

SEWM228GSK промышленный коммутатор

Руководство по настройке



WEB-интерфейс



Оглавление

Введение.....	8
Структура документа	8
Условные обозначения	9
1. Информация об устройстве	10
1.1 Основная информация о коммутаторе.....	10
1.2 Функциональные возможности ПО	10
2. Подключение к устройству	10
2.1 Варианты просмотра и отображения	11
2.2 Подключение через консольный порт	12
2.3 Подключение при помощи Telnet.....	14
2.4 Доступ через WEB-интерфейс.....	15
3. Управление устройством	17
4. Состояние устройства	17
4.1 Основная информация	17
4.2 Состояние портов.....	17
4.3 Статистика портов.....	19
4.4 Информация о работе системы.....	20
5. Базовая конфигурация.....	20
5.1 IP-адрес.....	20
5.2 Основная информация	21
5.3 Настройка портов.....	22
5.4 Изменение пароля.....	25
5.5 Обновления прошивки.....	25
5.5.1 Обновление при помощи FTP.....	25
5.6 Запрос версии программного обеспечения.....	29
5.7 Загрузка/выгрузка конфигурации	29
6. Расширенная конфигурация	30
6.1 Ограничение скорости порта.....	30
6.1.1 Введение.....	30
6.1.2 Настройка с помощью WEB-интерфейса	30
6.1.3 Пример типовой настройки	32
6.2 VLAN	32



6.2.1 Введение.....	32
6.2.2 Принцип работы	33
6.2.3 VLAN на основе портов.....	33
6.2.4 Настройка с помощью WEB-интерфейса	34
6.2.5 Пример типовой настройки	38
6.3 PVLAN	39
6.3.1 Введение.....	39
6.3.2 Настройка с помощью WEB-интерфейса	40
6.3.3 Пример типовой настройки	41
6.4 Зеркалирование портов	42
6.4.1 Введение.....	42
6.4.2 Описание	42
6.4.3 Настройка с помощью WEB-интерфейса	42
6.4.4 Пример типовой настройки	43
6.5 Агрегирование портов.....	44
6.5.1 Введение.....	44
6.5.2 Реализация	44
6.5.3 Описание	45
6.5.4 Настройка с помощью WEB-интерфейса	46
6.5.5 Пример типовой настройки	47
6.6 Проверка связи	48
6.6.1 Введение.....	48
6.6.2 Настройка с помощью WEB-интерфейса	48
6.7 Статическая настройка многоадресной рассылки.....	50
6.7.1 Введение.....	50
6.7.2 Настройка с помощью WEB-интерфейса	50
6.8 IGMP Snooping	52
6.8.1 Введение.....	52
6.8.2 Основные понятия	52
6.8.3 Принцип работы	52
6.8.4 Настройка с помощью WEB-интерфейса	53
6.8.5 Пример типовой настройки	54
6.9 Список управления доступом	55



6.9.1 Введение.....	55
6.9.2 Реализация	55
6.9.3 Настройка с помощью WEB-интерфейса	56
6.9.4 Пример типовой настройки	64
6.10 ARP.....	65
6.10.1 Введение.....	65
6.10.2 Описание	65
6.10.3 Настройка с помощью WEB-интерфейса	65
6.11 SNMP	67
6.11.1 Введение.....	67
6.11.2 Реализация	67
6.11.3 Описание	67
6.11.4 MIB.....	68
6.11.5 Настройка с помощью WEB-интерфейса	69
6.11.6 Пример типовой настройки	71
6.12 Sy2-Ring	71
6.12.1 Введение.....	71
6.12.2 Основные понятия	72
6.12.3 Реализация	72
6.12.4 Пояснение.....	76
6.12.5 Настройка с помощью WEB-интерфейса	76
6.12.6 Пример типовой настройки	81
6.13 STP/RSTP.....	81
6.13.1 Введение.....	82
6.13.2 Основные понятия	82
6.13.3 BPDU	82
6.13.4 Реализация	83
6.13.5 Настройка с помощью WEB-интерфейса	84
6.14 Прозрачная передача RSTP/STP.....	90
6.14.1 Введение.....	90
6.14.2 Настройка с помощью WEB-интерфейса	90
6.14.3 Пример типовой настройки	91
6.15 Sy2-RP.....	92



6.15.1 Введение.....	92
6.15.2 Основные понятия	92
6.15.3 Реализация	94
6.16 DHP	98
6.16.1 Введение.....	98
6.16.2 Основные понятия	99
6.16.3 Реализация	99
6.16.4 Пояснение.....	100
6.16.5 Настройка с помощью WEB-интерфейса	100
6.16.6 Пример типовой настройки	108
6.17 QoS.....	108
6.17.1 Введение.....	108
6.17.2 Принцип работы	109
6.17.3 Настройка с помощью WEB-интерфейса	110
6.17.4 Пример типовой настройки	113
6.18 Время устаревания MAC-адреса	114
6.18.1 Введение.....	114
6.18.2 Настройка с помощью WEB-интерфейса	114
6.19 LLDP	115
6.19.1 Введение.....	115
6.19.2 Настройка с помощью WEB-интерфейса	115
6.20 SNTP.....	116
6.20.1 Введение.....	116
6.20.2 Настройка с помощью WEB-интерфейса	116
6.21 Изоляция портов	119
6.21.1 Введение.....	119
6.21.2 Настройка с помощью WEB-интерфейса	119
6.21.3 Пример типовой настройки	120
6.22 Тревожная сигнализация	120
6.22.1 Введение.....	120
6.22.2 Настройка с помощью WEB-интерфейса	121
6.23 Сигнализация на основе трафика порта	124
6.23.1 Введение.....	124



6.23.2	Настройка с помощью WEB-интерфейса	124
6.24	GMRP	126
6.24.1	Протокол GARP	126
6.24.2	Протокол GMRP	127
6.24.3	Описание	127
6.24.4	Настройка с помощью WEB-интерфейса	127
6.24.5	Пример типовой настройки	131
6.25	RMON	132
6.25.1	Введение.....	132
6.25.2	Группы RMON	133
6.25.3	Настройка с помощью WEB-интерфейса	134
6.26	Системный журнал	138
6.26.1	Введение.....	138
6.26.2	Описание	138
6.26.3	Настройка с помощью WEB-интерфейса	138
6.27	Настройка одноадресной рассылки	140
6.27.1	Введение.....	140
6.27.2	Настройка с помощью WEB-интерфейса	140
6.28	DHCP	142
6.28.1	Настройка сервера DHCP.....	143
6.28.1.1	Введение	143
6.28.1.2	Пул адресов DHCP.....	144
6.28.1.3	Настройка с помощью WEB-интерфейса.....	144
6.28.1.4	Пример типовой настройки.....	150
6.28.2	DHCP Snooping.....	152
6.28.2.1	Введение	152
6.28.2.2	Настройка с помощью WEB-интерфейса.....	152
6.28.2.3	Пример типовой настройки.....	154
6.28.3	Настройка Option 82	154
6.28.3.1	Функция поддержки Option 82 в DHCP Snooping.....	156
6.28.3.1.1	Введение	156
6.28.3.1.2	Настройка с помощью WEB-интерфейса.....	157
6.28.3.2	Функция поддержки Option 82 DHCP-сервером.....	158
6.28.3.2.1	Введение	158



6.28.3.2.2 Настройка с помощью WEB-интерфейса	160
Расшифровка аббревиатур	163



Введение

Данный документ содержит информацию о настройках и возможностях программного обеспечения промышленных коммутаторов серии SEWM228GSK. Кроме того, в документе приводится детальная информация по настройке коммутаторов с помощью WEB-интерфейса.

Структура документа

Данное руководство включает следующую информацию:

Основная информация	Описание
1. Информация о продукте	<ul style="list-style-type: none"> • Описание продукта • Возможности программного обеспечения
2. Способы подключения к устройству	<ul style="list-style-type: none"> • Варианты просмотра и отображения • Подключение через консольный порт • Подключение с использованием Telnet • Подключение через Web-интерфейс
3. Управление	<ul style="list-style-type: none"> • Перезагрузка • Выход из системы
4. Информация о состоянии устройства	<ul style="list-style-type: none"> • Основная информация • Статус портов • Статистика портов • Информация о работе системы
5. Базовые настройки	<ul style="list-style-type: none"> • IP-адрес • Основная информация • Конфигурация порта • Изменение пароля • Обновление программного обеспечения (FTP) • Запрос версии программного обеспечения • Выгрузка/загрузка конфигурации
6. Расширенные настройки	<ul style="list-style-type: none"> • Ограничение скорости порта • VLAN • PVLAN • Зеркалирование портов • Агрегирование портов • Проверка связи • Статическая многоадресная рассылка • IGMP-отслеживание • Список управления доступом • ARP • SNMP • Sy2-Ring • RSTP/STP • Прозрачная передача RSTP/STP • Sy2-RP • QoS • Срок действия MAC-адреса



	<ul style="list-style-type: none"> • LLDP • SNMP • Изоляция портов • Тревожная сигнализация • Сигнализация на основе трафика порта • GMRP • RMON • Системный журнал • Одноадресная рассылка • DHCP
--	--

Условные обозначения

1. Условные обозначения в тексте

Формат	Описание
< >	Скобки < > обозначают «кнопки». Например, нажмите кнопку <Set>
[]	Скобки [] обозначают имя окна или имя меню. Например, нажмите пункт меню [File]
→	Мультиуровневое меню разделяется посредством знака «→». Например, [Start] → [All Programs] → [Accessories]. Нажмите меню [Start], войдите в подменю [All programs], затем войдите в подменю [Accessories]
/	Выбор одной, двух или более опций при помощи символа «/». Например, «Add/Subtract» означает добавить или удалить

2. Условные обозначения CLI

Формат	Описание
Bold	Означает команды и ключевые слова. Например, show version будет показываться с использованием шрифта Bold
<i>Italic</i>	Указывает на значение параметра, которое необходимо ввести. Например, для команды show vlan <i>vlan id</i> вместо <i>vlan id</i> следует вводить актуальный идентификатор VLAN

3. Условные символы

Символ	Описание
 Предостережение	Эти вопросы требуют внимания во время работы с устройством при настройке, а также дают дополнительную информацию
 Заметка	Необходимые пояснения к содержимому выполняемых операций с устройством
 Внимание	Вопросы, требующие особого внимания. Некорректная работа с устройством может привести к потере данных или повреждению



1. Информация об устройстве

1.1 Основная информация о коммутаторе

Коммутаторы серии SEWM228GSK могут использоваться различных отраслях промышленности, таких как энергетика, железнодорожный транспорт, горнодобывающие предприятия и т.д. Они могут эффективно работать в суровых условиях. Коммутаторы поддерживают протоколы резервирования, такие как RSTP, Sy2-Ring и IEC62439-6, обеспечивая надежную работу системы. Внутренняя модульная конструкция обеспечивает гибкое расширение. Коммутаторы серии SEWM228GSK соответствуют стандартам IEC61850-3 и IEEE1613.

1.2 Функциональные возможности ПО

Коммутаторы данной серии предоставляют множество программных функций, удовлетворяющих различным требованиям клиентов:

- Протоколы резервирования: RSTP/STP, Sy2-Ring и IEC62439-6;
- Протоколы многоадресной рассылки: IMGP-Snooping, GMRP, статическая настройка;
- Управление пропускной способностью: агрегирование и ограничение скорости портов;
- Безопасность: ACL, изоляция портов;
- Синхронизация времени: SNTP;
- Управление устройством: обновление при помощи FTP/TFTP, выгрузка/загрузка конфигурации;
- Диагностика устройства: зеркалирование портов, LLDP, проверка канала связи;
- Аварийная сигнализация: ошибка порта, ошибка питания, ошибка кольца, оповещения о высокой или низкой температуре, оповещения о проблемах с трафиком на портах;
- Сетевой доступ к устройству и управление: CLI, Telnet, Web.

2. Подключение к устройству

Устройство можно настраивать одним из нижеперечисленных способов:

- через консольный порт;
- посредством Telnet/SSH;
- с использованием WEB-интерфейса.



2.1 Варианты просмотра и отображения

Когда пользователь (администратор сети) подключается к устройству посредством CLI через консольный порт или Telnet, он имеет возможность, используя различные команды, получать информацию о состоянии устройства и выполнять настройки коммутатора:

Таблица 1 – Режимы настройки

Подсказка	Тип отображения	Функция	Команда
Switch>	Основной режим	<ul style="list-style-type: none"> • Просмотр недавно использованных команд • Просмотр версии программного обеспечения • Просмотр информации об ответе на операцию ping 	Введите «enable» для входа в привилегированный режим
Switch#	Привилегированный режим	<ul style="list-style-type: none"> • Загрузка/выгрузка файла конфигурации • Восстановление конфигурации по умолчанию • Просмотр информации об ответе на операцию ping • Перезапуск коммутатора • Сохранение текущей конфигурации • Отображение текущей конфигурации. • Обновление программного обеспечения 	Введите «configure terminal» для переключения из привилегированного режима в режим настройки Введите «exit» для возврата в основной режим
Switch (config)#	Режим настройки	Настройка всех функциональных возможностей коммутатора	Введите «exit» или «end» для возврата в привилегированный режим

Когда настройка коммутатора выполняется при помощи командной строки (CLI), для получения помощи по используемым командам может использоваться символ «?». Для получения помощи, нужно ввести описание параметров, например, <1,255> означает диапазон чисел, <Н.Н.Н.Н> означает IP адрес, <xx:xx:xx:xx:xx:xx> означает MAC адрес, word<1, 31> означает диапазон строк 1~31. Также символы ↑ и ↓ могут использоваться для просмотра недавно использованных команд.



2.2 Подключение через консольный порт

Пользователь может подключиться к устройству посредством консольного порта с помощью Hyper Terminal операционной системы Windows или с помощью другого программного обеспечения, которое поддерживает подключение по последовательному порту, например, НТТЗ.3. В примере ниже показано, как использовать консольный порт и Hyper Terminal для доступа к коммутатору.

1. Подключите кабель DB9-M12 к ПК и консольному интерфейсу устройства.
2. Запустите HyperTerminal в основном окне Windows, нажмите [Start] → [All Programs] → [Accessories] → [Communications] → [Hyper Terminal] (см. рисунок 1).

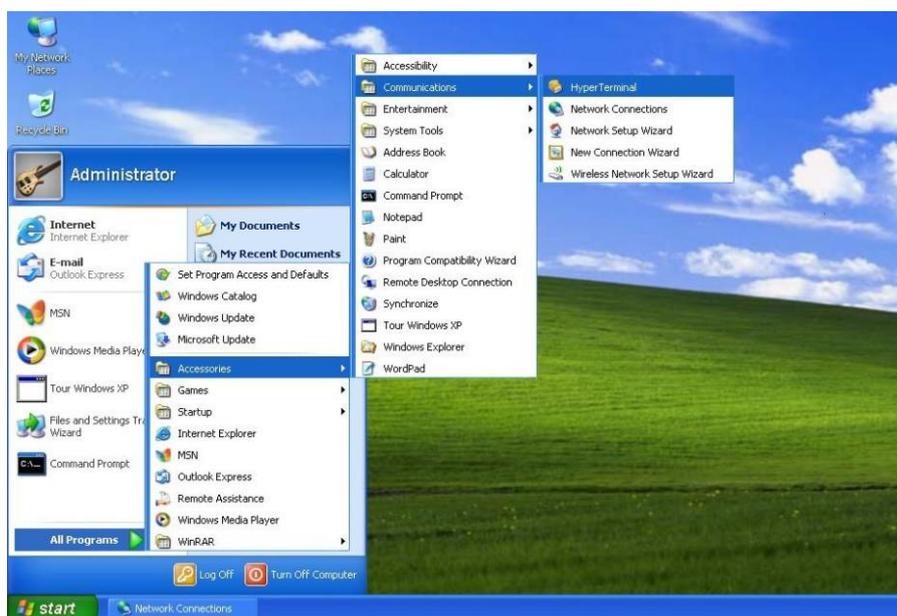


Рисунок 1 – Запуск Hyper Terminal

3. Создайте новое подключение, например, с именем «Switch» (см. рисунок 2).



Рисунок 2 – Создание нового подключения

4. Выберите COM-порт для подключения.



Рисунок 3 – Выбор COM порта для подключения



Чтобы убедиться, что консольный порт выбран верно, проверьте его статус в диспетчере устройств Windows: [My Computer] → [Property] → [Hardware] → [Device Manager] → [Port].

5. Настройте параметры COM порта. Скорость (Bits per second): 9600, биты данных (Data bits): 8, чётность (Parity): None, стоповые биты (Stop bits): 1, управление потоком (Flow control): None, как показано на рисунке 4.

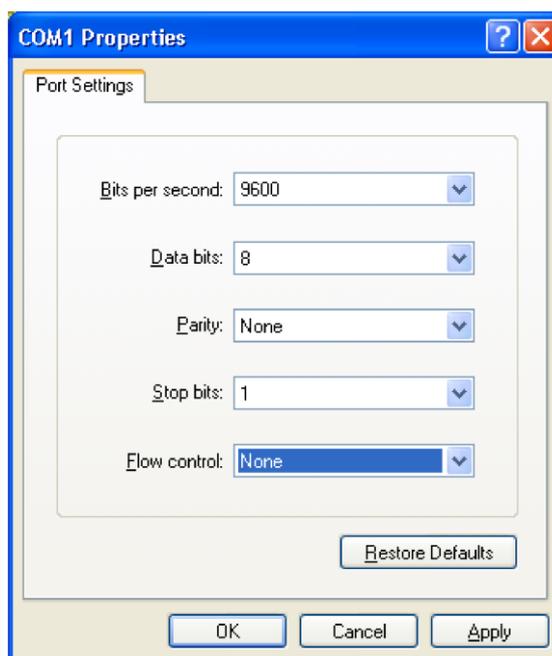


Рисунок 4 – Настройка параметров COM порта

6. Нажмите <OK> для входа в командную строку. Введите пароль «admin» и нажмите <Enter> для входа в основной режим.

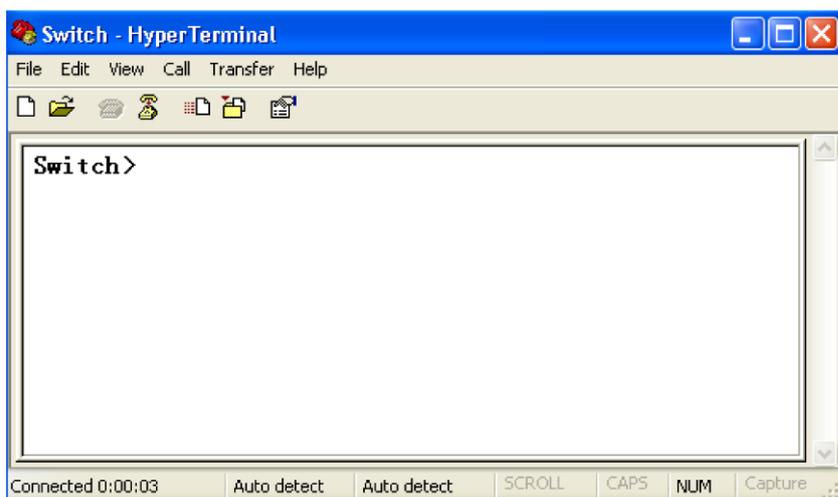


Рисунок 5 – Экран CLI

2.3 Подключение при помощи Telnet

Предварительным условием для доступа к коммутатору через Telnet является устойчивая связь между портами Ethernet ПК и коммутатора.

1. Введите «telnet IP-адрес» в диалоговом окне <Run>, как показано на следующем рисунке:

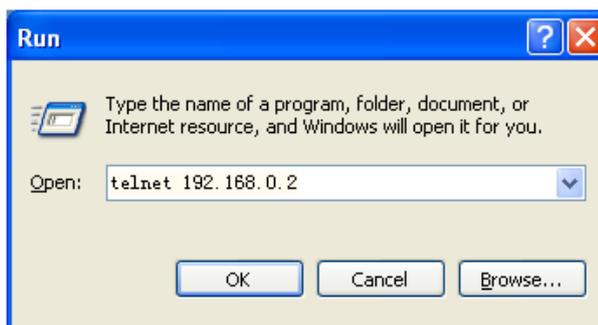


Рисунок 6 – Доступ через Telnet



Для дополнительной информации о подтверждении IP-адреса коммутатора обратитесь к разделу 5.1 настоящего руководства.

2. В интерфейсе Telnet введите имя пользователя «admin» и пароль «123». Нажмите <Enter> для входа.

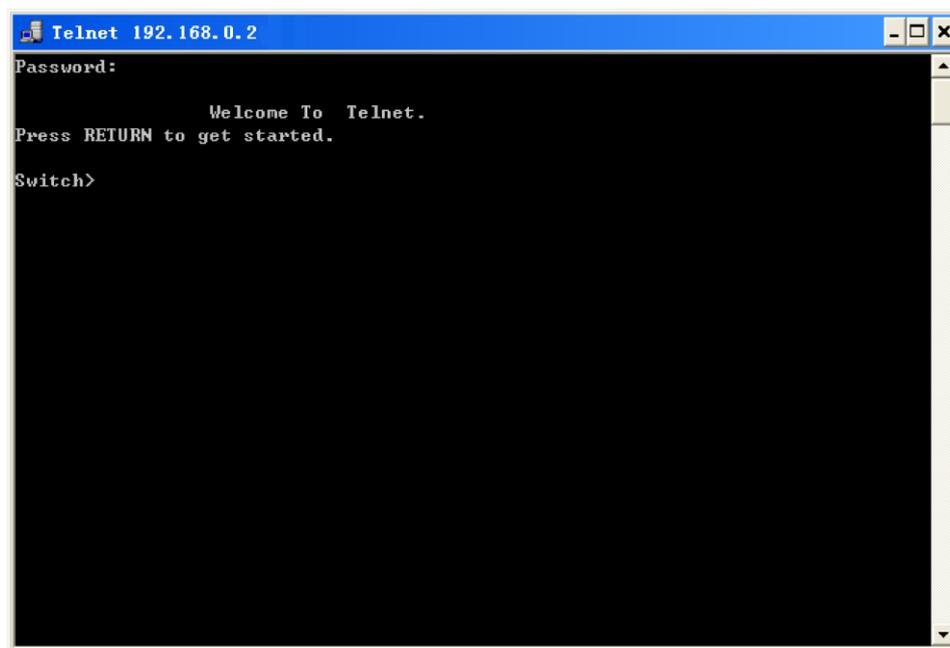


Рисунок 7 – Интерфейс терминала Telnet

2.4 Доступ через WEB-интерфейс

Предварительным условием для доступа к коммутатору через веб-интерфейс является устойчивая связь между портами Ethernet ПК и коммутатора.

1. Введите IP-адрес в адресную строку браузера. Отобразится интерфейс входа в систему, как показано на следующем рисунке. Введите имя пользователя по умолчанию «admin» и пароль «123». Нажмите <Login>.



Рисунок 8 – Вход через веб-интерфейс



Для дополнительной информации о подтверждении IP-адреса коммутатора обратитесь к разделу 5.1 настоящего руководства.

2. После успешного входа в систему в левой части интерфейса появится дерево навигации, как показано на следующем рисунке.

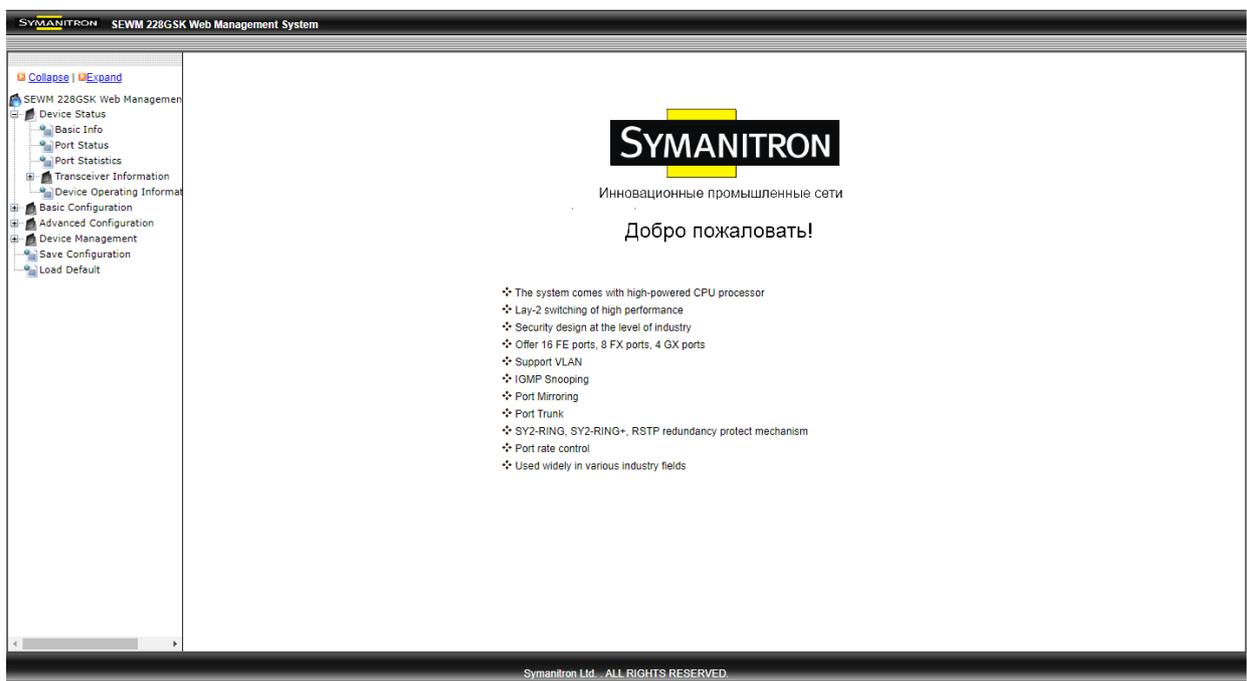


Рисунок 9 – Страница веб-интерфейса

Вы можете развернуть или свернуть дерево навигации, нажав <Expand> или <Collapse> в верхней части дерева навигации. Также можно сохранить конфигурацию или загрузить настройки по умолчанию, нажав [Save Configuration] или [Load Default] в верхнем меню.



После восстановления настроек по умолчанию необходимо перезагрузить устройство, чтобы настройки вступили в силу.

3. Управление устройством

Нажмите [Device Management] → [Reboot]/[Logout], чтобы перезагрузить устройство или выйти из веб-интерфейса. Перед перезагрузкой устройства сохраните текущие настройки по мере необходимости. Если вы сохранили настройки, коммутатор автоматически загрузится с этими настройками после перезапуска. В противном случае после перезагрузки коммутатор восстановит заводские настройки по умолчанию.

4. Состояние устройства

4.1 Основная информация

Основная информация о коммутаторе включает MAC-адрес, серийный номер, IP-адрес, маску подсети, шлюз, имя системы, модель устройства и информацию о версии, как показано на следующем рисунке.

Item	Information
MAC Address	00-00-00-00-19-39
SN	S3MOT12030189
IP Address	192.168.0.22
Subnet Mask	255.255.255.0
GateWay	192.168.0.1
System Name	SWITCH
Device Model	
Software Version	ID:1 R1004 (2023-12-24 14:53)
FW Version	V4.0.2 (2023-7-11 23:33)
Hardware Version	V4.0

Рисунок 10 – Основная информация

4.2 Состояние портов

На странице состояния отображается номер порта, статус администрирования и работы, состояние соединения, скорость, дуплекс и управление потоком, как показано на следующем рисунке.



Port ID	Administration Status	Operation Status	Link	Speed	Duplex	Flow Control	RX	TX
S1/FE1	Enable	Enable	Down	---	---	---	---	---
S1/FE2	Enable	Enable	Down	---	---	---	---	---
S1/FE3	Enable	Enable	Down	---	---	---	---	---
S1/FE4	Enable	Enable	Up	100M	Full-duplex	Off	Enable	Enable
S1/FE5	Enable	Enable	Down	---	---	---	---	---
S1/FE6	Enable	Enable	Down	---	---	---	---	---
S1/FE7	Enable	Enable	Down	---	---	---	---	---
S1/FE8	Enable	Enable	Down	---	---	---	---	---
S4/GE1	Enable	Enable	Down	---	---	---	---	---
S4/GE2	Enable	Enable	Down	---	---	---	---	---
S4/GE3	Enable	Enable	Down	---	---	---	---	---
S4/GE4	Enable	Enable	Down	---	---	---	---	---

Рисунок 11 – Состояние портов

Port ID

Отображение типа и идентификатора портов.

Идентификатор порта имеет формат $S\alpha/\beta$.

α указывает номер слота, в котором находится плата;

β указывает тип порта и идентификатор платы/панели, на которой находится порт.

FE/FX/GE/GX указывают типы портов.

FE: порт 10/100Base-TX RJ45;

FX: порт 100Base-FX;

GE: порт 10/100/1000Base-TX RJ45;

GX: гигабитный слот SFP.

Administration Status

Отображение статуса администрирования портов.

Enable: порт доступен и разрешает передачу данных.

Disable: порт заблокирован, без передачи данных.

Operation Status

Отображение состояния работы портов.

Link

Отображение состояния соединения портов.

Up: порт находится в состоянии соединения и может нормально обмениваться данными.

Down: порт находится в состоянии Link Down и не может нормально обмениваться данными.

Speed

Отображение скорости передачи данных портов в состоянии Link Up.

Duplex

Отображение дуплексного режима работающих портов.



Full-duplex: полнодуплексный режим, порт может одновременно принимать и передавать данные.

Half-duplex: полудуплекс, порт одновременно только принимает или передает данные.

Flow Control

Отображение статуса управления потоком работающих портов.

RX

Отображение статуса приема.

Варианты: Enable/Disable

Enable: порт может принимать данные.

Disable: порт не может принимать данные.

TX

Отображение статуса передачи.

Варианты: Enable/Disable

Enable: порт может передавать данные.

Disable: порт не может передавать данные.



Для дополнительной информации о настройке портов обратитесь к разделу 5.3 настоящего руководства.

4.3 Статистика портов

Статистика портов включает количество байтов/пакетов, которые каждый порт отправляет/получает, ошибки CRC и количество пакетов длиной менее 64 байтов, как показано на следующем рисунке.

Port ID	State	Link	Bytes Sent	Packets Sent	Bytes Received	Packets Received	CRC Error	Packets 64 bytes
S1/FE1	Enable	Down	0	0	0	0	0	0
S1/FE2	Enable	Down	0	0	0	0	0	0
S1/FE3	Enable	Down	0	0	0	0	0	0
S1/FE4	Enable	Up	1670419	7399	14367882	171176	0	0
S1/FE5	Enable	Down	0	0	0	0	0	0
S1/FE6	Enable	Down	0	0	0	0	0	0
S1/FE7	Enable	Down	0	0	0	0	0	0
S1/FE8	Enable	Down	0	0	0	0	0	0
S4/GE1	Enable	Down	0	0	0	0	0	0
S4/GX2	Enable	Down	0	0	0	0	0	0
S4/GE3	Enable	Down	0	0	0	0	0	0
S4/GE4	Enable	Down	0	0	0	0	0	0

Reset

Рисунок 12 – Статистика портов



Чтобы очистить данные статистики и возобновить их сбор с текущего момента, нажмите <Reset>.

4.4 Информация о работе системы

Информация о работе системы включает время работы устройства, загрузку ЦП, использование памяти, температуру устройства и локальное системное время, как показано на следующем рисунке.

Device Operating	
Device Operating Time:	1Days,0H:35M:50S
CPU Usage:	2%(30 seconds), 1%(5 minutes)
Memory Usage:	68%
Device Temperature:	+33C
Device Time:	2023.01.20 20:20:21 Tuesday

Рисунок 13 – Информация о работе системы

5. Базовая конфигурация

5.1 IP-адрес

1. Просмотр IP-адреса коммутатора через консольный порт.

Войдите в интерфейс командной строки через консольный порт коммутатора. Запустите команду **show interface** в привилегированном режиме, чтобы просмотреть IP-адрес коммутатора, как показано на следующем рисунке. IP-адрес обведен красным.

```

Switch - HyperTerminal
File Edit View Call Transfer Help
Switch>enable
No password set!
Switch#show interface
eth (unit number 0):
  Flags: (0x8063) UP BROADCAST MULTICAST ARP RUNNING
  Type: ETHERNET_CSMACD
  Internet address: 192.168.0.2
  Netmask 0xffffffff Subnetmask 0xffffffff0
  Net 0xc0a80000 Subnet 0xc0a80000
  Mac 001e.cd10.2338
lo (unit number 0):
  Flags: (0x8069) UP LOOPBACK MULTICAST ARP RUNNING
  Type: SOFTWARE_LOOPBACK
  Internet address: 127.0.0.1
  Netmask 0xff000000 Subnetmask 0xff000000
  Net 0x7f000000 Subnet 0x7f000000

Switch#_
    
```

Рисунок 14 – Отображение IP-адреса коммутатора



2. Настройка IP-адреса.

IP-адрес коммутатора и шлюз можно настроить вручную, как показано на следующем рисунке.

MAC Address	00-1E-CD-10-23-38
IP Address	192.168.0.119
Subnet Mask	255.255.255.0
GateWay	192.168.0.1

Apply

Рисунок 15 – Настройка IP-адреса



- IP-адрес и шлюз должны находиться в одном сегменте сети; в противном случае IP-адрес невозможно изменить.
- Для коммутаторов данной серии изменение IP-адреса вступает в силу сразу, без необходимости перезагрузки.

5.2 Основная информация

Основная информация включает название проекта, имя системы, часовой пояс, местоположение, контактные данные и системное время, как показано на следующем рисунке.

Project Name	PRJNAME
System Name	SWITCH
Time Zone	+3 (Hour) 0 (0-59 Min)
Location	Bunina Str.2
Contact	+7-916-8798888

Apply

Device time					
2023	year	1	month	20	day
20	hour	20	minute	20	second

Apply

Рисунок 16 – Информация об устройстве

Project Name

Диапазон: 1–64 символа.



System Name

Диапазон: 1–32 символа.

Time Zone

Варианты: 0, +1, +2, +3, +4, +5, +6, +7, +8, +9, +10, +11, +12, +13, -1, -2, -3, -4, -5, -6, -7, -8, -9, -10, -11, -12 ч.

0–59 мин.

По умолчанию: 0 часов 0 минут.

Функция: выбор местного часового пояса.

Location

Значение: строка символов с информацией о местоположении.

Диапазон: 1–255 символов

Contact

Значение: строка символов с контактными данными.

Диапазон: 1–32 символа.

Device time

Значение: {ГГГГ, ММ, ДД, ЧЧ, ММ, СС}

Диапазон: ГГГГ (year) находится в диапазоне от 2000 до 2099, ММ (month) от 1 до 12, ДД (day) от 1 до 31, ЧЧ (hour) от 0 до 23, а ММ (minute) и СС (second) от 0 до 59.

Функция: установка системной даты и времени. Коммутатор может продолжать отсчет времени после выключения питания.

5.3 Настройка портов

На странице конфигурации портов вы можете настроить статус, скорость, управление потоком и другие характеристики, как показано на следующем рисунке.

Port ID	Administration Status	Operation Status	Auto	Speed	Duplex	Flow Control	RX	TX	Reset
S1/FE1	Enable	Enable	Enable	100M	Full	Off	Enable	Enable	Noreset
S1/FE2	Enable	Enable	Enable	100M	Full	Off	Enable	Enable	Noreset
S1/FE3	Enable	Enable	Enable	100M	Full	Off	Enable	Enable	Noreset
S1/FE4	Enable	Enable	Enable	100M	Full	Off	Enable	Enable	Noreset
S1/FE5	Enable	Enable	Enable	100M	Full	Off	Enable	Enable	Noreset
S1/FE6	Enable	Enable	Enable	100M	Full	Off	Enable	Enable	Noreset
S1/FE7	Enable	Enable	Enable	100M	Full	Off	Enable	Enable	Noreset
S1/FE8	Enable	Enable	Enable	100M	Full	Off	Enable	Enable	Noreset
S4/GE1	Enable	Enable	Enable	1000M	Full	Off	Enable	Enable	Noreset
S4/GE2	Enable	Enable	Enable	1000M	Full	Off	Enable	Enable	Noreset
S4/GE3	Enable	Enable	Enable	1000M	Full	Off	Enable	Enable	Noreset
S4/GE4	Enable	Enable	Enable	1000M	Full	Off	Enable	Enable	Noreset

Рисунок 17 – Конфигурация портов



Administration Status

Варианты: Enable/Disable

По умолчанию: Enable

Функция: разрешение или запрет передачи данных на порт.

Описание: «Enable» указывает, что порт включен и разрешает передачу данных; «Disable» указывает, что порт отключен и передача данных запрещена. Эта опция напрямую влияет на аппаратное состояние порта и запускает сигналы тревоги, связанные с портом.

Operation Status

Описание: статус работы принудительно выставляется в соответствии со статусом администрирования.

Auto

Варианты: Enable/Disable

По умолчанию: Enable

Функция: настройка статуса автосогласования портов.

Описание: если для параметра «Auto» установлено значение «Enable», скорость порта и дуплексный режим будут автоматически согласовываться в соответствии с условиями подключения порта. Если установлено значение «Disable», скорость и дуплексный режим можно настроить вручную.



- Для портов 10/100/1000Base-T(X) принудительно установлено значение «Enable».
- Для портов 100Base-FX принудительно установлено значение «Disable».

Speed

Варианты: 10M/100M/1000M

Функция: принудительная настройка скорости портов.

Описание: если для параметра «Auto» установлено значение «Disable», можно настроить скорость порта.

Duplex

Варианты: Half/Full

Функция: настройка дуплексного режима портов.

Описание: если для параметра «Auto» установлено значение «Disable», можно настроить дуплексный режим порта.



- Порты 10/100Base-T(X) могут быть настроены на автоматическое согласование, 10M и полнодуплексный режим, 10M и полудуплекс, 100M и полнодуплексный режим или 100M и полудуплекс.



- Порты 100Base-FX принудительно настроены на 100М и полнодуплексный режим.
- Порты 10/100/1000Base-T(X) принудительно настроены на автосогласование.
- Оптоволоконные порты 1000М можно настроить на автоматическое согласование, а также на 1000М и полнодуплексный режим.

Рекомендуется включить автосогласование для каждого порта, чтобы избежать проблем с подключением, вызванных несоответствующей конфигурацией. Если вы хотите принудительно включить скорость/дуплексный режим порта, убедитесь, что данная конфигурация портов на обеих точках подключения одинакова.

Flow Control

Варианты: Off/On

По умолчанию: Off

Функция: включает/выключает функцию управления потоком данных на выбранном порту.

Описание: после включения функции управления потоком порт сообщит отправителю о необходимости замедлить скорость передачи, чтобы избежать потери пакетов из-за алгоритма или протокола, при котором полученный портом поток, превышает размер кэша порта. Если устройства работают в разных режимах дуплекса (Half/Full), то управление потоком у них реализуется по-разному. Если устройства работают в полнодуплексном режиме, принимающая сторона отправит специальный кадр паузы, чтобы сообщить передающей стороне о необходимости прекращения отправки пакетов. Когда отправитель получит кадр паузы, он прекратит отправку пакетов на период времени ожидания, указанный в кадре паузы, и продолжит отправку пакетов после окончания этого периода. Если устройства работают в полудуплексном режиме, они поддерживают управление потоком на основе противодействия. Принимающая сторона создает конфликт или сигнал несущей. Когда отправитель обнаруживает конфликт или несущую волну, он откладывает передачу данных.

RX

Варианты: Enable/Disable

По умолчанию: Enable

Функция: разрешает или запрещает порту принимать данные

Описание: «Enable» указывает, что порт может принимать данные; «Disable» означает, что порт не может принимать данные.

TX

Варианты: Enable/Disable

По умолчанию: Enable

Функция: разрешает или запрещает порту отправлять данные

Описание: «Enable» указывает, что порт может отправлять данные; «Disable» означает, что порт не может отправлять данные.



Reset

Варианты: Reset/Noreset

Функция: разрешает или запрещает порту перезагружаться в случае ошибок

5.4 Изменение пароля

Вы можете изменить пароль для имени пользователя «admin», как показано на следующем рисунке.

User Name	admin
Old Password	•••
New Password	••••••
Confirm Password	••••••

Apply

Рисунок 18 – Изменение пароля

5.5 Обновления прошивки

Обновления программного обеспечения могут помочь коммутатору улучшить его производительность. Для коммутаторов этой серии прошивка содержит версию загрузчика (BootROM) и версию системного программного обеспечения. Загрузчик необходимо обновлять до обновления системного ПО. Если версия BootROM не меняется, можно обновить только версию системного ПО.

Для обновления прошивки требуется FTP-сервер.

5.5.1 Обновление при помощи FTP

Установите FTP-сервер. Ниже в качестве примера для обновления используется программное обеспечение WFTPD.

1. Нажмите [Security] → [Users/Rights]. Откроется диалоговое окно «Users/Rights Security Dialog». Нажмите <New User>, чтобы создать нового пользователя FTP, как показано на рисунке 19. Задайте имя пользователя и пароль. Например, имя пользователя «admin» и пароль «123». Нажмите <OK>.

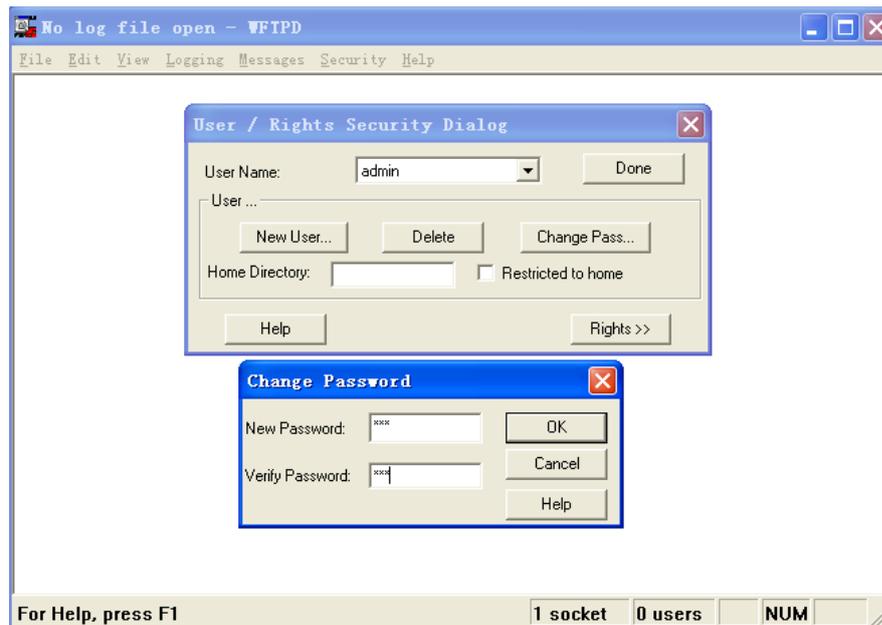


Рисунок 19 – Создание нового пользователя FTP

2. Укажите путь хранения файла с обновлением в «Home Directory», как показано на следующем рисунке. Нажмите <Done>.

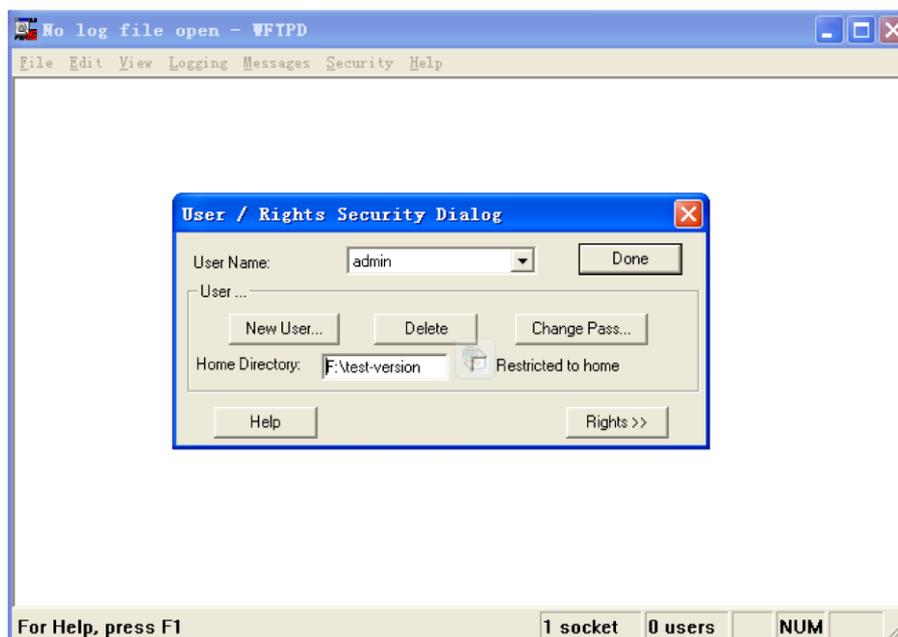


Рисунок 20 – Местоположения файла

3. Чтобы обновить программное обеспечение BootROM, введите следующую команду в привилегированном режиме:

Switch# **update bootrom** *File_name Ftp_server_ip_address User_name Password*

В таблице 2 приведены описания параметров.



Таблица 2 – Параметры для обновления загрузчика через FTP

Параметр	Описание
<i>File_name</i>	Имя файла версии BootROM
<i>Ftp_server_ip_address</i>	IP-адрес FTP-сервера
<i>User_name</i>	Созданное ранее имя пользователя FTP
<i>Password</i>	Созданный ранее пароль FTP

4. На следующем рисунке показана страница обновления программного обеспечения. Введите IP-адрес FTP-сервера, имя файла (на сервере), имя пользователя FTP и пароль. Нажмите <Apply>.

SoftwareID	<input type="text" value="2"/>
FTP Server IP Address	<input type="text" value="192.168.0.23"/>
FTP File Name	<input type="text" value="DC-1.5.5.bin"/>
FTP User Name	<input type="text" value="admin"/>
FTP Password	<input type="password" value="•••"/>

Рисунок 21 – Обновление системного ПО через FTP



Имя файла должно содержать расширение. В противном случае обновление может завершиться неудачно.

5. Убедитесь, что между FTP-сервером и коммутатором установлена нормальная связь, как показано ниже.



```

No log file open - WFTPD
File Edit View Logging Messages Security Help
[L 0132] 09/17/24 14:40:16 Connection accepted from 192.168.0.119
[C 0132] 09/17/24 14:40:16 Command "USER admin" received
[C 0132] 09/17/24 14:40:16 PASSword accepted
[L 0132] 09/17/24 14:40:16 User admin logged in.
[C 0132] 09/17/24 14:40:16 Command "TYPE I" received
[C 0132] 09/17/24 14:40:16 TYPE set to I N
[C 0132] 09/17/24 14:40:16 Command "PASV" received
[C 0132] 09/17/24 14:40:16 Entering Passive Mode [192,168,0,23,8,33]
[C 0132] 09/17/24 14:40:16 Command "RETR DC-1.5.5.bin" received
[C 0132] 09/17/24 14:40:16 RETRIEve started on file DC-1.5.5.bin
[C 0132] 09/17/24 14:41:33 Transfer finished
[G 0132] 09/17/24 14:41:33 Got file D:\TEST-VERSION\V3.1\DC-1.5.5.bin
[C 0132] 09/17/24 14:41:45 Command "QUIT" received
[C 0132] 09/17/24 14:41:45 QUIT or close - user admin logged out

For Help, press F1      1 socket  0 users  NUM
    
```

Рисунок 22 – Проверка связи с сервером FTP



Чтобы отобразить информацию журнала обновлений, как показано на рисунке 22, нужно нажать [Logging] → [Log Options] в WFTPD и выбрать «Enable Logging».

6. Когда обновление будет завершено, перезагрузите устройство и откройте страницу «Switch Basic Information», чтобы проверить, прошло ли обновление успешно и активна ли новая версия.

Result

The software is upgraded successfully!

Рисунок 23 – Успешное обновление ПО через FTP



- В процессе обновления прошивки не отключайте сервер FTP.
- После завершения обновления перезагрузите устройство, чтобы активировать новую версию.
- В случае сбоя обновления не перезагружайте устройство во избежание потери файла прошивки и некорректного запуска устройства.



5.6 Запрос версии программного обеспечения

На коммутатор можно загрузить две версии ПО, но одновременно в активном состоянии может находиться только одна.

Запрашивая версии программного обеспечения, вы можете узнать идентификаторы, даты выпуска и статусы двух версий, как показано на следующем рисунке.

ID	Version	Date	Status
1	R1004	2024-12-24 14:53	Active
2	R1003	2024-7-15 17:32	Inactive

Apply

Рисунок 24 – Запрос версии ПО

5.7 Загрузка/выгрузка конфигурации

Функция резервного копирования конфигурации позволяет сохранять текущие файлы настроек коммутатора на сервере. При нежелательном изменении настроек вы можете скачать исходные файлы конфигурации на коммутатор с сервера FTP.

Выгрузка файлов заключается в отправке конфигурации коммутатора на сервер и ее сохранении в файлах с расширением *.doc и *.txt. Загрузка заключается в скачивании сохраненных файлов конфигурации коммутатора с сервера, как показано на следующих рисунках.



После загрузки файла конфигурации на коммутатор необходимо перезапустить устройство, чтобы конфигурация вступила в силу.

Select Mode	Upload file
FTP Server IP Address	192.168.0.23
FTP File Name	config.txt
FTP User Name	admin
FTP Password	●●●

Apply

Рисунок 25 – Выгрузка файла конфигурации на сервер



Select Mode	Download file
FTP Server IP Address	192.168.0.23
FTP File Name	config.txt
FTP User Name	admin
FTP Password	•••

Apply

Рисунок 26 – Загрузка файла конфигурации на коммутатор

6. Расширенная конфигурация

6.1 Ограничение скорости порта

6.1.1 Введение

Данная функция используется для контроля количества пакетов данных, которые могут быть приняты или переданы через порт в определённый промежуток времени. Если скорость передачи пакетов превышает установленный порог, лишние пакеты будут отброшены. Функция действует на все исходящие пакеты, но только на определенные типы пакетов на входе.

Контролируются следующие входящие пакеты:

- одноадресные пакеты, добавленные статически или пакеты, исходные MAC-адреса которых изучены;
- пакеты многоадресной рассылки, добавленные статически или полученные посредством IGMP Snooping или GMRP;
- зарезервированные многоадресные пакеты с MAC-адресами в диапазоне от 0x0180c2000000 до 0x0180c200002f;
- широковещательные пакеты с MAC-адресом назначения FF:FF:FF:FF:FF:FF;
- неизвестные пакеты многоадресной рассылки, которые не были добавлены статически и не изучены с помощью IGMP Snooping или GMRP;
- неизвестные одноадресные пакеты, которые не были добавлены статически и чьи MAC-адреса источника не изучены;
- пакеты с MAC-адресами неизвестного источника.

6.1.2 Настройка с помощью WEB-интерфейса

1. Выберите типы пакетов, скорость которых будет контролироваться, как показано на следующем рисунке.



The restricted speed is disabled when it is set to 0.

Set Packet Type for Rate Control

Type	Service	Broadcast	Remark
Unicast	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Unicast packet type and address added statically or learned.
Multicast	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Multicast packet type and address added statically or learned through IGMP Snooping.
RSVM	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Mac control frame between 0x0180c2000000~0x0180c200002f.
Broadcast	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Broadcast address.
MLF	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Multicast packet and address not added statically and not learned through IGMP Snooping.
DLF	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Unicast packet type and address not added statically and not through source MAC.
Unknown SA	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Unknown source address in packet.

Рисунок 27 – Типы пакетов для контроля скорости

Приемник коммутатора разделяет управление скоростью передачи данных на два типа: управление скоростью обслуживания и управление скоростью широковещательной передачи. Каждый пакет данных может быть отнесен только к одному типу управления скоростью. Это значит, что для каждого пакета можно выбрать либо ограничение скорости обслуживания, либо ограничение скорости широковещательной передачи, но не оба одновременно.

2. Настройте управление скоростью порта, как показано на следующем рисунке.

Port ID	Service	Broadcast	OutRate
S1/FE1	0 Kbps	0 Kbps	0 Kbps
S1/FE2	70 Kbps	80 Kbps	90 Kbps
S1/FE3	0 Kbps	0 Kbps	0 Kbps
S1/FE4	0 Kbps	0 Kbps	0 Kbps
S1/FE5	0 Kbps	0 Kbps	0 Kbps
S1/FE6	0 Kbps	0 Kbps	0 Kbps
S1/FE7	0 Kbps	0 Kbps	0 Kbps
S1/FE8	0 Kbps	0 Kbps	0 Kbps
S4/GE1	0 Kbps	0 Kbps	0 Kbps
S4/GE2	0 Kbps	0 Kbps	0 Kbps
S4/GE3	0 Kbps	0 Kbps	0 Kbps
S4/GE4	0 Kbps	0 Kbps	0 Kbps

Apply

Рисунок 28 – Настройка управления скоростью порта

Service/Broadcast

Диапазон: 64–1000000Кбит/с

Функция: настройка контроля скорости входящего трафика на порту. Пакеты, скорость которых превышает указанное значение, отбрасываются.



Описание: скорость входящего трафика для порта 100М варьируется от 64 до 100000 Кбит/с. Скорость входящего трафика для порта 1000М варьируется от 64 до 1000000 Кбит/с.

OutRate

Диапазон: 64–1000000Кбит/с

Функция: ограничение скорости пакетов, пересылаемых портом.

Описание: скорость исходящего трафика для порта 100М варьируется от 64 до 100000 Кбит/с. Скорость исходящего трафика для порта 1000М варьируется от 64 до 1000000 Кбит/с.



Если значение скорости установлено на 0, это означает, что управление скоростью порта отключено.

6.1.3 Пример типовой настройки

Установите порог скорости для одноадресных и многоадресных пакетов на порту 2 на 70 Кбит/с, для широковещательных пакетов – на 80 Кбит/с и для исходящего трафика – на 90 Кбит/с.

Процесс настройки:

1. Выберите одноадресные и многоадресные пакеты в столбце «Service» и широковещательные пакеты в столбце «Broadcast», как показано на рисунке 28.
2. На порту 2 установите порог скорости обслуживания на 70 Кбит/с, порог скорости широковещательной передачи на 80 Кбит/с и скорость исходящего трафика в столбце «OutRate» на 90 Кбит/с, как показано на рисунке 28.

6.2 VLAN

6.2.1 Введение

Любая локальная сеть (LAN) может быть разделена на несколько логических виртуальных локальных сетей (VLAN). Устройство при этом может обмениваться данными только с устройствами, находящимися с ним в одной VLAN. В результате широковещательные пакеты ограничиваются своей VLAN, а также оптимизируется безопасность локальной сети.

Разделение на VLAN не ограничено физическим расположением устройств. Каждая VLAN рассматривается как логическая сеть. Если хосту в одной VLAN необходимо отправить пакеты данных на хост в другой VLAN, должен быть задействован маршрутизатор или коммутатор 3-го уровня.



6.2.2 Принцип работы

Чтобы сетевые устройства могли различать пакеты из разных VLAN, в пакеты необходимо добавить поля для идентификации VLAN. В настоящее время наиболее часто используемым протоколом для идентификации VLAN является IEEE802.1Q. В таблице 3 показана структура кадра 802.1Q.

Таблица 3 – Структура кадра 802.1Q

DA	SA	802.1Q Header				Length/Type	Data	FCS
		Type	PRI	CFI	VID			

В обычный Ethernet кадр добавляется 4-байтный заголовок 802.1Q, который служит тегом VLAN. Заголовок 802.1Q включает следующие поля:

Type: 16 бит. Используется для обозначения части кадра, несущего тег VLAN. Значение: 0x8100.

PRI: 3 бита. Обозначает приоритет кадра в соответствии с 802.1p.

CFI: 1 бит. «0» обозначает Ethernet, а «1» – Token Ring.

VID: 12 бит. Обозначает номер VLAN. Диапазон значений: от 1 до 4093. 0, 4094 и 4095 – зарезервированные значения.



- VLAN 1 – это VLAN по умолчанию, ее нельзя создать или удалить.
- VLAN с зарезервированными номерами нужны для системных функций и также не могут быть созданы или удалены.

Кадр, несущий заголовок 802.1Q является тегированным; не несущий заголовка 802.1Q – соответственно, нетегированным.

6.2.3 VLAN на основе портов

Разделение на сети VLAN может быть на основе портов или MAC-адресов. Данная серия коммутаторов поддерживает разделение на основе портов. Устройства, принадлежащие определенному VLAN, распознаются в соответствии с портами коммутатора. После добавления порта в указанную VLAN, он может передавать ее тегированные пакеты.

1. Тип порта.

Порты делятся на два типа в зависимости от того, как они обрабатывают теги VLAN при пересылке пакетов.

Нетегированный (untag) порт: пересылаемые им пакеты не имеют тегов VLAN. Нетегированные порты обычно используются для подключения к терминалам, которые не поддерживают 802.1Q. По умолчанию все порты коммутатора являются нетегированными и принадлежат VLAN1.



Тегированный (tag) порт: все пакеты, пересылаемые через тегированный порт, содержат тег VLAN. Эти порты обычно используются для соединения передающих сетевых устройств.

2. PVID.

Каждый порт имеет PVID (идентификатор VLAN порта). При получении нетегированного пакета порт добавляет к пакету тег в соответствии с PVID. По умолчанию PVID всех портов – VLAN 1.

В следующей таблице показано, как коммутатор обрабатывает полученные и пересылаемые пакеты в зависимости от типа порта и PVID.

Таблица 4 – Различные режимы обработки пакетов

Обработка входящих пакетов		Обработка исходящих пакетов	
Нетегированные пакеты	Тегированные пакеты	Тип порта	Обработка пакетов
Добавление тегов PVID к пакетам	<ul style="list-style-type: none"> ➤ Если VLAN ID пакета есть в списке разрешенных VLAN, пакет принимается ➤ Если VLAN ID пакета отсутствует в списке разрешенных VLAN, пакет отклоняется 	Нетегированный	Отправление пакета после удаления тега
		Тегированный	Сохранение тега и отправление пакета

6.2.4 Настройка с помощью WEB-интерфейса

1. Настройте режим прозрачной передачи VLAN, как показано на следующем рисунке.

Ingress VLAN Filter : Nonmember Drop ▼ Untagged Port VLAN List

PVLAN List	VLAN Group List
<input type="checkbox"/>	default--1

Apply Add

Рисунок 29 – Настройка режима прозрачной передачи VLAN

Ingress VLAN Filter

Варианты: Nonmember Drop/Nonmember Forward

По умолчанию: Nonmember Drop

Функция: настройка режима прозрачной передачи VLAN.



Описание: режим прозрачной передачи определяет, проверяет ли коммутатор входящие на порт пакеты. Когда выбран вариант «Nonmember Drop», пакет отбрасывается, если тег VLAN пакета отличается от VLAN порта. При выборе варианта «Nonmember Forward» пакет принимается, если тег VLAN пакета идентичен тегу любого другого подключенного порта коммутатора; в противном случае пакет отбрасывается.

2. Создайте VLAN.

Нажмите кнопку <Add> (см. рисунок 29), чтобы создать VLAN. Как показано на рисунке 30, выберите порты, которые необходимо добавить в VLAN, и установите параметры порта.

VLAN Name:

VLAN ID:

Port ID	VLAN Member	Priority	PVLAN
S1/FE1	<input type="text" value="Untagged"/>	<input type="text" value="0"/>	<input type="text" value="Disable"/>
S1/FE2	<input type="text" value="Untagged"/>	<input type="text" value="0"/>	<input type="text" value="Disable"/>
S1/FE3	<input type="text" value="-----"/>	<input type="text" value="0"/>	<input type="text" value="Disable"/>
S1/FE4	<input type="text" value="-----"/>	<input type="text" value="0"/>	<input type="text" value="Disable"/>
S1/FE5	<input type="text" value="-----"/>	<input type="text" value="0"/>	<input type="text" value="Disable"/>
S1/FE6	<input type="text" value="-----"/>	<input type="text" value="0"/>	<input type="text" value="Disable"/>
S1/FE7	<input type="text" value="Tagged"/>	<input type="text" value="0"/>	<input type="text" value="Disable"/>
S1/FE8	<input type="text" value="-----"/>	<input type="text" value="0"/>	<input type="text" value="Disable"/>
S2/FE1	<input type="text" value="-----"/>	<input type="text" value="0"/>	<input type="text" value="Disable"/>

Рисунок 30 – Настройка VLAN

VLAN Name

Диапазон: 1–31 символ

Функция: указание имени VLAN.

VLAN ID

Диапазон: 2–4093

Функция: настройка идентификатора VLAN.

Описание: идентификатор используется для распознавания различных VLAN. Коммутаторы этой серии поддерживают максимум 256 VLAN.

VLAN Member

Варианты: Tagged/Untagged

Функция: выбор типа порта в VLAN.

Priority

Диапазон: 0–7



По умолчанию: 0

Функция: установка приоритета порта по умолчанию. При добавлении тега 802.1Q к нетегированному пакету приоритетом является значение поля PRI.

PVLAN

Варианты: Enable/Disable

По умолчанию: Disable

Функция: чтобы добавить тегированный порт в VLAN, вам необходимо включить или отключить PVLAN. Подробную информацию о PVLAN см. в следующей главе.



Нетегированный порт можно добавить только к одной VLAN. Идентификатор VLAN – это PVID порта. Значение по умолчанию – 1. Тегированный порт можно добавить к нескольким VLAN.

3. Просмотрите список VLAN, как показано на следующем рисунке.

Ingress VLAN Filter : Nonmember Drop ▼ Untagged Port VLAN List

PVLAN List	VLAN Group List
<input type="checkbox"/>	default---1
<input type="checkbox"/>	vlan---2
<input type="checkbox"/>	vlan---100
<input type="checkbox"/>	vlan---200

Apply Add

Рисунок 31 – Отображение списка VLAN

PVLAN List

Варианты: select/deselect

Функция: включение или отключение PVLAN. Подробности смотрите в следующей главе.

4. Просмотрите PVID портов.

Нажмите <Untagged Port VLAN List> (см. рисунок 31). Откроется следующая страница.



Port ID	VLAN ID
S1/FE1	2
S1/FE2	2
S1/FE3	100
S1/FE4	100
S1/FE5	200
S1/FE6	200
S1/FE7	1
S1/FE8	1
S2/FE1	1
S2/FE2	1

Рисунок 32 – Список PVID портов



Каждый порт должен иметь атрибут «Untag». Если этот атрибут не задан, то нетегированный порт по умолчанию будет относиться к VLAN 1.

5. Измените или удалите VLAN.

Выберите VLAN в списке (см. рисунок 31). Вы можете изменить или удалить созданную VLAN. Нажмите <Delete> внизу. VLAN можно удалить и напрямую, как показано на следующем рисунке.

VLAN Name :
 VLAN ID :

Port ID	VLAN Member	Priority	PVLAN
S1/FE1	Untagged	0	Disable
S1/FE2	Untagged	0	Disable
S1/FE3	-----	0	Disable
S1/FE4	-----	0	Disable
S1/FE5	-----	0	Disable
S1/FE6	-----	0	Disable
S1/FE7	Tagged	0	Disable
S1/FE8	-----	0	Disable
S2/FE1	-----	0	Disable

Рисунок 33 – Изменение/удаление созданной VLAN



6.2.5 Пример типовой настройки

Как показано на рисунке 34, вся локальная сеть разделена на 3 VLAN: VLAN2, VLAN100 и VLAN200. Требуется, чтобы устройства в одной VLAN могли взаимодействовать друг с другом, но разные VLAN были изолированы. Конечные ПК не могут различать тегированные пакеты, поэтому порты, соединяющие коммутатор А и коммутатор В с ПК, настроены в режиме «Untag». Пакеты VLAN2, VLAN100 и VLAN200 должны передаваться между коммутаторами А и В, поэтому порты, соединяющие коммутаторы, должны быть настроены в режиме «Tag», что позволит пропускать пакеты VLAN 2, VLAN 100 и VLAN 200. В таблице 5 показана соответствующая конфигурация.

Таблица 5 – Настройка VLAN

VLAN	Настройка
VLAN2	Порты 1 и 2 коммутаторов А и В в режиме Untag, а порт 7 в режиме Tag
VLAN100	Порты 3 и 4 коммутаторов А и В в режиме Untag, а порт 7 в режиме Tag
VLAN200	Порты 5 и 6 коммутаторов А и В в режиме Untag, а порт 7 в режиме Tag

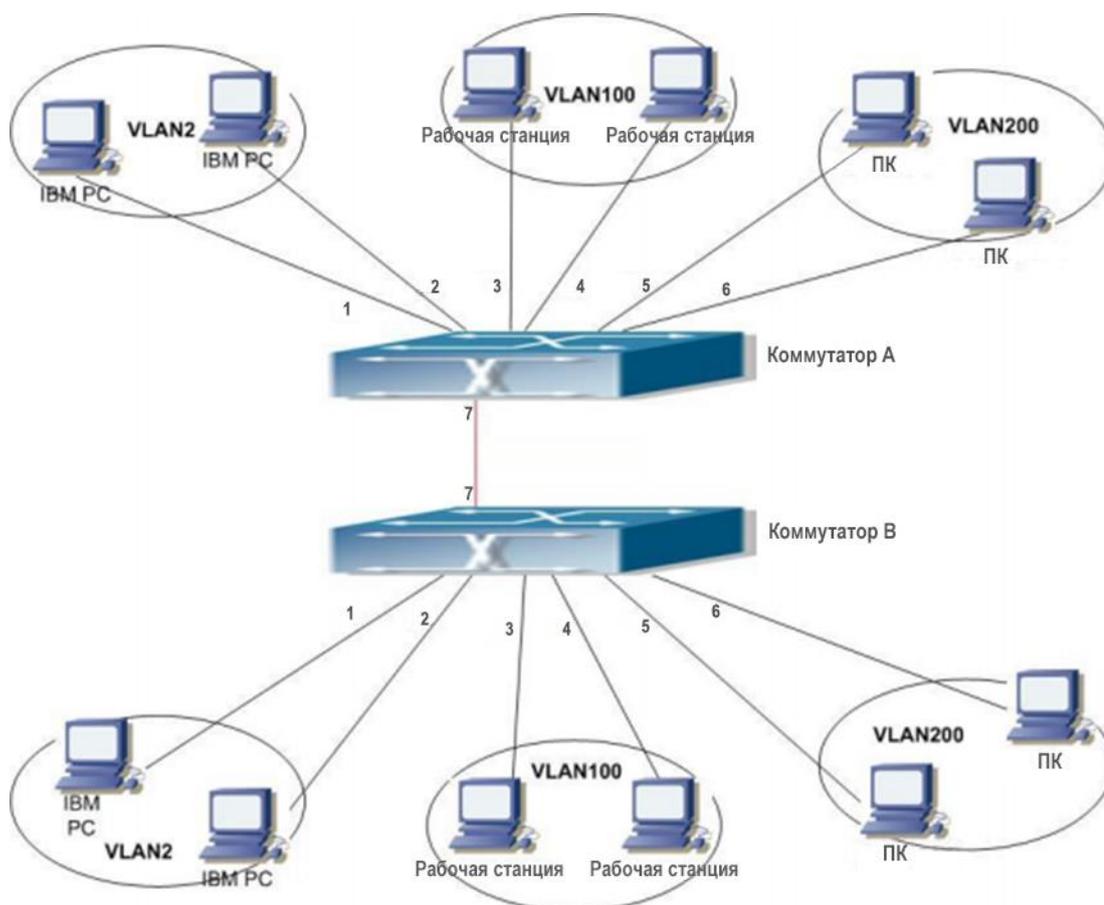


Рисунок 34 – Схема VLAN



Настройка коммутаторов А и В

1. Создайте VLAN 2. Добавьте в нее порт 1 и порт 2 в качестве портов «Untag» и порт 7 в качестве порта «Tag», как показано на рисунке 30.
2. Создайте VLAN 100. Добавьте в нее порт 3 и порт 4 в качестве портов «Untag» и порт 7 в качестве порта «Tag», как показано на рисунке 30.
3. Создайте VLAN 200. Добавьте в нее порт 5 и порт 6 в качестве портов Untag и порт 7 в качестве порта «Tag», как показано на рисунке 30.

6.3 PVLAN

6.3.1 Введение

Частная VLAN (PVLAN) использует двухуровневые технологии для реализации сложной функции изоляции трафика портов, обеспечивая сетевую безопасность и изоляцию широковещательного домена.

Верхняя VLAN – это VLAN общего домена, в которой порты являются портами восходящей линии связи. Нижние сети VLAN представляют собой изолированные домены, в которых порты являются портами нисходящей линии связи. Порты нисходящей линии связи могут быть назначены разным изолированным доменам, и они могут одновременно взаимодействовать с портом восходящей линии связи. Изолированные домены не могут взаимодействовать друг с другом.

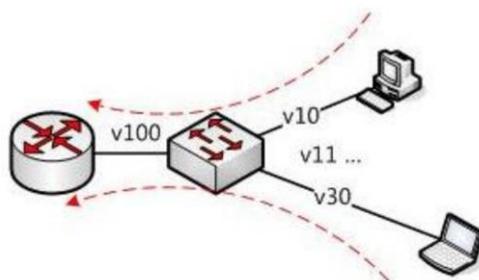


Рисунок 35 – Схема PVLAN

Как показано на рисунке 35, общим доменом является VLAN 100, а изолированными доменами – VLAN 10 и VLAN 30. Устройства в изолированных доменах могут устанавливать соединение с устройством в общем домене, например, VLAN 10 может связываться с VLAN 100; VLAN 30 также может взаимодействовать с VLAN100, но устройства в изолированных доменах не могут устанавливать соединение друг с другом, например, VLAN 10 не может связываться с VLAN 30.



Когда тегированный порт с поддержкой PVLAN пересылает кадр, содержащий тег VLAN, тег VLAN будет удален.



6.3.2 Настройка с помощью WEB-интерфейса

1. Включите PVLAN на порту, как показано на следующем рисунке.

VLAN Name:

VLAN ID:

Port ID	VLAN Member	Priority	PVLAN
S1/FE1	Untagged	0	Disable
S1/FE2	Untagged	0	Disable
S1/FE3	Tagged	0	Enable
S1/FE4	Tagged	0	Enable
S1/FE5	Tagged	0	Enable
S1/FE6	Tagged	0	Enable
S1/FE7	-----	0	Disable
S1/FE8	-----	0	Disable
S4/GE1	-----	0	Disable
S4/GE2	-----	0	Disable
S4/GE3	-----	0	Disable
S4/GE4	-----	0	Disable

Рисунок 36 – Включение PVLAN

Вы можете включить PVLAN на тегированном порту VLAN.

Если VLAN является общим доменом, порт восходящей линии связи будет нетегированным портом, а порт нисходящей линии связи должен быть добавлен в VLAN в качестве тегированного.

Если VLAN является изолированным доменом, порт нисходящей линии связи будет нетегированным портом, а порт восходящей линии связи должен быть добавлен в VLAN в качестве тегированного.

2. Выберите сети VLAN, входящие в PVLAN, как показано на следующем рисунке.

PVLAN List	VLAN Group List
<input type="checkbox"/>	default--1
<input checked="" type="checkbox"/>	vlan--100
<input checked="" type="checkbox"/>	vlan--200
<input checked="" type="checkbox"/>	vlan--300

Рисунок 37 – Выбор участников PVLAN



PVLAN List

Варианты: select/deselect

Функция: выбор участников PVLAN.



Участниками PVLAN являются VLAN как общего, так и изолированного домена.

6.3.3 Пример типовой настройки

На рисунке 38 показан пример настройки PVLAN. VLAN 300 является общим доменом, а порт 1 и порт 2 – портами восходящей линии связи. VLAN 100 и VLAN 200 являются изолированными доменами, а порты 3, 4, 5 и 6 – портами нисходящей линии связи.

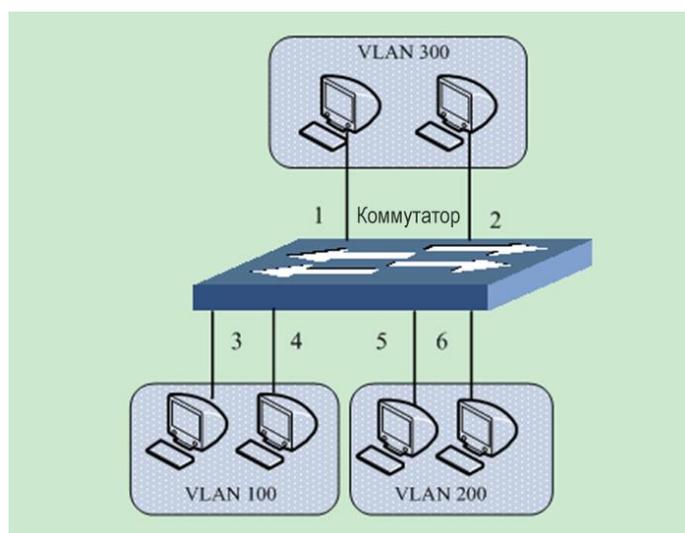


Рисунок 38 – Пример настройки PVLAN

Процесс настройки:

1. Настройте общий домен VLAN 300, как показано на рисунке 36.

Установите порты 1 и 2 в режим «Untag» и добавьте их в VLAN 300.

Установите порты 3 и 4 в режим «Tag» и добавьте их в VLAN 300. Включите PVLAN на обоих портах.

Установите порты 5 и 6 в режим «Tag» и добавьте их в VLAN 300. Включите PVLAN на обоих портах.

2. Настройте VLAN 100 в качестве изолированного домена, как показано на рисунке 36.

Установите порты 1 и 2 в режим «Tag» и добавьте их в VLAN 300. Включите PVLAN на обоих портах.



Установите порты 3 и 4 в режим «Untag» и добавьте их в VLAN 100.

3. Настройте VLAN 200 в качестве изолированного домена, как показано на рисунке 36.

Установите порты 1 и 2 в режим «Tag» и добавьте их в VLAN 200. Включите PVLAN на обоих портах.

Установите порты 5 и 6 в режим «Untag» и добавьте их в VLAN 200.

4. Назначьте VLAN 300, VLAN 100 и VLAN 200 членами PVLAN, как показано на рисунке 37.

6.4 Зеркалирование портов

6.4.1 Введение

При помощи функции зеркалирования портов «Port Mirroring» коммутатор копирует все полученные или переданные кадры данных на одном порту (исходный порт зеркалирования) на другой порт (порт назначения зеркалирования). Порт назначения зеркалирования подключается к анализатору протокола или RMON-монитору для отслеживания сети, управления и диагностики неисправностей.

6.4.2 Описание

Коммутатор поддерживает только один порт назначения для зеркалирования, но несколько портов-источников.

Порты, данные которых зеркалируются, могут быть в одной сети VLAN или в разных. При этом, порты источника и назначения зеркалирования также могут быть в одной или в разных VLAN.

Исходный порт и порт назначения не могут быть одним и тем же портом.



- Порт источника или назначения зеркалирования не может быть добавлен в группу агрегации, а порт из группы агрегации не может быть настроен в качестве порта назначения или источника зеркалирования.
- Порт источника или назначения зеркалирования не может быть настроен в качестве резервного порта, а резервный порт – в качестве порта источника или назначения зеркалирования.

6.4.3 Настройка с помощью WEB-интерфейса

1. Выберите порт назначения зеркалирования, как показано на следующем рисунке.



Рисунок 39 – Выбор порта назначения



Mirroring Port

Варианты: Disable/имя порта

По умолчанию: Disable

Функция: выбор порта, который будет портом назначения зеркалирования. Можно выбрать только один порт.

2. Выберите исходные порты и режим зеркалирования, как показано на следующем рисунке.

Mirrored Port	Mode
<input checked="" type="checkbox"/> S1/FE1	RX & TX
<input type="checkbox"/> S1/FE2	RX
<input checked="" type="checkbox"/> S1/FE3	RX
<input checked="" type="checkbox"/> S1/FE4	TX
<input type="checkbox"/> S1/FE5	RX
<input type="checkbox"/> S1/FE6	RX
<input type="checkbox"/> S1/FE7	RX
<input type="checkbox"/> S1/FE8	RX
<input type="checkbox"/> S4/GE1	RX
<input type="checkbox"/> S4/GE2	RX
<input type="checkbox"/> S4/GE3	RX
<input type="checkbox"/> S4/GE4	RX

Apply

Рисунок 40 – Исходные порты зеркалирования

Mode

Варианты: RX/TX/RX & TX

Функция: выбор данных для зеркалирования.

TX указывает, что зеркалируются только переданные портом пакеты;

RX указывает, что зеркалируются только полученные портом пакеты;

TX&RX указывает, что зеркалируются как переданные, так и полученные портом пакеты.

6.4.4 Пример типовой настройки

Как показано на рисунке 41, порт назначения зеркалирования – это порт 2, а порт источника – порт 1. Как передаваемые, так и принимаемые портом 1 пакеты зеркалируются на порт 2.



Рисунок 41 – Пример зеркалирования портов

Процесс настройки:

1. Настройте порт 2 в качестве порта назначения зеркалирования, как показано на рисунке 39.
2. Настройте порт 1 в качестве порта источника зеркалирования и установите режим зеркалирования на «TX&RX», как показано на рисунке 40.

6.5 Агрегирование портов

6.5.1 Введение

Технология агрегирования предназначена для объединения группы физических портов с одинаковой конфигурацией в один логический порт для увеличения пропускной способности и повышения скорости передачи. Порты-участники одной группы совместно используют трафик и служат друг для друга динамическими резервными копиями, повышая надежность соединения.

6.5.2 Реализация

Как показано на рисунке 42, три порта на коммутаторах А и В объединяются, образуя один агрегированный канал. Пропускная способность такого канала – это общая пропускная способность входящих в него трёх портов.

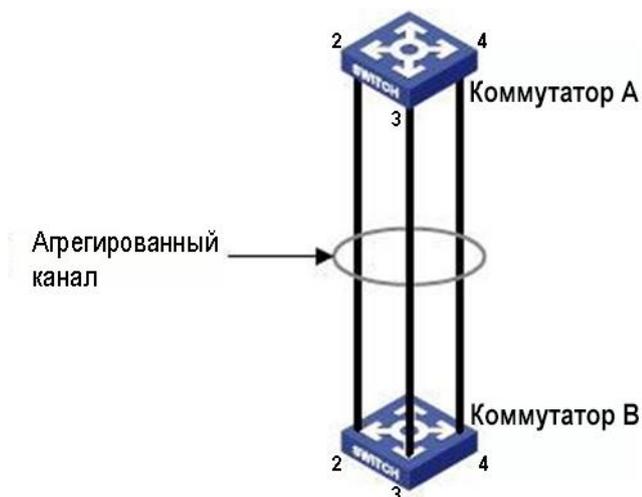


Рисунок 42 – Агрегированный канал

Если коммутатор А отправляет данные на коммутатор В через агрегированный канал, он использует порты группы в соответствии с алгоритмом балансировки нагрузки. Если один из портов группы выходит из строя, данные отправляются через оставшиеся порты также в соответствии с алгоритмом балансировки.

6.5.3 Описание

Группа агрегации и следующие конфигурации портов являются взаимоисключающими.

- Резервирование портов: порт, добавленный в группу агрегации, нельзя настроить как резервный порт, а резервный порт нельзя добавить в группу агрегации.
- Зеркалирование портов: порт, добавленный в группу агрегации, нельзя настроить в качестве порта назначения или источника зеркалирования, а порт назначения или источника зеркалирования нельзя добавить в группу агрегации.
- DHCP-Snooping: порт, добавленный в группу агрегации, не может быть настроен как доверенный порт DHCP-Snooping, а тот, в свою очередь, нельзя добавить в группу агрегации.

Кроме того, не рекомендуется выполнять следующие операции.

- Включать GMRP на порту агрегации.
- Добавлять порт с поддержкой GMRP в группу агрегации.
- Добавлять агрегированный порт в статическую запись одноадресной/многоадресной рассылки.
- Добавлять порт, имеющийся в статической записи одноадресной/многоадресной рассылки в группу агрегации.



- Гигабитные порты коммутаторов данной серии не поддерживают агрегирование.



- Порт можно добавить только в одну группу агрегации.

6.5.4 Настройка с помощью WEB-интерфейса

1. Добавьте группу агрегации.

Нажмите <Add>, чтобы добавить группу, как показано на следующем рисунке.



Рисунок 43 – Добавление группы агрегации

2. Настройте группу агрегации, как показано на следующем рисунке.

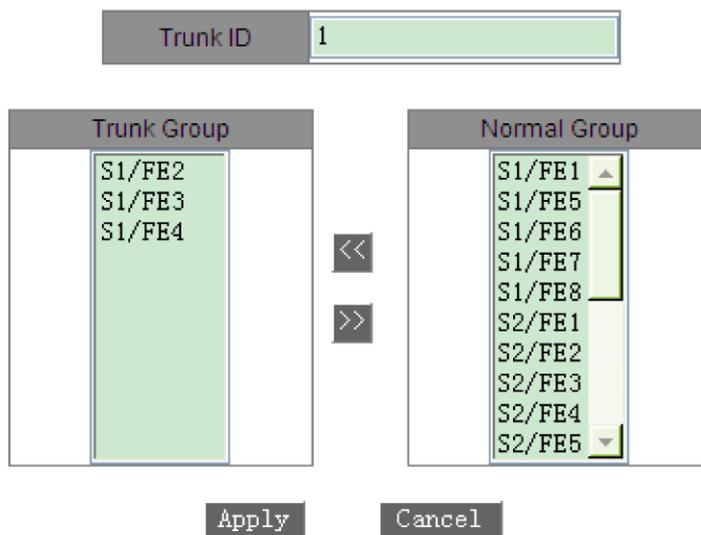


Рисунок 44 – Настройка группы агрегации

Trunk ID

Функция: указание идентификатора группы агрегации.

Описание: коммутаторы данной серии поддерживают до 14 групп. Каждая группа может содержать максимум 4 порта.

3. Просмотрите список групп агрегации, как показано на следующем рисунке.



Trunk List	Member Port	Lock
trunk--1	S1/FE2 S1/FE3 S1/FE4	<input type="checkbox"/>
trunk--2	S1/FE5 S1/FE6 S1/FE7	<input type="checkbox"/>

Add

Apply

Рисунок 45 – Список групп агрегации

Lock

Блокировка портов-членов группы агрегации. После удаления заблокированных портов-участников из группы необходимо вручную включить их, чтобы разблокировать.

Выберите группу агрегации (см. рисунок 45). Вы можете изменить или удалить группу, как показано на следующем рисунке.

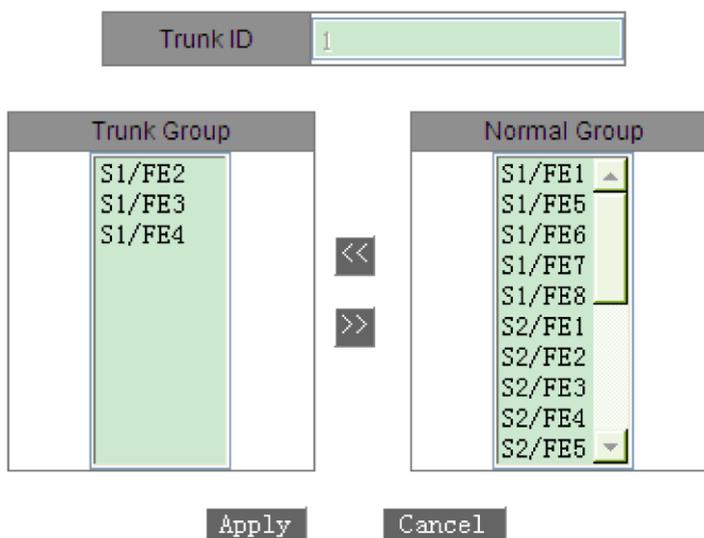


Рисунок 46 – Изменение/удаление группы агрегации

После изменения настроек группы (добавления нового порта в группу или удаления из группы порта-участника) нажмите <Apply>, чтобы изменения вступили в силу. Для удаления группы нажмите <Delete>.

6.5.5 Пример типовой настройки

Как показано на рисунке 42, порт 2, порт 3 и порт 4 коммутатора А подключены к портам коммутатора В соответственно, образуя группу агрегации 1 для достижения балансировки нагрузки между портами.

Процесс настройки:



1. Создайте группу агрегации 1 на коммутаторе А и добавьте в группу порты 2, 3 и 4, как показано на рисунке 44.
2. Создайте группу агрегации 1 на коммутаторе В и добавьте в группу порты 2, 3 и 4, как показано на рисунке 44.

6.6 Проверка связи

6.6.1 Введение

Функция проверки канала связи (Link Check) основана на обмене пакетами протокола для оценки состояния связи и отображения статуса подключения порта. В случае неисправности проблема может быть вовремя обнаружена и устранена.

Порт, для которого включена проверка состояния соединения, периодически (каждую секунду) отправляет контрольные пакеты link-check своему одноранговому устройству. Если порт не получает пакет link-check от удаленного устройства в течение 5 секунд, это означает, что связь не работает, и порт отображает ошибку приема. Если порт получает пакет link-check от удаленного устройства, и в нем содержится подтверждение получения локального пакета в пределах времени ожидания (5 секунд), то порт отображает нормальное состояние. Если же такого подтверждения в пакете удаленного устройства не содержится, локальный порт отображает ошибку передачи.

Порт, для которого отключена проверка состояния связи, работает в пассивном режиме. То есть он самостоятельно не отправляет пакет link-check. Однако после получения такого пакета от удаленного узла он немедленно возвращает свой пакет проверки, чтобы проинформировать удаленный узел о нормальном состоянии связи.



- Функция работает только на портах с включенным протоколом резервирования.
- Если кольцевой/резервный порт Sy2-RP или Sy2-Ring, для которого включена функция проверки канала связи, неисправен (например, ненормальный прием, ненормальная передача или отключение), протокол резервирования блокирует этот порт.

6.6.2 Настройка с помощью WEB-интерфейса

На следующем рисунке показана конфигурация функции проверки связи.



Link Check		
Port	Administration Status	Run Status
S1/FE1	Enable ▾	Normal Link
S1/FE2	Enable ▾	Send Fault
S1/FE3	Enable ▾	Receive Fault
S1/FE4	Disable ▾	Disable
S1/FE5	Disable ▾	Disable
S1/FE6	Disable ▾	Disable
S1/FE7	Disable ▾	Disable
S1/FE8	Disable ▾	Disable
S4/GE1	Disable ▾	Disable
S4/GE2	Disable ▾	Disable
S4/GE3	Disable ▾	Disable
S4/GE4	Disable ▾	Disable

Apply

Рисунок 47 – Окно настройки Link Check

Administration Status

Варианты: Enable/Disable

По умолчанию: Enable

Описание: включение/отключение проверки соединения на порту.



Если удаленное устройство не поддерживает эту функцию, она должна быть отключена на соединенном с ним локальном порту.

Run Status

Варианты: Normal Link/Receive Fault/Disable/Send Fault

Описание: если проверка связи включена для кольцевого порта и порт отправляет и получает данные нормально, отображается сообщение «Normal Link». Если удаленная сторона не получает пакеты обнаружения от устройства, отображается сообщение «Send Fault». Если устройство не получает пакеты обнаружения от удаленной стороны, отображается сообщение «Receive Fault». Если для порта не включена функция проверки канала связи, отображается сообщение «Disable».



6.7 Статическая настройка многоадресной рассылки

6.7.1 Введение

Таблица мультикастовых адресов может быть настроена статически. В таблицу добавляется запись в виде {Multicast MAC address, VLAN ID, Multicast member port}, и сообщения многоадресной рассылки будут перенаправляться на соответствующий порт-участник согласно записи.

Устройство поддерживает до 256 записей многоадресной рассылки.

6.7.2 Настройка с помощью WEB-интерфейса

1. Включите статическую многоадресную рассылку, как показано на следующем рисунке.

The screenshot shows two configuration fields. The first field, 'Multicast Filtrate Mode', has a dropdown menu with 'transmit unknown' selected. The second field, 'FDB Multicast Status', has a dropdown menu with 'Disable' selected. Below these fields is an 'Apply' button.

Рисунок 48 – Включение статической многоадресной рассылки

Multicast Filtrate Mode

Варианты: transmit unknown/drop unknown

По умолчанию: transmit unknown

Функция: настройка режима обработки неизвестных многоадресных пакетов.

Описание: неизвестные пакеты многоадресной рассылки – это пакеты, которые не добавляются вручную и не изучаются с помощью IGMP Snooping или GMRP.

«Transmit unknown» означает, что неизвестные многоадресные пакеты передаются в соответствующих сетях VLAN; «drop unknown» означает, что неизвестные многоадресные пакеты отбрасываются.

FDB Multicast Status

Варианты: Enable/Disable

По умолчанию: Disable

Описание: включение или отключение статической многоадресной рассылки. Статическую многоадресную рассылку и IGMP Snooping нельзя включить одновременно.

2. Добавьте статическую запись многоадресной рассылки, как показано на следующем рисунке.



Static FDB Multicast List Configuration

MAC	<input type="text" value="010101010101"/>	
VLAN ID	<input type="text" value="1"/>	(1-4093)

Port List

Member Port List

S1/FE1

S1/FE2

S1/FE3

<<

>>

Source Port List

S1/FE4 ▲

S1/FE5

S1/FE6

S1/FE7

S1/FE8

S2/FE1

S2/FE2

S2/FE3

S2/FE4

S2/FE5 ▼

Рисунок 49 – Добавление статической записи многоадресной рассылки

MAC

Значение: НННННННННННН (Н – шестнадцатеричное число)

Функция: настройка адреса группы многоадресной рассылки. Младший бит старшего байта равен 1.

VLAN ID

Варианты: все существующие VLAN

Функция: указывает VLAN ID многоадресной записи. Только порты-участники VLAN могут пересылать многоадресные пакеты.

Member Port List

Функция: выбор портов-участников для группы многоадресной рассылки. Если хостам, подключенным к порту, необходимо получать пакеты с данного адреса, вы можете настроить этот порт как порт-участник многоадресной рассылки.

3. Просмотрите, измените или удалите статическую запись многоадресной рассылки, как показано на следующем рисунке.

Static FDB Multicast List

Index	MAC	VLAN ID	Member Port
<input type="radio"/>	03-01-01-01-01-01	2	S1/FE1 S1/FE4
<input type="radio"/>	01-01-01-01-01-01	1	S1/FE1 S1/FE2 S1/FE3

Рисунок 50 – Операции со статической записью многоадресной рассылки



Список статических групповых адресов содержит MAC-адрес, идентификатор VLAN и порт-участник. Чтобы удалить запись, выберите ее и нажмите <Delete>. Чтобы изменить запись, выберите ее и нажмите <Modify>.

6.8 IGMP Snooping

6.8.1 Введение

Internet Group Management Protocol Snooping (IGMP Snooping) – многоадресный протокол второго уровня. Он используется для управления группами многоадресной передачи данных и их настройки. Коммутаторы с поддержкой IGMP Snooping анализируют принимаемые IGMP-пакеты, осуществляют сопоставление между портами и мультикастовыми MAC-адресами и отправляют данные в соответствии с этим сопоставлением.

6.8.2 Основные понятия

Генератор запросов: периодически отправляет IGMP-запросы для проверки и обновления информации о многоадресных группах. Если в сети присутствует несколько запросчиков, они автоматически определяют одного (с наименьшим IP адресом), который непосредственно и будет осуществлять запросы, остальные будут их только получать и передавать.

Маршрутизирующий порт: получает общие запросы (на IGMP-коммутаторе) от главного запрашивающего устройства. При получении IGMP-ответа, коммутатор инициализирует многоадресную группу и добавляет в неё порт, на который пришёл ответ. Если настроен маршрутизирующий порт, он также добавляется. Затем коммутатор ретранслирует IGMP-ответ другим устройствам через маршрутизирующий порт.

6.8.3 Принцип работы

IGMP Snooping управляет участниками групп многоадресной рассылки путём обмена связанными пакетами между поддерживающими IGMP устройствами.

Пакет общего запроса: генератор запросов периодически отправляет общие запросы (с IP адресом назначения 224.0.0.1) для уточнения, есть ли у мультикастовой группы порты-участники. При получении запроса, устройство, не являющееся генератором запросов, ретранслирует пакет на все свои порты.

Пакет конкретного запроса: если устройство хочет покинуть группу многоадресной рассылки, оно отправляет пакет IGMP «leave». После получения такого пакета, запросчик отправляет пакет конкретного запроса (с IP адресом назначения, равным IP адресу мультикастовой группы) для удостоверения, что у коммутатора остались какие-либо порты-участники данной группы.

Пакет отчёта о принадлежности: если устройство хочет получать данные группы многоадресной рассылки, оно отправляет пакет IGMP-оповещения (с IP адресом назначения, равным IP адресу мультикастовой группы) в ответ на IGMP-запрос группы.



Пакет «leave»: если устройство хочет покинуть группу многоадресной рассылки, оно отправляет IGMP-пакет «leave» (с IP адресом назначения: 224.0.0.2).

6.8.4 Настройка с помощью WEB-интерфейса

1. Включите IGMP Snooping, как показано на следующем рисунке.

The screenshot shows three configuration rows. Each row has a label on the left and a dropdown menu on the right. The first row is 'IGMP Snooping Status' with 'Enable' selected. The second row is 'Auto Query Status' with 'Enable' selected. The third row is 'IGMP Cross Status' with 'Enable' selected. Below these rows is a dark button labeled 'Apply'.

Рисунок 51 – Включение IGMP Snooping

IGMP Snooping Status

Варианты: Enable/Disable

По умолчанию: Disable

Функция: включение или отключение IGMP-отслеживания. IGMP Snooping и статическая многоадресная рассылка, а также GMRP не могут быть включены одновременно.

Auto Query Status

Варианты: Enable/Disable

По умолчанию: Disable

Функция: включение или выключение автоматического запроса для выбора запросчика.

Описание: функцию автоматического запроса можно включить только в том случае, если включена функция IGMP Snooping.



Функция автоматического запроса в сети должна быть включена хотя бы на одном коммутаторе.

IGMP Cross Status

Варианты: Enable/Disable

По умолчанию: Disable

Функция: если функция включена, IGMP-пакеты могут пересылаться через кольцевые порты Sy2-Ring.



2. Просмотрите список участников многоадресной рассылки, как показано на следующем рисунке.

MAC	VLAN ID	Member
01-00-5E-7F-FF-FA	1	S1/FE1
01-00-5E-0A-18-03	1	S1/FE1
01-00-5E-51-09-08	1	S1/FE1

Рисунок 52 – Список участников IGMP Snooping

IGMP Member List

Характеристики: {MAC, VLAN ID, Member}

Описание: в таблице многоадресной рассылки FDB, динамически заполняемой посредством IGMP Snooping, VLAN ID – это идентификатор VLAN портов-участников.

6.8.5 Пример типовой настройки

Как показано на рисунке 53, функция IGMP Snooping включена на коммутаторе 1, коммутаторе 2 и коммутаторе 3.

Автоматический запрос разрешен на коммутаторе 2 и коммутаторе 3. IP-адрес коммутатора 2 – 192.168.1.2, а коммутатора 3 – 192.168.0.2, поэтому коммутатор 3 выбран в качестве генератора запросов.

1. Включите IGMP Snooping на коммутаторе 1.
2. Включите IGMP Snooping и автоматический запрос на коммутаторе 2.
3. Включите IGMP Snooping и автоматический запрос на коммутаторе 3.

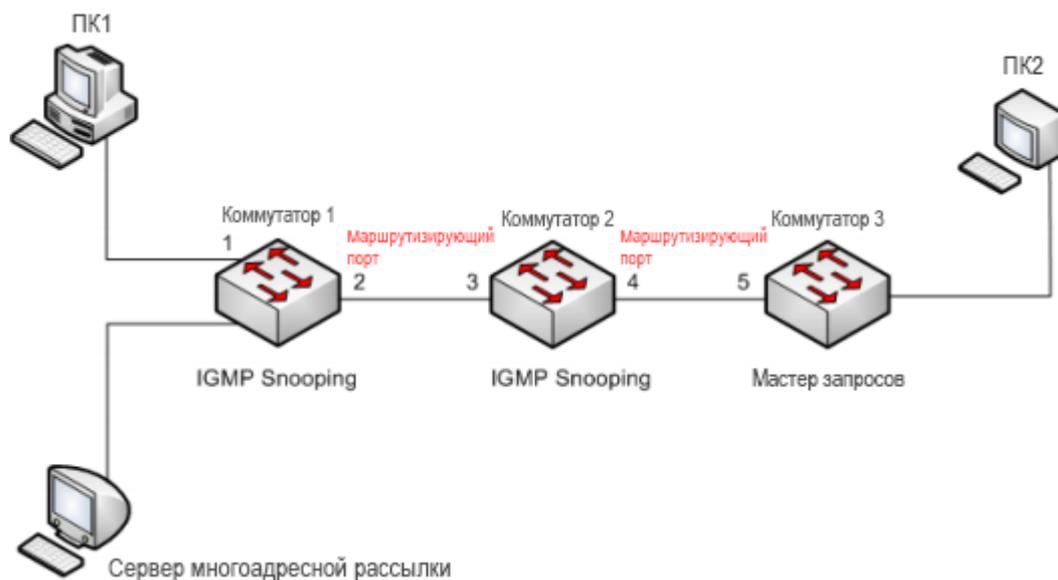


Рисунок 53 – Пример настройки IGMP Snooping



Поскольку коммутатор 3 выбран в качестве мастера запросов, он периодически отправляет сообщение общего запроса. Порт 4 коммутатора 2 принимает пакеты и поэтому выбирается в качестве порта маршрутизации. Коммутатор 2 пересылает пакеты через порт 3. Затем порт 2 коммутатора 1 принимает пакеты и, таким образом, выбирается в качестве порта маршрутизации.

Когда ПК 1 добавляется в группу многоадресной рассылки 225.1.1.1 и отправляет пакеты отчетов IGMP, порт 1 и порт 2 (порт маршрутизации) коммутатора 1 добавляются в группу многоадресной рассылки 225.1.1.1. Пакеты отчетов IGMP пересылаются на коммутатор 2 через порт 2. Затем порт 3 и порт 4 коммутатора 2 также добавляются в многоадресную группу 225.1.1.1. Коммутатор 2 пересылает пакеты отчетов на коммутатор 3 через порт 4. В результате порт 5 коммутатора 3 также добавляется в многоадресную группу 225.1.1.1.

Когда данные сервера многоадресной рассылки достигают коммутатора 1, они будут перенаправлены на ПК1 через порт 1. Поскольку маршрутизирующий порт 2 также является членом группы многоадресной рассылки, данные будут пересылаться через него. Таким образом, когда данные достигают порта 5 коммутатора 3, он прекратит пересылку, потому что получателя больше нет. Но если ПК2 также присоединится к группе 225.1.1.1, многоадресные данные будут перенаправлены на ПК2.

6.9 Список управления доступом

6.9.1 Введение

С развитием сетевых технологий вопросы безопасности становятся все более актуальными, требуя механизма контроля доступа. С помощью функции списка управления доступом (ACL) коммутатор сопоставляет пакеты со списком для реализации запрета и разрешения трафика различных устройств согласно определенным правилам.

6.9.2 Реализация

Коммутаторы данной серии фильтруют пакеты в соответствии с выбранным для сопоставления списком ACL. Каждая запись состоит из нескольких условий в логическом отношении «И». Записи ACL независимы друг от друга.

Коммутатор сравнивает пакет с записями ACL в порядке возрастания идентификаторов записей. Как только совпадение найдено, выполняется действие и дальнейшее сравнение не проводится, как показано на следующем рисунке.

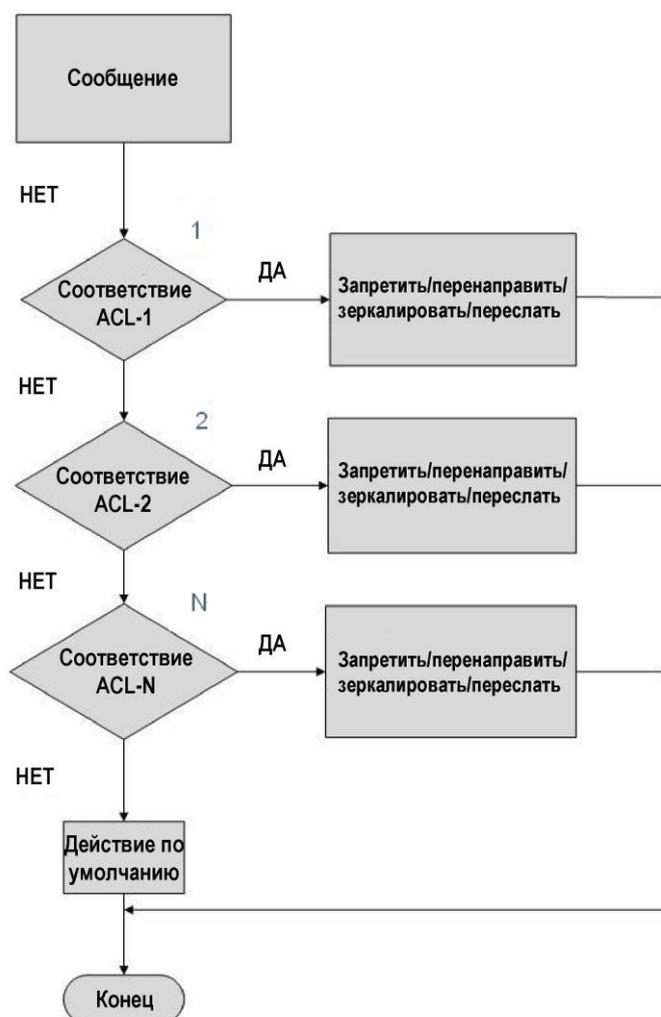


Рисунок 54 – Блок-схема обработки ACL



Действие по умолчанию указывает на режим обработки пакетов, не соответствующих ни одной записи ACL.

6.9.3 Настройка с помощью WEB-интерфейса

1. Добавьте запись ACL.

Нажмите <Add List>, чтобы добавить запись ACL, как показано на следующем рисунке.

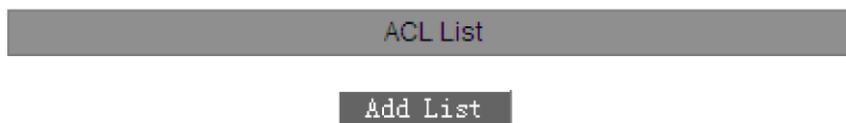


Рисунок 55 – Добавление записи ACL



2. Настройте параметры записи ACL, как показано на следующем рисунке.

Group	1					
Item	1 (1~1018)					
Action	Redir Port					
	S1/FE1					
Controlled Port	All <input type="checkbox"/>					
	S1/FE1	S1/FE2	S1/FE3	S1/FE4	S1/FE5	S1/FE6
	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	S1/FE7	S1/FE8	S2/FE1	S2/FE2	S2/FE3	S2/FE4
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	S2/FE5	S2/FE6	S2/FE7	S2/FE8	S3/FE1	S3/FE2
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
S3/FE3	S3/FE4	S3/FE5	S3/FE6	S3/FE7	S3/FE8	
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
S4/GX1	S4/GX2	S4/GX3	S4/GX4			
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>			
Source MAC	020202020202 MAC					
	ffffffffffff MASK					
Destination MAC	040404040404 MAC					
	ffffffffff00 MASK					
Source IP	192.168.0.202 IP					
	255.255.255.0 MASK					
Destination IP	192.168.0.208 IP					
	255.255.255.0 MASK					

Рисунок 56 – Настройка параметров записи ACL 1

Коммутатор предоставляет ряд параметров для записи ACL. Чтобы завершить их настройку, необходимо нажать <Next>, как показано на следующих рисунках.

Ethernet Type	1537 (1537~65535)	
TOS/DSCP	7 (0~255)	
IP Protocol	6 (0~255)	
IP TTL	2 (0~3)	
Max ICMP	1000 (0~1023)	
TCP Flag	60 (0~63)	
ICMP Type Code	5000 (0~65535)	
Vlan ID	(1~4093)	
Vlan ID Range 0	5 ~ 16	(1~4093)
Vlan ID Range 1	~	(1~4093)
Vlan ID Range 2	~	(1~4093)
Vlan ID Range 3	~	(1~4093)

Рисунок 57 – Настройка параметров записи ACL 2



Source L4 Port	<input type="text" value="65000"/>	(1~65535)
Src Port Range 0	<input type="text"/> ~ <input type="text"/>	(1~65535)
Src Port Range 1	<input type="text"/> ~ <input type="text"/>	(1~65535)
Src Port Range 2	<input type="text"/> ~ <input type="text"/>	(1~65535)
Src Port Range 3	<input type="text"/> ~ <input type="text"/>	(1~65535)
Destination L4 Port	<input type="text" value="21"/>	(1~65535)
Dst Port Range 0	<input type="text"/> ~ <input type="text"/>	(1~65535)
Dst Port Range 1	<input type="text"/> ~ <input type="text"/>	(1~65535)
Dst Port Range 2	<input type="text"/> ~ <input type="text"/>	(1~65535)
Dst Port Range 3	<input type="text"/> ~ <input type="text"/>	(1~65535)
L2 Format	None	▼
L3 Format	None	▼
L4 Format	None	▼
Same IP	Disable	▼
Same L4 Port	Disable	▼
TCP Sequence Zero	Disable	▼

Рисунок 58 – Настройка параметров записи ACL 3

User-Defined Field 0	Value	<input type="text" value="1"/>	(0~65535)
	Base Addr	End of Tag	▼
	Offset	<input type="text" value="4"/>	(0~80 step is 2)
User-Defined Field 1	Value	<input type="text"/>	(0~65535)
	Base Addr	End of Tag	▼
	Offset	<input type="text"/>	(0~80 step is 2)
User-Defined Field 2	Value	<input type="text"/>	(0~65535)
	Base Addr	End of Tag	▼
	Offset	<input type="text"/>	(0~80 step is 2)

Рисунок 59 – Настройка параметров записи ACL 4

Group

Обязательная конфигурация: 1

Item

Диапазон: 1–1018



Функция: установка идентификатора записи ACL. Вы можете настроить максимум 1023 записи ACL. Если настроено несколько записей, они сравниваются с пакетами в порядке возрастания идентификаторов.

Action

Варианты: Deny/Redir Port/Mirror Port/Forward

По умолчанию: Deny

Функция: настройка действия по отношению к пакету, соответствующему записи ACL.

Deny: пакеты, соответствующие записи, будут отклонены.

Redir Port: пакеты, соответствующие записи, будут перенаправлены на указанный порт. Вам необходимо указать порт в выпадающем списке.

Mirror Port: пакеты, соответствующие записи, будут направлены как на порт назначения, так и на порт, указанный в раскрывающемся списке.

Forward: пакеты, соответствующие записи, будут направлены на порт назначения.

Controlled Port

Варианты: все/один или несколько портов

Функция: выбор порта, на котором действует ACL.

Source MAC

Параметры: {MAC, MASK}

Формат: {NNNNNNNNNNNNNN, NNNNNNNNNNNNN} (N – шестнадцатеричное число)

Функция: настройка исходного MAC-адреса и маски подсети. Если MAC-адрес источника и маска подсети пакета совпадают со значением этого параметра, то условие выполнено.

Destination MAC

Параметры: {MAC, MASK}

Формат: {NNNNNNNNNNNNNN, NNNNNNNNNNNNN} (N — шестнадцатеричное число)

Функция: настройка MAC-адреса назначения и маски подсети. Если MAC-адрес назначения и маска подсети пакета совпадают со значением этого параметра, то условие выполнено.

Source IP

Параметры: {IP, MASK}

Формат: {ABCD, ABCCD}

Функция: настройка исходного IP-адреса и маски подсети. Если IP-адрес источника и маска подсети пакета совпадают со значением этого параметра, то условие выполнено.

Destination IP

Параметры: {IP, MASK}

Формат: {ABCD, ABCCD}



Функция: настройка IP-адреса назначения и маски подсети. Если IP-адрес назначения и маска подсети пакета совпадают со значением этого параметра, то условие выполнено.

Ethernet Type

Диапазон: 1537–65535

Функция: настройка типа Ethernet. Если поле «Ethernet Type» пакета идентично значению этого параметра, то условие выполнено.

TOS/DSCP

Диапазон: 0–255

Функция: настройка типа услуги. Если соответствующее поле пакета совпадает со значением этого параметра, то условие выполнено.

IP Protocol

Диапазон: 0–255

Функция: настройка значения протокола IP. Если соответствующее поле пакета совпадает со значением этого параметра, то условие выполнено.

IP TTL

Диапазон: 0–3

Функция: настройка поля TTL. Если значение установлено равным 0, TTL сопоставленного пакета должен быть равен 0; если значение установлено равным 1, TTL сопоставленного пакета должен быть равен 1; если значение установлено равным 2, TTL сопоставленного пакета находится в диапазоне от 2 до 254; если значение установлено равным 3, TTL сопоставленного пакета должен быть равен 255. Если соответствующее поле пакета соответствует этим правилам, то условие выполнено.

Max ICMP

Диапазон: 0–1023

Функция: настройка допустимой длины пакетов ICMP. Если длина данных пакета ICMP больше установленного значения, то условие выполнено.

TCP Flag

Диапазон: 0–63

Функция: настройка флага TCP. Если соответствующее поле пакета совпадает со значением этого параметра, то условие выполнено.

ICMP Type Code

Диапазон: 0–65535

Функция: настройка кода типа ICMP. Если соответствующее поле пакета совпадает со значением этого параметра, то условие выполнено.

Vlan ID

Диапазон: 1–4093



Функция: настройка идентификатора VLAN. Если соответствующее поле пакета совпадает со значением этого параметра, то условие выполнено.

Vlan ID Range (0–3)

Параметры: {X–Y} (X и Y ($X \leq Y$) находятся в диапазоне от 1 до 4093. X и Y обозначают нижний и верхний пределы значений VLAN ID соответственно).

Функция: настройка диапазона VLAN ID пакетов. Условие выполняется, когда идентификатор VLAN пакета находится в указанном диапазоне.

Source L4 Port

Диапазон: 1–65535

Функция: настройка номера исходного порта для пакетов протокола уровня 4. Если соответствующее поле пакета идентично значению, то условие выполнено.

Src Port Range (0–3)

Параметры: {X–Y} (X и Y ($X \leq Y$) находятся в диапазоне от 1 до 65535. X и Y обозначают нижний и верхний пределы номеров исходных портов уровня 4 соответственно).

Функция: настройка диапазона номеров исходных портов для пакетов протокола уровня 4. Если соответствующее поле пакета находится в указанном диапазоне, то условие выполнено.

DestinationL4 Port

Диапазон: 1–65535

Функция: настройка номера порта назначения для пакетов протокола уровня 4. Если соответствующее поле пакета идентично значению, то условие выполнено.

Dst Port Range (0–3)

Параметры: {X–Y} (X и Y ($X \leq Y$) находятся в диапазоне от 1 до 65535. X и Y обозначают нижний и верхний пределы номеров портов назначения уровня 4 соответственно).

Функция: настройка диапазона номеров портов назначения для пакетов протокола уровня 4. Если соответствующее поле пакета находится в указанном диапазоне, то условие выполнено.

L2 Format

Варианты: None/L2_Others/Ethernet_II/IEEE_802_2_SNAP

По умолчанию: None

Функция: настройка формата кадра Ethernet уровня 2. None указывает, что это правило не используется; L2_Others указывает на все остальные форматы кадров Ethernet, кроме Ethernet_II и IEEE_802_2_SNAP. Если формат кадра Ethernet-пакета соответствует указанному значению, условие выполнено.

L3 Format

Варианты: None/L3_Others/IPV4_without_frag/IPV6_without_exten

По умолчанию: None



Функция: настройка интернет-протокола уровня 3. None указывает, что это правило не используется; L3_Others указывает на все интернет-протоколы уровня 3, кроме IPV4_without_frag и IPV6_without_exten. Когда интернет-протокол уровня 3 пакета соответствует указанному значению, условие выполняется.

L4 Format

Варианты: None/L4_Others/TCP/UDP/(ICMP/IGMP)

По умолчанию: None

Функция: настройка типа протокола уровня 4. None указывает, что это правило не используется; L4_Others указывает все протоколы, кроме TCP, UDP, ICMP и IGMP. Если тип пакета протокола уровня 4 соответствует указанному значению, условие выполняется.

Same IP

Варианты: Disable/False/True

По умолчанию: Disable

Функция: проверка, совпадает ли IP-адрес источника пакета с IP-адресом назначения.

Disable указывает, что правило не используется.

False указывает на то, что условие выполняется, если IP-адрес источника пакета отличается от IP-адреса назначения.

True указывает, что условие выполняется, если IP-адрес источника пакета идентичен IP-адресу назначения.

Same L4 Port

Варианты: Disable/False/True

По умолчанию: Disable

Функция: проверка, совпадает ли номер исходного порта уровня 4 пакета с номером порта назначения уровня 4.

Disable указывает, что правило не используется.

False указывает на то, что условие выполняется, если номер исходного порта уровня 4 пакета отличается от номера порта назначения уровня 4.

True указывает, что условие выполняется, если номер исходного порта уровня 4 пакета идентичен номеру порта назначения уровня 4.

TCP Sequence Zero

Варианты: Disable/False/True

По умолчанию: Disable

Функция: проверка, равно ли нулю поле «TCP Sequence» пакета.

Disable указывает, что правило не используется.

False указывает на то, что условие выполняется, если поле «TCP Sequence» пакета не равно нулю.

True указывает, что условие выполняется, если поле TCP Sequence пакета равно нулю.



User-Defined Field (0–2)

Параметры: {Value, Base Addr, Offset}

Диапазон или варианты:

Value: 1–65535

Base Addr: End of Tag (по умолчанию)/End of EthType/End of IP Header

Offset: 0–80, шаг 2

Функция: определяет функцию пользовательского поля как условие ACL. Value указывает значение, которое должно соответствовать значению в пакете данных; Base Addr указывает контрольную точку пакета; End of Tag указывает, что точкой отсчета является конец поля тега; End of EthType указывает, что точкой отсчета является конец поля «EthType»; End of IP Header указывает, что точкой отсчета служит конец поля IP-заголовка; Offset указывает смещение значения относительно контрольной точки. Если смещение соответствует указанному значению Value, то условие считается выполненным.



Не обязательно задавать все эти параметры, но необходимо установить хотя бы один. Если требуется только один параметр, все остальные можно оставить пустыми.

3. Просмотрите список ACL.

ACL List
IPACL--1
IPACL--3
IPACL--70

Add List

Рисунок 60 – Записи ACL

Выберите запись ACL (см. рисунок 60). Затем измените или удалите запись, как показано на следующем рисунке.



Group	1					
Item	1 (1~1020)					
Action	Redir port					
	S1/FE1					
Control Port	All <input type="checkbox"/>					
	S1/FE1	S1/FE2	S1/FE3	S1/FE4	S1/FE5	S1/FE6
	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	S1/FE7	S1/FE8	S2/FE1	S2/FE2	S2/FE3	S2/FE4
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	S2/FE5	S2/FE6	S2/FE7	S2/FE8	S3/FE1	S3/FE2
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	S3/FE3	S3/FE4	S3/FE5	S3/FE6	S3/FE7	S3/FE8
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	S4/GX1	S4/GX2	S4/GX3	S4/GX4		
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		
Source MAC	020202020202 MAC					
	FFFFFFFFFFFF MASK					
Destination MAC	040404040404 MAC					
	FFFFFFFFF00 MASK					
Source IP	192.168.0.202 IP					
	255.255.255.0 MASK					
Destination IP	192.168.0.208 IP					
	255.255.255.0 MASK					

Рисунок 61 – Изменение/удаление записи ACL

Нажмите <Apply>, чтобы изменения вступили в силу после внесения изменений. Нажмите <Delete>, чтобы удалить запись ACL.

6.9.4 Пример типовой настройки

Подключите порт 2 коммутатора. Настройте порт для получения пакетов только с исходного MAC-адреса 02-02-02-02-02-02 и пересылайте пакеты через порт 1.

Процесс настройки:

1. В поле «Action» установите режим «Redir Port» и выберите порт 1 в раскрывающемся списке, как показано на рисунке 56.
2. Выберите FE2 в поле «Control Port», как показано на рисунке 56.
3. Установите MAC-адрес источника 020202020202 и маску подсети FFFFFFFFFF, как показано на рисунке 56.
4. Оставьте все остальные параметры пустыми.



6.10 ARP

6.10.1 Введение

Address Resolution Protocol (ARP) – протокол разрешения адресов, определяющий соответствие между IP-адресом и MAC-адресом через механизм запросов и ответов. Коммутатор может запоминать соответствие между IP-адресом и MAC-адресом устройств в сети. Также коммутаторы поддерживают статические записи ARP, связывающие IP- и MAC-адреса. Динамические ARP-записи периодически устаревают, что обеспечивает обновление информации.

Данные коммутаторы поддерживают не только коммутацию второго уровня, но и ARP-разрешение адресов, обеспечивая взаимодействие между NMS и управляемыми устройствами.

6.10.2 Описание

Записи ARP делятся на статические и динамические.

Динамические записи генерируются и поддерживаются на основании полученных коммутатором ARP-запросов. Динамические записи могут устаревать, обновляться благодаря обмену ARP-запросами и перезаписываться статическими записями.

Статические записи вводятся вручную и также вручную поддерживаются. Они не устаревают и не перезаписываются динамически.

Коммутаторы поддерживают до 512 записей ARP (до 256 статических) Если число ARP-записей превышает 512, новые записи автоматически начинают перезаписывать старые динамические.

6.10.3 Настройка с помощью WEB-интерфейса

1. Настройте время устаревания ARP, как показано на следующем рисунке.

ARP Aging Time

ARP Aging Time 20 (10-60min)

Apply

Рисунок 62 – Настройка времени устаревания

ARP Aging Time

Диапазон: 10–60 минут

По умолчанию: 20 минут

Функция: настройка времени устаревания ARP.

Описание: время устаревания ARP – это продолжительность времени с момента добавления динамической записи ARP в таблицу до момента ее удаления из таблицы.



2. Добавьте статическую запись ARP, как показано на следующем рисунке.

ARP address

IP address	192.168.0.41
MAC address	020000000223

Apply

Рисунок 63 – Добавление статической записи ARP

ARP address

Параметры: {IP address, MAC address}

Формат: {A.B.C.D, НННННННННН}, где Н – шестнадцатеричное число.

Функция: настройка статической записи ARP.



- IP-адрес статической записи ARP должен находиться в том же сегменте сети, что и IP-адрес коммутатора.
- Если IP-адрес статической записи является IP-адресом коммутатора, система автоматически сопоставляет IP-адрес с MAC-адресом коммутатора.
- Как правило, коммутатор автоматически создает и запоминает записи ARP. Ручная настройка не требуется.

3. Просмотрите или удалите запись ARP, как показано на следующем рисунке.

ARP address

Number	IP address	MAC address	Flags
<input type="radio"/>	192.168.0.23	90-FB-A6-3C-CA-7E	Dynamic
<input type="radio"/>	192.168.0.41	02-00-00-00-02-23	Static
<input type="radio"/>	192.168.0.94	00-00-AA-BB-CC-05	Dynamic
<input type="radio"/>	192.168.0.179	00-00-EE-EE-02-05	Dynamic

Add **Delete**

Рисунок 64 – Таблица адресов ARP

ARP-адрес

Параметры: {IP address, MAC address, Flags}

Функция: отображение записей ARP, включая статические и динамические.

Действие: выберите статическую запись в столбце «Number». Нажмите <Delete>, чтобы удалить запись.



Вы не можете удалить динамические записи ARP.

6.11 SNMP

6.11.1 Введение

Simple Network Management Protocol (SNMP) – протокол управления сетевыми устройствами через TCP/IP. Благодаря функции SNMP, администратор может запрашивать информацию об устройстве, менять настройки, следить за состоянием устройства и обнаруживать неполадки сети.

6.11.2 Реализация

Для управления устройствами, SNMP использует архитектуру «station/agent». Таким образом, по функциональности разделяется на два типа: NMS и агент.

- Network Management Station (NMS) – клиент, имеющий программное обеспечение, использующее SNMP. Он является ядром сетевого управления и архитектуры SNMP.
- Агент – это процесс, находящийся в памяти сетевого устройства. Он получает и обрабатывает запросы от NMS. Если возникает неполадка, агент самостоятельно оповещает о ней NMS.

NMS является средством управления сетью SNMP, а агент – частью управляемого устройства. NMS и агенты обмениваются данными, связанными с управлением, через SNMP. Протокол включает следующие основные команды:

- Get-Request
- Get-Response
- Get-Next-Request
- Set-Request
- Trap.

NMS отправляет команды Get-Request, Get-Next-Request и Set-Request для запроса данных, настройки и управления устройством. После получения этих запросов, агенты отвечают командами Get-Response. При возникновении неполадки, агент самостоятельно оповещает о них NMS с помощью trap-сообщения.

6.11.3 Описание

Коммутаторы данной серии поддерживают SNMPv2. SNMPv2 обратно совместима с SNMPv1.



Для аутентификации SNMPv1 использует имя комьюнити. Оно играет роль пароля, ограничивая доступ NMS к агентам. Если имя комьюнити в SNMP запросе неизвестно коммутатору, запрос отклоняется.

SNMPv2 также использует имя комьюнити для аутентификации. Протокол обратно совместим с SNMPv1, при этом расширяя его возможности.

Для поддержки соединения между NMS и агентом, их версии SNMP должны совпадать. На агенте может быть настроена своя версия SNMP, для возможности работы с разными NMS.

6.11.4 MIB

Любой настраиваемый ресурс называется объектом управления. Виртуальная база данных MIB (Management Information Base) хранит в себе все управляемые объекты. Она определяет иерархию объектов и их атрибуты, такие как имя, доступ, тип данных. Каждый агент имеет свою MIB. NMS может считывать и записывать данные в MIB, в зависимости от разрешений. На следующем рисунке показаны взаимосвязи между NMS, агентом и MIB.



Рисунок 65 – Взаимосвязи между NMS, агентом и MIB

MIB представляет из себя древовидную структуру. Узлы дерева являются объектами управления. Каждый узел имеет уникальный идентификатор (Object Identifier – OID), который определяет положение узла в структуре MIB. Как показано на следующем рисунке, OID объекта A равен 1.2.1.1.

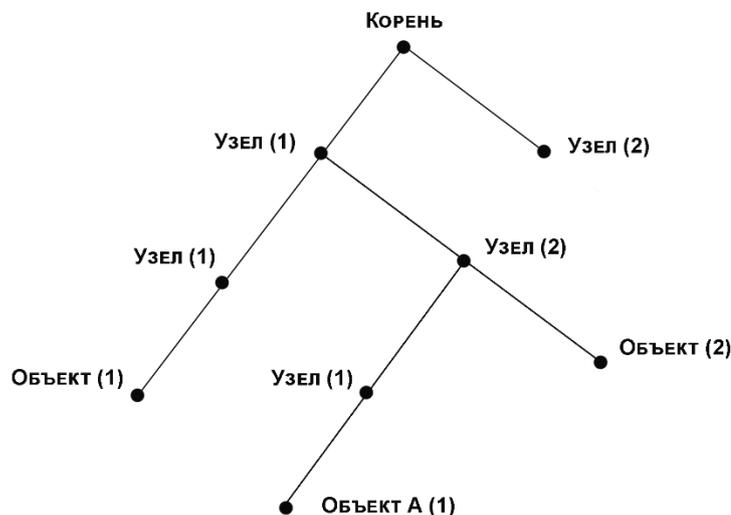


Рисунок 66 – Структура дерева MIB



6.11.5 Настройка с помощью WEB-интерфейса

1. Включите SNMP, как показано на следующем рисунке.

SNMP Status	Enable
-------------	--------

Рисунок 67 – Включение SNMP

SNMP Status

Варианты: Enable/Disable

По умолчанию: Enable

Функция: включение или отключение SNMP.

2. Настройте права доступа, как показано на следующем рисунке.

Read-Only Community	public	(3-16)
Read-Write Community	private	(3-16)
Request Port	161	(1-65535)

Рисунок 68 – Настройка прав доступа

Read-Only Community

Диапазон: 3–16 символов

По умолчанию: public

Функция: настройка имени комьюнити с доступом только для чтения.

Описание: информация MIB коммутатора может быть прочитана только в том случае, если имя комьюнити, передаваемое в пакете SNMP, идентично настроенному на коммутаторе.

Read-Write Community

Диапазон: 3–16 символов

По умолчанию: private

Функция: настройка имени комьюнити с доступом для чтения и записи.

Описание: информация MIB коммутатора может быть прочитана и изменена только в том случае, если имя комьюнити, передаваемое в пакете SNMP, идентично настроенному на коммутаторе.

Request Port

Диапазон: 1–65535



По умолчанию: 161

Функция: настройка номера порта для приема SNMP-запросов.

3. Настройте параметры для trap-сообщений, как показано на следующем рисунке.

Trap Settings

Trap on-off	Enable	
Trap Port ID	162	(1-65535)
Server IP Address1	192.168.0.23	(IP Addr)
Server IP Address2		(IP Addr)
Server IP Address3		(IP Addr)
Server IP Address4		(IP Addr)
Server IP Address5		(IP Addr)

Apply

Рисунок 69 – Настройка trap

Trap on-off

Варианты: Enable/Disable

По умолчанию: Enable

Функция: разрешение или запрет на отправку trap-сообщений.

Trap Port ID

Диапазон: 1–65535

По умолчанию: 162

Функция: настройка номера порта для отправки trap-сообщений.

Server IP Address

Формат: A.B.C.D.

Функция: настройка адреса сервера для получения trap-сообщений. Можно настроить до пяти серверов.

4. Просмотрите IP-адрес сервера управления, как показано на следующем рисунке.

Management Station

Server IP Address1	192.168.0.23	(IP Addr)
Server IP Address2		(IP Addr)
Server IP Address3		(IP Addr)

Рисунок 70 – IP-адрес сервера управления



IP-адрес сервера управления не требует ручной настройки. Коммутатор автоматически отображает его только в том случае, если на сервере работает NMS, считывая и записывая информацию MIB-узла устройства.

6.11.6 Пример типовой настройки

Сервер управления SNMP подключен к коммутатору через Ethernet. IP-адрес сервера управления – 192.168.0.23, а коммутатора – 192.168.0.2. NMS отслеживает и управляет агентом через SNMPv2c, а также считывает и записывает информацию MIB-узла агента. Когда агент неисправен, он сам отправляет trap-сообщения в NMS, как показано на следующем рисунке.

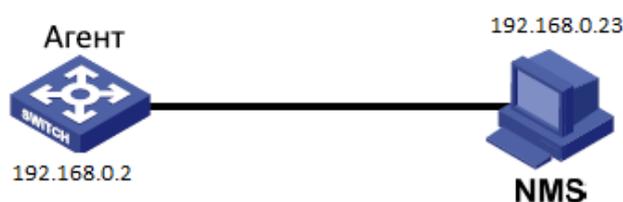


Рисунок 71 – Пример настройки SNMP

Настройка агента:

1. Включите SNMP, как показано на рисунке 78.
2. Настройте права доступа. Для комьюнити с правами на чтение установите режим «public», для комьюнити с правами на чтение и запись – режим «private» Порт приема запросов – 161, как показано на рисунке 68.
3. Разрешите отправку trap-сообщений, установите номер trap-порта 162 и IP-адрес сервера 192.168.0.23, как показано на рисунке 69.

Если вы хотите отслеживать агентские устройства и управлять ими, запустите соответствующее программное обеспечение управления на NMS.

6.12 Sy2-Ring

6.12.1 Введение

Sy2-Ring и Sy2-Ring+ – проприетарные кольцевые протоколы резервирования компании Symanitron. Они позволяют сети восстанавливаться менее чем за 50 мс при обрыве связи, обеспечивая надёжную работу.

Sy2-Ring бывают двух типов: кольцо, основанное на портах (Sy2-Ring-Port), и кольцо, основанное на VLAN (Sy2-Ring-VLAN).

- Sy2-Ring-Port: означает порт, через который необходимо передавать или блокировать данные.



- Sy2-Ring-VLAN: означает порт определённой VLAN, через который необходимо передавать или блокировать данные. Это позволяет настраивать несколько колец, относящихся к разным VLAN, на одном порту.

Sy2-Ring-Port и Sy2-Ring-VLAN нельзя использовать одновременно.

6.12.2 Основные понятия

- Мастер-узел: у одного кольца есть только один мастер. Мастер отправляет пакеты протокола Sy2-Ring и определяет состояние кольца. Когда кольцо замкнуто, два кольцевых порта ведущего устройства находятся в состоянии пересылки и блокировки соответственно.
- Мастер-порт: означает основной кольцевой порт (на ведущем устройстве), который настроен пользователем на принудительную пересылку при замыкании кольца.



Если на ведущем устройстве не настроен основной порт, первый порт, состояние канала которого меняется на «up» при замыкании кольца, находится в состоянии пересылки. Другой кольцевой порт находится в состоянии блокировки.

- Ведомый узел: устройство: кольцо может включать в себя несколько подчиненных устройств. Ведомые устройства прослушивают и пересылают пакеты протокола Sy2-Ring, сообщая информацию об ошибках ведущему устройству.
- Резервный порт: порт для связи между кольцами Sy2-Ring называется резервным портом.
- Главный резервный порт: если кольцо имеет несколько резервных портов, резервный порт с большим MAC-адресом является главным. Он находится в состоянии пересылки.
- Ведомый резервный порт: если кольцо имеет несколько резервных портов, все они, кроме главного, являются ведомыми резервными портами. Они находятся в состоянии блокировки.
- Состояние пересылки: если порт находится в состоянии пересылки, он может как получать, так и отправлять данные.
- Состояние блокировки: если порт находится в состоянии блокировки, он может принимать и пересылать только пакеты протокола Sy2-Ring, но не другие пакеты.

6.12.3 Реализация

Реализация Sy2-Ring-Port

Мастер-порт на мастер-узле периодически отправляет пакеты Sy2-Ring для определения состояния кольца. Если резервный порт мастер-узла получает пакеты, кольцо замкнуто, если нет, то разомкнуто.

Рабочий процесс коммутатора А, коммутатора В, коммутатора С и коммутатора D:



1. Коммутатор А настроен как ведущий (master), а остальные коммутаторы – как ведомые (slave).
2. Кольцевой порт 1 на ведущем устройстве находится в состоянии пересылки, а кольцевой порт 2 – в состоянии блокировки. Оба порта ведомого устройства находятся в состоянии пересылки данных.
3. Канал связи CD неисправен, как показано на рисунке 72.
 - а) Когда канал связи CD неисправен, порты 6 и 7 ведомого устройства находятся в состоянии блокировки. Порт 2 на ведущем устройстве переходит в состояние пересылки данных, обеспечивая нормальную связь.
 - б) Когда неисправность устранена, порты 6 и 7 ведомого устройства находятся в состоянии пересылки. Порт 2 на ведущем устройстве переходит в состояние блокировки. Происходит переключение каналов, и они восстанавливаются до состояния, предшествующего отказу канала CD.



Рисунок 72 – Неисправность канала связи CD



Если порт 1 на ведущем устройстве А настроен как основной порт, процессы сбоя и восстановления после сбоя идентичны описанным выше.

4. Канал связи AC неисправен, как показано на рисунке 73.
 - а) Когда канал AC неисправен, порт 1 находится в состоянии блокировки, а порт 2 переходит в состояние пересылки, обеспечивая нормальную связь.
 - б) После устранения неисправности
 - Если на ведущем устройстве А не настроен мастер-порт, порт 1 все еще находится в состоянии блокировки, а порт 8 – в состоянии пересылки. Никакого переключения не происходит.



- Если порт 1 на ведущем устройстве А настроен как мастер-порт, он должен находиться в состоянии пересылки при замкнутом кольце. Следовательно, он возобновляет передачу данных. Порт 8 находится в состоянии пересылки, а порт 2 – в состоянии блокировки. Происходит переключение каналов.

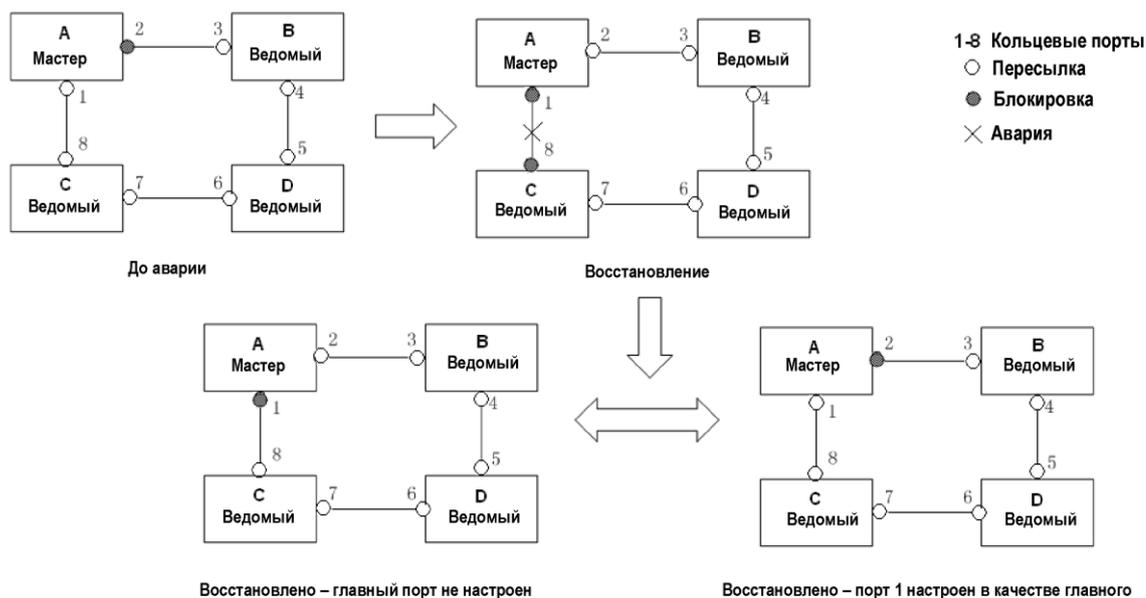


Рисунок 73 – Неисправность канала связи AC



Изменение состояния соединения влияет на состояние кольцевых портов.

Реализация Sy2-Ring-VLAN

Sy2-Ring-VLAN позволяет пересылать пакеты из разных VLAN по разным путям.

Каждый путь пересылки для VLAN образует Sy2-Ring-VLAN. У разных колец Sy2-Ring-VLAN могут быть разные мастер-узлы. Как показано на рисунке 137, настроены две Sy2-Ring-VLAN:

VLAN 10: AB-BC-CD-DE-EA.

VLAN 20: FB-BC-CD-DE-EF.

Два кольца могут объединяться на определённых участках. В данном примере это связи BC, CD и DE. Коммутатор С и коммутатор D используют в двух кольцах одни и те же порты, но разные логические каналы на основе VLAN.

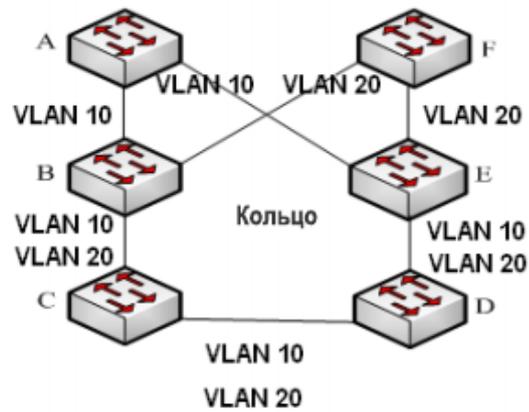


Рисунок 74 – Sy2-Ring-VLAN



В каждом логическом кольце Sy2-Ring-VLAN реализация идентична реализации Sy2-Ring-Port.

Реализация Sy2-Ring+

Sy2-Ring+ может обеспечивать резервирование для двух колец Sy2, как показано на следующем рисунке. Один резервный порт настроен соответственно на коммутаторе С и коммутаторе D. Какой порт является резервным мастер-портом, зависит от MAC-адресов двух портов. Если главный резервный порт или его канал выходят из строя, ведомый резервный порт будет пересылать пакеты, предотвращая образование петель и обеспечивая нормальную связь между резервными кольцами.

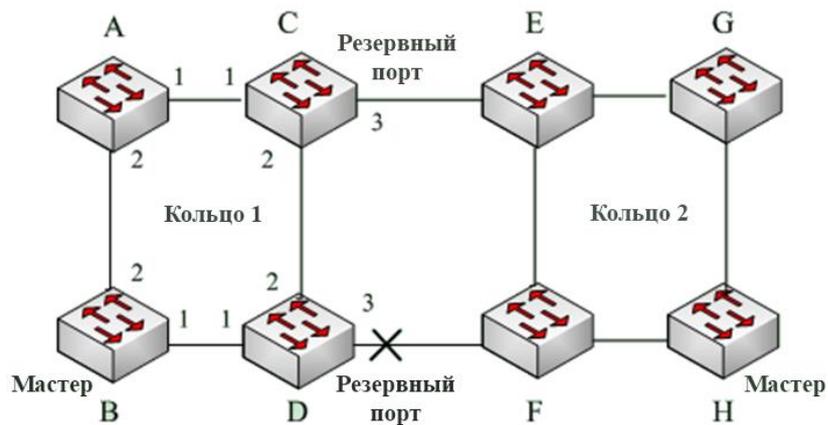


Рисунок 75 – Топология Sy2-Ring+



Изменение состояния соединения влияет на состояние резервных портов.



6.12.4 Пояснение

Конфигурации Sy2-Ring должны соответствовать следующим условиям:

- Все коммутаторы в одном кольце должны иметь одинаковый номер домена.
- В каждом кольце может быть только один мастер-узел и несколько ведомых узлов.
- На каждом коммутаторе можно настроить только два порта для кольца.
- Для двух соединенных колец резервные порты можно настроить только в одном кольце.
- Для одного кольца можно настроить не более двух резервных портов.
- На коммутаторе для одного кольца можно настроить только один резервный порт.
- Sy2-Ring-Port и Sy2-Ring-VLAN нельзя настроить на одном коммутаторе одновременно.

6.12.5 Настройка с помощью WEB-интерфейса

1. Настройте режим кольцевого резервирования, как показано на следующем рисунке.

Select Redundancy Mode	SY2-RING-PORT ▼
Check Loop Status	Disable ▼

Apply

Рисунок 76 – Настройка режима кольцевого резервирования

Select Redundancy Mode

Варианты: SY2-RING-PORT/SY2-RING-VLAN

По умолчанию: SY2-RING-PORT

Функция: выбор режима резервирования.



- К протоколам резервирования на основе портов относятся RSTP, Sy2-Ring-Port и Sy2-RP-Port, а к протоколам на основе VLAN – Sy2-Ring-VLAN и Sy2-RP-VLAN.
- Кольцевые протоколы на основе VLAN являются взаимоисключающими, и для одного устройства можно настроить только тип кольцевого протокола на основе VLAN.
- Кольцевой протокол на основе порта и кольцевой протокол на основе VLAN являются взаимоисключающими, и для одного устройства можно выбрать только один режим кольцевого протокола.

Check Loop Status



Варианты: Disable/Enable

По умолчанию: Disable

Функция: включение или отключение определения состояния кольца.

Описание: после включения данной функции коммутатор автоматически определяет состояние кольца. Когда некольцевой порт получает пакеты Sy2-Ring, он будет заблокирован. Поэтому используйте эту функцию с осторожностью.

2. Создайте кольцо Sy2, как показано на следующем рисунке.

SY2-RING List

Domain ID	Station Type	Ring Port(1,2)	Primary Port	SY2-RING+ Status	Backup Port	Change times
-----------	--------------	----------------	--------------	------------------	-------------	--------------

Add

Рисунок 77 – Создание кольца Sy2

Нажмите <Add> и настройте кольцо Sy2.

3. Настройте Sy2-Ring и Sy2-Ring-VLAN, как показано на следующих рисунках.

Redundancy	SY2-RING
Domain ID	<input type="text" value="1"/>
Domain name	<input type="text" value="a"/>
Station Type	<input type="text" value="Master"/> ▾
Ring Port1	<input type="text" value="S1/FE1"/> ▾
Ring Port2	<input type="text" value="S1/FE1"/> ▾
Primary Port	<input type="text" value="Disable"/> ▾

SY2-RING+

SY2-RING+	<input type="text" value="Enable"/> ▾
Backup Port	<input type="text" value="S1/FE1"/> ▾

Рисунок 78 – Настройка Sy2-Ring



Redundancy	SY2-RING	
Domain ID	<input type="text" value="1"/>	
Domain Name	<input type="text" value="a"/>	
Station Type	Master ▾	
Ring Port1	S1/FE1 ▾	
Ring Port2	S1/FE1 ▾	
Primary Port	Disable ▾	

SY2-RING+		
SY2-RING+	Disable ▾	
Backup Port	S1/FE1 ▾	

Add VLAN List		
VLAN Choose	VLAN ID	VLAN Name
<input type="checkbox"/>	1	default

Рисунок 79 – Настройка Sy2-Ring-VLAN

Redundancy

Обязательная конфигурация: Sy2-RING

Domain ID

Диапазон: 1–32

Функция: дифференциация колец. На одном коммутаторе можно настроить максимум 16 колец на основе портов или 8 колец на основе VLAN.

Domain Name

Диапазон: 1–31 символ

Функция: настройка доменного имени.

Station Type

Варианты: Master/Slave

По умолчанию: Master

Функция: выбор роли коммутатора в текущем кольце.

Ring Port1/Ring Port2

Варианты: все порты коммутатора

Функция: выбор двух кольцевых портов.



- Кольцевой или резервный порт Sy2-Ring нельзя добавить в группу агрегации. Порт, добавленный в группу агрегации, нельзя настроить как кольцевой или резервный порт Sy2-Ring.
- Кольцевой или резервный порт Sy2-Ring нельзя настроить как порт источника или назначения зеркалирования. Порт источника или назначения зеркалирования не может быть настроен как кольцевой или резервный порт Sy2-Ring.
- Настройка портов RSTP, Sy2-Ring-Port и Sy2-RP-Port является взаимоисключающей. То есть, кольцевой или резервный порт Sy2-Ring-Port не должны быть настроены как порт RSTP, Sy2-RP-Port, кольцевой или резервный порт Sy2-RP-Port. Соответственно, порт RSTP, кольцевой и резервный порт Sy2-RP-Port не должны быть настроены как кольцевой или резервный порт Sy2-Ring-Port.
- Не рекомендуется одновременно настраивать порты в группе изоляции как кольцевые и резервные порты Sy2-Ring, а кольцевые и резервные порты Sy2-Ring нельзя одновременно добавлять в группу изоляции.

Primary Port

Варианты: Disable/Все порты коммутатора

По умолчанию: Disable

Функция: настройка мастер-порта.

Описание: когда кольцо замкнуто, мастер-порт находится в состоянии пересылки.



- Настройка в качестве главного порта вступает в силу только тогда, когда кольцо замкнуто.
- Мастер-порт должен быть одним из двух кольцевых портов ведущего устройства.

SY2-RING+

Варианты: Enable/Disable

По умолчанию: Disable

Функция: включение или отключение функции Sy2-Ring+.

Backup Port

Варианты: все порты коммутатора.

Функция: выбор одного порта в качестве резервного.

Описание: резервный порт можно настроить только после включения функции Sy2-Ring+.



Add VLAN List

Варианты: все созданные VLAN.

Функция: выбор VLAN, управляемых текущим кольцом Sy2-Ring-VLAN.

После завершения настройки созданные кольца перечисляются в окне «SY2-RING List», как показано на следующем рисунке.

SY2-RING List

Domain ID	Station Type	Ring Port(1,2)	Primary Port	SY2-RING+ Status	Backup Port	Change times
a-1	Master	S1/FE1,S1/FE2	Disable	Enable	S2/FE3	0
b-2	Slave	S3/FX2,S3/FX5	Disable	Disable	--	0

Add

Рисунок 80 – Кольца Sy2-RING

4. Просмотрите и измените конфигурацию Sy2-Ring.

Нажмите на параметры Sy2-Ring (см. рисунок 80). Вы можете просмотреть и изменить конфигурации кольца, как показано на следующем рисунке.

SY2-RING Configuration

Redundancy	SY2-RING
Domain ID	<input type="text" value="1"/>
Domain Name	<input type="text" value="a"/>
Station Type	<input type="text" value="master"/> ▼
Ring Port1	<input type="text" value="S1/FE1"/> ▼
Ring Port2	<input type="text" value="S1/FE2"/> ▼
Primary Port	<input type="text" value="Disable"/> ▼
SY2-RING+	<input type="text" value="Enable"/> ▼
Backup Port	<input type="text" value="S2/FE3"/> ▼

Apply

Delete

Cancel

Рисунок 81 – Настройка Sy2-Ring

Нажмите <Apply>, чтобы изменения вступили в силу после настройки. Нажмите <Delete>, чтобы удалить запись конфигурации Sy2-Ring.



5. Просмотрите состояние Sy2-Ring и порта, как показано на следующем рисунке.

SY2-RING State List	
Redundancy	SY2-RING
Ring Port 1	Block
Ring Port 2	Block
Ring State	RING-OPEN
Clean Change times	CLEAN

Redundancy	SY2-RING+
Equipment IP	192.168.0.2
Equipment MAC	48-BE-2D-00-E8-FD
Backup Port Status	blocking

Рисунок 82 – Состояние Sy2-Ring

6.12.6 Пример типовой настройки

Как показано на рисунке 75, коммутаторы А, В, С и D образуют кольцо 1; коммутаторы Е, F, G и Н образуют кольцо 2. Каналы CE и DF являются резервными соединениями между кольцом 1 и кольцом 2. Далее описан пример настройки данных коммутаторов при помощи веб-интерфейса (см. рисунок 78).

Конфигурация коммутатора А:

1. Идентификатор домена: 1; доменное имя: Ring; кольцевой порт: port 1, port 2; тип узла: Slave; Sy2-Ring+: Disable. Резервные порты не назначены.

Конфигурация коммутатора В:

2. Идентификатор домена: 1; доменное имя: Ring; кольцевой порт: port 1, port 2; тип узла: Master; Sy2-Ring+: Disable. Резервные порты не назначены.

Конфигурация коммутаторов С и D:

3. Идентификатор домена: 1; доменное имя: Ring; кольцевой порт: port 1, port2; тип узла: Slave; Sy2-Ring+: Enable; резервный порт: port 3.

Конфигурация коммутаторов Е, F и G:

4. Идентификатор домена: 2; доменное имя: Ring; кольцевой порт: port 1, port2; тип узла: Slave; Sy2-Ring+: Disable. Резервные порты не назначены.

Конфигурация коммутатора Н:

5. Идентификатор домена: 2; доменное имя: Ring; кольцевой порт: port 1, port2; тип узла: Master; Sy2-Ring+: Disable. Резервные порты не назначены.

6.13 STP/RSTP



6.13.1 Введение

Протокол STP (Spanning Tree Protocol) основан на стандарте IEEE802.1D и разработан для предотвращения широковещательных штормов, вызванных циклическими соединениями, а также используется для резервирования связей. Устройства, поддерживающие STP, обмениваются служебными пакетами и блокируют определённые порты для разрыва «петель» и создания «деревьев», предотвращая бесконечную передачу данных по кругу. Недостатком STP является то, что он не поддерживает быстрый переход порта в рабочее состояние и существует необходимость выдерживать техническую паузу перед переходом в режим пересылки.

Для решения проблемы с протоколом STP, IEEE разработал стандарт 802.1w в качестве дополнения стандарта 802.1D. Стандарт IEEE802.1w даёт определение протоколу Rapid Spanning Tree Protocol (RSTP). По сравнению с STP, RSTP работает быстрее за счёт добавления альтернативных и резервных портов для корневых и назначенных портов соответственно. Когда корневой/назначенный порт выходит из строя, его альтернативный/резервный порт немедленно переходит в состояние пересылки.

6.13.2 Основные понятия

Корневой мост (Root bridge): является «корнем дерева». Сеть может иметь только один корневой мост. Какой из коммутаторов будет корневым, зависит от сетевой топологии. Корневой мост меняется вместе с топологией сети. Он периодически отправляет BPDU другим устройствам, которые пересылают их для обеспечения стабильности топологии.

Корневой порт (Root port): порт некорневого коммутатора, расстояние от которого до корневого коммутатора наименьшее. Под наименьшим расстоянием понимается расстояние до корневого коммутатора с наименьшей стоимостью пути. Все коммутаторы сети связываются с корневым коммутатором через корневые порты. При этом у всех некорневых устройств может быть только один корневой порт. На корневом коммутаторе нет корневого порта.

Назначенный порт (Designated port): порт, который отвечает за пересылку BPDU другим устройствам или локальным сетям. Все порты корневого моста являются назначенными.

Альтернативный порт (Alternate port): резервный порт корневого порта. Если корневой порт выходит из строя, альтернативный порт становится новым корневым.

Резервный порт (Backup port): резервный для назначенного порта. Когда назначенный порт выходит из строя, резервный порт становится новым назначенным портом и передаёт данные вместо него.

6.13.3 BPDU

Для предотвращения петель все устройства в сети совместно вычисляют структуру логического дерева (ST). Они подтверждают топологию сети путем доставки сообщений BPDU между собой. В следующей таблице показана структура данных BPDU.

Таблица 6 – BPDU



...	Root bridge ID	Root path cost	Designated bridge ID	Designated port ID	Message age	Max age	Hello time	Forward delay	...
...	8 байт	4 байта	8 байт	2 байта	2 байта	2 байта	2 байта	2 байта	...

Структура данных BPDU включает:

Идентификатор корневого моста (Root bridge ID): приоритет корневого коммутатора (2 байта) + MAC-адрес корневого коммутатора (6 байт).

Стоимость пути (Root path cost): стоимость кратчайшего пути до корневого моста

Идентификатор назначенного моста (Designated bridge ID): приоритет назначенного коммутатора (2 байта) + MAC-адрес назначенного моста (6 байт).

Идентификатор назначенного порта (Designated port ID): приоритет порта + номер порта.

Возраст сообщения (Message age): время, в течение которого BPDU может распространяться по сети.

Максимальный возраст или время старения (Max age): максимальное время хранения BPDU на устройстве. Когда возраст сообщения больше, чем время старения, BPDU отбрасывается.

Время приветствия (Hello time): интервал времени для отправки BPDU.

Задержка отправки (Forward delay): задержка изменения статуса (отбрасывание – обучение – пересылка).

6.13.4 Реализация

Процесс вычисления логического дерева для всех устройств следующий:

1. Начальная стадия.

Все устройства на всех своих портах генерируют BPDU, считая себя корневым мостом. И идентификатор корневого моста, и идентификатор назначенного моста являются идентификатором локального устройства; стоимость корневого пути равна 0; назначенный порт является локальным портом.

2. Выбор оптимальной конфигурации BPDU.

Все устройства отсылают свои BPDU и получают BPDU от других устройств. При получении BPDU, каждый порт сравнивает полученный BPDU со своим.

- Если приоритет конфигурации BPDU, сгенерированного локальным портом выше, чем приоритет в BPDU, принятом от другого узла, устройство не выполняет никакой обработки.
- Если приоритет полученного BPDU выше, то порт заменяет локальный BPDU полученным.

Устройство выбирает оптимальную конфигурацию после сравнения BPDU всех портов. Принципы сравнения BPDU:



- BPDU с наименьшим идентификатором корневого моста имеет наивысший приоритет.
- Если ID корневого коммутатора двух BPDU одинаковы, сравнивается стоимость пути до корневого коммутатора. Если стоимость пути в BPDU плюс стоимость пути локального порта меньше, приоритет BPDU выше.
- Если стоимость пути в двух BPDU также одинаковы, по порядку сравниваются ID назначенных коммутаторов, ID назначенных портов и ID портов, получивших BPDU. BPDU с наименьшим ID будет иметь наивысший приоритет.

3. Выбор корневого моста.

Корневым мостом связующего дерева является устройство с наименьшим ID.

4. Выбор корневых портов.

Некорневые коммутаторы сделают свои порты, получающие BPDU с наилучшей конфигурацией, корневыми.

5. Расчет BPDU для назначенного порта.

В соответствии с BPDU корневого порта и его стоимостью пути, BPDU назначенного порта рассчитывается для каждого порта следующим образом:

- Идентификатор корневого моста заменяется идентификатором корневого моста, взятым из BPDU корневого порта.
- Стоимость пути до корневого моста заменяется на стоимость пути до корневого моста из BPDU корневого порта плюс стоимость пути корневого порта.
- ID назначенного моста заменяется на ID локального устройства.
- ID назначенного порта заменяется на ID данного локального порта.

6. Выбор назначенного порта.

Если вычисленные значения BPDU лучше, устройство делает этот порт назначенным, заменяет BPDU порта вычисленным и отправляет новый BPDU. Если текущие значения BPDU лучше, устройство не обновляет его и блокирует порт. Заблокированные порты могут принимать и отправлять только служебную информацию RSTP, но не данные.

6.13.5 Настройка с помощью WEB-интерфейса

1. Включите STP/RSTP, как показано на следующем рисунке.

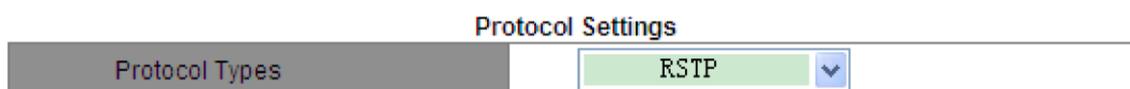


Рисунок 83 – Включение RSTP/STP

Protocol Types

Варианты: Disable/RSTP/STP

По умолчанию: Disable



Функция: отключение или включение RSTP (STP).



- К протоколам на основе портов относятся RSTP, Sy2-Ring-Port и Sy2-RP-Port, а к протоколам на основе VLAN – Sy2-Ring-VLAN и Sy2-RP-VLAN.
- Кольцевые протоколы на основе порта и VLAN являются взаимоисключающими, и для одного устройства можно выбрать только один тип протокола.

2. Установите временные параметры сетевого моста, как показано на следующем рисунке.

Spanning Tree Priority	<input type="text" value="32768"/>	(0-65535)
Hello Time	<input type="text" value="2"/>	(1-10)Sec
Max Age Time	<input type="text" value="20"/>	(6-240)Sec
Forward Delay Time	<input type="text" value="15"/>	(4-128)Sec
Message-age Increment	<input type="text" value="Default"/>	▼

Apply

Рисунок 84 – Настройка временных параметров сетевого моста

Spanning Tree Priority

Диапазон: 0–65535; шаг: 4096.

По умолчанию: 32768

Функция: настройка приоритета сетевого моста.

Описание: приоритет используется для выбора корневого моста. Чем меньше значение, тем выше приоритет.

Hello Time

Диапазон: 1–10 с

По умолчанию: 2 с

Функция: настройка интервала отправки BPDU.

Max Age Time

Диапазон: 6–240 с

По умолчанию: 20 с

Функция: настройка максимального возраста сообщения.

Описание: если возраст BPDU больше указанного значения, то BPDU отбрасывается.

Forward Delay Time



Диапазон: 4–128 с

По умолчанию: 15 с

Функция: настройка времени изменения статуса с отбрасывания на обучение или с обучения на пересылку.

Message-age Increment

Варианты: Compulsion/Default

Значение по умолчанию: Default

Функция: настройка значения, которое будет добавляться к возрасту сообщения, когда BPDU проходит через сетевой мост.

Описание: в принудительном (compulsion) режиме значение равно 1.

В режиме по умолчанию (default) значение равно max (max age time/16, 1).

Forward Delay Time, Max Age Time, Hello Time должны соответствовать следующим требованиям:

$2 \times (\text{Forward Delay Time} - 1.0 \text{ с}) \geq \text{Max Age Time}$;

$\text{Max Age Time} \geq 2 \times (\text{Hello Time} + 1.0 \text{ с})$.

3. Включите RSTP на портах, как показано на следующем рисунке.

Port Settings

Port	Protocol State	Port Priority(0~255)	Path Cost(1~200000000)	Cost Count
S1/FE1	Enable	128	2000000	Yes
S1/FE2	Enable	128	2000000	No
S1/FE3	Enable	128	2000000	Yes
S1/FE4	Enable	128	2000000	No
S1/FE5	Disable	128	2000000	Yes
S1/FE6	Disable	128	2000000	Yes
S1/FE7	Disable	128	2000000	Yes
S1/FE8	Disable	128	2000000	Yes
S4/GE1	Disable	128	2000000	Yes
S4/GE2	Disable	128	2000000	Yes
S4/GE3	Disable	128	2000000	Yes
S4/GE4	Disable	128	2000000	Yes

Apply

Рисунок 85 – Настройки портов

Protocol State

Варианты: Enable/Disable

По умолчанию: Disable

Функция: включение или отключение STP на портах.



- Порт RSTP нельзя настроить как порт источника или назначения зеркалирования; порт источника или назначения зеркалирования не может быть настроен как порт RSTP.
- Порт RSTP нельзя добавить в группу агрегации; порт из группы агрегации не может быть настроен как порт RSTP.
- Настройка портов RSTP, Sy2-Ring-Port и Sy2-RP-Port является взаимоисключающей. То есть, кольцевой или резервный порт Sy2-Ring-Port не должны быть настроены как порт RSTP, Sy2-RP-Port, кольцевой или резервный порт Sy2-RP-Port. Соответственно, порт RSTP, кольцевой и резервный порт Sy2-RP-Port не должны быть настроены как кольцевой или резервный порт Sy2-Ring-Port.
- Не рекомендуется настраивать порты в группе изоляции одновременно как порты RSTP, а порты RSTP нельзя добавлять в группу изоляции.

Port Priority

Диапазон: 0–255; шаг: 16

По умолчанию: 128

Функция: настройка приоритета порта, который определяет его роль.

Path Cost

Диапазон: 1–200000000

По умолчанию: 2000000 (порт 10M), 200000 (порт 100M), 20000 (порт 1000M)

Описание: данная функция используется для расчета наилучшего пути. Значение параметра зависит от полосы пропускания. Чем больше значение, тем ниже стоимость. Вы можете изменить роль порта, поменяв его стоимость пути. Чтобы настроить значение вручную, выберите «No» для параметра «Cost Count».

Cost Count

Варианты: Yes/No

По умолчанию: Yes

Функция: вычисление стоимости пути для порта.

Описание: «Yes» указывает, что стоимость пути порта принимает значение по умолчанию. «No» означает, что вы можете настроить стоимость пути вручную.

4. Просмотрите состояние RSTP, как показано на следующем рисунке.



Root Info

Root MAC	00:1e:cd:11:01:b1
Root Priority	0x1000
Root Path Cost	200000
Root Port	S1/FE2
Max Age(s)	20
Hello Time(s)	2
Forward Delay(s)	15

Bridge Info

Bridge MAC	00:00:00:00:19:39
Bridge Priority	0x8000
Bridge Version	2
Max Age(s)	20
Hello Time(s)	2
Forward Delay(s)	15

Port Info

Port	Priority	Path Cost	Role	State	Link State
S1/FE1	0x80	2000000	Disabled	Discarding	Down
S1/FE2	0x80	200000	Root	Forwarding	Up
S1/FE3	0x80	2000000	Disabled	Discarding	Down
S1/FE4	0x80	200000	Alternate	Discarding	Up

Рисунок 86 – Информация о состоянии RSTP

Пример типовой настройки

Приоритеты коммутаторов А, В и С – 0, 4096 и 8192. Стоимость пути каналов связи – 4, 5 и 10, как показано на следующем рисунке.

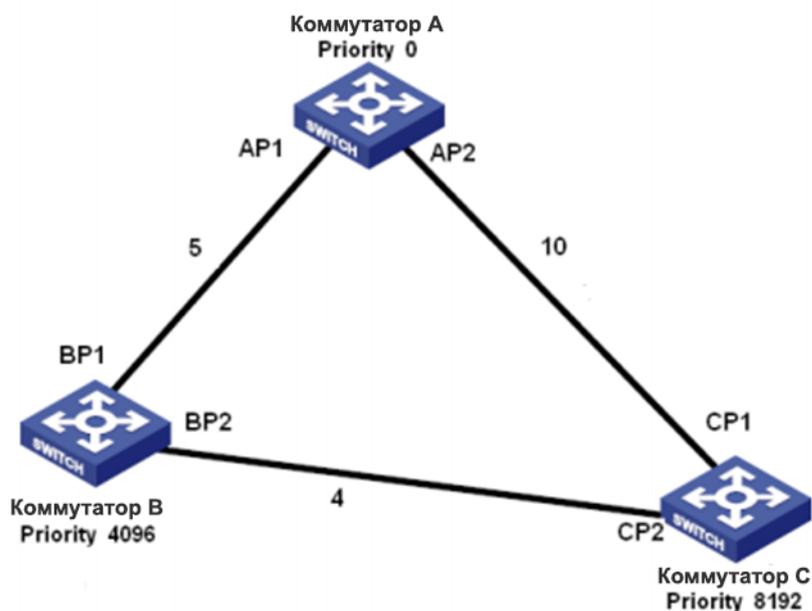


Рисунок 87 – Пример конфигурации RSTP

Настройка коммутатора А:

1. Установите приоритет на «0» и временные параметры на значения по умолчанию, как показано на рисунке 84.
2. Установите стоимость пути для порта 1 на «5», а для порта 2 на «10», как показано на рисунке 85.

Настройка коммутатора В:

1. Установите приоритет на «4096» и временные параметры на значения по умолчанию, как показано на рисунке 84.
2. Установите стоимость пути для порта 1 на «5», а для порта 2 на «4», как показано на рисунке 85.

Настройка коммутатора С:

1. Установите приоритет на «8192» и временные параметры на значения по умолчанию, как показано на рисунке 84.
 2. Установите стоимость пути для порта 1 на «10», а для порта 2 на «4», как показано на рисунке 85.
- Приоритет коммутатора А равен 0, а его корневой идентификатор является наименьшим. Таким образом, коммутатор А является корневым мостом.
 - Стоимость пути от AP1 к BP1 равна 5, а от AP2 к BP2 – 14. Таким образом, BP1 является корневым портом.
 - Стоимость пути от AP1 к CP2 равна 9, а от AP2 к CP1 – 10. Следовательно, CP2 – это корневой порт, а BP2 – назначенный порт.



6.14 Прозрачная передача RSTP/STP

6.14.1 Введение

RSTP соответствует стандарту IEEE. Sy2-Ring/Sy2-RP – это проприетарный протокол резервирования компании Symanitron, но он не может сосуществовать с RSTP в одной сети. Чтобы решить эту проблему, была разработана функция прозрачной передачи RSTP/STP. Эта функция позволяет коммутатору использовать другие резервные протоколы при прозрачной передаче пакетов RSTP, что соответствует требованиям промышленной связи.

Коммутаторы, использующие другие резервные протоколы, могут получать и пересылать пакеты RSTP только в том случае, если включена функция его прозрачной передачи. Коммутаторы с поддержкой прозрачной передачи RSTP можно рассматривать как прозрачный канал связи.

Как показано на следующем рисунке, коммутаторы A, B, C и D образуют кольцо Sy2. На этих четырех коммутаторах включена функция прозрачной передачи, поэтому коммутаторы E и F могут получать пакеты RSTP друг от друга.

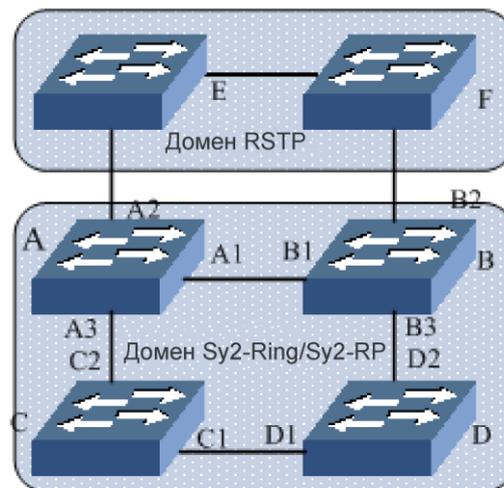


Рисунок 88 – Прозрачная передача RSTP

6.14.2 Настройка с помощью WEB-интерфейса

Настройте прозрачную передачу RSTP на портах, как показано на следующем рисунке.



Port	RSTP Transparent Transmission
S1/FE1	Disable
S1/FE2	Disable
S1/FE3	Disable
S1/FE4	Disable
S1/FE5	Enable
S1/FE6	Enable
S1/FE7	Disable
S1/FE8	Disable
S4/GE1	Disable
S4/GE2	Disable
S4/GE3	Disable
S4/GE4	Disable

Apply

Рисунок 89 – Настройка прозрачной передачи

RSTP Transparent Transmission

Варианты: Enable/Disable

По умолчанию: Disable

Функция: включение или отключение прозрачной передачи RSTP на портах.



Прозрачную передачу RSTP нельзя включить на порту с поддержкой RSTP.

6.14.3 Пример типовой настройки

Как показано на рисунке 88, коммутаторы А, В, С и D образуют кольцо Sy2, а коммутаторы Е и F – домен RSTP. В домене RSTP все кольцо Sy2 служит прозрачным каналом для пересылки пакетов RSTP на коммутаторы Е и F.

Настройте коммутаторы А, В, С и D как кольцо Sy2. Подробную информацию см. в разделе 6.12 Sy2-Ring.

Включите RSTP на задействованных портах коммутаторов Е и F, как показано на рисунках 83 и 85.

Включите прозрачную передачу RSTP на портах А1, А2, А3, В1, В2, В3, С1, С2, D1 и D2, как показано на рисунке 89.



6.15 Sy2-RP

6.15.1 Введение

Протокол Sy2-RP (Symanitron Redundancy Protocol) разработан для передачи данных в кольцевых сетях. Он может предотвращать широкоэвещательные штормы в кольцевых топологиях. Если канал или узел выходят из строя, вместо них задействуется резервная связь, обеспечивающая бесперебойную передачу данных.

Совместимый со стандартом IEC 62439-6, протокол Sy2-RP использует механизм выбора мастера без привязки к определенному узлу. Sy2-RP предоставляет следующие возможности:

- Время восстановления сети, не зависящее от размеров сети.

Sy2-RP обеспечивает время восстановления, не зависящее от размера сети, за счет оптимизации механизма определения передачи данных по кольцу. Sy2-RP позволяет сетям восстанавливаться менее, чем за 20 мс, благодаря функции оповещения, обеспечивающей надёжную передачу данных реального времени. Эта функция позволяет коммутаторам обеспечивать максимальную надёжность приложений в энергетике, железнодорожном транспорте и многих других отраслях, где требуется управление в реальном времени.

- Функция диверсифицированного определения сбоя соединения.

Для увеличения сетевой стабильности Sy2-RP предоставляет функцию диверсифицированного определения сбоя соединения для типичных сетевых проблем, включая быстрое определение отсутствия соединения, определение однонаправленной передачи данных в оптоволоконных каналах, исследование качества связи и проверку состояния оборудования.

- Применимость к различным сетевым топологиям.

Кроме быстрого восстановления для простых кольцевых топологий, Sy2-RP также поддерживает топологии сложных колец, например, пересекающиеся кольца и кольца с общими участками. Также Sy2-RP поддерживает множественные кольца, основанные на VLAN и таким образом подходит для использования в различных сетях.

- Функции диагностики и поддержки

Sy2-RP имеет функции запроса статуса и механизм создания тревожных событий, используемые для сетевой диагностики и поддержки, а также механизм предотвращения непреднамеренных воздействий на сеть и создания настроек, которые могут привести к широкоэвещательным штормам.

6.15.2 Основные понятия

1. Режимы Sy2-RP

Sy2-RP имеет два режима: Sy2-RP-Port-Base и Sy2-RP-VLAN-Base.

Sy2-RP-Port-Base: пересылает или блокирует данные на основе определенных портов.



Sy2-RP-VLAN-Base: пересылает или блокирует пакеты на основе VLAN. Если порт находится в состоянии блокировки, блокируются только пакеты данных указанной VLAN. Таким образом, на портах пересекающихся колец можно настроить несколько VLAN. Порт может принадлежать разным кольцам Sy2-RP в соответствии с конфигурациями VLAN.

2. Статус Sy2-RP порта

Состояние пересылки данных: если порт находится в режиме пересылки, он может принимать и отправлять данные.

Состояние блокировки: если порт находится в режиме блокировки, он может принимать и отправлять Sy2-RP пакеты, но не другие данные.



Порт на корневом устройстве, находящийся в состоянии блокировки, может активно отправлять пакеты Sy2-RP.

3. Роли Sy2-RP

Sy2-RP определяет роли коммутаторов путём передачи пакетов Announce, предотвращая создание петель в кольцах резервирования.

INIT: обозначает устройство, на котором Sy2-RP включен и оба его кольцевых порта находятся в состоянии «Link Down».

Корневой (Root): обозначает устройство, на котором Sy2-RP включен и как минимум один его порт активен. В кольце корневой коммутатор выбирается согласно векторам пакетов Announce. Эта роль может измениться при изменении топологии. Корневой коммутатор периодически отправляет свои собственные Announce-пакеты. Статус кольцевых портов: один кольцевой порт в состоянии пересылки, а второй – в состоянии блокировки. После получения пакета Announce от другого устройства, корневой коммутатор сравнивает вектор полученного пакета со своим собственным пакетом Announce. Если полученный вектор больше, Root меняет свою роль на Normal или «B-Root», в зависимости от состояния соединения и CRC-деградации портов.

B-Root: обозначает устройство, на котором Sy2-RP включен, один порт активен, а второй – неактивен или в режиме деградации CRC. B-Root сравнивает и передаёт пакеты Announce. Если вектор полученного пакета Announce меньше, чем вектор собственного пакета, B-Root меняет свою роль на Root, в противном случае он передаёт полученный пакет и не меняет собственной роли. Статусы кольцевых портов: один кольцевой порт в состоянии пересылки.

Обычный (Normal): обозначает устройство, на котором Sy2-RP включен и оба порта активны без CRC-деградации. Обычные коммутаторы только передают пакеты Announce, без проверки содержимого. Статус кольцевых портов: оба порта в состоянии пересылки.



Деградация CRC указывает, что число пакетов CRC превышает пороговое значение за 15 минут.



6.15.3 Реализация

Каждый коммутатор поддерживает свой собственный вектор пакета Announce. Коммутатор с большим вектором будет выбран корневым.

Вектор пакета Announce содержит следующую информацию для назначения роли:

Таблица 7 – Вектор пакета Announce

Статус соединения	Деградация CRC		Ролевой приоритет	IP-адрес устройства	MAC-адрес устройства
	Статус деградации CRC	Скорость деградации CRC			

Статус соединения: значение устанавливается равным 1, если один кольцевой порт находится в состоянии «Link Down», и устанавливается в 0, если оба кольцевых порта находятся в состоянии «Link Up».

Статус деградации CRC: если на одном из портов присутствует деградация CRC, значение равно 1. Если ни на одном порту ее нет, значение равно 0.

Скорость деградации CRC: отношение количества пакетов CRC к пороговому значению за 15 минут.

Ролевой приоритет: значение можно установить через веб-интерфейс.

IP-адрес устройства.

MAC-адрес устройства.

Параметры вектора из таблицы 7 сравниваются следующим образом:

1. Сначала проверяется статус соединения. Устройство с большим значением этого поля считается устройством с большим вектором.
2. Если два сравниваемых устройства имеют одинаковое значение поля статуса соединения, сравниваются значения поля деградации CRC. Устройство с большим значением считается устройством с большим вектором. Если значение статуса деградации CRC всех сравниваемых устройства равно 1, считается, что устройство с большим значением скорости деградации CRC имеет больший вектор.
3. Если два сравниваемых устройства имеют одинаковый статус соединения и значение деградации CRC, последовательно сравниваются ролевой приоритет, IP-адрес и MAC-адрес. Устройство с большим значением считается устройством с большим вектором.
4. Устройство с большим вектором выбирается корневым.



Только когда значение состояния деградации CRC равно 1, в сравнении векторов участвует значение скорости деградации CRC. В противном случае векторы сравниваются независимо от значения этого параметра.

➤ Реализация режима Sy2-RP на основе портов

Роль коммутатора определяется следующим образом:

1. Во время запуска, все коммутаторы находятся в режиме INIT. Когда статус одного порта меняется на активный, коммутатор становится корневым и начинает отсылать пакеты Announce другим коммутаторам в кольце.
2. Коммутатор с наибольшим вектором Announce выбирается корневым. Его кольцевой порт, перешедший в активное состояние первым переходит в режим пересылки данных, второй порт переходит в режим блокировки. Среди остальных коммутаторов тот, у которого один из портов в неактивном состоянии или в режиме CRC-деградации, переходит в режим B-Root. Коммутаторы с двумя активными кольцевыми портами, не имеющими деградации CRC, получают статус Normal.

Процедура устранения неисправности следующая:

1. В исходной топологии А является корневым (Root); порт 1 находится в состоянии пересылки, а порт 2 в состоянии блокировки. В, С и D являются обычными (Normal), и их кольцевые порты находятся в состоянии пересылки, как показано на следующем рисунке.

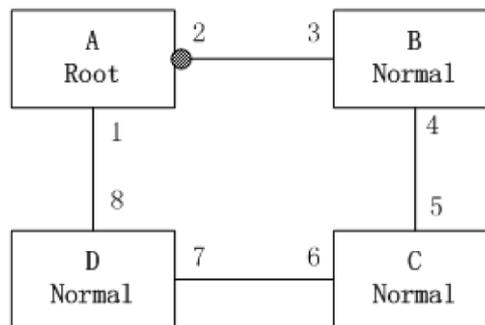


Рисунок 90 – Топология Sy2-RP

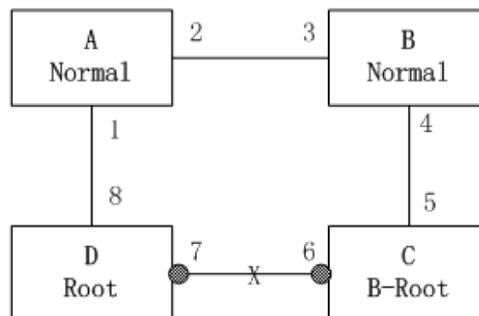


Рисунок 91 – Обрыв связи



2. Когда связь CD обрывается, Sy2-RP изменяет статусы портов 6 и 7 на блокировку. В результате С и D становятся корневыми. Поскольку А, С и D в данный момент являются корневыми, все они отправляют пакеты Announce. Векторы С и D больше, чем векторы А, потому что порты 7 и 6 находятся в состоянии «Link Down». В этом случае, если вектор D больше, чем вектор С, D выбирается в качестве Root, а С становится B-Root. При получении пакета Announce от D, А обнаруживает, что вектор D больше, чем его собственный вектор, и оба его кольцевых порта находятся в состоянии «Link Up». Таким образом, А становится обычным (Normal) и изменяет статус порта 2 на пересылку данных, как показано на рисунке 91.

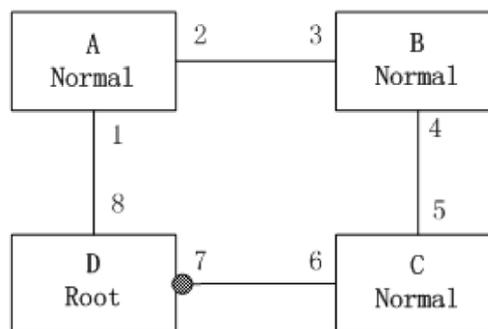


Рисунок 92 – Восстановление связи

3. Когда связь CD восстанавливается, D все еще является корневым, потому что его вектор больше, чем вектор С.

Поскольку D является корневым, порт 7 находится в состоянии блокировки. В этом случае порт 6 находится в состоянии «Link Up», поэтому Sy2-RP изменяет статус порта 6 на состояние пересылки. В результате С переходит в статус Normal. Таким образом, роли коммутаторов не меняются при восстановлении канала связи.



В кольцевой сети Sy2-RP роли коммутаторов меняются при сбое линии связи, но не меняются при её восстановлении. Этот механизм повышает безопасность сети и надежность передачи данных.

➤ Реализация режима Sy2-RP на основе VLAN

Кольцо на основе Sy2-RP-VLAN позволяет пересылать пакеты из разных VLAN по разным путям. Каждый путь пересылки для VLAN образует Sy2-RP-VLAN-Base. Различные кольца Sy2-RP на основе VLAN могут иметь разные корни. Как показано на следующем рисунке, на основе VLAN настроены два кольца Sy2-RP.

Кольцевые связи Sy2-RP на основе VLAN10/20: AB-BC-CD-DE-EA.

Кольцевые связи Sy2-RP на основе VLAN30: FB-BC-CD-DE-EF.



Два кольца соприкасаются участками BC, CD и DE. Коммутатор С и коммутатор D используют в двух кольцах одни и те же порты, но разные логические связи на основе VLAN.

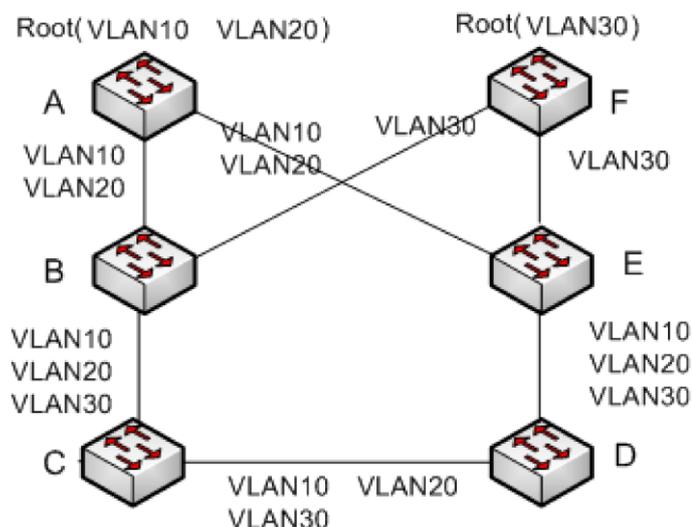


Рисунок 93 – Sy2-RP-VLAN-Base



Статусы и роли в каждом кольце Sy2-RP-VLAN-Base такие же, как и в кольце Sy2-RP-Port-Base.

➤ Резервирование Sy2-RP

Sy2-RP также может обеспечивать резервируемое соединение между двумя кольцами, обеспечивая для них надёжную связь и предотвращая появление петель.

Резервный порт: обозначает порт связи между кольцами Sy2-RP. Можно назначать множество резервных портов, однако все они должны быть в одном кольце. Первый активный порт становится главным (резервным мастер-портом) и переходит в режим пересылки данных. Все остальные резервные порты становятся ведомыми и переходят в режим блокировки.

Как показано на следующем рисунке, на каждом коммутаторе можно настроить один резервный порт. Главный резервный порт находится в состоянии пересылки, а ведомые – в состоянии блокировки. Если мастер-порт выходит из строя, один из ведомых резервных портов займёт его место.

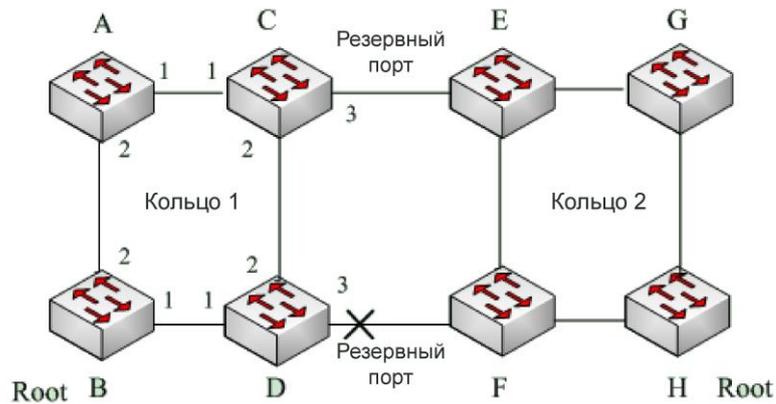


Рисунок 94 – Резервирование Sy2-RP



Изменение статуса соединения влияет на статус резервных портов.

6.16 DHP

6.16.1 Введение

Как показано на следующем рисунке, коммутаторы A, B, C и D подключены к кольцу. Протокол Dual Homing (DHP) выполняет следующие функции, если он включен на коммутаторах A, B, C и D:

- Коммутаторы A, B, C и D могут связываться друг с другом, не влияя на корректную работу устройств в кольце.
- Если связь между коммутаторами A и B нарушена, коммутатор A все еще может связываться с коммутаторами B, C и D, используя пути устройств 1 и 2.

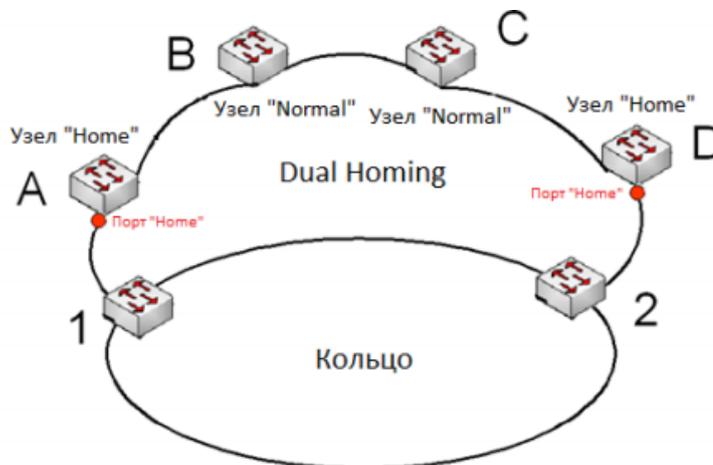


Рисунок 95 – Реализация протокола Dual Homing



6.16.2 Основные понятия

Реализация Dual Homing основана на Sy2-RP. Механизм выбора и назначения ролей в Dual Homing такой же, как и в Sy2-RP. Dual Homing обеспечивает резервирование канала связи через настройки узлов «Home», «Normal» и порта «Home». Узлы «Home» – это устройства, находящиеся на обоих концах канала Dual Homing и принимающие пакеты Sy2-RP. Порт «Home» означает порт, соединяющий узел «Home» с внешней сетью. Порт «Home» обеспечивает следующие функции:

- Отправку ответных пакетов корневому коммутатору при получении от него пакетов Announce. Если корневой коммутатор получает ответные пакеты, он считает, что кольцо замкнуто. В противном случае кольцо считается разомкнутым.
- Блокировку пакетов Sy2-RP внешних сетей и изоляцию канала Dual Homing от внешних сетей.
- Отправку пакетов очистки записей подключенным устройствам во внешних сетях при изменении топологии канала Dual Homing.

Узел «Normal»: означает все устройства в канале Dual Homing, за исключением крайних устройств, т.е. узлов «Home». Узлы «Normal» передают ответные пакеты узлов «Home».

6.16.3 Реализация

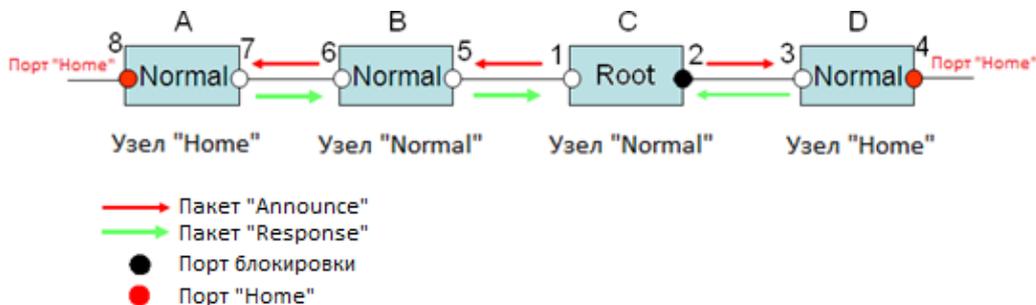


Рисунок 96 – Конфигурация Dual Homing

Как показано на рисунке 96, настройки коммутаторов A, B, C и D следующие:

- Конфигурация Sy2-RP: C – корневой коммутатор; порт 2 находится в состоянии блокировки; коммутаторы A, B и D – обычные («Normal»); все остальные порты кольца находятся в состоянии пересылки.
- Конфигурация Dual Homing: коммутаторы A и D – узлы «Home»; порты 8 и 4 являются портами «Home»; коммутаторы B и C – «Normal».

Реализация:

Корневой коммутатор C отправляет пакеты Announce через два своих кольцевых порта. Порты «Home» 8 и 4 получают пакеты Announce и отправляют ответные пакеты



коммутатору С. Коммутатор С соответственно идентифицирует состояние кольца как закрытое. Порт 2 находится в состоянии блокировки.

Если линия связи между коммутаторами А и В заблокирована, в топологии остаются два канала: А и В-С-Д.

Коммутатор А назначается корневым. Порт 7 находится в состоянии блокировки.

В канале В-С-Д коммутатор В выбирается в качестве корневого. Порт 6 находится в состоянии блокировки. Коммутатор С становится «Normal». Порт 2 находится в состоянии пересылки. Коммутатор А может связываться с коммутаторами В, С и D через устройства 1 и 2, как показано на следующем рисунке.

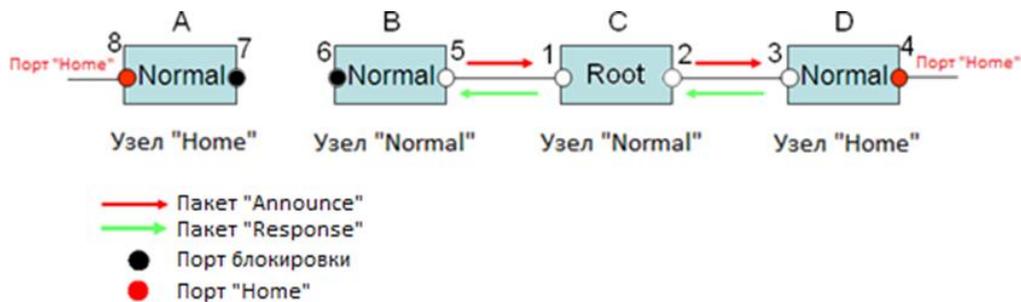


Рисунок 97 – Восстановление связи Dual Homing

6.16.4 Пояснение

Конфигурации Sy2-RP должны соответствовать следующим требованиям:

- Все коммутаторы в одном кольце должны иметь одинаковый номер домена.
- Одно кольцо включает только один корневой коммутатор, но при этом может включать несколько коммутаторов В-Root или «Normal».
- На каждом коммутаторе для кольца можно настроить только два порта.
- Для двух объединенных колец резервные порты можно настроить только в одном кольце.
- В одном кольце можно настроить несколько резервных портов.
- На коммутаторе только один резервный порт может быть настроен для одного кольца.

6.16.5 Настройка с помощью WEB-интерфейса

1. Настройте режим Sy2-RP, как показано на следующем рисунке.

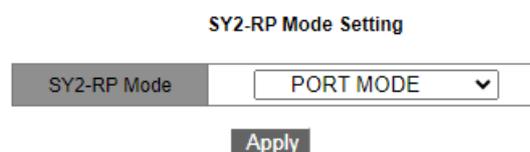


Рисунок 98 – Настройка режима Sy2-RP



SY2-RP Mode

Варианты: PORT MODE/VLAN MODE

По умолчанию: PORT MODE

Функция: настройка режима Sy2-RP.



- К протоколам резервирования на основе портов относятся RSTP, Sy2-Ring-Port и Sy2-RP-Port, а к протоколам на основе VLAN – Sy2-Ring-VLAN и Sy2-RP-VLAN.
- Кольцевые протоколы на основе VLAN являются взаимоисключающими, и для одного устройства можно настроить только тип кольцевого протокола на основе VLAN.
- Кольцевые протоколы на основе порта и на основе VLAN являются взаимоисключающими, и для одного устройства можно выбрать только один из этих режимов.

2. Настройте кольцо Sy2-RP на основе портов, как показано на следующем рисунке.

SY2-RP Domain Setting

Redundancy	SY2-RP
Domain ID	1
Domain Name	a
DHP Mode	Disable
Home Port	Ring Port 1
Role Priority	128 (0~255)
CRC Threshold	100 (25~65535)
Ring Port 1	S1/FE1
Ring Port 2	S1/FE2
Backup Port	S1/FE3

Рисунок 99 – Настройка Sy2-RP-Port-Base

Redundancy

Обязательная конфигурация: Sy2-RP

Domain ID



Диапазон: 1–32

Функция: каждое кольцо имеет уникальный идентификатор домена. На одном коммутаторе можно настроить максимум 16 колец Sy2-RP-Port-Base.

Domain Name

Диапазон: 1–31 символ

Функция: настройка доменного имени.

DHP Mode

Варианты: Disable/Normal Node/Home Node

По умолчанию: Disable

Функция: включение/отключение DHP или настройка режима DHP.



Протокол DHP доступен только в режиме SY2-RP-Port-Base.

Home Port

Варианты: Ring Port 1/Ring Port 2/Ring Port 1-2

Функция: настройка домашнего порта для домашнего узла DHP.

Описание: если в канале DHP имеется только одно устройство, оба кольцевых порта узла Home должны быть настроены как Home-порты.

Role Priority

Диапазон: 0–255

По умолчанию: 128

Функция: настройка приоритета коммутатора.

CRC Threshold

Диапазон: 25–65535

По умолчанию: 100

Функция: настройка порогового значения CRC.

Описание: этот параметр используется при выборе корня. Если количество ошибок CRC, обнаруженных на одном из кольцевых портов, превышает установленное пороговое значение, то система рассматривает это как признак деградации качества соединения на этом порту. В результате значение CRC-деградации устанавливается равным 1 в векторе пакета Announce порта.

Ring Port 1/Ring Port 2

Варианты: все порты коммутатора

Функция: выбор двух кольцевых портов.

Backup Port



Варианты: все порты коммутатора

Функция: выбор резервного порта.



Не настраивайте кольцевой порт в качестве резервного.

После завершения настройки созданные кольца отображаются в окне «SY2-RP List», как показано на следующем рисунке.

SY2-RP List

Domain ID	Role Status	Ring Port(1,2)	Backup Port	Ring Status
1-a	INIT	S1/FE1,S1/FE2	S1/FE3	----

Рисунок 100 – Список колец Sy2-RP-Port-Base



- Кольцевой или резервный порт Sy2-RP нельзя добавить в группу агрегации. Порт, добавленный в группу агрегации, нельзя настроить как кольцевой или резервный порт Sy2-RP.
- Кольцевой или резервный порт Sy2-RP нельзя настроить как порт источника или назначения зеркалирования. Порт источника или назначения зеркалирования не может быть настроен как кольцевой или резервный порт Sy2-RP.
- Настройка портов RSTP, Sy2-Ring-Port и Sy2-RP-Port является взаимоисключающей. То есть, кольцевой или резервный порт Sy2-Ring-Port не должны быть настроены как порт RSTP, Sy2-RP-Port, кольцевой или резервный порт Sy2-RP-Port. Соответственно, порт RSTP, кольцевой и резервный порт Sy2-RP-Port не должны быть настроены как кольцевой или резервный порт Sy2-Ring-Port.
- Не рекомендуется одновременно настраивать порты в группе изоляции как кольцевые и резервные порты Sy2-RP, а кольцевые и резервные порты Sy2-RP нельзя одновременно добавлять в группу изоляции.

- Просмотрите настройки параметров Sy2-RP-Port-Base.

Выберите запись SY2-RP (см. рисунок 100). Вы можете просмотреть и изменить настройки параметров записи, как показано на следующем рисунке.



SY2-RP Setting

Redundancy	SY2-RP
Domain ID	1
Domain Name	a
DHP Mode	Disable ▾
Home Port	Ring Port 1 ▾
Role Priority	128 (0~255)
CRC Threshold	100 (25~65535)
Ring Port 1	S1/FE1 ▾
Ring Port 2	S1/FE2 ▾
Backup Port	S1/FE3 ▾

Apply Delete Cancel Help

Рисунок 101 – Запрос и изменение записи Sy2-RP-Port-Base

После завершения настройки нажмите <Apply>, чтобы изменения вступили в силу. Вы можете удалить запись Sy2-RP, нажав <Delete>.

- Просмотрите роли и состояние портов кольца Sy2-RP, как показано на следующем рисунке.

SY2-RP Status

Role Status	INIT
Ring Port 1	BLOCK
Ring Port 2	BLOCK
Backup Port	BLOCK
Ring Status	----
IP Address	192.168.0.2
MAC Address	48-BE-2D-00-E8-FD
ROOT IP	0.0.0.0

Рисунок 102 – Статус кольца Sy2-RP-Port-Base

3. Настройте кольцо Sy2-RP на основе VLAN, как показано на следующем рисунке.



SY2-RP Domain Setting

Redundancy	SY2-RP
Domain ID	1
Domain Name	a
DHP Mode	Disable ▾
Home Port	Ring Port 1 ▾
Role Priority	128 (0~255)
CRC Threshold	100 (25~65535)
Ring Port 1	S1/FE1 ▾
Ring Port 2	S1/FE2 ▾
Backup Port	S1/FE3 ▾
Protocol Vlan	2 (1~4093)
Service Vlan	2-4 (e.g. 1,2,3,6-8)

Apply

Help

Рисунок 103 – Настройка Sy2-RP-VLAN-Base

Redundancy

Обязательная конфигурация: Sy2-RP

Domain ID

Диапазон: 1–32

Функция: каждое кольцо имеет уникальный идентификатор домена. На одном коммутаторе можно настроить максимум 8 колец Sy2-RP-VLAN-Base.

Domain Name

Диапазон: 1–31 символ

Функция: настройка доменного имени.

Role Priority

Диапазон: 0–255

По умолчанию: 128

Функция: настройка приоритета коммутатора.

CRC Threshold

Диапазон: 25–65535



По умолчанию: 100

Функция: настройка порогового значения CRC.

Описание: этот параметр используется при выборе корня. Если количество ошибок CRC, обнаруженных на одном из кольцевых портов, превышает установленное пороговое значение, то система рассматривает это как признак деградации качества соединения на этом порту. В результате значение CRC-деградации устанавливается равным 1 в векторе пакета Announce порта.

Ring Port 1/Ring Port 2

Варианты: все порты коммутатора

Функция: выбор двух кольцевых портов.

Backup Port

Варианты: все порты коммутатора

Функция: выбор резервного порта.



Не настраивайте кольцевой порт в качестве резервного.

Protocol VLAN

Диапазон: 1–4093

Функция: VLAN, передающая пакеты протокола Sy2-RP, которые служат основой для диагностики и поддержки кольца Sy2-RP- VLAN-Base. VLAN ID должен быть из диапазона «Service VLAN».

Service VLAN

Варианты: все созданные VLAN

Функция: выбор сетей VLAN, управляемых текущим кольцом Sy2-RP-VLAN-Base.

После завершения настройки созданные кольца отображаются в окне «SY2-RP List», как показано на следующем рисунке.

SY2-RP List

Domain ID	Role	Status	Ring Port(1,2)	Backup Port	Ring Status	Protocol Vlan	Service Vlan
<u>1-a</u>	ROOT		S1/FE1,S1/FE2	S1/FE3	Ring-Close	2	2-4

Рисунок 104 – Список колец SY2-RP-VLAN-Base



- Кольцевой или резервный порт Sy2-RP нельзя добавить в группу агрегации. Порт, добавленный в группу агрегации, нельзя настроить как кольцевой или резервный порт Sy2-RP.



- Кольцевой или резервный порт Sy2-RP нельзя настроить как порт источника или назначения зеркалирования. Порт источника или назначения зеркалирования не может быть настроен как кольцевой или резервный порт Sy2-RP.
- Не рекомендуется одновременно настраивать порты в группе изоляции как кольцевые и резервные порты Sy2-RP, а кольцевые и резервные порты Sy2-RP нельзя одновременно добавлять в группу изоляции.

- Просмотрите настройки параметров Sy2-RP-VLAN-Base.

Выберите запись SY2-RP (см. рисунок 104). Вы можете просмотреть и изменить настройки параметров записи, как показано на следующем рисунке.

SY2-RP Setting

Redundancy	DRP
Domain ID	<input type="text" value="1"/>
Domain Name	<input type="text" value="a"/>
DHP Mode	<input type="text" value="Disable"/> ▾
Home Port	<input type="text" value="Ring Port 1"/> ▾
Role Priority	<input type="text" value="128"/> (0~255)
CRC Threshold	<input type="text" value="100"/> (25~65535)
Ring Port 1	<input type="text" value="S1/FE1"/> ▾
Ring Port 2	<input type="text" value="S1/FE2"/> ▾
Backup Port	<input type="text" value="S1/FE3"/> ▾
Protocol Vlan	<input type="text" value="2"/>
Service Vlan	<input type="text" value="2-4"/>

Рисунок 105 – Запрос и изменение записи Sy2-RP- VLAN-Base

После завершения настройки нажмите <Apply>, чтобы изменения вступили в силу. Вы можете удалить запись Sy2-RP, нажав <Delete>.

- Просмотрите роли и состояние портов кольца Sy2-RP, как показано на следующем рисунке.



SY2-RP Status

Role Status	ROOT
Ring Port 1	FORWARD
Ring Port 2	BLOCK
Backup Port	BLOCK
Ring Status	Ring-Close
IP Address	192.168.0.222
MAC Address	08-00-3E-32-53-22

Рисунок 106 – Статус кольца Sy2-RP-VLAN-Base

6.16.6 Пример типовой настройки

Как показано на рисунке 94, А, В, С и D образуют кольцо 1; Е, F, G и H образуют кольцо 2; CE и DF являются резервными каналами кольца 1 и кольца 2.

Настройка коммутаторов А и В:

1. Установите для идентификатора домена значение 1, а для имени домена значение Ring. Выберите кольцевой порт 1 и кольцевой порт 2. Оставьте значения по умолчанию для ролевого приоритета и резервного порта, как показано на рисунке 99.

Настройка коммутаторов С и D:

2. Установите для идентификатора домена значение 1, для имени домена значение Ring, а для резервного порта значение 3. Выберите кольцевой порт 1 и кольцевой порт 2. Оставьте значение по умолчанию для ролевого приоритета, как показано на рисунке 99.

Настройка коммутаторов Е, F, G и H:

3. Установите для идентификатора домена значение 2, для имени домена значение Ring. Выберите кольцевой порт 1 и кольцевой порт 2. Оставьте значения по умолчанию для ролевого приоритета и резервного порта, как показано на рисунке 99.

6.17 QoS

6.17.1 Введение

Quality of Service (QoS) позволяет дифференцировать сервисы, в зависимости от разных требований в условиях ограниченной пропускной способности путем контроля трафика и изменения его движения в IP-сетях. QoS пытается оптимизировать передачу данных различных сервисов, снизить задержки передачи и минимизировать их эффект в зависимости от приоритета сервиса.



Основная задача QoS – идентификация сервисов, управление перегрузкой при передаче данных и ее предотвращение.

Объекты идентифицируются на основе определенных правил сопоставления. Например, объектами могут быть теги приоритета, переносимые пакетами, приоритеты, отображаемые портами и сетями VLAN, или иная информация о приоритете. Идентификация сервисов – основополагающая функция QoS.

Управление перегрузками: это обязательная функция для решения проблемы конкуренции за ресурсы. Управление перегрузками кэширует пакеты в очередях и определяет последовательность их пересылки на основе определенного алгоритма планирования, обеспечивая приоритетную пересылку для ключевых служб.

Предотвращение перегрузки: чрезмерная перегрузка может привести к нарушению работы сети. Функция предотвращения перегрузки отслеживает использование сетевых ресурсов. При обнаружении нарастания перегрузки функция использует упреждающее отбрасывание пакетов и регулирует объем трафика для решения возникшей проблемы.

6.17.2 Принцип работы

Каждый порт коммутатора имеет четыре очереди для кэшированных данных, от 0 до 3 в порядке возрастания приоритета.

Вы можете настроить сопоставление между приоритетом и очередями. Когда кадр достигает порта, коммутатор определяет очередь для кадра в соответствии с информацией в его заголовке. Коммутатор поддерживает следующие режимы сопоставления очередей для определения приоритета: наивысший приоритет (Nq-preempt), на основе порта (Port-Based), DIFF, и 802.1p.

- Если для порта настроен наивысший приоритет, то пересылаемые пакеты помещаются в очередь 3.
- Если настроен режим сопоставления очередей на основе порта, полученные пакеты ставятся в очередь в соответствии с приоритетом порта по умолчанию. Сопоставление между приоритетом по умолчанию и очередями соответствует соотношению между приоритетом 802.1p и очередями.
- Значение DIFF зависит от DSCP в пакетах. Вы можете настроить сопоставление между приоритетом и очередями.
- Когда пакет тегирован, значение 802.1p зависит от приоритета 802.1Q в пакете. Если пакет не тегирован, значение 802.1p зависит от приоритета порта по умолчанию. Вы можете настроить сопоставление между приоритетом 802.1p и очередями.

При пересылке данных порт использует режим планирования для распределения данных по четырем очередям и управления полосой пропускания каждой очереди. Коммутатор поддерживает два режима планирования: взвешенный циклический перебор (WRR), режим Nq-preempt и режим STRICT.

- WRR планирует распределение потоков данных в зависимости от весового коэффициента. На его основе очереди получают свою полосу пропускания. WRR отдает



приоритет очередям с высоким весовым коэффициентом. Для них выделяется большая ширина полосы пропускания.

- В режиме `Nq-preempt` преимущественно пересылаются пакеты с высоким приоритетом. Он в основном используется для передачи чувствительных сигналов, таких как голосовые данные или видеоконференции. Если кадр попадает в очередь с высоким приоритетом, коммутатор прекращает планирование очередей с низким приоритетом и начинает обрабатывать данные очереди с высоким приоритетом. Когда очередь с высоким приоритетом опустеет, коммутатор возвращается к обработке данных из очередей с более низким приоритетом.
- В режиме `STRICT` коммутатор строго следует установленным приоритетам очередей. Пакеты из очереди с высшим приоритетом всегда будут обрабатываться в первую очередь, независимо от загруженности. Коммутатор не перейдет к обработке пакетов из очереди с более низким приоритетом, пока не обработает все пакеты из очереди с более высоким приоритетом.

Основное отличие заключается в том, что `Nq-preempt` может временно прерывать обработку низкоприоритетных очередей для обслуживания высокоприоритетных пакетов, в то время как `STRICT` полностью исключает обработку низкоприоритетных очередей до тех пор, пока не будут обработаны все пакеты из очереди с более высоким приоритетом. Это может привести к задержкам или даже потере пакетов низкого приоритета при высокой загруженности сети.

6.17.3 Настройка с помощью WEB-интерфейса

1. Настройте режим QoS, как показано на следующем рисунке.



Рисунок 107 – Режим QoS

Qos Mode

Варианты: `Disable/WRR/STRICT`

По умолчанию: `STRICT`

Функция: настройка режима планирования для порта.

2. Настройте весовой коэффициент очереди, как показано на следующем рисунке.

Weight of Priority Queues

3--HIGHEST	2--SECHIGH	1--SECLW	0--LOWEST
8	4	2	1

Рисунок 108 – Настройка весового коэффициента очереди



{3-HIGHEST, 2-SECHIGH, 1-SECLOW, 0-LOWEST}

Диапазон: {1–55, 1–55, 1–55, 1–55}

По умолчанию: {8, 4, 2, 1}

Функция: настройка весового коэффициента очереди.

Описание: настройте весовой коэффициент, соблюдая следующие правила:

вес очереди 3 \geq 2 \times вес очереди 2, вес очереди 2 \geq 2 \times вес очереди 1, вес очереди 1 \geq 2 \times вес очереди 0.

3. Настройте режим сопоставления приоритетов портов QoS, как показано на следующем рисунке.

Set the Port Priority

Port	Port-Based	DIFF	802.1P Priority
S1/FE1	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
S1/FE2	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
S1/FE3	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
S1/FE4	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
S1/FE5	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
S1/FE6	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
S1/FE7	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
S1/FE8	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
S4/GE1	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
S4/GE2	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
S4/GE3	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
S4/GE4	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>

Apply

Рисунок 109 – Настройка режима сопоставления приоритетов портов QoS

Set the Port Priority

Варианты: Port-Based/DIFF/802.1P Priority

По умолчанию: 802.1P Priority

Функция: настройка режима сопоставления приоритетов портов.

Описание: для каждого порта можно выбрать только один режим сопоставления приоритетов.

4. Настройте сопоставление приоритетных очередей port-based/802.1p.



Сопоставление очередей в режиме Port-Based соответствует сопоставлению в режиме 802.1p Priority. Если вы хотите настроить любой из двух режимов, установите параметры в таблице сопоставления приоритетов 802.1p. Для этого нажмите <802.1p Priority>, как показано на рисунке 107. Откроется страница настройки.

802.1P Priority 0~7

Priority	Queue
0	0
1	0
2	1
3	1
4	2
5	2
6	3
7	3

Queue: 0--LOWEST, 1--SECLow, 2--SECHIGH, 3--HIGHEST

Apply

Back

Рисунок 110 – Сопоставление приоритетных очередей 802.1p

802.1P Priority

Параметры: {Priority, Queue}

Диапазон: {0–7, 0–3}

По умолчанию: приоритеты 0 и 1 сопоставлены с очередью 0; приоритеты 2 и 3 соответствуют очереди 1. Приоритеты 4 и 5 сопоставлены с очередью 2; приоритеты 6 и 7 – с очередью 3.

Функция: настройка сопоставления между приоритетом 802.1p и очередью.

5. Настройте сопоставление на основе приоритетов DSCP.

Нажмите <DSCP Priority> как показано на рисунке 107. Откроется страница настройки.



DSCP Priority 0-63

DSCP	Qos Queue						
DSCP 0	0	DSCP 1	0	DSCP 2	0	DSCP 3	0
DSCP 4	0	DSCP 5	0	DSCP 6	3	DSCP 7	0
DSCP 8	0	DSCP 9	0	DSCP 10	0	DSCP 11	0
DSCP 12	0	DSCP 13	0	DSCP 14	0	DSCP 15	0
DSCP 16	0	DSCP 17	0	DSCP 18	0	DSCP 19	0
DSCP 20	0	DSCP 21	0	DSCP 22	0	DSCP 23	0
DSCP 24	0	DSCP 25	0	DSCP 26	0	DSCP 27	0
DSCP 28	0	DSCP 29	0	DSCP 30	0	DSCP 31	0
DSCP 32	0	DSCP 33	0	DSCP 34	0	DSCP 35	0
DSCP 36	0	DSCP 37	0	DSCP 38	0	DSCP 39	0
DSCP 40	0	DSCP 41	0	DSCP 42	0	DSCP 43	0
DSCP 44	0	DSCP 45	0	DSCP 46	0	DSCP 47	0
DSCP 48	0	DSCP 49	0	DSCP 50	0	DSCP 51	0
DSCP 52	0	DSCP 53	0	DSCP 54	0	DSCP 55	0
DSCP 56	0	DSCP 57	0	DSCP 58	0	DSCP 59	0
DSCP 60	0	DSCP 61	0	DSCP 62	0	DSCP 63	0

Queue: 0--LOWEST, 1--SECLow, 2--SECHIGH, 3--HIGHEST

Apply

Back

Рисунок 111 – Сопоставление приоритетных очередей DSCP

DSCP Priority

Параметры: {DSCP, Qos Queue}

Диапазон: {0-63, 0-3}

По умолчанию: приоритет от 0 до 63 сопоставлен с очередью 0.

Функция: настройка сопоставления между приоритетом DSCP и очередью.

6.17.4 Пример типовой настройки

Как показано на следующем рисунке, порты 1, 2, 3 и 4 перенаправляют пакеты на порт 5. На порту 1 настроен режим Port-Based. Приоритет порта 1 по умолчанию – 6. Пакеты порта 1 соответствуют очереди 3. Приоритет 802.1p, переносимый пакетами из порта 2, равен 2, который отображается в очередь 1. Приоритет 802.1p, переносимый пакетами порта 3, равен 4 и соответствует очереди 2. Приоритет DSCP, переносимый пакетами порта 4 равен 6 и соответствует очереди 3. Порт 5 использует режим планирования WRR.

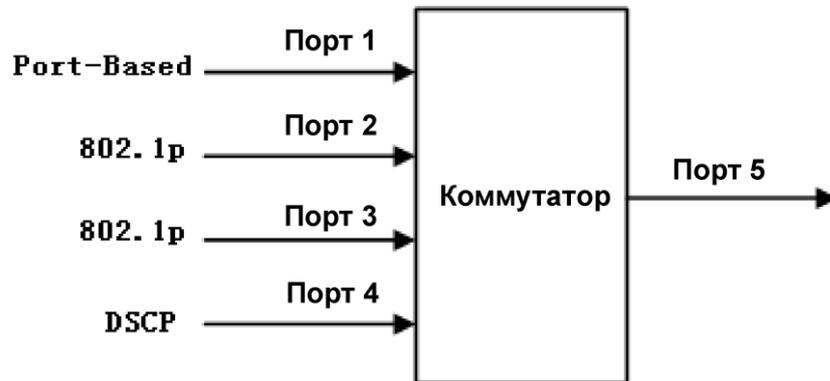


Рисунок 112 – Пример конфигурации QoS

Пакеты, полученные через порт 1 и порт 4, помещаются в очередь 3; пакеты, полученные через порт 2, помещаются в очередь 1; пакеты, полученные через порт 3, помещаются в очередь 2. Согласно сопоставлению очередей и весов, вес очереди 1 равен 2, вес очереди 2 равен 4, а вес очереди 3 равен 8. В результате пропускная способность для пакетов в очереди 1 будет $2/(2+4+8)$, пакетов в очереди 2 – $4/(2+4+8)$, а пакетов в очереди 3 – $8/(2+4+8)$. Пакеты, полученные через порт 1 и порт 4, помещаются в очередь 3 и пересылаются согласно механизму FIFO. Общая доля пропускной способности порта 1 и порта 4 составляет $8/(2+4+8)$.

6.18 Время устаревания MAC-адреса

6.18.1 Введение

Порты коммутатора могут автоматически изучать адреса. Коммутатор добавляет адреса источников (MAC-адрес источника, номер порта коммутатора) полученных кадров в таблицу MAC-адресов. Срок устаревания начинается с момента добавления динамического MAC-адреса в таблицу. Если ни один порт не получает кадр с динамически изученным MAC-адресом в течение одно-двукратного времени устаревания, коммутатор удаляет запись MAC-адреса из таблицы. Таблица статических MAC-адресов не учитывает время устаревания.

6.18.2 Настройка с помощью WEB-интерфейса

Настройте время устаревания MAC-адресов, как показано на следующем рисунке.



Рисунок 113 – Настройка времени устаревания MAC-адресов



MAC Aging Time

Диапазон: 15–3600 секунд

По умолчанию: 300 секунд

Описание: время устаревания MAC-адресов можно настроить в зависимости от условий конкретной сети.

6.19 LLDP

6.19.1 Введение

LLDP (Link Layer Discovery Protocol) предоставляет стандартный механизм обнаружения второго уровня. Он собирает информацию, такую как возможности устройства, адрес, идентификатор устройства и интерфейса в пакет Link Layer Discovery Protocol Data Unit (LLDPDU), и передаёт LLDPDU своим непосредственно подключенным соседям. При получении LLDPDU, соседние устройства сохраняют эту информацию в MIB для предоставления NMS данной информации, а также информации о состоянии соединения между устройствами.

6.19.2 Настройка с помощью WEB-интерфейса

1. Включите протокол LLDP, как показано на следующем рисунке.



Рисунок 114 – Включение LLDP

LLDP

Варианты: Enable/Disable

По умолчанию: Enable

Функция: включение/отключение протокола LLDP.

Описание: если LLDP включен, коммутатор будет отправлять сообщения LLDP своим соседним устройствам, одновременно получая и обрабатывая такие же сообщения от соседних устройств. Если протокол отключен, коммутатор не отправляет и не обрабатывает сообщения LLDP.

2. Просмотрите информацию LLDP о соединениях, как показано на следующем рисунке.



LLDP Information

Local Port	Remote Port	Neighbor IP	Neighbor MAC
1/1	0/1	192.168.0.109	00:00:ee:ee:02:05

Рисунок 115 – Информация LLDP

На этой странице вы можете просмотреть информацию о соседних устройствах, включая номер порта, IP-адрес и MAC-адрес соседнего устройства, подключенного к локальному коммутатору.



Чтобы отобразить информацию LLDP, протокол должен быть включен на двух подключенных устройствах. LLDP – это протокол обнаружения канального уровня, включенный по умолчанию.

6.20 SNTP

6.20.1 Введение

SNTP (Simple Network Time Protocol) синхронизирует время между сервером и клиентом при помощи запросов и ответов. В роли клиента коммутатор синхронизирует свое время с временем сервера. Для одного коммутатора можно назначить несколько SNTP серверов, однако активным будет только один из них. Коммутатор также может служить SNTP-сервером для синхронизации времени клиентов.

Клиент SNTP отправляет запрос каждому серверу, одному за другим, посредством одноадресной рассылки. Сервер, который ответит первым, будет считаться находящимся в активном состоянии. Остальные серверы расцениваются как неактивные.



- Для синхронизации времени по SNTP должен существовать активный сервер SNTP.
- Вся информация о времени, передаваемая протоколом SNTP, является стандартной информацией для часового пояса 0.

6.20.2 Настройка с помощью WEB-интерфейса

1. Включите SNTP. Выберите сервер и установите соответствующие параметры, как показано на следующем рисунке.



SNTP Client State	Enable	
Server IP	192.168.0.23	
Interval Time	16	(16-16284Sec)

Apply

Рисунок 116 – Настройка SNTP

SNTP Client State

Варианты: Enable/Disable

По умолчанию: Disable

Функция: включение/отключение SNTP.

Server IP

Формат: A.B.C.D.

Функция: установка IP-адреса SNTP-сервера. Клиент синхронизирует время с сервером на основе полученных от него пакетов.

Interval Time

Диапазон: 16–16284 с

Функция: настройка интервала отправки запросов синхронизации от SNTP-клиента на сервер.

time zone

Варианты: 0, +1, +2, +3, +4, +5, +6, +7, +8, +9, +10, +11, +12, +13, -1, -2, -3, -4, -5, -6, -7, -8, -9, -10, -11, -12

По умолчанию: 0

Функция: выбор местного часового пояса.

2. Выберите режим синхронизации между клиентом и сервером, как показано на следующем рисунке.

Server Time	2024.08.08 10:38:31	
Device Time	2024.08.08 10:38:45	
update	automatism	Apply

Рисунок 117 – Режим синхронизации времени

Server Time

Функция: отображение последнего временного штампа, полученного с сервера.



Device Time

Функция: отображение локального времени устройства.

update

Варианты: automatism/manual

По умолчанию: automatism

Функция: выбор режима синхронизации времени между устройством и сервером.

3. Просмотрите конфигурацию SNTP, как показано на следующем рисунке. Вы можете установить флажок напротив номера SNTP-сервера и нажать <Delete>, чтобы удалить его.

Number	Server IP	Server State	Time Zone	Interval Time	Synchronization
<input checked="" type="checkbox"/> 1	192.168.0.23	active	+ 8	16	Synch
<input type="checkbox"/> 2	192.168.0.84	repose	+ 8	20	Synch

Delete

Рисунок 118 – Конфигурация SNTP

Server State

Варианты: active/repose

Описание: активный сервер предоставляет клиенту время по протоколу SNTP. Одновременно в активном состоянии может находиться только один сервер.

Synchronization

Чтобы синхронизировать время вручную, нажмите <Synch>.

4. Настройте коммутатор в качестве SNTP-сервера, как показано на следующем рисунке.

SNTP State	Enable
Apply	
Local IP	192.168.0.2
Device Time	2024.08.08 10:47:47

Рисунок 119 – Настройка коммутатора в качестве SNTP-сервера

SNTP State

Варианты: Enable/Disable

По умолчанию: Disable

Функция: включение или отключение функции SNTP-сервера.



6.21 Изоляция портов

6.21.1 Введение

Чтобы реализовать изоляцию пакетов на 2-м уровне, можно добавлять порты в разные VLAN. Однако этот метод приведет нерациональному расходованию ограниченных ресурсов VLAN. Функция изоляции портов предоставляет пользователям более безопасное и гибкое сетевое решение, позволяя изолировать порты в одной и той же VLAN друг от друга.



- Группа изоляции может состоять из портов только одного коммутатора.
- После настройки группы изоляции порты, находящиеся в этой группе, не смогут обмениваться пакетами друг с другом. В то же время настройка не повлияет на связь между портами внутри группы изоляции и портами вне группы.

6.21.2 Настройка с помощью WEB-интерфейса

Разрешите изоляцию портов, как показано на рисунке 120.

Port	Isolate Enable
S1/FE1	<input checked="" type="checkbox"/>
S1/FE2	<input checked="" type="checkbox"/>
S1/FE3	<input checked="" type="checkbox"/>
S1/FE4	<input type="checkbox"/>
S1/FE5	<input type="checkbox"/>
S1/FE6	<input type="checkbox"/>
S1/FE7	<input type="checkbox"/>
S1/FE8	<input type="checkbox"/>
S2/FE1	<input type="checkbox"/>

Рисунок 120 – Конфигурация изоляции портов

Isolate Enable

Варианты: выбрать/отменить выбор

По умолчанию: не выбрано

Функция: включение или отключение функции изоляции для порта.



Устройство поддерживает только одну группу изоляции, что означает, что порты с включенной функцией изоляции не могут обмениваться информацией друг с другом, в то время как связь между портами с включенной изоляцией и с отключенной не будет нарушена.

6.21.3 Пример типовой настройки

Подключите ПК1, ПК2 и ПК3 к портам Ethernet 1, 2 и 3 коммутатора, а порт 4 подключите к внешней сети. Порты 1, 2, 3 и 4 входят в сеть VLAN 1. ПК1, ПК2 и ПК3 не должны обмениваться данными друг с другом, но должны иметь доступ к внешней сети, как показано на рисунке 121.

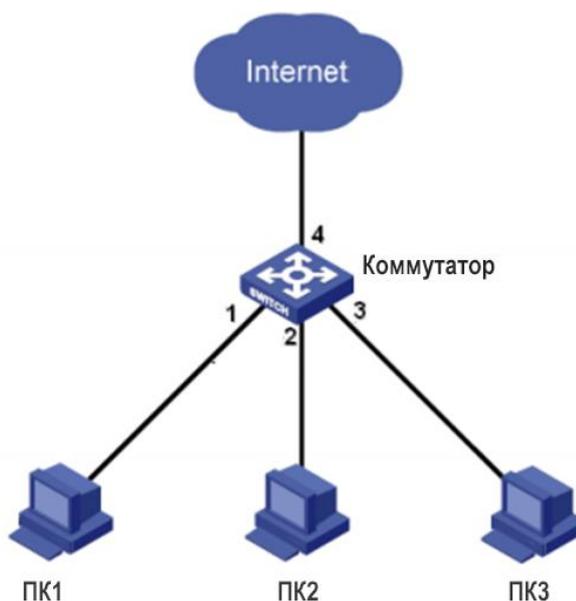


Рисунок 121 – Схема подключения изолированных портов

Добавьте порты 1, 2 и 3 в группу изоляции, чтобы изолировать ПК1, ПК2 и ПК3, как показано на рисунке 120.

6.22 Тревожная сигнализация

6.22.1 Введение

Коммутаторы этой серии поддерживают следующие типы сигналов тревоги:

Power Alarm – сигнализация электропитания. Если включена данная функция, сигнализация будет срабатывать в случае проблем с источником электропитания;



Temperature Alarm – сигнализация температуры. Если функция включена, то сигнал тревоги будет генерироваться, когда температура достигает установленного верхнего или нижнего предела.

IP, MAC Conflict – сигнализация конфликта IP- и MAC-адресов. Если функция включена, то при конфликте IP/MAC будет генерироваться сигнал тревоги.

Port Alarm – сигнализация состояния порта. Если функция включена, то для порта, находящегося в состоянии «Link Down», будет генерироваться сигнал тревоги.

Sy2-Ring/Sy2-RP Alarm – сигнализация состояния кольца. Если функция включена, то при разомкнутом кольце будет сгенерирован сигнал тревоги.



Только мастер-узел Sy2-Ring и корневой узел Sy2-RP поддерживают функцию сигнализации состояния колец.

6.22.2 Настройка с помощью WEB-интерфейса

1. Установите параметры сигнализации, как показано на следующих рисунках.

IP, MAC Conflict

Alarm Name	Enable Alarm	Alarm Time
IP, MAC Conflict	<input checked="" type="checkbox"/>	300 (180~600sec.)

Power Alarm

Alarm Name	Enable Alarm
Power Alarm	<input checked="" type="checkbox"/>

Temperature Alarm

Alarm Name	Enable Alarm	Temperature Alarm Bound
Temperature Alarm	Enable <input type="button" value="v"/>	T-High <input type="button" value="+"/> <input type="text" value="80"/> ~ T-Low <input type="button" value="-"/> <input type="text" value="30"/>

Рисунок 122 – Сигнализация IP/MAC, электропитания и температуры

Port Alarm

Port	Alarm Status	Port	Alarm Status	Port	Alarm Status	Port	Alarm Status
S1/FE1	<input checked="" type="checkbox"/>	S1/FE2	<input checked="" type="checkbox"/>	S1/FE3	<input checked="" type="checkbox"/>	S1/FE4	<input type="checkbox"/>
S1/FE5	<input type="checkbox"/>	S1/FE6	<input type="checkbox"/>	S1/FE7	<input type="checkbox"/>	S1/FE8	<input type="checkbox"/>
S2/FE1	<input type="checkbox"/>	S2/FE2	<input type="checkbox"/>	S2/FE3	<input type="checkbox"/>	S2/FE4	<input type="checkbox"/>
S2/FE5	<input type="checkbox"/>	S2/FE6	<input type="checkbox"/>	S2/FE7	<input type="checkbox"/>	S2/FE8	<input type="checkbox"/>
S3/FE1	<input type="checkbox"/>	S3/FE2	<input type="checkbox"/>	S3/FE3	<input type="checkbox"/>	S3/FE4	<input type="checkbox"/>
S3/FE5	<input type="checkbox"/>	S3/FE6	<input type="checkbox"/>	S3/FE7	<input type="checkbox"/>	S3/FE8	<input type="checkbox"/>
S4/GX1	<input type="checkbox"/>	S4/GX2	<input type="checkbox"/>	S4/GX3	<input type="checkbox"/>	S4/GX4	<input type="checkbox"/>

Рисунок 123 – Сигнализация состояния портов



SY2-RING Alarm	
DT-RING ID	Enable Alarm
1	<input checked="" type="checkbox"/>
2	<input checked="" type="checkbox"/>

SY2-RP Alarm	
DRP ID	Enable Alarm
1	<input checked="" type="checkbox"/>
2	<input checked="" type="checkbox"/>

Рисунок 124 – Сигнализация состояния колец

IP, MAC Conflict

Варианты: выбрать/отменить выбор

По умолчанию: выбрать

Функция: включение или отключение сигнала о конфликте IP/MAC.

Alarm Time

Диапазон: 180–600 с

По умолчанию: 300 с

Функция: настройка интервала обнаружения конфликтов IP/MAC.

Power Alarm

Варианты: выбрать/отменить выбор

По умолчанию: выбрать

Функция: включить или отключить сигнализацию по питанию.

Temperature Alarm (Alarm Enable, T-High~T-Low)

Диапазон: {Enable/Disable, +150°C~-55°C}

По умолчанию: {Disable, +80°C~-30°C}

Функция: включение или отключение сигнала тревоги по температуре и настройка верхнего и нижнего пределов.

Port Alarm

Варианты: выбрать/отменить выбор

По умолчанию: отменить выбор

Функция: включение или отключение сигнализации о состоянии порта.

Sy2-Ring/Sy2-RP Alarm

Варианты: выбрать/отменить выбор

По умолчанию: отменить выбор



Функция: включение или отключение сигнализации о состоянии колец.

2. После включения функции сигнализации информация о тревожных событиях выглядит следующим образом:

Alarm Title	Alarm Status
power	WARN
temperature	NONE
IP Alarm	Normal
MAC Alarm	Normal

Рисунок 125 – Общее представление

Port	Alarm Status						
S1/FE1	Link Up	S1/FE2	Link Up	S1/FE3	Link Down	S1/FE4	-
S1/FE5	-	S1/FE6	-	S1/FE7	-	S1/FE8	-
S2/FE1	-	S2/FE2	-	S2/FE3	-	S2/FE4	-
S2/FE5	-	S2/FE6	-	S2/FE7	-	S2/FE8	-
S3/FE1	-	S3/FE2	-	S3/FE3	-	S3/FE4	-
S3/FE5	-	S3/FE6	-	S3/FE7	-	S3/FE8	-
S4/GX1	-	S4/GX2	-	S4/GX3	-	S4/GX4	-

Рисунок 126 – Состояние портов

DT-RING ID	Alarm Status
2	Ring Open
1	Ring Close

DRP ID	Alarm Status
1	Normal
2	Alarm

Рисунок 127 – Состояние колец

power

Варианты: Normal/WARN

Описание: после включения сигнала тревоги для неисправного входа питания отображается «WARN».



temperature

Варианты: NONE/HIGH/LOW

Описание: когда температура коммутатора равна верхнему пределу или превышает его, отображается «HIGH»; когда температура равна нижнему пределу или опускается ниже его, отображается «LOW»; в остальных случаях отображается «NONE».

IP/MAC Alarm

Варианты: Normal/Alarm

Описание: при возникновении конфликта IP/MAC отображается сообщение «Alarm»; в противном случае отображается «Normal».

Port Alarm

Варианты: Link Up/Link Down

Описание: после включения сигнализации для порта, подключенного правильно, отображается сообщение «Link Up». Для отключенного или подключенного некорректно порта отображается «Link Down».

Sy2-Ring/Sy2-RP Alarm

Варианты для Sy2-Ring: Ring Open/Ring Close

Варианты для Sy2-RP: Normal/Alarm

Описание: после включения сигнализации для разомкнутого кольца отображается сообщение «Ring Open/Alarm», а для замкнутого – «Ring Close/Normal».

6.23 Сигнализация на основе трафика порта

6.23.1 Введение

Благодаря функции сигнализации коммутатор генерирует сигнал тревоги, если скорость трафика порта превышает указанный порог или возникает ошибка CRC.



- Функция сигнализации о трафике основана на порте. Сигнал тревоги генерируется только в том случае, если функция включена на порту.
- Функция сигнализации зависит от направления. Входящему и исходящему трафику соответствуют разные тревоги.
- Если возникает ошибка CRC, об этом событии генерируется отдельный сигнал.

6.23.2 Настройка с помощью WEB-интерфейса

1. Настройте сигнализацию трафика порта, как показано на следующем рисунке.



Port	S1/FE1	▼
Alarm Type	Input Rate	▼
Alarm Status	enable	▼
Alarm Threshold	100	bps ▼

Apply Refresh

Рисунок 128 – Настройка сигнализации трафика порта

Port

Варианты: все порты коммутатора

Функция: выбор порта для сигнализации о трафике.

Alarm Type

Варианты: Input Rate/Output Rate/CRC Error

Функция: настройка тревоги на основе входящего/исходящего трафика или ошибок CRC.

Alarm Status

Options: enable/disable

По умолчанию: disable

Функция: включить или отключить выбранный тип сигнала тревоги.

Alarm Threshold

Диапазон: 1–1000000000 бит/с или 1–1000000кбит/с.

Функция: настройка порога для генерации сигнала тревоги.

2. Просмотрите информацию о тревогах на основе трафика порта, как показано на следующем рисунке.

Port	Input Rate	Alarm Status	Output Rate	Alarm Status	Error CRC	Alarm Status		
S1/FE1	enable	100bps	alarm	enable	1000bps	alarm	enable	alarm
S1/FE2	enable	100kbps	normal	enable	100bps	normal	enable	normal
S1/FE3	disable	-	-	disable	-	-	disable	-
S1/FE4	disable	-	-	disable	-	-	disable	-
S1/FE5	disable	-	-	disable	-	-	disable	-
S1/FE6	disable	-	-	disable	-	-	disable	-
S1/FE7	disable	-	-	disable	-	-	disable	-
S1/FE8	disable	-	-	disable	-	-	disable	-
S4/GE1	disable	-	-	disable	-	-	disable	-
S4/GE2	disable	-	-	disable	-	-	disable	-
S4/GE3	disable	-	-	disable	-	-	disable	-
S4/GE4	disable	-	-	disable	-	-	disable	-

Рисунок 129 – Информация о тревогах на основе трафика



6.24 GMRP

6.24.1 Протокол GARP

Протокол регистрации общих атрибутов (GARP) используется для распространения, регистрации и отмены определенной информации (VLAN, многоадресного адреса) между коммутаторами в одной сети. На базе GARP работают протоколы GVRP и GMRP.

Благодаря GARP, информация о настройках коммутатора может быть передана по всей локальной сети. Объекты GARP, передают друг другу инструкции о регистрации или отмене тех или иных настроек путём отправки соответствующих Join и Leave-сообщений.

GARP предусматривает три типа сообщений: Join, Leave и LeaveAll.

- Когда объект GARP хочет передать свои настройки другим коммутаторам, он отправляет Join-сообщение. Join-сообщения бывают двух типов: JoinEmpty и JoinIn. Сообщение JoinIn отправляется для зарегистрированного свойства, в то время как JoinEmpty – для свойства, которое ещё не было зарегистрировано.
- Когда объект GARP хочет удалить свои настройки с других коммутаторов, он отправляет сообщение Leave.
- После запуска объекта GARP, он начинает отсчитывать период LeaveAll. Когда период заканчивается, объект отправляет сообщение LeaveAll.



Объект GARP означает порт, на котором включен протокол GARP.

Для работы GARP использует таймеры Hold, Join, Leave и LeaveAll.

Таймер Hold. При получении сообщения о регистрации настроек, объект GARP не отправляет сообщение Join сразу, а запускает таймер Hold. Когда таймер заканчивает отсчёт, объект отправляет все сообщения о настройках, полученные за этот период в одном Join-сообщении, что уменьшает количество передаваемых по сети данных.

Таймер Join. Для того, чтобы убедиться, что Join-сообщения получены другими объектами, после отправки сообщения Join объект GARP запускает таймер Join. Если за период до истечения установленного срока в ответ не получено JoinIn-сообщение, объект отправляет Join-сообщение снова. В противном случае, сообщение Join не отправляется.

Таймер Leave. Если объект GARP хочет удалить информацию об атрибуте, он отправляет Leave-сообщение. Объект, получивший это сообщение, запускает таймер Leave. Если он не получает ни одного Join-сообщения до истечения таймера, он удаляет информацию о данном атрибуте.

Таймер LeaveAll. При старте объекта GARP, запускается таймер LeaveAll. По его истечении, объект отправляет LeaveAll-сообщение для того, чтобы другие объекты GARP перерегистрировали все атрибуты. После этого объект запускает таймер LeaveAll заново.



6.24.2 Протокол GMRP

GMRP – протокол регистрации многоадресной рассылки, основанный на принципах GARP. Он используется для поддержки информации о многоадресных группах на коммутаторах. Все коммутаторы, поддерживающие GMRP, могут получать регистрационную информацию от других коммутаторов, динамически обновлять информацию о зарегистрированных многоадресных группах, а также передавать собственную регистрационную информацию другим коммутаторам. Механизм обмена информацией гарантирует единообразие информации о многоадресной рассылке на всех GMRP-коммутаторах сети.

Если коммутатор или терминал хотят войти или выйти из многоадресной группы, GMRP-порт передаёт информацию об этом в широковещательном режиме на все порты своей VLAN.

6.24.3 Описание

Порт-агент: обозначает порт, на котором включены функции GMRP и агента.

Порт распространения: обозначает порт, на котором включена только функция GMRP, без функции агента.

Динамически изученные многоадресные записи GMRP и записи агентов передаются портом распространения на аналогичные порты устройств нижнего уровня.

Все таймеры GMRP в одной сети должны быть согласованными, чтобы предотвратить взаимные помехи. Таймеры должны следовать следующим правилам:

Hold < Join, 2*Join < Leave, Leave < LeaveAll.

6.24.4 Настройка с помощью WEB-интерфейса

1. Включите глобальный протокол GMRP, как показано на следующем рисунке.

Protocol Configure

GMRP State	Enable
LeaveAll Timer	10000 ms

Apply

Рисунок 130 – Глобальная конфигурация GMRP

GMRP State

Варианты: Enable/Disable

По умолчанию: Disable

Функция: включение или отключение глобальной функции GMRP. Нельзя использовать одновременно с IGMP Snooping.



LeaveAll Timer

Диапазон: 100–327600 мс

По умолчанию: 10000 мс

Функция: указывает интервал отправки сообщений LeaveAll. Значение должно быть кратно 100.

Описание: если таймеры LeaveAll на разных устройствах истекают одновременно, одновременно будет отправлено несколько сообщений LeaveAll, что приведет к увеличению количества ненужных пакетов. Чтобы предотвратить эту проблему, фактическое время ожидания таймера LeaveAll представляет собой случайное значение между указанным числом и числом, в 1,5 раза больше указанного.

2. Настройте функцию GMRP на каждом порту, как показано на следующем рисунке.

Port Configure

Port	GMRP Enable	Agent Enable	Hold Timer	Join Timer	Leave Timer
S1/FE1	Enable	Enable	100 ms	500 ms	3000 ms
S1/FE2	Enable	Disable	100 ms	500 ms	3000 ms
S1/FE3	Enable	Disable	100 ms	500 ms	3000 ms
S1/FE4	Disable	Disable	100 ms	500 ms	3000 ms
S1/FE5	Disable	Disable	100 ms	500 ms	3000 ms
S1/FE6	Disable	Disable	100 ms	500 ms	3000 ms
S1/FE7	Disable	Disable	100 ms	500 ms	3000 ms
S1/FE8	Disable	Disable	100 ms	500 ms	3000 ms
S4/GE1	Disable	Disable	100 ms	500 ms	3000 ms
S4/GE2	Disable	Disable	100 ms	500 ms	3000 ms
S4/GE3	Disable	Disable	100 ms	500 ms	3000 ms
S4/GE4	Disable	Disable	100 ms	500 ms	3000 ms

Apply

Рисунок 131 – Настройка GMRP на портах

GMRP Enable

Варианты: Enable/Disable

По умолчанию: Disable

Функция: включение или отключение функции GMRP на порту.

Agent Enable

Варианты: Enable/Disable

По умолчанию: Disable

Функция: включение или отключение агента GMRP на порту.



- Агентский порт не может распространять запись агента.
- Чтобы включить функцию агента GMRP на порту, необходимо сначала включить функцию GMRP.

Hold Timer

Диапазон: 100–327600 мс

По умолчанию: 100 мс

Описание: таймер удержания. Это значение должно быть кратно 100. Рекомендуется устанавливать таймеры удержания на всех портах с поддержкой GMRP на одно и то же время.

Join Timer

Диапазон: 100–327600 мс

По умолчанию: 500 мс

Описание: это значение должно быть кратно 100. Рекомендуется устанавливать таймеры Join на всех портах с поддержкой GMRP на одно и то же время.

Leave Timer

Диапазон: 100–327600 мс

По умолчанию: 3000 мс

Описание: это значение должно быть кратно 100. Рекомендуется устанавливать таймеры Leave на всех портах с поддержкой GMRP на одно и то же время.

3. Добавьте запись агента GMRP, как показано на следующем рисунке.

GMRP Agent Set

MAC	010000000001
VLAN ID	1 (1-4093)

Port List

NOTE: Multicast propagation port cannot be set as member port!

Member Port List	Source Port List
S1/FE1	

<< >>

Apply

Рисунок 132 – Настройка записи агента GMRP



MAC

Формат: НННННННННННН (Н — шестнадцатеричное число)

Функция: настройка MAC-адреса многоадресной группы. Младший бит первого байта равен 1.

VLAN ID

Варианты: номера всех существующих VLAN.

Функция: настройка идентификатора VLAN для записи агента GMRP.

Описание: запись агента GMRP может быть отправлена только с порта распространения с идентификатором VLAN, совпадающим с идентификатором VLAN этой записи.

Member Port List

Описание: выбор порта-участника для записи агента. Можно выбрать только из портов с поддержкой агента GMRP.

Source Port List

Варианты: все порты с поддержкой агента GMRP.

Описание: список исходных портов.

4. Просмотрите, измените или удалите запись агента GMRP, как показано на следующем рисунке.

GMRP Agent List

Index	MAC	VLAN ID	Member Port
<input type="radio"/> 1	01-00-00-00-00-01	1	S1/FE1
<input type="radio"/> 2	01-00-00-00-00-02	2	S1/FE1

Рисунок 133 – Операции с записями агентов GMRP

Запись агента GMRP состоит из MAC-адреса, идентификатора VLAN и порта-участника. Чтобы удалить запись, выберите ее и нажмите <Delete>. Чтобы изменить запись, выберите ее и нажмите <Modify>.

5. Просмотрите участников многоадресной рассылки этой записи агента на подключенном соседнем устройстве, как показано на следующем рисунке.

Должны быть соблюдены следующие условия:

- GMRP включен на взаимосвязанных устройствах.



- Два порта, соединяющие устройства, должны быть портами распространения, а идентификатор VLAN порта распространения на локальном устройстве должен совпадать с идентификатором в записи агента.

GMRP Dynamic Multicast List

Index	Multicast MAC	VLAN ID	Member Port
1	01-00-00-00-00-01	1	S0/FE1

Рисунок 134 – Таблица динамической многоадресной рассылки GMRP

GMRP Dynamic Multicast List

Параметры: {Index, Multicast MAC, VLAN ID, Member Port}

Функция: просмотр динамических записей многоадресной рассылки GMRP.

6.24.5 Пример типовой настройки

Как показано на рисунке 135, коммутатор А и коммутатор В подключены через порт 2. Порт 1 коммутатора А настроен как порт агента и создает две многоадресные записи:

- MAC-адрес: 01-00-00-00-00-01, VLAN: 1;
- MAC-адрес: 01-00-00-00-00-02, VLAN: 2.

После настройки различных атрибутов VLAN на портах наблюдайте за динамической регистрацией между коммутаторами и обновлением информации о многоадресной рассылке.

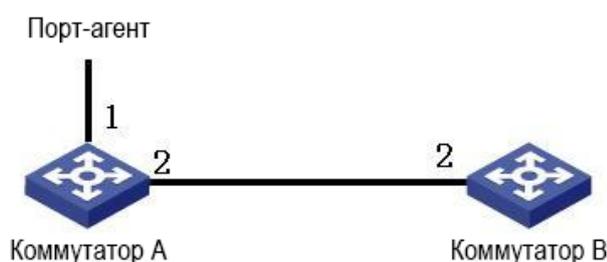


Рисунок 135 – Сеть GMRP

Настройка коммутатора А:

1. Включите глобальную функцию GMRP на коммутаторе А; установите для таймера LeaveAll значение по умолчанию, как показано на рисунке 130.
2. Включите функцию GMRP и функцию агента для порта 1; включите только функцию GMRP для порта 2; установите для таймеров значения по умолчанию, как показано на рисунке 131.



3. Настройте многоадресную запись агента. Установите <MAC address, VLAN ID, Member port> на <01-00-00-00-00-01, 1, 1> и <01-00-00-00-00-02, 2, 1>, как показано на рисунке 132.

Настройка коммутатора В:

4. Включите глобальную функцию GMRP на коммутаторе В; установите для таймера LeaveAll значение по умолчанию, как показано на рисунке 130.

5. Включите функцию GMRP на порту 2; установите для таймеров значения по умолчанию, как показано на рисунке 131.

В таблице 8 перечислены динамические записи многоадресной рассылки GMRP на коммутаторе В.

Таблица 8 – Динамические многоадресные записи

Атрибут порта 2 на коммутаторе А	Атрибут порта 2 на коммутаторе В	Многоадресные записи, полученные на коммутаторе В
Untag1	Untag1	MAC: 01-00-00-00-00-01 VLAN ID: 1 Member port: 2
Untag2	Untag2	MAC: 01-00-00-00-00-02 VLAN ID: 2 Member port: 2
Untag1	Untag2	MAC: 01-00-00-00-00-01 VLAN ID: 2 Member port: 2

6.25 RMON

6.25.1 Введение

Основанный на архитектуре SNMP, удаленный мониторинг сети (RMON) позволяет устройствам управления сетью активно отслеживать управляемые устройства и управлять ими. Сеть RMON обычно включает в себя станцию сетевого управления (NMS) и агентов. NMS управляет агентами, а они собирают статистику по различным типам трафика на своих портах.

RMON в основном выполняет функции сбора статистики и сигнализации. С помощью функции статистики агенты могут периодически собирать данные по различным типам трафика на портах, например, количество пакетов, полученных из определенного



сегмента сети за определенный период. Функция сигнализации заключается в том, что агенты могут отслеживать значения указанных переменных MIB. Когда значение достигает порога тревоги (например, количество пакетов достигает указанного значения), агент может автоматически записывать тревожное событие в журнал RMON или отправлять сообщение Trap на устройство управления.

6.25.2 Группы RMON

Согласно RFC2819 определяется несколько групп RMON. Устройства данной серии поддерживают группу статистики, группу истории, группу событий и группу сигналов тревоги в общедоступной базе MIB. Каждая группа может содержать до 32 записей.

➤ Группа статистики

С помощью группы статистики система собирает статистику по всем типам трафика на портах и сохраняет ее в таблице статистики Ethernet для дальнейшего запроса устройством управления. Статистика включает количество сетевых коллизий, пакетов с ошибками CRC, пакетов недостаточного или слишком большого размера, широковещательных и многоадресных пакетов, полученных байтов и полученных пакетов. После успешного создания записи статистики на указанном порту группа статистики продолжает подсчет пакетов на этом порту и статистика представляет собой постоянно накапливаемое значение.

➤ Группа истории

Группа истории требует, чтобы система периодически производила выборку всех видов трафика на портах и сохраняет значения выборки в таблице записей истории для дальнейшего запроса устройством управления. Группа истории подсчитывает статистические значения всех видов данных в интервале выборки.

➤ Группа событий

Группа событий используется для определения индексов событий и методов обработки событий. События, определенные в группе, используются для настройки элемента группы сигналов тревоги. Событие инициируется, когда контролируемое устройство достигает установленного состояния тревоги. Система обрабатывает события следующими способами:

Log: регистрирует событие и связанную с ним информацию в таблице журнала событий.

Trap: отправляет trap-сообщение в NMS и информирует NMS о событии.

Log-Trap: регистрирует событие и отправляет trap-сообщение в NMS.

None: никакие действия не выполняются.

➤ Группа сигналов тревоги

Управление сигнализацией RMON может отслеживать указанные переменные сигналов тревоги. После определения записей сигналов тревоги система получит значения контролируемых переменных этих сигналов за определенный период. Когда значение переменной больше или равно верхнему пределу, срабатывает тревожное событие превышения контролируемого значения. Когда значение тревожной переменной меньше



или равно нижнему пределу, срабатывает сигнал о падении значения. Тревоги будут обрабатываться в соответствии с определением события.



Если выборочное значение тревожной переменной несколько раз превышает пороговое значение в одном и том же направлении, то тревожное событие инициируется только в первый раз. Поэтому сигнализация повышения и понижения контролируемого значения генерируется попеременно.

6.25.3 Настройка с помощью WEB-интерфейса

1. Настройте таблицу статистики, как показано на следующем рисунке.

Set Statistics Information

Index	Owner	DataSource
1	a	S1/GX1

Apply

Рисунок 136 – Таблица статистики RMON

Index

Диапазон: 1–65535

Функция: настройка номера записи статистики.

Owner

Диапазон: 1–32 символа

Функция: настройка имени записи статистики.

Data Source

Функция: выбор порта, статистику которого нужно собирать.

2. Настройте таблицу истории, как показано на следующем рисунке.

Index	2
DataSource	S1/GX1
Owner	b
Sampling Number	10
Sampling Space	20

Apply

Рисунок 137 – Таблица истории RMON



Index

Диапазон: 1–65535

Функция: настройка номера записи истории.

Owner

Диапазон: 1–32 символа

Функция: настройка имени записи истории.

Data Source

Функция: выбор порта, статистику которого нужно собирать.

Sampling Number

Диапазон: 1–65535

Функция: настройка количества выборок для порта.

Sampling Space

Диапазон: 1–3600 с

Функция: настройка периода выборки для порта.

3. Настройте таблицу событий, как показано на следующем рисунке.

Index	<input type="text" value="3"/>
Owner	<input type="text" value="c"/>
Event Type	<input type="text" value="LogandTrap"/> ▾
Event Description	<input type="text" value="alarm"/>
Event Community	<input type="text" value="public"/>

Рисунок 138 – Таблица событий RMON

Index

Диапазон: 1–65535

Функция: настройка номера записи события.

Owner

Диапазон: 1–32 символа

Функция: настройка имени записи события.



Event Type

Варианты: NONE/LOG/Snmp-Trap/Log and Trap

По умолчанию: NONE

Функция: настройка типа события для сигнализации, то есть режима обработки тревожных событий.

Event Description

Диапазон: 1–127 символов.

Функция: описание события.

Event Community

Диапазон: 1–127 символов.

Функция: Настройка имени комьюнити для отправки trap-сообщений. Значение должно быть идентично значению в SNMP.

4. Настройте таблицу сигналов тревоги, как показано на следующем рисунке.

Index	4
OID	1.3.6.1.2.1.2.2.1.16
Owner	d
DataSource	S1/GX1
Sampling Type	Absolute
Alarm Type	RisingAlarm
Sampling Space	20
Rising Threshold	100
Falling Threshold	20
Rising EventIndex	3
Falling EventIndex	3

Apply

Рисунок 139 – Таблица сигналов тревоги RMON

Index

Диапазон: 1–65535

Функция: настройка номера записи тревоги.

OID

Описание: указывает OID текущего узла MIB.

**Owner**

Диапазон: 1–32 символа

Функция: настройка имени записи тревоги.

Data Source

Функция: выбор порта, информацию о котором необходимо отслеживать.

Sampling Type

Варианты: Absolute/Delta

По умолчанию: Absolute

Функция: тип выборки «Absolute» используется для измерения точного значения переменной в конце периода выборки. Тип «Delta» используется для измерения изменения значения переменной за период выборки.

Alarm Type

Варианты: RisingAlarm/FallingAlarm/RisOrFallAlarm

По умолчанию: RisingAlarm

Функция: выбор типа сигнала тревоги, включая сигнал тревоги при превышении порогового значения, сигнал при падении ниже порогового значения, а также сигнал при падении и превышении.

Sampling Space

Диапазон: 1–65535

Функция: настройка периода выборки. Значение должно быть идентично значению в таблице истории.

Rising Threshold

Диапазон: 0–65535

Функция: настройка верхнего порога. Когда значение выборки превышает пороговое значение и тип сигнала тревоги установлен на RisingAlarm или RisOrFallAlarm, генерируется сигнал тревоги и запускается Rising Event Index.

Falling Threshold

Диапазон: 0–65535

Функция: настройка нижнего порога. Когда значение выборки опускается ниже порогового значения и тип сигнала тревоги установлен на FallingAlarm или RisOrFallAlarm, генерируется сигнал тревоги и запускается Falling Event Index.

Rising Event Index

Диапазон: 0–65535

Функция: настройка индекса нарастающего события, то есть режима обработки сигналов тревоги переднего фронта.

Falling Event Index



Функция: настройка индекса спадающего события, то есть режима обработки сигналов тревоги заднего фронта.

6.26 Системный журнал

6.26.1 Введение

Функция логирования записывает в системный журнал информацию о работе коммутатора, позволяя администратору читать историю событий и обнаруживать неисправности.

Журналирование выполняет следующие задачи:

- Отслеживает и записывает проблемы с электропитанием устройства, случаи превышения нормального диапазона температур, конфликты IP/MAC-адресов, проблемы, связанные с портами коммутатора, включая аномальный трафик и неисправности в кольцевой топологии Sy2-Ring.
- Записывает события, когда сеть перегружена из-за избыточного широковещательного трафика.
- Фиксирует случаи перезапуска системного программного обеспечения.

6.26.2 Описание

Текущий журнал содержит максимум 1024 записи. Когда возникает более 1024 записей, новые данные записываются поверх старых.

6.26.3 Настройка с помощью WEB-интерфейса

1. Включите функцию логирования, как показано на следующем рисунке.



Рисунок 140 – Настройка состояния журналирования

Enable Runlog

Варианты: Enable/Disable

По умолчанию: Enable

Функция: включение или отключение функции записи событий в журнал. Если функция включена, текущая информация будет записываться.



2. Настройте функцию выгрузки журнала на FTP-сервер, как показано на следующем рисунке.

RunLog Uploaded

FTP Server IP Address	<input type="text" value="192.168.0.23"/>
FTP File Name	<input type="text" value="log.txt"/>
FTP User Name	<input type="text" value="admin"/>
FTP Password	<input type="password" value="•••"/>

Apply

Рисунок 141 – Настройка записи журнала на сервер

FTP Server IP Address

Формат: A.B.C.D.

Функция: настройка IP-адреса FTP-сервера.

FTP File Name

Диапазон: 1–20 символов

Функция: настройка имени файла журнала, сохраняемого на сервере.

FTP User Name

Диапазон: 1–20 символов

Функция: настройка имени пользователя FTP.

FTP Password

Диапазон: 1–20 символов

Функция: настройка пароля FTP.



Программное обеспечение FTP-сервера должно быть запущено во время загрузки журнала.

3. Просмотрите текущий журнал, как показано на следующем рисунке.



Performance log

Index	LogType	Time	Description
10	Ring Open/Close	THU SEP 13 15:24:42 2024	Ring alarm: entity id:1 state:Ring open
9	PortLink Alarm	THU SEP 13 15:24:42 2024	Port alarm: entity id:1/2 port:1/2 state:Link down
8	Ring Open/Close	THU SEP 13 15:24:07 2024	Ring alarm: entity id:1 state:Ring close
7	PortLink Alarm	THU SEP 13 15:24:07 2024	Port alarm: entity id:1/2 port:1/2 state:Link up
6	Output rate	THU SEP 13 15:23:44 2024	Output alarm: entity id:1 state:Alarm
5	Input rate	THU SEP 13 15:23:43 2024	Input alarm: entity id:1 state:Alarm
4	PortLink Alarm	THU SEP 13 15:23:39 2024	Port alarm: entity id:1/1 port:1/1 state:Link up
3	Output rate	THU SEP 13 15:22:58 2024	Output alarm: entity id:2 state:Normal
2	PortLink Alarm	THU SEP 13 15:22:55 2024	Port alarm: entity id:1/2 port:1/2 state:Link down
1	PowerAlarm	THU SEP 13 15:21:49 2024	Power alarm: entity id:2 state:Power down
0	Output rate	THU SEP 13 15:21:28 2024	Output alarm: entity id:2 state:Alarm

Рисунок 142 – Запрос журнала

Performance log

Параметры: {Index, LogType, Time, Description}

Функция: отображение текущего журнала.

6.27 Настройка одноадресной рассылки

6.27.1 Введение

При пересылке пакета коммутатор ищет порт пересылки в таблице MAC-адресов на основе MAC-адреса назначения пакета.

MAC-адрес может быть статическим или динамическим.

Статические MAC-адреса настроены вручную. Они имеют наивысший приоритет (не переопределяются динамическими MAC-адресами) и действительны постоянно.

Динамические MAC-адреса запоминаются коммутатором при пересылке данных и действительны только в течение определенного периода. Коммутатор периодически обновляет свою таблицу MAC-адресов. При получении кадра данных для пересылки коммутатор узнает MAC-адрес его источника, устанавливает сопоставление с принимающим портом и запрашивает порт пересылки в таблице MAC-адресов на основе MAC-адреса назначения кадра. Если совпадение обнаружено, коммутатор пересылает кадр данных из соответствующего порта. Если совпадение не найдено, коммутатор передает кадр в своем широковещательном домене.

Коммутатор поддерживает максимум 256 статических одноадресных записей.

6.27.2 Настройка с помощью WEB-интерфейса

1. Добавьте запись статического MAC-адреса, как показано на следующем рисунке.



Set FDB Unicast

MAC	VLAN ID (1~4093)	Member Port
ecde12345678	2	S1/FE2

Apply

Рисунок 143 – Добавление статической одноадресной записи в таблицу FDB

MAC

Формат: НННННННННННН (Н – шестнадцатеричное число)

Функция: настройка юникастового MAC-адреса. Младший бит в первом байте равен 0.

VLAN ID

Варианты: идентификаторы всех созданных VLAN

Member Port

Варианты: все порты коммутатора

Функция: выбор порта для пересылки пакетов, предназначенных для MAC-адреса. Порт должен находиться в указанной VLAN.

2. Просмотрите список статических адресов одноадресной рассылки, как показано на следующем рисунке.

FDB Unicast Mac List

Index	MAC	VLAN ID	Member Port
<input type="radio"/>	ec:de:12:34:56:78	2	S1/FE2
<input type="radio"/>	00:01:01:01:01:01	1	S1/FE1

Add

Delete

Modify

Рисунок 144 – Статическая таблица FDB одноадресной передачи

Выберите запись. Вы можете удалить или изменить ее.

3. Просмотрите список динамических адресов одноадресной рассылки, как показано на следующем рисунке.



Dynamic Unicast Mac List

Index	MAC	VLAN ID	Member Port
1	ac:16:2d:03:a7:22	1	S1/FE2
2	70:71:bc:95:cc:22	1	S1/FE2
3	d0:67:e5:29:82:6e	1	S1/FE2
4	d4:be:d9:b9:47:ce	1	S1/FE2
5	c8:9c:dc:57:3e:96	1	S1/FE2
6	00:00:00:98:00:54	1	S1/FE2
7	40:16:9f:f0:b0:0e	1	S1/FE2
8	d0:67:e5:19:71:e2	1	S1/FE2
9	80:c1:6e:e0:5b:9a	1	S1/FE2
10	d0:27:88:70:5b:cd	1	S1/FE2
11	d4:be:d9:b9:46:fb	1	S1/FE2
12	d4:be:d9:b9:46:bb	1	S1/FE2
13	44:87:fc:40:02:be	1	S1/FE2
14	c8:3a:35:d3:cc:2a	1	S1/FE2
15	d0:27:88:45:ff:25	1	S1/FE2
16	00:1e:cd:17:83:6d	1	S1/FE2

Clear

Рисунок 145 – Динамическая таблица FDB одноадресной передачи

6.28 DHCP

В связи с постоянным увеличением масштаба сети и ростом её сложности, в условиях частого перемещения компьютеров (таких как ноутбуки или устройства с беспроводным подключением), а также ввиду того, что число компьютеров значительно превышает выделяемые для них IP-адреса, протокол BootP, предназначенный для статической конфигурации хоста, всё чаще становится неспособным удовлетворить существующие потребности. Для быстрого доступа в сеть, выхода из сети и улучшения коэффициента использования ресурсов IP-адресов было необходимо разработать автоматический механизм распределения IP-адресов на основе протокола BootP, в результате чего был представлен протокол динамической конфигурации хоста DHCP.

Данный протокол работает согласно модели «клиент-сервер». На этапе конфигурации клиент обращается к серверу, который в ответ сообщает необходимые параметры настроек, такие как IP-адрес, используя динамическую конфигурацию IP-адресов. На рисунке 146 показана типичная структура применения DHCP-протокола.

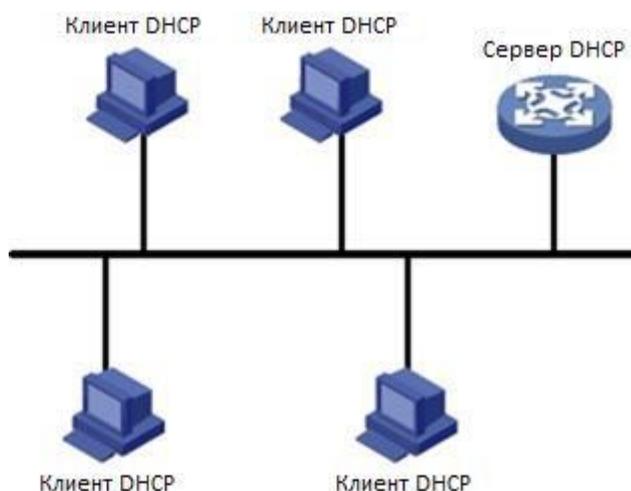


Рисунок 146 – Типовая схема DHCP



В процессе динамического распределения IP-адресов происходит отправка широковещательного сообщения, поэтому необходимо, чтобы DHCP-клиент и DHCP-сервер находились в одном сегменте. Если они находятся в разных сегментах, чтобы получить IP-адрес и другие параметры конфигурации, клиент может связаться с сервером через ретранслятор DHCP-протокола. Коммутаторы данной серии не поддерживают ретрансляцию DHCP, поэтому клиент и сервер должны находиться в одном сегменте.

Протокол DHCP поддерживает два механизма распределения IP-адресов. Статическое распределение: сетевой администратор статично привязывает фиксированные IP-адреса к нескольким конкретным клиентам, таким как, например, WWW-сервер, и отправляет привязанные IP-адреса клиентам через протокол DHCP. Динамическое распределение: DHCP-сервер производит динамическую выдачу IP-адреса клиенту. Этот механизм распределения может назначить для клиента постоянный IP-адрес или адрес с ограниченным сроком пользования. Когда время аренды адреса истекает, клиент должен повторно запросить IP-адрес. Сетевой администратор может выбирать для каждого клиента свой механизм распределения по протоколу DHCP.

6.28.1 Настройка сервера DHCP

6.28.1.1 Введение

DHCP-сервер – это поставщик услуг DHCP-протокола. Он использует DHCP-сообщения для связи с клиентом, чтобы назначить ему подходящий IP-адрес и при необходимости сообщить другие сетевые параметры. DHCP-сервер обычно используется для выделения IP-адресов в следующих случаях:

- большой масштаб сети. При ручном распределении рабочая нагрузка возрастает и управлять всей сетью становится трудно;



- количество хостов превышает число распределяемых IP-адресов, отчего становится невозможно назначить фиксированный IP-адрес каждому хосту;
- только несколько хостов в сети нуждаются в фиксированных IP-адресах.

6.28.1.2 Пул адресов DHCP

DHCP-сервер выбирает IP-адрес из пула адресов и выделяет его клиенту вместе с другими параметрами. Существует следующий порядок распределения IP-адресов:

- IP-адрес, статически привязанный к MAC-адресу клиента или идентификатору порта, подключающегося к серверу;
- IP-адрес, записанный на DHCP-сервере, который когда-либо был выделен клиенту;
- IP-адрес, указанный в сообщении запроса клиента;
- Первый свободный IP-адрес, найденный в пуле адресов;
- Если доступный IP-адрес отсутствует, проверяется IP-адрес, срок аренды которого истекает и тот, у которого был конфликт. Если такой IP-адрес найден, он выделяется клиенту, если нет – подключения не происходит.

6.28.1.3 Настройка с помощью WEB-интерфейса

1. Включите DHCP-сервер, как показано на следующем рисунке.



Рисунок 147 – Состояние DHCP-сервера

DHCP server status

Варианты: Enable/Disable

По умолчанию: Disable

Функция: выбор текущего коммутатора в качестве DHCP-сервера для выделения IP-адресов клиентам. Если во время включения функции выбран VLAN ID, DHCP-сервер выделяет IP-адреса только клиентам, отправляющим запрос в эту VLAN. Если выбран параметр «All Vlans», DHCP-сервер выделяет IP-адреса всем клиентам, отправляющим запрос. При выборе параметра «Vlan-ID» разрешается указать только один идентификатор VLAN.

2. Выберите режим DHCP-сервера, как показано на следующем рисунке.



Рисунок 148 – Режимы DHCP-сервера



DHCP server mode

Варианты: Common-Mode/Port-Mode

По умолчанию: Port-Mode

Описание: общий режим «Common-Mode» означает динамическое распределение IP-адресов и назначение фиксированных IP-адресов определенным MAC-адресам. «Port-Mode» означает назначение конкретного IP-адреса через определенный порт коммутатора.

3. Настройка режима на основе порта

При выборе на DHCP-сервере режима «Port-Mode» привяжите к портам статические IP-адреса для их дальнейшего распределения клиентам, как показано на следующем рисунке.

Port	IP
S1/FE1	
S1/FE2	
S1/FE3	192.168.0.6
S1/FE4	
S1/FE5	
S1/FE6	
S1/FE7	
S1/FE8	
S2/FE1	

Рисунок 149 – Привязка IP-адреса к порту

Выделение IP-адреса на основе порта – это статическая настройка. Когда порт получает сообщение запроса от клиента, именно IP-адрес, привязанный к порту, будет выделен клиенту. Таким образом, любое устройство, подключенное к этому порту, будет всегда получать указанный IP-адрес. Этот режим выделения IP имеет наивысший приоритет, а срок аренды составляет 1000 дней 23 часа 59 минут.



IP-адрес, привязанный к порту, и DHCP-сервер должны находиться в одном сегменте.

Если для назначения IP выбран режим «Port-Mode», вам необходимо настроить DHCP-сервер, как показано на следующем рисунке.



Configuration Options		Configuration Information
DHCP server status	<input checked="" type="radio"/> Enable All Vlans: <input checked="" type="checkbox"/> Vlan-id: <input type="text"/> <input type="radio"/> Disable	
DHCP server mode	<input type="radio"/> Common-Mode <input checked="" type="radio"/> Port-Mode	
DHCP server IP-pool name	<input type="text" value="pool"/>	
The domain name for the IP-Pool	<input type="text" value="domain"/>	
The starting IP address of the IP-Pool	<input type="text"/>	
The ending IP address of the IP-Pool	<input type="text"/>	
The subnet mask of the network-address	<input type="text" value="255.255.255.0"/>	
The default lease time of the IP address	Infinite: <input type="checkbox"/> <input type="text" value="0"/> Days <input type="text" value="1"/> Hours <input type="text" value="0"/> Minutes	
The maximum lease time of the IP address	<input type="text" value="1"/> Days <input type="text" value="0"/> Hours <input type="text" value="0"/> Minutes	
The routers on the IP-Pool's subnet	IP Address 1:	<input type="text"/>
	IP Address 2:	<input type="text"/>
The dns-server for the IP-Pool's subnet	DNS1:	<input type="text"/>
	DNS2:	<input type="text"/>
<input type="button" value="Run"/>		<input type="button" value="Run"/>
<input type="button" value="Apply"/>		<input type="button" value="Help"/>

Рисунок 150 – Настройка сервера в режиме «Port-Mode»

DHCP server IP-pool name

Диапазон: 1–15 символов

Функция: настройка имени пула IP-адресов.

The domain name for the IP-Pool

Диапазон: 1–60 символов

Функция: настройка доменного имени пула IP-адресов.

The subnet mask of the network-address

Маска подсети представляет собой число длиной 32 бита, состоящее из единиц и нулей. «1» соответствует полям номера сети и подсети, в то время как «0» соответствует полям номера хоста. Обычно маска настраивается как 255.255.255.0.



- После настройки нажмите кнопку <Run>, чтобы назначить клиентам правильные IP-адреса.
- После изменения конфигурации снова нажмите кнопку <Run>, чтобы назначить клиентам правильные IP-адреса.



4. Настройка общего режима

Когда режим DHCP-сервера установлен на «Common-Mode», он использует статическую привязку MAC-адреса и динамическое выделение IP-адреса. При наличии статической привязки IP/MAC система предпочтительно выделяет IP-адрес, привязанный к MAC-адресу; в противном случае динамически выделяет IP-адреса из пула адресов. Настройка статической привязки MAC-адреса показана на рисунках 151 и 152; Настройка динамического выделения IP-адресов показана на рисунке 153.

Static Binding Between IP and MAC

IP address	192.168.0.36
MAC address	00-1e-cd-02-01-03

Рисунок 151 – Статическая привязка MAC-адреса

Статическая привязка MAC-адреса заключается в привязке MAC-адреса клиента к IP-адресу. Когда сервер получает сообщение с запросом IP-адреса, MAC-адрес источника которого является MAC-адресом, настроенным как показано на рисунке 151, клиенту будет выделен IP-адрес, привязанный к этому MAC-адресу.

Этот тип режима выделения IP требует настройки сервера, как показано на рисунке 153.

После настройки список статических привязок между IP и MAC показывает настроенные связи. Чтобы удалить привязку установите флажок в столбце «Index» напротив соответствующей записи, как показано на рисунке 152.

The list of Static Binding Between IP and MAC

Index	IP Address	MAC Address
<input type="checkbox"/>	192.168.0.26	02-00-AA-BB-CC-05
<input type="checkbox"/>	192.168.0.36	00-1E-CD-02-01-03

Рисунок 152 – Список статических привязок IP/MAC



Configuration Options		Configuration Information
DHCP server status	<input checked="" type="radio"/> Enable All Vlans: <input checked="" type="checkbox"/> Vlan-id: <input type="text"/> <input type="radio"/> Disable	
DHCP server mode	<input checked="" type="radio"/> Common-Mode <input type="radio"/> Port-Mode	
DHCP server IP-pool name	<input type="text" value="pool"/>	
The domain name for the IP-Pool	<input type="text" value="domain"/>	
The starting IP address of the IP-Pool	<input type="text" value="192.168.0.100"/>	
The ending IP address of the IP-Pool	<input type="text" value="192.168.0.200"/>	
The subnet mask of the network-address	<input type="text" value="255.255.255.0"/>	
The default lease time of the IP address	Infinite: <input type="checkbox"/> <input type="text" value="0"/> Days <input type="text" value="1"/> Hours <input type="text" value="0"/> Minutes	
The maximum lease time of the IP address	<input type="text" value="1"/> Days <input type="text" value="0"/> Hours <input type="text" value="0"/> Minutes	
The routers on the IP-Pool's subnet	IP Address 1:	<input type="text"/>
	IP Address 2:	<input type="text"/>
The dns-server for the IP-Pool's subnet	DNS1:	<input type="text"/>
	DNS2:	<input type="text"/>
Run		Run

Рисунок 153 – Настройка сервера в режиме «Common-Mode»

DHCP server IP-pool name

Диапазон: 1–15 символов

Функция: настройка имени пула IP-адресов.

The domain name for the IP-Pool

Диапазон: 1–60 символов

Функция: настройка доменного имени пула IP-адресов.

The starting IP address of the IP-Pool/The ending IP address of the IP-Pool

Формат: A.B.C.D

Функция: настройка начального и конечного IP-адресов адресного пула. Оба адреса должны находиться в одном сетевом сегменте.

The subnet mask of the network-address

Маска подсети представляет собой число длиной 32 бита, состоящее из единиц и нулей. «1» соответствует полям номера сети и подсети, в то время как «0» соответствует полям номера хоста. Обычно маска настраивается как 255.255.255.0. При динамическом распределении адресов необходимо установить диапазон пула IP-адресов, который определяется маской подсети.



The default lease time of the IP address

Диапазон: 0 дней 0 часов 1 минута – 1000 дней 23 часа 59 минут/бесконечно

По умолчанию: 0 дней 1 час 0 минут

Функция: настройка времени аренды IP-адреса по умолчанию.

Описание: если сообщение с запросом IP-адреса, полученное от клиента, не содержит допустимого времени аренды, время, которое сервер выделит клиенту, будет равным настроенному здесь значению по умолчанию.

The maximum lease time of the IP address

Диапазон: 0 дней 0 часов 1 минута – 1000 дней 23 часа 59 минут

По умолчанию: 1 день 0 часов 0 минут

Функция: настройка максимального времени аренды IP-адреса.

Описание: если клиент запрашивает IP-адрес, сервер DHCP предоставит его на время, не превышающее максимально возможное, даже если клиент запросит больше. Время аренды можно настроить индивидуально для каждого пула адресов, но все адреса в одном пуле будут иметь одинаковое время аренды.

The routers on the IP-Pool's subnet

Функция: настройка адресов маршрутизаторов в подсети IP-пула.

Описание: если DHCP-клиент посещает хост, находящийся в другом сегменте, данные должны пересылаться через шлюзы. Когда DHCP-сервер выделяет клиентам IP-адреса, он может одновременно указывать адреса шлюзов. В пуле адресов DHCP можно настроить максимум два адреса шлюза.

The dns-server for the IP-Pool's subnet

Функция: настройка адресов DNS-серверов в подсети IP-пула.

Описание: при посещении узла сети через доменное имя, оно должно быть преобразовано в IP-адрес. Это преобразование осуществляет сервер DNS. Чтобы позволить DHCP-клиенту посещать сетевой хост через доменное имя, одновременно с назначением IP-адресов клиентам, DHCP-сервер может указать IP-адреса серверов доменных имен. В пуле адресов DHCP можно настроить максимум два адреса DNS.



- Настройте правильную подсеть на основе топологии сети клиента.
- После настройки нажмите кнопку <Run>, чтобы назначить клиентам правильные IP-адреса.
- После изменения конфигурации снова нажмите кнопку <Run>, чтобы назначить клиентам правильные IP-адреса.



6.28.1.4 Пример типовой настройки

Как показано на рисунке 154, коммутатор А работает как DHCP-сервер, а коммутатор В – как DHCP-клиент. Порт 3 коммутатора А соединяется с портом 4 коммутатора В. Клиент отправляет запросы на выделение ему IP-адреса. Сервер может назначить IP-адрес клиенту тремя способами.

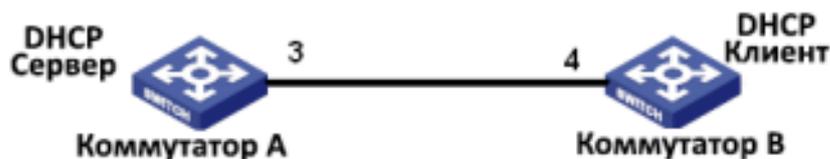


Рисунок 154 – Пример типовой настройки DHCP

Назначение IP-адреса на основе порта

➤ Настройка коммутатора А:

1. Включите статус DHCP-сервера, как показано на рисунке 147.
2. Выберите «Port-Mode» в качестве режима DHCP-сервера, как показано на рисунке 148.
3. Установите для «IP-pool name» значение «pool», установите для «the domain name for the IP-pool» значение «domain», установите для «the subnet mask» значение 255.255.255.0, как показано на рисунке 150.
4. Порт 3 привяжите к IP-адресу 192.168.0.6, как показано на рисунке 149.
5. Нажмите кнопку <Run> в интерфейсе настройки сервера, чтобы запустить его.

➤ Конфигурация коммутатора В:

1. В качестве DHCP-клиента коммутатор В автоматически получает IP-адрес.
2. Коммутатор В получает IP-адрес 192.168.0.6 и маску подсети 255.255.255.0 от DHCP-сервера, как показано на рисунке 155.

MAC Address	00-1E-CD-02-01-03
Auto IP Configuration	<input type="radio"/> Disable <input checked="" type="radio"/> DHCP Client IP
IP Address	192.168.0.6
Subnet Mask	255.255.255.0
GateWay	0.0.0.0

Рисунок 155 – DHCP-клиент получает IP-адрес (1)



Метод статической привязки MAC-адреса

➤ Настройка коммутатора А:

1. Включите статус DHCP-сервера, как показано на рисунке 147.
2. Выберите «Common-Mode» в качестве режима DHCP-сервера, как показано на рисунке 148.
3. Установите для «IP-pool name» значение «pool», установите для «the domain name for the IP-pool» значение «domain», установите для «the starting IP address of the IP-pool» значение 192.168.0.3 и для «the ending IP address of the IP-pool» значение 192.168.0.201. Установите для «the subnet mask» значение 255.255.255.0, а для времени аренды оставьте значение по умолчанию, как показано на рисунке 153.
4. Привяжите MAC-адрес коммутатора В 00-1E-CD-02-01-03 к IP-адресу 192.168.0.36, как показано на рисунке 151.
5. Нажмите кнопку <Run> в интерфейсе настройки сервера, чтобы запустить его.

➤ Конфигурация коммутатора В:

1. В качестве DHCP-клиента коммутатор В автоматически получает IP-адрес.
2. Коммутатор В получает IP-адрес 192.168.0.36 и маску подсети 255.255.255.0 от DHCP-сервера, как показано на рисунке 156.

MAC Address	00-1E-CD-02-01-03
Auto IP Configuration	<input type="radio"/> Disable <input checked="" type="radio"/> DHCP Client IP
IP Address	192.168.0.36
Subnet Mask	255.255.255.0
GateWay	0.0.0.0

Рисунок 156 – DHCP-клиент получает IP-адрес (2)

Динамическое назначение IP-адреса из пула адресов

➤ Настройка коммутатора А:

1. Включите статус DHCP-сервера, как показано на рисунке 147.
2. Выберите «Common-Mode» в качестве режима DHCP-сервера, как показано на рисунке 148.
3. Установите для «IP-pool name» значение «pool», установите для «the domain name for the IP-pool» значение «domain», установите для «the starting IP address of the IP-pool» значение 192.168.0.3 и для «the ending IP address of the IP-pool» значение 192.168.0.201. Установите для «the subnet mask» значение 255.255.255.0, а для времени аренды оставьте значение по умолчанию, как показано на рисунке 153.
4. Нажмите кнопку <Run> в интерфейсе настройки сервера, чтобы запустить его.



➤ Конфигурация коммутатора В:

1. В качестве DHCP-клиента коммутатор В автоматически получает IP-адрес.
2. DHCP-сервер по порядку ищет свободные IP-адреса в пуле и выделяет коммутатору В первый найденный адрес и другие сетевые параметры. Маска подсети – 255.255.255.0, как показано на рисунке 157.

MAC Address	00-1E-CD-02-01-03
Auto IP Configuration	<input type="radio"/> Disable <input checked="" type="radio"/> DHCP Client IP
IP Address	192.168.0.3
Subnet Mask	255.255.255.0
GateWay	0.0.0.0

Рисунок 157 – DHCP-клиент получает IP-адрес (3)

6.28.2 DHCP Snooping

6.28.2.1 Введение

DHCP Snooping – это функция мониторинга служб DHCP на втором уровне, являющаяся одной из функций безопасности DHCP, которая дополнительно обеспечивает безопасность клиента. Механизм безопасности DHCP Snooping позволяет контролировать, чтобы только доверенные порты могли пересылать запросы клиента DHCP к законному серверу. Также он контролирует источник ответных сообщений сервера DHCP, гарантируя, что клиент получит IP-адрес от действительного сервера и предотвращая выдачу IP-адресов или других параметров конфигурации поддельными или недействительными серверами DHCP.

Механизм безопасности DHCP Snooping разделяет порты на доверенные и недоверенные.

Доверенный порт – это порт, который прямо или косвенно соединяется с законным DHCP-сервером. Доверенный порт обычно пересылает сообщения запросов клиентов и ответные сообщения серверов, чтобы гарантировать получение клиентами действительных IP-адресов.

Недоверенный порт – это порт, который подключается к незаконному DHCP-серверу. Недоверенные порты блокируются от отправки или получения данных DHCP, чтобы предотвратить возможные атаки или несанкционированное распределение IP-адресов.

6.28.2.2 Настройка с помощью WEB-интерфейса

1. Включите функцию DHCP Snooping, как показано на следующем рисунке.



DHCP Snooping Status

 Enable
 Disable

Apply
Help

Рисунок 158 – Состояние DHCP Snooping

DHCP Snooping Status

Варианты: Enable/Disable

По умолчанию: Disable

Функция: включение/отключение функции отслеживания DHCP.



Коммутатор, работающий как DHCP-сервер и клиент, не может включить функцию DHCP Snooping.

2. Настройте доверенные порты, как показано на следующем рисунке.

Port	Protocol Status
S1/FE1	<input checked="" type="radio"/> Trust <input type="radio"/> Untrust
S1/FE2	<input type="radio"/> Trust <input checked="" type="radio"/> Untrust
S1/FE3	<input type="radio"/> Trust <input checked="" type="radio"/> Untrust
S1/FE4	<input type="radio"/> Trust <input checked="" type="radio"/> Untrust
S1/FE5	<input type="radio"/> Trust <input checked="" type="radio"/> Untrust
S1/FE6	<input type="radio"/> Trust <input checked="" type="radio"/> Untrust
S1/FE7	<input type="radio"/> Trust <input checked="" type="radio"/> Untrust
S1/FE8	<input type="radio"/> Trust <input checked="" type="radio"/> Untrust

Рисунок 159 – Настройка доверенных портов

Protocol Status

Варианты: Trust/Untrust

По умолчанию: Untrust

Функция: указывает для порта доверенный (Trust) или недоверенный (Untrust) режим. Порты, которые прямо или косвенно соединяются с законными DHCP-серверами, являются доверенными.



Настройка порта в качестве доверенного и участие в группе агрегации являются взаимоисключающими. Порт, входящий в группу агрегации, не может быть настроен как доверенный. Доверенный порт не может присоединиться к группе агрегации.



6.28.2.3 Пример типовой настройки

Как показано на рисунке 160, DHCP-клиент запрашивает IP-адрес у DHCP-сервера. В сети существует неавторизованный DHCP-сервер. Установите для порта 1 доверенный режим с помощью DHCP Snooping, чтобы сервер и клиент могли свободно обмениваться DHCP-сообщениями. Порт 3 настройте как недоверенный, чтобы запретить ему пересылать DHCP-сообщения между сервером и клиентом. Таким образом гарантируется, что клиент сможет получить действительный IP-адрес от действительного DHCP-сервера.

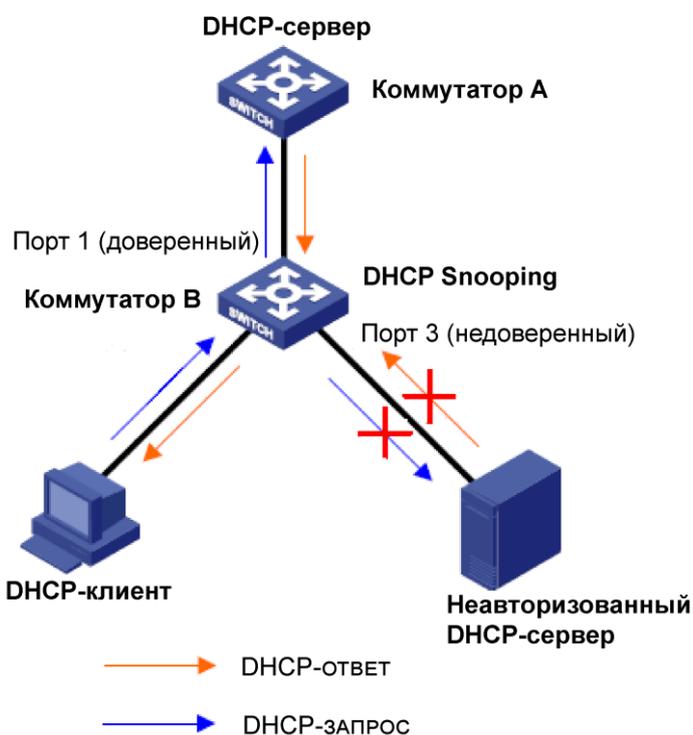


Рисунок 160 – Типовая конфигурация DHCP Snooping

➤ Настройка коммутатора В:

1. Включите функцию DHCP Snooping, как показано на рисунке 158.
2. Настройте порт 1 коммутатора В в качестве доверенного, а порт 3 – в качестве недоверенного, как показано на рисунке 159.

6.28.3 Настройка Option 82

Option 82 (запись информации агента ретрансляции) используется для записи дополнительной информации о клиенте. Эта функция позволяет DHCP Snooping добавлять



специальную информацию в запросы клиентов, что помогает серверу DHCP принимать решения о выделении IP-адресов.

Option 82 включает две подопции, несущие разные типы информации:

- Sub-option 1 – идентификатор цепи (Circuit ID), который может указывать, на местоположение клиента;
 - Sub-option 2 – удалённый идентификатор (Remote ID), который может быть использован для идентификации устройства или пользователя.
- Sub-option 1 содержит идентификатор VLAN и номер порта, который получает сообщение запроса от DHCP-клиента, как показано в таблице 9.

Таблица 9 – Формат поля Sub-option 1

Тип подопции (0x01)	Длина (0x04)	VLAN ID	Номер порта
1 байт	1 байт	2 байта	2 байта

Тип подопции равен 1.

Длина указывает на количество байтов, которые занимают идентификатор VLAN и номер порта.

VLAN ID на устройстве с включенным DHCP Snooping обозначает идентификатор VLAN порта, который получает сообщение запроса от клиента DHCP.

Номер порта, который получает сообщение запроса от DHCP-клиента.

- Содержимым Sub-option 2 является MAC-адрес устройства DHCP Snooping, которое получает сообщение запроса от клиента DHCP, как показано в таблице 10, или строка символов, настроенная пользователями, как показано в таблице 11.

Таблица 10 – Sub-option 2, формат поля MAC-адреса

Тип подопции (0x02)	Длина (0x06)	MAC-адрес
1 байт	1 байт	6 байт

Таблица 11 – Sub-option 2, формат поля символьной строки

Тип подопции (0x02)	Длина (0x10)	Строка символов
Один байт	Один байт	16 байт

Тип подопции равен 2.

Длина указывает на количество байтов, которые занимает содержимое Sub-option 2. MAC-адрес занимает 6 байт, а строка символов – 16 байт.



MAC-адрес относится к устройству с включенным DHCP Snooping, которое получает сообщение запроса от DHCP-клиента.

Строка символов: содержимое Sub-option 2 составляет 1–16 символов, заданных пользователем. Символы вводятся в кодировке ASCII, и каждый символ занимает один байт. Длина фиксирована и равна 16. Если настроена строка длиной менее 16 байт, позиции недостающих символов заполняются нулями.

6.28.3.1 Функция поддержки Option 82 в DHCP Snooping

6.28.3.1.1 Введение

Если устройство DHCP Snooping поддерживает функцию Option 82, то, получив DHCP-сообщение запроса, оно обрабатывает его в зависимости от того, содержит ли сообщение Option 82 и политику клиента, а затем пересылает обработанное сообщение на DHCP-сервер. Конкретный метод обработки показан в таблице 12.

Таблица 12 – Режимы обработки сообщений запроса (DHCP Snooping)

Получение сообщения запроса от DHCP-клиента	Политика конфигурации	Обработка сообщения запроса устройством DHCP Snooping
Сообщение содержит Option 82	Drop	Удаляет сообщение запроса
	Keep	Сохраняет формат сообщения неизменным и пересылает его
	Replace	Заменяет поле Option 82 в сообщении на свое поле Option 82 и пересылает новое сообщение
Сообщение не содержит Option 82	Drop/Keep/Replace	Добавляет свое поле Option 82 в сообщение и пересылает его

Когда устройство DHCP Snooping получает ответное сообщение от DHCP-сервера, если сообщение содержит поле Option 82, устройство удаляет это поле и пересылает сообщение клиенту. Если сообщение не содержит поля Option 82, устройство обрабатывает ответное сообщение в соответствии с политикой сервера, как показано в таблице 13.

Таблица 13 – Режимы обработки ответных сообщений (DHCP Snooping)

Получение ответного сообщения от DHCP-сервера	Политика конфигурации	Обработка ответного сообщения устройством DHCP Snooping
Сообщение содержит Option 82	Drop/Keep	Удаляет поле Option 82 в ответном сообщении и пересылает сообщение
Сообщение не содержит Option 82	Drop	Удаляет ответное сообщение
	Keep	Сохраняет формат неизменным и пересылает сообщение



6.28.3.1.2 Настройка с помощью WEB-интерфейса

Конфигурация Option 82 DHCP Snooping показана на следующем.

Option82 Configuration

Option82 Status	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Client Policy	<input type="radio"/> Drop <input type="radio"/> Replace <input checked="" type="radio"/> Keep
Server Policy	<input type="radio"/> Drop <input checked="" type="radio"/> Keep
Remote-ID Type	<input type="radio"/> String <input checked="" type="radio"/> MAC
Remote-ID Content	<input type="text" value="00-22-55-AA-BB-04"/>

Рисунок 161 – Конфигурация Option 82

Option82 Status

Варианты: Enable/Disable

По умолчанию: Disable

Функция: включение/выключение функции Option 82 на устройстве DHCP Snooping.

Client Policy

Варианты: Drop/Replace/Keep

По умолчанию: Keep

Функция: настройка клиентской политики. Устройство DHCP Snooping обрабатывает сообщение запроса, отправленное от клиента, в соответствии с клиентской политикой, как показано в таблице 12.

Server Policy

Варианты: Drop/Keep

По умолчанию: Keep

Функция: настройка политики сервера. Устройство DHCP Snooping обрабатывает ответное сообщение, отправленное с сервера, в соответствии с политикой сервера, как показано в таблице 13.

Remote-ID Type

Варианты: String/MAC

По умолчанию: MAC

Функция: настройка содержимого подопции 2.

Описание: «MAC» означает, что содержимое Sub-option 2 представляет собой MAC-адрес устройства DHCP Snooping, которое получает сообщение запроса от клиента. «String»



означает, что содержимое Sub-option 2 представляет собой строку символов, определенную пользователем.

Remote-ID Content

Варианты: MAC-адрес/1–16 символов

По умолчанию: MAC-адрес

Описание: когда «Remote-ID Type» настроен на «MAC», содержимое удаленного идентификатора принудительно заменяется MAC-адресом текущего устройства отслеживания. Если для «Remote-ID Type» установлено значение «String», содержимое удаленного идентификатора настраивается пользователем. Строка может содержать 1–16 символов (каждый символ занимает один байт).

6.28.3.2 Функция поддержки Option 82 DHCP-сервером

6.28.3.2.1 Введение

Если DHCP-сервер настроен на поддержку функции Option 82, то, получая сообщение запроса DHCP, он предоставляет разные решения по выделению адреса в зависимости от того, содержит ли сообщение поле Option 82 и конфигурацию сервера.

На сервере DHCP можно создать до 32 различных классов для группировки клиентов.

Каждый класс имеет диапазон IP-адресов и настройки для сопоставления с информацией ретрансляции (Option 82).

Если включена функция «Match Always» (всегда совпадает), сервер автоматически считает, что клиент принадлежит к классу, без дополнительной проверки.

Если функция «Match Always» выключена, сервер должен проверить, соответствует ли информация клиента установленным критериям класса.

Это позволяет серверу DHCP более гибко управлять выдачей IP-адресов, основываясь на дополнительной информации о клиенте.

Таблица 14 – Режимы обработки сообщений запроса (DHCP-сервер с поддержкой Option 82)

Получение сообщения запроса от DHCP-клиента	Политика конфигурации		Обработка сообщения запроса DHCP-сервером
Сообщение содержит поле Option 82	Функция Match Always включена		Добавляет поле Option 82 в ответное сообщение и назначает IP-адрес и другие параметры клиенту
	Функция Match Always	Настроить значение параметра	Значение параметра информации



	выключена	информации ретрансляции	ретрансляции соответствует полю Option 82: сервер добавляет поле Option 82 в ответное сообщение и назначает IP-адрес и другие параметры клиенту
			Значение параметра информации ретрансляции не соответствует полю Option 82: сервер не выделяет IP-адрес клиенту
	Не настраивать значение параметра информации ретрансляции	Сервер не выделяет IP-адрес клиенту	
Сообщение не содержит поля Option 82	Функция Match Always включена		Ответное сообщение не содержит поля Option 82, сервер выделяет клиенту IP-адрес и другие параметры
	Функция Match Always выключена		Сервер не выделяет IP-адрес клиенту

Если DHCP-сервер не поддерживает функцию Option 82, то в случае получения сообщения, содержащего поле Option82, ответное сообщение не содержит этого поля и сервер может выделить клиенту IP-адрес и другие параметры. В этом случае сервер обрабатывает сообщение запроса, как показано в таблице 15.

Таблица 15 – Режимы обработки сообщений запроса (DHCP-сервер без поддержки Option 82)

Получение сообщения запроса от DHCP-клиента	Обработка сообщения запроса DHCP-сервером
Сообщение содержит поле Option 82	Ответное сообщение не содержит поля Option 82, сервер выделяет клиенту IP-адрес и другие параметры
Сообщение не содержит поля Option 82	



6.28.3.2.2 Настройка с помощью WEB-интерфейса

1. Включите функцию Option 82 на устройстве DHCP-сервера, как показано на следующем рисунке.

DHCP Server Option82 Enable	Enable
-----------------------------	--------

Apply

Рисунок 162 – Статус Option 82 на DHCP-сервере

DHCP Server Option82 Enable

Варианты: Enable/Disable

По умолчанию: Disable

Функция: включение или отключение функции Option 82 на устройстве DHCP-сервера.

2. Настройте Option 82 DHCP-сервера, как показано на следующем рисунке.

Operation	<input checked="" type="radio"/> Add <input type="radio"/> Delete
Operation Object	class
Class Name	1
Relay Information	010400010001
Start IP	192.168.0.10
End IP	192.168.0.20
Match Always	<input checked="" type="radio"/> Open <input type="radio"/> Close

Apply

Рисунок 163 – Настройка Option 82 на DHCP-сервере

Operation

Варианты: Add/Delete

По умолчанию: Add

Функция: добавление или удаление указанного класса.

Operation Object

Варианты: class/Relay Information/start & end ip/Match Always

По умолчанию: class



Описание: «class» – это категория настроек, которую можно добавить на DHCP-сервере. Каждый класс содержит определенные параметры, такие как диапазон IP-адресов и правила сопоставления.

«Relay Information» – информация ретрансляции. Это дополнительные данные, которые можно привязать к классу. Они помогают серверу определить, как обрабатывать запросы от клиентов.

«start & end ip» – это диапазон IP-адресов, который выделяется для класса.

«Match Always» – всегда совпадает. Если эта опция включена, сервер будет считать, что информация ретрансляции всегда соответствует классу, без необходимости дополнительной проверки.

При добавлении класса вы настраиваете эти параметры. Если вы удаляете класс, достаточно указать его имя. Вы можете добавить несколько элементов информации ретрансляции к существующему классу, чтобы уточнить, какие запросы должны обрабатываться в рамках этого класса. При удалении информации ретрансляции вы удаляете её из класса, чтобы она больше не влияла на обработку запросов.

Class Name

Диапазон: 1–15 символов

Функция: настройка имени класса.

Relay Information

Диапазон: 12–60 шестнадцатеричных чисел

Функция: настройка информации ретрансляции класса.

Start IP/End IP

Формат: A.B.C.D.

Функция: настройка начального/конечного IP-адреса класса. Этот диапазон должен быть выбран из пула адресов DHCP-сервера.

Match Always

Варианты: Open/Close

Функция: включение и выключение функции «Match Always». Если функция включена, предполагается, что значение параметра «Relay Information» всегда соответствует значению, указанному в поле Option 82, без необходимости проверки. Если функция «Match Always» отключена, необходимо определить, соответствует ли значение параметра «Relay Information» значению поля Option 82.



Когда вы создаёте на DHCP-сервере несколько классов, сервер присваивает IP-адрес клиенту в соответствии с классом, данные которого совпадают с информацией ретрансляции. Если у нескольких классов информация ретрансляции одинакова, для назначения IP-адреса клиенту сервер выберет класс, который был создан первым.



3. Запросите класс Option 82 DHCP-сервера, как показано на следующем рисунке.

DHCP Query Option82 Query

Class Name	<input type="text"/>
------------	----------------------

Query

Query Result
Class Name: 1 Relay Information: 010400010001 01040001000103 Start IP: 192.168.0.100 End IP: 192.168.0.200 Match Always: Open

Рисунок 164 – Запрос класса Option 82 DHCP-сервера



Расшифровка аббревиатур

ACL	Access Control List	Список управления доступом
ARP	Address Resolution Protocol	Протокол определения MAC-адреса другого узла по известному IP-адресу
BootP	Bootstrap Protocol	Протокол, используемый для автоматического получения клиентом IP-адреса
BPDU	Bridge Protocol Data Unit	Блок данных протокола управления сетевыми мостами
CLI	Command Line Interface	Интерфейс командной строки
CoS	Class of Service	Класс сервиса
CRC	Cyclic Redundancy Check	Циклический избыточный код. Алгоритм нахождения контрольной суммы, предназначенный для проверки целостности данных
DHCP	Dynamic Host Configuration Protocol	Протокол динамической настройки узла
DHP	Dual Homing Protocol	Протокол, позволяющий подключить устройство к двум разным коммутаторам, обеспечивая резервирование подключения
DNS	Domain Name System	Система доменных имен
DSCP	Differentiated Services Code Point	Точка кода дифференцированных услуг. Использует 6-битное поле 8-битного IP-заголовка DS
FDB	Forwarding Data Base	Таблица коммутации
FTP	File Transfer Protocol	Протокол передачи файлов
GARP	Generic Attribute Registration Protocol	Протокол регистрации основных атрибутов
GMRP	GARP Multicast Registration Protocol	Протокол GARP для регистрации многоадресных групп
GVRP	GARP VLAN Registration Protocol	Протокол GARP для регистрации VLAN
ICMP	Internet Control Message Protocol	Протокол межсетевых управляющих сообщений
IGMP	Internet Group Management Protocol	Протокол управления многоадресной передачей данных в сетях, основанных на протоколе IP. Используется только в сетях IPv4. Аналогичную роль в стеке протоколов IPv6 выполняет протокол MLD
IGMP Snooping	Internet Group Management Protocol Snooping	Протокол отслеживания сетевого трафика IGMP
IP	Internet Protocol	Интернет-протокол
LAN	Local Area Network	Локальная сеть
LLDP	Link Layer Discovery Protocol	Протокол обнаружения канального уровня



LLDPDU	Link Layer Discovery Protocol Data Unit	Блок данных протокола обнаружения канального уровня
MIB	Management Information Base	Виртуальная база данных, используемая для управления объектами в сети связи
NMS	Network Management System	Система сетевого управления
OID	Object Identifier	Идентификатор объекта
PVID	Port VLAN Identifier	Идентификатор VLAN по умолчанию для порта
PVLAN	Private VLAN	Частная виртуальная локальная сеть
QoS	Quality of Service	Качество обслуживания (технология предоставления различным классам трафика различных приоритетов в обслуживании)
RMON	Remote Network Monitoring	Дистанционный мониторинг сети (расширение SNMP, разработанное IETF)
RSTP	Rapid Spanning Tree Protocol	Быстрый протокол связующего дерева (версия протокола STP с ускоренной реконфигурацией дерева)
SNMP	Simple Network Management Protocol	Простой протокол сетевого управления (интернет-протокол для управления устройствами в IP-сетях на основе архитектур TCP/UDP)
SNTP	Simple Network Time Protocol	Простой протокол синхронизации времени (является упрощённой реализацией протокола NTP)
SSH	Secure Shell	«Безопасная оболочка», сетевой протокол прикладного уровня
STP	Spanning Tree Protocol	Протокол связующего дерева
ToS	Type of Service	Однооктетное поле в структуре IP-пакета, характеризует то, как должна обрабатываться дейтограмма
TTL	Time to Live	предельный период времени или число итераций (переходов), которые пакет данных может осуществить (прожить) до своего исчезновения
VLAN	Virtual Local Area Network	Виртуальная локальная сеть