IEEE802.3ah и предоставляет функции мониторинга сбоев в канале, удаленного циклического обхода и извлечения MIB для связи между двумя напрямую подключенными устройствами.

8.3.1 Конфигурация порта

Страница конфигурации Link OAM. Как показано ниже.

Link OAM Port Configuration

Port	OAM Enabled	OAM Mode	Loopback Support	Link Monitor Support	MIB Retrieval Support	Loopback Operation
*	<input type="checkbox"/>	<>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
G1	<input type="checkbox"/>	Passive	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
G2	<input type="checkbox"/>	Passive	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
G3	<input type="checkbox"/>	Passive	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
G4	<input type="checkbox"/>	Passive	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
G5	<input type="checkbox"/>	Passive	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
G6	<input type="checkbox"/>	Passive	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
G7	<input type="checkbox"/>	Passive	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
G8	<input type="checkbox"/>	Passive	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
G9	<input type="checkbox"/>	Passive	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
G10	<input type="checkbox"/>	Passive	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
G11	<input type="checkbox"/>	Passive	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
G12	<input type="checkbox"/>	Passive	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
G13	<input type="checkbox"/>	Passive	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
G14	<input type="checkbox"/>	Passive	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Описание каждого параметра представлено в следующей таблице:

Параметр	Описание
port	Номер порта, автомат состояний OAM работает независимо на каждом порте.
OAM enable	Переключатель включения OAM на уровне порта
OAM working mode	<p>Установить режим работы OAM.</p> <ul style="list-style-type: none"> Активный: В этом режиме порт будет активно отправлять сообщения Information OAMPDU партнеру для выполнения процесса обнаружения OAM. Пассивный: В этом режиме порт не будет активно отправлять сообщения Information OAMPDU. После получения сообщений Information OAMPDU, отправленных партнером, и проверки, что партнер находится в режиме Активный, он начнет участвовать в обнаружении OAM
support remote loopback	Переключатель функции удаленного циклического обхода для этого узла. При отключении игнорирует запрос на удаленный циклический обход узла и приводит к тайм-ауту запроса на удаленный циклический обход узла.
support link monitoring	По умолчанию включен. При включении локальный конец обнаруживает ухудшение качества связи и отправляет соответствующие уведомления о событиях ошибок.
support MIB search	Переключение для поддержки функции извлечения MIB.
initiate remote loopback	Немедленно после включения отправляет запрос на удаленный циклический обход узлу



Описание:

- Пассивный режим не поддерживает инициирование запросов на извлечение MIB и управление циклическим обходом.
- Для ответа на запросы на извлечение MIB и управление циклическим обходом требуется, чтобы рабочий режим партнера был Активным.
- При конфигурации необходимо обратить внимание на то, что на обоих концах соединения должно быть как минимум одно OAM в режиме Активный, иначе переговоры OAM не будут успешными

8.3.2 Конфигурация событий

Страница конфигурации событий Link OAM показана на рисунке ниже

Event Configuration for G1

G1 ▾

Event Name	Error Window	Error Threshold
Error Frame Event	1	1
Symbol Period Error Event	1	1
Seconds Summary Event	60	1

Save

Reset

Общие события связи передаются с помощью PDU уведомлений о событиях. Когда один конец OAM мониторит общее событие связи, он отправляет уведомление о событии OAMPDU, содержащее метку превышения предела ошибок, метку превышения предела ошибочных кадров или метку превышения предела секунд ошибочных кадров, на противоположный конец для отчетности, чтобы обеспечить мониторинг состояния сети в реальном времени и достижение эффективного управления сетью.

OAM периодически проверяет, достигает ли количество ошибочных кадров, полученных на порту, порога в пределах окна событий ошибок. В случае достижения порога он отправляет соответствующие уведомления о событиях.

Описание каждого параметра представлено в следующей таблице:

Типы общих событий связи	Описание
error frame event	В пределах заданного окна мониторинга, если порт обнаруживает,

Типы общих событий связи	Описание
	что количество принятых ошибочных кадров достигает порога, устройство сгенерирует событие ошибочного кадра и уведомит партнера.
bad symbol cycle event	В пределах заданного окна мониторинга, если порт обнаруживает, что количество кадров с ошибками проверки кода достигает порога, устройство сгенерирует событие периода ошибочных символов и уведомит партнера.
error frame seconds summary event	Если интерфейс получает ошибочный кадр в течение определенной секунды, эта секунда называется секундой ошибочного кадра. В пределах заданного окна мониторинга, если количество обнаруженных портом секунд ошибочных кадров достигает порога, устройство сгенерирует событие сводки секунд ошибочных кадров и уведомит партнера



Описание:

Рекомендуется не устанавливать порог события ошибки равным 0, а выбирать соответствующий порог срабатывания события для фактических условий канала связи, чтобы гарантировать, что частота уведомлений о событиях ошибок остается в разумных пределах.

8.3.3 Статистика

Эта страница используется для просмотра статистики пакетов OAM, отправленных и полученных через соединение. Как показано ниже.

Detailed Link OAM Statistics for G1 G1 Auto-refresh Refresh Clear

Receive Total	Transmit Total
Rx OAM Information PDU's	0 Tx OAM Information PDU's 0
Rx Unique Error Event Notification	0 Tx Unique Error Event Notification 0
Rx Loopback Control	0 Tx Loopback Control 0
Rx Variable Request	0 Tx Variable Request 0
Rx Variable Response	0 Tx Variable Response 0
Rx Org Specific PDU's	0 Tx Org Specific PDU's -
Rx Unsupported Codes	0 Tx Unsupported Codes 0
Rx Link Fault PDU's	0 Tx Link Fault PDU's 0
Rx Dying Gasp	0 Tx Dying Gasp 0
Rx Critical Event PDU's	0 Tx Critical Event PDU's 0

Описание каждого параметра представлено в следующей таблице:

Параметр	Описание
Number of information messages received/sent from OAM	Количество полученных/отправленных пакетов информации OAM через порт.
Number of unique error event notifications received/sent	Количество сообщений об ошибках, полученных/отправленных портом.
Number of received/sent loopback control frames	Количество кадров контроля приема/циклического обхода, полученных/отправленных портом.
Receive/send variable requests	Количество запросов на получение/отправку переменных MIB, полученных/отправленных портом.
Receive/send variable replies	Количество ответов на запросы на получение переменных MIB, полученных/отправленных портом.
Number of unique frames received/sent by organization	Количество кадров, уникальных для организации, полученных/отправленных портом (LinkOAM не поддерживает отправку кадров, уникальных для организации).
Number of invalid message encoding frames received/sent	Количество кадров с неверным кодированием, полученных/отправленных портом.
Number of receive/transmit link failures	Количество ошибок связи приема/передачи портом.
Number of receive/send fatal errors	Количество фатальных ошибок приема/передачи портом.
Number of emergency events received/sent	Количество аварийных событий, полученных/отправленных портом

8.3.4 Статус порта

Эта страница позволяет пользователям просматривать текущие результаты переговоров с партнером по OAM и информацию о состоянии, как показано на рисунке ниже.

Detailed Link OAM Status for G1

G1 Auto-refresh Refresh

PDU Permission	Receive only
Discovery State	Fault state
Peer MAC Address	*****

Local	Peer
Mode	Passive Mode
Unidirectional Operation Support	Disabled Unidirectional Operation Support
Remote Loopback Support	Disabled Remote Loopback Support
Link Monitoring Support	Enabled Link Monitoring Support
MIB Retrieval Support	Disabled MIB Retrieval Support
MTU Size	1500 MTU Size
Multiplexer State	Forwarding Multiplexer State
Parser State	Forwarding Parser State
Organizational Unique Identification	00-00-00 Organizational Unique Identification
PDU Revision	0 PDU Revision

Описание каждого параметра представлено в следующей таблице:

Параметр	Описание
OAM negotiation status	Значение статуса OAM
message status	<p>Возможности обработки сообщений:</p> <ul style="list-style-type: none"> Только прием: может только принимать сообщения. Ошибка соединения: Не может отправлять и принимать, обнаружена ошибка соединения. Обмен информацией: может только отправлять и принимать информационные сообщения. Любой: Может отправлять и принимать любые сообщения OAM
discovery status	<p>Определение состояний машины состояний:</p> <ul style="list-style-type: none"> Состояние ошибки: отказ в соединении. Активное состояние: активный режим, отправка внешних сообщений о переговорах. Пассивное состояние: пассивный режим, ожидание получения сообщений о переговорах. SEND_LOCAL_REMOTE_STATE: получено сообщение от партнера и оно не соответствует локальным требованиям к

Параметр	Описание
	<p>переговорам.</p> <ul style="list-style-type: none"> SEND_LOCAL_REMOTE_OK_STATE: получено сообщение от партнера и оно соответствует локальным требованиям к переговорам. SEND_ANY_STATE: успешные переговоры
peer MAC address	Полученный MAC-адрес партнера в сообщении.
OAM port status	Статус порта OAM.
Operating mode	Отображение режима работы устройства.
support one-way sending	Показывает, поддерживает ли устройство одностороннюю отправку.
respond to remote loopback	Показывает, поддерживает ли устройство ответы на запросы удаленного циклического обхода от партнерского конца.
support link monitoring	Показывает, поддерживает ли устройство мониторинг соединения.
support MIB search	Показывает, поддерживает ли устройство извлечение MIB.
OAMPDU maximum length	Отображает максимальную длину пакета OAM, поддерживаемую конфигурацией OAM устройства.
multicast status	Отображает возможность порта OAM отправлять пакеты.
protocol parsing status	Отображает возможность порта OAM пересылать пакеты.
manufacturer's unique identifier	Отображает уникальный идентификатор производителя устройства.
number of message changes	Когда определенные значения в сообщении информации изменяются, добавляется 1

8.3.5 Статус события

Эта страница позволяет пользователям просматривать текущие подробности событий передачи OAM по ссылке, как показано на рисунке ниже.

Detailed Link OAM Link Status for G1 G1 Auto-refresh Refresh

Local Frame Error Status		Remote Frame Error Status	
Frame Error Event Timestamp	0	Frame Error Event Timestamp	0
Frame Error Event Window	0	Frame Error Event Window	0
Frame Error Event Threshold	0	Frame Error Event Threshold	0
Frame Errors	0	Frame Errors	0
Total Frame Errors	0	Total Frame Errors	0
Total Frame Error Events	0	Total Frame Error Events	0
Local Frame Period Status		Remote Frame Period Status	
Frame Period Error Event Timestamp	-	Frame Period Error Event Timestamp	0
Frame Period Error Event Window	-	Frame Period Error Event Window	0
Frame Period Error Event Threshold	-	Frame Period Error Event Threshold	0
Frame Period Errors	-	Frame Period Errors	0
Total Frame Period Errors	-	Total Frame Period Errors	0
Total Frame Period Error Events	-	Total Frame Period Error Events	0
Local Symbol Period Status		RemoteSymbolPeriodStatus	
Symbol Period Error Event Timestamp	0	Symbol Period Error Event Timestamp	0
Symbol Period Error Event Window	0	Symbol Period Error Event Window	0

Описание каждого параметра представлено в следующей таблице:

Параметр	Описание
error frame event	Одно из событий ошибки связи, поддерживаемых мониторингом OAM по ссылке.
bad symbol cycle event	Одно из событий ошибки связи, поддерживаемых мониторингом OAM по ссылке.
error frame period event	Одно из событий ошибки связи, поддерживаемых мониторингом OAM по ссылке. LinkOAM не поддерживает отправку событий периода ошибок кадров.
error frame seconds summary event	Одно из событий ошибки связи, поддерживаемых мониторингом OAM по ссылке.
timestamp	Отметка времени возникновения события. Временная метка представляет собой относительное время после запуска системы. Единица времени - (секунды * 100), диапазон от 0 до 65535.
window	Временное окно для наблюдения за событиями.
threshold	Порог возникновения события в течение окна наблюдения.
number of errors	Записать количество ошибок, которые привели к последнему уведомлению о событии ошибки.
total number of errors	Записать количество ошибок.
total number of error events	Количество записанных событий ошибки

8.3.6 MIB поиск

Эта страница позволяет пользователю извлекать объекты MIB, как показано на изображении ниже.

Link OAM MIB Retrieval

Local ☒ (Local refers to the local information stored on the remote device)

Peer ☐ (Peer refers to the peer information stored on the remote device)

G1 ▾

Start

Описание каждого параметра представлено в следующей таблице:

Параметр	Описание
local end	MIB извлекает локальную информацию о состоянии OAM, хранящуюся на отвечающем устройстве.
peer	MIB извлекает удаленную информацию о состоянии OAM, хранящуюся на отвечающем устройстве

Объяснение поля поиска в MIB:

Результаты поиска локальных объектов MIB:

Структура пакета	Описание
branch: Attribute (0x07)	Ветвь: Свойства
leaf: aOAMID (0x00ec)	Номер локального порта начинается с 0
leaf: aOAMLocalConfiguration (0x014e)	Конфигурация локального OAM. (Следующие биты конфигурации отображаются от младшего к старшему) Биты 0-4: <ul style="list-style-type: none"> • Режим работы • Поддержка односторонней отправки • Ответ на удаленный циклический обход • Поддержка мониторинга соединения • Поддержка извлечения MIB
leaf: aOAMLocalPDUPConfiguration	Максимальная длина OAMPDU в локальной

Структура пакета	Описание
(0x014f)	конфигурации.
Leaf: aOAMLocalRevision (0x0150)	Количество изменений локальных пакетов
leaf: aOAMLocalState (0x0151)	<p>Состояние локального OAM.</p> <p>Биты 1-0:</p> <ul style="list-style-type: none"> 0x00: разбор и пересылка 0x01: разбор и циклический обход 0x03: разбор и отбрасывание <p>Бит 2:</p> <ul style="list-style-type: none"> 0x0: пересылка 0x1: отбрасывание

Результаты поиска MIB на партнере

Структура пакета	Описание
branch: Attribute (0x07)	Ветвь: Свойства
leaf: aOAMRemoteConfiguration (0x00f0)	<p>Конфигурация OAM партнера</p> <p>Биты 0-4:</p> <ul style="list-style-type: none"> Режим работы Поддержка односторонней отправки Ответ на удаленный циклический обход Поддержка мониторинга соединения Поддержка извлечения MIB
leaf: aOAMRemotePDUPConfiguration (0x00f1)	Максимальная длина OAMPDU в конфигурации партнера.
leaf: aOAMRemoteRevision (0x00f4)	Количество изменений в сообщениях партнера
leaf: aOAMRemoteState (0x00f5)	<p>Статус OAM партнера:</p> <p>Биты 1-0:</p> <ul style="list-style-type: none"> 0x00: разбор и пересылка 0x01: разбор и циклический обход

Структура пакета	Описание
	<ul style="list-style-type: none"> 0x03: разбор и отбрасывание <p>Бит 2:</p> <ul style="list-style-type: none"> 0x0: пересылка 0x1: отбрасывание

8.4 CFM

CFM (Connectivity Fault Management) следует стандарту IEEE802.1ag и представляет собой технологию OAM (управление доступом к объектам) для обнаружения связности от конца к концу на уровне VLAN в сети Layer 2.

8.4.1 Глобальная конфигурация

Страница глобальной конфигурации CFM. Как показано ниже.

Описание каждого параметра представлено в следующей таблице:

Параметр	Описание
sender ID TLV	<ul style="list-style-type: none"> None: Не отправлять TLV идентификатора отправителя; Chassis: Использовать MAC-адрес для создания TLV; Manage: Использовать IP-адрес для создания TLV; ChassisManage: Использовать MAC-адрес + IP-адрес для создания TLV;
port status TLV	<ul style="list-style-type: none"> Включить: Включить отправку TLV состояния порта; Отключить: Отключить отправку TLV состояния порта;
interface status TLV	<ul style="list-style-type: none"> Включить: Включить отправку TLV состояния интерфейса;

Параметр	Описание
	<ul style="list-style-type: none"> Отключить: Отключить отправку TLV состояния интерфейса;
manufacturer characteristics TLV	<ul style="list-style-type: none"> Включить: Включить передачу TLV характеристики производителя; Отключить: Отключить отправку TLV характеристики производителя;
manufacturer characteristics TLV manufacturer unique ID	Укажите значение OUI (Organizational Unique Identifier) для характеристического TLV производителя.
vendor characteristic TLV subtype	Укажите подтип характеристического TLV производителя.
manufacturer characteristic TLV value	Укажите значение характеристического TLV производителя.

8.4.2 Конфигурация домена обслуживания

На странице конфигурации домена обслуживания CFM отображена визуализация, как показано на рисунке ниже.

Домен обслуживания представляет собой диапазон тестирования обнаружения связности, указанный серией узлов обслуживания. Пакеты обнаружения в домене обслуживания имеют уровни 0-7, которые также являются уровнями всех терминалов обслуживания в домене.

Описание каждого параметра представлено в следующей таблице:

Параметр	Описание
maintenance domain	Настройка ключевых слов для сущностей домена обслуживания в локальных поисках.
format/name	Тег идентификации в сообщении протокола CFM должен иметь тот же формат/название в одном и том же домене обслуживания.
grade	В протоколе CFM уровень оборудования узла обслуживания в домене обслуживания.

Параметр	Описание
TLV options	Переключатель для отправки дополнительных TLV в домене обслуживания. Если выбрано "отложить", это означает использование глобальной конфигурации.



Описание:

- Домены обслуживания CFM могут быть вложенными или смежными, но не могут пересекаться.
- Когда домен обслуживания включает только узлы на обоих концах прямой связи, рекомендуется установить уровень домена обслуживания на уровне 0.

8.4.3 Конфигурация служб

На странице конфигурации служб CFM отображается визуализация, как показано на рисунке ниже.

CFM Service Configuration Refresh

Delete	MD	Service	Format	Name	VLAN	CCM Interval	TLV Option Select			
							Sender ID	Port Status	Interface Status	Org. Specific
<div style="border: 1px solid #ccc; height: 20px; margin-bottom: 5px;"></div>										

Add Entry

Save Reset

Служба представляет собой набор терминалов обслуживания в домене обслуживания, разделенных на основе определенных услуг, таких как VLAN.

Описание каждого параметра представлено в следующей таблице:

Параметр	Описание
maintain domain/service	Используйте [Домен обслуживания: Служба] локально для извлечения и конфигурации сущности службы.
format/name	Тег идентификации в сообщении протокола CFM должен иметь тот же формат/название в одной и той же службе
VLAN	Служба может привязать VLAN к терминалу обслуживания, к которому она принадлежит. Значение означает: <ul style="list-style-type: none"> • 0: Служба не привязана к VLAN; • 1-4095: Служба привязана к определенному идентификатору VLAN

Параметр	Описание
continuity detection packet sending interval	<p>Интервал периодической отправки сообщений о проверке непрерывности из терминала обслуживания поддерживает следующие конфигурации:</p> <ul style="list-style-type: none"> • 300 Гц: 3.3 мс • 10 мс • 100 мс • 1 с • 10 с <p>Если терминал обслуживания не получает сообщение о проверке непрерывности от партнера в течение 3.5 циклов, считается, что соединение неработоспособно. Интервал отправки пакетов по умолчанию составляет 1 секунду.</p>
TLV options	<p>Переключатель для отправки дополнительных TLV в рамках службы. Если выбрана опция "отложить", это означает использование глобальной конфигурации.</p>

Описание:

- Служба, домен обслуживания и глобальная конфигурация могут все включить функцию отправки дополнительных TLV. В терминах приоритета управления: Служба > Домен обслуживания > Глобальная конфигурация.
- Формат ICC Y1731 в службе, формат ICC CC Y1731 должен быть настроен, когда формат домена обслуживания равен "нет".
- В службе, привязанной к VLAN, терминал обслуживания называется VLAN MEP. В службе, не привязанной к VLAN, терминал обслуживания называется Port MEP. Port MEP обычно настраивается на прямой связи для мониторинга статуса одноразового канала, и на одном физическом порте одновременно может быть включен только один Port MEP.

8.4.4 Конфигурация терминала обслуживания

Страница конфигурации терминала обслуживания CFM, как показано на рисунке ниже.

CFM Maintenance association End Point Configuration Refresh

Delete	MD	Service	MEPID	Direction	Port	VLAN	PCP	SMAC	Alarm Control			State Control		Remote MEPID
									Level	Present	Absent	CCM	Admin	
*														

Add Entry

Save Reset

Терминал обслуживания определяет область домена обслуживания и получает конфигурации, такие как уровень, VLAN и интервал отправки пакетов, из домена обслуживания и службы, к которым он принадлежит. Терминал обслуживания должен быть настроен вручную на порту устройства, и поддерживается только один удаленный узел.

Описание каждого параметра представлено в следующей таблице:

Параметр	Описание
maintain domain/service	Локальная идентификация указывает на домен обслуживания и службу, к которым принадлежит терминал обслуживания.
maintain terminal ID	Он идентифицирует сущность терминала обслуживания в домене обслуживания и должен быть уникален в службе
direction	<p>Идентифицирует направление, в котором терминал обслуживания отправляет протокольные сообщения.</p> <ul style="list-style-type: none"> Вверх: Не отправляет протокольные пакеты с порта, на котором он находится, а отправляет пакеты на другие порты устройства. Вниз: Отправляет пакеты только на порт, на котором он находится. <p>Терминал обслуживания поддерживает только направление Вниз..</p>
port	Настройте номер порта MEP на устройстве
VLAN	<p>Вы можете привязать VLAN к терминалу обслуживания. После привязки VLAN все пакеты, отправляемые терминалом обслуживания в службе, могут нести тег. Значение означает:</p> <ul style="list-style-type: none"> 0: Терминал обслуживания не привязан к VLAN; 1-4095: Привязать терминал обслуживания к определенному идентификатору VLAN
PCP	Приоритет PCP, диапазон от 0 до 7.
source MAC address	MAC-адрес источника пакетов проверки непрерывности CFM, отправляемых портом. Если не настроено, будет автоматически сгенерирован системой
activation level	<p>Уровень активации относится к самому низкому уровню тревоги, которая может быть сгенерирована.</p> <p>У CFM есть следующие тревоги:</p>

Параметр	Описание
	<ul style="list-style-type: none"> • RDICCM: Ошибка в удаленном терминале обслуживания. Уровень тревоги 1. • MACstatus: Состояние порта или интерфейса удаленного терминала обслуживания аномально. Уровень тревоги 2. • RemoteCCM: Удаленный терминал обслуживания не получил действительное сообщение о проверке непрерывности. Уровень тревоги 3. • ErrorCCM: Идентификатор терминала обслуживания в сообщении о проверке непрерывности аномальный или интервал отправки пакета не соответствует. Уровень тревоги 4. • XconCCM: Получены сообщения о проверке непрерывности, отправленные различными терминалами в домене обслуживания. Уровень тревоги 5. <p>По умолчанию уровень тревоги составляет 2. При настройке уровня тревоги как 1 все тревоги разрешены для генерации. При настройке уровня тревоги как 6 ни одна тревога не разрешена для генерации</p>
generate anti-shake time	Время ожидания, когда терминал обслуживания обнаруживает сбой в связи. В течение времени ожидания, если сбой устраняется, терминал обслуживания не генерирует тревогу. Если сбой не устранен, соответствующая тревога генерируется по истечении времени ожидания.
restore anti-shake time	Когда терминал обслуживания генерирует тревогу, время ожидания восстановления тревоги. В течение времени ожидания, если тревога восстанавливается, терминал сообщает, что тревога была восстановлена после истечения времени ожидания. В течение времени ожидания терминал продолжает генерировать тревоги только при обнаружении более высокого уровня сбоя, а тревоги более низкого уровня игнорируются.
continuity check enabled	Переключатель функции проверки непрерывности связи
CFM enable	Переключатель включения функции CFM терминала обслуживания
remote maintenance terminal ID	<p>Идентификатор удаленного терминала обслуживания, соответствующий терминалу обслуживания. Существует следующая конфигурация:</p> <ul style="list-style-type: none"> • 0: Терминал обслуживания не привязан к удаленному терминалу обслуживания. • 1-8191: Терминал обслуживания привязан к идентификатору удаленного терминала обслуживания



Описание:

- Оба VLAN MEP и Port MEP могут устанавливать атрибуты VLAN в конфигурации MEP, и они могут отличаться от атрибутов VLAN сервиса, к которому они принадлежат. CFM предпочтительно использует атрибуты VLAN в конфигурации MEP и помещает соответствующий тег VLAN в пакет CCM.
- Носит ли пакеты CCM, отправляемые портом CFM, теги VLAN, зависит от типа MEP и атрибутов VLAN порта. После того как CFM настроен для привязки VLAN в конфигурации сервиса или терминала обслуживания, VLAN порта должен быть настроен для поддержки прохода пакетов с тегами VLAN.
- На одном физическом порте разрешено включение только одного Port MEP.
- На том же порту и в той же VLAN разрешено только одно VLAN MEP. Включенный VLAN MEP должен иметь более высокий уровень обслуживания домена, чем Port MEP.
- Удаленный MEP должен иметь то же имя обслуживания домена, уровень обслуживания домена, имя сервиса, интервал пакетов и домен VLAN, что и локальный, чтобы быть признанным локально. MEP должен быть привязан к идентификатору удаленного терминала обслуживания, чтобы функция проверки непрерывности могла работать.
- Когда MAC-адрес источника не настроен, система генерирует виртуальный адрес в качестве источника MAC-адреса пакета. При ручной настройке MAC-адреса источника следует быть осторожным, чтобы не допустить повторного появления исходного MAC-адреса в сети.
- Переключатель включения CFM контролирует открытие и закрытие протокола CFM на порту; переключатель включения проверки непрерывности контроля контролирует, отправляет ли порт сообщения CCM. Когда CFM включен и проверка непрерывности отключена, CFM все равно может получать сообщения CCM и генерировать тревоги.

8.4.5 Статус терминала обслуживания

Эта страница позволяет пользователям просматривать подробную информацию о текущем состоянии терминала обслуживания, как показано на изображении ниже.

CFM Maintenance Association End Point Status

Auto-refresh ☐ Refresh

MD	Service	MEPID	Port	State		SMAC	Defects		CCM Rx			CCM Tx
				Active	Fng		Highest	Defects	Valid	Invalid	Errors	

Описание каждого параметра представлено в следующей таблице:

Параметр	Описание
operating status	Отображает текущий статус работы МЕР (Maintenance Endpoint) - терминала обслуживания
fault status	Статус неисправности определяется следующим образом: <ul style="list-style-type: none"> • Reset: Сброс тревоги. • Defect: Тревога сгенерирована, и происходит антидребезговая задержка. • reportDefect: Отчет о тревоге. • defectReported: Неисправность продолжается. • defectClearing: Происходит антидребезговая задержка восстановления тревоги. Любые неисправности, не скрытые уровнем неисправности МЕР, будут вызывать срабатывание тревоги
superlative	Показать только дефекты самого высокого уровня
detailed defects	Дефекты представлены следующими аббревиатурами: <ul style="list-style-type: none"> • -: Нет дефектов • R: RDICCM • M: MACstatus • C: RemoteCCM • E: ErrorCCM • X: XconCCM
valid frame	Количество полученных действительных сообщений о проверке непрерывности.
invalid frame	Количество полученных недействительных сообщений о проверке непрерывности.
error frame	Количество полученных сообщений о проверке непрерывности с ошибкой последовательного номера



Описание:

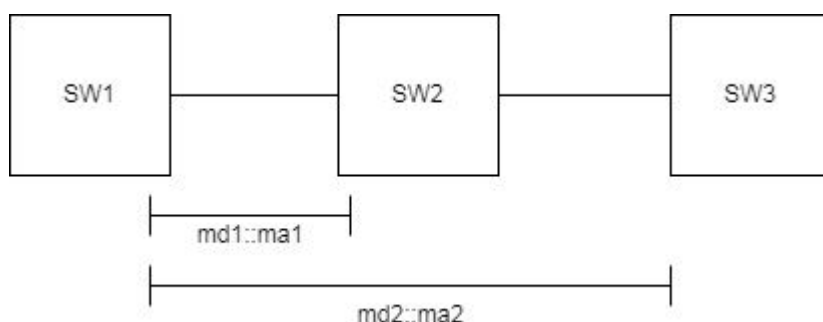
- Когда операционный статус МЕР аномальный, вы можете навести курсор мыши, чтобы просмотреть описание и подтвердить, вызвано ли это конфигурацией. Прежде всего необходимо решить проблемы локальной конфигурации.
- Если МЕР обнаруживает дефект низкого уровня во время времени восстановления

высокоуровневой тревоги, он не отменяет высокоуровневую тревогу. Вместо этого он продолжает отображать статус высокоуровневой тревоги до тех пор, пока все дефекты низкого уровня не исчезнут.

8.4.6 Примеры типичной конфигурации CFM

Цель конфигурации:

Настроить два соединения CFM между SW1, SW2 и SW3. Настроить Port MEP на основе md1::ma1 между SW1 и SW2, а также настроить VLAN MEP на основе md2::ma2 между SW1 и SW3. В конечном итоге CFM может отслеживать статус коммуникации между SW1-SW2 и между SW1-SW2-SW3.



8.4.6.1 Конфигурация CFM для прямой связи SW1-SW2

Step 1. Настроить обслуживающий домен md1 для SW1 и SW2.

CFM Maintenance Domain Configuration

Delete	MD	Format	Name	Level	TLV Option Select			
					Sender ID	Port Status	Interface Status	Org. Specific
*		<>		<>	<>	<>	<>	<>
<input type="checkbox"/>	md1	String	md1	0	Defer	Defer	Defer	Defer

Настроить обслуживающий домен md1 на обоих SW1 и SW2, и уровень обслуживающего домена равен 0.

Step 2. Настройте ma1 с атрибутом VLAN 0 на SW1 и SW2.

CFM Service Configuration

Delete	MD	Service	Format	Name	VLAN	CCM Interval	TLV Option Select			
							Sender ID	Port Status	Interface Status	Org. Specific
*			<>			<>	<>	<>	<>	<>
<input type="checkbox"/>	md1	ma1	String	ma1	0	1 sec	Defer	Defer	Defer	Defer

Step 3. Настройте соответствующие портовые MEP на порту 1 SW1 и порту 1 SW2.

Удаленный идентификатор обслуживания - это идентификатор обслуживания другой стороны.

SW1:

CFM Maintenance association End Point Configuration Refresh

Delete	MD	Service	MEPID	Direction	Port	VLAN	PCP	SMAC	Alarm Control			State Control		Remote MEPID
									Level	Present	Absent	CCM	Admin	
*														
<input type="checkbox"/>	md1	ma1	1	Down	G1	0	0	00:00:00:00:00:00	2	2500	10000	<input checked="" type="checkbox"/>	<input type="checkbox"/>	2

Add Entry

Save Reset

SW2:

CFM Maintenance association End Point Configuration Refresh

Delete	MD	Service	MEPID	Direction	Port	VLAN	PCP	SMAC	Alarm Control			State Control		Remote MEPID
									Level	Present	Absent	CCM	Admin	
*												<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	md1	ma1	2	Down	G1	0	0	00:00:00:00:00:00	2	2500	10000	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	1

Add Entry

Save Reset

Step 4. Снимок экрана статуса MEP SW2 представлен ниже:

CFM Maintenance association End Point Configuration Refresh

Delete	MD	Service	MEPID	Direction	Port	VLAN	PCP	SMAC	Alarm Control			State Control		Remote MEPID
									Level	Present	Absent	CCM	Admin	
*												<input type="checkbox"/>	<input type="checkbox"/>	
<input type="checkbox"/>	md1	ma1	1	Down	G1	0	0	00:00:00:00:00:00	2	2500	10000	<input checked="" type="checkbox"/>	<input type="checkbox"/>	2

Add Entry

Save Reset

Конфигурация CFM на связи SW1-SW2 завершена. Проверьте статус CFM на SW2. MEP не имеет неисправностей, и количество отправленных и полученных пакетов нормальное.

8.4.6.2 Конфигурация CFM для связи SW1-SW2-SW3

на SW1 и SW3, и установите атрибут VLAN на 100. Атрибуты VLAN портов должны быть настроены между SW1-SW2-SW3, чтобы разрешить прохождение пакетов с тегом VLAN100.

Step 1. Настройте атрибуты порта VLAN на SW2 и установите режим порта на Trunk.

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
*	<>		<>	<input type="checkbox"/>	<>	<>		
G1	Trunk	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag Port VLAN	1-4095	
G2	Trunk	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag Port VLAN	1-4095	
G3	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag All	1	
G4	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag All	1	

Step 2. Настройте обслуживаемый домен md2 на SW1, и уровень обслуживаемого домена равен 7.

<input type="checkbox"/>	md2	String	md2	7	Defer	Defer	Defer	Defer
--------------------------	-----	--------	-----	---	-------	-------	-------	-------

Step 3. Настройте сервис ma2 на SW1, и атрибут VLAN равен 100.

<input type="checkbox"/>	md2	ma2	String	ma2	100	1 sec	Defer	Defer	Defer	Defer
--------------------------	-----	-----	--------	-----	-----	-------	-------	-------	-------	-------

Step 4. Настройте MEP на SW1.

<input type="checkbox"/>	md2	ma2	3	Down	G1	0	0	00:00:00:00:00:00	2	2500	10000	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	4
--------------------------	-----	-----	---	------	----	---	---	-------------------	---	------	-------	-------------------------------------	-------------------------------------	---

Step 5. Настройка обслуживаемого домена и сервиса на SW3 аналогична SW1, а конфигурация MEP выглядит следующим образом:

CFM Maintenance association End Point Configuration

Delete	MD	Service	MEPID	Direction	Port	VLAN	PCP	SMAC	Alarm Control			State Control		Remote MEPID
									Level	Present	Absent	CCM	Admin	
*				<>	<>		<>		<>			<input type="checkbox"/>	<input type="checkbox"/>	
<input type="checkbox"/>	md2	md2	4	Down	G1	0	0	00:00:00:00:00:00	2	2500	10000	<input checked="" type="checkbox"/>	<input type="checkbox"/>	0

Add Entry

Save Reset

Step 6. Скриншот статуса MEP на SW1 выглядит следующим образом.

CFM Maintenance Association End Point Status

MD	Service	MEPID	Port	State		SMAC	Defects		CCM Rx			CCM Tx
				Active	Fng		Highest	Defects	Valid	Invalid	Errors	
md2	md2	4	G1		reset	00:00:00:0A:11:23	none	- - - -	0	0	0	0

SW1 может одновременно контролировать статус CFM двух ссылок.

8.5 UDLD

UDLD (UNIDirectional Link Detection) - это частный протокол уровня 2 от Cisco, используемый для мониторинга Ethernet-связей, установленных с помощью оптических волокон и скрученных пар проводов. Когда происходит односторонняя связь (данные могут передаваться только в одном направлении), UDLD может обнаружить эту ситуацию и обработать соответствующий порт. Односторонние связи могут вызывать множество проблем, особенно в структуре Spanning Tree, что может приводить к появлению петель.



Примечания:

Для нормального обнаружения односторонних связей функция UDLD должна быть включена на обоих концах связи, которые нужно проверить.

8.5.1 UDLD конфигурация

Страница конфигурации UDLD показана на рисунке ниже.

UDLD Port Configuration

Port	UDLD Mode	Message Interval
*	<> ▾	<input type="text"/>
G1	Disable ▾	7 <input type="text"/>
G2	Disable ▾	7 <input type="text"/>
G3	Disable ▾	7 <input type="text"/>
G4	Disable ▾	7 <input type="text"/>
G5	Disable ▾	7 <input type="text"/>
G6	Disable ▾	7 <input type="text"/>
G7	Disable ▾	7 <input type="text"/>
G8	Disable ▾	7 <input type="text"/>
G9	Disable ▾	7 <input type="text"/>
G10	Disable ▾	7 <input type="text"/>
G11	Disable ▾	7 <input type="text"/>
G12	Disable ▾	7 <input type="text"/>
G13	Disable ▾	7 <input type="text"/>
G14	Disable ▾	7 <input type="text"/>

Описание каждого параметра представлено в следующей таблице:

Параметр	Описание
UDLD port configuration	Настройка режима работы порта
port	Номер порта устройства

Параметр	Описание
model	<p>Дополнительные параметры: отключено/обычное/агрессивное:</p> <ul style="list-style-type: none"> Отключено: указывает на отключение функции UDLD порта. Обычное: после настройки этого режима, когда обнаруживается статус однонаправленной ссылки, будет сообщаться только информация о статусе однонаправленной ссылки, а статус работы порта не будет изменен. Агрессивное: после настройки этого режима, порт будет отключен при обнаружении статуса однонаправленной ссылки. <p>После отключения порта в агрессивном режиме его можно восстановить только отключением функции UDLD</p>
message interval	<p>Настройте интервал времени для отправки сообщений-запросов UDLD. Диапазон конфигурации составляет от 7 до 90 секунд, а значение по умолчанию — 7 секунд.</p>

8.5.2 UDLD статус

На странице статуса UDLD вы можете просмотреть связанную с UDLD информацию о порту, включая состояние локального порта устройства, идентификатор устройства, имя устройства и состояние соединения, а также номер порта подключенного соседнего устройства, идентификатор устройства, состояние соединения и имя устройства. Как показано ниже.

Detailed UDLD Status for G1

G1

UDLD Status	
UDLD Admin State	Disable
Device ID(local)	00:00:00:0A:11:22
Device Name(local)	-
Bidirectional State	Indeterminant

Neighbor Status

Port	Device ID	Link Status	Device Name
No Neighbor ports enabled or no existing partners			

Описание каждого параметра представлено в следующей таблице:

Параметр	Описание
UDLD status	Статус UDLD локального порта
port status	<p>Отображает текущий статус работы UDLD для данного порта, который может быть отображен следующим образом:</p> <ul style="list-style-type: none"> Включен: указывает, что текущий режим работы порта находится в нормальном режиме или агрессивном режиме. Отключен: указывает, что функция UDLD для текущего порта отключена.
device ID (local)	Адрес MAC локального устройства.
device name (local)	Имя локального устройства
connection Status	<p>Текущий статус соединения может быть отображен следующим образом:</p> <ul style="list-style-type: none"> Loopback: указывает на то, что текущее соединение находится в состоянии обратной связи. Bi-directional: указывает на то, что текущее соединение находится в состоянии двунаправленной связи, то есть в нормальном рабочем состоянии. Uni-directional: указывает на то, что текущее соединение находится в состоянии однонаправленного соединения. Multiple neighbors connected: указывает на то, что текущее соединение имеет несколько подключенных соседних устройств. Indeterminant: указывает на то, что текущее соединение находится в неопределенном состоянии.
neighbor status	Текущий статус соединения с соседними устройствами может быть отображен следующим образом:
port	Номер порта соседнего устройства
device ID	MAC-адрес соседнего устройства
connection status	Текущий статус соединения
device name	Имя соседнего устройства

8.6 Линейная диагностика

Линейная диагностика позволяет пользователю определить текущее состояние кабеля, соединяющего интерфейс Ethernet на устройстве. Содержание диагностики включает в себя наличие короткого замыкания или обрыва в кабеле, а также длину поврежденного кабеля.

VeriPHY Cable Diagnostics

Port

Start

Cable Status								
Port	Pair A	Length A(m)	Pair B	Length B(m)	Pair C	Length C(m)	Pair D	Length D(m)
G1	--	--	--	--	--	--	--	--
G2	--	--	--	--	--	--	--	--
G3	--	--	--	--	--	--	--	--
G4	--	--	--	--	--	--	--	--
G5	--	--	--	--	--	--	--	--
G6	--	--	--	--	--	--	--	--
G7	--	--	--	--	--	--	--	--
G8	--	--	--	--	--	--	--	--

Описание каждого параметра представлено в следующей таблице:

Параметр	Описание
port	Обнаружение порта. Выберите один порт для обнаружения выбранного порта; выберите все, чтобы обнаружить все порты.
line pair	A/B/C/D пары проводов могут быть протестированы одновременно. <ul style="list-style-type: none"> А пара проводов: оранжевая/бело-оранжевая В пара проводов: зеленая/бело-зеленая С пара проводов: синяя/бело-синяя Д пара проводов: коричневая/бело-коричневая
state	Результаты теста следующие: <ul style="list-style-type: none"> Норма: указывает на отсутствие неисправности в линии и нормальное соединение. Обрыв: указывает на разрыв в линии. Короткое замыкание: указывает на короткое замыкание в линии.

Параметр	Описание
	<ul style="list-style-type: none"> Ненормально: указывает на другие неисправности, такие как неправильная последовательность линий. --: указывает на то, что статус неизвестен или статус не был получен и требуется обновление.
pair length	<p>Расстояние между точкой неисправности на линии и портом. Диапазон длины тестируемой линии: от 7 до 120 метров, с точностью до 5 метров.</p> <p>Примечание:</p> <p>Результаты теста за пределами указанного диапазона длины могут быть неточными</p>



Описание:

- Оптические порты (включая оптические модули) не поддерживают диагностику линии.
- Соединение будет прервано во время проведения диагностики и восстановится после завершения диагностики.
- Результаты диагностики могут незначительно отличаться в зависимости от количества портов. Для одного порта это занимает около 5 секунд, а для всех портов - от 10 до 30 секунд.
- Результаты этой функции диагностики не являются абсолютно точными и предназначены только для справки.

8.7 sFlow

sFlow система включает в себя sFlow агент, встроенный в устройство, и удаленный sFlowCollector. sFlow агент получает статистику интерфейса и информацию о данных через сэмплирование sFlow и инкапсулирует информацию в сообщения sFlow. Когда буфер сообщений sFlow заполняется или время кэширования сообщений sFlow истекает (время кэширования составляет 1 секунду), sFlow агент отправляет сообщения sFlow в указанный sFlowCollector. sFlowCollector анализирует сообщения sFlow и отображает результаты анализа.

8.7.1 sFlow конфигурация

Страница конфигурации sFlow. Как показано ниже.

8.7.1.1 Конфигурация агента

sFlow Configuration

Agent Configuration

IP Address 127.0.0.1

Refresh

Описание каждого параметра представлено в следующей таблице:

Параметр	Описание
IP address	Прокси-адрес sFlow не используется в качестве исходного IP-адреса для связи. Его можно настроить как любой IPv4 или IPv6 адрес и служит в качестве флага коммутатора в сообщении. Состояние по умолчанию - 127.0.0.1

8.7.1.2 Конфигурация приемника

Receiver Configuration

Owner	<none>	Release
IP Address/Hostname	0.0.0.0	
UDP Port	6343	
Timeout	0	Seconds
Max. Datagram Size	1400	bytes

Описание каждого параметра представлено в следующей таблице:

Параметр	Описание
freed	Очистить конфигурацию приемника и прекратить отправку сообщений sFlow.
owner	Владелец приемника — это организация или лицо, которое контролирует и управляет sFlow.
IP address/hostname	IP-адрес или имя хоста приемника sFlow. Для использования доменного имени необходимо сначала настроить DNS-сервер. Если хост не может быть найден на основе доменного имени, IP-адрес будет очищен. Это используется для указания устройства или приложения, которое будет получать данные sFlow.
UDP port	По умолчанию используется порт 6343
overtime time	sFlow мониторит время работы в реальном времени. Если оно превышает это время, отправка пакетов будет прекращена. Диапазон конфигурации составляет от 0 до 2147483647 секунд
maximum message length	Это относится к максимальному значению пакетов UDP в пакетах sFlow при настройке адреса типа IPV4. При настройке в качестве адреса IPV6 адрес занимает больше байт, чем адрес типа IPV4, поэтому размер данных пакета увеличится соответственно. Диапазон конфигурации составляет от 200 до 1468.

8.7.1.3 Конфигурация порта

Port Configuration

Port	Flow Sampler			Counter Poller	
	Enabled	Sampling Rate	Max. Header	Enabled	Interval
*	<input type="checkbox"/>			<input type="checkbox"/>	
G1	<input type="checkbox"/>	0	128	<input type="checkbox"/>	0
G2	<input type="checkbox"/>	0	128	<input type="checkbox"/>	0
G3	<input type="checkbox"/>	0	128	<input type="checkbox"/>	0
G4	<input type="checkbox"/>	0	128	<input type="checkbox"/>	0
G5	<input type="checkbox"/>	0	128	<input type="checkbox"/>	0
G6	<input type="checkbox"/>	0	128	<input type="checkbox"/>	0
G7	<input type="checkbox"/>	0	128	<input type="checkbox"/>	0
G8	<input type="checkbox"/>	0	128	<input type="checkbox"/>	0
G9	<input type="checkbox"/>	0	128	<input type="checkbox"/>	0
G10	<input type="checkbox"/>	0	128	<input type="checkbox"/>	0
G11	<input type="checkbox"/>	0	128	<input type="checkbox"/>	0
G12	<input type="checkbox"/>	0	128	<input type="checkbox"/>	0

Описание каждого параметра представлено в следующей таблице:

Параметр	Описание
port	Номер порта.
enable	Указывает, включен ли сэмплер потока.
sampling rate	Пропорция трафиков, фактически отобранных в указанный временной интервал. Например, конфигурация 100 означает, что 100 пакетов отбираются один раз. Диапазон конфигурации составляет от 0 до 32767, а значение по умолчанию равно 0, что означает отсутствие отбора. Пороговое значение отбора sFlow составляет 500pps. Пожалуйста, настройте соответствующий интервал в соответствии с трафиком.
maximum packet header	Максимально допустимый размер заголовка пакета. Диапазон конфигурации составляет от 14 до 200.
enable	Указывает, включен ли опросный сэмплер.
polling interval	Временной интервал, в течение которого происходит сбор выборок счетчика. Диапазон конфигурации составляет от 0 до 3600 секунд

8.7.2 sFlow статистика

Страница статистики sFlow показана на рисунке ниже.

sFlow Statistics

Receiver Statistics

Owner	<none>
IP Address/Hostname	0.0.0.0
Timeout	0
Tx Successes	0
Tx Errors	0
Flow Samples	0
Counter Samples	0

Port Statistics

Port	Flow Samples	Counter Samples
G1	0	0
G2	0	0
G3	0	0
G4	0	0
G5	0	0
G6	0	0
G7	0	0

Auto-refresh ☐ Refresh Clear Receiver Clear Ports

Описание каждого параметра представлено в следующей таблице:

Параметр	Описание
clear receiver	Очистить статистику приемника
clear port	Очистить статистику на порту
owner	Владелец приемника — это сущность или частное лицо, которое контролирует и управляет sFlow.
IP address/hostname	Представляет собой IP-адрес или имя хоста приемника sFlow. Используется для указания устройства или приложения, которое будет получать данные sFlow.
overtime time	Время, в течение которого данные sFlow сохраняются на приемнике, после чего они будут очищены.
number of successfully transmitted packets	Количество успешно отправленных пакетов передачи sFlow.
number of transmission error packets	Количество ошибок передачи sFlow, возникших во время отправки.
number of flow samples	Общее количество сгенерированных образцов потока. Образцы потока — это трафиковые данные, захваченные sFlow на сетевых устройствах и используемые для анализа характеристик и поведения сетевого трафика.
counter samples	Общее количество сгенерированных образцов счетчика. Образцы счетчика используются для записи различных статистических данных сетевых устройств, таких как трафик, ошибки и потеря

Параметр	Описание
	пакетов и т. д.
port	Номер порта
number of flow samples	Количество образцов потока, сгенерированных на порту. Образцы потока — это трафиковые данные, захваченные sFlow на сетевых устройствах и используемые для анализа характеристик и поведения сетевого трафика.
counter samples	Количество образцов счетчика, сгенерированных на порту. Образцы счетчика используются для записи различных статистических данных сетевых устройств, таких как трафик, ошибки и потеря пакетов и т. д.

8.8 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.

8.8.1 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 ranger 0-255)
Packet Count	<input type="text" value="5"/>	packets
TTL Value	<input type="text" value="64"/>	
VID for Source Interface	<input type="text"/>	(Optional)
Source Port Number	<input type="text" value="None"/>	(Optional)
IP Address for Source Interface	<input type="text"/>	(Optional)
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.
Packet data	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 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.



Примечания:

- Информацию, которую необходимо заполнить, включает IP-адрес или доменное имя, размер пакета, заполнение данных, количество пакетов и значение TTL.
- Требуется настройка только одного или ни одного из следующих параметров: VID исходного порта, номера исходного порта и IP-адреса источника.
- При указании IP-адреса источника через VLAN ID исходного порта убедитесь, что адрес назначения находится в том же сегменте сети, что и IP-адрес этого интерфейса VLAN.

8.8.2 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 ranger 0-255)
Packet Count	<input type="text" value="5"/>	packets
VID for Source Interface	<input type="text"/>	(Optional)
Source Port Number	<input type="text" value="None"/>	(Optional)
IP Address for Source Interface	<input type="text"/>	(Optional)
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.
Packet data	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.
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.



Примечания:

- Информацию, которую необходимо заполнить, включает IP-адрес или доменное имя, размер пакета, данные заполнения и количество пакетов.
- Необходимо настроить только один или ни один из следующих параметров: VID исходного порта, номер исходного порта и IP-адрес источника.

8.9 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.

8.9.1 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="5"/>	seconds
First TTL Value	<input type="text" value="1"/>	
Max TTL Value	<input type="text" value="30"/>	
VID for Source Interface	<input type="text"/>	(Optional)
IP Address for Source Interface	<input type="text"/>	(Optional)
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	Определите количество проб (пакетов), отправляемых на

Параметр	Описание
per hop	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.



Примечания:

- Необходимая информация включает в себя IP-адрес или доменное имя, значение DSCP, количество попыток для каждого перехода, время ожидания ответа, значение TTL для первого перехода и максимальное значение TTL.
- Значение TTL для первого перехода должно быть меньше, чем максимальное значение TTL.

8.9.2 Traceroute (IPv6)

Настройка страницы информации Traceroute (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 ranger 0-255)
Packet Count	<input type="text" value="5"/>	packets
VID for Source Interface	<input type="text"/>	(Optional)
Source Port Number	<input type="text" value="None"/>	(Optional)
IP Address for Source Interface	<input type="text"/>	(Optional)
Quiet (only print result)	<input type="checkbox"/>	
<input type="button" value="Start"/>		

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.

**Примечания:**

Необходимая информация включает в себя IP-адрес или доменное имя, значение DSCP, количество попыток для каждого перехода, время ожидания ответа и максимальное значение TTL.

8.10 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..

BMC алгоритм

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

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

Набор данных, используемый алгоритмом BMC 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 RTP выполняет динамический алгоритм выбора источника ВМС, порядок приоритетного выбора определяется следующим образом: Приоритет1 > КлассЧасов > ТочностьЧасов > ОтклонениеШкалированнаяЛогВариация > 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 RTP, тем самым выбирая часовой сигнал, который они хотят синхронизировать. Алгоритм ВМС позволяет реализовать распределение и защиту синхронизации часов RTP.

Синхронизация частоты RTP:

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

RTP 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 RTP 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.

8.10.1 Мастер настройки PTP



Примечания:

- Для настройки функции синхронизации времени PTP веб-интерфейсом вам нужно лишь настроить необходимые параметры в соответствии с указанными шагами. Другие конфигурации не требуют изменений. Большая часть работы по установке значений по умолчанию уже выполнена, когда веб-интерфейс выбирает предустановленный файл.
- При добавлении источника времени PTP устройство может субъективно выбрать тип часов - мастер или рабочее, или выбрать общие часы, и выбрать мастерские и рабочие часы через алгоритм BMC (уровень часов, точность, приоритет и т. д.).

8.10.1.1 Настройка внешнего источника сигнала времени

Интерфейс отображения режима внешнего источника синхронизации.

PTP External Clock Mode

One_PPS_Mode	Output	▼
Adjust Method	Auto	▼

Описание каждого параметра представлено в следующей таблице:

Параметр	Описание
1PPS mode	Режим ввода и вывода сигнала импульса 1PPS.
Calibration	Режим калибровки: AUTO или LTC (локальный подсчет времени).

Параметр	Описание
method	

8.10.1.2 Настройка часов PTP

- 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 type="button" value="Delete"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	Ord-Bound ▾	1588 ▾

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.

Параметр	Описание
profile	Предустановленные файлы включают 1588 и 802.1AS. Параметры по умолчанию каждого предустановленного файла различаются. Выберите предустановленный файл в соответствии с фактическим применением.

- На интерфейсе отображения настройки часов РТР 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	1588	Apply	BASIC

Port Enable and Configuration

Port Enable																								Configuration						
G1	G2	G3	G4	G5	G6	G7	G8	G9	G10	G11	G12	G13	G14	G15	G16	G17	G18	G19	G20	G21	G22	G23	G24	X1	X2	X3	X4	X5	X6	Ports
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Configuration

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 РТР

- Интерфейс таблицы данных часов по умолчанию выглядит следующим образом:

Clock Parent DataSet

Parent Port ID	Port	PStat	Var	Rate	GrandMaster ID	GrandMaster Clock Quality	Pri1	Pri2
00:00:00:ff:fe:0a:11:22	0	False	0	0	00:00:00:ff:fe:0a:11:22	Cl:248 Ac:Unknwn Va:00000	128	128

Clock Default DataSet

Device Type	One-Way	2 Step Flag	Ports	Clock Identity	Dom	Clock Quality	
Ord-Bound	<div>False</div>	<div>False</div>	30	00:00:00:ff:fe:0a:11:22	<div>0</div>	Cl:248 Ac:Unknwn Va:00000	
Pri1	Pri2	Local Prio	Protocol			PCP	DSCP
<div>128</div>	<div>128</div>	<div>128</div>	<div>Ethernet</div>			<div>0</div>	<div>0</div>

Описание каждого параметра представлено в следующей таблице:

Параметр	Описание
One Way	Если вы выбираете значение true, то в данный момент устройство находится в режиме одноступенчатой синхронизации; если выбираете false, то в данный момент устройство находится в режиме двухступенчатой синхронизации.

Параметр	Описание
Two Steps	При выборе значения true, текущий режим — двухступенчатая синхронизация; при выборе значения false, текущий режим — одноступенчатая синхронизация.
Cock Domain	Домен программных часов, диапазон от 0 до 127.
Priority 1	Приоритет 1, участвует в выборе мастерского и рабочего часов, диапазон от 0 до 255.
Priority 2	Приоритет 2, участвует в выборе мастерского и рабочего часов, диапазон от 0 до 255.
Local Priority	Локальный приоритет, участвует в выборе мастерского и рабочего часов, диапазон от 0 до 255.
Agreement Type	Протокол сетевой передачи, Ethernet/EthernetMixed/IPV4Multi/IPv4Mixed/IPv4Uni/onePPS/EthIPv4IPv6combo.
PCP	Приоритет PCP, диапазон от 0 до 7.
DSCP	Приоритет DSCP, диапазон от 0 до 63



Примечания:

- Протокол 802.1AS не поддерживает модель E2eTransp/P2pTransp/mastronly/slaveonly.
- Протокол 802.1AS поддерживает только двухступенчатый режим.
- Протокол 802.1AS поддерживает только протокол Ethernet.
- Уникастный IPv4 не поддерживает механизм задержки точка-точка (p2p).
- Протокол 802.1AS настраивается с использованием VLAN, и необходимо настроить PVID порта, который совпадает с VLAN.

Интерфейс локальной синхронизации времени выглядит следующим образом:

Local Clock Current Time

PTP Time	Clock Adjustment method	Settings
1970-01-01T10:44:31+08:00 921,353,040	Internal Timer	Synchronize to System Clock Synchronized to System Clock

Описание каждого параметра представлено в следующей таблице:

Параметр	Описание
Synchronize system time	Синхронизировать системное время с PTP временем.
Synchronize to system time	Синхронизировать PTP время с системным временем. Поддерживается только синхронизация времени экземпляра часов 0



Примечания:

- После синхронизации РТР времени с системным временем, любые вручную внесенные изменения в системное время будут перезаписаны обновлением времени РТР. Чтобы вручную обновить системное время, необходимо сначала удалить часы РТР.
- Только режим `mastrOnly` протокола 1588 поддерживает синхронизацию системного времени, и протокол 802.1AS не имеет ограничений.

Интерфейс набора данных временных характеристик выглядит следующим образом:

Clock Time Properties DataSet

UtcOffset	Valid	leap59	leap61	Time Trac	Freq Trac	ptp Time Scale	Time Source
0	False	False	False	False	False	True	160
Leap Pending		Leap Date		Leap Type			
False		1970-01-01		leap61			

Описание каждого параметра представлено в следующей таблице:

Параметр	Описание
utc offset	Смещение UTC, диапазон 010000, значение по умолчанию 0
effectiveness	Смещение UTC, скорректированное по главным часам, значение по умолчанию False
leap59	Последняя минута високосной даты UTC составляет 59 секунд, значение по умолчанию False
leap61	Последняя минута високосной даты UTC составляет 61 секунду, значение по умолчанию False
time tracking	Время рабочих часов может быть отслежено по главным часам. Значение по умолчанию False.
frequency tracking	Частота рабочих часов может быть отслежена по главным часам. Значение по умолчанию False.
ptp time measurement	Измерение времени РТР использует эпоху как временную точку отсчета, значение по умолчанию True
time source	Значение, измеряющее уровень источника времени, диапазон 0255, значение по умолчанию 160
leap pending	Ожидание високосной секунды, значение по умолчанию False
leap date	Дата високоса, значение по умолчанию 1970-01-01
leap type	Тип високоса, значение по умолчанию leap61

4. Интерфейс текущего набора данных часов выглядит следующим образом:

Clock Current DataSet

stpRm	Offset From Master	Mean Path Delay
0	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
00:00:00:ff:fe:0a:11:22	0	False	0	0	00:00:00:ff:fe:0a:11:22	Cl:248 Ac:Unknwn Va:00000	128	128

Описание каждого параметра представлено в следующей таблице:

Параметр	Описание
wxua	Расстояние до главных часов
master clock bias	Отклонение от главных часов
average path delay	Когда E2E — это среднее время задержки между главными и рабочими часами, а P2P — среднее время задержки на конечной точке просмотра
parent clock ID	Идентификатор главных часов-родителей
P stat	Статус главных часов-родителей
variance	Дисперсия времени главных часов-родителей
rate	Частота главных часов-родителей
ancestor clock ID	Идентификатор предковых часов
ancestral clock quality	Качество предковых часов (ранг, точность, дисперсия)

5. 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
G16	dsbl	0	0.000,000,000,000	1	3	0	e2e	0	0	0	0	2	Default	False	128	Cloc	False

Save Reset

Описание каждого параметра представлено в следующей таблице:

Параметр	Описание
Announce interval	Интервал объявления, время t , 2 в степени t , например, при $t=1$ это 2 секунды, при $t=-1$ это 0.5 секунды, диапазон t составляет от -3 до 4.
Announce timeout	Таймаут объявления, время t , 2 в степени t , например, при $t=1$ это 2 секунды, при $t=-1$ это 0.5 секунды, t находится в диапазоне от 1 до 10.
Sync interval	Интервал синхронизации времени, время t , 2 в степени t , например, при $t=1$ это 2 секунды, при $t=-1$ это 0.5 секунды, диапазон t составляет от -7 до 4.

Параметр	Описание
Delay mechanism	Настройка механизма задержки, p2p, e2e.
Request message interval	Интервал запроса задержки/pdelay, время t, 2 в степени t, например, при t=1 это 2 секунды, при t=-1 это 0.5 секунды, диапазон t составляет от -7 до 5.
Delay asymmetry	Асимметричное время задержки порта, единица измерения нс, диапазон -100000100000, значение по умолчанию 0.
Entrance delay	Значение компенсации задержки на входе порта, единица измерения нс, диапазон -100000100000, значение по умолчанию 0.
Exit delay	Значение компенсации задержки на выходе порта, единица измерения нс, диапазон -100000100000, значение по умолчанию 0.
Multicast address	Мультикаст-адрес, значение по умолчанию
Non-slave clock	Не рабочие часы, значение по умолчанию false
local priority	Локальный приоритет, диапазон 0255, значение по умолчанию 128
two steps	Двухступенчатый режим, значение по умолчанию clock def
non-master clock	Не основные часы, значение по умолчанию false
MDR	Средняя задержка запросов.



Примечания:

- Режим e2eTC поддерживает только e2e, режим p2pTC поддерживает только p2p.

6. Основная конфигурация фильтрации:

Basic Filter Parameters

Delay Filter	Period	Dist
<input type="text" value="6"/>	<input type="text" value="1"/>	<input type="text" value="2"/>

Basic Servo Parameters

Display	P-enable	I-enable	D-enable	'P' constant	'I' constant	'D' constant	Gain constant
False <input type="button" value="v"/>	True <input type="button" value="v"/>	True <input type="button" value="v"/>	True <input type="button" value="v"/>	<input type="text" value="3"/>	<input type="text" value="80"/>	<input type="text" value="40"/>	<input type="text" value="1"/>

Описание каждого параметра представлено в следующей таблице:

Параметр	Описание
delayed filtering	Параметр фильтра задержки, диапазон 0-6, значение по умолчанию 6.
cycle	Период фильтра, диапазон 1-10000, значение по умолчанию 1.
hop count	Расстояние, диапазон 0-10, значение по умолчанию 2.
show	Отображение смещения от мастера, средней задержки пути, коррекции часов и значение по умолчанию False.

Параметр	Описание
P-enable	Включение пропорциональной части, true/false, значение по умолчанию True.
I-enable	Включение дифференциальной части, true/false, значение по умолчанию False.
D-enable	Включение интегральной части, true/false, значение по умолчанию False.
P-constant	Пропорциональная константа, настройка алгоритма фильтра, диапазон 1-1000, значение по умолчанию 3.
I-constant	Дифференциальная константа, настройка алгоритма фильтра, диапазон 1-10000, значение по умолчанию 30.
D-constant	Интегральная константа, настройка алгоритма фильтра, диапазон 1-10000, значение по умолчанию 40.
Gain constant	Константа коэффициента пропорционального усиления, настройка алгоритма фильтра, диапазон 1-10000, значение по умолчанию 1

7. Конфигурация набора данных порта 802.1 AS.

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
G16	Disabled	False	False	0	0	-3	0.000,000,000,000	0	FALSE	2	800	3	9	9

Port	useMgmtSync	SyncIntrvl	useMgmtAnnounce	AnnounceIntrvl	useMgmtPdelay	PdelayIntrvl	uMSCNRR	MSCNRR	uMSCMLD	MSCML
G16	<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
G16	<input type="checkbox"/>	3	3	3

Описание каждого параметра представлено в следующей таблице:

Параметр	Описание
NPDT	Порог средней задержки, диапазон 0~4000000000 нс, значение по умолчанию 800.
sync receive timeout	Тайм-аут приема синхронизации, диапазон 1~255, значение по умолчанию 3.
number of lost responses allowed	Количество допустимых потерянных ответов, диапазон 0~10, значение по умолчанию 9.
number of faults allowed	Количество допустимых неисправностей, диапазон 1~255, значение по умолчанию 9.
sync interval	Интервал синхронизации, диапазон -7~4, значение по умолчанию -3.
announce interval	Интервал объявления, диапазон -3~4, значение по умолчанию 0.
pdelay interval	Интервал pdelay, диапазон -7~5, значение по умолчанию 0.
Gtp interval	Интервал Gtp, диапазон -24~24, значение по умолчанию 3.

Параметр	Описание
Gtp receive timeout	Тайм-аут приема Gtp, диапазон 1~255, значение по умолчанию 3.
initialize Gtp interval	Инициализировать интервал Gtp, диапазон -24~24, значение по умолчанию 3

8. Конфигурация специфического порта общего сервиса 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
G16	800	0	0	<input type="checkbox"/>	0	True	<input type="checkbox"/>	True	True	<input type="checkbox"/>	True	9

Описание каждого параметра представлено в следующей таблице:

Параметр	Описание
average delay threshold	Средний порог задержки, диапазон 0~4000000000 нс, значение по умолчанию 800.
delay asymmetry	Конфигурация асимметричной задержки, диапазон -100000~100000, значение по умолчанию 0.
delay request interval	Интервал запроса задержки, диапазон -7~5, значение по умолчанию 0.
number of lost responses allowed	Количество допустимых потерянных ответов, диапазон 0~10, значение по умолчанию 9.
number of faults allowed	Количество допустимых неисправностей, диапазон 1~255, значение по умолчанию 9

8.10.1.3 PTP статус

Интерфейс отображения статуса PTP:

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	1588	BASIC	NONE

Local Clock Current Time

PTP Time	Clock Adjustment method	Ports Monitor Page
1970-01-01T08:01:19+08:00 854,447,794	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
Ord-Bound	False	False	30	00:00:00:ff:fe:0a:11:22	0	Cl:248 Ac:Unknwn Va:00000	128	128	128	Ethernet	1	0	0

Clock Current DataSet

stpRm	Offset From Master	Mean Path Delay	Slave Port	Slave State	Holdover(ppb)
0	0.000,000,000,000	0.000,000,000,000	0	FREERUN	NA

Clock Parent DataSet

Parent Port ID	port	PStat	Var	Rate	GrandMaster ID	GrandMaster Clock Quality	Pri1	Pri2
00:00:00:ff:fe:0a:11:22	0	False	0	0	00:00:00:ff:fe:0a:11:22	Cl:248 Ac:Unknwn Va:00000	128	128

Clock Time Properties DataSet

UtcOffset	Valid	leap59	leap61	Time Trac	Freq Trac	ptp Time Scale	Time Source
0	False	False	False	False	False	True	160

Описания каждого элемента параметра см. в описании конфигурации часов PTP.

Параметр	Описание
clock instance	Экземпляр часов.
hardware clock domain	Аппаратный домен часов.
equipment type	Тип устройства: Ord-Bound/E2eTransp/P2pTransp/mastronly/slaveonly.
profile	Предустановленные файлы: параметры каждого предустановленного файла по умолчанию различны. Выберите предустановленный файл в соответствии с фактическим применением.
filter type	Тип фильтра: базовый алгоритм фильтрации.
filter mode	Режим фильтра: ПАКЕТ / НЕТ
PTP time	РTP время.
time calibration method	Метод калибровки времени.
one way	Односторонний.
two steps	Двухступенчатый.
clock ID	Идентификатор часов.
clock domain	Программный домен часов.
clock quality	Качество часов.
priority 1	Приоритет 1.
priority 2	Приоритет 2.
local priority	Локальный приоритет.
agreement type	Тип протокола: Ethernet/EthernetMixed/IPV4Multi/IPv4Mixed/IPv4Uni /onePPS/EthIPv4IPv6combo.
PCP	Приоритет PCP.

Параметр	Описание
DSCP	Приоритет DSCP.
GM capable	Функция GM.
sdold	Идентификатор разработки организации стандартов.
wxya	Расстояние до главных часов.
offset from master	Смещение главных часов.
mean path delay	Средняя задержка пути, для P2P равна 0.
last GM phase change	Последнее изменение фазы GM.
GM time base	Базовое время GM.
GM change count	Количество изменений GM.
last GM change event	Значение изменения события GM.
last GM phase change event	Значение изменения фазы GM.
last GM freq. change event	Значение изменения частоты GM.
slave state	Статус рабочих часов.
hold over	Длительность рабочих часов.
parent clock ID	Идентификатор главных часов-родителей.
P stat	Статус главных часов-родителей.
variance	Дисперсия времени главных часов-родителей.
rate	Частота главных часов-родителей.
ancestor clock ID	Идентификатор предковых часов.
ancestral clock quality	Качество предковых часов (ранг, точность, дисперсия).
CRR	Соседняя скорость

8.10.1.4 802.1AS статистика

Интерфейс отображения статистики 802.1 AS:

802.1AS Clock Instance Specific Statistics

Clock Instance 0 ▾ Auto-refresh ☐ Refresh Clear

Port	Sync Count		FollowUp Count		Pdelay Request Count		Pdelay Response Count		Pdelay Response FollowUp Count		Announce Count		PTP Packet Discard Count	Sync Receipt Timeout Count	Announce Receipt Timeout Count	Pdelay Allowed Lost Responses Exceeded Count	
	Rx	TX	Rx	TX	Rx	TX	Rx	TX	Rx	TX	Rx	TX	Count	Count	Count	Count	
G1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
G2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
G3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
G4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
G5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
G6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
G7	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
G8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
G9	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
G10	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
G11	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
G12	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
G13	0	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
Sync Count	Количество пакетов синхронизации
Follow Up Count	Количество пакетов FollowUp
Pdelay Request Count	Количество сообщений PdelayRequest
Pdelay Response Count	Количество сообщений PdelayResponse
Pdelay Response Follow Up Count	Количество сообщений PdelayResponseFollowUp
Announce Count	Количество сообщений Announce
PTP Packet Discard Count	Количество отброшенных пакетов PTP
Sync Receipt Timeout Count	Количество превышений таймаута приема синхронизации
Announce Receipt Timeout Count	Количество превышений таймаута приема объявления
Pdelay Allowed Lost Responses Exceeded Count	Количество превышений допустимого количества потерянных ответов на Pdelay

8.10.2 Пример конфигурации PTP

8.10.2.1 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	Output
Adjust Method	Auto

- ♦ Добавить источник часов PTP, выбрав тип устройства Ord-Bound, и установить предустановленный файл в 1588.

PTP Clock Configuration

Delete	Clock Instance	HW Domain	VID	Device Type	Profile
<input type="checkbox"/>	0	0	1	Ord-Bound	1588
<input type="checkbox"/>	2	2	2	Ord-Bound	802.1AS

- ♦ Пример настройки часов:

a. Выбрать тип фильтра BASIC.

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	1588	<input type="button" value="Apply"/>	BASIC

b. Выберите порт, соединяющий устройства главных и ведомых часов.

Port Enable and Configuration

Port Enable																								Configuration						
G1	G2	G3	G4	G5	G6	G7	G8	G9	G10	G11	G12	G13	G14	G15	G16	G17	G18	G19	G20	G21	G22	G23	G24	X1	X2	X3	X4	X5	X6	<u>Ports</u>
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<u>Configuration</u>

2. Конфигурация ведомых часов.

- ♦ Настроить внешние часы: установить режим 1PPS на вывод.

PTP External Clock Mode

One_PPS_Mode	Output
Adjust Method	Auto

- ♦ Добавить источник часов PTP, выбрав slaveonly или Ord-Bound в качестве типа устройства, и установить предустановленный файл на 1588.

PTP Clock Configuration

Delete	Clock Instance	HW Domain	VID	Device Type	Profile
<input type="checkbox"/>	0	0	1	Ord-Bound	1588

- ♦ Пример настройки часов:

a. Выбрать тип фильтра BASIC.

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	1588	<input type="button" value="Apply"/>	BASIC

b. Выберите порт, который соединяет устройства главных и ведомых часов.

Port Enable and Configuration

Port Enable																								Configuration						
G1	G2	G3	G4	G5	G6	G7	G8	G9	G10	G11	G12	G13	G14	G15	G16	G17	G18	G19	G20	G21	G22	G23	G24	X1	X2	X3	X4	X5	X6	Ports
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Configuration	

3. Просмотр результатов синхронизации PTP ведомых часов:

- ♦ Состояние ведомых часов отображается как PHASE_LOCKED или FREQ_LOCKED.
- ♦ Смещение от мастера отображается как смещение мастерского часов.
- ♦ Средняя задержка пути отображается как задержка пути.
- ♦ Идентификатор главных часов отображается как идентификатор родительских часов.
- ♦ Идентификатор предковых часов отображается как идентификатор предковых 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	1588	Apply	BASIC

Port Enable and Configuration

Port Enable																								Configuration						
G1	G2	G3	G4	G5	G6	G7	G8	G9	G10	G11	G12	G13	G14	G15	G16	G17	G18	G19	G20	G21	G22	G23	G24	X1	X2	X3	X4	X5	X6	Ports
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Configuration

Local Clock Current Time

PTP Time	Clock Adjustment method	Settings
1970-01-01T08:08:31+08:00	Internal Timer	Synchronize to System Clock
057,191,429		Synchronized to System Clock

Clock Current DataSet

stpRm	Offset From Master	Mean Path Delay
0	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
00:00:00:ff:fe:0a:11:22	0	False	0	0	00:00:00:ff:fe:0a:11:22	Cl:248 Ac:Unknwn Va:00000	128	128

8.10.2.2 Конфигурация предустановленного файла 802.1AS

4. Конфигурация главных часов:

- ◆ Настроить внешние часы: режим 1PPS установлен на вывод.

PTP External Clock Mode

One_PPS_Mode	Output	▼
Adjust Method	Auto	▼

- ◆ Добавить источник часов PTP, выбрав тип устройства Ord-Bound, и установить 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

- ◆ Пример настройки часов:

- a. Выберите тип фильтра - BASIC.

PTP Clock's Configuration and Status

Clock Type and Profile

Clock	HW	Device	Profile	Apply Profile Defaults	Filter Type
Instance	Domain	Type			
0	0	Ord-Bound	802.1AS	Apply	BASIC

- b. Выберите порт, соединяющий главные часы и ведомые часы.

Port Enable and Configuration

Port Enable																								Configuration						
G1	G2	G3	G4	G5	G6	G7	G8	G9	G10	G11	G12	G13	G14	G15	G16	G17	G18	G19	G20	G21	G22	G23	G24	X1	X2	X3	X4	X5	X6	<u>Ports</u>
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<u>Configuration</u>

- c. Конфигурация приоритета. Приоритет главных часов обычно меньше 128, а приоритет ведомых часов обычно больше 128.

Clock Default DataSet

Device Type	One-Way	2 Step Flag	Ports	Clock Identity	Dom	Clock Quality
Ord-Bound	False	True	30	00:00:00:ff:fe:0a:11:22	0	Cl:248 Ac:Unknwn Va:17258
Pri1	Pri2	Local Prio	Protocol	PCP	DSCP	
246	248	128	Ethernet	0	0	

- d. Другие настройки не требуют изменений. Большая часть работы по установке по умолчанию завершена, когда веб-интерфейс выбирает предустановленный файл.
5. Конфигурация ведомых часов.

- ♦ Настроить внешние часы: режим 1PPS установлен на вывод.

PTP External Clock Mode

One_PPS_Mode	Output
Adjust Method	Auto

- ♦ Добавить источник часов PTP, выбрав тип устройства Ord-Bound, и установить 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

♦ Пример настройки часов:

a. Выберите тип фильтра - BASIC.

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

b. Выберите порт, соединяющий главные и ведомые часы.

Port Enable and Configuration

Port Enable																								Configuration						
G1	G2	G3	G4	G5	G6	G7	G8	G9	G10	G11	G12	G13	G14	G15	G16	G17	G18	G19	G20	G21	G22	G23	G24	X1	X2	X3	X4	X5	X6	<u>Ports</u>
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<u>Configuration</u>

c. Другие конфигурации не требуют изменений. Большая часть работы по установке по умолчанию завершена, когда веб-интерфейс выбирает предустановленный файл.

6. Просмотр результатов синхронизации PTP ведомых часов:

- ♦ Состояние ведомых часов отображается как PHASE_LOCKED.
- ♦ Смещение от мастера отображается в значениях ns (наносекунд).
- ♦ Идентификатор главных часов отображается как идентификатор родительских часов.
- ♦ Идентификатор предковых часов отображается как идентификатор предковых часов.

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	NONE

Local Clock Current Time

PTP Time	Clock Adjustment method	Ports Monitor Page
1970-01-01T08:13:21+08:00 241,780,840	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	sdoId
Ord-Bound	False	True	30	00:00:00:ff:fe:0a:11:22	0	Cl:248 Ac:Unknown 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)
0	0.000,000,000,000	0.000,000,000,000	0.000,000,000	0.000000	0	0	0	0	0	0	FREERUN	NA

Clock Parent DataSet

Parent Port ID	port	PStat	Var	Rate	GrandMaster ID	GrandMaster Clock Quality	Pri1	Pri2	CRR
00:00:00:ff:fe:0a:11:22	0	False	0	0	00:00:00:ff:fe:0a:11:22	Cl:248 Ac:Unknown Va:17258	246	248	0

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
<u>admin</u>	15

[Add User](#)

Описание каждого параметра представлено в следующей таблице:

Параметр	Описание
Username	Отображается текущее имя пользователя. Щелкните ссылку с

Параметр	Описание
	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.

EditUser

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 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.

EditUser

Users Configuration

User Name

Change Password No ▼

Privilege Level 0 ▼

Save
Reset
Cancel

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"> • Да • Нет
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:

- При первом входе на веб-страницу коммутатора в окне браузера и открытии новой вкладки в том же окне для доступа к коммутатору диалоговое окно входа больше не будет появляться, и вход будет производиться автоматически с использованием ранее введенного имени пользователя и пароля по умолчанию. Если вы хотите использовать другую учетную запись пользователя для входа на веб-страницу коммутатора, вам достаточно щелкнуть кнопку выхода в правом верхнем углу веб-страницы или снова

открыть окно браузера.

- Имя пользователя администратора по умолчанию для коммутатора - admin, пароль - admin, уровень привилегий - 15, и у него есть все права управления.
- Пользователь администратора по умолчанию admin не может быть удален, но его пароль и уровень привилегий могут быть изменены. Другие вручную добавленные пользователи могут быть удалены, и их пароли и уровни привилегий могут быть изменены. Пожалуйста, будьте осторожны при изменении уровня привилегий пользователя-администратора admin.
- После удаления веб-страницы или командной строки текущего вошедшего пользователя или изменения пароля и уровня привилегий текущего вошедшего пользователя вас не попросят снова войти в систему немедленно. Текущая сессия продолжит использовать старые атрибуты пользователя, и в файле конфигурации будут отображаться новые атрибуты. Когда сессия завершится или будет выполнен выход из сеанса и потребуются повторный вход в систему, новые атрибуты пользователя вступят в силу.
- На странице редактирования указанного пользователя вы можете изменить только пароль пользователя и уровень привилегий, но не его имя пользователя.

9.2 DHCPv4

9.2.1 DHCPv4 сервер

Введение в протокол DHCP

DHCP (Dynamic Host Configuration Protocol) является улучшенной версией BOOTP. Он принимает модель клиент-серверного взаимодействия. Все параметры настройки IP-сети централизованно управляются DHCP-сервером и отвечают за обработку запроса DHCP клиента; клиент использует назначенные сервером параметры сети IP для общения.

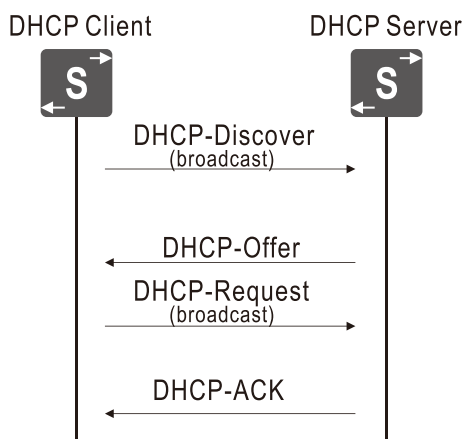
Для использования механизма динамического выделения адресов DHCP администратор должен настроить DHCP-сервер таким образом, чтобы он мог предоставить группу IP-адресов, называемую пулом адресов. Каждый раз, когда новый компьютер подключается к сети, компьютер обращается к серверу и запрашивает IP-адрес. Сервер выбирает адрес из настроенного пула адресов и назначает его компьютеру.

Для динамического получения и использования действительного IP-адреса необходимо пройти следующие этапы:

1. Этап обнаружения: фаза, в которой клиент DHCP ищет DHCP-сервер.
2. Этап предоставления: фаза, в которой DHCP-сервер предоставляет IP-адрес.

3. Этап выбора: то есть фаза, в которой клиент DHCP выбирает IP-адрес, предоставленный определенным DHCP-сервером.
4. Этап подтверждения: то есть 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 Configuration

Global Mode

Mode

Mode

VLAN	Enabled
1	<input type="checkbox"/>
10	<input type="checkbox"/>

Описание каждого параметра представлено в следующей таблице:

Параметр	Описание
Global mode	Глобальный режим
mode	Настройте режим работы DHCP-сервиса для всей системы, включая: <ul style="list-style-type: none"> Включить: включить глобальный DHCP-сервис; Отключить: отключить глобальный DHCP-сервис
Mode	VLAN режим
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"> Выбрано: включить DHCP-сервис соответствующего интерфейса VLAN; Не выбрано: отключить DHCP-сервис соответствующего интерфейса VLAN



Примечания:

Перед запуском службы DHCP для каждого интерфейса VLAN на веб-странице, пожалуйста, создайте соответствующий интерфейс VLAN уровня 3 на странице "Функции уровня 3 > Управление IP > Конфигурация IP" и завершите его на странице "Функции уровня 2 > VLAN > Глобальная конфигурация". Настройте атрибуты VLAN, такие как PVID, для каждого порта.

9.2.1.2 Отсутствие выделения IP-адресов

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

Exclude IP

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



Примечания:

Необходимо исключить зарезервированный IP-адрес из пула адресов DHCP, чтобы он не выделялся. Это приведет к тому, что зарезервированный IP-адрес, настроенный для порта в адресном пуле, не будет выделяться.

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	SubnetMask	Reserved Only	Lease Time
--------	------	------	----	------------	---------------	------------

Add New Pool

Save 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"> Сеть: Этот пул адресов может обслуживать несколько DHCP-клиентов; Хост: Этот пул адресов может обслуживать только определенных DHCP-клиентов, идентифицируемых идентификаторами клиентов или аппаратными адресами
IP	<ul style="list-style-type: none"> Представляет собой сегмент сети, из которого можно выделять адреса в адресном пуле сети. В адресном пуле типа "хост" представляет собой IP-адрес, назначенный клиенту, соответствующему этому адресному пулу
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:

Параметр	Описание
	<ul style="list-style-type: none"> Включено: Только зарезервированные IP-адреса назначаются на привязанный интерфейс. Выключено: Назначить зарезервированный IP на привязанный интерфейс, а также назначить другие динамические IP-адреса на другие интерфейсы.
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 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

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.

DHCP Server Pool Configuration

Pool Setting

Delete	Name	Type	IP	SubnetMask	Reserved Only	Lease Time
Delete	<input type="text"/>	-	-	-	-	1 Days 0 Hours 0 Minutes

Add New Pool

Save Reset



Описание:

"-" во всех списках означает неопределенное значение

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.

Описание каждого параметра представлено в следующей таблице:

Параметр	Описание
Address pool	Пул адресов
Name	Список выбора имени пула адресов, в котором можно выбрать различные пулы адресов для конфигурации.
Configuration	Конфигурация
Address pool name	Имя пула адресов, доступное только для чтения, соответствует выбору имени пула адресов выше

Параметр	Описание
Type	<p>Тип пула адресов имеет следующие два значения:</p> <ul style="list-style-type: none"> Сеть: Этот пул адресов может обслуживать несколько DHCP-клиентов, и адрес, который может быть выделен, является сетевым адресом (например, 192.168.1.0/24); 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)
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"> Включено: Только зарезервированные IP-адреса выделяются для связанного интерфейса. Выключено: Выделяется зарезервированный IP-адрес для связанного интерфейса, а также выделяются другие динамические IP-адреса для других интерфейсов.
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.
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"> Узел класса В (B-node): "В" означает широковещательную рассылку, то есть этот тип узла использует широковещательную рассылку для получения отношений отображения. Исходный узел

Параметр	Описание
	<p>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.</p> <ul style="list-style-type: none"> Узел типа P (P-node): "P" 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. Узел типа M (M-node): "M" означает смешанный, это узел типа P 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. Узел H (H-node): "H" означает гибридный, это узел класса B 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
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.
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"> None: Не указывать идентификатор.

Параметр	Описание
	<ul style="list-style-type: none"> Name: Любой идентификатор, не являющийся аппаратным. В этом случае в поле ввода должна быть введена любая строка, не содержащая китайских символов; 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.
Hardware address	Задайте 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.
CPU name	DHCP-опция 12. Указывает имя хоста клиента для использования при настройке пула адресов типа "хост".
Manufacturer classification mark	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.
Manufacturer feature information	DHCP-опция 43. Указывает конкретную информацию о каждом идентификаторе производителя для обмена информацией между DHCP-сервером и DHCP-клиентом.
Reserve IP address	Зарезервированный IP-адрес
Delete	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.
Reserved address	IP-адрес зарезервирован для указанного физического порта уровня 2.
Interface	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"


Примечания:

- Сначала необходимо настроить тип, IP-адрес и маску подсети для адресного пула, а затем настроить записи зарезервированных IP-адресов для этого пула.
- Только когда адресный пул имеет тип "сеть", необходимо настраивать записи зарезервированных IP-адресов и "выделять только зарезервированные записи", причем зарезервированный IP-адрес должен находиться в пределах диапазона подсети

адресного пула.

- После настройки параметра "Выделять только зарезервированные записи" пожалуйста, настройте как минимум одну запись зарезервированного IP-адреса, иначе этот DHCP адресный пул не сможет назначить ни одного IP.
- Только когда адресный пул имеет тип "хост", необходимо использовать идентификатор клиента, аппаратный адрес и имя клиента; когда адресный пул имеет тип "сеть", необходимость в настройке этих трех атрибутов отсутствует.
- Для настройки опций в адресном пуле, помимо соответствующих опций, передаваемых в сообщении ответа DHCP-сервера, их эффективность также зависит от реализации клиента. Пожалуйста, настройте в соответствии с фактической ситуацией

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.



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"> • Пул адресов: количество пулов адресов. • Не выделять IP: количество исключенных диапазонов IP-адресов. • Отклоненные IP: количество отклоненных IP-адресов
Binding statistics	<p>Отображается статистика количества различных привязок DHCP-сервера.</p> <ul style="list-style-type: none"> • Автоматическая привязка: количество автоматически связанных записей адресов в пуле адресов типа Network.

Параметр	Описание
	<ul style="list-style-type: none"> Ручная привязка: количество записей привязки адресов, назначенных администратором клиенту в пуле адресов типа Host. Срок действия привязки: количество записей привязки адресов, которые истекли срок аренды или были удалены из записей привязки автоматического/ручного типа.
Received DHCP message statistics	<p>Отображение статистического числа DHCP-сообщений, полученных DHCP-сервером.</p> <ul style="list-style-type: none"> Поиск: количество DHCP-сообщений DHCP-DISCOVER, полученных DHCP-сервером. Запрос: количество DHCP-сообщений DHCP-REQUEST, полученных DHCP-сервером. Отклонение: количество DHCP-сообщений DHCP-DECLINE, полученных DHCP-сервером. Освобождение: количество DHCP-сообщений DHCP-RELEASE, полученных DHCP-сервером. Уведомление: количество DHCP-сообщений DHCP-INFORM, полученных DHCP-сервером.
Statistics on sending DHCP messages	<p>Отображается статистика количества отправленных DHCP-пакетов DHCP-сервером.</p> <ul style="list-style-type: none"> Предложение: количество сообщений DHCP-OFFER, отправленных DHCP-сервером. Подтверждение: количество сообщений DHCP-ACK, отправленных DHCP-сервером. Не подтверждено: количество сообщений DHCP-NAK, отправленных DHCP-сервером.

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

Delete	IP	Type	State	Pool Name	Server/Relay IP
--------	----	------	-------	-----------	-----------------

Описание каждого параметра представлено в следующей таблице:

Параметр	Описание
delete	Проверка флажка "Удалить" означает, что запись, связанная с IP-адресом в этой строке, будет удалена.
IP	IP-адрес, назначенный клиенту DHCP
type	Тип привязки адреса. Возможные типы: <ul style="list-style-type: none"> Автоматическая: Адрес, назначенный сетевым пулом; Ручная: Адрес, назначенный хост-пулом; Истекший: Адрес, достигший окончания арендного срока;
state	Состояние привязки адреса. Возможные состояния: <ul style="list-style-type: none"> Зафиксировано: Адрес используется клиентом; Выделено: Адрес был выделен сервером, но не был запрошен клиентом; Истекший: Адрес, достигший окончания арендного срока
address pool name	Имя адресного пула, к которому привязан IP-адрес.
server/relay IP	IP-адрес DHCP-сервера или агента ретрансляции, который предоставил 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.



Примечания:

После удаления записи о привязанном IP-адресе сервер может назначить этот IP-адрес другим новым клиентам. Если клиент, соответствующий этой записи о привязанном IP-адресе, все еще подключен к сети, в это время может возникнуть конфликт сетевых адресов. Поэтому, перед удалением неистекших записей о привязанных IP-адресах, убедитесь, что соответствующий клиент отключен от сети или больше не использует этот IP-адрес;

Детали

Щелкните на любом IP-адресе в списке привязанных IP-адресов, и страница данных привязки IP-адреса DHCP-сервера будет отображена, как показано на рисунке ниже.

На этой странице отображаются подробные данные о записях привязанных IP-адресов. В верхнем левом углу страницы находится окно выбора опции привязки IP-адреса.

Пользователи могут выбрать привязанный IP-адрес, соответствующий IP-данным текущей страницы, из выпадающего списка IP. По умолчанию IP-адрес, на который пользователь щелкнул в списке привязанных IP-адресов, отображается по умолчанию.

DHCP 服务器绑定 IP

自动刷新☐刷新

绑定IP

IP

3.3.3.1

绑定的 IP 数据

IP	3.3.3.1
类型	Automatic
状态	Committed
地址池名称	pool1
服务器/中继 IP	3.3.3.3
VLAN	1
子网掩码	255.255.255.0
客户端 ID 类型	MAC
客户端 ID	48-5f-08-ca-4a-52
MAC 地址	48-5f-08-ca-4a-52
租期	1 days 0 hours 0 minutes 0 seconds
剩余租期	23 hours 59 minutes 5 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.
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">"-" : указывает на то, что DHCP-клиент не упаковывает опцию 61 в сообщение DHCP.Имя: указывает на то, что идентификатор клиента имеет тип, отличный от аппаратного.MAC: указывает на то, что тип идентификатора клиента - аппаратный MAC-адрес

Параметр	Описание
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 IP-адрес, присвоенный ему сервером, конфликтует, он уведомляет сервер, отправляя сообщение DHCP-DECLINE, и повторно запрашивает адрес у сервера. В то же время сервер регистрирует этот адрес при получении данного сообщения и больше не выделяет его клиенту, если в пуле адресов есть другие доступные адреса. Страница DHCP-клиента, сообщающая о конфликте IP-адресов, отображает все записи IP-адресов, для которых DHCP-клиент отправляет сообщения DHCP-DECLINE для уведомления о конфликтах. Страница выглядит следующим образом:



Описание каждого параметра представлено в следующей таблице:

Параметр	Описание
client reports conflicting IP	Конфликтующий IP-адрес, сообщенный клиентом DHCP.



Примечания:

Когда на этой странице есть данные, это означает, что текущее сетевое развертывание неразумно и вызывает сетевые конфликты. Рекомендуется использовать этот контент для расследования причин конфликта адресов. После решения проблемы можно очистить соответствующие записи конфликтов через командную строку `clear ip dhcp server declined <ipv4_ucast>`.

9.2.2 DHCPv4 отслеживание

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

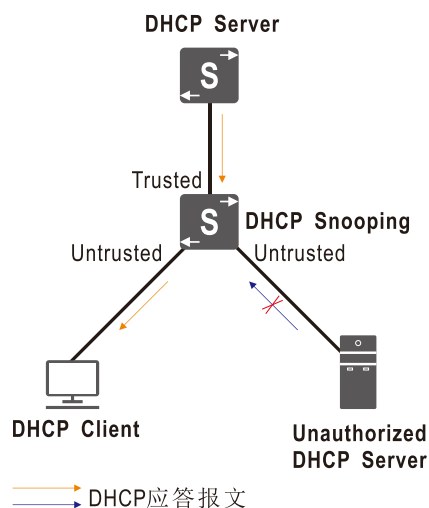
- DHCP Snooping является функцией прослушивания уровня 2 службы DHCP. В целях безопасности отделу безопасности необходимо регистрировать IP-адрес, используемый пользователем при выходе в Интернет, и подтверждать соответствие между IP-адресом, запрошенным пользователем, и MAC-адресом используемого им 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 Disabled

Port Mode Configuration

Port	Mode
*	<>
G1	Trusted
G2	Trusted
G3	Trusted
G4	Trusted
G5	Trusted
G6	Trusted
G7	Trusted
G8	Trusted
G9	Trusted
G10	Trusted
G11	Trusted
G12	Trusted
G13	Trusted
G14	Trusted
G15	Trusted
G16	Trusted
G17	Trusted

Описание каждого параметра представлено в следующей таблице:

Параметр	Описание
Snooping mode	<p>Выберите режим прослушивания DHCP.</p> <ul style="list-style-type: none"> 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. Отключить: отключить функцию DHCP Snooping.
Port mode configuration	Конфигурация режима порта.
Port	Номер порта устройства.
Mode	<p>Выберите режим доверия порта DHCP.</p> <ul style="list-style-type: none"> Доверенный: Настройте порт как доверенный источник сообщений DHCP. Недоверенный: Настройте порт как недоверенный источник сообщений DHCP

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.

MAC Address	VLAN ID	S Port	IP Address	IP Subnet Mask	DHCP Server Address
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.



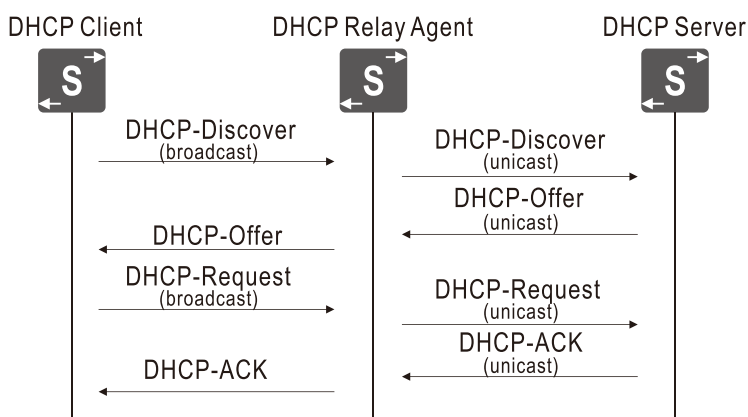
Примечания:

Правильно настроенный порт DHCP-сервера должен быть установлен как доверенный порт, в противном случае DHCP-клиент, подключенный к прослушивающему устройству, не сможет получить 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.

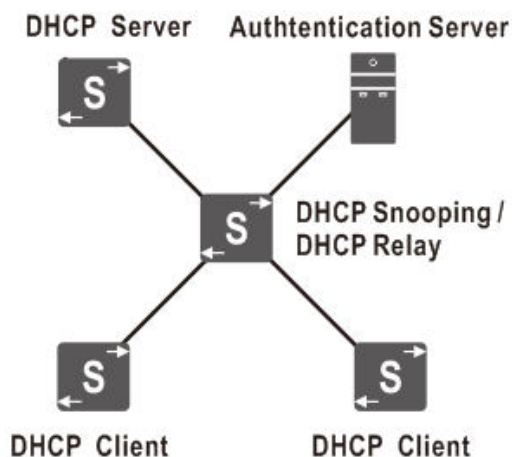
Опция информации ретранслятора (Option 82)

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.

9.2.3.1 Конфигурация транка

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

Relay Mode	Disabled ▼
Relay Server	0.0.0.0
Relay Information Mode	Disabled ▼
Relay Information Policy	Keep ▼

Save Reset

Описание каждого параметра представлено в следующей таблице:

Параметр	Описание
Relay mode	<p>Выберите режим включения реле DHCP. По умолчанию функция реле DHCP отключена.</p> <ul style="list-style-type: none"> 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. Отключить: Отключить функцию реле DHCP на коммутаторе
Relay server	<p>Введите IP-адрес DHCP-сервера реле. По умолчанию этот элемент не указан.</p>
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"> Включить: включить опцию информации агента реле DHCP. Отключить: отключить опцию информации агента реле DHCP.
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"> Замена: когда полученное сообщение запроса DHCP содержит опцию 82, исходная информация опции 82 в сообщении заменяется и пересылается. Сохранение: когда полученное сообщение запроса DHCP содержит опцию 82, исходная информация опции 82 в сообщении сохраняется и пересылается без изменений.

Параметр	Описание
	<ul style="list-style-type: none"> Отбросить: когда полученное сообщение запроса DHCP содержит опцию 82, отбросить сообщение.



Примечания:

- Когда DHCP-клиент получает IP-адрес через ретранслятор DHCP, DHCP-сервер должен быть настроен с тем же пулом адресов, что и сегмент сети (сетевой номер и маска) IP-адреса интерфейса, к которому подключен DHCP-ретранслятор. В противном случае DHCP-клиент не сможет получить правильный IP-адрес.
- Опция информации о ретрансляторе DHCP может вступить в силу только после включения функции ретранслятора DHCP.

9.2.3.2 Статистика ретранслятора

На странице статистики реле DHCP, показанной на рисунке ниже.

DHCP Relay Statistics							
DHCP 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
Server statistics	Статистика сервера:
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.

Параметр	Описание
Client statistics	Статистика клиента:
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

Combined G1 Auto-refresh Refresh Clear

Rx Data Packet	Tx Data Packet
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/TXDiscover	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).
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



Примечания:

- Пакеты, отклоненные RX из-за отсутствия доверия, действительны только в режиме

слежения за DHCP и смешанном режиме.

- Если вход пакетов DHCP осуществляется через механизм маршрутизации уровня 3, стандартная статистика TX для каждого порта не будет увеличиваться, и очистка статистики для конкретного порта может не повлиять на глобальную статистику, поскольку они собирают данные разных уровней.

9.3 DHCPv6

9.3.1 DHCPv6 отслеживание

9.3.1.1 Конфигурация прослушивания.

На странице конфигурации отслеживания DHCPv6, изображенной на рисунке ниже.

DHCPv6 Snooping Configuration

Switch Configuration

Snooping Mode Disabled ▾

Port Configuration

Port	Trust Mode
*	<> ▾
G1	Trusted ▾
G2	Trusted ▾
G3	Trusted ▾
G4	Trusted ▾
G5	Trusted ▾
G6	Trusted ▾
G7	Trusted ▾
G8	Trusted ▾
G9	Trusted ▾
G10	Trusted ▾
G11	Trusted ▾
G12	Trusted ▾
G13	Trusted ▾
G14	Trusted ▾
G15	Trusted ▾

Описание каждого параметра представлено в следующей таблице:

Параметр	Описание
listening mode	<p>Выберите режим прослушивания DHCPv6.</p> <ul style="list-style-type: none"> Включить: Включить функцию прослушивания DHCPv6. Когда функция отслеживания DHCPv6 включена, сообщения DHCPv6 запросов будут перенаправляться на доверенные порты, и только ответные пакеты с доверенных портов будут разрешены к получению. Выключить: Отключить функцию отслеживания DHCPv6
Port configuration	Конфигурация порта
port	Номер порта устройства
mode	<p>Выберите режим доверия для порта DHCPv6.</p> <ul style="list-style-type: none"> Доверие: Настройте порт как доверенный источник сообщений DHCPv6. Недоверие: Настройте порт как недоверенный источник сообщений DHCPv6.



Примечания:

- После включения отслеживания DHCPv6 DHCPv6-клиент на этом устройстве больше не сможет получать сообщения DHCPv6 и работать нормально.
- В настоящее время отслеживание DHCPv6 не может анализировать сообщения ретрансляции DHCPv6. Поэтому в сетях с ретрансляцией информация о клиентах DHCPv6 может быть записана только тогда, когда отслеживание DHCPv6 размещено между клиентом DHCPv6 и ретранслятором DHCPv6.
- Легальный порт DHCPv6-сервера должен быть установлен как доверенный порт, иначе ответное сообщение DHCPv6-сервера не сможет пройти, что приведет к тому, что DHCPv6-клиент не сможет получить IPv6-адрес.

Таблица прослушивания

На странице таблицы прослушивания отображается информация о динамическом выделении IP-адресов IPv6, прослушиваемая на устройстве после включения функции отслеживания DHCPv6. Динамическая таблица отслеживания DHCPv6 на странице перечислит динамические IP-адреса IPv6, полученные всеми клиентами DHCPv6, подключенными к устройству через DHCPv6-сервер.

DHCPv6 Snooping Table

Total entries: 0

Auto-refresh ☐ Refresh

Client DUID	MAC Address	IAID	VLAN ID	Ingress Port	Assigned Address	Lease Time	DHCP Server Address
-------------	-------------	------	---------	--------------	------------------	------------	---------------------

Описание каждого параметра представлено в следующей таблице:

Параметр	Описание
Total number of entries	Статистика количества адресов, полученных клиентом из таблицы прослушивания.
ClientDUID	DUID: Уникальный идентификатор устройства DHCPv6. Этот идентификатор генерируется устройством с включенной функцией DHCPv6.
MAC address	Клиент DHCPv6.
IAID	Клиент DHCPv6 запросил выделение идентификаторов адресов, и сервер выделил различные IPv6-адреса соответственно;
VLAN ID	Этот VLAN ID сообщения клиента DHCPv6 получено на устройстве прослушивания DHCPv6.
Source port	Последний раз, когда устройство прослушивания DHCPv6 получило это сообщение IAID от клиента.
Assign address	IPv6-адрес, назначенный соответствующему IAID клиента DHCPv6.
Release time	Максимальное время жизни адреса, соответствующего IAID, в секундах.
DHCP server address	Адрес DHCPv6-сервера, который выделяет IP-адреса IPv6 клиентам

9.3.1.2 Статистика прослушивания

DHCPv6 Snooping Statistics

G1 Auto-refresh ☐ Refresh Clear

Receive Packets		Transmit Packets	
Rx Solicit	0	Tx Solicit	0
Rx Request	0	Tx Request	0
Rx InfoRequest	0	Tx InfoRequest	0
Rx Confirm	0	Tx Confirm	0
Rx Renew	0	Tx Renew	0
Rx Rebind	0	Tx Rebind	0
Rx Decline	0	Tx Decline	0
Rx Advertise	0	Tx Advertise	0
Rx Reply	0	Tx Reply	0
Rx Reconfigure	0	Tx Reconfigure	0
Rx Release	0	Tx Release	0
Rx DiscardUntrust	0		

Параметр	Описание
Rx /Tx Solicit	DHCPv6 Solicit: сообщения полученные/отправленные через этот порт согласно статистике прослушивания DHCPv6.
Rx /Tx Request	DHCPv6 Request: сообщения полученные/отправленные через

Параметр	Описание
	этот порт согласно статистике прослушивания DHCPv6.
Rx /Tx InfoRequest	DHCPv6 InfoRequest: сообщения полученные/отправленные через этот порт согласно статистике прослушивания DHCPv6.
Rx /Tx Confirm	DHCPv6 Confirm: сообщения полученные/отправленные через этот порт согласно статистике прослушивания DHCPv6.
Rx /Tx Renew	DHCPv6 Renew: пакеты полученные/отправленные через этот порт согласно статистике прослушивания DHCPv6.
Rx /Tx Rebind	DHCPv6 Rebind: пакеты полученные/отправленные через этот порт согласно статистике прослушивания DHCPv6.
Rx /Tx Advertise	DHCPv6 Advertisement: сообщения полученные/отправленные через этот порт согласно статистике прослушивания DHCPv6.
Rx /Tx Reconfigure	DHCPv6 Reconfigure: сообщения полученные/отправленные через этот порт согласно статистике прослушивания DHCPv6.
Rx /Tx Release	DHCPv6 Release: сообщения полученные/отправленные через этот порт согласно статистике прослушивания DHCPv6.
Rx DiscardUntrust	Статистика прослушивания DHCPv6 показывает количество сообщений DHCPv6 сервера, которые этот порт получил и отбросил из-за нахождения в недоверенном режиме

9.3.2 Ретрансляция DHCPv6

9.3.2.1 Конфигурация транка

DHCPv6 Relay Configuration

Delete	Interface	Relay Interface	Relay Destination
<input type="checkbox"/>	VLAN 1	VLAN 2	ff05::1:3

Add Entry

Save Reset

Описание каждого параметра представлено в следующей таблице:

Параметр	Описание
delete	-
interface	Устройство-ретранслятор получает DHCPv6-сообщение клиента;
trunk interface	Устройство-ретранслятор пересылает DHCPv6-сообщения от клиента;
relay destination address	По умолчанию используется многоадресный адрес всех DHCPv6-серверов (ff05::1:3). Если известен сервер, можно указать уникаст-адрес интерфейса сервера

9.3.2.2 Статистика ретранслятора

Страница статистики ретрансляции DHCPv6 показана на рисунке ниже.



араметры представлены в следующей таблице:

Параметр	Описание
number of discarded server packets due to missing interface options	DHCPv6-сообщения сервера с неправильной опцией несуществующего интерфейса (Опция 18), полученные ретранслятором и отброшенные.
interface	Устройство-ретранслятор получает DHCPv6-сообщение клиента.
trunk interface	Устройство-ретранслятор пересылает DHCPv6-сообщения от клиента.
relay address	IP-адрес IPv6 назначения, заполненный при пересылке пакетов DHCPv6 клиента с интерфейса ретранслятора.
message sent to server	Количество пакетов, отправленных на сервер через соответствующий интерфейс ретранслятора.
receive server messages	Количество пакетов, полученных от сервера через соответствующий интерфейс ретранслятора.
drop server messages	Количество пакетов от сервера, отброшенных соответствующим интерфейсом ретранслятора.
sent to client	Количество пакетов, отправленных клиенту через соответствующий интерфейс ретранслятора.
receive client messages	Количество пакетов, полученных от клиента через соответствующий интерфейс ретранслятора.
discard client packets	Количество пакетов от клиента, отброшенных соответствующим интерфейсом ретранслятора.

9.4 Системное время

Используйте функцию настройки времени для установки системного времени, часового пояса, летнего времени и аббревиатуры летнего времени коммутатора.

9.4.1 Настройка времени

Эта страница настраивает параметры системного времени, как показано на рисунке ниже.

Setting Time

Setting Time	<input type="text"/>	Year	<input type="text"/>	Month	<input type="text"/>	Day	<input type="text"/>	Hours	<input type="text"/>	Minutes	<input type="text"/>	Seconds	<input type="text"/>
--------------	----------------------	------	----------------------	-------	----------------------	-----	----------------------	-------	----------------------	---------	----------------------	---------	----------------------

TimeZone Configuration

TimeZone Configuration	
TimeZone	(UTC+08:00) Beijing, Chongqing, Hong Kong, Urumqi
Hours	8
Minutes	0
Abbreviation	<input type="text"/> (0-16 Characters)

Daylight Saving Time Configuration

Daylight Saving Time Mode	
Daylight Saving Time	Disabled

Start Time Setting	
Day	1
Month	Jan
Year	2000
Hours	0
Minutes	0

End Time Setting	
Day	1
Month	Jan
Year	2097

Описание каждого параметра представлено в следующей таблице:

Параметр	Описание
set time	Локальное время можно вручную обновить на коммутаторе, и порог конфигурации составляет с 1 января 2000 года по 31 декабря 2097 года
time zone	<p>Разделение часовых поясов мира основано на нулевом меридиане. От 7,5° западной долготы до 7,5° восточной долготы (интервал долготы 15°) - это нулевая зона. От двух границ нулевого часового пояса на восток и на запад соответственно каждые 15° долготы делится часовой пояс. Восточные и западные 12 часовых поясов совпадают; мир делится на 24 часовых пояса. Каждый часовой пояс использует местное среднее солнечное время на центральном меридиане как стандартное время зоны. В принципе, границы часовых поясов делятся по географической долготе, но на практике они часто определяются на основе административных или естественных границ каждой страны. Поэтому не все смежные часовые пояса разнесены на один час, и из-за географических особенностей существуют часовые пояса +13 и +14.</p> <p>Устройство может выбирать соответствующие часовые пояса на основе типичных регионов, и устройство автоматически корректирует внутренний временной сдвиг на основе выбранного часового пояса</p>

Параметр	Описание
hour	После настройки часового пояса здесь будет отображаться количество часов, отличающихся от времени UTC.
minute	После установки часового пояса здесь будет отображаться разница в минутах от времени UTC
abbreviation	Существует много стран, использующих одинаковый часовой пояс, и вы можете настроить описание этого часового пояса самостоятельно.
summer time	Летнее время, также известное как "летнее время" или "летнее время", является системой, которая искусственно регулирует местное время для экономии энергии. Существует три варианта настройки летнего времени: отключено, циклическое и непериодическое. При отключении не будет создано никаких сдвигов; при настройке режима летнего времени на циклический, вы можете настроить время начала (неделя, день, месяц, час, минута), время окончания (неделя, день, месяц, час, минута) и сдвиг. Смещение часов между начальным и конечным временем каждого года; в непериодическом режиме настройте время начала (месяц, день, год, час, минута), время окончания (месяц, день, год, час, минута) и сдвиг, часы отстают на время этого времени

9.5 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

Mode	Disabled
Pool Interval	6
Server 1	
Server 2	
Server 3	
Server 4	
Server 5	

Save Reset

Описание каждого параметра представлено в следующей таблице:

Параметр	Описание
model	Включить или выключить функцию NTP.
polling interval	Настроить интервал времени для NTP и синхронизацию сообщений с сервером. Интервал сообщения составляет 2^n секунд. Порог конфигурации составляет от 4 до 14, а значение по умолчанию - 6.
server 1-5	Адрес сервера NTP можно настроить с использованием IP-адреса или доменного имени сервера. Клиент будет синхронизировать время с сервером с наивысшим номером первым. Если текущий сервер не удастся подключиться или не может дать правильное время, будет использован последующий сервер для синхронизации времени

9.6 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.

9.6.1 Конфигурация журнала

Страница конфигурации журнала выглядит следующим образом, как показано на рисунке ниже.

System Log Configuration

Server Mode	Disabled
Server Address	
Log Level	Informational

Save Refresh

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"> Ошибка: Отправляет конкретное сообщение с кодом серьезности меньше Ошибка (3). Предупреждение: Отправляет конкретное сообщение, код серьезности которого меньше или равен Предупреждению (4). Уведомление: Отправляет конкретное сообщение с кодом серьезности меньше или равным Уведомлению (5). Информационное: Отправляет конкретное сообщение с кодом серьезности меньше Информационного (6)

9.6.2 Информация о журнале

Страница информации о журнале выглядит следующим образом, как показано на рисунке ниже.

System Log Information

Auto-refresh ☐ Refresh Clear First Page Previous Page Next Page Last Page

Level All

Clear Level All

Entries For A Given Level: 8

Start From ID: 1 Entries Per Page: 20

ID	Level	Time	Informational
1	Informational	1970-01-01T08:00:07+08:00	SYS-BOOTING: Switch just made a cold boot.
2	Notice	1970-01-01T08:00:07+08:00	LINK-UPDOWN: IP Interface VLAN 1 changed state to down.
3	Notice	1970-01-01T08:00:07+08:00	LINK-UPDOWN: IP Interface VLAN 1 changed state to down.
4	Notice	1970-01-01T08:00:10+08:00	LINK-UPDOWN: Interface G1, changed state to up.
5	Notice	1970-01-01T08:00:12+08:00	LINK-UPDOWN: IP Interface VLAN 1 changed state to up.
6	Notice	1970-01-01T08:12:44+08:00	LINK-UPDOWN: Interface G1, changed state to down.
7	Notice	1970-01-01T08:12:46+08:00	LINK-UPDOWN: IP Interface VLAN 1 changed state to down.
8	Notice	1970-01-01T08:14:31+08:00	LINK-UPDOWN: Interface G1, changed state to up.
9	Notice	1970-01-01T08:14:37+08:00	LINK-UPDOWN: IP Interface VLAN 1 changed state to up.
10	Notice	1970-01-01T08:30:55+08:00	LINK-UPDOWN: Interface G1, changed state to down.
11	Notice	1970-01-01T08:30:58+08:00	LINK-UPDOWN: IP Interface VLAN 1 changed state to down.
12	Notice	1970-01-01T08:30:58+08:00	LINK-UPDOWN: Interface G2, changed state to up.
13	Notice	1970-01-01T08:31:04+08:00	LINK-UPDOWN: IP Interface VLAN 1 changed state to up.
14	Notice	1970-01-01T08:53:51+08:00	LINK-UPDOWN: Interface G2, changed state to down.
15	Notice	1970-01-01T08:53:52+08:00	LINK-UPDOWN: IP Interface VLAN 1 changed state to down.
16	Notice	1970-01-01T08:53:56+08:00	LINK-UPDOWN: Interface G1, 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

- **Start ID:** Поле ввода начального идентификатора позволяет пользователю изменить начальную точку отображаемых элементов, то есть с какого элемента начинать отображение. Если идентификатор существует, элементы будут отображаться начиная с записи с этим идентификатором. Если идентификатор не существует, элементы будут отображаться начиная со следующей ближайшей записи с идентификатором. После ввода нажмите кнопку "Обновить", чтобы изменения вступили в силу.
- **Бары/страница:** Измените количество отображаемых записей на странице через поле ввода "Бары/страница". Максимальное количество записей на странице - 999.
- **Автоматическое обновление:** Когда выбран флажок автоматического обновления, 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.
- Домой: Обновить записи таблицы, начиная с первой доступной записи.
- Предыдущая страница: Обновить записи таблицы с первой в настоящее время отображаемой записью как конечной записью.
- Следующая страница: Обновить записи таблицы, начиная с последней в настоящее время отображаемой записи.
- Последняя страница: Обновить записи таблицы с последней доступной записи как конечной записью.



Примечания:

Четыре кнопки "Домашняя страница, Предыдущая страница, Следующая страница и Последняя страница" немного отличаются от обычно представляемых "домашней страницы, предыдущей страницы, следующей страницы и последней страницы".

9.6.3 Подробные журналы

Страница подробного журнала выглядит следующим образом, как показано на рисунке ниже.



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: Обновляет запись системного журнала до текущего идентификатора записи.
- Домой: Обновляет записи системного журнала до первого доступного идентификатора

записи.

- Предыдущая страница: Обновляет записи системного журнала до предыдущих доступных идентификаторов записей.
- Следующая страница: Обновляет записи системного журнала до следующих доступных идентификаторов записей.
- Последняя страница: Обновляет записи системного журнала до последнего доступного идентификатора записи.

9.7 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.

9.7.1 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



Примечания:

Чем больше нетиповых конфигураций, тем больше времени потребуется на создание файла конфигурации.

9.7.2 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"/> cfm
<input type="radio"/> default-config
<input type="radio"/> 8030ptp-cfm
<input type="radio"/> running-config-8030ptp-default
<input type="radio"/> running-config-8030ptp-ldp-mstp
<input type="radio"/> startup-config

Download Configuration

Описание каждого параметра представлено в следующей таблице:

Параметр	Описание
File name	Имя загружаемого файла конфигурации на коммутаторе.

Параметр	Описание
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



Примечания:

Перед загрузкой текущей рабочей конфигурации необходимо сгенерировать файл конфигурации, поэтому это потребует дополнительного времени.

9.7.3 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

Select File ... No File Selected

Destination File

File Name	Parameters
<input type="radio"/> running-config	<input checked="" type="radio"/> Replace <input type="radio"/> Merge
<input type="radio"/> cfm	
<input type="radio"/> 8030ptp-cfm	
<input type="radio"/> running-config-8030ptp-default	
<input type="radio"/> running-config-8030ptp-lldp-mstp	
<input type="radio"/> startup-config	
<input type="radio"/> New File	<input type="text"/>

Upload Configuration

The description of each parameter item is shown in the following table:

Параметр	Описание
Uploaded file	Загруженный файл
Select a document	Нажмите кнопку "Выбрать файл", чтобы выбрать локальный файл конфигурации для загрузки. После выбора будет отображено имя

Параметр	Описание
	выбранного файла за кнопкой.
Destination file	Целевой файл
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"> • Заменить: полностью заменить текущую рабочую конфигурацию загруженной конфигурацией. • Объединить: объединить загруженную конфигурацию с текущей рабочей конфигурацией. <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..



Примечания:

Файл конфигурации по умолчанию на коммутаторе доступен только для чтения и не может быть заменен.

9.7.4 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
<input type="radio"/> cfm
<input type="radio"/> default-config
<input type="radio"/> 8030ptp-cfm
<input type="radio"/> running-config-8030ptp-default
<input type="radio"/> running-config-8030ptp-lldp-mstp
<input type="radio"/> startup-config

Activate Configuration

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



Примечания:

- 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.

9.7.5 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.

Delete Configuration File

☐ cfm

☐ 8030ptp-cfm

☐ running-config-8030ptp-default

☐ running-config-8030ptp-lldp-mstp

☐ 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



Примечания:

- По умолчанию конфигурация коммутатора 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.

9.8 Перезагрузка

Страница перезагрузки устройства показана на рисунке ниже.

Restart Device

Are you sure you want to perform a restart?

Yes No

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?

Keep Current Static IP Configuration ☒

Yes No

Описание каждого параметра представлено в следующей таблице:

Параметр	Описание
keep current static IP configuration	Конфигурация статического IP-адреса для интерфейса VLAN1 устройства будет сохранена во время сброса к заводским настройкам. В противном случае, IP-адрес устройства будет восстановлен на 192.168.16.253 во время сброса к заводским настройкам. Этот пункт по умолчанию отмечен.

Кнопки

- Да: Нажмите, чтобы восстановить заводскую конфигурацию по умолчанию.
- Нет: Нажмите, чтобы вернуться на главную страницу без восстановления заводской конфигурации по умолчанию.



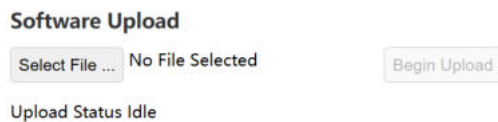
Примечания:

После восстановления коммутатора к заводской конфигурации, новая конфигурация немедленно вступает в силу. Система не будет автоматически перезагружаться, и конфигурация запуска не будет изменена.

9.10 Управление образом

9.10.1 Обновление

Страница обновления образа отображена на рисунке ниже.



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.



Примечания:

- После успешной загрузки файла образа прошивки начнется процесс обновления прошивки. Процесс обновления занимает около минуты, после чего коммутатор автоматически перезагрузится, но не восстановит заводскую конфигурацию.
- Пожалуйста, не перезагружайте коммутатор и не отключайте питание коммутатора во время процесса обновления, иначе коммутатор может работать неправильно.

9.10.2 Образ программного обеспечения.

Страница переключения изображений отображает информацию о компиляции текущего активного изображения и резервного изображения на коммутаторе, включая имя файла изображения, версию прошивки и время компиляции. На этой странице вы можете выбрать,

нужно ли откатиться к предыдущему резервному изображению, как показано на рисунке ниже.

Software Image Selection

Active Image	
Image	MISCOM8030PTP-1.0.62a85c68.240125.img
Date	2024-01-25T17:20:54+08:00

Alternate Image	
Image	MISCOM8030PTP-1.0.0b60d06e.240229.img
Date	2024-02-29T10:42:05+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



Примечания:

Если есть резервный образ, кнопка "Активировать резервный образ" будет активна; в противном случае кнопка будет отключена

10 Ремонт и обслуживание

У компании Wuhan Maiwe Communication Co., Ltd. предоставляется гарантия на продукцию в течение 5 лет с даты отгрузки продукта. Согласно спецификациям продукта Wuhan Maiwe Communication Co., Ltd., в течение гарантийного периода, если продукт имеет какой-либо дефект или отказ в функционировании, Wuhan Maiwe Communication Co., Ltd. обязуется бесплатно провести ремонт или замену продукта для пользователя. Однако указанные обязательства не распространяются на повреждения, вызванные неправильным использованием, авариями, стихийными бедствиями, неправильной эксплуатацией или неправильной установкой. Для обеспечения получения потребителями положительного

опыта использования продукции Wuhan Maiwe Communication Co., Ltd. им предоставляются следующие методы помощи и решения проблем:

- Интернет-сервисы
- Техническая поддержка по телефону
- Возврат или замена продукции

10.1 Интернет-сервисы

Вы можете получить более полезную информацию и советы по использованию через раздел технической поддержки на веб-сайте компании Wuhan Maiwe Communication Co., Ltd.

10.2 Техническая поддержка по телефону

Пользователи, использующие продукцию Wuhan Maiwe Communication Co., Ltd., могут обращаться в техническую поддержку офиса Wuhan Maiwe Communication Co., Ltd. Компания имеет профессиональных технических инженеров, которые готовы общаться с вами и помочь вам решить проблему как можно скорее. Проблемы, возникающие при использовании продукта.

10.3 Возврат или замена продукции

Для ремонта, замены или возврата продукции следуйте процедурам Wuhan Maiwe Communication Co., Ltd. Сначала уточните с техническим персоналом Wuhan Maiwe Communication Co., Ltd., а затем согласуйте с продажами Wuhan Maiwe Communication Co., Ltd., чтобы завершить ремонт, замену или возврат продукции.

Приложение А: Список фильтров сервопривода

Список фильтров сервопривода (эта форма предоставлена третьей стороной):

FilterName	Profile	DescriptionofUse	PacketRate
aci-basic-phase	None	Фильтр низких частот для фазы, также доступен в ZLS30387	>16pps
aci-basic-phase-low	1588	Фильтр низких частот для фазы, также доступен в ZLS30387	≤16pps
aci-basic-phase-low-synce	None	Фильтр низких частот для фазы с восстановленной частотой через SyncE, также доступен в ZLS30387	≤16pps
aci-basic-phase-synce	None	Фильтр низких частот для фазы с восстановленной частотой через SyncE, также доступен в ZLS30387	>16pps
aci-bc-full-on-path-freq	None	Используется для синхронизированного ТС с базовым фильтром, также доступен в ZLS30387	
aci-bc-full-on-path-phase	G.8275.1	Фильтр низких частот с полосой пропускания 0,1 Гц, также доступен в ZLS30384	16pps
aci-bc-full-on-path-phase-beta	None	Не используется	
aci-bc-full-on-path-phase-q	None	Не используется	
aci-bc-full-on-path-phase-synce	G.8275.1	Частота восстановлена через SyncE, а фаза восстановлена через PTP, также доступно в ZLS30384	16pps
aci-bc-partial-on-path-freq	None	Не используется	
aci-bc-partial-on-path-phase	None	Фаза и частота восстановлены через PTP	16pps
aci-bc-partial-on-path-phase-synce	None	Частота восстановлена через SyncE	16pps
aci-default	None	Не используется	
aci-elec-freq	None	Не используется	
aci-elec-phase	None	Не используется	
aci-freq-accuracy-fdd	G.8265.1	PTPunawareforfrequency	64pps
aci-freq-accuracy-xdsl	None	Не используется	
aci-freq-ocxo-s3e	G.8265.1	РТР невероятно для частоты. Локальный ОСХО степень 3Е	64pps
aci-freq-tcxo	G.8265.1	РТР невероятно для частоты. Локальный ТСХО	64pps
aci-freq-xo	G.8265.1	PTPunawareforfrequency.LocalOSCtypeXO	64pps
aci-phase-ocxo-s3e	None	Не используется	

aci-phase-ocxo-s3e-r4-6-1	None	Не используется	
aci-phase-relaxed-c150	None	Не используется	
aci-phase-relaxed-c180	None	Не используется	
aci-phase-relaxed-c240	None	Не используется	
aci-phase-relaxed-c60w	None	Не используется	
aci-phase-tcxo	None	Не используется	
aci-phase-tcxo-q	None	Не используется	
aci-phase-xo	None	Не используется	

maiwe

