



Руководство по настройке
коммутаторов
SEWM20-D, SEWM228GS, SEWM228M



Оглавление

1. Информация об устройстве	9
1.1. Основная информация о коммутаторе	9
1.2. Функциональные возможности ПО	9
2. Подключение к устройству	9
2.1. Варианты просмотра и отображения	9
2.2. Подключение через консольный порт	10
2.3. Подключение к коммутатору посредством Telnet	13
2.4. Доступ через WEB-интерфейс	14
3. Управление устройством	16
4. Статус устройства	16
4.1. Основная информация о коммутаторе	16
4.2. Информация о статусе портов	17
4.3. Статистика работы порта	19
4.4. Информация о работе системы	20
5. Основные настройки коммутатора	20
5.1. IP адрес	20
5.2. Информация об устройстве	21
5.3. Настройка портов	22
5.4. Изменение пароля	24
5.5. Обновление программного обеспечения (ПО)	25
5.5.1. Обновление ПО через FTP	25
5.6. Запрос версии ПО	28
5.7. Функция резервного копирования и загрузки настроек	28
6. Расширенная настройка	29
6.1. Ограничение скорости портов (Port Rate Limiting)	29
6.1.1. Введение	29
6.1.2. Настройка через WEB-интерфейс	30
6.1.3. Пример типовой настройки	31
6.2. Виртуальные локальные сети VLAN	31
6.2.1. Введение	31
6.2.2. Принцип работы	31



6.2.3.	VLAN на основе портов (Port-based VLAN)	32
6.2.4.	Настройка через WEB-интерфейс	33
6.2.5.	Пример типовой настройки	36
6.3.	Изолированная VLAN (Private VLAN, PVLAN).....	38
6.3.1.	Введение	38
6.3.2.	Настройка через WEB- интерфейс	38
6.3.3.	Пример типовой настройки.....	40
6.4.	Зеркалирование портов (Port Mirroring).....	41
6.4.1.	Введение	41
6.4.2.	Описание	41
6.4.3.	Настройка через WEB-интерфейс	41
6.4.4.	Пример типовой настройки.....	42
6.5.	Транковые порты (Trunk Port).....	42
6.5.1.	Введение	42
6.5.2.	Реализация функции	43
6.5.3.	Описание	43
6.5.4.	Настройка через WEB-интерфейс	44
6.5.5.	Пример типовой настройки.....	45
6.6.	Проверка связи (Link Check)	46
6.6.1.	Введение	46
6.6.2.	Настройка через WEB-интерфейс	46
6.7.	Статическая многоадресная таблица (FDB)	47
6.7.1.	Введение	47
6.7.2.	Настройка через WEB-интерфейс	47
6.8.	IMGP Snooping	49
6.8.1.	Введение	49
6.8.2.	Концепция	49
6.8.3.	Принцип работы	49
6.8.4.	Настройка через WEB-интерфейс	50
6.8.5.	Пример типовой настройки.....	51
6.9.	Протокол ACL	52
6.9.1.	Введение	52



6.9.2.	Настройка через WEB-интерфейс	52
6.9.3.	Пример типовой настройки.....	54
6.10.	Протокол разрешения адресов (ARP)	54
6.10.1.	Введение.....	54
6.10.2.	Описание	54
6.10.3.	Настройка с помощью Web-интерфейса	55
6.11.	Протокол SNMP.....	56
6.11.1.	Введение.....	56
6.11.2.	Реализация	56
6.11.3.	Описание	57
6.11.4.	Описание MIB (Management Information Base).....	57
6.11.5.	Настройка через WEB-интерфейс.....	58
6.11.6.	Пример типовой настройки	60
6.12.	Sy2-Ring.....	60
6.12.1.	Введение.....	60
6.12.2.	Концепция	61
6.12.3.	Реализация	61
6.12.4.	Настройка через WEB-интерфейс.....	64
6.12.5.	Пример типовой настройки	68
6.13.	STP/RSTP	68
6.13.1.	Описание	68
6.13.2.	Концепция	68
6.13.3.	Настройка BPDU	69
6.13.4.	Реализация	69
6.13.5.	Настройка через WEB-интерфейс.....	70
6.13.6.	Пример типовой настройки	73
6.14.	Прозрачная передача STP/RSTP	74
6.14.1.	Описание	74
6.14.2.	Настройка через WEB-интерфейс.....	75
6.14.3.	Пример типовой настройки	76
6.15.	Настройка QoS.....	76
6.15.1.	Введение.....	76



6.15.2.	Принцип работы	77
6.15.3.	Настройка через Web-интерфейс.....	77
6.15.4.	Пример типовой настройки	81
6.16.	Время старения MAC адреса (MAC Address Aging Time)	82
6.16.1.	Введение.....	82
6.16.2.	Настройка через WEB-интерфейс.....	82
6.17.	Настройка LLDP	82
6.17.1.	Введение.....	82
6.17.2.	Настройка через WEB-интерфейс.....	82
6.18.	Протокол SNTP	83
6.18.1.	Введение.....	83
6.18.2.	Настройка через WEB-интерфейс.....	83
6.19.	Протокол MSTP	85
6.19.1.	Введение.....	85
6.19.2.	Концепция	87
6.19.3.	Реализация	90
6.19.4.	Настройка через WEB-интерфейс.....	90
6.19.5.	Пример типовой настройки	98
6.20.	Аварийная сигнализация (Alarm)	100
6.20.1.	Введение.....	100
6.20.2.	Настройка через WEB-интерфейс.....	101
6.21.	Аварийная сигнализация передачи трафика на порту (Port Traffic Alarm)	105
6.21.1.	Введение.....	105
6.21.2.	Настройка через WEB-интерфейс.....	105
6.22.	GMRP.....	106
6.22.1.	GARP	106
6.22.2.	Протокол GMRP	107
6.22.3.	Описание	108
6.22.4.	Настройка через WEB-интерфейс.....	108
6.22.5.	Пример типовой настройки	111
6.23.	Протокол RMON (Remote Network Monitoring)	113
6.23.1.	Введение.....	113



6.23.2.	Группы RMON (RMON Group).....	113
6.23.3.	Настройка через WEB-интерфейс.....	114
6.24.	Настройка одноадресной рассылки (Unicast).....	118
6.24.1.	Введение.....	118
6.24.2.	Настройка через WEB-интерфейс.....	119
7.	Расшифровка аббревиатур	121



Введение

Данный документ содержит информацию о настройках и возможностях программного обеспечения коммутаторов серий SEWM20-D, SEWM228GS, SEWM228M. 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 • Модели • Возможности программного обеспечения
2. Способы подключения к устройству	<ul style="list-style-type: none"> • Обзор возможностей • Подключение через консольный порт • Подключение с использованием Telnet • Подключение через Web-интерфейс
3. Управление устройством	<ul style="list-style-type: none"> • Перезагрузка • Вход в систему и выход из системы
4. Статус устройства	<ul style="list-style-type: none"> • Основная информация • Статус портов • Статистика портов • Информация о работе системы
5. Основные настройки	<ul style="list-style-type: none"> • Настройка IP адресов • Информация об устройстве • Настройка портов • Изменение пароля • Обновление программного обеспечения • Запрос версии программного обеспечения • Скачивание и загрузка настроек
6. Дополнительные настройки	<ul style="list-style-type: none"> • Ограничение скорости портов • VLAN • PVLAN • Зеркалирование портов (Port mirroring) • Транковые порты (Port Trunk) • Проверка линий связи (Link check) • Статическая многоадресная рассылка (Static multicast) • IMGP Snooping • ACL • ARP • SNMP • Sy2-Ring • RSTP/STP • Прозрачная передача RSTP/STP



	<ul style="list-style-type: none"> • QoS • LLDP • SNTP • MSTP • Аварийная сигнализация (Alarm) • GMRP • RMON
--	---

Условные обозначения




1. Условные обозначения в тексте

Формат	Описание
< >	Скобки < > обозначают «кнопки». Например, нажмите кнопку <Apply>
[]	Скобки [] обозначают имя окна или имя меню. Например, нажмите пункт меню [File]
{ }	Скобки { } обозначают группу. Например {IP address, MAC address} означает, что IP адрес и MAC адрес составляют группу и могут быть настроены и показаны вместе.
→	Мультиуровневое меню разделяется посредством знака «→». Например, Start→AllPrograms→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.
~	Знак «~» обозначает диапазон значений. Например, «1~255» указывает на диапазон от 1 до 255

2. Условные обозначения CLI

Формат	Описание
Bold	Означает Команды и ключевые слова. Например, show version будет показываться с использованием шрифта Bold
<i>Italic</i>	Параметры, для которых вы указываете значения с помощью шрифта <i>italic</i> . Например, для команды show vlan <i>vlan id</i> указывается актуальное значение команды <i>vlan id</i> посредством шрифта <i>italic</i>

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

Промышленные коммутаторы серий SEWM20-D, SEWM228GS, SEWM228M могут использоваться в различных областях промышленности: системах передачи данных в энергетике, на транспорте, в горнодобывающей промышленности и т.д. Данные серии коммутаторов поддерживает протокол MSTP и проприетарный протокол Sy2-Ring. Это высокопроизводительная серия коммутаторов может обеспечить потребности сетей передачи данных для многих отраслей промышленности.

1.2. Функциональные возможности ПО

Программное обеспечение коммутатор STWM10GP-D поддерживает множество различных функций:

- Протоколы кольцевого резервирования: RSTP/STP, Sy2-Ring и MSTP;
- Протоколы мультиадресной рассылки (Multicast): IGMP Snooping, GMRP, Static;
- Функции коммутации: VLAN, PVLAN, QoS, ARP;
- Управление пропускной способностью: транковые порты (Port Trunk), лимитирование скорости портов;
- Безопасность: ACL
- Протокол синхронизации времени: SNMP;
- Управление устройством: обновление через FTP, скачивание/загрузка конфигурации;
- Диагностика устройства: зеркалирование портов (port mirroring), LLDP, проверка статуса соединения (Link check);
- Система тревожных оповещений: ошибка порта (port alarm), ошибка питания (power alarm), ошибка кольца (ring alarm), оповещения о конфликтах IP и MAC адресов;
- Сетевой доступ к устройству и управление: CLI, Telnet, Web, NMS Symanitron, SNMP.
-

2. Подключение к устройству

Устройство можно настраивать одним из четырех нижеперечисленных способов:

- через консольный порт
- посредством Telnet
- с использованием WEB-интерфейса
- с помощью программы Symanitron NMS

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:



Подсказка	Тип отображения	Функция	Команда
SWITCH>	Основной режим	Отобразить текущие пользовательские команды Отобразить IP адрес Отобразить версию ПО Отображение результатов команды ping	Введите «Enable» для входа в привилегированный режим
SWITCH #	Привилегированный режим	Загрузить/выгрузить конфигурационный файл Вернуться к заводским настройкам Отобразить результаты команды ping Перезагрузить коммутатор Записать текущую конфигурацию Обновить ПО	Введите « Configure terminal » для переключения из привилегированного режима в режим настройки Введите « exit » для возврата в основной режим
SWITCH (config) #	Режим Настройки	Настроить все функциональные возможности коммутатора	Введите « exit » или « end » для возврата в привилегированный режим

Когда выполняется настройка коммутатора посредством сервиса CLI, символ «?» может использоваться для получения помощи по используемым командам. Для получения помощи, нужно ввести описание параметров, например, <1,255> означает диапазон чисел, <Н.Н.Н.Н> означает IP адрес, <Н:Н:Н:Н:Н> означает MAC адрес, word<1,31> означает диапазон строк. Также символы ↑ и ↓ могут использоваться для просмотра последних 10 команд.

2.2. Подключение через консольный порт

Пользователь может подключиться к устройству посредством консольного порта с помощью HyperTerminal операционной системы Windows или с помощью другого программного обеспечения, которое поддерживает подключение по последовательному порту, например HTT3.3. В примере ниже показано, как использовать консольный порт и HyperTerminal для доступа к коммутатору.

1. Подключите USB кабель к ПК и консольному интерфейсу устройства (кабель должен быть оснащён разъёмом DB9 с одной стороны и RJ45 с другой).
2. Запустите HyperTerminal в основном окне Windows, нажмите [Start]—>[All Programs]—>[Accessories]—>[Communications]—>[Hyper Terminal] (см. Рис. 1).



Рис. 1. Запуск HyperTerminal

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

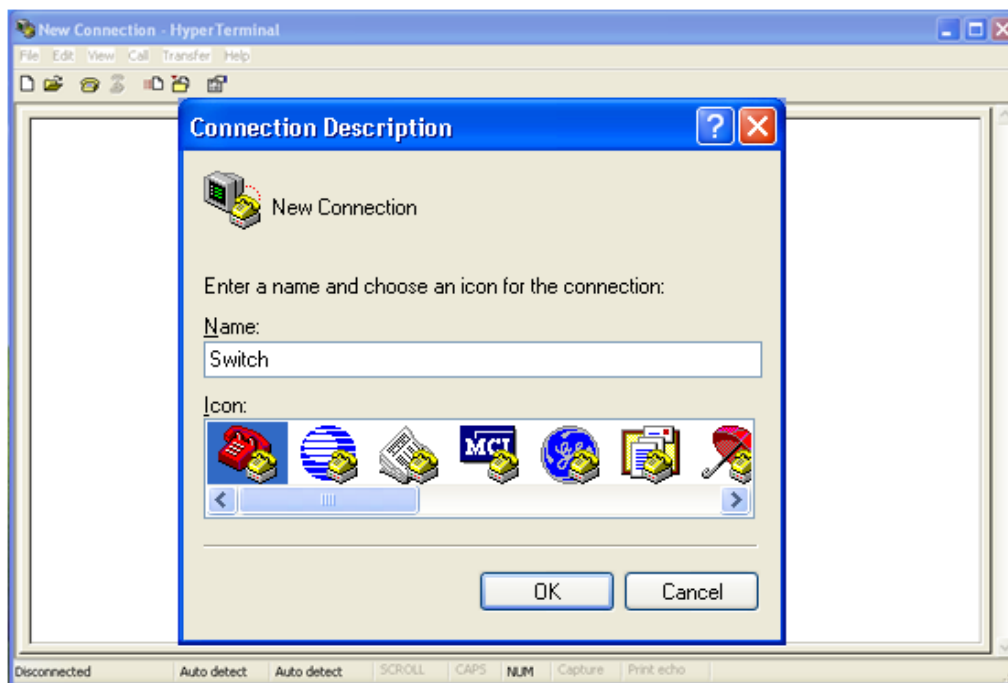


Рис. 2. Создание нового подключения



4. Выберите COM порт для подключения.

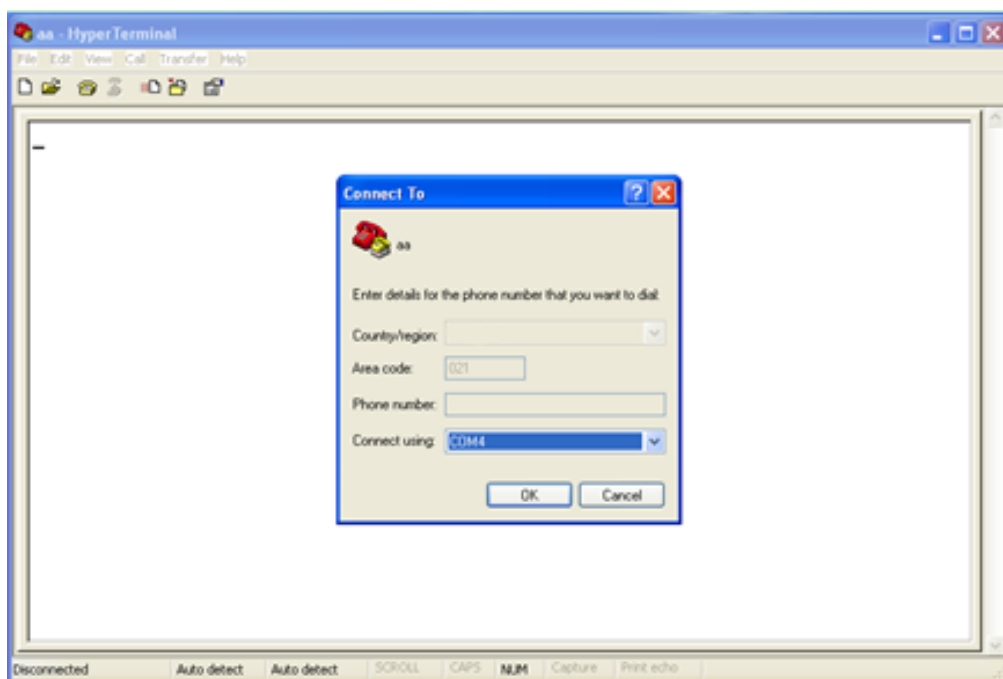


Рис. 3. Выбор COM порта для подключения



Для подтверждения COM порта нажмите [My Computer]->[Property]->[Hardware]->[Device Manager]->[Port] и проверьте работу порта, который используется как консольный.

5. Настройте параметры COM порта. Скорость (Baud rate): 9600, Биты данных (Data bits): 8, Чётность (Parity): None, Стоповые биты (Stop bits): 1, Контроль потока (Flow control): None.

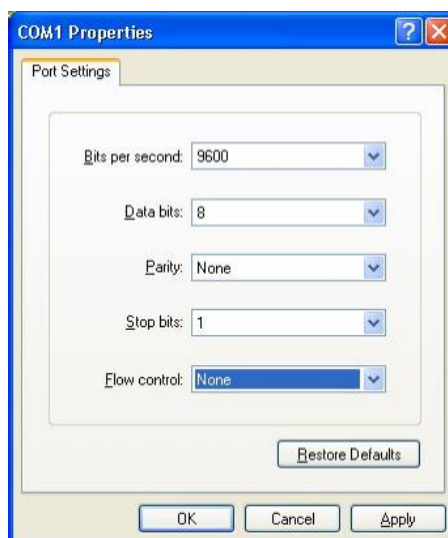


Рис. 4. Настройка параметров COM порта



6. Нажмите <OK> для входа в командную строку CLI. Нажмите <Enter> для входа в пользовательский режим.

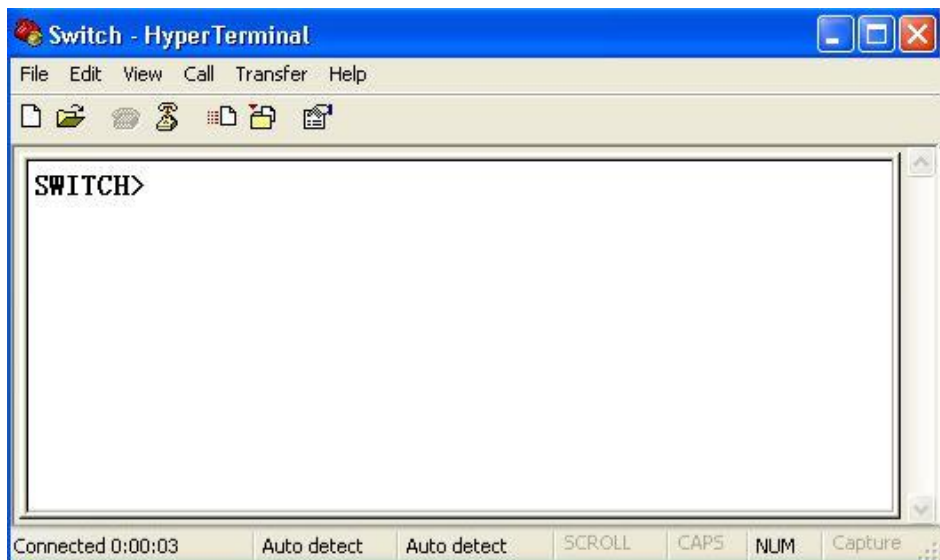


Рис. 5. Экран CLI

2.3. Подключение к коммутатору посредством Telnet

1. Подключите любой RJ45 порт коммутатора к Ethernet порту ПК.
2. Откройте <Выполнить> на ПК, там введите «telnet IP-адрес», по умолчанию IP-адрес - 192.168.0.2.

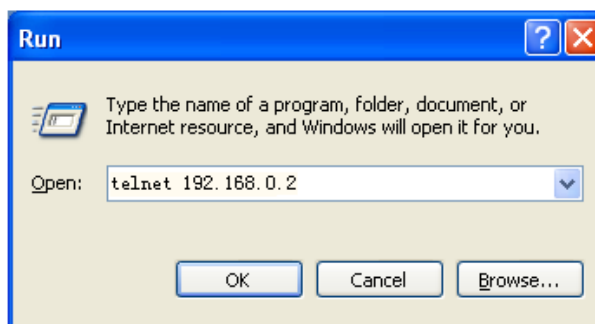


Рис. 6. Доступ через Telnet



При подтверждении IP-адреса, пожалуйста, обратитесь к разделу «IP адрес» настоящего руководства для получения информации о IP адресе.

3. Нажмите “OK”, откроется интерфейс терминала Telnet. Нажмите <Enter> для подключения к коммутатору.

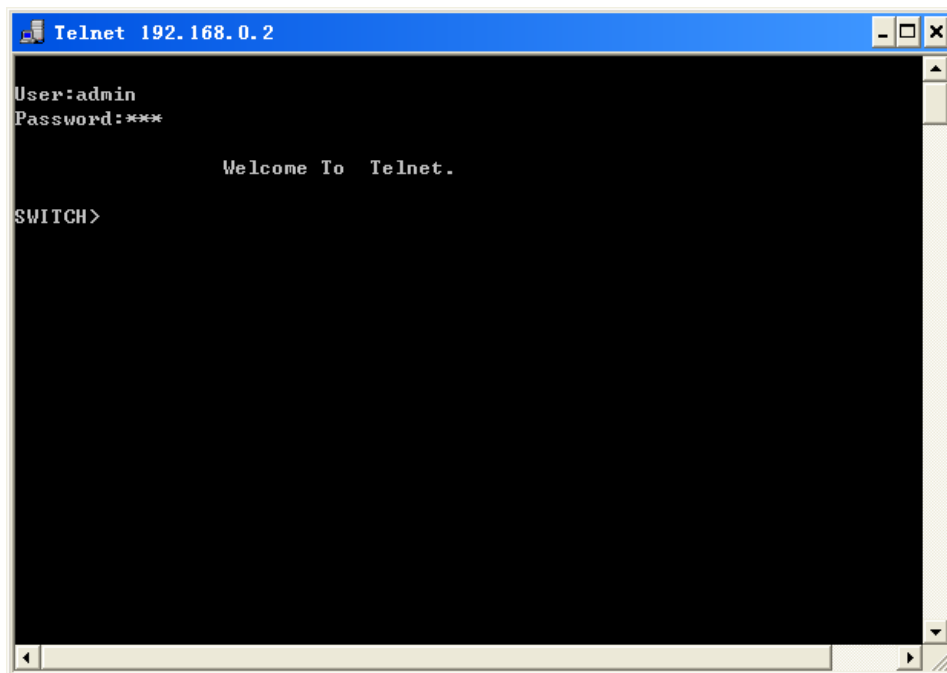


Рис. 7. Интерфейс терминала Telnet

2.4. Доступ через WEB-интерфейс

1. Подключите любой RJ45 порт коммутатора к Ethernet порту ПК.
2. Введите IP адрес коммутатора в web-браузере (IP адрес по умолчанию - 192.168.0.2). Появится диалоговое окно авторизации, показанное ниже. Введите:

Логин - **admin**

Пароль – **123**

Нажмите кнопку <Login>.



При использовании Internet Explorer, рекомендуется использовать версию не ниже 8.0.



Layer 2 Switch

User Name :

Password :

Save the password

Serial Number : S30A0001A141000005
System Name : SWITCH
Location : 121087, Moscow Russia, 6 Barclay st., 3 bldg
Contact : Symanitron Ltd., phone number +7 499
685 1790;www.symanitron.ru

Symanitron Ltd. All Rights Reserved 2013.

Рис. 8. Авторизация через WEB-интерфейс

3. После подключения к Web-интерфейсу коммутатора вы увидите «навигационное дерево» (меню) в левой части экрана:

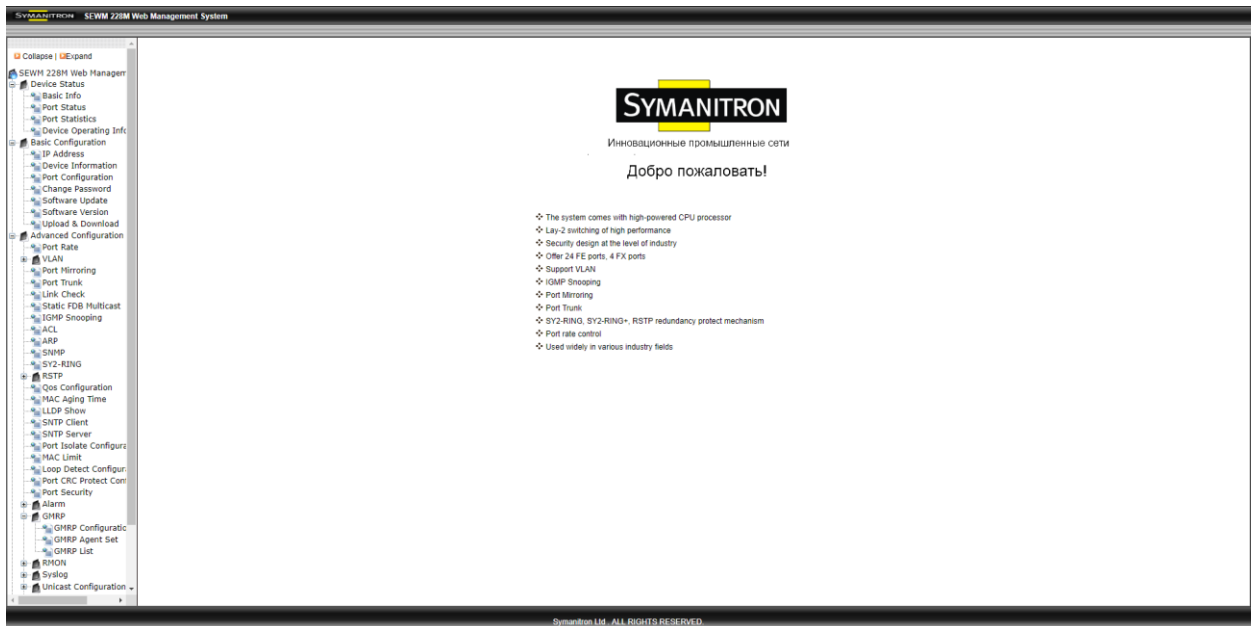


Рис. 9. Страница WEB-интерфейса

У вас есть возможность сворачивать или разворачивать меню, нажимая на кнопки <Expand> или <Collapse>, которые находятся сверху навигационного дерева. Вы можете выполнить соответствующие операции, нажав [Save Settings] или [Load Default] в верхней части меню.



После того как вы изменили заводские установки и записали новые параметры, необходимо перезагрузить устройство для того, чтобы новые параметры вступили в силу.

3. Управление устройством

Нажмите [Device Management]→[Reboot]/[Logout]. Вы сможете перезагрузить устройство или выйти из WEB-интерфейса. Перед перезагрузкой устройство сообщит вам, что необходимо сохранить текущие настройки. Если настройки были сохранены ранее, коммутатор автоматически загрузит их после перезагрузки. Если настройки не сохранялись, коммутатор по умолчанию восстановит после перезагрузки заводские настройки.

4. Статус устройства

4.1. Основная информация о коммутаторе

Основная информация о коммутаторе включает имя устройства, серийный номер, MAC-адрес, IP адрес, адрес маски подсети, адрес шлюза, модель, имя системы, версию и дату прошивки (рис.10).



Item	Information
MAC Address	00-72-74-76-78-7A
SN	S3J4M090083
IP Address	192.168.0.102
Subnet Mask	255.255.255.0
GateWay	192.168.0.40
System Name	switch
Device Model	SEWM228M
Software Version	ID:1 V1.5.42 (2012-8-4 11:11)
FW Version	v1.1.9 (2011-12-28 9:59)

Рис. 10. Основная информация о коммутаторе

4.2. Информация о статусе портов

Страница с информацией о статусе порта выводит на экран номер порта, тип порта, статус администратора, статус соединения, скорость, тип способа связи и тип управления потоком (рис. 11,12).

Port ID	Administration Status	Operation Status	Link	Speed	Duplex	Flow Control	RX	TX
FE1	Enable	Enable	Down	---	---	---	---	---
FE2	Enable	Enable	Down	---	---	---	---	---
FE3	Enable	Enable	Up	100M	Full-duplex	Off	Enable	Enable
FE4	Enable	Enable	Up	100M	Full-duplex	Off	Enable	Enable
FE5	Enable	Enable	Down	---	---	---	---	---
FE6	Enable	Enable	Down	---	---	---	---	---
FE7	Enable	Enable	Up	100M	Full-duplex	Off	Enable	Enable
FE8	Enable	Enable	Down	---	---	---	---	---
FE9	Enable	Enable	Down	---	---	---	---	---
FE10	Enable	Enable	Down	---	---	---	---	---
FE11	Enable	Enable	Down	---	---	---	---	---
FE12	Enable	Enable	Down	---	---	---	---	---
FE13	Enable	Enable	Down	---	---	---	---	---
FE14	Enable	Enable	Down	---	---	---	---	---
FE15	Enable	Enable	Down	---	---	---	---	---
FE16	Enable	Enable	Down	---	---	---	---	---
FX17	Enable	Enable	Down	---	---	---	---	---
FX18	Enable	Enable	Down	---	---	---	---	---
FX19	Enable	Enable	Down	---	---	---	---	---
FX20	Enable	Enable	Down	---	---	---	---	---

Рис. 11. Статус портов



Port ID	Administration Status	Link	Speed	Duplex	Flow Control	RX	TX
FE1	Enable	Down	---	---	---	---	---
FE2	Enable	Down	---	---	---	---	---
FE3	Enable	Down	---	---	---	---	---
FE4	Enable	Down	---	---	---	---	---
FE5	Enable	Up	100M	Full-duplex	Off	Enable	Enable
FE6	Enable	Down	---	---	---	---	---
FE7	Enable	Down	---	---	---	---	---
FE8	Enable	Down	---	---	---	---	---
FE9	Enable	Down	---	---	---	---	---
FE10	Enable	Down	---	---	---	---	---
FE11	Enable	Down	---	---	---	---	---
FE12	Enable	Down	---	---	---	---	---
FE13	Enable	Down	---	---	---	---	---
FE14	Enable	Down	---	---	---	---	---
FE15	Enable	Down	---	---	---	---	---
FE16	Enable	Down	---	---	---	---	---
FE17	Enable	Down	---	---	---	---	---
FE18	Enable	Down	---	---	---	---	---
FE19	Enable	Down	---	---	---	---	---
FE20	Enable	Down	---	---	---	---	---
FE21	Enable	Down	---	---	---	---	---
FE22	Enable	Down	---	---	---	---	---
FE23	Enable	Down	---	---	---	---	---
FE24	Enable	Down	---	---	---	---	---

Рис. 12. Статус портов (SEWM228M)

Идентификатор порта (Port ID)

Отображает информацию о портах, номера которых указаны на передней панели коммутатора.

FE: 10/100Base-TX RJ45

FX: 100Base-FX

GE: 10/100/1000Base-TX RJ45

GX: Gigabit SFP

Статус администрирования (Administration Status)

Отображение текущего статуса портов.

Enable: порт доступен и готов передаче данных.

Disable: порт заблокирован и не имеет возможность передавать данные.

Рабочий статус порта (Operation Status)

Отображение состояния функционирования портов.

Статус соединения (Link)

Отображение текущего статуса соединения на порту.

Up: порт находится в состоянии LinkUp, т.е. в состоянии соединения.

Down: порт находится в состоянии Link Down, т.е. порту соединения нет.

Скорость (Speed)

Отображение текущей скорости портов в состоянии LinkUp, т.е. в состоянии соединения.

Способ связи (Duplex)

Отображение способа связи на порту в состоянии LinkUp, т.е. в состоянии соединения.

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



Half-duplex: порт может только либо принимать, либо передавать данные.

Управление потоком (Flow Control)

Показывает статус режима управления потоком порта в состоянии LinkUp, т.е в состоянии соединения.

Прием данных (RX)

Настраиваемые опции: Enable/Disable (Включено/Выключено).

Enable: порт может принимать данные.

Disable: порт не может принимать данные.

Передача данных (TX)

Настраиваемые опции: Enable/Disable (Включено/Выключено).

Enable: порт может передавать данные.

Disable: порт не может передавать данные.



Для получения детальной информации о настройках портов, обратитесь, пожалуйста, к разделу «Port Configuration» настоящего руководства.

4.3. Статистика работы порта

Интерфейс статистики порта выводит на экран количество байт и пакетов, переданных и принятых на каждом порту, количество ошибок CRC, а также количество пакетов, длина которых менее 64 байт.

Port ID	State	Link	Bytes Sent	Packets Sent	Bytes Received	Packets Received	CRC Error	Packets 64 bytes
FE1	Enable	Down	5277997	48294	25630813	214991	2	5
FE2	Enable	Down	0	0	0	0	0	0
FE3	Enable	Up	7483954286	74000288	6112054	28784	0	0
FE4	Enable	Up	7591050482	74423769	42852999	176630	0	0
FE5	Enable	Down	1695205	12564	4461954	47023	0	0
FE6	Enable	Down	0	0	0	0	0	0
FE7	Enable	Up	33029822	135134	7545970975	74166185	0	0
FE8	Enable	Down	0	0	0	0	0	0
FE9	Enable	Down	0	0	0	0	0	0
FE10	Enable	Down	0	0	0	0	0	0
FE11	Enable	Down	0	0	0	0	0	0
FE12	Enable	Down	0	0	0	0	0	0
FE13	Enable	Down	0	0	0	0	0	0
FE14	Enable	Down	0	0	0	0	0	0
FE15	Enable	Down	0	0	0	0	0	0
FE16	Enable	Down	0	0	0	0	0	0
FX17	Enable	Down	0	0	0	0	0	0
FX18	Enable	Down	0	0	0	0	0	0
FX19	Enable	Down	0	0	0	0	0	0
FX20	Enable	Down	0	0	0	0	0	0

Reset

Рис. 13. Статистика порта

Вы можете нажать кнопку <Reset> для обнуления информации и сбора статистики заново.



4.4. Информация о работе системы

Информация о работе системы отображает время работы устройства и использование ЦП (центрального процессора).

Device Operating	
Device Operating Time:	1Days,2H:14M:41S
CPU:	0%(short-term), 1%(long-term)

Рис. 14. Информация о работе системы

5. Основные настройки коммутатора

5.1. IP адрес

1. Показать IP адрес, используя консольный порт.

Подключитесь к коммутатору через консольный порт и используйте интерфейс CLI. Введите команду «show interface» в основном режиме для проверки IP адреса коммутатора:

```

aa - HyperTerminal
File Edit View Call Transfer Help
[Icons]
SWITCH>show interface
marfec (unit number 0):
  Flags: (0x8063) UP BROADCAST MULTICAST ARP RUNNING
  Type: ETHERNET_CSMACD
  Internet address: 192.168.0.2
  Netmask 0xffffffff Subnetmask 0xffffffff
  Net 0xc0a80000 Subnet 0xc0a80000
  Mac 7200.0000.00aa
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>_
Connected 0:14:39 Auto detect SCROLL CAPS NUM Capture Print echo
  
```

Рис. 15. Отображение IP адреса



2. Настройка IP адреса

IP адрес коммутатора и адрес шлюза могут быть настроены вручную.

MAC Address	00-72-74-76-78-7A
IP Address	192.168.0.102
Subnet Mask	255.255.255.0
GateWay	192.168.0.40

Apply

Рис. 16. Настройка IP адреса



- IP адрес и адрес шлюза должны находиться в одном сегменте сети, в противном случае изменить IP адрес будет невозможно
- Для данной серии коммутаторов изменение IP адреса вступит в действие немедленно и перезагрузка коммутатора не требуется

5.2. Информация об устройстве

Информация об устройстве включает следующую информацию: имя проекта, имя коммутатора, местоположение и контакты:

Project Name	PRJNAME
System Name	switch
Location	121087, Moscow Russia,..
Contact	+7-499-685-17-90

Apply

Рис. 17. Информация об устройстве

Имя проекта (Project Name)

Настраиваемый диапазон: 1~64 символов.

Имя коммутатора (Switch Name)

Настраиваемый диапазон: 1~32 символов.

Местоположение (Location)

Настраиваемый диапазон: 1~255 символов.

Контакты (Contact)

Настраиваемый диапазон: 1~32 символов.



5.3. Настройка портов

При помощи функции настройки портов можно сконфигурировать скорость порта (port speed), статус порта (port status), тип управления потоком (flow control) и другие параметры:

Port ID	Administration Status	Operation Status	Auto	Speed	Duplex	Flow Control	RX	TX	Reset
FE1	Enable	Enable	Disable	100M	Full	Off	Enable	Enable	Noreset
FE2	Enable	Enable	Enable	100M	Full	Off	Enable	Enable	Noreset
FE3	Enable	Enable	Enable	100M	Full	Off	Enable	Enable	Noreset
FE4	Enable	Enable	Enable	100M	Full	Off	Enable	Enable	Noreset
FE5	Enable	Enable	Enable	100M	Full	Off	Enable	Enable	Noreset
FE6	Enable	Enable	Enable	100M	Full	Off	Enable	Enable	Noreset
FE7	Enable	Enable	Enable	100M	Full	Off	Enable	Enable	Noreset
FE8	Enable	Enable	Enable	100M	Full	Off	Enable	Enable	Noreset
FE9	Enable	Enable	Enable	100M	Full	Off	Enable	Enable	Noreset
FE10	Enable	Enable	Enable	100M	Full	Off	Enable	Enable	Noreset
FE11	Enable	Enable	Enable	100M	Full	Off	Enable	Enable	Noreset
FE12	Enable	Enable	Enable	100M	Full	Off	Enable	Enable	Noreset
FE13	Enable	Enable	Enable	100M	Full	Off	Enable	Enable	Noreset
FE14	Enable	Enable	Enable	100M	Full	Off	Enable	Enable	Noreset
FE15	Enable	Enable	Enable	100M	Full	Off	Enable	Enable	Noreset
FE16	Enable	Enable	Enable	100M	Full	Off	Enable	Enable	Noreset
FX17	Enable	Enable	Disable	100M	Full	Off	Enable	Enable	Noreset
FX18	Enable	Enable	Disable	100M	Full	Off	Enable	Enable	Noreset
FX19	Enable	Enable	Disable	100M	Full	Off	Enable	Enable	Noreset
FX20	Enable	Enable	Disable	100M	Full	Off	Enable	Enable	Noreset

Apply

Рис. 18. Настройка портов

Port ID	Administration Status	Auto	Speed	Duplex	Flow Control	RX	TX	Reset
FE1	Enable	Enable	100M	Full	Off	Enable	Enable	Noreset
FE2	Enable	Enable	100M	Full	Off	Enable	Enable	Noreset
FE3	Enable	Enable	100M	Full	Off	Enable	Enable	Noreset
FE4	Enable	Enable	100M	Full	Off	Enable	Enable	Noreset
FE5	Enable	Enable	100M	Full	Off	Enable	Enable	Noreset
FE6	Enable	Enable	100M	Full	Off	Enable	Enable	Noreset
FE7	Enable	Enable	100M	Full	Off	Enable	Enable	Noreset
FE8	Enable	Enable	100M	Full	Off	Enable	Enable	Noreset
FE9	Enable	Enable	100M	Full	Off	Enable	Enable	Noreset
FE10	Enable	Enable	100M	Full	Off	Enable	Enable	Noreset
FE11	Enable	Enable	100M	Full	Off	Enable	Enable	Noreset
FE12	Enable	Enable	100M	Full	Off	Enable	Enable	Noreset
FE13	Enable	Enable	100M	Full	Off	Enable	Enable	Noreset
FE14	Enable	Enable	100M	Full	Off	Enable	Enable	Noreset
FE15	Enable	Enable	100M	Full	Off	Enable	Enable	Noreset
FE16	Enable	Enable	100M	Full	Off	Enable	Enable	Noreset
FE17	Enable	Enable	100M	Full	Off	Enable	Enable	Noreset
FE18	Enable	Enable	100M	Full	Off	Enable	Enable	Noreset
FE19	Enable	Enable	100M	Full	Off	Enable	Enable	Noreset
FE20	Enable	Enable	100M	Full	Off	Enable	Enable	Noreset
FE21	Enable	Enable	100M	Full	Off	Enable	Enable	Noreset
FE22	Enable	Enable	100M	Full	Off	Enable	Enable	Noreset
FE23	Enable	Enable	100M	Full	Off	Enable	Enable	Noreset
FE24	Enable	Enable	100M	Full	Off	Enable	Enable	Noreset

Apply

Рис. 19. Настройка портов (SEWM228M)



Статус администрирования (Administration Status)

Настраиваемые опции: Enable/Disable (Включить/Выключить).

Значение по умолчанию: Enable (Включено).

Описание: Enable (Включено) означает, что порт включен и передача данных разрешена; Disable (Выключено) означает, что порт заблокирован и передача данных запрещена. Данная опция позволяет напрямую отключить порт и аварийные сообщения. Когда порт выключен, нельзя изменить состояние порта в разделе «Operation Status».

Рабочий статус порта (Operation Status)

Описание: Когда статус администрирования находится в состоянии «Enable» (Включено), рабочий статус порта принудительно устанавливается в режим «Enable» (Включено); когда статус администрирования находится в состоянии «Disable» (Выключено), рабочий статус порта принудительно устанавливается в режим «Disable» (Выключено).

Режим автосогласования (Auto)

Настраиваемые опции: Enable/Disable (Включить/Выключить).

Значение по умолчанию: Enable (Включено).

Описание: Настройка режима автосогласования (auto-negotiation) на портах. Когда режим «Auto» включен (Enable), скорость порта и дуплексный (duplex) режим способа связи будут автоматически согласованы в соответствии со статусом подключения порта; когда режим «Auto» выключен (Disable), скорость порта и режим способа связи могут быть настроены вручную пользователем.



Порты 100Base-FX принудительно установлены в режим «Disable» (Выключено).

Скорость порта (Speed)

Настраиваемые опции: 10M/100M/1000M

Описание: Принудительная настройка скорости порта. Когда режим «Auto» выключен (Disable), скорость порта можно настраивать вручную.

Способ связи (Duplex)

Настраиваемые опции: Half/Full (Полудуплекс/Дуплекс).

Описание: Настройка режима способа связи для порта; когда режим «Auto» выключен, настройку способа связи можно производить вручную.



- Порты 10/100Base-TX могут быть настроены в режиме автосогласования (auto-negotiation) а также в режимах 10M/дуплекс, 10M/полудуплекс, 100M/дуплекс, 100M/полудуплекс.
- Порты 100Base-FX могут быть настроены в режим 100M/дуплекс.
- Оптические порты 1000M могут быть настроены в режимах автосогласования (auto-negotiation) и 1000M/дуплекс.

Рекомендуется включить автосогласование (auto-negotiation) для каждого порта, чтобы избежать проблем подключения, вызванных несогласованной конфигурацией портов. Если требуется принудительно использовать режим speed/duplex, нужно убедиться, что



на каждом подключенном порту установлены одинаковые настройки скорости и режима передачи (дуплекс/полудуплекс).

Управление потоком (Flow Control)

Настраиваемые опции: Off/On (Выключено/Включено).

Значение по умолчанию: Off (Выключено).

Описание: Включить/Выключить режим управления потоком для определенного порта. После того, как функция управления потоком (Flow Control) будет включена, порт сообщит отправителю о замедлении скорости передачи, чтобы избежать потери пакетов в соответствии с каким-либо алгоритмом или протоколом, в том случае, если поток, полученный портом больше, чем размер кэша порта. Настройка режимов управления потоком для устройств, работающих по разным типам способа связи (дуплекс/полудуплекс) выполняется разными способами. Для устройств, работающих в полнодуплексном режиме, принимающая сторона должна отправить специальный кадр (Pause frame), чтобы сообщить отправителю о прекращении отправки сообщений. Когда отправитель получит Pause frame, он должен прекратить отправку сообщений на период «времени ожидания» (wait time), указанного в Pause frame и продолжить отправку сообщений после окончания «времени ожидания». Для устройств, работающих в полудуплексном режиме, обеспечивается поддержка режима управления потоком методом обратного давления. Дело в том, что принимающая сторона намеренно создает конфликт или выдает сигнал несущей. Соответственно, когда отправитель обнаруживает конфликт или сигнал несущей, необходима задержка передачи данных.

Прием данных (RX)

Настраиваемые опции: Enable/Disable (Включено/Выключено).

Значение по умолчанию: Enable (Включено).

Описание: данная функция включает или выключает режим приема данных на порту. Значение «Enable» (Включено) означает, что порт может принимать данные. Соответственно, значение «Disable» («Выключено») означает, что порт не может принимать данные.

Передача данных (TX)

Настраиваемые опции: Enable/Disable (Включено/Выключено).

Значение по умолчанию: Enable (Включено).

Описание: данная функция включает или выключает режим передачи данных на порту. Значение «Enable» (Включено) означает, что порт может передавать данные. Соответственно, значение «Disable» («Выключено») означает, что порт не может передавать данные.

Обнуление данных порта (Reset)

Настраиваемые опции: Reset/Nonreset (Обнулить/Не обнулять).

Значение по умолчанию: Nonreset (Не обнулять).

Описание: Обнулить данные порта или нет.

5.4. Изменение пароля

При первоначальной настройке коммутатора пользователь имеет возможность изменить пароль доступа «Администратора»:



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

Apply

Рис. 20. Изменение пароля

5.5. Обновление программного обеспечения (ПО)

При обновлении программного обеспечения коммутатор может получить больше возможностей. Для этих серий коммутаторов обновления программного обеспечения содержат обновление версии программного обеспечения BootROM и обновление версии системного программного обеспечения. Сначала обновите версию программного обеспечения BootROM, а затем обновите версию системного программного обеспечения. Если изменения в версии BootROM нет, пользователи смогут обновить только версию системного программного обеспечения.

Для обновления системного программного обеспечения требуется наличие сервера FTP.

5.5.1. Обновление ПО через FTP

Установите сервер FTP. В нашем примере мы покажем, как настроить сервер FTP и выполнить процедуру обновления ПО с помощью программы WFTPD.

1. Нажмите [Security]→[Users/Right], чтобы открыть раздел «Users/Right Security Dialog»; Нажмите кнопку <New User> для создания нового пользователя сервера FTP, как показано на рис. 21. Создайте имя пользователя и пароль, например, пользовательское имя «admin» и пароль «123», затем нажмите <OK>.

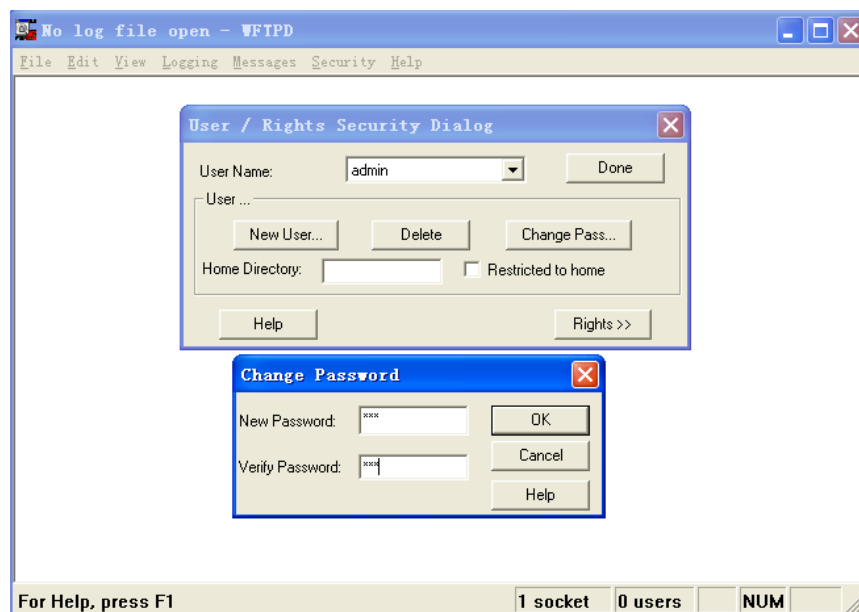


Рис. 21. Создание нового пользователя FTP



- Укажите путь к месторасположению файла обновления в разделе «Home Directory», как показано на рис. 22 и нажмите <Done>.

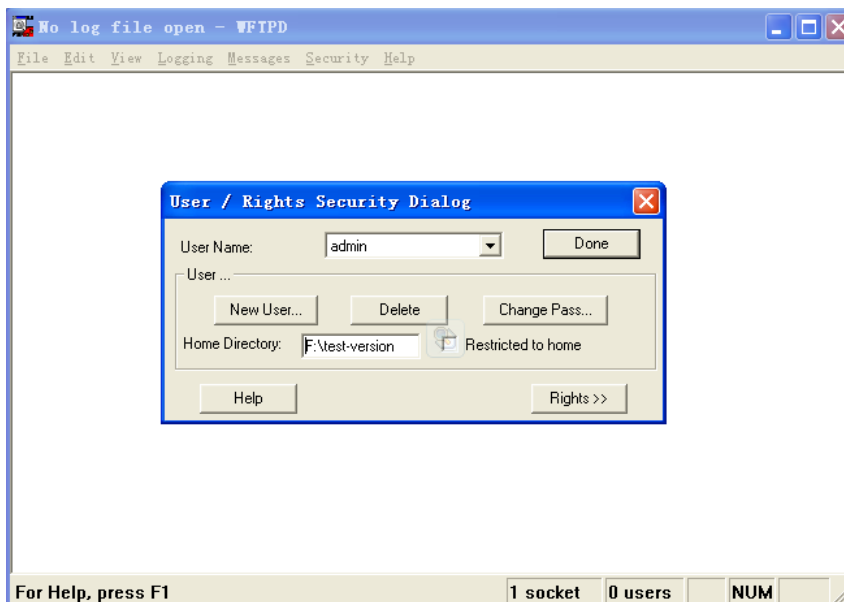


Рис. 22. Месторасположение файла

- Для обновления ПО BootROM введите следующую команду:

Switch#**update ftp-mode bootrom** *File_name Ftp_server_ip_address User_name Password*

Параметры команд для обновления BootROM через FTP:

Параметр	Описание
<i>File_name</i>	Имя версии BootROM
<i>Ftp_server_ip_address</i>	IP адрес сервера FTP
<i>User_name</i>	Создание нового пользователя FTP
<i>Password</i>	Создание нового пароля FTP

- На рис.23 показана страница обновления ПО. Введите IP адрес сервера FTP, имя файла (на сервере), имя пользователя FTP и пароль. Нажмите <Apply>.



SoftwareID	2
FTP Server IP Address	192.168.0.23
FTP File Name	SEWM228M-1.5.24.bin
FTP User Name	admin
FTP Password	•••••

Apply

Рис. 23. Обновление ПО через FTP



- Только версия системного программного обеспечения в активном состоянии может быть использована для обновления через WEB-интерфейс.
- Имя файла должно содержать расширение. В противном случае обновление может завершиться ошибкой.

5. Убедитесь в нормальном соединении сервера FTP и коммутатора:

```

No log file open - WFTPD
File Edit View Logging Messages Security Help
[L 0034] 08/25/11 17:41:06 Connection accepted from 192.168.99.43
[C 0034] 08/25/11 17:41:06 Command "USER admin" received
[C 0034] 08/25/11 17:41:06 PASSword accepted
[L 0034] 08/25/11 17:41:06 User admin logged in.
[C 0034] 08/25/11 17:41:06 Command "TYPE I" received
[C 0034] 08/25/11 17:41:06 TYPE set to I N
[C 0034] 08/25/11 17:41:06 Command "PASV" received
[C 0034] 08/25/11 17:41:06 Entering Passive Mode (192,168,99,23,4,183)
[C 0034] 08/25/11 17:41:06 Command "RETR SEWM228M.bin" received
[C 0034] 08/25/11 17:41:06 RETRIEve started on file SEWM10GP-D.bin
[C 0034] 08/25/11 17:41:18 Transfer finished
[G 0034] 08/25/11 17:41:18 Got file D:\WMSOFT\SEWM228M\SEWM228M.bin
[C 0034] 08/25/11 17:41:18 Command "QUIT" received
[C 0034] 08/25/11 17:41:18 QUIT or close - user admin logged out

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

Рис. 24. Соединение коммутатора и сервера FTP



Чтобы отобразить информацию журнала обновлений, как показано на рис. 21, нужно нажать [Logging]->[Log Option] в WFTPD и выбрать режим «Enable Logging» и информацию журнала будет отображена на экране.



6. Когда обновление будет завершено, перезагрузите устройство и откройте страницу «Основная информация о коммутаторе», чтобы проверить, было ли обновление успешным и убедиться, что новая версия активна.



The software is upgraded successfully!

Рис. 25. Обновление через FTP завершено



- В процессе обновления ПО сервер FTP должен быть постоянно загружен.
- После завершения обновления перезагрузите устройство, чтобы активировать новую версию ПО.
- Если обновление завершено с ошибкой, не перезагружайте устройство, чтобы избежать потери файла с ПО. Есть вероятность того, коммутатор не сможет функционировать корректно.

5.6. Запрос версии ПО

Две версии программного обеспечения могут быть загружены в коммутатор, но только одна может быть в активном состоянии. В веб-интерфейсе вы можете обновить только неактивную версию.

При запросе версии программного обеспечения вы можете узнать номер версии, даты выпуска и статусы двух версий (см. рис. 26).



ID	Version	Date	Status
1	v1.5.42	2012-8-4 11:11	Active
2	v1.5.41	2012-7-25 10:19	Inactive

Apply

Рис. 26. Обновление через FTP завершено

5.7. Функция резервного копирования и загрузки настроек

У коммутатора имеется функция резервного копирования настроек. Данная функция позволяет сохранять текущие файлы с конфигурацией коммутатора на сервере. После того, как настройки коммутатора были изменены, пользователи имеют возможность загрузить файлы с исходными настройками с сервера на коммутатор с использованием протоколов FTP/TFTP.

Файлы с настройками коммутатора хранятся на сервере в форматах *.doc и *.txt. Процедура загрузки сохраненных файлов с настройками с сервера на коммутатор показана на рис. 27-28.



После того, как файл конфигурации загружен в коммутатор, необходимо перезагрузить устройство для того, чтобы новые параметры вступили 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

Рис. 27. Настройка загрузки файла

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

Apply

Рис. 28. Настройка выгрузки файла

6. Расширенная настройка

6.1. Ограничение скорости портов (Port Rate Limiting)

6.1.1. Введение

Настройка скорости порта ограничивает количество принимаемых/передаваемых сообщений и отбрасывает данные, превышающие пороговое значение. Данная функция обеспечивает возможность для входящих пакетов ограничивать скорость определенных типов сообщений, в то время как для исходящих пакетов ограничивается скорость всех сообщений.

Следующие типы входящих пакетов могут контролироваться данной функцией:

- Unicast packets: одноадресные пакеты, добавленные статически или на основании определения MAC адреса источника;
- Multicast packets: пакеты, добавленные статически или полученные через IGMP Snooping или GMRP;
- Broadcast packets: пакеты с MAC-адресом назначения FF: FF: FF: FF: FF: FF;
- Reserved multicast packets: пакеты с MAC адресами в диапазоне от 0x0180c2000000 до 0x0180c200002f;
- Unknown multicast packets: пакеты, которые не были добавлены статически или не были определены через IGMP Snooping или GMRP;
- Unknown unicast packets: пакеты, которые не были добавлены статически или у которых не был определен источник MAC адреса;



- Unknown source packets: пакеты с неопознанным источником MAC адреса.

6.1.2. Настройка через WEB-интерфейс

1. Выбор типа пакетов для управления скоростью передачи.

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

Рис. 29. Типы пакетов для управления скоростью передачи

Принимающая сторона разделяет функцию управления скоростью на два типа: управление скоростью сервисных пакетов и управление скоростью широковещательных пакетов. Каждый пакет может быть добавлен только к одному типу управления скоростью.

2. Настройка управления скоростью на портах.

Port ID	Service	Broadcast	OutRate
FE1	0 Kbps	0 Kbps	0 Kbps
FE2	70 Kbps	80 Kbps	90 Kbps
FE3	0 Kbps	0 Kbps	0 Kbps
FE4	0 Kbps	0 Kbps	0 Kbps
FE5	0 Kbps	0 Kbps	0 Kbps

Рис. 30. Управление скоростью на портах

Сервисные пакеты/Широковещательные пакеты (Service/Broadcast)

Настраиваемый диапазон: 64~1000000 Кбит/с

Описание: Настройка контроля скорости пакетов на порту. Пакеты, чья скорость выше указанного значения, отбрасываются. Входящая скорость для портов 100М находится в диапазоне от 64 до 100000 Кбит/с. Входящая скорость для портов 1000М находится в диапазоне от 64 до 1000000 Кбит/с.

Исходящая скорость (OutRate)

Настраиваемый диапазон: 64~1000000 Кбит/с

Описание: Ограничение скорости пакетов, пересылаемых портом. Исходящая скорость для портов 100М находится в диапазоне от 64 до 100000 Кбит/с. Исходящая скорость для портов 1000М находится в диапазоне от 64 до 100000 Кбит/с.



Если установлено значение скорости «0», то для данного порта функция управления скоростью находится в состоянии «Disable» (Выключено).

6.1.3. Пример типовой настройки

Настройка порогового значения скорости одноадресных и многоадресных пакетов на порту 2 в значение 70 Кбит/с, настройте значение скорости 80 Кбит/с для многоадресных, неизвестных многоадресных и одноадресных пакетов, а для исходящей скорости установите значение 90 Кбит/с.

Шаги настройки:

1. Выберите пакеты одноадресной и многоадресной рассылки в колонке «Service», выделите многоадресные, неизвестные многоадресные, одноадресные и широковещательные пакеты в колонке «Broadcast» (см. рис. 29);
2. На порту 2 установите пороговое значение скорости сервисных пакетов 70 Кбит/с, установите пороговое значение скорости широковещательных пакетов 80 Кбит/с и исходящую скорость 90 Кбит/с (см рис. 30).

6.2. Виртуальные локальные сети VLAN

6.2.1. Введение

VLAN (Virtual Local Area Networks) делит LAN на несколько логических VLAN. Устройства в одной и той же VLAN могут взаимодействовать друг с другом, а устройства в разных VLAN – нет. Таким образом, широковещательные сообщения ограничены в VLAN, что повышает безопасность локальной сети.

Разделение сети на VLAN не ограничено физическим расположением устройств. Каждый VLAN рассматривается как отдельная логическая сеть. Для передачи данных между двумя разными VLAN необходим маршрутизатор, либо коммутатор 3-го уровня.

6.2.2. Принцип работы

Для того, чтобы сетевые устройства могли различать пакеты из разных VLAN, в кадры добавляются специальные идентификационные поля. На данный момент, самым распространённым протоколом для идентификации VLAN является IEEE802.1Q. Структура кадров 802.1Q показана в таблице:

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

В обычный Ethernet кадр добавляется 4-х байтный заголовок 802.1Q, который служит тегом VLAN.

Тип: 16 бит, используемые для идентификации того, что кадр содержит тег VLAN, а значение: 0x8100.

PRI: три бита, показывающие приоритет кадра 802.1p.

CFI: один бит. 0 обозначает Ethernet, а 1 - Token Ring.

VID: 12 бит, указывающие идентификатор VLAN в диапазон значений: от 1 до 4093. При этом 0, 4094 и 4095 - зарезервированные значения.



- VLAN 1 - это VLAN по умолчанию, Пользователь не может его создать или удалить вручную.
- Резервированные номера VLAN нужны для реализации специальных системных функций и также не могут быть созданы или удалены вручную.

Сообщение, содержащее заголовок 802.1Q, представляет собой тегированное сообщение (Tag message); если заголовка нет, то это сообщение нетегированное (Untag). Все сообщения в коммутаторе имеют тег 802.1Q.

6.2.3. VLAN на основе портов (Port-based VLAN)

Разделение на VLAN может быть либо по портам, либо по MAC адресам. Данная серия коммутаторов поддерживает разделение VLAN на основе портов. Данная функция определяет членов VLAN на основе портов коммутатора. Она добавляет порты в назначенные VLAN, а затем порты могут пересылать назначенные сообщения VLAN.

1. Тип порта

В соответствии с методами обработки тегов VLAN при передаче сообщений, порт можно разделить на два типа:

- Untag port (нетегированный порт): сообщения, отправленные с этого типа порта, не имеют тега. Как правило, этот тип порта используется для подключения к терминальному оборудованию, которое не поддерживает протокол 802.1Q. По умолчанию все порты коммутатора являются портами Untag и относятся к VLAN1.
- Tag port (тегированный порт): все сообщения, пересылаемые с этого типа порта, несут тег VLAN. Этот тип порта обычно используется для подключения сетевых передающих устройств.

2. Идентификатор порта с VLAN (Port VLAN Identifier, PVID)

Каждый порт имеет атрибут PVID. Когда порт получает сообщение нетегированное сообщение, он добавляет тег в сообщение в соответствии с PVID.

Порт PVID - это идентификатор VLAN для нетегированного порта. По умолчанию PVID всех портов является VLAN 1.

Существует определенные процессы в коммутаторе при обработке сообщений, получаемых и передаваемых через порт в соответствии с типом порта и PVID (см. таблицу):



Обработка полученных пакетов		Обработка пакетов для пересылки	
Нетегированные пакеты	Тегированные пакеты	Тип порта	Обработка пакетов
Добавить теги PVID в нетегированные пакеты.	<ul style="list-style-type: none"> Если идентификатор (ID) VLAN в пакете находится в списке разрешенных VLAN, принять пакет Если идентификатор (ID) VLAN в пакете отсутствует в списке разрешенных VLAN, отбросить пакет. 	Untag	Переслать пакет после удаления тега.
		Tag	Сохранить тег и переслать пакет.

6.2.4. Настройка через WEB-интерфейс

1. Настройка прозрачного режима передачи VLAN



Рис. 31. Настройка прозрачного режима передачи VLAN

Фильтр прав доступа VLAN (Ingress VLAN Filter)

Настраиваемые опции: Nonmember Drop/Nonmember Forward.

Значение по умолчанию: Nonmember Drop

Описание: Настройка прозрачного режима передачи VLAN. Прозрачный режим передачи предполагает проверку коммутатором входящих пакетов на порту. Если выбран режим «Nonmember Drop», пакеты будут отбрасываться, в случае когда пакеты с тегом VLAN отличается от VLAN порта. Если выбран режим «Nonmember Forward», пакет принимается, когда пакет с тегом VLAN пакета идентичен VLAN любого подключенного порта на коммутаторе; в противном случае пакет отбрасывается.

2. Создание VLAN

Нажмите <Add> (см. рис.31) для создания VLAN. Затем выберите порты, которые должны быть добавлены к VLAN и настройте параметры портов (см. рис. 32).



VLAN Name:

VLAN ID:

Port ID	VLAN Member	Priority	PVLAN
FE1	<input type="text" value="-----"/>	<input type="text" value="0"/>	<input type="text" value="Disable"/>
FE2	<input type="text" value="-----"/>	<input type="text" value="0"/>	<input type="text" value="Disable"/>
FE3	<input type="text" value="-----"/>	<input type="text" value="0"/>	<input type="text" value="Disable"/>
FE4	<input type="text" value="-----"/>	<input type="text" value="0"/>	<input type="text" value="Disable"/>
FE5	<input type="text" value="Tagged"/>	<input type="text" value="0"/>	<input type="text" value="Disable"/>
FE6	<input type="text" value="Untagged"/>	<input type="text" value="1"/>	<input type="text" value="Disable"/>
FE7	<input type="text" value="Untagged"/>	<input type="text" value="4"/>	<input type="text" value="Disable"/>
FE8	<input type="text" value="-----"/>	<input type="text" value="0"/>	<input type="text" value="Disable"/>
FE9	<input type="text" value="-----"/>	<input type="text" value="0"/>	<input type="text" value="Disable"/>
FE10	<input type="text" value="-----"/>	<input type="text" value="0"/>	<input type="text" value="Disable"/>
FE11	<input type="text" value="-----"/>	<input type="text" value="0"/>	<input type="text" value="Disable"/>
FE12	<input type="text" value="-----"/>	<input type="text" value="0"/>	<input type="text" value="Disable"/>
FE13	<input type="text" value="-----"/>	<input type="text" value="0"/>	<input type="text" value="Disable"/>

Рис. 32. Настройка VLAN

Имя VLAN (VLAN Name)

Настраиваемый диапазон: 1~31 символов.

Описание: Настройка имени VLAN.

Идентификатор VLAN (VLAN ID)

Настраиваемый диапазон: 2~4093.

Описание: Настройка идентификатора VLAN. ID VLAN используется для распознавания соответствующего VLAN. Данные серии коммутаторов поддерживает до 256 VLAN.

Настройка участника VLAN (VLAN Member)

Настраиваемые опции: Тегированный/Нетегированный (Tagged/Untagged).

Описание: Выбор типа порта в VLAN.

Приоритет (Priority)

Настраиваемый диапазон: 0~7.

Значение по умолчанию: 0

Описание: Настройка приоритета порта по умолчанию. При добавлении тега 802.1Q в нетегированное сообщение, значение поля PRI является этим приоритета.

Настройка PVLAN (PVLAN)

Настраиваемые опции Enable/Disable (Включить/Выключить).

Значение по умолчанию: Disable (Выключено).

Описание: Чтобы добавить тегированный порт к VLAN, необходимо включить или выключить функцию PVLAN. Более подробная информация содержится в разделе «PVLAN».



Нетегированный порт может быть добавлен только к одной VLAN. Идентификатор VLAN - это PVID порта. По умолчанию это VLAN 1, при этом тегированный порт может подключаться к нескольким VLAN.



3. Отображение списка VLAN

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---3

Apply Add

Рис. 33. Отображение списка VLAN

Список PVLAN (PVLAN List)

Настраиваемые опции: Select/Deselect (Выбрать/Не выбрано)

Описание: Включение или выключение функции PVLAN. Дополнительная информация будет представлена в разделе «PVLAN».

4. Для отображения PVID портов нажмите <Untagged Port VLAN List> (см. рис. 33).

Untagged Port VLAN List

Port ID	VLAN ID
FE1	1
FE2	1
FE3	1
FE4	1
FE5	1
FE6	2
FE7	2
FE8	1
FE9	1
FE10	1
FE11	1
FE12	1
FE13	1
FE14	1
FE15	1
FE16	1
FX17	1
FX18	1
FX19	1
FX20	1

Рис. 34. Список портов PVID



Каждый порт должен иметь атрибут Untag (нетегированный). Если атрибут не установлен, нетегированный порт по умолчанию используется в VLAN 1.

5. Изменение/Удаление VLAN

Нажмите <VLAN list> (см. рис. 33). Вы сможете изменить или удалить созданный VLAN. Нажмите <Delete>, чтобы удалить выбранную VLAN. Кроме того, вы можете удалить VLAN напрямую (см. рис. 35).

VLAN Name :

VLAN ID :

Port ID	VLAN Member	Priority	PVLAN
FE1	<input type="text" value="-----"/>	<input type="text" value="0"/>	<input type="text" value="Disable"/>
FE2	<input type="text" value="-----"/>	<input type="text" value="0"/>	<input type="text" value="Disable"/>
FE3	<input type="text" value="-----"/>	<input type="text" value="0"/>	<input type="text" value="Disable"/>
FE4	<input type="text" value="-----"/>	<input type="text" value="0"/>	<input type="text" value="Disable"/>
FE5	<input type="text" value="Tagged"/>	<input type="text" value="0"/>	<input type="text" value="Disable"/>
FE6	<input type="text" value="Untagged"/>	<input type="text" value="1"/>	<input type="text" value="Disable"/>
FE7	<input type="text" value="Untagged"/>	<input type="text" value="4"/>	<input type="text" value="Disable"/>
FE8	<input type="text" value="-----"/>	<input type="text" value="0"/>	<input type="text" value="Disable"/>
FE9	<input type="text" value="-----"/>	<input type="text" value="0"/>	<input type="text" value="Disable"/>
FE10	<input type="text" value="-----"/>	<input type="text" value="0"/>	<input type="text" value="Disable"/>
FE11	<input type="text" value="-----"/>	<input type="text" value="0"/>	<input type="text" value="Disable"/>
FE12	<input type="text" value="-----"/>	<input type="text" value="0"/>	<input type="text" value="Disable"/>
FE13	<input type="text" value="-----"/>	<input type="text" value="0"/>	<input type="text" value="Disable"/>
FE14	<input type="text" value="-----"/>	<input type="text" value="0"/>	<input type="text" value="Disable"/>
FE15	<input type="text" value="-----"/>	<input type="text" value="0"/>	<input type="text" value="Disable"/>
FE16	<input type="text" value="-----"/>	<input type="text" value="0"/>	<input type="text" value="Disable"/>
FX17	<input type="text" value="-----"/>	<input type="text" value="0"/>	<input type="text" value="Disable"/>
FX18	<input type="text" value="-----"/>	<input type="text" value="0"/>	<input type="text" value="Disable"/>
FX19	<input type="text" value="-----"/>	<input type="text" value="0"/>	<input type="text" value="Disable"/>
FX20	<input type="text" value="-----"/>	<input type="text" value="0"/>	<input type="text" value="Disable"/>

Рис. 35. Изменение, удаление, создание VLAN

6.2.5. Пример типовой настройки

Как показано на рис. 36, сеть разделена на 3 VLAN: VLAN2, VLAN100 и VLAN200. Необходимо, чтобы устройства в одной VLAN могли взаимодействовать друг с другом, при этом другие VLAN были изолированы. ПК не могут различать теги сообщений, поэтому порты коммутаторов А и В, подключенные к ПК, настроены как нетегированные (Untag). Сообщения VLAN2, VLAN100 и VLAN200 должны передаваться между коммутатором А и



коммутатором В, поэтому порты, соединяющие коммутаторы А и В, должны быть настроены как тегированные (Tag), что позволит транслировать сообщения VLAN2, VLAN100 и VLAN200. В таблице показана конфигурация устройств:

VLAN	Настройка
VLAN2	Настройте порты 1 и 2 на коммутаторах А и В как нетегированные порты (Untag ports), а порт 7 как тегированный порт (Tag port)
VLAN100	Настройте порты 3 и 4 на коммутаторах А и В как нетегированные порты (Untag ports), а порт 7 как тегированный порт (Tag port)
VLAN200	Настройте порты 5 и 6 на коммутаторах А и В как нетегированные порты (Untag ports), а порт 7 как тегированный порт (Tag port)

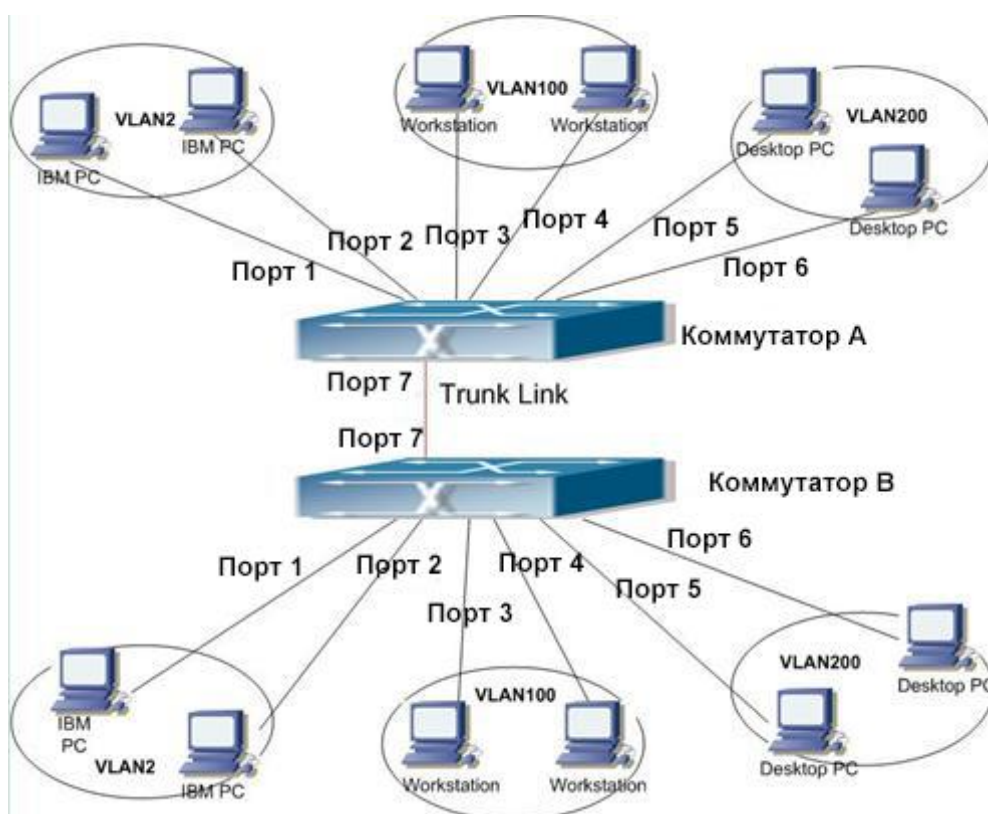


Рис. 36. Настройка VLAN

Настройте коммутаторы А и В, как показано ниже:

1. Создайте VLAN2, добавьте в VLAN2 порты 1 и 2 как нетегированные (Untag); добавьте порт 7 в VLAN2 как тегированный (Tag) порт (см. рис. 32).



2. Создайте VLAN100, добавьте в VLAN100 порты 3 и 4 как нетегированные (Untag); добавьте порт 7 в VLAN100 как тегированный (Tag) порт (см. рис. 32).
3. Создайте VLAN200, добавьте в VLAN 200 порты 5 и 6 как нетегированные (Untag); добавьте порт 7 в VLAN200 как тегированный (Tag) порт (см. рис. 32).

6.3. Изолированная VLAN (Private VLAN, PVLAN)

6.3.1. Введение

Для реализации комплексной функции изоляции трафика порта, обеспечения безопасности сети и изоляции широковещательного домена PVLAN использует два уровня технологии изоляции.

Верхняя (upper) VLAN - это VLAN с общим доменом, в которой порты являются магистральными (Uplink). Нижняя (lower) VLAN - это VLAN с изолированными доменами, в которых порты являются оконечными (Downlink). Оконечные порты могут быть назначены в различных изолированных доменах, и они могут одновременно устанавливать соединение с магистральным портом. Изолированные домены не могут устанавливать соединение друг с другом.

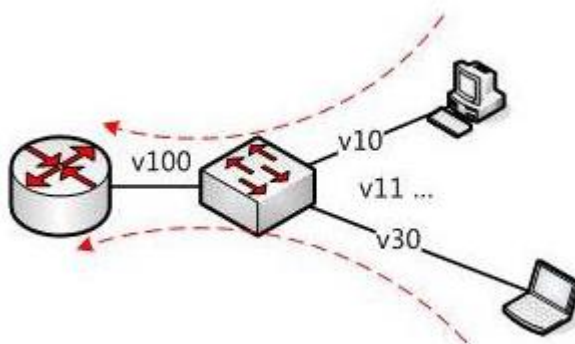


Рис. 37. Схема PVLAN

Как показано на рис. 37, общим доменом является VLAN100, а изолированными доменами являются VLAN10 и VLAN30; устройства в изолированных доменах могут устанавливать соединение с устройством в общем домене, например, VLAN10 может связываться с VLAN100; VLAN30 также может взаимодействовать с VLAN100, но устройства в изолированных доменах не могут устанавливать соединение друг с другом, например, VLAN10 не может связываться с VLAN30.



Когда тегированный порт с включенной функцией PVLAN пересылает фрейм с тегом VLAN, тег VLAN будет удален.

6.3.2. Настройка через WEB- интерфейс

1. Включение на порту функции PVLAN.



VLAN Name:

VLAN ID:

Port ID	VLAN Member	Priority	PVLAN
FE1	Tagged	0	Enable
FE2	Tagged	0	Enable
FE3	Untagged	0	Disable
FE4	Untagged	0	Disable
FE5	Tagged	0	Enable
FE6	Tagged	1	Enable
FE7	-----	4	Disable
FE8	-----	0	Disable
FE9	-----	0	Disable
FE10	-----	0	Disable

Рис. 38. Включение функции PVLAN

Вам необходимо включить PVLAN на тегированных портах в VLAN.

Если VLAN является общим доменом, магистральный порт должен быть настроен как нетегированный, а оконечный порт должен быть настроен как тегированный.

Если VLAN является изолированным доменом, оконечный порт должен быть настроен как нетегированный, а магистральный порт должен быть настроен как тегированный.

2. Выбор участников VLAN для включения в PVLAN.

Ingress VLAN Filter :

Untagged Port VLAN List

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

Рис. 39. Настройка участников PVLAN

Список PVLAN (PVLAN list)

Настраиваемые опции: Select/Deselect (Выбрать/Не выбрано)

Значение по умолчанию: Deselect (Не выбрано).

Описание: Выбор участников PVLAN.



Участниками PVLAN являются как общие, так изолированные домены.



6.3.3. Пример типовой настройки

На рис. 40 показан пример конфигурации PVLAN. VLAN300 является общим доменом, а порт 1 и порт 2 – магистральными портами; VLAN100 и VLAN200 являются изолированными доменами, а порты 3, 4, 5 и 6 являются оконечными портами.

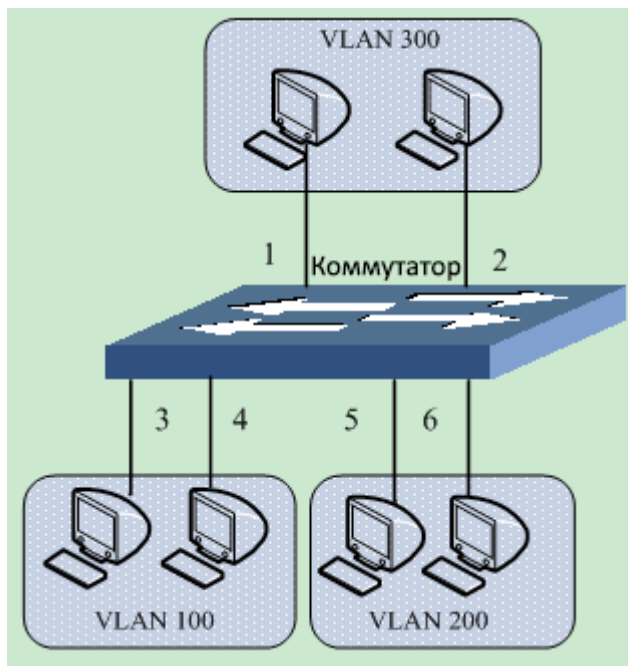


Рис. 40. Пример конфигурации PVLAN

Настройка коммутатора:

1. Настройте VLAN300 как открытый домен (см. рис. 38).
 - Порты 1 и 2 должны быть настроены как нетегированные и назначены в открытый домен VLAN 300;
 - Порты 3 и 4 должны быть настроены как тегированные и назначены в открытый домен VLAN 300, функция PVLAN должна быть включена;
 - Порты 5 и 6 должны быть настроены как тегированные и назначены в открытый домен VLAN 300, функция PVLAN должна быть включена.
2. Настройте VLAN 100 как изолированный домен (см. рис. 38).
 - Порты 1 и 2 должны быть настроены как тегированные и назначены в изолированный домен VLAN 100, функция PVLAN должна быть включена;
 - Порты 3 и 4 должны быть настроены как нетегированные и назначены в изолированный домен VLAN 100.
3. Настройте VLAN 200 как изолированный домен (см. рис. 38).
 - Порты 1 и 2 должны быть настроены как тегированные и назначены в изолированный домен VLAN 200, функция PVLAN должна быть включена;
 - Порты 5 и 6 должны быть настроены как нетегированные и назначены в изолированный домен VLAN 200.
4. Настройте VLAN 300, VLAN 100 и VLAN 200 как участников PVLAN (см. рис. 39).



6.4. Зеркалирование портов (Port Mirroring)

6.4.1. Введение

Port Mirroring – зеркалирование портов. Благодаря функции зеркалирования портов, порт копирует все переданные и принятые данные одного порта (порт источника) на другой (порт назначения). Порт назначения, на который передаются данные, как правило, подключается к анализатору протоколов или RMON-монитору, для управления, мониторинга и диагностики неисправностей.

6.4.2. Описание

Коммутатор поддерживает только один порт зеркалирования, на который отправляются данные (порт назначения), но при этом нет ограничений на количество портов источника. Порты, данные которых зеркалируются, могут быть как в одном VLAN так и в разных. При этом порты источника и назначения зеркалирования также могут быть в одном или в разных VLAN.

Порты источника и назначения должны быть разными портами.



- Настройка порта в режиме зеркалирования и в режиме транковой группы – взаимоисключающие. Порт источника/назначения зеркалирования не может быть добавлен в транковую группу, в то же время порты, входящие в транковую группу нельзя настроить в режиме портов источника/назначения зеркалирования.
- Настройка порта в режиме зеркалирования и в режиме кольцевого порта - взаимоисключающие. Порт источника/назначения зеркалирования не может быть назначен кольцевым портом и на нем нельзя включать кольцевые протоколы. В то же время порт с поддержкой кольцевого протокола не может быть настроен как порт зеркалирования.

6.4.3. Настройка через WEB-интерфейс

1. Выбор порта назначения в режиме зеркалирования.



Рис. 41. Выбор порта зеркалирования

Порт зеркалирования (Mirroring Port)

Настраиваемые опции: Disable/A switch port (Выключено/Выбор порта коммутатора)

Значение по умолчанию: Disable (Выключено)

Описание: Выбор порта назначения режима зеркалирования. Только один порт может быть настроен как порт назначения.



2. Выбор порта источника и режима зеркалирования.

Mirrored Port	Mode
<input checked="" type="checkbox"/> FE1	RX & TX
<input type="checkbox"/> FE2	RX
<input checked="" type="checkbox"/> FE3	RX
<input type="checkbox"/> FE4	RX
<input checked="" type="checkbox"/> FE5	TX
<input type="checkbox"/> FE6	RX

Рис. 42. Настройка порта источника

Режим (Mode)

Настраиваемые опции: RX/TX/RX&TX

Описание: Выбор данных для зеркалирования.

TX – зеркало передаваемых сообщений портом источником.

RX – зеркало принимаемых сообщений портом источником.

RX&TX – зеркало всех принимаемых и передаваемых сообщений порта источника.

6.4.4. Пример типовой настройки

Как видно на рисунке 43, порт 2 это порт назначения режима зеркалирования, а порт 1 – порт источник. Все сообщения на порту 1 зеркалируются на порт 2.



Рис. 43. Настройка порта источника

Процесс настройки:

1. Настройте порт 2 в режим порта назначения, как показано на рис. 41.
2. Настройте порт 1 как порт источник зеркалирования, режим порта зеркалирования установите как RX&TX, как показано на рис. 42.

6.5. Транковые порты (Trunk Port)

6.5.1. Введение

Транковые порты связывают группу физических портов с одинаковой конфигурацией в один логический порт. Порты в группе не только могут использовать логический канал



совместно, но также могут стать динамическим резервированием каждого канала, для повышения надежности соединения.

6.5.2. Реализация функции

Как показано на рис.44, три порта коммутатора А объединены (агрегированы) в Транковую группу и пропускная способность Транковой группы является общей пропускной способностью трех портов.

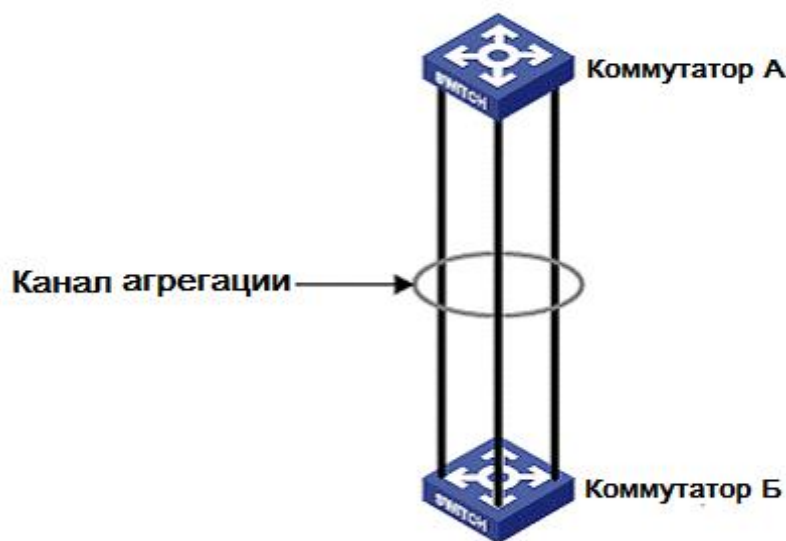


Рис. 44. Транковые порты

Когда коммутатор А передает данные для коммутатора В через агрегированный канал, транковая группа коммутатора А будет распределять потоки данных в соответствии с определенным алгоритмом, при этом только один порт будет выбран для передачи данных. Если произойдет сбой на одном из портов транковой группы, то в соответствии с алгоритмом, данные передаваемые этим портом, будут перераспределены на другой нормально работающий порт.

6.5.3. Описание

Режим настройки порта как транкового и следующие операции с портами являются взаимоисключающими:

- Порт с работающим протоколом кольцевого резервирования не может быть включен в состав транковой группы. На порту, входящем в транковую группу нельзя включить протокол кольцевого резервирования, т.е. он не может быть конфигурирован как порт в составе кольца, в то же время порт с включенным протоколом кольцевого резервирования нельзя подключить к транковой группе.
- Порт, сконфигурированный в режиме зеркалирования портов, не может быть включен в состав транковой группы. На порту, входящему в транковую группу, нельзя включить режим зеркалирования портов, а порт, на котором включен режим зеркалирования портов, нельзя включить в состав транковой группы.

Кроме того, не рекомендуется выполнять следующие операции:



- Включать протокол GMRP на транковых портах.
- Добавлять порты с включенным протоколом GMRP в транковые группы.
- Добавлять транковые порты к записям статических одноадресных/многоадресных рассылок.
- Добавлять порты, включенные в записи статических одноадресных/многоадресных рассылок, к транковым группам.



- Гигабитные порты данных серий коммутаторов не поддерживают режим транковых портов.
- Порт может быть подключен только к одной транковой группе.

6.5.4. Настройка через WEB-интерфейс

1. Добавление транкового порта. Нажмите <Add>, чтобы добавить транковую группу (см. рис. 45).



Рис. 45. Добавление транковой группы

2. Настройка транковой группы.

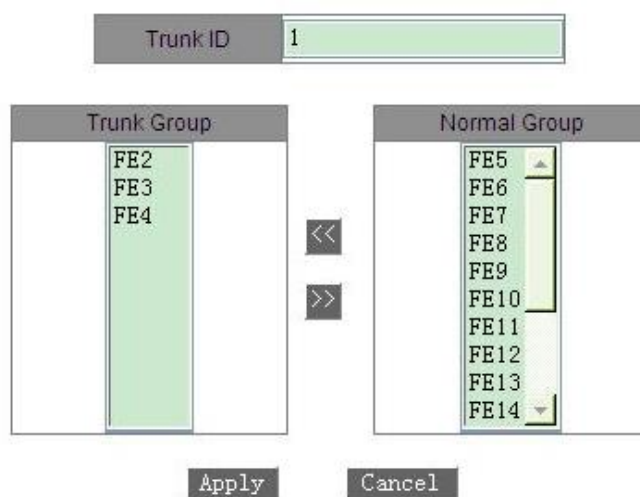


Рис. 46. Настройка транковой группы

Идентификатор транковой группы (Trunk ID)

Настраиваемый диапазон: 1~2

Описание: Установки идентификатора транковой группы. Данная серия коммутаторов поддерживает максимум 2 транковых группы. Каждая транковая группа поддерживает максимум 4 порта.



3. Просмотр списка транковых групп

Trunk List	Member Port	Lock
trunk--1	FE2 FE3 FE4	<input type="checkbox"/>
trunk--2	FE5 FE6 FE7 FE8	<input type="checkbox"/>

Рис. 47. Просмотр списка транковых групп

Блокировка (Lock)

Установите «флажок» в соответствующем поле для блокировки портов участников транковой группы. После того, как заблокированные порты участники будут удалены из транковой группы, необходимо вручную разблокировать порты.

Нажмите на имя транковой группы (см. рис. 47). Вы сможете изменять или удалять транковые группы (см. рис. 48).

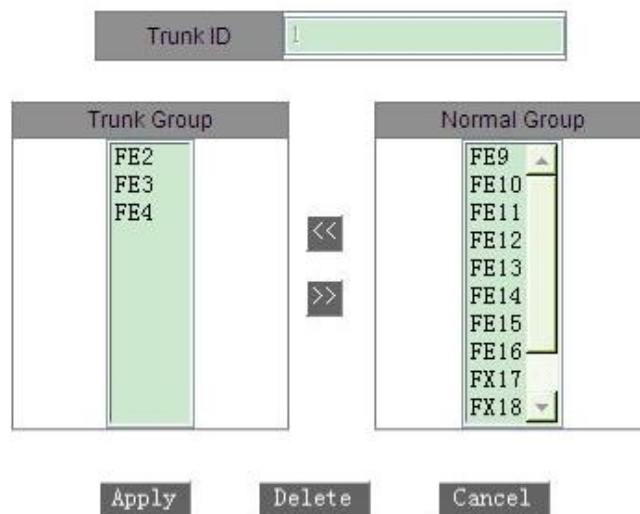


Рис. 48. Изменение параметров или удаление транковой группы

После изменения параметров участника группы (добавления нового порта к группе или удаления порта участника из группы), нажмите <Apply>, чтобы изменения вступили в силу. Если вы нажмете <Delete>, вы можете удалить группу.

6.5.5. Пример типовой настройки

Как показано на рисунке 44, порта 2, 3 и 4 коммутатора А подключаются к портам коммутатора В соответственно для формирования транковой группы 1, чтобы реализовать разделение потоков между портами.

Настройка коммутатора:

1. Создайте транковую группу 1 на коммутаторе А и добавьте порты 2, 3 и 4 в группу (см. рис. 46).



- Создайте транковую группу 1 на коммутаторе В и добавьте порты 2, 3 и 4 в группу (см. рис. 46).

6.6. Проверка связи (Link Check)

6.6.1. Введение

Проверка связи (Link Check) - это проверка того, насколько корректно порты с включенными протоколами кольцевого резервирования (STP/RSTP/Sy2-RP/Sy2-Ring) передают данные. Когда происходит аварийное переключение, режим проверки своевременно может обнаружить проблему.

6.6.2. Настройка через WEB-интерфейс

1. Настройка проверки связи

Link Check			
Port	Administration Status		Run Status
FE1	Enable	▼	Normal Link
FE2	Enable	▼	Receive Fault
FE3	Enable	▼	Send Fault
FE4	Disable	▼	Disable
FE5	Disable	▼	Disable
FE6	Disable	▼	Disable
FE7	Disable	▼	Disable
FE8	Disable	▼	Disable
FE9	Disable	▼	Disable
FE10	Disable	▼	Disable
FE11	Disable	▼	Disable
FE12	Disable	▼	Disable
FE13	Disable	▼	Disable
FE14	Disable	▼	Disable
FE15	Disable	▼	Disable
FE16	Disable	▼	Disable
FX17	Disable	▼	Disable
FX18	Disable	▼	Disable
FX19	Disable	▼	Disable
FX20	Disable	▼	Disable

Apply

Рис. 49. Проверка связи

Режим администрирования (Administration Status)

Настраиваемые опции: Enable/Disable (Включено/Выключено)

Значение по умолчанию: Enable (Включено)

Описание: Включение данной функции возможно только на портах с включенным режимом кольцевого резервирования.



Если одноранговое устройство не поддерживает эту функцию, функция должна быть отключена на подключенном порту локального устройства.

Режим работы (Run Status)

Режим работы: Normal Link/Receive Fault/Disable/Send Fault (Нет ошибок/Прием ошибок/Выключено/Передача ошибок)

Описание: Если функция «Проверка связи» включена на резервном порту, и порт нормально посылает и получает данные, в статусе указывается «Normal Link» (Нет ошибок). Если одноранговый узел не получает пакеты, отображается сообщение «Send Fault» (Передача ошибок). Если устройство не принимает пакеты от однорангового узла, статусе указывается «Receive Fault» (Прием ошибок). Если функция «Проверка связи» не включена на порту, отображается сообщение «Disable» (Выключено).

6.7. Статическая многоадресная таблица (FDB)

6.7.1. Введение

Вы можете настраивать таблицы адресов статических многоадресных рассылок. Запись добавляется в таблицу адресов многоадресной рассылки в формате {multicast MAC address, VLAN ID, multicast member port}. При приеме многоадресных сообщений коммутатор ищет в таблице соответствующий порт участник, к которому будут перенаправлены пакеты.

Устройство поддерживает до 256 записей многоадресной рассылки.

6.7.2. Настройка через WEB-интерфейс

1. Включение статической многоадресной таблицы.

The screenshot shows two configuration fields. The first field is labeled 'Multicast Filtrate Mode' and has a dropdown menu set to 'transmit unknown'. The second field is labeled 'FDB Multicast Status' and has a dropdown menu set to 'Enable'. Below these fields is an 'Apply' button.

Рис. 50. Статическая многоадресная таблица

Настройка режима фильтрации (Multicast Filtrate Mode)

Настраиваемые варианты: transmit unknown/drop unknown (передавать неопознанные пакеты / отбрасывать неопознанные пакеты)

Значение по умолчанию: transmit unknown (передавать неопознанные пакеты)

Описание: Настройка процессингового режима для неопознанных пакетов многоадресной рассылки. Неопознанные пакеты многоадресной рассылки – это пакеты, которые не были добавлены вручную или не опознаны посредством IMGP Snooping и GMRP.



Передача неопознанных пакетов означает, что неопознанные пакеты многоадресной рассылки передаются в соответствующих VLAN; сброс неопознанных пакетов означает, что неизвестные многоадресные пакеты будут забракованы.

Статус FDB (FDB Multicast Status)

Настраиваемые варианты: Enable/Disable (Включить/Выключить)

Значение по умолчанию: Disable (Выключено)

Описание: Включение/Выключение статической многоадресной таблицы. Статическая многоадресная рассылка и IGMP Snooping не могут быть включены одновременно.

2. Добавление статической многоадресной записи

Static FDB Multicast List Configuration

MAC	010101010101	
VLAN ID	1	(1-4093)

Port List

Member Port List		Source Port List
<ul style="list-style-type: none"> FE1 FE2 FE3 	<< >>	<ul style="list-style-type: none"> FE4 FE5 FE6 FE7 FE8 FE9 FE10 FE11 FE12 FE13

Apply
Cancel

Рис. 51. Добавление записей в статическую многоадресную таблицу

MAC адрес (MAC)

Настраиваемый формат: HH-HH-HH-HH-HH-HH (H – шестнадцатеричное число);

Описание: Настройка группового адреса группы. Самый младший бит старшего байта равен 1.

Идентификатор VLAN (VLAN ID)

Настраиваемые опции: все созданные VLAN ID;

Описание: Настройка идентификатора VLAN записей статической многоадресной рассылки. Только порты участники VLAN могут пересылать пакеты многоадресной рассылки.

Список портов участников (Member Port List)

Описание: Выбор портов участников многоадресной рассылки. Если хост, подключенный к порту, хочет получить пакеты адресов многоадресной рассылки, необходимо настроить порт как порт участник адресов многоадресной рассылки.



3. Просмотр, изменение и удаление статических записей многоадресной рассылки.

Static FDB Multicast List

Index	MAC	VLAN ID	Member Port
<input type="radio"/>	03-01-01-01-01-01	2	FE4 FE5
<input type="radio"/>	01-01-01-01-01-01	1	FE1 FE2 FE3

Рис. 52. Операции с записями статической многоадресной группы

В списке записей статической многоадресной рассылки отображаются MAC адрес, идентификатор (ID) VLAN и порты участники. Выберите запись, нажмите <Delete> для удаления записи; нажмите <Modify> для изменения портов участников записи.

6.8. IGMP Snooping

6.8.1. Введение

Internet Group Management Protocol Snooping (IGMP Snooping) - многоадресный протокол второго уровня, работающий на уровне канала передачи данных. Он используется для управления и настройки многоадресных групп передачи данных. Коммутаторы с поддержкой IGMP Snooping анализируют принимаемые IGMP пакеты, устанавливают соответствие между портами и MAC-адресами многоадресной рассылки и отправляют многоадресные сообщения согласно этим соответствиям.

6.8.2. Концепция

- Мастер запросов: периодически отправляет IGMP запросы для проверки и обновления информации о многоадресных группах чтобы узнать активны ли они и обеспечить поддержку групповой передачи. Если в сети присутствует несколько мастеров запросов, они автоматически определяют одного (с наименьшим IP адресом), который непосредственно и будет осуществлять запросы, остальные будут только получать и передавать IGMP запросы.
- Маршрутизирующий порт: получает запросы (на IGMP-коммутаторе) от мастера. 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 членами многоадресных групп путём обмена пакетами между поддерживающих IGMP устройств. Данные запросы содержат следующие важные сообщения:

- Сообщение с общим запросом: Мастер запросов периодически отправляет общие запросы (с фиксированным IP адресом назначения: 224.0.0.1) для уточнения, есть ли у многоадресной группы порты участники группы. При получении запроса,



устройство, не являющееся мастером запросов, ретранслирует пакет на все свои порты.

- Сообщение с конкретным запросом: Если устройство хочет покинуть многоадресную группу, оно отправляет пакет "IGMP leave". После получения такого пакета, мастер запросов отправляет пакет конкретного запроса (с IP адресом назначения, соответствующим IP адресу многоадресной группы) для подтверждения того, что у коммутатора остались какие-либо порты участники данной группы.
- Сообщение с отчетом участника группы: Если устройство хочет получать определенные данные многоадресной группы, оно отправляет пакет IGMP оповещения (с IP адресом назначения, соответствующим IP адресу многоадресной группы, к которой устройство планирует присоединиться) в ответ на IGMP запрос группы.
- Пакет "IGMP leave": Если устройство хочет покинуть многоадресную группу, оно отправляет пакет "IGMP leave" (с фиксированным IP адресом назначения: 224.0.0.2).

6.8.4. Настройка через WEB-интерфейс

1. Включите протокол IGMP Snooping, включите или выключите режим автоматического запроса.



Рис. 53. Включение IMGP Snooping

Настройка IGMP Snooping (IGMP Snooping Status)

Настраиваемые опции: Enable/Disable (Включено/Выключено)

Значение по умолчанию: Disable (Выключено)

Описание: Включение или выключение функции IGMP Snooping. IGMP Snooping и GMRP не могут быть включены одновременно.

Настройка автоматического запроса (Auto Query Status)

Настраиваемые опции: Enable/Disable (Включено/Выключено)

Значение по умолчанию: Disable (Выключено)

Описание: Включение или выключение функции запросов. Если функция выключена, коммутатор не имеет возможности посылать автоматические запросы. Данную функцию можно включить только при включенной функции IGMP Snooping.



По крайней мере, хотя бы на одном коммутаторе должна быть включена функция автоматического запроса.



Настройка перекрестного IGMP (IGMP Cross Status)

Настраиваемые опции: Enable/Disable (Включено/Выключено)

Значение по умолчанию: Disable (Выключено)

Описание: Если функция включена, отчеты и оставшиеся пакеты могут быть перенаправлены портами Sy2-Ring.

2. Отображение списка участников многоадресной рассылки.

MAC	VLAN ID	Member
01-00-5E-7F-FF-FE	1	FE1
01-00-5E-00-01-01	1	FE1
01-00-5E-26-4C-DA	1	FE1
01-00-5E-51-09-08	1	FE1
01-00-5E-0A-18-03	1	FE1
01-00-5E-7F-FF-FA	1	FE1

Рис. 54. Отображение списка участников IGMP Snooping

Список участников IGMP (IGMP Member List)

Отображение групп: {MAC address, VLAN ID, Member Port} (MAC адрес, идентификатор VLAN, участник группы).

Описание: отображает таблицу адресов многоадресной рассылки FDB с включенной функцией IGMP Snooping. Идентификатор VLAN – это идентификатор участника группы.

6.8.5. Пример типовой настройки

Как показано на рис. 55, функция IGMP Snooping включена на коммутаторах 1, 2, 3. На коммутаторах 2 и 3 включена функция автоматического запроса. IP адрес коммутатора 2: 192.168.1.2; IP адрес коммутатора 3: 192.168.0.2, соответственно коммутатор 3 выбран в качестве генератора запросов.

1. Включите функцию IGMP Snooping на коммутаторе 1.
2. Включите функции IGMP Snooping и автоматического запроса на коммутаторе 2.
3. Включите функции IGMP Snooping и автоматического запроса на коммутаторе 3.



Рис. 55. Пример типовой настройки IGMP Snooping



- Т.к. коммутатор 3 является генератором запросов, он будет периодически отправлять сообщение с общим запросом, а порт 4 коммутатора 2 будет принимать это сообщение, соответственно данный порт будет выбран как маршрутизирующий порт. Далее сообщение с запросом будет перенаправлено из порта 3 коммутатора 2 в порт 2 коммутатора 1, который получив это сообщение будет назначен маршрутизирующим портом.
- Когда PC 1 подключается к многоадресной группе 225.1.1.1, он должен будет отправить сообщение с отчетом участника многоадресной группы коммутатору 1, соответственно порт 1 и маршрутизирующий порт 2 коммутатора 1 будут подключены к многоадресной группе 225.1.1.1; затем сообщение с отчетом IMGP будет перенаправлено к коммутатору 2 через маршрутизирующий порт 2, соответственно порты 3 и 4 коммутатора 2 также будут подключены к многоадресной группе 225.1.1.1; далее сообщение с отчетом IMGP будет перенаправлено к коммутатору 3 через маршрутизирующий порт 4, соответственно порт 5 коммутатора 3 также будет включен в многоадресную группу 225.1.1.1.
- Как только данные от многоадресного сервера достигнут коммутатора 1, они будут перенаправлены к PC 1 посредством порта 1; т.к. маршрутизирующий порт 2 также является участником многоадресной группы, данные многоадресной передачи им также будут перенаправлены. Таким образом, когда данные достигнут порта 5 коммутатора 3, пересылка остановится, т.к. отсутствует принимающая сторона. Но, если PC 2 также является участником 225.1.1.1, к нему также будут перенаправлены данные многоадресной рассылки.

6.9. Протокол ACL

6.9.1. Введение

С помощью функции ACL (Access Control List, Список контроля доступа) коммутатор фильтрует принятые пакеты в соответствии с согласованными правилами, определенными в ACL, предотвращая доступ неавторизованных пользователей и обеспечивая сохранение сетевых ресурсов.

6.9.2. Настройка через WEB-интерфейс

1. Настройка режима ACL для соответствующих портов



Set Port ACL

Port	Mode
FE1	Accept
FE2	Reject
FE3	None
FE4	None
FE5	None
FE6	None
FE7	None
FE8	None
FE9	None
FE10	None
FE11	None
FE12	None
FE13	None
FE14	None
FE15	None
FE16	None
FX17	None
FX18	None
FX19	None
FX20	None

Apply

Рис. 56. Пример типовой настройки IGMP Snooping

Настройка режима (Mode)

Настраиваемые опции: None/Accept/Reject (Выключено/Принять/Отказать)

Значение по умолчанию: None (Выключено)

Описание: Настройка режима ACL, т.е. режима обработки согласованных пакетов.

2. Настройка параметров для записей ACL

Set Port ACL MAC

Port	Configure MAC
FE1	000000010101

Apply

Рис. 57. Настройка записей ACL

Настройка порта (Port)

Настраиваемые опции: Все порты коммутатора

Описание: Настройка портов, на которых будет включен протокол ACL.

Настройка MAC адреса (Configure MAC)

Настраиваемый формат: {NNNNNNNNNN} (N – шестнадцатеричное число)



Описание: Настройка MAC адреса источника для записей протокола ACL. Принимаемый пакет соответствует записи, если исходный MAC адрес пакета идентичен настроенному в данном разделе MAC адресу. Каждый порт поддерживает не более 24-х записей ACL.

3. Отображение записей ACL

Port ACL MAC List

Index	Port	MAC
<input type="radio"/>	FE1	02-00-00-00-00-01
<input type="radio"/>	FE1	00-00-00-01-01-01

Рис. 58. Просмотр записей ACL

Отметьте соответствующую запись ACL (см. рис. 58). Вы можете удалить эту запись.

6.9.3. Пример типовой настройки

Порт 1 принимает только пакеты, для которых MAC адрес источника 00-00-00-01-01-01.

Шаги настройки:

1. Настройте для порта 1 режим ACL как «Ассерт» (см. рис. 56).
2. Настройте MAC адрес источника записи ACL для порта 1 как 00-00-00-01-01-01 (см. рис. 57).

6.10. Протокол разрешения адресов (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 определять соответствие между IP адресом и MAC адресом других устройств в сети. Также, коммутаторы поддерживают статические ARP записи, связывающие IP адреса и MAC адреса. Динамические ARP записи периодически устаревают, что обеспечивает обновление информации.

Данные серии коммутаторов поддерживает не только коммутацию на 2 уровне, но и функцию ARP, которая обеспечивает получение информации о IP адресах других устройств, находящихся в одном сегменте сети с коммутаторами, а также взаимодействия с системой управления сетью и другими управляемыми устройствами.

6.10.2. Описание

ARP записи делятся на статические и динамические.

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

Статические записи вводятся вручную, и также вручную поддерживаются. Они не устаревают и не перезаписываются динамическими записями.



Коммутаторы поддерживают до 512 ARP записей (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 жизни (действия, aging time) ARP:

ARP Aging Time

ARP Aging Time	20	(10-60min)
----------------	----	------------

Apply

Рис. 59. Настройка времени жизни ARP

Время жизни ARP (ARP Aging Time):

Настраиваемый диапазон: 10~60 мин.

Значение по умолчанию: 20 мин.

Описание: настройка время жизни (действия, aging time) ARP. Время старта ARP начинается после добавления динамической записи ARP в таблицу адресов. Когда время закончится, эта динамическая запись будет удалена из таблицы.

2. Настройка статического адреса в записи ARP:

ARP address

IP address	192.168.0.41
MAC address	020202020202

Apply

Рис. 60. Настройка статического адреса в ARP

Адрес ARP (ARP address):

Групповая настройка: {IP address, MAC address} (IP адрес, MAC адрес).

Формат: {A.B.C.D, HH-HH-HH-HH-HH-HH}. (H – шестнадцатеричный номер)

Описание: Настройка статического адреса в ARP.



- IP адрес, назначаемый для статической записи ARP, должен находиться с коммутатором в одном и том же сегменте сети.
- Когда IP адрес коммутатора назначен в статической записи ARP, система будет автоматически передавать MAC адрес коммутатора.
- Как правило, коммутатор может автоматически обнаруживать записи ARP без необходимости настройки статической записи администратором.



3. Отображение или удаление адреса в записи ARP:

ARP address

Number	IP address	MAC address	Flags
<input type="radio"/>	192.168.0.2	00-00-00-00-00-02	Dynamic
<input type="radio"/>	192.168.0.41	02-02-02-02-02-02	Static
<input type="radio"/>	192.168.0.200	00-0E-CD-18-50-33	Dynamic
<input type="radio"/>	192.168.0.217	90-FB-A6-3C-CA-7E	Dynamic

Рис. 61. Таблица адресов в ARP

Адрес ARP:

Групповое отображение: {IP address, MAC address, Flags} (IP адрес, MAC адрес, Флаги).

Функция: отображение статических и динамических записей ARP.

Действие: Выберите статическую запись и нажмите <Delete> для удаления данной записи.



Запись динамического ARP не может быть удалена.

6.11. Протокол SNMP

6.11.1. Введение

Simple Network Management Protocol (SNMP) - протокол управления сетевыми устройствами с использованием протокола 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» (станция/агент). Таким образом, по функциональности он включает две составляющие: «NMS» и «Агент».

- Network Management Station (NMS) - это рабочая станция, на которой работает SNMP-приложение для управления сетью клиентов, играющая основную роль в управлении сетью с помощью протокола SNMP.
- Агент - это программный процесс на управляемом устройстве. Он отвечает за прием и обработку запросов от NMS. При возникновении аварийной ситуации агент автоматически информирует об этом NMS.

NMS является средством управления сетью SNMP, соответственно Агент управляется сетью SNMP. Обмен информацией управления между NMS и Агентом осуществляется через SNMP. Протокол SNMP обеспечивает выполнение 5 основных операций:

- 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 тревоги агент автоматически отправит сообщение «Trap» в NMS, чтобы сообщить о возникновении аномальных событий.

6.11.3. Описание

Данные серии коммутаторов поддерживают версию SNMPv2. При этом SNMPv2 совместим с SNMPv1.

SNMPv1 использует принцип аутентификации по имени сообщества (Community Name Authentication). Имя сообщества работает как пароль и используется для ограничения доступа Агента SNMP к SNMP NMS. Если имя сообщества SNMP-сообщения не может пройти аутентификацию устройства, отправленное сообщение будет удалено.

SNMPv2 также использует аутентификацию по имени сообщества. Он не просто совместим с SNMPv1, но и расширяет функции SNMPv1. Корректная совместная работа NMS и Агента основывается на согласованной версии SNMP. Агент может быть настроен для работы с несколькими версиями одновременно и использовать разные версии для связи с разными NMS.

6.11.4. Описание MIB (Management Information Base)

Любой управляемый ресурс можно рассматривать как объект, соответственно он называется управляемым объектом.

MIB (Management Information Base) - это совокупность всех управляемых объектов. MIB определяет иерархические отношения между управляемыми объектами и определяет основные атрибуты объектов, например, имя объекта, права доступа, типы данных и т.д. У каждого Агента есть своя MIB. NMS может читать или записывать объекты в MIB в соответствии со своими правами. Связь NMS, Агента и MIB показана на рисунке 156.

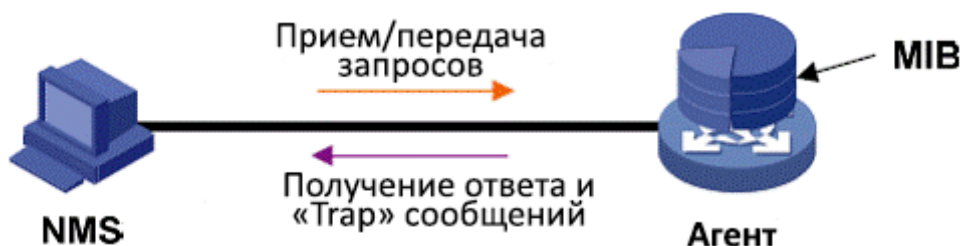


Рис. 62. Взаимосвязь NMS, Агента и базы MIB

MIB определяет древовидную структуру, где каждый узел дерева является управляемым объектом. Каждый узел дерева содержит OID (Идентификатор объекта), который может указывать позицию узла в структуре дерева MIB. OID управляемого объекта А равен 1.2.1.1 (см. рис. 157).

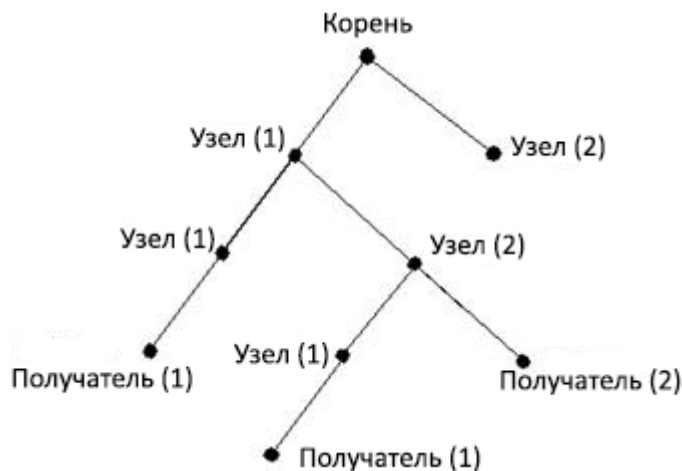


Рис. 63. Структура дерева MIB

6.11.5. Настройка через WEB-интерфейс

1. Включение протокола SNMP

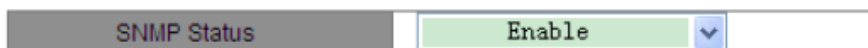


Рис. 64. Включение протокола SNMP

Статус SNMP (SNMP Status)

Настраиваемые опции: Enable/Disable (Включить/Выключить)

Значение по умолчанию: Enable (Включено)

Описание: Включение/Выключение протокола SNMP.

2. Настройка прав доступа

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

Рис. 65. Настройка прав доступа

Сообщество «Только чтение» (Read-Only Community)

Настраиваемый диапазон: 3~16 символов

Значение по умолчанию: Public (Открытый)

Описание: NMS может только читать информацию MIB, если имя сообщества, переданное в сообщении SNMP, отправленном из NMS, совпадает с именем сообщества, установленным здесь.

Сообщество «Чтение/Запись» (Read-Write Community)

Настраиваемый диапазон: 3~16 символов



Значение по умолчанию: Private (Персональный)

Описание: NMS может и читать и записывать информацию MIB, если имя сообщества, переданное в сообщении SNMP, отправленным из NMS, совпадает с именем сообщества, установленным здесь.

Порт запроса (Request Port)

Настраиваемый диапазон: 1~65535

Значение по умолчанию: 161

Описание: Настройка порта, который принимает запросы SNMP.

3. Настройка параметров передачи сообщений «Trap».

Trap Settings	
Trap on-off	Enable <input type="button" value="v"/>
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)

Рис. 66. Настройка «Trap»

Включение/Выключение сообщений «Trap» (Trap on-off)

Настраиваемые опции: Enable/Disable (Включить/Выключить)

Значение по умолчанию: Enable (Включено)

Описание: Включение/Выключение функции отправки коммутатором сообщений «Trap».

Настройка идентификатора порта для отправки сообщений «Trap» (Trap Port ID)

Настраиваемый диапазон: 3~65535

Значение по умолчанию: 162

Описание: Настройка идентификатора порта, передающего сообщения «Trap».

IP адрес сервера (Server IP Address)

Настраиваемый формат: A.B.C.D

Описание: Настройка IP адреса сервера, который будет получать сообщения «Trap». Максимально поддерживается до пяти (5) IP адресов.

4. Отображение IP адресов сервера управления.

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

Рис. 67. IP адрес сервера управления



Нет необходимости вручную устанавливать IP адреса сервера. Они будут автоматически отображаться в процессе загрузки на сервере программного обеспечения управления сетью и в информации о модуле MIB на устройстве с функцией чтение/запись.

6.11.6. Пример типовой настройки

NMS с SNMP подключается к коммутатору через сеть Ethernet. IP адрес NMS: 192.168.1.23, а IP адрес коммутатора: 192.168.1.2. NMS управляет и контролирует Агента с помощью протокола SNMPv2, который может читать и записывать информацию MIB Агента, а Агент автоматически отправляет сообщения «Trap» в NMS, когда у Агента происходит аварийная ситуация (см. рис. 68).

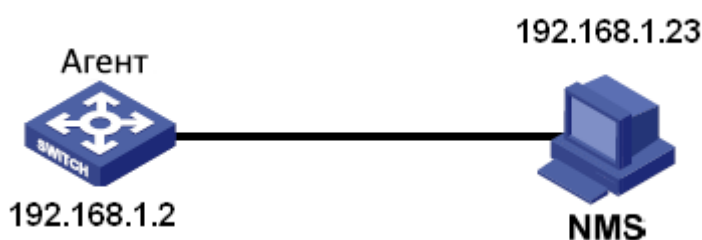


Рис. 68. Пример настройки SNMPv2

Настройка Агента:

1. Включите протокол SNMP (см. рис. 64).
2. Настройте права доступа для имени сообщества «Read-Only» как «public», а для имени сообщества «Read-Write» установите значение «private»; порту запроса присвойте значение 161 (см. рис. 65).
3. Включите режим «Trap», идентификатору порта с включенным режимом «Trap» должно быть присвоено значение 162, IP адресу сервера: 192.168.1.23 (см. рис. 66).

Если пользователю необходимо контролировать статус Агента, необходимо использовать соответствующее программное обеспечение, например, Symanitron NMS.

6.12. Sy2-Ring

6.12.1. Введение

Sy2-Ring и Sy2-Ring+ - проприетарные протоколы резервирования компании Symanitron. Они позволяют сети восстанавливаться менее чем за 50мс при сбое связи, обеспечивая надёжное и стабильное соединение.

Sy2-Ring бывают двух типов: кольцо, основанное на конфигурации по портам (Sy2-Port-Ring), и кольцо, основанное на конфигурации по VLAN (Sy2-VLAN-Ring):

- Sy2-Port-Ring: определяет порт, через который необходимо передавать или блокировать пакеты данных.
- Sy2-VLAN-Ring: определяет через который необходимо передавать или блокировать пакеты данных по определённому VLAN. Это позволяет настраивать несколько колец на одном порту, относящихся к разным VLAN.

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



6.12.2. Концепция

Концептуально протоколы работают следующим образом:

- Мастер-узел (Master station): кольцо может иметь только один мастер-узел. Мастер-узел отправляет пакеты Sy2-Ring и следит за текущим статусом кольца.
- Мастер-порт (Master port): первый порт, чье состояние на мастер-узле меняется на рабочее, называется мастер-порт. Он находится в режиме пересылки пакетов.
- Ведомый порт (Slave port): это порт на мастер-узле, чье состояние меняется на рабочее позже мастер-порта. Когда кольцо замкнуто, ведомый порт находится в режиме отбрасывания пакетов. Если кольцо разомкнуто, например, из-за обрыва связи или выхода из строя порта, статус ведомого порта меняется на режим пересылки пакетов.
- Ведомый узел (Slave station): кольцо может иметь множество ведомых узлов. Ведомые узлы ждут Sy2-Ring пакетов и оповещают мастер-узел о неисправностях.
- Резервный порт (Backup port): Порт для связи между SY2 кольцами называется резервным портом.
- Резервный мастер-порт (Master Backup Port): если в кольце имеется два резервных порта, резервный порт с наибольшим MAC-адресом будет резервным мастер-портом. Порт находится в состоянии пересылки пакетов.
- Резервный ведомый порт (Slave Backup Port): если в кольце два резервных порта, резервный порт с наименьшим MAC адресом будет резервным ведомым портом. Он находится в режиме отбрасывания пакетов.
- Режим перенаправления пакетов (Forwarding state): если порт находится в режиме пересылки пакетов, он может передавать и получать данные.
- Режим отбрасывания (Blocking state): если порт находится в режиме отбрасывания пакетов, он может только принимать данные, но не может их передавать.

6.12.3. Реализация

1. Реализация протокола Sy2-Ring

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

Если кольцо замкнуто, мастер-порт на мастер-узле находится в режиме пересылки пакетов, а резервный порт в режиме отбрасывания пакетов; все кольцевые порты запасных узлов находятся в состоянии пересылки пакетов.

Кольцо может быть разомкнуто в следующих случаях:

- Мастер-порт мастер-узла вышел из строя. Ведомый порт мастер-узла и все кольцевые порты ведомых узлов в этом случае переходят в режим пересылки пакетов.
- Ведомый порт мастер-узла вышел из строя. Мастер-порт на мастер-узле и все кольцевые порты ведомых узлов переходят в режим пересылки пакетов.
- Другие порты вышли из строя или неисправно соединение между ними. Оба порта мастер-узла и все кольцевые порты ведомых узлов переходят в режим пересылки пакетов.

Настройки Sy2-Ring должны соответствовать следующим условиям:

- Все коммутаторы одного кольца должны иметь одинаковый номер домена.



- Каждое кольцо может иметь только один мастер-узел, но множество ведомых узлов.
- Только два порта каждого коммутатора могут быть в кольце.
- Для двух объединенных колец резервные порты могут быть настроены только в одном кольце.
- В одном кольце можно настроить максимум два резервных порта.
- На коммутаторе может быть только один резервный порт для одного кольца.
- Sy2-Port-Ring и Sy2-VLAN-Ring не могут настроены в одном коммутаторе одновременно.

Как показано на рисунке ниже, рабочие процессы коммутаторов А, В, С и D будут следующими:

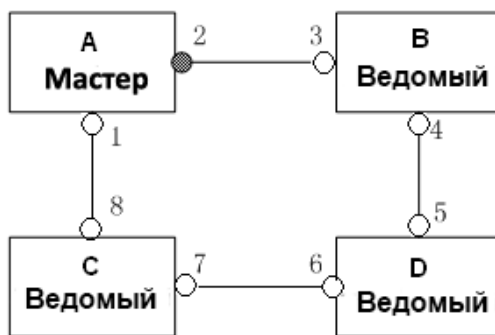


Рис. 69. Топология Sy2-Ring

1. Настройте коммутатор А как мастер-узел, а другие коммутаторы как ведомые узлы.
2. Порт 1 будет первым портом мастер-узла, у которого состояние связи изменяется на «включено» и он находится в состоянии пересылки. Порт 2 в данном случае находится в состоянии блокировки. Два кольцевых порта каждого ведомого узла находятся в состоянии пересылки.
3. В случае обрыва связи между коммутаторами С и D, статус порта 2 коммутатора А будет изменен и будет находиться в состоянии пересылки, а порты 6 и 7 будут находиться в состоянии блокировки (см. рис. 51).

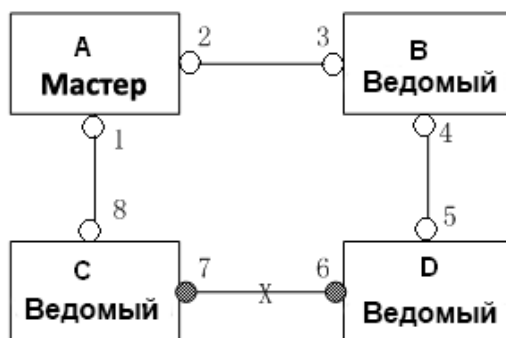


Рис. 70. Обрыв соединения Sy2-Ring



Изменение статуса канала влияет на состояние кольцевых портов.



2. Реализация протокола Sy2-Ring+

Протокол Sy2-Ring+ обеспечивает резервирование для двух колец Sy2-Ring. По одному резервному порту настроено на коммутаторе С и коммутаторе D соответственно. Какой порт будет резервным мастер-портом, зависит от MAC-адресов двух портов. Если резервный мастер-порт выходит из строя, его место займёт один из резервных ведомых портов, предотвращая возникновение колец и обеспечивая резервную связь между кольцами.

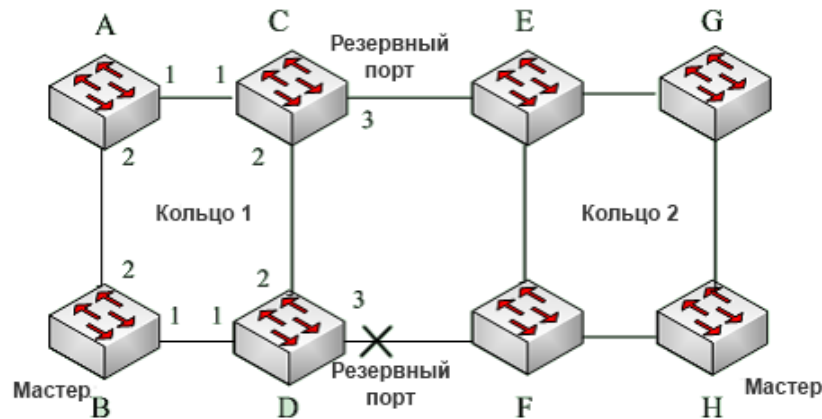


Рис. 71. Топология Sy2-Ring+

3. Реализация протокола Sy2-VLAN-Ring

Протокол Sy2-VLAN-Ring дает возможность данным разных VLAN быть переданными различными путями. Каждый путь пересылки для VLAN формируется посредством Sy2-VLAN-Ring. Разные Sy2-VLAN-Ring могут иметь разные мастер-узлы. На рис. 53 показана конфигурация двух Sy2-VLAN-Ring.

Линии связи кольца DT-VLAN-Ring10: AB-BC-CD-DE-EA.

Линии связи кольца DT-VLAN-Ring20: FB-BC-CD-DE-EF.

Два кольца соприкасаются связями BC, CD, DE. Коммутаторы С и D используют одни и те же порты в двух кольцах, но при этом используют разные логические связи, которые основаны на VLAN.

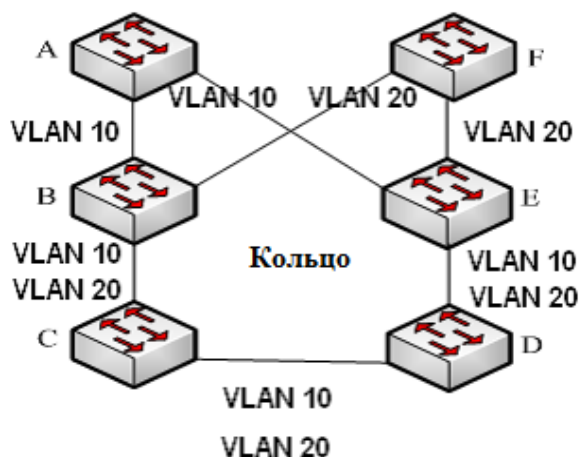


Рис. 72. Sy2-VLAN-Ring



6.12.4. Настройка через WEB-интерфейс

1. Настройка режима резервирования и определения статуса кольца.

Рис. 73. Настройка режима резервирования

Настройка режима резервирования (Select Redundancy Mode)

Настраиваемые значения: Sy2-RING-PORT/Sy2-VLAN-RING

Значение по умолчанию: Sy2-RING-PORT

Функция: Выбор режима резервирования.

Проверка статуса петли (Check Loop Status)

Настраиваемые опции: Enable/Disable (Включить/Выключить)

Значение по умолчанию: Disable (Выключено)

Функция: Включение и выключение определения статуса кольца. После включения определения статуса кольца коммутатор автоматически определяет статус кольца. Когда не кольцевой порт принимает пакеты Sy-Ring, порт будет заблокирован. Поэтому используйте эту функцию с осторожностью.

2. Создание кольца Sy2-Ring.

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

Рис. 74. Создание кольца Sy2-Ring

Нажмите <Add> для создания кольца Sy2-Ring.



3. Настройка Sy2-Ring-Port и Sy2-VLAN-Ring

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="FE1"/> ▼	
Ring Port2	<input type="text" value="FE2"/> ▼	

SY2-RING+		
SY2-RING+	<input type="text" value="Enable"/> ▼	
Backup Port	<input type="text" value="FE3"/> ▼	

Apply
Cancel

Рис. 75. Настройка Sy2-Ring-Port

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="FE1"/> ▼	
Ring Port2	<input type="text" value="FE2"/> ▼	

SY2-RING+		
SY2-RING+	<input type="text" value="Enable"/> ▼	
Backup Port	<input type="text" value="FE3"/> ▼	

Add VLAN List		
VLAN Choose	VLAN ID	VLAN Name
<input checked="" type="checkbox"/>	1	default
<input checked="" type="checkbox"/>	2	vlan

Apply
Cancel

Рис. 76. Настройка Sy2-VLAN-Ring

Резервирование (Redundancy)

Принудительное значение: Sy2-Ring

Идентификатор домена (Domain ID)

Диапазон значений: 1~32

Описание: Идентификатор домена используется для разграничения колец. Один коммутатор поддерживает до 16 колец, определяемых по портам и до 8 колец, определяемых по VLAN.

Имя домена (Domain name)

Диапазон значений: 1~31 символов



Описание: Назначение доменного имени.

Тип узла (Station Type)

Настраиваемые значения: Master/Slave (Мастер/Ведомый)

По умолчанию: Master (Мастер)

Описание: Выбор роли коммутатора в кольце.

Кольцевой порт 1/Кольцевой порт 2 (Ring Port1/Ring Port2)

Настраиваемые значения: все порты коммутатора

Описание: Выбор двух кольцевых портов.

Sy2-Ring+

Настраиваемые значения: Enable/Disable (Включить/Выключить)

Значение по умолчанию: Disable (Выключен)

Функция: Включение/выключение протокола Sy2-Ring+.

Резервный Порт (Backup Port)

Настраиваемые значения: все порты коммутатора

Функция: Настройка одного порта в качестве резервного. Вы можете настроить резервный порт только после включения функции Sy2-Ring+.

Добавление списка VLAN (Add VLAN List)

Настраиваемые значения: Список всех созданных VLAN (All created VLAN lists)

Функция: Выбор VLAN, чьи пакеты могут быть переданы через текущий кольцевой порт.

После того, как настройка завершена, кольца созданы, вы можете посмотреть информацию о Sy2-Ring:

SY2-RING List

Domain ID	Station Type	Ring Port(1,2)	SY2-RING+ Status	Backup Port	Change times
a-1	master	FE1,FE2	Enable	FE3	0
b-2	slave	FE4,FE5	Enable	FE6	0

Add

Рис. 77. Список Sy2-Ring



- В транковую группу нельзя добавить кольцевой или резервный порт. Порт, добавленный в транковую группу, не может быть настроен как кольцевой или резервный порт.
- Кольцевой или резервный порт не могут быть настроены в качестве источника зеркалирования или порта назначения. Источник зеркалирования или порт назначения не могут быть настроены как кольцевой или резервный порт.
- Протокол STP не может быть включен на кольцевом или резервном порту. Порт, с включенным протоколом STP не может быть настроен как кольцевой или резервный порт.



4. Просмотр и модификация настроек Sy2-Ring

Нажмите запись Sy2-Ring (см. рис. 77) для отображения или изменения настроек кольца (см. рис. 78):

SY2-RING Configuration

Redundancy	DT-RING
Domain ID	1
Domain Name	a
Station Type	master
Ring Port1	FE1
Ring Port2	FE2
SY2-RING+	Enable
Backup Port	FE3

Рис. 78. Просмотр и модификация настроек Sy2-Ring

После завершения изменений нажмите <Apply>, чтобы изменения вступили в силу. Вы можете удалить настройки Sy-Ring, нажав на кнопку <Delete>.

5. Просмотр статуса Sy2-Ring и портов:

SY2-RING State List

Redundancy	SY2-RING
Ring Port 1	forwarding
Ring Port 2	blocking
Ring State	RING-CLOSE
Clean Change times	CLEAN

Redundancy	SY2-RING+
Equipment IP	192.168.0.222
Equipment MAC	00-15-7E-0A-40-80
Backup Port Status	blocking
Equipment IP	192.168.0.223
Equipment MAC	00-80-CD-11-01-B1
Backup Port Status	blocking

Рис. 79. Просмотр статуса Sy-Ring



6.12.5. Пример типовой настройки

Как показано на рисунке 71, коммутаторы А, В, С, D формируют кольцо 1; коммутаторы Е, F, G, H формируют кольцо 2; связи СЕ и DF являются резервными для колец 1 и 2.

Настройка коммутатора А:

1. Домен: 1; Имя домена: Ring; Тип узла: Slave; Кольцевые порты: 1 и 2; Sy-Ring: Disable; Резервный порт: none, как показано на рис. 75.

Настройка коммутатора В:

2. Домен: 1; Имя домена: Ring; Тип узла: Master; Кольцевые порты: 1 и 2; основной порт: no; Sy-Ring: Disable; Резервный порт: none, как показано на рис. 75.

Настройка коммутаторов С и D:

3. Домен: 1; Имя домена: Ring; Тип узла: Slave; Кольцевые порты: 1 и 2; Sy-Ring: Enable; Резервный порт: 3, как показано на рис. 75.

Настройка коммутаторов Е, F и G:

4. Домен: 2; Имя домена: Ring; Тип узла: Slave; Кольцевые порты: 1 и 2; Sy-Ring: Disable; Резервный порт: none, как показано на рис. 75.

Настройка коммутатора H:

5. Домен: 2; Имя домена: Ring; Тип узла: Master; Кольцевые порты: 1 и 2; основной порт: no; Sy-Ring: Disable; Резервный порт: none, как показано на рис. 75.

6.13. STP/RSTP

6.13.1. Описание

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. 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 порт/порт назначения выходит из строя, его альтернативный порт/резервный порт немедленно переходит в состояние пересылки.

6.13.2. Концепция

- Корневой мост (Root bridge): является "корнем дерева". Сеть может иметь только один корневой мост. Какой из коммутаторов будет корневым зависит от сетевой топологии и данная ситуация может измениться при изменении топологии сети. Для определения сетевой целостности, корневой коммутатор периодически отправляет BPDU другим узлам, которые пересылают их дальше, чтобы гарантировать стабильность 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 корневых портов нет.
- Порт назначения (Designated port): порт на мосту назначения, который отвечает за пересылку конфигурации BPDU другому устройству или локальной сети. Все порты в корневом мосту являются портами назначения.
- 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 порта назначения. Когда порт назначения выходит из строя, резервный порт становится новым портом назначения и передаёт данные вместо него.

6.13.3. Настройка BPDU

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

Структура данных BPDU:

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

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 Моста назначения (Designated bridge ID): приоритет коммутатора назначения (2 байт) + MAC-адрес моста назначения (6 байт).

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

Возраст сообщения (Message age): как далеко BPDU может быть передан по сети.

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

Hello интервал (Hello time): интервал для отправки BPDU.

Задержка отправки (Forward delay): задержка изменения статуса (отбрасывание--изучение--пересылка).

6.13.4. Реализация

Процесс вычисления логического дерева посредством сообщения BPDU:



1. Начальная стадия: все устройства на всех своих портах генерируют BPDU, считая себя корневым мостом; ID корневого моста – это ID устройства; стоимость пути до корневого коммутатора равна 0; ID моста назначения – это ID устройства, порт назначения – локальный порт.
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 принятые настройки BPDU, устройство не выполняет никакой обработки.
 - Если приоритет конфигурации BPDU, сгенерированный локальным портом, ниже, чем принятая конфигурация BPDU, устройство заменит содержимое BPDU конфигурации, сгенерированное локальным портом, содержимым принятой конфигурации BPDU.

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

- Конфигурация 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 до корневого коммутатора плюс стоимость пути до локального порта меньше, приоритет BPDU выше.
 - Если стоимость пути до корневого коммутатора 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 коммутатором логического дерева (spanning tree) является устройство с наименьшим идентификатором (ID) устройства.
 4. Выбор корневых портов. Некорневые коммутаторы сделают свои порты, получающие наилучшую конфигурацию BPDU, корневыми.
 5. Вычисление конфигурации BPDU порта назначения. В соответствии с конфигурацией BPDU и стоимостью пути корневого порта, конфигурация BPDU порта назначения рассчитывается для каждого порта:
 - Идентификатор корневого моста заменяется идентификатором конфигурации BPDU корневого порта.
 - Стоимость корневого пути заменяется на стоимость конфигурации BPDU корневого порта плюс соответствующая стоимость пути корневого порта.
 - ID моста назначения заменяется ID устройства.
 - ID порта назначения заменяется на ID данного порта.
 6. Выбор порта назначения. Если вычисленное значение BPDU лучше, устройство делает этот порт назначенным, заменяет BPDU порта вычисленным и отправляет новый BPDU. Если текущее значение BPDU лучше, устройство не обновляет его и блокирует порт. Заблокированные пакеты могут принимать и отправлять только техническую информацию RSTP, но не данные.

6.13.5. Настройка через WEB-интерфейс

1. Включите протокол STP/RSTP:

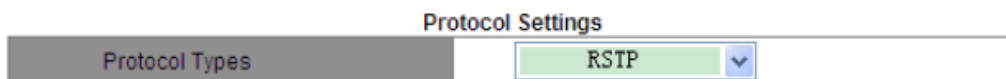


Рис. 80. Включение протокола STP/RSTP

Типы протокола

Настраиваемые опции: Disable/RSTP/STP (Выключить/RSTP/STP)

Значение по умолчанию: Выключено (Disable)

Описание: Включить или выключить протоколы RSTP или STP.

2. Настройка временных параметров сетевого моста:

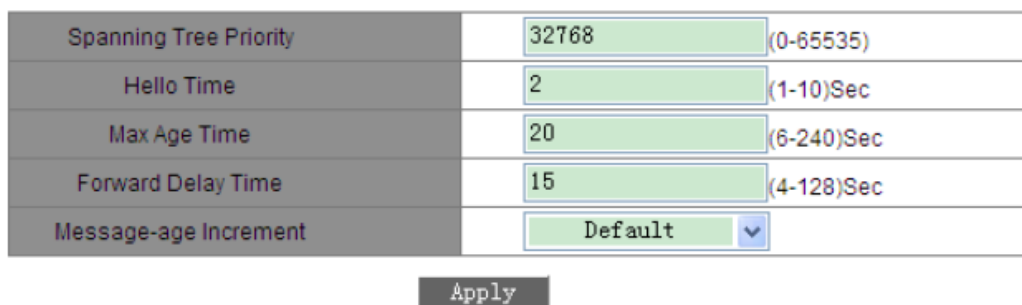


Рис. 81. Настройка временных параметров моста BPDU

Приоритет STP (Spanning Tree Priority)

Настраиваемый диапазон: 0~65535 с шагом 4096.

Значение по умолчанию: 32768

Описание: Настройка приоритета сетевого моста. Приоритет используется для выбора корневого моста. Чем меньше значение, тем выше приоритет.

Время параметра Hello (Hello Time)

Настраиваемый диапазон: 1~10 сек.

Значение по умолчанию: 2 сек.

Описание: Настройка временного интервала отправки настроек BPDU.

Максимальное время старения (Max Age Time)

Настраиваемый диапазон: 6~40 сек.

Значение по умолчанию: 20 сек.

Описание: Если значение возраста сообщения в BPDU больше указанного значения, тогда BPDU отбрасывается.

Время задержки пересылки (Forward Delay Time)

Настраиваемый диапазон: 4~128 сек.

Значение по умолчанию: 15 сек.

Описание: настройка статуса изменения времени от «Отбрасывания» до «Изучения» или от «Изучения» до «Пересылки».

Увеличение возраста сообщения (Message-age Increment)

Настраиваемые варианты: Принудительно/По умолчанию (Compulsion/Default)

Значение по умолчанию: По умолчанию (Default)



Описание: Настройка значения, которое нужно добавить в возраст сообщения, когда BPDU проходит через мост. В принудительном режиме (Compulsion) значение возраста сообщения – 1. В режиме «По умолчанию» (Default) значение возраста сообщения будет максимальным (максимальное время возраста/16, 1).

Время задержки пересылки (Forward Delay Time), максимальное время старения (Max Age Time) и время Hello (Hello Time) должны удовлетворять следующим требованиям:
 $2 \times (\text{Время задержки пересылки} - 1.0 \text{ секунда}) \geq \text{Максимальное время старения};$
 $\text{Максимальное время старения} \geq 2 \times (\text{Время Hello} + 1.0 \text{ секунда})$

3. Включение RSTP на портах:

Port Settings

Port	Protocol State	Port Priority(0~255)	Path Cost(1~200000000)	Cost Count
FE1	Enable	128	2000000	Yes
FE2	Enable	128	2000000	Yes
FE3	Enable	128	2000000	Yes
FE4	Enable	128	2000000	Yes
FE5	Disable	128	2000000	Yes
FE6	Disable	128	2000000	Yes
FE7	Disable	128	2000000	Yes
FE8	Disable	128	2000000	Yes
FE9	Disable	128	2000000	Yes
FE10	Disable	128	2000000	Yes
FE11	Disable	128	2000000	Yes
FE12	Disable	128	2000000	Yes
FE13	Disable	128	2000000	Yes
FE14	Disable	128	2000000	Yes
FE15	Disable	128	2000000	Yes
FE16	Disable	128	2000000	Yes
FX17	Disable	128	200000	Yes
FX18	Disable	128	200000	Yes
FX19	Disable	128	200000	Yes
FX20	Disable	128	200000	Yes

Apply

Рис. 82. Настройка портов

Статус протокола (Protocol Status)

Настраиваемые опции: Включить/Выключить (Enable/Disable)

Значение по умолчанию: Выключено (Disable)

Описание: Включение или Выключение STP/RSTP на портах.



- Порт, на котором настроена функция зеркалирования и порт с настройками кольцевых протоколов являются взаимоисключающими. На порту с настройками зеркалирования нельзя включить STP и наоборот.



- Транковый порт и порт с настройками кольцевых протоколов являются взаимоисключающими. На порту, входящем в транковую группу, нельзя включить STP, в тоже время порт с включенным протоколом STP, нельзя включить в транковую группу.
- Порт с поддержкой STP не может быть настроен как кольцевой или резервный порт. Соответственно, STP нельзя включить на кольцевом или резервном порту.

Приоритет порта (Port Priority)

Настраиваемый диапазон: 0~255 с шагом 16

Значение по умолчанию: 128

Описание: Настройка приоритета порта, который определяет роль порта.

Стоимость пути (Path Cost)

Настраиваемый диапазон: 1~200000000

Значение по умолчанию: 2000000 (10М порт), 200000 (100М порт), 20000 (1000М порт)

Описание: Стоимость пути порта используется для расчета наилучшего пути. Значение параметра зависит от ширины полосы. Чем больше значение, тем ниже стоимость. Вы можете изменить роль порта, изменив значение параметра стоимости пути. Чтобы настроить значение, вручную выберите «Нет» (No) в поле «Cost Count».

Счетчик стоимости (Cost Count)

Настраиваемые варианты: Да/Нет (Yes/No)

Значение по умолчанию: Да (Yes)

Описание: если выбрано «Да», стоимость пути порта принимает значение по умолчанию; если выбрать «Нет», пользователи могут самостоятельно настроить стоимость порта.

6.13.6. Пример типовой настройки

Как показано на рис. 83, приоритеты коммутаторов А, В, С имеют значения 0, 4096, 8192 соответственно, а стоимость пути (path cost) трех связей имеет значения 4, 5, и 10 соответственно.

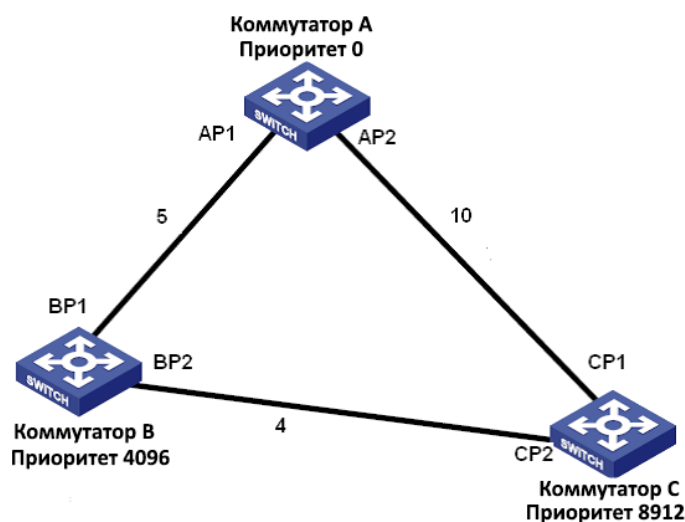


Рис. 83. Пример настройки RSTP



Настройка коммутатора А:

1. Установите значение приоритета «0», а временные параметры в значение «по умолчанию» (см. рис. 81).
2. Присвойте стоимости пути порта 1 значение 5, а стоимости пути порта 2 значение 10 (см. рис. 82).

Настройка коммутатора В:

1. Установите значение приоритета «4096» а временные параметры в значение «по умолчанию» (см. рис. 81).
2. Присвойте стоимости пути порта 1 значение 5, а стоимости пути порта 2 значение 4 (см. рис. 82).

Настройка коммутатора С:

1. Установите значение приоритета «8192» а временные параметры в значение «по умолчанию» (см. рис. 81).
2. Присвойте стоимости пути порта 1 значение 10, а стоимости пути порта 2 значение 4 (см. рис. 82).
 - Приоритет коммутатора А равен «0» и имеет наименьший идентификатор (ID) моста, поэтому он является корневым мостом.
 - Стоимость пути от AP1 до BP1 равна 5, а стоимость пути от AP2 до BP2 равна 14, поэтому BP1 является корневым портом.
 - Стоимость пути от AP1 до CP2 равна 9, а стоимость пути от AP2 до CP1 равна 10, поэтому CP2 он является корневым портом, а BP2 – портом назначения.

6.14. Прозрачная передача STP/RSTP

6.14.1. Описание

Протокол RSTP является протоколом, стандартизированным IEEE, а Sy2-Ring - это проприетарный протокол резервирования Симанитрон. Протоколы RSTP и Sy2-Ring не могут работать совместно. Чтобы решить эту проблему, Симанитрон разработал специальную функцию передачи RSTP/STP, которая поддерживает работу различных протоколов резервирования на коммутатор и которая позволяет прозрачно передавать сообщения протокола RSTP.

Когда на коммутаторах, у которых включены собственные протоколы резервирования, включена функция прозрачной передачи RSTP на портах, они могут принимать и пересылать сообщения протокола RSTP. Включенную на коммутаторе функцию прозрачной передачи RSTP можно рассматривать как прозрачный канал (link).

На рисунке 84 коммутаторы А, В, С и D образуют кольцо Sy2-Ring. После включения функции прозрачной передачи на этих четырех коммутаторах, коммутаторы Е и F могут получать сообщения протокола RSTP друг от друга.

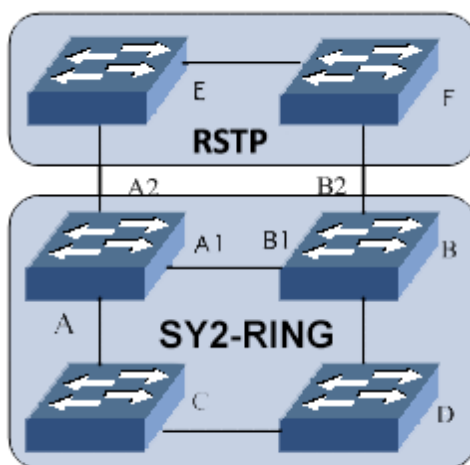


Рис. 84. Режим прозрачной передачи RSTP

6.14.2. Настройка через WEB-интерфейс

Настройте функцию прозрачной передачи RSTP на порту, как показано на рис. 85.

Port	RSTP Transparent Transmission
FE1	Enable
FE2	Enable
FE3	Enable
FE4	Disable
FE5	Disable
FE6	Disable
FE7	Disable
FE8	Disable
FE9	Disable
FE10	Disable
FE11	Disable
FE12	Disable
FE13	Disable
FE14	Disable
FE15	Disable
FE16	Disable
FX17	Disable
FX18	Disable
FX19	Disable
FX20	Disable

Apply

Рис. 85. Настройка режима прозрачной передачи RSTP



Прозрачная передача RSTP/STP

Настраиваемые опции: Выключить/Выключить (Enable/Disable)

Значение по умолчанию: Выключено (Disable)

Описание: Включение на порту функции прозрачной передачи RSTP.



Если на порту включен протокол RSTP, функция прозрачной передачи RSTP не может быть включена.

6.14.3. Пример типовой настройки

Как показано на рисунке 84, коммутаторы А, В, С и D формируют кольцо Sy2-Ring; коммутаторы Е и F формируют кольцо RSTP. В кольце RSTP кольцо Sy2-Ring служит каналом прозрачной передачи сообщений протокола RSTP коммутатора Е или коммутатора F.

- Настройте коммутаторы А, В, С и D как кольцо Sy2-Ring; описание настроек можно посмотреть в разделе «Sy2-Ring Configuration».
- Включите протокол RSTP на соответствующих портах коммутаторов Е и F (см. рис. 80 и 82).
- Необходимо включить функцию прозрачной передачи RSTP на портах А1, А2, В1, В2, В3, С1, С2, D1, D2 у коммутаторов А, В, С и D (см. рис. 85).

6.15. Настройка QoS

6.15.1. Введение

Функция QoS (Quality of Service) позволяет дифференцировать сервисы, в зависимости от разных требований в условиях ограниченной пропускной способности путём контроля трафика и управления потоком трафика в IP сетях. QoS пытается удовлетворить задачи передачи данных различных сервисов, снизить задержки в передачи данных и минимизировать эффект от задержек, в зависимости от приоритета сервиса.

Основные задачи QoS: идентификация трафика, управлением задержками передачи данных и предотвращение перегрузок в сети.

Идентификация трафика: идентификация объектов происходит в соответствии с определенными правилами. Например, объектами могут быть поля приоритетов в пакетах; приоритеты, определяемые по портам и VLAN-ам; либо другая информация о приоритетах. Идентификация трафика - основополагающая функция QoS.

Управление задержками: обязательная функция для определения важности данных. Управление задержками представляет собой комбинацию следующих техник: создание приоритетных очередей, определение последовательности передачи данных в зависимости от определённого алгоритма, что позволяет достичь приоритета передачи для самых важных сервисов.

Предотвращение перегрузок: чрезмерное количество задержек передачи данных могут повредить данным, передаваемым через сеть. Функция предотвращения перегрузок следит за использованием всех сетевых ресурсов. При обнаружении повышенного числа задержек, данная функция запускает механизм предупредительного отбрасывания пакетов и изменяет количество передаваемых данных для избавления от перегрузки сети.



6.15.2. Принцип работы

Каждый порт данной серии коммутаторов поддерживает 4 очереди кэширования (0, 1, 2, 3) по принципу: чем выше число - тем выше приоритет. При поступлении кадра на порт, коммутатор определяет подходящую для него очередь в зависимости от его заголовка. Коммутатор поддерживает три режима определения соответствия очередей и приоритетов: высокий приоритет, TOS/DIFF и 802.1p.

- Если наивысший приоритет установлен на порт, то пересылаемым пакетам будет установлена очередь 3.
- Значение TOS/DIFF зависит от наличия TOS/DSCP в пакетах. Вы можете настроить сопоставление между приоритетом и очередями.
- Если сообщение является тегированным, значение 802.1p зависит от приоритета тега 802.1p в сообщении. Когда сообщение является нетегированным, значение 802.1p зависит от приоритета порта по умолчанию. Можно настроить отношение отображения приоритета 802.1p и очереди.

При передаче данных, для распределения кадров по 4 приоритетным очередям порт использует режим планирования. Данные коммутаторы используют два режима постановки в очередь: WRR (Weighted Round Robin, взвешенная очередь) и режим упреждения (Hq-preempt).

- WRR распределяет данные в зависимости от взвешенного коэффициента. Размер очередей зависит от их взвешенного коэффициента. WRR отдаёт приоритет очередям с наибольшим значением коэффициента.
- Режим упреждения (Hq-preempt) гарантирует, что данные с максимальным приоритетом будут передаваться в первую очередь. Как только на коммутатор поступают данные с максимальным приоритетом, устройство прекращает обработку данных с более низкими приоритетами и начинает передачу тех, что максимальным приоритетом. Только когда очередь максимального приоритета пуста, устройство переходит к передаче данных следующей по важности очереди и так далее.

6.15.3. Настройка через Web-интерфейс

1. Настройка режима QoS:

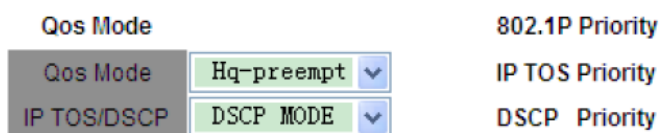


Рис. 86. Настройка QoS

Режим QoS (QoS Mode)

Настраиваемые опции: Disable/WRR/Hq-preempt

Значение по умолчанию: Hq-preempt

Описание: Настройка режима планирования порта.

Режим IP TOS/DSCP (IP TOS/DSCP)

Настраиваемые опции: DSCP MODE/IP TOS MODE

Значение по умолчанию: DSCP MODE



Описание: DSCP и IP TOS используют одно и то же поле. В режиме DSCP обеспечивается сопоставление очереди приоритетов DSCP, а в режиме IP TOS - сопоставление очереди приоритетов IP TOS.

2. Настройка соотношения весового коэффициента и очереди.

Weight of Priority Queues

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

Рис. 87. Настройка порта QoS

Очередь {3-HIGHEST, 2-SECHIGH, 1-SECLow, 0-LOWEST} (3-наивысший, 2-высокий, 1-низкий, 0-наименьший)

Настраиваемый диапазон: {1~55, 1~55, 1~55, 1~55}

Значение по умолчанию: {8, 4, 2, 1}

Описание: Настройте соотношение веса очереди, соблюдая следующие правила:

Вес очереди 3 ≥ 2*Вес очереди 2, Вес очереди 2 ≥ 2*Вес очереди 1, Вес очереди 1 ≥ 2*Вес очереди 0

3. Настройка режима соответствия приоритетов портов QoS

Set the Port Priority

Port	Highest priority	TOS/DIFF	802.1P Priority
FE1	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
FE2	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
FE3	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
FE4	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
FE5	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
FE6	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
FE7	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
FE8	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
FE9	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
FE10	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
FE11	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
FE12	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
FE13	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
FE14	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
FE15	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
FE16	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
FX17	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
FX18	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
FX19	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
FX20	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>

Apply

Рис. 88. Настройка режима соответствия приоритетов портов QoS



Настройка приоритетов портов (Set the Port Priority)

Настраиваемые опции: Highest priority/TOS/DIFF/802.1p Priority (Наивысший приоритет/приоритет TOS/приоритет DIFF/приоритет 802.1p)

Значение по умолчанию: 802.1p Priority (приоритет 802.1p).

Описание: Настройка режима соответствия приоритетов портов. Только один режим соответствия приоритетов может быть выбран для каждого порта.

4. Настройка соответствия приоритета 802.1 p к очереди

Нажмите <802.1p Priority> (см. рис. 86) для того, чтобы настроить приоритет 802.1 p к очереди (рис. 89.).

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

Рис. 89. Настройка отношения приоритета 802.1 p к очереди

Настройка приоритета 802.1P (802.1p Priority Configuration)

Групповая настройка: {Priority, Queue} (Приоритет, Очередь)

Диапазон значений: {0~7, 0~3}

Значение по умолчанию: приоритеты 0 и 1 соответствуют очереди 0; приоритеты 2 и 3 соответствуют очереди 1; приоритеты 4 и 5 соответствуют очереди 2; приоритеты 6 и 7 соответствуют очереди 3.

Описание: Настройка соответствия приоритета 802.1 p к очереди.

5. Настройка отношения приоритета IP TOS к очереди.

Нажмите <IP TOS Priority> (см. рис. 86) для того, чтобы настроить приоритет IP TOS к очереди (рис. 90).



IP TOS Priority 0-7

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

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

Apply

Back

Рис. 90. Настройка отношения приоритета IP TOS к очереди

Настройка приоритета IP TOS (IP TOS Priority Configuration)

Групповая настройка: {Priority, Queue} (Приоритет, Очередь)

Диапазон значений: {0~7, 0~3}

Значение по умолчанию: приоритеты от 0 до 7 соответствуют очереди 0.

Описание: Настройка соответствия между приоритетом IP TOS и очередью.

6. Настройка соответствия приоритета DSCP к очереди.

Нажмите <DSCP Priority> (см. рис. 86) для того, чтобы настроить приоритет DSCP к очереди (рис. 91).

DSCP Priority 0-63

DSCP	Qos Queue	DSCP	Qos Queue	DSCP	Qos Queue	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

Рис. 91. Настройка отношения приоритета DSCP к очереди



Приоритет DSCP

Групповая настройка: {Priority, Queue}

Диапазон значений: {0~63, 0~3}

Значение по умолчанию: приоритеты от 0 до 63 соответствуют очереди 0.

Описание: Настройка соответствия между приоритетом DSCP и очередью.

6.15.4. Пример типовой настройки

Как показано на рис. 92, порты 1, 2, 3, 4 пересылают сообщения в порт 5. Наивысший режим приоритета настроен на порту 1. Пакеты, отправляемые из порта 1, соответствуют очереди 1. Пакеты с приоритетом 802.1p, пересылаемые из порта 2 имеют приоритет 2 и соответствуют очереди 1. Пакеты с приоритетом 802.1p, пересылаемые из порта 3 имеют приоритет 4 и соответствуют очереди 2. Пакеты с приоритетом DSCP, пересылаемые из порта 4, имеют приоритет 6 и соответствуют очереди 3. Порт 5 использует режим постановки в очередь WRR.

Шаги настройки коммутатора:

1. Выберите тип очереди WRR для режима QoS и DSCP для IP TOS/DSCP. Настройте значения по умолчанию для весового коэффициента очереди WRR, как показано на рис. 86 и рис. 87.
2. Настройте для порт 1 соотношение наивысший приоритет/очередь, установите приоритет 802.1p на портах 2 и 3 и приоритет TOS/DIFF на порту 4, как показано на рис. 88.
3. Установите приоритетам 802.1p 2 и 4 очереди 1 и 2 соответственно, как показано на рис. 89.
4. Настройте приоритету DSCP 6 соответствие очереди 3, как показано на рис. 91.

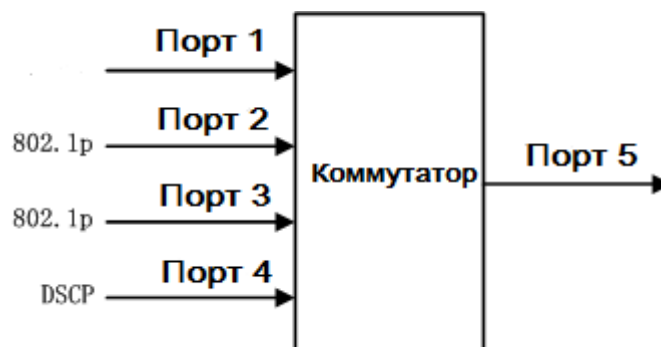


Рис. 92. Пример настройки QoS

Пакеты, принимаемые через порты 1 и 4 добавляются в очередь 3; пакеты принимаемые через порт 2 добавляются в очередь 1; пакеты, принимаемые через порт 3 добавляются в очередь 2. Согласно соответствующей зависимости между очередью и весом, весовое отношение очереди 1 равно 2, весовое отношение очереди 2 равно 4, весовое отношение очереди 3 равно 8. В результате мы получаем, что отношение пропускной способности к пакетам в очереди 1 соответствует значению $2/(2+4+8)$; отношение пропускной способности к пакетам в очереди 2 соответствует значению $4/(2+4+8)$; отношение пропускной способности к пакетам в очереди 3, соответствует значению $8/(2+4+8)$. Кроме того, все пакеты от портов 1 и 4 входят в очередь 3 и они пересылаются на основе



механизма FIFO. Общее отношение пропускной способности, выделенное для пакетов портов 1 и 4 должно соответствовать значению $8/(2+4+8)$.

6.16. Время старения MAC адреса (MAC Address Aging Time)

6.16.1. Введение

Каждый порт коммутатора имеет функцию автоматического определения адресов. Функция предназначена для того, чтобы узнать адрес источника принимаемого кадра, включая исходный MAC-адрес и номер порта коммутатора, и сохранить его в таблице адресов. Режим времени старения (Aging Time) начинает работать после добавления динамического адреса в таблицу адресов. Если все порты коммутатора не получают кадр с этим адресом источника в течение одной или двух стадий времени старения, адрес будет удален из таблицы динамических переадресаций. Статическая таблица MAC-адресов не зависит от времени старения.

6.16.2. Настройка через WEB-интерфейс

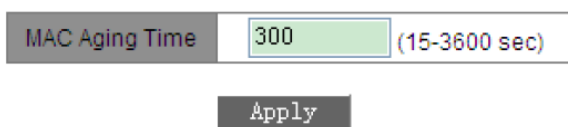


Рис. 93. Настройка времени старения MAC-адресов

Настройка времени старения (MAC Aging Time)

Диапазон значений: 15~3600 сек.

Значение по умолчанию: 300 сек.

Описание: Пользователи могут изменить время старения в соответствии с конкретной ситуацией, чтобы эффективно использовать функцию старения MAC адресов.

6.17. Настройка LLDP

6.17.1. Введение

Протокол Link Layer Discovery Protocol (LLDP) предоставляет собой стандартный метод обнаружения уровня канала (2-го уровня). Он инкапсулирует различную информацию, например, возможности устройства, адрес, идентификатор устройства и интерфейса, в пакет Link Layer Discovery Protocol Data Unit (LLDPDU, блок данных протокола обнаружения уровня канала), и передаёт LLDPDU своим непосредственно подключённым соседям. При получении LLDPDU, соседи сохраняют эту информацию в MIB для предоставления NMS данной информации, а также информации о состоянии соединения между устройствами.

6.17.2. Настройка через WEB-интерфейс

Просмотр информации LLDP:



LLDP Information			
Local Port	Remote Port	Neighbor IP	Neighbor MAC
1	3	192.168.0.201	00:15:21:17:cd:dd
5	10	192.168.183.53	00:21:cd:12:21:15

Рис. 94. Информация LLDP

В информации LLDP будет отображаться информация о соседнем устройстве, включая информацию о номере локального порта коммутатора и удаленного порта на соседнем устройстве, а также IP-адрес и MAC-адрес соседнего устройства (см. рис.94).



Информация о LLDP может быть показана только после того, как протокол LLDP будет включен на каждом из соседних устройств. Т.к. данный протокол является стандартным механизмом, по умолчанию он всегда будет включен.

6.18. Протокол SNTP

6.18.1. Введение

Протокол SNTP (Simple Network Time Protocol) обеспечивает синхронизацию времени между сервером и клиентом путём запросов и ответов. Если коммутатор выступает в качестве клиента, он синхронизирует своё время со временем сервера. Для одного коммутатора одновременно можно назначить до 4-х SNTP серверов, однако активным из них может быть только один.

Клиент SNTP последовательно отправляет запрос каждому серверу в виде одноадресной рассылки. Сервер, первым ответивший на запрос становится активным. Остальные серверы будут неактивны.



- Чтобы синхронизировать время по SNTP, должен быть активный SNTP-сервер.

6.18.2. Настройка через WEB-интерфейс

1. Включите протокол. Выберите сервер и настройте соответствующие параметры.

SNTP State	Enable
Server IP	192.168.0.23
Interval Time	16 (16-16284Sec)
time zone	GMT + 8
Apply	

Рис. 95. Настройка SNTP



Статус SNTP (SNTP State)

Настраиваемые опции: Enable/Disable (Включить/Выключить)

Значение по умолчанию: Disable (Выключено)

Описание: Включение или выключение SNTP.

IP адрес сервера (Server IP)

Формат: A.B.C.D

Описание: Настройка IP адреса сервера SNTP. Клиенты будут синхронизировать своё время в соответствии с сообщениями этого сервера.

Интервал времени (Interval Time)

Настраиваемый диапазон (сек.): 16~16284

Описание: Настройка интервала для отправки запросов синхронизации на сервер SNTP.

Настройка часового пояса (Time Zone)

Настаиваемые опции: 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.

Значение по умолчанию: 0

Описание: Настройка часового пояса.

- Выбор режима синхронизации времени между клиентом и сервером.

Server Time	2012.08.22 16:49:46	
Device Time	2012.08.22 16:49:48	
update	<input type="button" value="automatism"/>	<input type="button" value="Apply"/>

Рис. 96. Настройка режима синхронизации

Время сервера (Server Time)

Описание: Отображение последних показаний времени, полученных от сервера.

Время устройства (Device Time)

Функция: Отображение времени устройства.

Выбор режима синхронизации (Update)

Настраиваемые опции: Automatism/Manual (Автоматически/Вручную)

Значение по умолчанию: Automatism (Автоматически)

Функция: Выбор режима синхронизации времени между клиентом и сервером.

- Отображение информации о настройках SNTP. Вы можете выбрать сервер SNTP, нажать <Delete> и удалить его.

Number	Server IP	Server State	Time Zone	Interval Time	Synchronization
<input type="checkbox"/> 1	192.168.0.23	active	+ 8	16	<input type="button" value="Synch"/>
<input checked="" type="checkbox"/> 2	192.168.1.217	repose	+ 8	32	<input type="button" value="Synch"/>

Рис. 97. Информация о настройках SNMP

Статус сервера (Server Status)

Отображаемые значения: active/repose (активный/неактивный)



Сервер в активном состоянии выполняет синхронизацию времени SNTP для клиента. Существует один сервер, который находится в активном состоянии, а все другие находятся в неактивном состоянии.

Синхронизация (Synchronization)

Описание: Нажмите кнопку <Synch>, если у вас установлен режим синхронизации «Manual».

4. Настройка коммутатора в режиме сервера SNTP.

SNTP State	Enable
time zone	GMT + 8

Apply

Local IP	192.168.0.102
Device Time	2012.08.22 16:53:16
Time Zone	8

Рис. 98. Настройка коммутатора в режиме сервера SNTP

Статус сервера SNTP (SNTP State)

Настраиваемые опции: Enable/Disable (Включить/Выключить)

Значение по умолчанию: Disable (Выключено)

Описание: Включение или выключение функции сервера SNTP.

Настройка часового пояса (Time Zone)

Настраиваемые опции: 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.

Значение по умолчанию: +8

Описание: Настройка часового пояса сервера времени.

6.19. Протокол MSTP

6.19.1. Введение

Несмотря на то, что протокол RSTP обеспечивает быструю конвергенцию, он имеет следующую проблему, которая похожа на проблему протокола STP: все мосты в LAN используют одно связующее дерево (spanning tree), а пакеты всех VLAN пересылаются по всему связующему дереву. Как показано на рис. 99, определенные конфигурации могут блокировать связь между коммутаторами А и С. Поскольку коммутатор В и коммутатор D не находятся в VLAN 1, они не могут пересылать пакеты VLAN 1. В результате порт VLAN 1 коммутатора А не может связаться с коммутатором С.

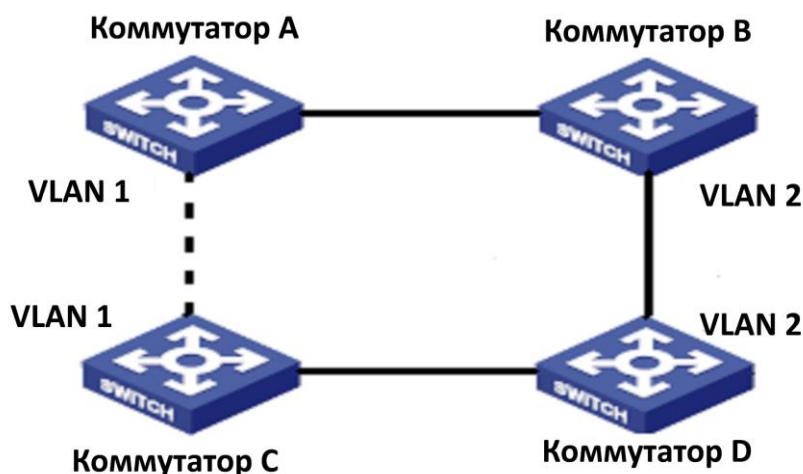


Рис. 99. Проблема RSTP

С помощью MSTP можно решить эту проблему. Данный протокол обеспечивает не только быструю конвергенцию, но и возможность создания отдельных путей пересылки трафика разных VLAN, обеспечивая качественный механизм распределения нагрузки для избыточных связей.

MSTP сопоставляет одну или несколько VLAN в одном инстансе (instance). Коммутаторы с одинаковой конфигурацией образуют регион (region). Каждый регион содержит несколько взаимно независимых связующих деревьев (spanning trees). Этот регион является, по сути, виртуальным коммутатором, т.е. узлом. Он участвует в обработке данных совместно с другими регионами на основе алгоритма «spanning tree», вычисляя общее связующее дерево. На основе этого алгоритма сеть (см. рис. 99) формирует топологию (см. рис. 100). Коммутаторы А и С находятся в Регионе 1. Связи не заблокированы, потому что объект не содержит петель. То же самое происходит с Регионом 2. Регион 1 и Регион 2 аналогичны друг другу и являются виртуальными узлами (коммутаторами). Эти два «коммутатора» образуют петлю. Следовательно, линии связи должны быть заблокированы.

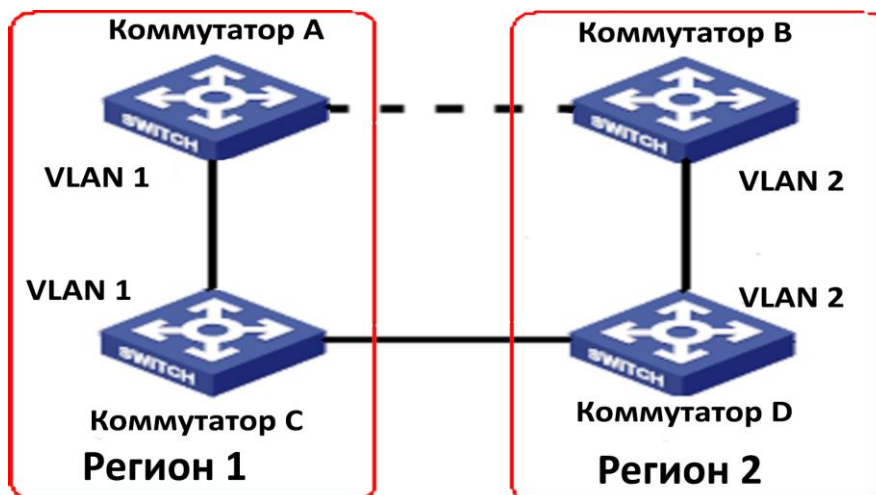


Рис. 100. Топология MSTP



6.19.2. Концепция

Внимательно рассмотрите схемы и рисунки, на которых изложена концепция MSTP (рис. 101 - рис. 104).

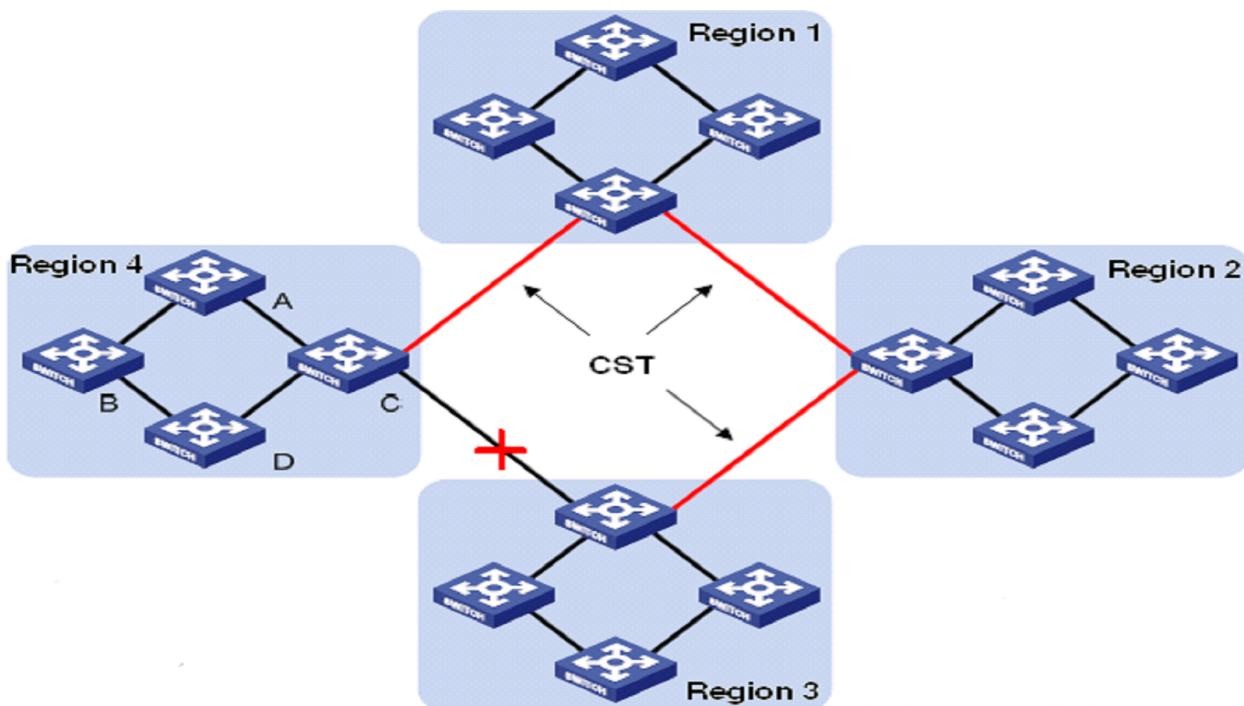


Рис. 101. Концепция MSTP

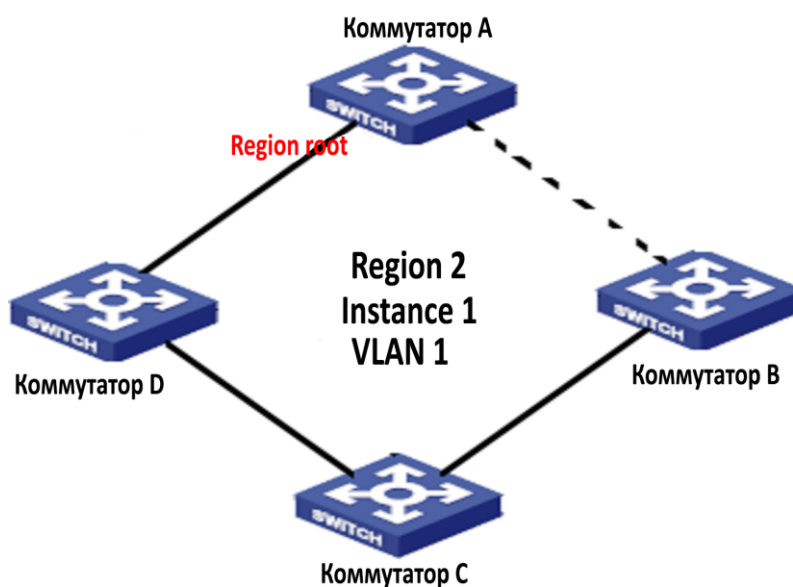


Рис. 102. Соответствие VLAN 1 инстансу 1

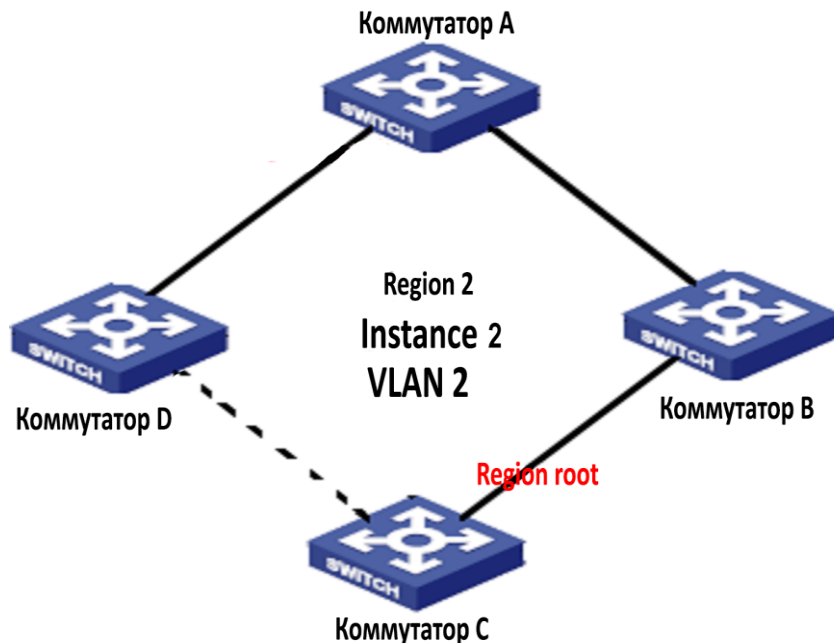


Рис. 103. Соответствие VLAN 2 инстансу 2

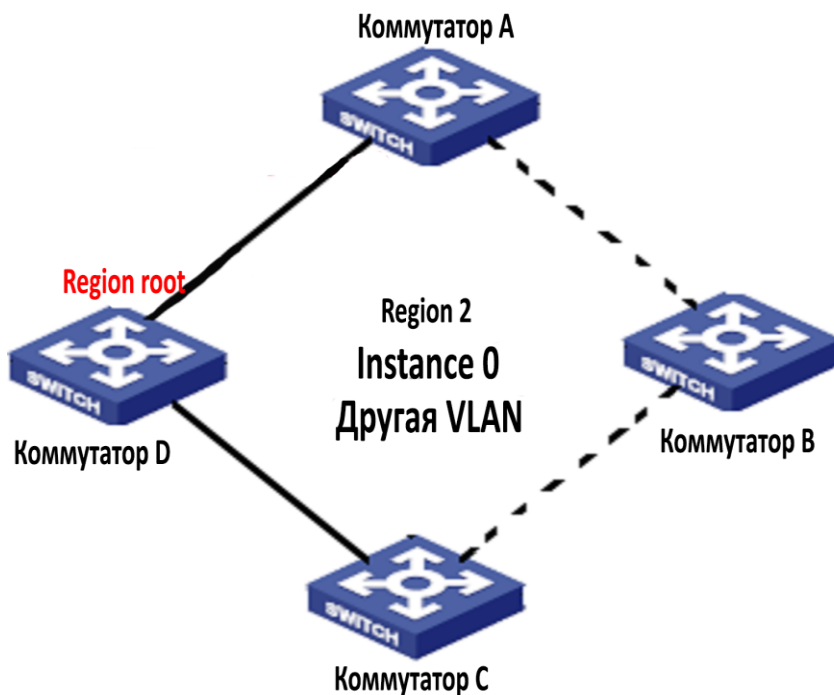


Рис. 104. Соответствие других VLAN инстансу 0

- Instance (инстанс): набор из нескольких VLAN. Одна VLAN (как показано на рис. 102 и рис. 103) или несколько VLAN с одинаковой топологией (как показано на рис. 104) могут быть отнесены к одному инстансу; то есть одна VLAN может сформировать связующее дерево, соответственно несколько VLAN могут совместно использовать одно связующее дерево. Разные инстансы могут быть отнесены к разным связующим



деревьям. Инстанс 0 - это связующее дерево для устройств всех регионов, а остальные - связующие деревья для устройств определенного региона.

- MST регионы (Multiple Spanning Tree Regions): коммутаторы имеют то же имя региона, что и регион MSTP, одинаковые параметры изменения конфигурации (revision level), а соответствующие инстансы VLAN находятся в одном и том же регионе MST. Как показано на рис. 101, Регион 1, Регион 2, Регион 3 и Регион 4 являются четырьмя различными регионами MST.
- Таблица соответствия VLAN (VLAN mapping table): состоит из соответствий VLAN к связующим деревьям. На рис. 101 таблица соответствия VLAN Региона 2 представляет собой соответствие VLAN 1 и инстанса 1 (см. рис. 102); VLAN 2 соответствует инстансу 2 (см. рис. 103). Другие VLAN соответствуют инстансу 0 (см. рис. 104).
- CIST дерево (Common and Internal Spanning Tree): данный термин означает инстанс 0, т.е. связующее дерево, которое включает все устройства в сети. Как показано на рис. 101, CIST содержит IST (Internal Spanning Tree) и CST (Common Spanning Tree).
- IST дерево (Internal Spanning Tree): данный термин указывает на сегмент дерева CIST в регионе MST, то есть инстанс 0 для каждого региона (см. рис. 104).
- CST дерево (Common Spanning Tree): это связующее дерево, соединяющее все регионы MST в коммутационной сети. Если каждый регион MST является узлом, то CST является связующим деревом, вычисленным на основе протоколов STP/RSTP этими узлами. Красные линии указывают на связующее дерево (см. рис. 101).
- Инстанс MSTI (Multiple Spanning Tree Instance): одна область MST может формировать множество связующих деревьев, и они независимы друг от друга. Каждое связующее дерево является инстансом MSTI (см. рис. 102 и рис. 103). IST также является специальным MSTI.
- Общий корень (Common root): корневым мостом CIST. Коммутатор с наименьшим идентификатором корневого моста в сети является общим корнем.
- Региональный корень (Regional root): в регионе MST у связующих деревьев могут быть разные топологии, соответственно их региональные корни также могут быть разными. Как показано на рис. 102, рис. 103 и рис. 104, три инстанса имеют разные региональные корни. Корневым мостом MSTI вычисляется на основе протокола STP/RSTP в текущем регионе MST. Корневым мостом IST - это устройство, которое подключено к другому региону MST и выбрано на основе полученной информации о приоритете.
- Пограничный порт (Boundary port): это порт, который соединяет один регион MST с другим регионом MST, рабочим регионом STP или рабочим регионом RSTP.
- Состояние порта (Port state): если порт определяет MAC адреса и передает трафик, он может находиться в любом из следующих состояний:
 - Состояние пересылки (Forwarding state): данное состояние указывает на то, что порт определяет MAC адреса и пересылает трафик.
 - Состояние обучения (Learning state): это состояние означает, что порт определяет MAC адреса, но не передает трафик.
 - Состояние отбрасывания: означает, что порт не определяет MAC адреса и не пересылает трафик.



- Корневой порт (Root port): означает наилучший порт между мостами (корневым и не корневым), то есть порт с наименьшей стоимостью. Не корневой мост связывается с корневым мостом через корневой порт и имеет только один корневой порт. Корневой мост не имеет корневого порта. Корневой порт может находиться в состоянии пересылки, обучения или отбрасывания.
- Порт назначения (Designated port): это порт для пересылки BPDU на другие устройства или LAN. Все порты на корневом мосту являются портами назначения. Порт назначения может находиться в состоянии пересылки, обучения или отбрасывания.
- Мастер порт (Master port): данный порт соединяет область MST с общим корнем. Мастер порт имеет кратчайший путь к общему корню. В CST главный порт является корневым портом региона (который в свою очередь является узлом). Мастер порт представляет собой специальный пограничный порт. Он является корневым портом для CIST и мастер портом для других инстансов. Мастер порт может находиться в состоянии пересылки, обучения или отбрасывания.
- Альтернативный порт (Alternate port): это резервный порт для корневого порта или мастер порта. Когда корневой порт или мастер порт выходят из строя, альтернативный порт становится новым корневым портом или мастер портом. Мастер порт может находиться только в состоянии отбрасывания.
- Резервный порт (Backup port): когда порт назначения выходит из строя, резервный порт становится портом назначения и пересылает данные без какой-либо задержки. Резервный порт может находиться только в состоянии отбрасывания.

6.19.3. Реализация

MSTP делит сеть на несколько регионов MST. Значение CST рассчитывается между регионами. В регионе вычисляются несколько связующих деревьев. Каждое связующее дерево - это MSTI. Инстанс 0 - это IST, а другие инстансы – это MSTI.

1. Вычисление CIST

- Устройство отправляет и принимает пакеты BPDU. Основываясь на сравнении сообщений о конфигурации MSTP, устройство с наивысшим приоритетом выбирается как общий корень CIST.
- IST рассчитывается в каждом регионе MST.
- Каждый регион MST рассматривается как единое устройство, а CST рассчитывается между регионами.
- CST и IST формируют CIST всей сети.

2. Вычисление MSTI

- В MST регионе MSTP генерирует различные связующие деревья для VLAN на основе сопоставления между VLAN и связующими деревьями. Каждое связующее дерево вычисляется независимо. Процесс вычисления аналогичен процессу STP.
- В области MST пакеты VLAN передаются по соответствующим MSTI. Между регионами MST пакеты VLAN отправляются по CST.

6.19.4. Настройка через WEB-интерфейс

1. Включение MSTP



Open/Close MSTP

Mstp State	<input type="text" value="Enable"/>
------------	-------------------------------------

Рис. 105. Включение MSTP

Статус Mstp (Mstp State)

Настраиваемые опции: Включить/Выключить (Enable/Disable)

Значение по умолчанию: Выключено (Disable)

Описание: Включение или выключение протокола MSTP.

2. Настройка рабочего режима MSTP

MSTP Mode Config

Mstp Mode	<input type="text" value="MSTP"/>
-----------	-----------------------------------

Рис. 106. Настройка рабочего режима MSTP

Режим Mstp (Mstp Mode)

Настраиваемые опции: MSTP/STP

Значение по умолчанию: MSTP

Описание: Настройка режима работы коммутатора. В режиме STP все порты коммутатора могут отправлять только пакеты STP BPDU. В режиме MSTP все порты коммутатора отправляют пакеты MSTP BPDU, но если коммутатор подключен к устройству с поддержкой STP, порт автоматически переключается в режим STP.

3. Принудительная настройка порта в режим MSTP.

MSTP Port Mcheck

Port	<input type="text" value="FE3"/>
------	----------------------------------

Рис. 107. Принудительная настройка порта в режим MSTP

Настройка порта (Port)

Настраиваемые опции: все порты коммутатора

Описание: Когда порт с поддержкой MSTP подключен к устройству с поддержкой STP, подключенный порт автоматически переключится в режим STP. Если устройство с поддержкой STP будет удалено, порт автоматически не сможет вернуться в режим MSTP. Если вы хотите, чтобы в этом режиме коммутатор переключился в режим MSTP, настройте



эту функцию для порта. Соответственно, если порт снова получит сообщение STP, порт снова переключится в режим STP.



Эти настройки будут эффективны только когда коммутатор работает в режиме MSTP. В противном случае они будут некорректны.

4. Настройка статуса порта MSTP

Open/Close Port MSTP

Operation type	Add ▼
Port	FE3 ▼

Apply

Рис. 108. Настройка MSTP на порту

Выбор рабочего режима (Operation type)

Настраиваемые опции: Add/Del (Добавить/Удалить)

Значение по умолчанию: Add (Добавить)

Описание: Включение/Выключение MSTP на порту. Значение «Add» включает MSTP на порту; значение «Del» выключает MSTP на порту. Если протокол MSTP включен глобально, то по умолчанию он будет включен на всех портах.

5. Настройка параметров региона MST

MSTP Region Config

OperationType	Set ▼
MSTP Region Name Config	001ecd17c067
MSTP Revisionlevel Config	0

Apply

Рис. 109. Настройка параметров региона MSTP

Выбор рабочего режима (Operation type)

Настраиваемые опции: Set/Default (Настроить/По умолчанию).

Описание: Выбор рабочего режима параметров региона MST.

Настройка имени региона MSTP (MSTP Region Name Config)

Настраиваемый диапазон: 1~32 символов.

Значение по умолчанию: MAC адрес устройства.

Описание: Настройка имени региона MSTP.

Настройка уровня изменения параметров конфигурации (MSTP Region Level Config)

Настраиваемый диапазон: 0~65535.

Значение по умолчанию: 0.



Описание: Настройка уровня изменения параметров конфигурации региона MSTP. Параметры конфигурации, имя региона MST и таблица сопоставления VLAN определяют область MST, к которой принадлежит устройство. Когда все конфигурации одинаковы, устройства находятся в одной и той же области MST.

6. Настройка таблицы сопоставления VLAN.

Add/Del Instance

OperationType	Add ▾
MSTP Instance ID	3
Vlan List	5

Apply

Instance List

Instance ID	Vlan List
0	1 4 - 4094
2	2
3	3

Рис. 110. Настройка таблицы сопоставления VLAN

Выбор рабочего режима (Operation type)

Настраиваемые опции: Add/Del (Добавить/Удалить).

Описание: Выбор рабочего режима таблицы сопоставления VLAN.

Настройка сопоставления <MSTP Instance ID, VLAN list> (Идентификатор инстанса MSTP, список VLAN)

Настраиваемый диапазон: <0~16, 1~4094>.

Значение по умолчанию: <0, 1~4094>.

Описание: Настройка таблицы VLAN в регионе MST. По умолчанию все VLAN соответствуют инстансу 0. Одна VLAN соответствует только одному инстансу связующего дерева. Если VLAN с существующим соответствием будет сопоставлена с другим инстансом, предыдущее соответствие отменяется. Если сопоставление между VLAN и инстансом удаляется, эта VLAN будет сопоставлена с инстансом 0.



Значение не может удалять список VLAN, относящихся к инстансу 0.

«Список инстансов» (Instance List) отображает сопоставление между VLAN и инстансом после завершения настройки.

7. Настройка приоритета моста для удаленного инстанса.



MSTP MST Priority

OperationType	Add
MSTP Instance ID	0
MSTP Bridge Priority	32768

Apply

Рис. 111. Настройка приоритета моста в удаленном инстансе

Выбор рабочего режима (Operation type)

Настраиваемые опции: Add/Default (Добавить/По умолчанию).

Описание: Выбор рабочего режима приоритета моста для коммутатора в удаленном инстансе.

Настройка идентификатора инстанса MSTP (MSTP Instance ID)

Настраиваемые опции: все созданные инстансы.

Приоритет моста MSTP (MSTP Bridge Priority)

Настраиваемый диапазон: 0~61440 с шагом 4096.

Значение по умолчанию: 32768.

Описание: Настройка приоритета моста коммутатора для удаленного инстанса. Приоритет моста определяет, может ли коммутатор быть выбран в качестве регионального корневого для инстанса связующего дерева. Чем меньше значение, тем выше приоритет. Установив более низкий приоритет, конкретное устройство может быть обозначено как корневой мост связующего дерева. Устройство с поддержкой MSTP может быть настроено с различными приоритетами в разных инстансах связующего дерева.

8. Настройка приоритета порта и стоимости пути в удаленном инстансе.

MSTP MST Port Cost and Priority

OperationType	Add
MSTP Instance ID	0
Port	FE3
Priority	128
MSTP Port Pathcost	200000

Apply

Рис. 112. Настройка приоритета порта и стоимости пути в удаленном инстансе

Выбор рабочего режима (Operation type)

Настраиваемые опции: Add/Default (Добавить/По умолчанию).

Описание: Выбор рабочего режима приоритета и стоимости пути порта в удаленном инстансе.

Настройка идентификатора инстанса MSTP (MSTP Instance ID)

Настраиваемые опции: все созданные инстансы.



Настройка портов (Port)

Настраиваемые опции: все порты коммутатора.

Настройка приоритета (MSTP Bridge Priority)

Настраиваемый диапазон: 0~240 с шагом 16.

Значение по умолчанию: 128.

Описание: Настройка приоритета порта в удаленном экземпляре. Приоритет порта определяет, будет ли он выбран в качестве корневого порта. Порт с более низким приоритетом будет выбран в качестве корневого порта. Порты с поддержкой MSTP могут быть настроены с различными приоритетами и обеспечивают разные роли портов в разных экземплярах связующего дерева.

Настройка стоимости пути (MSTP Port Path cost)

Настраиваемый диапазон: 1~2000000000.

Значение по умолчанию: см табл. ниже.

Стоимость пути по умолчанию для общих портов:

Тип порта	Стоимость пути по умолчанию	Рекомендованный диапазон
10 Мбит/с	2000000	2000000~20000000
100 Мбит/с	200000	200000~2000000
1 Гбит/с	20000	20000~200000

Стоимость пути по умолчанию для портов агрегации:

Тип порта	Номер порта агрегации	Рекомендация
10 Мбит/с	N	2000000/N
100 Мбит/с	N	200000/N
1 Гбит/с	N	20000/N

Описание: Настройка стоимости пути для порта в удаленном экземпляре. Стоимость пути порта используется для расчета оптимального пути. Этот параметр зависит от полосы пропускания. Чем больше пропускная способность, тем ниже стоимость. Изменение стоимости пути порта может изменить путь передачи данных между устройством и корневым мостом, тем самым изменив роль порта. Порт с поддержкой MSTP может быть настроен с разной стоимостью пути в разных экземплярах связующего дерева.



9. Настройка временных параметров MSTP.

MSTP Time Config

OperationType	Set
MSTP Forward Time Config	15
MSTP Hello Time	2
MSTP Maxage Time	20
MSTP Max Hop	20

Apply

Рис. 113. Настройка временных параметров MSTP

Выбор рабочего режима (Operation type)

Настраиваемые опции: Set/Default (Настроить/По умолчанию).

Описание: Выбор рабочего режима временных параметров MSTP.

Настройка времени пересылки (MSTP Forward Time Config)

Настраиваемый диапазон: 4~30 сек.

Значение по умолчанию: 15 сек.

Описание: Настройка интервала времени переходного состояния порта (отбрасывание-изучение или изучение-пересылка).

Время параметра Hello (MSTP Hello Time)

Настраиваемый диапазон: 1~10 сек.

Значение по умолчанию: 2 сек.

Описание: Настройка временного интервала отправки настроек BPDU.

Максимальное время старения (MSTP Max Age Time)

Настраиваемый диапазон: 6~40 сек.

Значение по умолчанию: 20 сек.

Описание: Настройка максимального возраста пакетов BPDU.



- Значения «Forward Delay Time», «Hello Time» и «Max Age Time» должны соответствовать следующим условиям: $2 \times (\text{Forward Delay Time} - 1.0 \text{ секунда}) \geq \text{Max Age Time}$; $\text{Max Age Time} \geq (\text{Hello Time} + 1.0 \text{ секунд})$.
- Рекомендуется использовать значения по умолчанию.

Максимальное количество хопов MSTP (MSTP Max Hop)

Настраиваемый диапазон: 6~40.

Значение по умолчанию: 20.

Описание: Настройка максимального количества хопов региона MST. Максимальное количество хопов в регионе MST ограничивают масштаб региона MST; максимальное количество хопов регионального корня является максимальным количеством хопов региона MST.

Начиная от корневого моста связующего дерева в регионе MST, номер хопа уменьшается на 1, когда пакет BPDU транслируется через устройство в регионе. Устройство отбрасывает BPDU с номером хопа 0.



- Действительна только максимальная конфигурация хоба корневого моста MST региона. Устройство без корневого моста использует максимальную конфигурацию хоба корневого моста.
- Рекомендуется использовать значения по умолчанию.

10. Настройка быстрой передачи MSTP.

MSTP Fast Transfer Config

OperationType	Add
Port	FE3
MSTP Port Link Type	AUTO
Set/Cancel Marginal Port	Ordinary port

Apply

Рис. 114. Настройка быстрой передачи MSTP

Выбор рабочего режима (Operation type)

Настраиваемые опции: Add/Default (Добавить/По умолчанию).

Описание: Выбор рабочего режима быстрой передачи MSTP.

Настройка портов (Port)

Настраиваемые опции: все порты коммутатора.

Настройка режима связи порта (MSTP Port Link Type)

Настраиваемые опции: AUTO/Force True/Force False.

Значение по умолчанию: AUTO.

Описание: Настройка режима связи порта. Если порт подключен в режиме «точка-точка», для порта доступен режим быстрой передачи.

AUTO: означает, что коммутатор автоматически определит тип канала связи в соответствии с режимом работы порта (дуплекс/полудуплекс). Когда порт работает в дуплексном режиме, протокол MSTP автоматически предполагает, что канал связи, подключенный к порту, работает в режиме «точка-точка». Когда порт настроен на работу в полудуплексном режиме, протокол MSTP автоматически предполагает, что канал связи, подключенный к порту, является общим каналом.

Force True: означает, что канал связи, подключенный к локальному порту, работает в режиме «точка-точка».

Force False: означает, что канал связи, подключенный к локальному порту, является общим каналом.

Назначение/Отмена граничного порта (Set/Cancel Marginal Port)

Настраиваемые опции: Marginal port/Ordinary port (Граничный порт/Обычный порт).

Значение по умолчанию: Ordinary port (Обычный порт).

Описание: Настройка порта в режиме граничного порта или обычного порта. Когда порт напрямую подключен к оконечным устройствам, и при этом не подключен к каким-либо другим устройствам или открытым сегментам сети, этот порт является граничным портом.



Состояние граничного порта может без задержки осуществлять переход от блокировки к пересылке. Как только граничный порт получает пакет BPDU, состояние порта будет изменено на обычный порт.

11. Просмотр конфигурации MSTP.

```

Information Display
-- MSTP Bridge Config Info --
Bridge MAC : 00:1e:cd:17:c0:67
Bridge Times : Max Age 20, Hello Time 2, Forward Delay 15
Force Version: 3
##### Instance 0 #####
Self Bridge Id : 32768 - 00:1e:cd:17:c0:67
Root Id : this switch
Ext.RootPathCost : 0
Region Root Id : this switch
Int.RootPathCost : 0
Root Port ID : 0
Current port list in Instance 0:
10 1 (Total 2)
PortName ID ExtRPC IntRPC State Role DsgBridge DsgPort
-----
10 128.010 0 0 FWD DSGN 32768.001ecd17c067 128.010
1 128.001 0 0 FWD DSGN 32768.001ecd17c067 128.001
##### Instance 2 #####
Self Bridge Id : 32768.00:1e:cd:17:c0:67
Region Root Id : this switch
Int.RootPathCost : 0
Root Port ID : 0
Current port list in Instance 2:
(Total 0)
PortName ID IntRPC State Role DsgBridge DsgPort
-----
##### Instance 3 #####
Self Bridge Id : 32768.00:1e:cd:17:c0:67
Region Root Id : this switch
Int.RootPathCost : 0
Root Port ID : 0
Current port list in Instance 3:
(Total 0)
PortName ID IntRPC State Role DsgBridge DsgPort
-----

```

Рис. 115. Конфигурация MSTP

6.19.5. Пример типовой настройки

Как показано на рис. 116, коммутаторы А, В, С и D относятся к одному и тому же региону MST. VLAN, отмеченные красным цветом, означают, что пакеты VLAN могут быть переданы по соответствующим каналам связи. После того, как настройка будет выполнена, пакеты VLAN могут быть отправлены по разным инстансам связующего дерева. Пакеты VLAN 10 пересылаются по инстансу 1, при этом корневой мост инстанса 1 - это коммутатор А; пакеты VLAN 30 пересылаются по инстансу 3, а корневой мост инстанса 3 - это коммутатор В. Пакеты VLAN 40 пересылаются по инстансу 4, а корневой мост инстанса 4 - это коммутатор С. Пакеты VLAN 20 пересылаются по инстансу 0, а корневым мостом инстанса 0 является коммутатор В.

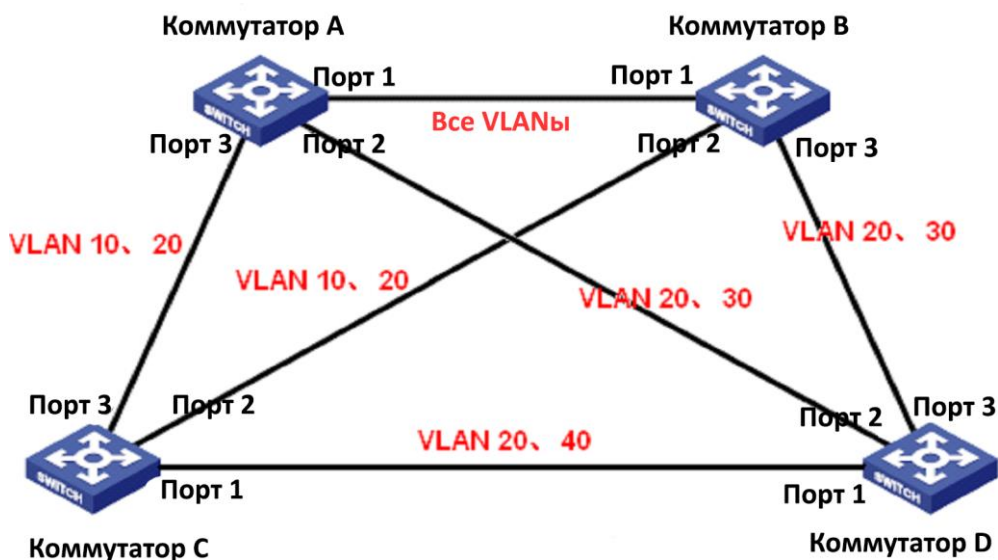


Рис. 116. Типовой пример настройки MSTP

Настройка коммутатора А:

1. Создайте VLAN 10, 20 и 30 на коммутаторе А. Настройте порты, чтобы разрешить прохождение пакетов соответствующих VLAN.
2. Включите протокол MSTP глобально (см. рис. 105).
3. Присвойте региону MST имя «Region», а уровню изменения параметров конфигурации установите значение «0» (см. рис. 109).
4. Создайте инстансы 1, 3, 4 и присвойте соответствия VLAN 10, 30, 40 инстансам 1, 3, 4 соответственно (см. рис. 110).
5. Установите для коммутатора приоритет моста в инстансе 1 равным 4096, а для других инстансов приоритет должен быть установлен «по умолчанию» (см. рис. 111).

Настройка коммутатора В:

6. Создайте VLAN 10, 20 и 30 на коммутаторе В. Настройте порты, чтобы разрешить прохождение пакетов соответствующих VLAN.
7. Включите протокол MSTP глобально (см. рис. 105).
8. Присвойте региону MST имя «Region», а уровню изменения параметров конфигурации установите значение «0» (см. рис. 109).
9. Создайте инстансы 1, 3, 4 и присвойте соответствия VLAN 10, 30, 40 инстансам 1, 3, 4 соответственно (см. рис. 110).
10. Установите для коммутатора приоритет моста в инстансе 3 равным 4096, а для других инстансов приоритет должен быть установлен «по умолчанию» (см. рис. 111).

Настройка коммутатора С:

11. Создайте VLAN 10, 20 и 30 на коммутаторе С. Настройте порты, чтобы разрешить прохождение пакетов соответствующих VLAN.
12. Включите протокол MSTP глобально (см. рис. 105).
13. Присвойте региону MST имя «Region», а уровню изменения параметров конфигурации установите значение «0» (см. рис. 109).



14. Создайте инстансы 1, 3, 4 и присвойте соответствия VLAN 10, 30, 40 инстансам 1, 3, 4 соответственно (см. рис. 110).
15. Установите для коммутатора приоритет моста в инстансе 4 равным 4096, а для других инстансов приоритет должен быть установлен «по умолчанию» (см. рис. 111).

Настройка коммутатора D:

16. Создайте VLAN 10, 20 и 30 на коммутаторе D. Настройте порты, чтобы разрешить прохождение пакетов соответствующих VLAN.
17. Включите протокол MSTP глобально (см. рис. 105).
18. Присвойте региону MST имя «Region», а уровню изменения параметров конфигурации установите значение «0» (см. рис. 109).
19. Создайте инстансы 1, 3, 4 и присвойте соответствия VLAN 10, 30, 40 инстансам 1, 3, 4 соответственно (см. рис. 110).

Когда расчет MSTP будет завершен, MSTI каждой VLAN будут следующими:

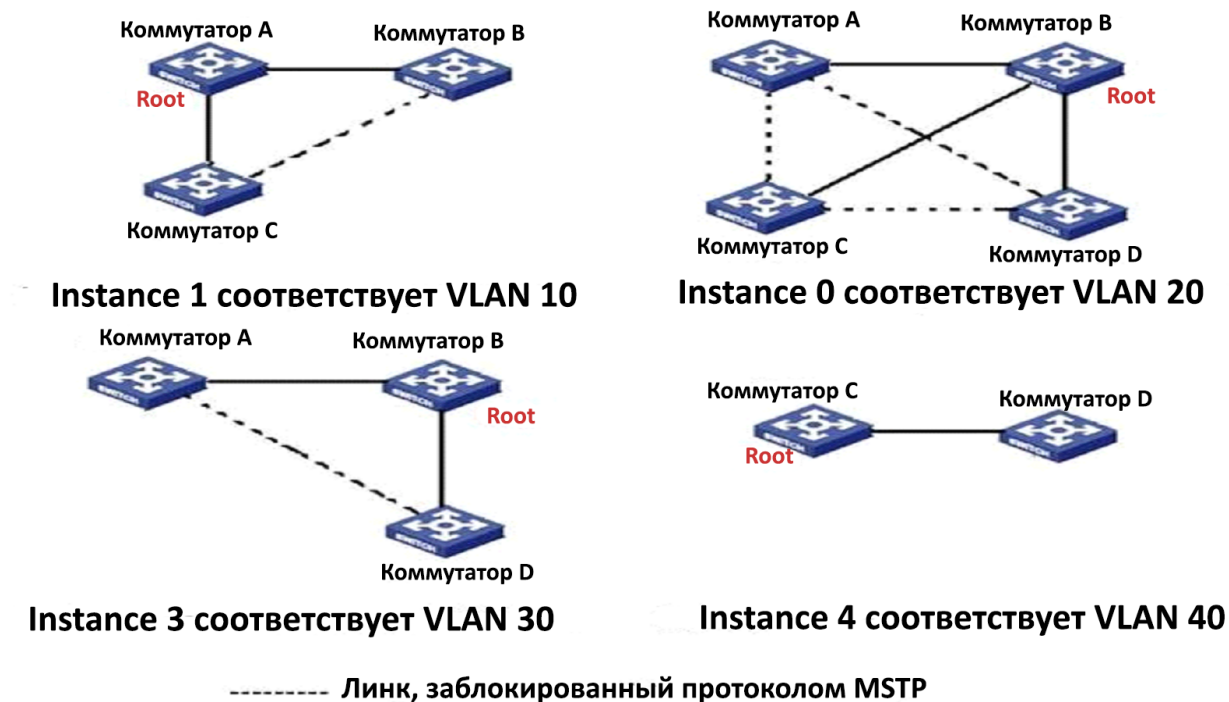


Рис. 117. Инстансы связующих деревьев каждой VLAN

6.20. Аварийная сигнализация (Alarm)

6.20.1. Введение

Данная серия коммутаторов поддерживает следующие типы аварийной сигнализации:

- Аварийная сигнализация при конфликте IP и/или MAC адресов (IP/MAC conflict alarm): если данная функция включена, аварийная сигнализация будет срабатывать в случае, если в сети будут обнаружены одинаковые IP и/или MAC адреса;



- Аварийная сигнализация электропитания (Power alarm): если включена данная функция, аварийная сигнализация будет срабатывать в случае проблем с одним из источников электропитания;
- Аварийная сигнализация порта (Port alarm): если включена данная функция, аварийная сигнализация будет срабатывать в случае получении информации об отключении соответствующего порта (состояние Link Down).
- Аварийная сигнализация кольца (Ring alarm): если включена данная функция, аварийная сигнализация будет срабатывать в случае нарушения кольцевой топологии, т.к. размыкании кольца.



Только один «мастер» кольца протокола Sy2-Ring поддерживается функцией аварийной сигнализации кольца.

6.20.2. Настройка через WEB-интерфейс

1. Настройка аварийной сигнализации.

IP, MAC Conflict

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

Port Alarm

Port	Alarm Status	Port	Alarm Status	Port	Alarm Status	Port	Alarm Status
FE1	<input checked="" type="checkbox"/>	FE2	<input type="checkbox"/>	FE3	<input type="checkbox"/>	FE4	<input type="checkbox"/>
FE5	<input checked="" type="checkbox"/>	FE6	<input type="checkbox"/>	FE7	<input type="checkbox"/>	FE8	<input type="checkbox"/>
FE9	<input type="checkbox"/>	FE10	<input type="checkbox"/>	FE11	<input type="checkbox"/>	FE12	<input type="checkbox"/>
FE13	<input type="checkbox"/>	FE14	<input type="checkbox"/>	FE15	<input type="checkbox"/>	FE16	<input type="checkbox"/>
FX17	<input type="checkbox"/>	FX18	<input type="checkbox"/>	FX19	<input type="checkbox"/>	FX20	<input type="checkbox"/>

SY2-RING Alarm

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

Apply

Рис. 118. Настройка аварийной сигнализации (SEWM20-D)



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"/>

Port Alarm

Port	Alarm Status	Port	Alarm Status	Port	Alarm Status	Port	Alarm Status
FE1	<input checked="" type="checkbox"/>	FE2	<input checked="" type="checkbox"/>	FE3	<input type="checkbox"/>	FE4	<input type="checkbox"/>
FE5	<input type="checkbox"/>	FE6	<input type="checkbox"/>	FE7	<input type="checkbox"/>	FE8	<input type="checkbox"/>
FE9	<input type="checkbox"/>	FE10	<input type="checkbox"/>	FE11	<input type="checkbox"/>	FE12	<input type="checkbox"/>
FE13	<input type="checkbox"/>	FE14	<input type="checkbox"/>	FE15	<input type="checkbox"/>	FE16	<input type="checkbox"/>
FE17	<input type="checkbox"/>	FE18	<input type="checkbox"/>	FE19	<input type="checkbox"/>	FE20	<input type="checkbox"/>
FE21	<input type="checkbox"/>	FE22	<input type="checkbox"/>	FX23	<input type="checkbox"/>	FX24	<input type="checkbox"/>

SY2-RING Alarm

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

Apply

Рис. 119. Настройка аварийной сигнализации (SEWM228GS)

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"/>

Port Alarm

Port	Alarm Status	Port	Alarm Status	Port	Alarm Status	Port	Alarm Status
FE1	<input checked="" type="checkbox"/>	FE2	<input type="checkbox"/>	FE3	<input type="checkbox"/>	FE4	<input type="checkbox"/>
FE5	<input checked="" type="checkbox"/>	FE6	<input type="checkbox"/>	FE7	<input type="checkbox"/>	FE8	<input type="checkbox"/>
FE9	<input type="checkbox"/>	FE10	<input type="checkbox"/>	FE11	<input type="checkbox"/>	FE12	<input type="checkbox"/>
FE13	<input type="checkbox"/>	FE14	<input type="checkbox"/>	FE15	<input type="checkbox"/>	FE16	<input type="checkbox"/>
FE17	<input type="checkbox"/>	FE18	<input type="checkbox"/>	FE19	<input type="checkbox"/>	FE20	<input type="checkbox"/>
FE21	<input type="checkbox"/>	FE22	<input type="checkbox"/>	FE23	<input type="checkbox"/>	FE24	<input type="checkbox"/>

Apply

Рис. 119. Настройка аварийной сигнализации (SEWM228M)



Аварийная сигнализация при конфликте IP и/или MAC адресов (IP/MAC conflict)

Настраиваемые опции: Select/Deselect (Включить/Выключить).

Значение по умолчанию: Select (Включено).

Описание: Включение/Выключение аварийной сигнализации при конфликте IP и/или MAC адресов.

Интервал времени (Alarm Time)

Настраиваемый диапазон: 180~600 сек.

Значение по умолчанию: 300 сек.

Описание: Настройка интервала времени для определения конфликта IP и/или MAC адресов.

Аварийная сигнализация порта (Port Alarm)

Настраиваемые опции: Select/Deselect (Включить/Выключить).

Значение по умолчанию: Deselect (Выключено).

Описание: Включение/Выключение аварийной сигнализации порта.

Аварийная сигнализация кольца (Sy2-Ring Alarm)

Настраиваемые опции: Select/Deselect (Включить/Выключить).

Значение по умолчанию: Deselect (Выключено).

Описание: Включение/Выключение аварийной сигнализации при работе протокола Sy2-Ring.

2. Отображение статуса аварийной сигнализации после включения функции извещения о тревогах.

Basic Vision

Alarm Title	Alarm Status
IP Alarm	Alarm
MAC Alarm	Normal

Port Alarm

Port	Alarm Status	Port	Alarm Status	Port	Alarm Status	Port	Alarm Status
FE1	Link Up	FE2	-	FE3	-	FE4	-
FE5	Link Down	FE6	-	FE7	-	FE8	-
FE9	-	FE10	-	FE11	-	FE12	-
FE13	-	FE14	-	FE15	-	FE16	-
FX17	-	FX18	-	FX19	-	FX20	-

SY2-RING Alarm

DT-RING ID	Alarm Status
1	Ring Open

Рис. 120. Отображение статуса аварийной сигнализации (SEWM20-D)



Basic Vision

Alarm Title	Alarm Status
IP Alarm	Alarm
MAC Alarm	Normal

Port Alarm

Port	Alarm Status	Port	Alarm Status	Port	Alarm Status	Port	Alarm Status
FE1	Link Up	FE2	-	FE3	-	FE4	-
FE5	Link Down	FE6	-	FE7	-	FE8	-
FE9	-	FE10	-	FE11	-	FE12	-
FE13	-	FE14	-	FE15	-	FE16	-
FX17	-	FX18	-	FX19	-	FX20	-

SY2-RING Alarm

DT-RING ID	Alarm Status
1	Ring Open

Рис. 121. Отображение статуса аварийной сигнализации (SEWM228GS)

Basic Vision

Alarm Title	Alarm Status
power	WARN
IP Alarm	Alarm
MAC Alarm	Normal

Port Alarm

Port	Alarm Status	Port	Alarm Status	Port	Alarm Status	Port	Alarm Status
FE1	Link Down	FE2	-	FE3	-	FE4	-
FE5	Link Up	FE6	-	FE7	-	FE8	-
FE9	-	FE10	-	FE11	-	FE12	-
FE13	-	FE14	-	FE15	-	FE16	-
FE17	-	FE18	-	FE19	-	FE20	-
FE21	-	FE22	-	FE23	-	FE24	-

Рис. 122. Отображение статуса аварийной сигнализации (SEWM228M)

Статус аварийной сигнализации электропитания (Power Alarm Status)

Отображаемые опции: Normal/WARN

Описание: После включения функции аварийной сигнализации электропитания состояние Normal отображается, если включены два источника питания, а состояние WARN отображается, если включен один источник питания.

Статус аварийной сигнализации при конфликте IP и/или MAC адресов (IP/MAC conflict Alarm)

Отображаемые опции: Normal/Alarm.

Описание: Если присутствует конфликт IP и/или MAC адресов, будет отображаться сообщение аварийной сигнализации; в противном случае отображается состояние «Normal».



Статус аварийной сигнализации порта (Port Alarm)

Отображаемые опции: Link Up/Link Down

Описание: После того, как функция аварийной сигнализации порта активирована, состояние «Link Up» отображается, если порт функционирует в нормальном режиме, а если на порту отсутствует соединение или обнаруживается аномальное соединение, тогда отображается состояние «Link Down».

Статус аварийной сигнализации кольца (Sy2-Ring Alarm)

Настраиваемые опции: Ring Open/Ring Close

Описание: После того, как функция аварийной сигнализации кольца включена, состояние «Ring Close» будет отображаться, если кольцо находится в закрытом, т.е. работоспособном, состоянии, а если в топологии кольца обнаружена коллизия, т.е. кольцо разомкнуто, отображается состояние «Ring Open».

6.21. Аварийная сигнализация передачи трафика на порту (Port Traffic Alarm)

6.21.1. Введение

С помощью функции аварийной сигнализации передачи трафика на порту коммутатор генерирует сигнал тревоги, если скорость трафика порта превышает обозначенное пороговое значение или возникает ошибка CRC.



- Информация об аварийной ситуации генерируется только в том случае, если данная функция включена на порту.
- Данная функция имеет специфику различия направления движения трафика на порту. Входящий и исходящий трафик соответствует различным аварийным сигналам.
- Если возникает ошибка CRC, генерируется сигнал ошибки CRC.

6.21.2. Настройка через WEB-интерфейс

1. Настройка аварийной сигнализации передачи трафика на порту

Port	FE1	▼
Alarm Type	Input Rate	▼
Alarm Status	enable	▼
Alarm Threshold	1000	bps ▼

Apply

Refresh

Рис. 123. Настройка аварийной сигнализации передачи трафика на порту

Настройка порта (Port)

Настраиваемые опции: Все порты коммутатора.

Описание: Выбор портов, на которых будет настроена аварийная сигнализация передачи трафика.



Настройка типа аварийной сигнализации (Alarm Type)

Отображаемые опции: Input Rate/Output Rate/CRC Error (Входящий трафик/Исходящий трафик/Ошибки CRC).

Описание: Настройка типа аварийной сигнализация передачи трафика.

Настройка статуса аварийной сигнализации (Alarm Status)

Отображаемые опции: Enable/Disable (Включено/Выключено)

Значение по умолчанию: Disable (Выключено)

Описание: Включение/Выключение типа аварийной сигнализации.

Настройка порогового значения (Alarm Threshold)

Настраиваемый диапазон: 1~1000000000 бит/с или 1~1000000 Кбит/с.

Описание: Настройка порогового значения скорости трафика.

2. Отображение информации аварийной сигнализации передачи трафика на порту.

Port	Input Rate		Alarm Status	Output Rate		Alarm Status	Error CRC	Alarm Status
FE1	enable	1000bps	alarm	enable	100bps	alarm	enable	alarm
FE2	enable	1000000000bps	normal	enable	1000000000bps	normal	enable	normal
FE3	disable	-	-	disable	-	-	disable	-
FE4	disable	-	-	disable	-	-	disable	-
FE5	disable	-	-	disable	-	-	disable	-
FE6	disable	-	-	disable	-	-	disable	-
FE7	disable	-	-	disable	-	-	disable	-
FE8	disable	-	-	disable	-	-	disable	-
FE9	disable	-	-	disable	-	-	disable	-
FE10	disable	-	-	disable	-	-	disable	-
FE11	disable	-	-	disable	-	-	disable	-
FE12	disable	-	-	disable	-	-	disable	-
FE13	disable	-	-	disable	-	-	disable	-
FE14	disable	-	-	disable	-	-	disable	-
FE15	disable	-	-	disable	-	-	disable	-
FE16	disable	-	-	disable	-	-	disable	-
FX17	disable	-	-	disable	-	-	disable	-
FX18	disable	-	-	disable	-	-	disable	-
FX19	disable	-	-	disable	-	-	disable	-
FX20	disable	-	-	disable	-	-	disable	-

Рис. 124. Отображение информации аварийной сигнализации передачи трафика на порту

6.22. GMRP

6.22.1. GARP

Протокол GARP (Generic Attribute Registration Protocol) используется для распространения, регистрации и удаления определённой информации (VLAN, адреса мультикастовых групп) между коммутаторами в сети.

Благодаря механизму GARP, информация о настройках коммутатора может быть передана по всей локальной сети. Устройства, поддерживающие GARP, передают друг другу инструкции о регистрации или отмене тех или иных настроек путём отправки соответствующих сообщений «Join» и «Leave». При этом GARP может регистрировать или отменять информацию о настройках других членов в соответствии с их сообщениями «Join/ Leave».

GARP предусматривает три типа сообщений: «Join», «Leave» и «Leave All».



- Когда GARP устройство хочет передать свои настройки другим коммутаторам, оно отправляет сообщение «Join». Сообщения «Join» бывают двух типов: «Join Empty» и «Join In». Сообщение «Join In» отправляется для зарегистрированных настроек, в то время как «Join Empty» - для настроек, которые ещё не были зарегистрированы.
- Когда GARP устройство хочет удалить свои настройки с других коммутаторов, оно отправляет сообщение «Leave».
- После запуска GARP, он начинает отсчитывать период «Leave All». Когда период заканчивается, устройство отправляет сообщение «Leave All».



В качестве приложения указывается порт с поддержкой GARP.

Таймеры GARP включают таймеры «Hold», «Join», «Leave» и «Leave All».

- Таймер Hold (Hold Timer): При получении сообщения о регистрации настроек, приложение GARP не отправляет сообщение «Join» сразу, а запускает таймер «Hold». Когда таймер заканчивает отсчёт, приложение отправляет все полученные сообщения о настройках, полученные за этот период в одном «Join» сообщении, что уменьшает количество передаваемых данных по сети.
- Таймер Join (Join Timer): Чтобы гарантировать, что сообщения «Join» может быть надёжно передано другим коммутаторам, коммутатор с включенным GARP будет ожидать временной интервал таймера «Join» после передачи первого сообщения «Join». Если в течение в ответ не получено сообщение «JoinIn», приложение снова отправляет сообщение «Join». В противном случае, сообщение «Join» не отправляется.
- Таймер Leave (Leave Timer): Когда коммутатор с включенным GARP хочет, чтобы другие коммутаторы удалили информацию о настройках, он отправляет «Leave» сообщение. Коммутаторы, получившее это сообщение, запускают таймер «Leave». Если они не получают ни одного сообщения «Join» до истечения времени таймера, коммутаторы удаляют эту информацию о настройках.
- Таймер Leave All (LeaveAll Timer): При запуске GARP приложения, запускается таймер «Leave All». По его истечении, приложение отправляет сообщение «Leave All» другим коммутаторам с включенным GARP для того, чтобы они могли перерегистрировать всю свою информацию о настройках. После этого, приложение запускает таймер LeaveAll заново, чтобы начать новый цикл.

6.22.2. Протокол GMRP

GARP Multicast Registration Protocol (GMRP) - протокол регистрации многоадресной передачи, основанный на принципах GARP. Он используется для управления информацией о многоадресных группах коммутаторов. 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 многоадресных группах для всех коммутаторов сети.

Если коммутатор регистрирует или отменяет регистрацию в многоадресной группе, порт с поддержкой GMRP передаёт информацию на другие порты в том же VLAN.



6.22.3. Описание

Порт-агент (Agent port): обозначает порт, на котором включены функции GMRP и агента.

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

Для GMRP необходимо наличие одного и нескольких портов-агентов. Динамически полученные многоадресные записи GMRP и информация об агенте передаётся портом распространения на порты распространения следующих устройств.

Все таймеры GMRP одной сети должны подчиняться одним и тем же правилам во избежание взаимоисключений. Таймеры должны следовать следующим правилам: таймер «Hold» < таймер «Join», $2 * \text{таймер «Join»} < \text{таймер «Leave»}$, а таймер «Leave» < таймер «Leave All».

6.22.4. Настройка через WEB-интерфейс

1. Включите протокол GMRP, как показано на рис. 125.

Protocol Configure	
GMRP State	Enable
LeaveAll Timer	10000 ms

Apply

Рис. 125. Включение/Выключение GMRP

Функция GMRP (GMRP State)

Настраиваемые опции: Enable/Disable (Включить/Выключить)

Значение по умолчанию: Disable (Выключено)

Описание: Включение/выключение функции GMRP. Протокол не может работать одновременно с протоколом IGMP Snooping.

Таймер Leave-All (LeaveAll Timer)

Настраиваемый диапазон: 100~327600 мс.

Значение по умолчанию: 10000 мс.

Описание: Настройка временного интервала для отправки сообщений «Leave All». Интервал должен быть кратен 100. Если на разных устройствах таймеры «Leave All» истекнут одновременно, они отправят множество сообщений «Leave All» одновременно. Для того чтобы избежать подобной ситуации, которая может повысить нагрузку на сеть, рабочее значение таймеров «Leave All» должно быть случайным значением, которое больше изначального значения таймера «Leave All», но меньше чем 1,5 значения этого таймера.



2. Настройка функции GMRP для каждого порта.

Port Configure

Port	GMRP Enable	Agent Enable	Hold Timer	Join Timer	Leave Timer
FE1	Enable	Enable	100 ms	500 ms	3000 ms
FE2	Enable	Disable	100 ms	500 ms	3000 ms
FE3	Enable	Disable	100 ms	500 ms	3000 ms
FE4	Disable	Disable	100 ms	500 ms	3000 ms
FE5	Disable	Disable	100 ms	500 ms	3000 ms
FE6	Disable	Disable	100 ms	500 ms	3000 ms
FE7	Disable	Disable	100 ms	500 ms	3000 ms
FE8	Disable	Disable	100 ms	500 ms	3000 ms
FE9	Disable	Disable	100 ms	500 ms	3000 ms
FE10	Disable	Disable	100 ms	500 ms	3000 ms
FE11	Disable	Disable	100 ms	500 ms	3000 ms
FE12	Disable	Disable	100 ms	500 ms	3000 ms
FE13	Disable	Disable	100 ms	500 ms	3000 ms
FE14	Disable	Disable	100 ms	500 ms	3000 ms
FE15	Disable	Disable	100 ms	500 ms	3000 ms
FE16	Disable	Disable	100 ms	500 ms	3000 ms
FX17	Disable	Disable	100 ms	500 ms	3000 ms
FX18	Disable	Disable	100 ms	500 ms	3000 ms
FX19	Disable	Disable	100 ms	500 ms	3000 ms
FX20	Disable	Disable	100 ms	500 ms	3000 ms

Apply

Рис. 126. Настройка GMRP на портах

Включение GMRP на порту (GMRP Enable)

Настраиваемые опции: Enable/Disable (Включить/Выключить)

Значение по умолчанию: Disable (Выключено)

Описание: Включение или выключение функции GMRP на порту

Включение агента GMRP (Agent Enable)

Варианты: Enable/Disable (Включить/Выключить)

По умолчанию: Disable (Выключено)

Описание: Включение или выключение функции агента GMRP на порту



- Порт-агент не может распространять информацию об агенте.
- До включения функции GMRP агента нужно включить функцию GMRP на данном порту.

Таймер Hold (Hold Timer)

Настраиваемый диапазон: 100~327600 мс.

Значение по умолчанию: 100 мс.

Описание: Значение должно быть кратно 100. Рекомендуется устанавливать одинаковое значение для всех GMRP портов.

Таймер Join (Join Timer)

Настраиваемый диапазон: 100~327600 мс.



Значение по умолчанию: 500 мс.

Описание: Значение должно быть кратно 100. Рекомендуется устанавливать одинаковое значение для всех GMRP портов.

Таймер Leave (Leave Timer)

Настраиваемый диапазон: 100~327600 мс.

Значение по умолчанию: 3000 мс.

Описание: Значение должно быть кратно 100. Рекомендуется устанавливать одинаковое значение для всех GMRP портов.

3. Добавление записи GMRP агента.

GMRP Agent Set

MAC	<input type="text" value="010000000001"/>	
VLAN ID	<input type="text" value="1"/>	(1-4093)

Port List

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

<p style="text-align: center; font-weight: bold; font-size: small;">Member Port List</p> <div style="border: 1px solid gray; height: 100px; position: relative;"> <div style="position: absolute; top: 5px; left: 5px; background-color: #d9ead3; padding: 2px;">FE1</div> </div>	<div style="border: 1px solid gray; width: 20px; height: 20px; margin: 5px auto; background-color: #333; color: white; line-height: 20px;"><<</div> <div style="border: 1px solid gray; width: 20px; height: 20px; margin: 5px auto; background-color: #333; color: white; line-height: 20px;">>></div>	<p style="text-align: center; font-weight: bold; font-size: small;">Source Port List</p> <div style="border: 1px solid gray; height: 100px; position: relative;"> <div style="position: absolute; top: 5px; left: 5px; background-color: #d9ead3; width: 100%; height: 100%;"></div> </div>
---	---	---

Рис. 127. Настройка записи GMRP агента

MAC адрес (MAC)

Настраиваемый формат: FF-FF-FF-FF-FF-FF (F - это шестнадцатеричное число)

Описание: Настройка MAC-адреса многоадресной группы. Наименее значимый бит первого байта равен 1.

Идентификатор VLAN (VLAN ID)

Настраиваемые опции: все созданные идентификаторы VLAN

Описание: Настройка идентификатора VLAN для записей агента GMRP. Запись агента GMRP может быть отправлена только из порта распространения, идентификатор VLAN которого совпадает с идентификатором агента.

Список портов участников (Member Port List)

Выбор портов участников записей агента и выбор портов агента. Порт можно выбрать только из портов с поддержкой агента GMRP.

Список портов источников (Source Port List)

Настраиваемые опции: все порты с поддержкой GMRP агента.



4. Отображение, изменение и удаление записей агентов GMRP.

GMRP Agent List

Index	MAC	VLAN ID	Member Port
1	01-00-00-00-00-01	1	FE1
2	01-00-00-00-00-02	2	FE1

Рис. 128. Операции с записями агентов GMRP

Записи агента GMRP содержат MAC адреса агента, идентификаторы VLAN и информацию о портах участника. Нажмите <Delete> для удаления соответствующей записи; нажмите <Modify> для изменения портов участников записи агента.

5. Проверка участников многоадресных групп агента на подключенном соседнем устройстве.

Их статус должен удовлетворять следующим условиям:

- На подключенных устройствах должна быть включена функция GMRP.
- Два порта, которые соединяют два устройства, должны быть портами распространения, а идентификатор VLAN порта распространения на локальном устройстве должен быть идентичен идентификатору в записи агента.

GMRP Dynamic Multicast List

Index	Multicast MAC	VLAN ID	Member Port
1	01-00-00-00-00-01	1	FE2

Рис. 129. Таблица многоадресных динамических GMRP

Список многоадресных динамических GMRP (GMRP Dynamic Multicast List)

Групповое отображение: {Index, Multicast MAC, VLAN ID, Member Port}

Описание: Отображение многоадресных динамических записей GMRP.

6.22.5. Пример типовой настройки

Как показано на рисунке 130, коммутаторы А и В соединены между собой портом 2 каждый. Порт 1 коммутатора А настроен как порт-агент и содержит две многоадресных записи:

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

Для того, чтобы увидеть динамическую регистрацию между коммутаторами и обновление информации о многоадресной рассылке, необходимо установить различные значение VLAN для портов.

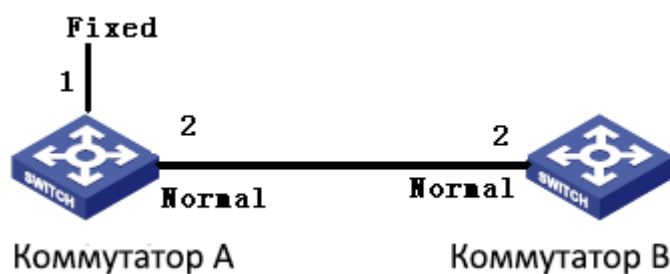


Рис. 130. Сеть GMRP

Настройка коммутатора А:

1. Включите функцию GMRP на коммутаторе А; используйте значение «По умолчанию» для таймера «Leave All» (см. рис. 125);
2. Включите функцию GMRP и функцию агента на порту 1; на порту 2 включите только функцию GMRP; все таймеры должны быть установлены в режим «По умолчанию» (см. рис. 126);
3. Настройте запись многоадресного агента. <MAC address, VLAN ID, Member port> настройте как <01-00-00-00-00-01, 1, 1> и <01-00-00-00-00-02, 2, 1> (см. рис. 127).

Настройка коммутатора В:

1. Включите функцию GMRP на коммутаторе В; используйте значение «По умолчанию» для таймера «Leave All» (см. рис. 125);
2. Включите функцию GMRP на порту 2; все таймеры должны быть установлены в режим «По умолчанию» (см. рис. 126);

Динамические записи многоадресной передачи GMRP в коммутаторе В показаны в таблице:

Свойства порта 2 коммутатора А	Свойства порта 2 коммутатора В	Многоадресные записи коммутатора-приемника 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



6.23. Протокол RMON (Remote Network Monitoring)

6.23.1. Введение

Протокол RMON (Remote Network Monitoring) основан на архитектуре SNMP и позволяет сетевым устройствам управления более интенсивно контролировать устройства. реализация протокола RMON основана на модели клиент/сервер и включает NMS (Network Management Station, Станция управления сетью), по сути являющейся сервером и специального Агента (Agent), который является клиентом. NMS управляет Агентом, который выполняет сбор статистики всех видов информации о трафике на порту.

Основные функции RMON – сбор статистики и сигнализация о тревогах. Функция сбора статистики предполагает, что агент может периодически выполнять сбор статистики всех видов информации о трафике на порте, например, получение информации о количестве сообщений, полученных в конкретном сегменте сети в течение конкретного периода времени. Функция сигнализации о тревогах обеспечивает выполнение агентом функций контроля за значениями указанных переменных MIB (Management Information Base) файлов. Когда значение достигает определенного порога (например, количество сообщений превышает указанное значение), агент может автоматически записывать события тревоги в журнал RMON или отправлять специальные Trap-сообщение на устройство управления.

6.23.2. Группы RMON (RMON Group)

Протокол RMON (стандарт RFC2819) подразделяется на несколько групп, которые включают: группу статистики (Statistics Group), группу истории (History Group), группу событий (Event Group) и группу тревог (Alarm Group) открытых MIB. Каждая группа поддерживает максимум 32 записи.

- Группа сбора статистики (Statistics Group)

Наличие данной группы подразумевает, что система может вести сбор статистики всех видов информации о трафике на порту. Статистическая информация содержит много разной информации: количество коллизий в сети, сообщения об ошибках CRC, информацию о сообщениях со слишком маленьким или слишком большим размерами данных, информацию о широковещательных и многоадресных сообщениях, количество полученных байт, количество принятых сообщений и т.д. После успешного создания записи статистики по указанному интерфейсу, данная группа подсчитывает количество сообщений на текущем интерфейсе, а результатом является непрерывное накопление значений статистики.

- Группа записи истории (History Group)

Система периодически просматривает выборку всех видов информации о трафике на порту и сохраняет значения выборки в таблице записей истории, следовательно устройство управления может просматривать эту информацию в любое время. Группа истории учитывает значения статистики всех видов данных в интервале выборки сообщений, полученных портом в каждом цикле приема/передачи информации, причем периодичность данных циклов можно настраивать.

- Группа контроля событий (Event group)



Группа событий используется для определения индексов событий и методов обработки событий. События, обработанные в группе событий, используются в элементе конфигурации группы тревог. Действие события начинается, когда контролируемое устройство достигает состояния тревоги.

Существует несколько способов обработки событий:

Журнал (Log): ведение журнала события и связанной с ним информации;

Прерывание (Trap): отправка Trap-сообщения в NMS и дальнейшее информирование о событии;

Log-Trap: запись и отправка Trap-сообщения;

Нет (None): не выполнять никаких действий

- Группа тревожной сигнализации (Alarm Group)

Функция управления тревожной сигнализации протокола RMON обеспечивает контроль за различными аварийными событиями. После того, как пользователь обнаружит запись аварийной сигнализации, система получит значения контролируемых переменных сигнала тревоги за определенный период. Когда значение переменной сигнала тревоги больше или равно пороговому значению, пользователь будет информирован о важности данного события. Когда значение переменной тревоги ниже порогового значения, пользователь будет информирован о второстепенном событии. Сообщения тревожной обрабатываются в соответствии с определением конкретного события.



Если выборочное значение переменной аварийного сигнала превышает пороговое значение несколько раз в одном и том же направлении, инициирование события о тревоге возможно только первый раз. Это означает, что увеличение количества тревог и уменьшение количества тревог чередуются.

6.23.3. Настройка через WEB-интерфейс

1. Настройка группы статистики.

Set Statistics Information

Index	Owner	DataSource
1	a	ifIndex.2

Apply

Рис. 131. Настройка статистики RMON

Индекс (Index)

Настраиваемый диапазон: 1~65535

Описание: Настройка номера (индекса) записи информации о статистике.

Владелец (Owner)

Настраиваемый диапазон: 1~32 символов

Описание: Настройка имени владельца записей информации о статистике.

Источник данных (Data Source)

Настраиваемые опции: ifIndex.portid

Описание: Выбор порта для сбора статистики.



2. Настройка группы записи истории.

Index	<input type="text" value="2"/>
DataSource	<input type="text" value="ifIndex.2"/> ▾
Owner	<input type="text" value="b"/>
Sampling Number	<input type="text" value="10"/>
Sampling Space	<input type="text" value="20"/>

Рис. 132. Настройка истории RMON

Индекс (Index)

Настраиваемый диапазон: 1~65535

Описание: Настройка индекса записи управления историей.

Источник данных (Data Source)

Настраиваемые опции: ifIndex.portid

Описание: Выбор порта для отбора записей управления историей.

Владелец (Owner)

Настраиваемый диапазон: 1~32 символов

Описание: Настройка имени владельца записей управления историей.

Номер выборки (Sampling Number)

Настраиваемый диапазон: 1~65535

Описание: Настройка номера выборки записей управления историей.

Интервал выборки (Sampling Space)

Настраиваемый диапазон (сек.): 1~3600

Описание: Настройка интервала выборки записей управления историей.

3. Настройка группы контроля событий.

Index	<input type="text" value="3"/>
Owner	<input type="text" value="c"/>
Event Type	<input type="text" value="NONE"/> ▾
Event Description	<input type="text" value="alarm"/>
Event Community	<input type="text" value="public"/>

Рис. 133. Настройка контроля событий RMON

Индекс (Index)

Настраиваемый диапазон: 1~65535

Описание: Настройка индекса записи контроля событий.



Владелец (Owner)

Настраиваемый диапазон: 1~32 символов

Описание: Настройка имени владельца записей контроля событий.

Тип события (Event Type)

Настраиваемые опции: NONE/LOG/Snmp-trap/log and Trap

Значение по умолчанию: NONE

Описание: Настройка типа события при возникновении тревоги. Это метод обработки сигналов тревоги.

Значение события (Event Description)

Настраиваемый диапазон: 1~32 символов

Описание: Настройка значения события.

Имя группы событий (Event Community)

Настраиваемый диапазон: 1~32 символов

Описание: Настройка имени группы, отправляющего события Trap, которые должны соответствовать группе с наименованием SNMP.

4. Настройка группы аварийной сигнализации.

Index	4
OID	1.3.6.1.2.1.2.2.1.10
Owner	d
DataSource	ifIndex.2
Sampling Type	Absolute
Alarm Type	RisingAlarm
Sampling Space	20
Rising Threshold	100
Falling Threshold	20
Rising EventIndex	3
Falling EventIndex	3

Apply

Рис. 134. Настройка аварийной сигнализации RMON – 1213 MIB узел



Index	5
OID	1.3.6.1.2.1.18.1.1.1.
Owner	e
Stat Group	1
Sampling Type	Absolute
Alarm Type	RisingAlarm
Sampling Space	20
Rising Threshold	100
Falling Threshold	20
Rising EventIndex	3
Falling EventIndex	3

Apply

Рис. 135. Настройка аварийной сигнализации RMON – RMON MIB узел

Индекс (Index)

Настраиваемый диапазон: 1~65535

Описание: Настройка индекса записи контроля аварийных сообщений.

Идентификатор объектов (OID)

Описание: Настройка номера OID текущего узла MIB.

Владелец (Owner)

Настраиваемый диапазон: 1~32 символов

Описание: Настройка имени владельца записей контроля аварийных сообщений.

Источник данных (Data Source)

Настраиваемые опции: ifIndex.portid

Описание: Выбор порта для контроля.

Группа статистики (Stat Group)

Настраиваемые опции: индексация записей в таблице статистики RMON.

Описание: Выбор записи статистики, по которой будет выполняться мониторинг порта.

Тип выборки (Sampling Type)

Настраиваемые опции: Absolute/Delta

Значение по умолчанию: Absolute

Описание: Выбор метода сравнения значения выборки и порогового значения. Absolute: прямое сравнение каждого значения выборки с пороговым значением; Delta: текущее значение выборки минус предыдущее значение выборки, затем используется разница для сравнения с пороговым значением.

Тип аварийной сигнализации (Alarm Type)

Настраиваемые опции: RisingAlarm/FallingAlarm/RisOrFallAlarm

Значение по умолчанию: RisingAlarm

Описание: Выбор типа аварийного сообщения.

**Интервал выборки (Sampling Space)**

Настраиваемый диапазон: 1~65535

Описание: Настройка периода выборки, оптимальное значение которого должно соответствовать значению интервала выборки записей управления историей.

Верхнее пороговое значение (Rising Threshold)

Настраиваемый диапазон: 0~65535

Описание: Настройка верхнего порогового значения. Когда значение выборки превышает пороговое значение, а тип сигнала тревоги установлен как RisingAlarm или RisOrFallAlarm, тревога будет активирована, кроме того активируется индекс события Rising.

Нижнее пороговое значение (Falling Threshold)

Настраиваемый диапазон: 0~65535

Описание: Настройка нижнего порогового значения. Когда значение выборки ниже порогового значения, а тип сигнала тревоги установлен как FallingAlarm или RisOrFallAlarm, тревога будет активирована, кроме того активируется индекс события Falling.

Индекс события Rising (Rising Event Index)

Настраиваемый диапазон: 0~65535

Описание: Настройка индекса события Rising. Это метод обработки возрастания аварийных событий.

Индекс события Falling (Falling Event Index)

Настраиваемый диапазон: 0~65535

Описание: Настройка индекса события Falling. Это метод обработки уменьшения аварийных событий.

6.24. Настройка одноадресной рассылки (Unicast)

6.24.1. Введение

Когда коммутатор пересылает сообщение, он для подтверждения номера порта назначения ищет в таблице MAC адресов соответствующий MAC адрес, для которого предназначено данное сообщение.

MAC адреса могут быть статическими и динамическими.

Значение статического MAC адреса устанавливается пользователем, имеет наивысший приоритет (он не может быть автоматически заменен динамическим MAC адресом) и является постоянно действующими.

Динамические MAC-адреса появляются в таблице во время проверки передаваемых данных. Они считаются достоверными только в течение определённого периода времени. Коммутатор периодически обновляет свою таблицу MAC-адресов. При получении кадра, коммутатор записывает в свою таблицу MAC-адрес отправителя, содержащийся в этом кадре, наряду с портом, на который кадр был получен, а затем проверяет в своей таблице наличие MAC-адрес назначения, также содержащийся в кадре. Если этот адрес присутствует в таблице, коммутатор передаёт данные на соответствующий порт. Если совпадения не найдено, коммутатор рассылает этот кадр на все порты.

Коммутаторы поддерживают максимум 256 статических одноадресных записей.



6.24.2. Настройка через WEB-интерфейс

1. Добавьте запись статического MAC адреса.

Set FDB Unicast

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

Apply

Рис. 136. Настройка записи статического одноадресного FDB

Настройка MAC адреса (MAC)

Настраиваемый формат: HH-HH-HH-HH-HH-HH (H означает шестнадцатеричное число).

Описание: Настройка одноадресного (Unicast) MAC адреса; младший бит в старшем байте равен 0.

Настройка идентификатора VLAN (VLAN ID)

Описание: Настройка идентификатора VLAN для соответствующего порта.

Настройка порта участника (Member Port)

Настраиваемые опции: Все порты коммутатора

Описание: Выбор порта для пересылки сообщения с данным MAC адресом назначения, при этом выбранный порт должен быть участником указанной выше VLAN.

2. Отображение статических одноадресных (Unicast) MAC адресов

FDB Unicast Mac List

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

Add
Delete
Modify

Рис. 137. Таблица статических FDB

Выберите в таблице запись для удаления или изменения параметров.

3. Отображение списка динамических одноадресных (Unicast) MAC адресов.



Dynamic Unicast Mac List

Index	MAC	VLAN ID	Member Port
1	00:0c:29:f1:68:d9	1	FE7
2	00:00:00:98:01:06	1	FE7
3	00:00:00:98:01:07	1	FE7
4	00:00:00:98:01:05	1	FE7
5	d0:67:e5:19:71:e2	1	FE7
6	00:0c:29:e5:73:fe	1	FE7
7	00:aa:bb:cc:cc:dd	1	FE7
8	00:00:00:98:00:54	1	FE7
9	80:c1:6e:fa:42:52	1	FE7
10	00:00:ff:ff:aa:96	1	FE7
11	c8:3a:35:d3:cd:13	1	FE7
12	d0:67:e5:20:16:c0	1	FE7
13	c8:9c:dc:a9:00:1c	1	FE7
14	c8:3a:35:d3:cd:b1	1	FE7

Рис. 138. Таблица динамических одноадресных FDB



7. Расшифровка аббревиатур

Аббревиатура	Полное наименование	Наименование на русском языке
ACL	Access Control List	Список контроля доступа
ARP	Address Resolution Protocol	Протокол определения адреса
BPDU	Bridge Protocol Data Unit	Протокол управления сетевыми мостами
CIST	Common and Internal Spanning Tree	Общее и внутреннее связующее дерево
CLI	Command Line Interface	Интерфейс командной строки
CRC	Cyclic Redundancy Check	Циклический избыточный код (алгоритм нахождения контрольной суммы, предназначенный для проверки целостности данных)
CST	Common Spanning Tree	Общее связующее дерево
DSCP	Differentiated Services Code Point	Точка кода дифференцированных услуг (элемент архитектуры компьютерных сетей, описывающий простой масштабируемый механизм классификации, управления трафиком)
FTP	File Transfer Protocol	Протокол передачи данных
GARP	Generic Attribute Registration Protocol	Протокол регистрации основных атрибутов
GMRP	GARP Multicast Registration Protocol	Протокол GARP для регистрации многоадресных групп
IGMP	Internet Group Management Protocol	Протокол управления группами Интернета (протокол управления групповой (multicast) передачей данных в сетях, основанных на протоколе IP)
IGMP Snooping	Internet Group Management Protocol Snooping	Протокол отслеживания сетевого трафика IGMP
IST	Internal Spanning Tree	Внутреннее связующее дерево
LLDP	Link Layer Discovery Protocol	Протокол обнаружения уровня канала
MAC	Media Access Control	Управление доступом к среде (обеспечивает адресацию и механизмы управления доступом к
MIB	Management Information Base	База управляющей информации



MSTI	Multiple Spanning Tree Instance	Инстанс множественного протокола связующего дерева
MSTP	Multiple Spanning Tree Protocol	Множественный протокол связующего дерева (В один инстанс MSTP могут входить несколько виртуальных сетей при условии, что их топология одинакова)
NMS	Network Management Station	Станция управления сетью
OID	Object Identifier	Идентификатор объекта
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)
STP	Spanning Tree Protocol	Протокол связующего дерева
TCP	Transmission Control Protocol	Протокол управления передачей
ToS	Type of Service	Тип сервиса
VLAN	Virtual Local Area Network	Виртуальная локальная сеть
WRR	Weighted Round Robin	Взвешенная очередь