

# Промышленный управляемый Ethernet коммутатор SWM-240

Руководство пользователя



## Содержание

1. Описание устройства .....	4
1.1. Описание SWM-240 ..	4
1.2. Характеристики ПО ..	4
1.3. Характеристики устройства .....	4
2. Настройка устройства .....	6
2.1. Установка коммутатора на DIN-рейку.....	6
2.1.1. Крепление SWM-240 на DIN-рейку .....	6
2.2. Установка коммутатора на стену.....	6
3. Обзор устройства.....	8
3.1. Передняя панель .....	8
3.2. Индикаторы на передней панели .....	9
3.3. Верхняя панель .....	10
4. Кабели... ..	11
4.1. Ethernet кабели.....	11
4.1.1. Назначение контактов 100BASE-TX/10BASE-T .....	11
4.2. Консольный кабель ... ..	12
5. WEB-управление .....	13
5.1. Настройка через web-браузер .....	13
5.1.1. О web-управлении .....	13
5.1.2. Информация о системе .....	15
5.1.3. Передняя панель ..	15
5.1.4. Основные настройки .....	16
5.1.4.1. Настройка коммутатора .....	16
5.1.4.2. Пароль администратора .....	16
5.1.4.3. Настройка IP ... ..	17
5.1.4.4. Настройка времени.....	18
5.1.4.5. LLDP .....	21
5.1.4.6 Modbus TCP.....	22
5.1.4.7. Автоконфигурирование .....	23
5.1.4.8. Резервное копирование и восстановление .....	23
5.1.4.9. Обновление прошивки .....	25
5.1.5. Резервирование ....	25
5.1.5.1. Технология Sy-Ring.....	25
5.1.5.2. Технология All-Ring.....	27
5.1.5.3. Sy-Chain .....	28
5.1.5.6. Технология RSTP .....	30
5.1.5.7. Технология MSTP.....	33

5.1.6. Групповая рассылка.....	37
5.1.6.1. IGMP snooping .....	37
5.1.6.2 MVR.....	38
5.1.6.3. Статическая фильтрация группового трафика .....	39
5.1.7. Конфигурация портов.....	40
5.1.7.1. Управление портами .....	40
5.1.7.2. Состояние портов .....	41
5.1.7.3. Наименование порта .....	42
5.1.7.4. Ограничение скорости .....	42
5.1.7.5. Транки.....	43
5.1.7.6. Loop Guard.....	45
5.1.8. VLAN .....	45
5.1.8.1. Настройка VLAN .....	46
5.1.8.2. Настройка VLAN на основе портов.....	47
5.1.9. Приоритезация трафика .....	49
5.1.9.1 Qos policy.....	49
5.1.9.2 Port-base priority .....	50
5.1.9.3 COS/802.1p .....	50
5.1.9.4 TOS/DSCP .....	51
5.1.10. DHCP сервер.....	52
5.1.10.1. DHCP сервер – Установка .....	52
5.1.10.2. DHCP сервер – список устройств .....	53
5.1.10.3. DHCP сервер – Закрепление IP адресов за портами .....	53
5.1.10.4. DHCP сервер - агент DHCP .....	54
5.1.11. SNMP.....	55
5.1.11.1. SNMP - Настройка агента .....	55
5.1.11.2. SNMP - Настройка SNMP traps .....	57
5.1.11.3. SNMPv3 .....	58
5.1.12. Безопасность.....	60
5.1.12.1. Безопасность IP.....	60
5.1.12.2. Безопасность портов .....	61
5.1.12.3. Черный список MAC адресов.....	62
5.1.12.4. 802.1x .....	62
5.1.12.5 IP Guard .....	65
5.1.13. Оповещения.....	68
5.1.14. Мониторинг и диагностика.....	71
5.1.14.1. Журнал событий .....	71
5.1.14.2. Таблица MAC адресов .....	72
5.1.14.3. Статистика портов.....	73
5.1.14.4 Счётчики портов.....	74
5.1.14.5. Мониторинг портов.....	77

5.1.14.6. Мониторинг трафика.....	78
5.1.14.7. Ping.....	79
5.1.15. Сохранение конфигурации .....	80
5.1.16. Сброс настроек... ..	80
5.1.17. Перезагрузка системы .....	80
6. Командная строка.....	81
6.1. Управление с помощью командной строки.....	81
6.2. Список команд - системные команды .....	86
6.3. Список команд – команды портов.....	88
6.4. Список команд – команд транков.....	91
6.5. Список команд – команды VLAN .....	92
6.6. Список команд - команды Spanning Tree.....	93
6.7. Список команд - команды QoS .....	94
6.8. Список команд - команды IGMP .....	95
6.9. Список команд - команды MAC .....	96
6.10. Список Commands Set - Набор команд SNMP .....	96
6.11. Список команд - команды «зеркалирования» портов .....	98
6.12. Список команд - команды 802.1x .....	98
6.13. Список команд - команды TFTP .....	100
6.14. Список команд - команды SYSLOG, SMTP, EVENT .....	100
6.15. Список команд - команды SNTP .....	102
6.16. Список команд - команды Sy-Ring.....	103

## 1. Описание устройства

### 1.1. Описание SWM-240

SWM-240 - производительный промышленный коммутатор с множеством функций. Коммутатор может работать в широком диапазоне температур, в пыльной и влажной среде. Его можно настраивать через интернет, Telnet, Консоль или другие SNMP программы. Кроме того, коммутаторы можно настраивать через утилиту Windows, которая называется Sy-View. Sy-View - это мощное ПО управления сетью. Благодаря его удобному и мощному интерфейсу, вы можете легко настраивать коммутаторы одновременно, а так же просматривать их состояние.

### 1.2. Характеристики ПО

- Самая быстрая в мире технология кольцевого резервирования в Ethernet сетях (время восстановления <10 мс при 250 устройствах)
- Поддерживает технологию Ring Coupling, технологию Dual Homing параллельно с Sy-Ring
- Поддержка SNMPv1/v2/v3, RMON и управление сетью VLAN на основе портов/802.1Q
- Уведомления о событиях с помощью Email, SNMP trap и реле
- Возможность настройки с помощью Web, Telnet и консоли (CLI)
- Включение/отключение портов, списки доступа на основе MAC
- Контроль доступа к сети по портам (802.1x)
- VLAN (802.1Q) для разделения сетевого трафика и обеспечения безопасности
- Централизованное управление паролями с помощью Radius
- Шифрованная аутентификация SNMPv3 для безопасного доступа
- Поддержка RSTP (802.1w)
- Quality of Service (802.1p) для трафика в режиме реального времени
- VLAN (802.1Q) с двойным тегированием и поддержкой GVRP
- IGMP Snooping для многоадресной фильтрации
- Настройка портов, состояние, статистика, зеркалирование, безопасность
- Удаленный мониторинг (RMON)

### 1.3. Характеристики устройства

- 2 источника питания
- Рабочая температура: от -40 до 70 °С
- Температура хранения: -40 до 85 °С

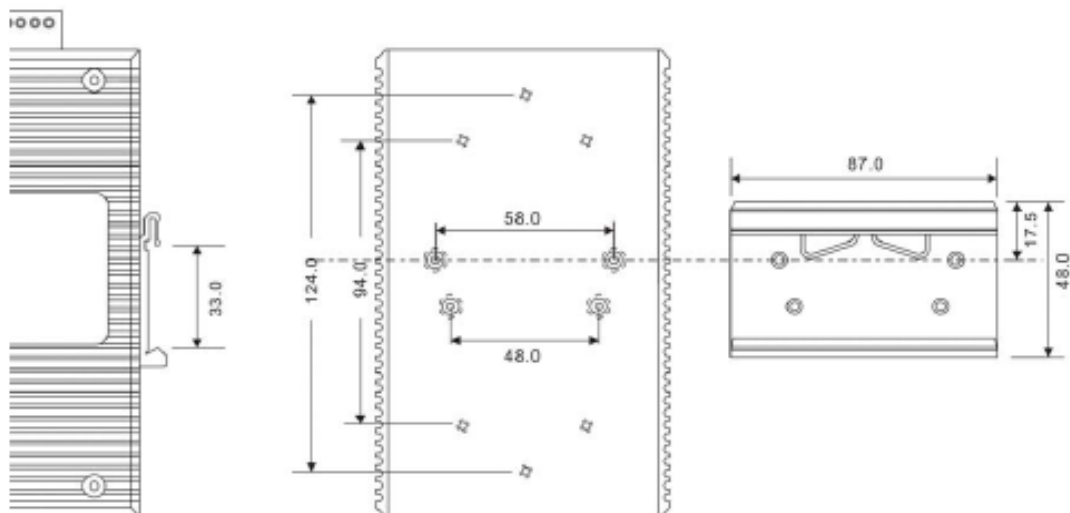
- Допустимая рабочая влажность: от 5% до 95%, без конденсата
- Корпус IP-30
- 10/100Base-T(X) Ethernet порты
- Консольный порт
- Габариты: 96 мм (ширина) x 109.2 мм (толщина) x 153.6 мм (высота)

## 2. Настройка устройства

### 2.1. Установка коммутатора на DIN-рейку

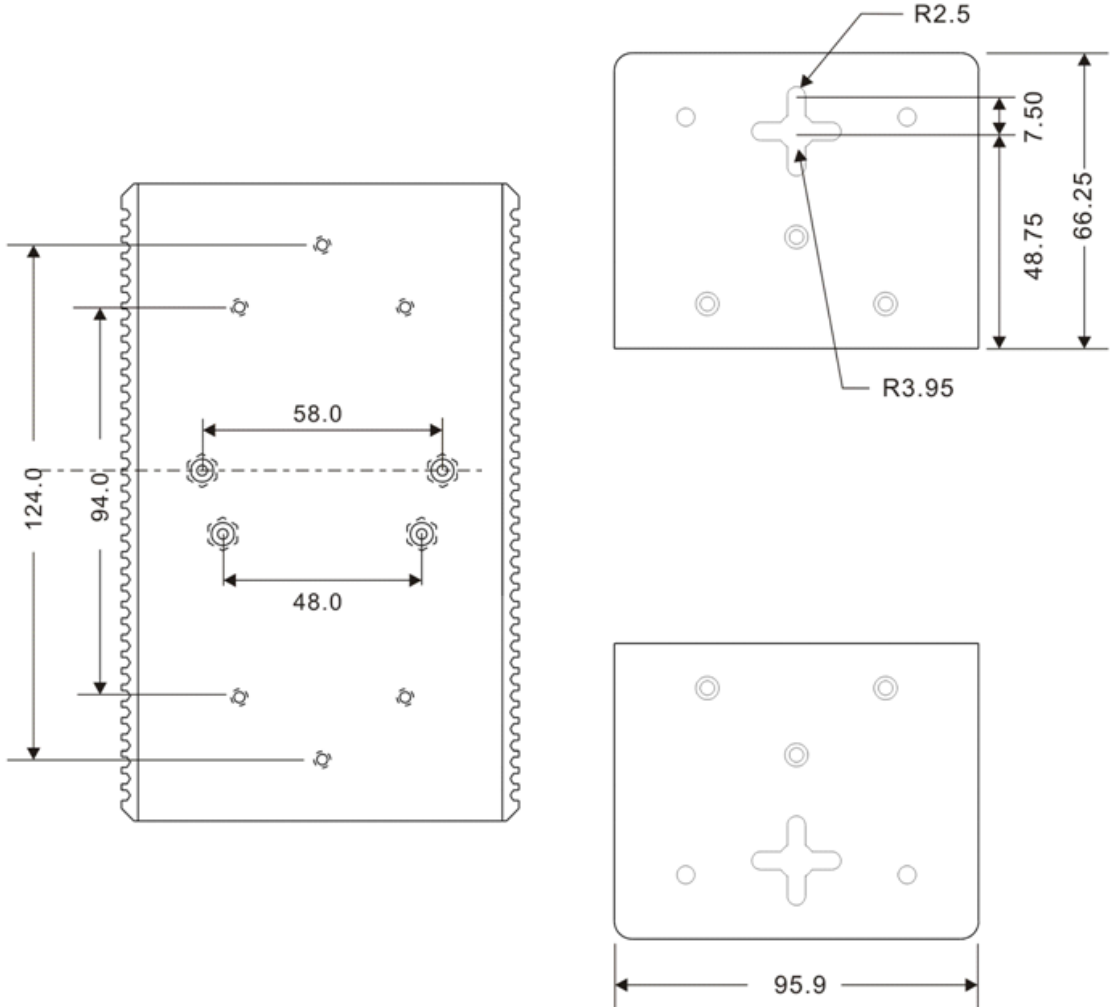
Каждый коммутатор имеет крепление на DIN-рейку на нижней панели. Крепление на DIN-рейку позволяет зафиксировать коммутатор.

#### 2.1.1. Крепление SWM-240 на DIN-рейку



### 2.2. Установка коммутатора на стену

Панель настенного крепления можно найти в упаковке. Следующие шаги показывают, как закрепить коммутатор на стене.



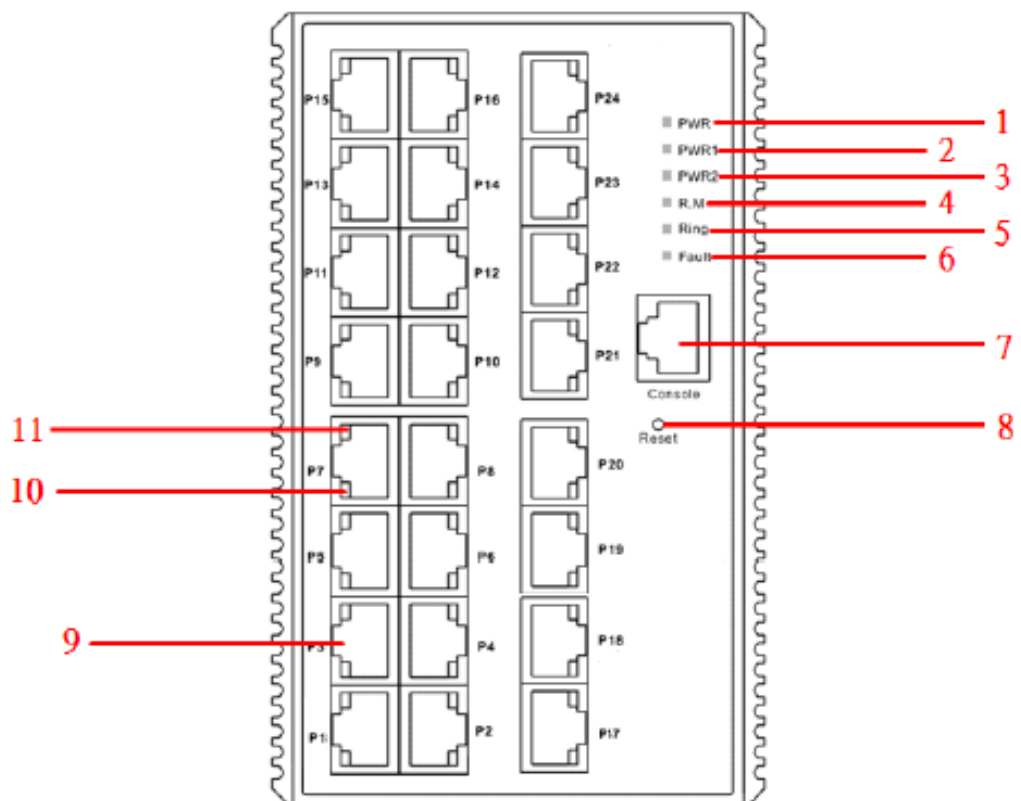


### 3. Обзор устройства

#### 3.1. Передняя панель

В таблице описана маркировка на SWM-240.

Порт	Описание
<b>Fast Ethernet порты 10/100 RJ-45</b>	6 10/100BaseTX RJ45 Fast Ethernet портов, поддерживающих автоматическое согласование Настройки по умолчанию: Speed: auto Duplex: auto Flow control: Disable
<b>Консоль</b>	Используйте переходник RS-232 - RJ45.
<b>Reset</b>	Нажмите и удерживайте кнопку Reset в течение 2-3 секунд, чтобы перезагрузить коммутатор Нажимайте и удерживайте кнопку сброса в течение 5 секунд чтобы сбросить настройки коммутатора до заводских настроек



SWM-240

1. Индикатор PWR. Если устройство получает питание, эта лампочка будет гореть.
2. Индикатор PWR1. При подключении PWR1 загорается зеленая лампочка.
3. Индикатор PWR2. При подключении PWR2 загорается зеленая лампочка.
4. Индикатор R.M. (Ring Master). Когда загорается индикатор, это значит, что коммутатор является главным в кольцевой топологии.
5. Индикатор кольцевой связи. Когда загорается индикатор, это значит, что технология Sy-Ring активирована.
6. Индикатор сигнального реле. Когда поступает аварийный сигнал, загорается оранжевая лампочка.
7. Консольный порт (RJ45)
8. Кнопка Reset. Нажимайте на кнопку в течение 3 секунд для перезагрузки; 5 секунд для сброса до заводских настроек.
9. 10/100Base-T(X) Ethernet порты
- 10-11. Индикаторы Link/ACT состояния Ethernet портов

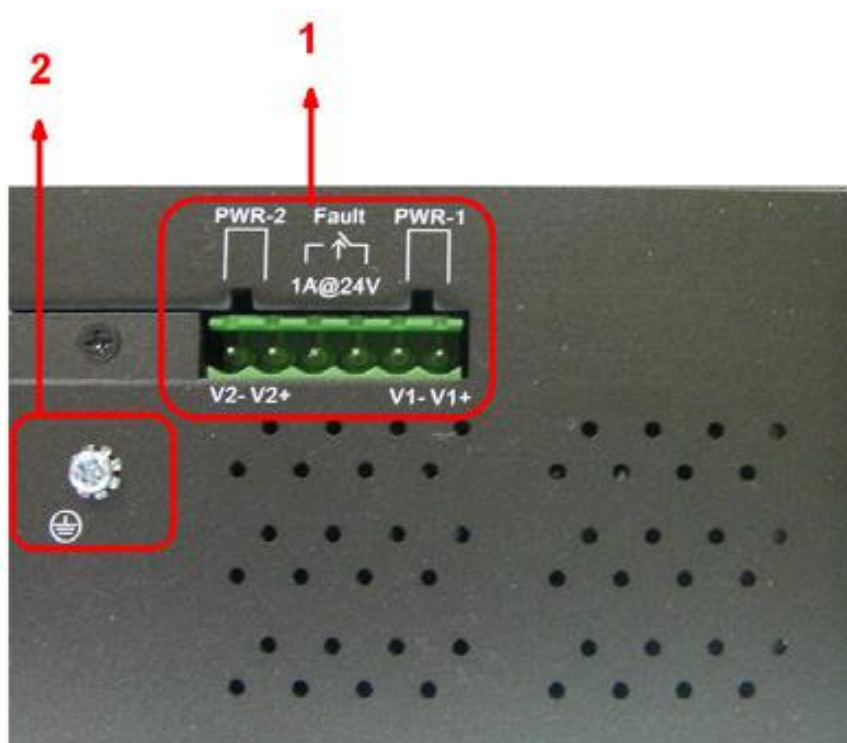
### 3.2. Индикаторы на передней панели

Индикатор	Цвет	Состояние	Описание
PWR	Зеленый	Включен	Питание подключено
PW1	Зеленый	Включен	1ое питание активно
PW2	Зеленый	Включен	2ое питание активно
R.M.	Зеленый	Включен	Корневое устройство в Sy-Ring
<b>Ring</b>	Зеленый	Включен	Sy-Ring включен
		Медленно мигает	В топологии Sy-Ring только одно соединение (не хватает одного соединения, чтобы построить кольцо)
		Быстро мигает	Sy-Ring работает нормально
<b>Fault</b>	Оранжевый	Включен	Реле сбоя. Сбой питания или отказ порта
<b>10/100Base-T(X) Fast Ethernet порты</b>			
<b>LNK/ACT</b>	Зеленый	Включен	Порт подсоединен
		Мигает	Передача данных
<b>Full Duplex</b>	Оранжевый	Включен	Порт работает в режиме полного дуплекса

### 3.3. Верхняя панель

Компоненты верхней панели коммутаторов SWM-240:

1. На клемной колодке находятся: PWR1, PWR2 (12-48V DC) и выход реле (1A@24VDC).
2. Заземление



## 4. Кабели

### 4.1. Ethernet кабели

Коммутаторы SWM-240 имеют стандартные Ethernet порты. Согласно типу соединения, коммутаторы используют UTP кабели CAT 3, 4, 5, 5e для подключения к любым другим сетевым устройствам (ПК, серверы, коммутаторы, роутеры, или концентраторы). Характеристики кабелей представлены в таблице:

Типы и характеристики кабелей

Кабель	Тип	Максимальная длина	Коннектор
10Base-T	Cat. 3, 4, 5 100 Ом	UTP 100 м (328 футов)	RJ-45
100Base-TX	Cat. 5 100 Ом UTP	UTP 100 м (328 футов)	RJ-45

#### 4.1.1. Назначение контактов 100BASE-TX/10BASE-T

С кабелями 100Base-TX/10Base-T контакты 1 и 2 используются для передачи данных, и контакты 3 и 6 используются для получения данных.

Назначения контактов 10/100Base-T RJ45:

Номер контакта	Назначение
1	TD+
2	TD-
3	RD+
4	Не используется
5	Не используется
6	RD-
7	Не используется
8	Не используется

Коммутатор SWM-240 поддерживает автоматическую работу MDI/MDI-X. Можно использовать прямой кабель для соединения ПК и коммутатора. В таблице указаны контакты портов MDI и MDI-X 10Base-T/100Base-TX.

Назначение контактов 10/100Base-T(X) MDI/MDI-X:

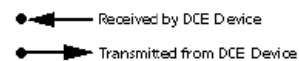
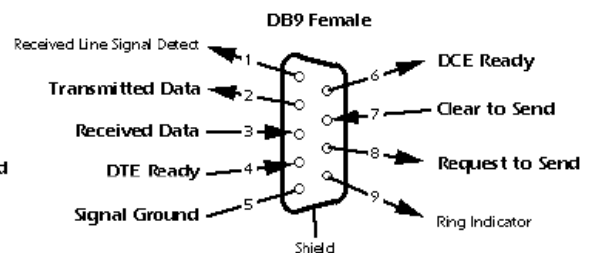
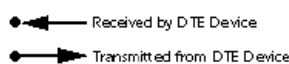
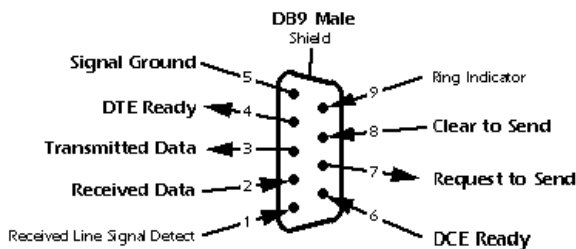
Номер контакта	Порт MDI	Порт MDI-X
1	TD+(передача)	RD+(получение)
2	TD-(передача)	RD-(получение)
3	RD+(получение)	TD+(передача)
4	Не используется	Не используется
5	Не используется	Не используется
6	RD-(получение)	TD-(передача)
7	Не используется	Не используется
8	Не используется	Не используется

Примечание: + и – означают полярность проводов, которые составляют проводную пару.

#### 4.2. Консольный кабель

Коммутаторами SWM-240 можно управлять с помощью консольного порта. Кабель DB9 – RJ45 можно найти в упаковке. Их можно подключить к компьютеру через RS-232 кабель с коннектором DB9 «мама», и другой конец (коннектор RJ45) подключается к консольному порту коммутатора.

Назначение схемы контактов компьютера «папа»	RS-232 с коннектором DB9 «мама»	DB9-RJ45
Контакт (Pin) #2 RD	Контакт (Pin) #2 TD	Контакт (Pin) #2
Контакт (Pin) #3 TD	Контакт (Pin) #3 RD	Контакт (Pin) #3
Контакт (Pin) #5 GD	Контакт (Pin) #5 GD	Контакт (Pin) #5



## 5. WEB-управление

**Внимание!!!** Прежде чем производить любые настройки или обновления программного обеспечения устройства, отключите кабели кольцевого резервирования. НЕ выключайте оборудование во время обновления прошивки!

### 5.1. Настройка через web-браузер

Этот раздел описывает настройку через Веб-браузер.

#### 5.1.1. О web-управлении

Встроенный веб-сайт HTML находится во флеш-памяти на плате центрального процессора. Он содержит расширенные функции управления и позволяет управлять коммутатором из любой точки сети через стандартный веб-браузер, такой как Microsoft Internet Explorer.

Функция web-управления поддерживает Internet Explorer 5.0 и выше. Она основана на Java-апплетах с целью уменьшить размер передаваемых данных, увеличить скорость доступа и предоставить простой интерфейс.

Примечание: По умолчанию, IE 5.0 или выше не позволяет Java-апплетам открывать сокет. Необходимо самостоятельно разрешить сокет для Java-апплетов в настройках браузера

#### Настройка web-управления.

Значения по умолчанию:

IP адрес: 192.168.10.1

Subnet Mask: 255.255.255.0

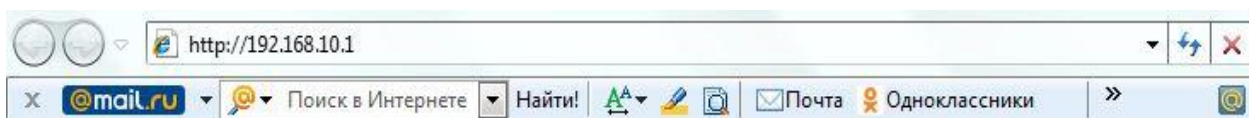
Default Gateway: 192.168.10.254

User Name: admin

Password: admin

#### Авторизация

1. Запустите Internet Explorer.
2. Наберите http:// и IP адрес коммутатора. Нажмите Enter



3. Появится окно входа
4. Введите имя пользователя и пароль. Имя пользователя и пароль по умолчанию – admin.
5. Нажмите Enter или кнопку ОК, затем появится главный интерфейс веб-управления

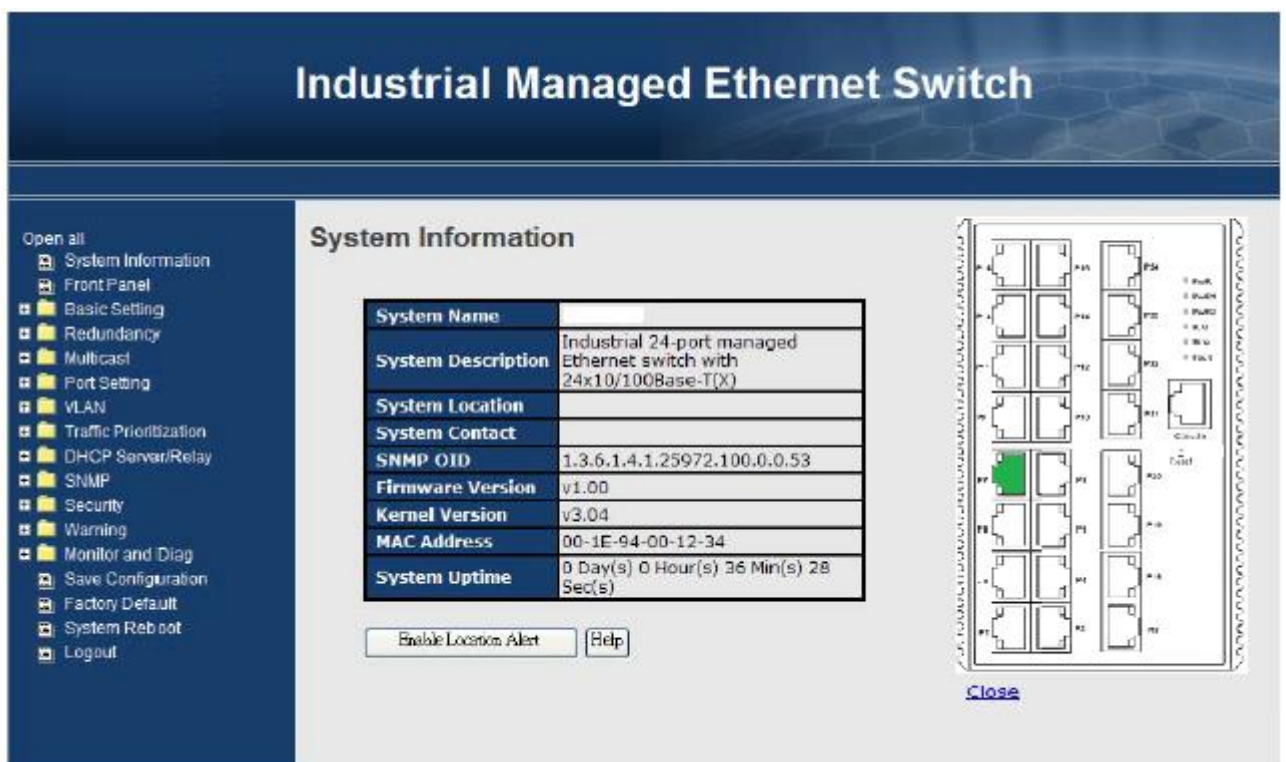


Рис. Основной интерфейс

### 5.1.2. Информация о системе

<b>System Name</b>	
<b>System Description</b>	Industrial 24-port managed Ethernet switch with 24x10/100Base-T(X)
<b>System Location</b>	
<b>System Contact</b>	
<b>SNMP OID</b>	1.3.6.1.4.1.25972.100.0.0.53
<b>Firmware Version</b>	v1.00
<b>Kernel Version</b>	v3.04
<b>MAC Address</b>	00-1E-94-00-12-34
<b>System Uptime</b>	0 Day(s) 0 Hour(s) 37 Min(s) 8 Sec(s)

Рис. Информация о системе

#### Информация о системе

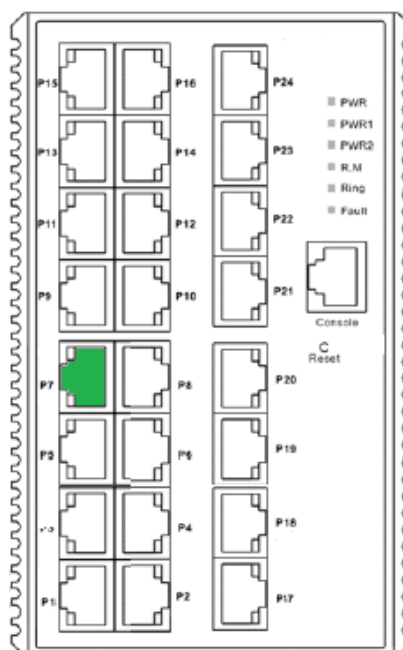
Информация о системе показывает основные настройки коммутатора.

#### Включение функции оповещения о местоположении

При нажатии Enable Location Alert индикаторы коммутатора PWR1, PWR2 и PWR3 начнут одновременно мигать, при нажатии Disable Location Alert – перестанут мигать.

### 5.1.3. Передняя панель

Показана передняя панель SWM-240. Нажмите Close, чтобы закрыть панель в веб-браузере.





## 5.1.4. Основные настройки

### 5.1.4.1. Настройка коммутатора

<b>System Name</b>	<input type="text"/>
<b>System Description</b>	Industrial 24-port managed Ethernet switch with 24x10/100Base-T(X)
<b>System Location</b>	<input type="text"/>
<b>System Contact</b>	<input type="text"/>

Рис. Настройка коммутатора

В таблице описаны основные поля:

Поле	Описание
<b>System Name</b>	Имя коммутатора. Максимальная длина 64 байта
<b>System Description</b>	Описание коммутатора
<b>System Location</b>	Физический адрес коммутатора. Максимальная длина 64 байта
<b>System Contact</b>	Имя контактного лица или организации

### 5.1.4.2. Пароль администратора

Для повышения безопасности смените имя пользователя и пароль веб-интерфейса.

#### Admin Password

<b>User Name</b>	<input type="text" value="admin"/>
<b>New Password</b>	<input type="password"/>
<b>Confirm Password</b>	<input type="password"/>

Рис. Интерфейс администратора

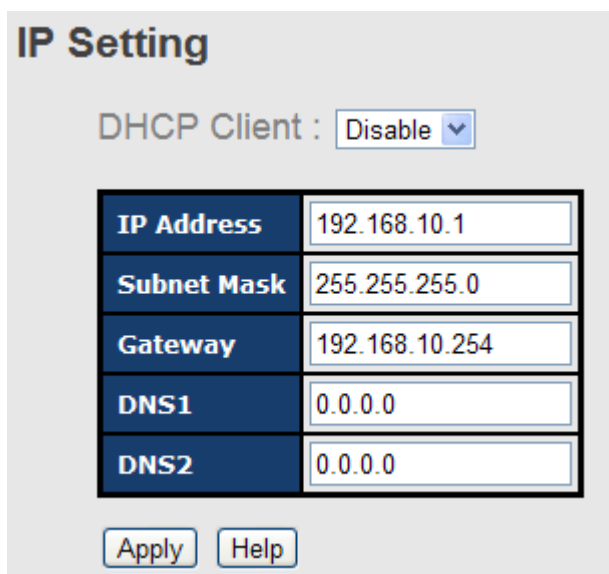
В таблице описаны основные поля:

Поле	Описание
<b>User Name</b>	Введите новое имя пользователя (по умолчанию – admin)

<b>New Password</b>	Введите новый пароль (по умолчанию – admin)
<b>Confirm Password</b>	Повторите новый пароль
<b>Apply</b>	Нажмите «Применить» чтобы активировать настройки

### 5.1.4.3. Настройка IP

Вы можете изменить настройки IP и функции DHCP клиента через меню IP Configuration.



**IP Setting**

DHCP Client :

<b>IP Address</b>	<input type="text" value="192.168.10.1"/>
<b>Subnet Mask</b>	<input type="text" value="255.255.255.0"/>
<b>Gateway</b>	<input type="text" value="192.168.10.254"/>
<b>DNS1</b>	<input type="text" value="0.0.0.0"/>
<b>DNS2</b>	<input type="text" value="0.0.0.0"/>

Рис. Интерфейс IP настроек

В таблице описаны основные поля:

Поле	Описание
DHCP Client	Включает или отключает функцию DHCP клиента. При включении функции коммутатор получит IP адрес от DHCP сервера. IP адрес по умолчанию будет заменен на тот, который назначил DHCP сервер. После нажатия кнопки Apply покажется раскрывающееся диалоговое окно, информируя о том, что DHCP клиент включен.
IP Address	Назначьте IP адрес, принадлежащий к подсети. Если функция DHCP клиента включена, вам не нужно назначать IP адрес. DHCP сервер сети назначит коммутатору IP адрес и он появится в этой графе. IP адрес по умолчанию 192.168.10.1
Subnet Mask	Назначьте маску подсети для IP адреса. Если функция DHCP клиента включена, назначать маску подсети не нужно.

Gateway	Назначьте сетевой шлюз для коммутатора. Сетевой шлюз по умолчанию: 192.168.10.254
DNS1	Назначьте IP адрес первичного DNS
DNS2	Назначьте IP адрес вторичного DNS
Apply	Нажмите Apply, чтобы активировать настройки

#### 5.1.4.4. Настройка времени

##### Системное время

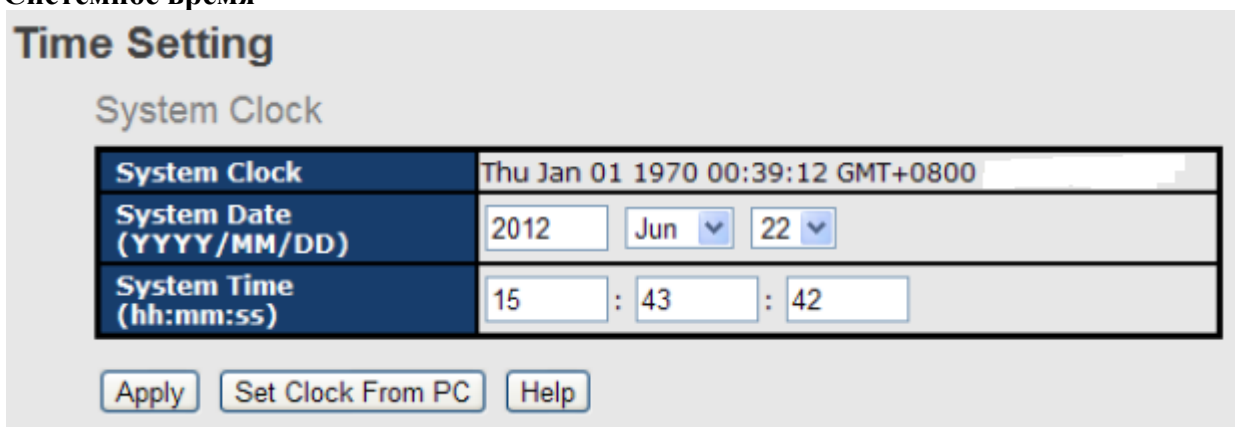


Рис. Системное время

В таблице описаны основные поля:

Поле	Описание
<b>System clock</b>	Текущее время на устройстве. Оно может быть установлено вручную или SNTP сервером.
<b>System Date</b>	Выберите год, месяц и день (YYYY/MM/DD). Год: 2006-2015. Месяц: Янв-Дек. День: 1-31 (28)
<b>System Time</b>	Выберите час, минуту и секунду (hh:mm:ss). Час: 0-24, Минута: 0-59, Секунда: 0-59

##### SNTP

Настройки протокола SNTP позволяют вам синхронизировать время на коммутаторе через интернет.

SNTP Client :

<b>UTC Timezone</b>	(GMT)Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London
<b>SNTP Server Address</b>	0.0.0.0

Daylight Saving Time :

<b>Daylight Saving Period</b>	2012 Jun 22 07 ~
	2012 Jun 22 07
<b>Daylight Saving Offset</b>	0 (hours)

Рис. Настройка времени

В таблице описаны основные поля:

Поле	Описание
<b>SNTP Client</b>	Включение или отключение функции SNTP для получения времени с SNTP сервера
<b>Daylight Saving Time</b>	Включение или отключение опции перехода между зимним и летним временем. При включении опции нужно установить даты перевода часов.
<b>UTC Time Zone</b>	Установите часовой пояс расположения коммутатора. В следующей таблице перечислены часовые пояса различных зон

Зона местного времени	Отклонение от UTC	Время в 12:00 UTC
November Time	-1 час	11:00
Oscar Time Zone	-2 часа	10:00
ADT – Atlantic Daylight	-3 часа	9:00
AST – Atlantic Standard EDT – Eastern Daylight	-4 часа	8:00
EST – Eastern Standard CDT – Central Daylight	-5 часов	7:00

CST – Central Standard MDT – Mountain Daylight	-6 часов	6:00
MST – Mountain Standard PDT - Pacific Daylight	-7 часов	5:00
PST - Pacific Standard ADT - Alaskan Daylight	-8 часов	4:00
ALA - Alaskan Standard	-9 часов	3:00
HAW - Hawaiian Standard	-10 часов	2:00
Nome, Alaska	-11 часов	1:00
CET – Central European FWT – French Winter MET - Middle European MEWT – Middle European Winter SWT – Swedish Winter	+1 час	13:00
EET – Eastern European, USSR Zone 1	+2 часа	14:00
BT – Baghdad, USSR Zone 2	+3 часа	15:00
ZP4 – USSR Zone 3	+4 часа	16:00
ZP5 – USSR Zone 4	+5 часов	17:00
ZP6 – USSR Zone 5	+6 часов	18:00
WAST – West Australian Standard	+7 часов	19:00
CCT – China Coast, USSR Zone 6	+8 часов	20:00
JST – Japan Standard, USSR Zone 7	+9 часов	21:00
EAST – East Australian Standard GST – Guam Standard, USSR Zone 9	+10 часов	22:00
IDLE – International Date Line NZST - New Zealand Standard NZT – New Zealand	+12 часов	0:00

Поле	Описание
<b>SNTP Server Address</b>	Укажите IP адрес SNTP сервера
<b>Daylight Saving Period</b>	Укажите начало и окончание периода летнего времени. Каждый год они будут разными.
<b>Daylight Saving Offset</b>	Установите разницу, на которую смещаются стрелки часов
<b>Switch Timer</b>	Показывает текущее время на коммутаторе
<b>Apply</b>	Нажмите, чтобы активировать настройки

### PTP Client

PTP (Протокол точного времени) – протокол передачи времени, описанный в стандарте IEEE 1588-2002, обеспечивающий точную синхронизацию сетей (например, Ethernet). Погрешность менее наносекунды может быть достигнута с помощью этого протокола при использовании устройств, генерирующих временные метки.

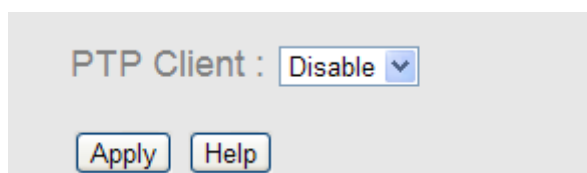


Рис. PTP Client

В таблице описаны основные поля:

Поле	Описание
<b>PTP Client</b>	Включение/выключение PTP клиента

### 5.1.4.5. LLDP

Функция LLDP (Протокол канального уровня) позволяет коммутатору передавать свою информацию о сети на другие узлы и хранить полученную информацию.

**LLDP**

LLDP Protocol:

LLDP Interval:  sec

**Neighbor Info Table**

Port	System Name	MAC Address	IP Address
Port. 8		00-1E-94-3A-04-B0	192.168.10.20

Рис. LLDP параметры

В таблице описаны основные поля:

Поле	Описание
<b>LLDP Protocol</b>	Включение или отключение функции LLDP
<b>LLDP Interval</b>	Интервал повторной отправки LLDP (по умолчанию 30 секунд)
<b>Apply</b>	Нажмите, чтобы активировать настройки
<b>Help</b>	Показать справку
<b>Neighbor info table</b>	Отображает информацию о соседях

#### 5.1.4.6 Modbus TCP

Поддержка Modbus TCP (подробнее на <http://modbus.org/>).

**Modbus TCP**

Mode :

Рис. Modbus TCP

В таблице описаны основные поля:

Поле	Описание
Mode	Включить или выключить функцию Modbus TCP

#### 5.1.4.7. Автоконфигурирование

Функция Auto Provision позволяет автоматически обновлять прошивку коммутатора.

Вы можете поместить прошивку или файл конфигурации на TFTP сервер. При перезагрузке коммутатора прошивка обновится автоматически. Перед обновлением убедитесь, что ваш TFTP сервер готов, а файлы прошивки или конфигурации находятся на TFTP сервере.

**Auto Provision**

Auto install configuration file from TFTP server?

**TFTP Server IP Address** 192.168.10.66

**Configuration File Name** data.bin

Auto install firmware image file from TFTP server?

**TFTP Server IP Address** 192.168.10.66

**Firmware File Name** image.bin

Apply Help

Рис. Автоконфигурирование

#### 5.1.4.8. Резервное копирование и восстановление

На этой странице, вы можете сохранить текущие настройки коммутатора на TFTP сервере или восстановить конфигурацию с TFTP сервера.



**Restore Configuration**  
From TFTP Server

<b>TFTP Server IP Address</b>	192.168.10.2
<b>Restore File Name</b>	data.bin

From Local PC

**Backup Configuration**  
To TFTP Server

<b>TFTP Server IP Address</b>	192.168.10.2
<b>Backup File Name</b>	data.bin

To Local PC

Рис. Резервное копирование и восстановление

В таблице описаны основные поля:

Поле	Описание
TFTP Server IP Address	Введите IP адрес TFTP сервера
Restore File Name	Введите название файла
Restore	Нажмите Restore, чтобы восстановить настройки
Form Local PC	Пользователь может сам выбрать файл для восстановления, без TFTP сервера.
Restore File Name	Имя файла.
To Local PC	Пользователь может скачать файл с коммутатора, без TFTP сервера.

Backup

Нажмите Backup, чтобы сделать резервное копирование настроек

#### 5.1.4.9. Обновление прошивки

Эта функция позволяет обновлять прошивку коммутатора. Перед обновлением убедитесь, что ваш TFTP сервер готов, и что файл прошивки находится на TFTP сервере.

**Upgrade Firmware**

From TFTP Server

TFTP Server IP	192.168.10.2
Firmware File Name	image.bin

Upgrade Help

From Local PC

瀏覽...

Upgrade

Рис. Обновление прошивки

#### 5.1.5. Резервирование

##### 5.1.5.1. Технология Sy-Ring

Sy-Ring - одна из самых эффективных кольцевых технологий резервирования в мире. Время восстановления составляет менее 10 мс при 250 устройствах. Она позволяет избежать неожиданных сбоев, вызванных изменениями в сетевой топологии. Технология Sy-Ring поддерживает три Ring-топологии для сетевого резервирования: Sy-Ring, Ring Coupling и Dual Homing.

<input checked="" type="checkbox"/> <b>Enable Ring</b>		
<input type="checkbox"/> <b>Enable Ring Master</b>		
<b>1st Ring Port</b>	Port.01 ▾	LINKDOWN
<b>2nd Ring Port</b>	Port.02 ▾	LINKDOWN
<input type="checkbox"/> <b>Enable Couple Ring</b>		
<b>Couple Port</b>	Port.03 ▾	LINKDOWN
<input type="checkbox"/> <b>Enable Dual Homing</b>		
<b>Homing Port</b>	Port.05 ▾	LINKDOWN

Apply Help

Рис. Sy-Ring интерфейс

В таблице описаны основные поля:

Поле	Описание
<b>Enable Ring</b>	Отметьте для включения кольца.
<b>Enable Ring Master</b>	В кольце может быть один и только один Ring Master в кольце. В любом случае, если в кольце несколько устройств с установленными свойствами Ring Master, активным из них будет тот, что имеет минимальный MAC адрес. Остальные станут резервными.
<b>1st Ring Port</b>	Основной порт, если коммутатор является Ring master-ом.
<b>2nd Ring Port</b>	Резервный порт, если коммутатор является Ring master-ом.
<b>Enable Coupling Ring</b>	Нажмите для включения Ring Coupling. Технология используется для разделения большого кольца на два меньшего размера для предотвращения длительного перестроения сети при большом количестве устройств. также используется для объединения независимых колец.
<b>Coupling Port</b>	Связь с coupling портом коммутатора в другом кольце. Она необходимо для построения активной и резервной связей. Четыре коммутатора из двух сетей образуют две связи, одна из которых будет активной, а вторая - резервной.
<b>Control Port</b>	Связь с контрольным портом на устройстве в своём кольце. Используется для передачи контрольных сигналов.
<b>Enable</b>	Нажмите для включения Dual Homing. С его помощью, кольцо может быть

<b>Dual Homing</b>	подключено к двум некольцевым узлам через RSTP линки. Эти два соединения работают как активная и резервная связи.
<b>Apply</b>	Нажмите для сохранения конфигурации.

Примечание: Мы не советуем устанавливать один коммутатор одновременно как Ring Master (как основной) и как Ring Coupling из-за высокой нагрузки.

### 5.1.5.2. Технология All-Ring

Технология необходима для использования устройств в проприетарных кольцах других производителей.

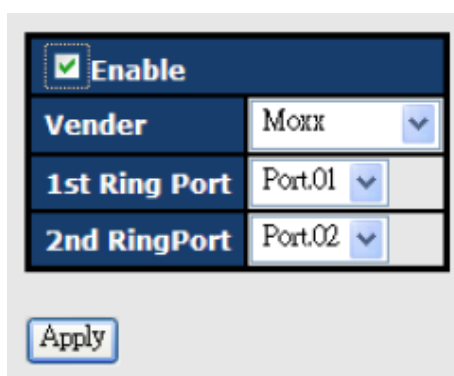
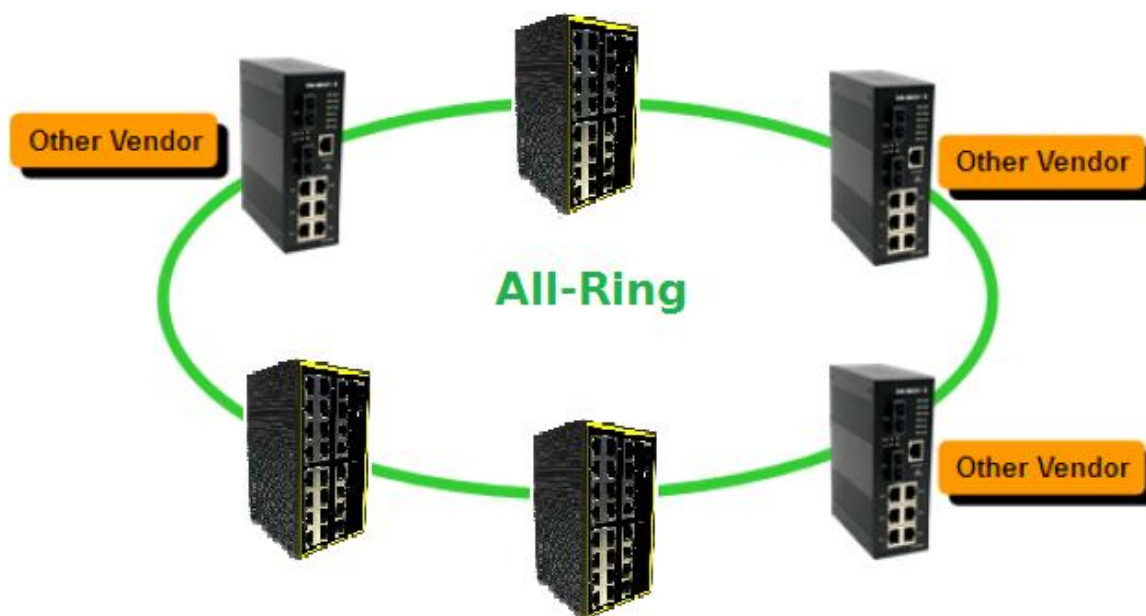


Рис. All-Ring интерфейс

В таблице описаны основные поля:

Поле	Описание
<b>Enable</b>	Включение функции All-Ring
<b>Vender</b>	Выбор производителя, к кольцевым топологиям которого вы хотите подключиться
<b>1sr Ring Port</b>	Выбор подключенного к кольцу порта
<b>2nd Ring Port</b>	Выбор подключающего к кольцу порта

Применение All-Ring показано на схеме:



### 5.1.5.3. Sy-Chain

Sy-Chain - технология резервирования, позволяющая объединять различные технологии резервирования в единую топологию, преодолевая ограничения каждого отдельно взятого протокола и используя их преимущества.

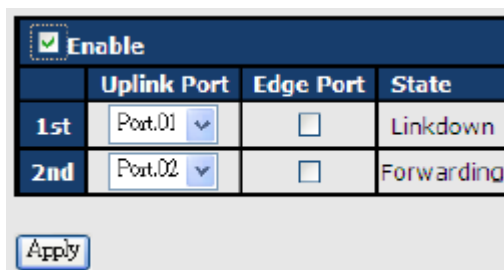
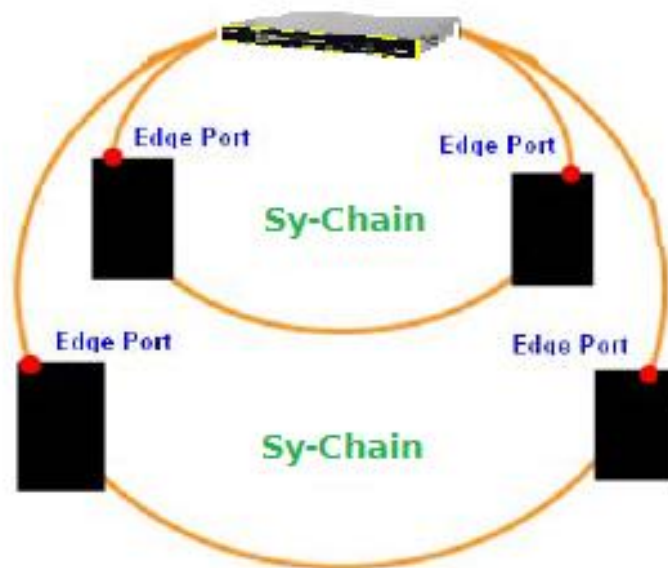


Рис. Sy-Chain интерфейс

В таблице описаны основные поля:

Поле	Описание
<b>Enable</b>	Включение Sy-Chain
<b>1st Ring Port</b>	Выберите порт, подключённый к кольцу
<b>2nd Ring Port</b>	Выберите порт, подключённый к кольцу
<b>Edge Port</b>	В топологии Sy-Chain начальный и конечный порт должны быть Edge (см. рисунок)



### 5.1.5.4 RSTP - повторитель

RSTP-повторитель - это простая функция, которая может передавать BPDU пакеты, как если бы устройства были подключены непосредственно.

#### RSTP-Repeater

<input type="checkbox"/> Enable		
	<b>Uplink Port</b>	<b>RSTP Edge Port</b>
<b>1st</b>	Port.01	<input type="checkbox"/>
<b>2nd</b>	Port.02	<input type="checkbox"/>

Рис. RSTP-повторитель

В таблице описаны основные поля:

Поле	Описание
<b>Enable</b>	Включить функцию RSTP-повторителя
<b>1st Ring Port</b>	Выберите порт, подключенный к RSTP
<b>2nd Ring Port</b>	Выберите порт, подключенный к RSTP
<b>Edge Port</b>	RSTP Edge порт.

### 5.1.5.5 Быстрое восстановление

Режим быстрого восстановления используется для подключения нескольких портов к одному или нескольким коммутаторам. Режим Fast Recovery поддерживает 5 приоритетов, только порт с наивысшим приоритетом будет рабочим, остальные - резервными.

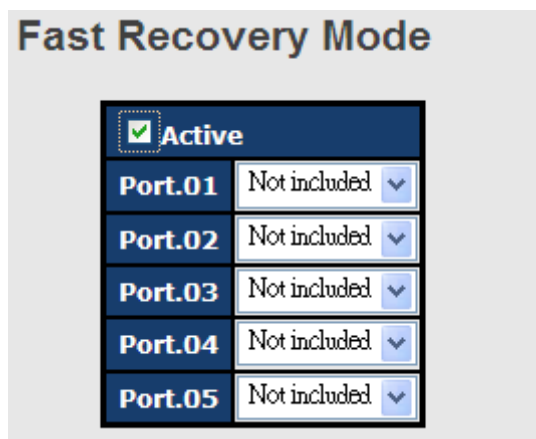


Рис. Интерфейс быстрого восстановления

В таблице описаны основные поля:

Поле	Описание
Active	Активировать режим быстрого восстановления
Port	Порту можно настроить один из пяти приоритетов. Только порт с наивысшим приоритетом будет активным. 1-й приоритет - наивысший.
Apply	Нажмите для активации конфигурации.

### 5.1.5.6. Технология RSTP

RSTP - это улучшенная версия STP. RSTP обеспечивает быструю сходимость логического дерева из-за изменений в топологии. Система также поддерживает STP и автоматически обнаруживает подключённое устройство, которое работает по протоколам STP или RSTP.

#### Настройка RSTP

Вы можете включить или отключить функцию RSTP и установить параметры для каждого порта.

### RSTP - Bridge Setting

<b>RSTP Mode</b>	Enable <input type="button" value="v"/>
<b>Priority (0-61440)</b>	<input type="text" value="32768"/>
<b>Max Age (6-40)</b>	<input type="text" value="20"/>
<b>Hello Time (1-10)</b>	<input type="text" value="2"/>
<b>Forward Delay Time (4-30)</b>	<input type="text" value="15"/>

**Priority must be a multiple of 4096.  
 2\*(Forward Delay Time-1) should be greater than or equal to the Max Age.  
 The Max Age should be greater than or equal to 2\*(Hello Time + 1).**

Рис. Настройка RSTP

В таблице описаны основные поля:

Поле	Описание
<b>RSTP mode</b>	Перед настройкой сопутствующих параметров, нужно сначала включить RSTP
<b>Priority (0-61440)</b>	Приоритет используется для выбора корневого узла. Коммутатор с наименьшим приоритетом выбирается как корневой. Если значение приоритета изменилось, устройство необходимо перезагрузить. Значение приоритета должно быть кратно 4096, согласно требованиям стандарта.
<b>Max Age Time(6-40)</b>	Время в секундах, которое устройство будет ожидать получения сообщений о конфигурации логического дерева перед попыткой реконфигурации.
<b>Hello Time (1-10)</b>	Время, через которое устройство отправляет BPDU пакеты для проверки статуса RSTP.
<b>Forwarding Delay Time (4-30)</b>	Время в секундах, через которое устройство сменит статус с прослушивания на продвижение.
<b>Apply</b>	Применить.

Примечание: Следуйте правилу, чтобы настроить Max Age, Hello Time и Forward Delay Time:

$$2 \times (\text{Forward Delay Time} - 1) \geq \text{Max Age} \geq 2 \times (\text{Hello Time} + 1)$$



Результат алгоритма RSTP показан в таблице

### Root Bridge Information

<b>Bridge ID</b>	8000001E94011E7A
<b>Root Priority</b>	32768
<b>Root Port</b>	ROOT
<b>Root Path Cost</b>	0
<b>Max Age</b>	20
<b>Hello Time</b>	2
<b>Forward Delay</b>	15

### RSTP - Port Setting

Port	Path Cost (1-200000000)	Priority (0-240)	Admin P2P	Admin Edge	Admin Non Stp
Port.01					
Port.02					
Port.03	200000	128	auto	true	false
Port.04					
Port.05					

priority must be a multiple of 16

Apply Help

### Port Status

Port	Path Cost	Port Priority	Oper P2P	Oper Edge	Stp Neighbor	State	Role
Port.01	200000	128	True	True	False	Disabled	Disabled
Port.02	200000	128	True	True	False	Disabled	Disabled
Port.03	200000	128	True	True	False	Disabled	Disabled
Port.04	200000	128	True	True	False	Disabled	Disabled
Port.05	200000	128	True	True	False	Disabled	Disabled

Рис. Результат алгоритма RSTP

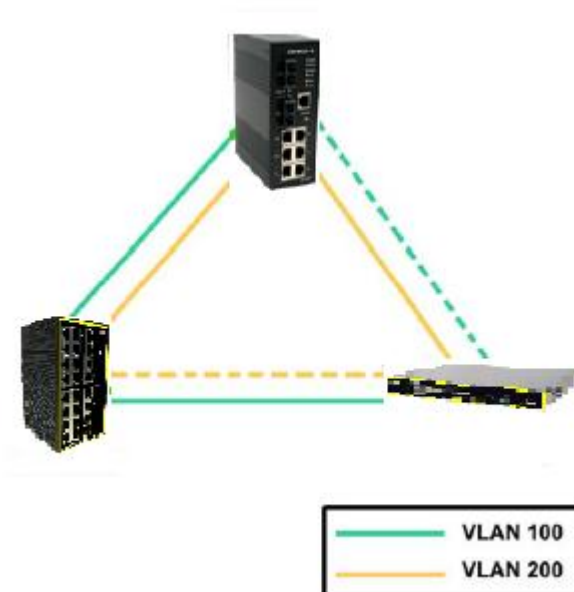
В таблице описаны основные поля:

Поле	Описание
<b>Path Cost (1-</b>	Стоимость соединения. Значения от 1 до 200000000.

<b>200000000)</b>	
<b>Port Priority (0-240)</b>	Выберите порт, который должен быть заблокирован в LAN. Введите значение от 0 до 240. Значение приоритета должно быть кратно 16.
<b>Admin P2P</b>	Некоторые быстрые смены состояний в RSTP могут быть осуществлены только при условии подключения только к одному соседнему узлу (то есть, при соединении точка-точка (P2P)), или при подключении только к двум и более устройствам (при использовании разделяемой среды). Такое разнообразие сегментов требует административного участия. True значит включение P2P, False - выключение.
<b>Admin Edge</b>	Порт подключен к конечному устройству и не может создать петли в сети.
<b>Admin Non STP</b>	Порт не поддерживает STP вычисления.
<b>Apply</b>	Применить

### 5.1.5.7. Технология MSTP

MSTP – стандартный протокол, основанный на IEEE 802.1s. Функция позволяет создавать свои собственные логические деревья STP в одной физической сети для VLAN сетей. MSTP поддерживает схему балансирования нагрузки, используя меньше ресурсов, чем PVST (проприетарная технология Cisco).



## MSTP - Bridge Setting

<b>MSTP Enable</b>	Enable <input type="button" value="v"/>
<b>Force Version</b>	MSTP <input type="button" value="v"/>
<b>Configuration Name</b>	MSTP_SWITCH
<b>Revision Level (0-65535)</b>	0
<b>Priority (0-61440)</b>	32768
<b>Max Age Time (6-40)</b>	20
<b>Hello Time (1-10)</b>	2
<b>Forward Delay Time (4-30)</b>	15
<b>Max Hops (1-40)</b>	20

**Priority must be a multiple of 4096.  
 $2 * (\text{Forward Delay Time} - 1)$  should be greater than or equal to the Max Age.  
The Max Age should be greater than or equal to  $2 * (\text{Hello Time} + 1)$ .**

Рис. Интерфейс MSTP

В таблице описаны основные поля:

Поле	Описание
<b>MSTP Enable</b>	Вы должны включить или отключить функцию MSTP до настройки связанных параметров.
<b>Force Version</b>	Функция Force Version заставляет VLAN устройство, поддерживающее RSTP, работать в режиме, совместимом с STP
<b>Configuration Name</b>	Все устройства в одном MST должны иметь одинаковое MST Configuration Name.
<b>Revision Level (0-65535)</b>	Все устройства в одном MST должны иметь одинаковое MST Configuration Name.
<b>Priority (0-61400)</b>	Значение используется для идентификации корневого устройства. Устройство с самым низким значением имеет самый высокий приоритет и выбирается как корневой. Если значение изменяется, вам следует перезагрузить коммутатор. Согласно стандартному правилу протокола, значение должно быть кратным 4096
<b>Max Age Time (6-40)</b>	Количество секунд, которое выжидает устройство без получения сообщений конфигурации STP до попытки реконфигурации. Введите

	значение от 6 до 40.
<b>Hello Time (1-10)</b>	Функция, зависящая от правил настройки Max Age, Hello Time и Forward Delay Time. Это время, которое определяет, с какой периодичностью коммутатор должен отправлять пакеты BPDU для проверки текущего состояния дерева. Введите значение от 1 до 10. $2 \times (\text{Forward Delay Time} - 1) \geq \text{Max Age} \geq 2 \times (\text{Hello Time} + 1)$
<b>Forwarding Delay Time (4-30)</b>	Количество секунд, которое порт выжидает до изменения из состояния обучения и прослушивания его RSTP в состояние пересылки. Введите значение от 4 до 30
<b>Max Hops (1-40)</b>	Дополнительная функция, предназначенная для RSTP. Одно значение применимо ко всем логическим деревьям в пределах MST региона (CIST и все MSTI), для которых мост является корневым устройством региона.
<b>Apply</b>	Нажмите Apply, чтобы активировать настройки

### MSTP - Bridge Port

Port No.	Priority (0-240)	Path Cost (1-200000000, 0:Auto)	Admin P2P	Admin Edge	Admin Non Stp
Port.01					
Port.02					
Port.03	128	0	auto	true	false
Port.04					
Port.05					

**priority must be a multiple of 16**

Apply

Рис. MSTP порт

В таблице описаны основные поля:

Поле	Описание
<b>Port NO.</b>	Выберите порт, который хотите настроить
<b>Priority (0-240)</b>	Решите, какой порт должен быть заблокирован по приоритету в LAN. Введите значение от 0 до 240. Значение приоритета должно быть кратно 16
<b>Path Cost (1-200000000)</b>	Стоимость пути между двумя устройствами на указанном порту. Введите значение от 1 до 200000000

<b>Admin P2P</b>	В зависимости от типа соединения, сегменты могут быть P2P (то есть, подключены в режиме точка-точка) или в режиме разделяемой среды (когда к одному сегменту подключено несколько устройств). В случае работы в режиме P2P в целях оптимизации работы отсутствуют некоторые лишние функции. Опция позволяет управлять этим свойством вручную. True – P2P включен. False – P2P выключен.
<b>Admin Edge</b>	Порт напрямую соединен с конечными станциями и не может создавать петли в сети. Чтобы настроить порт как edge port, установите значение портов True.
<b>Admin Non STP</b>	На порту используется алгоритм вычислений STP. True - содержит математический расчёт STP. False -не содержит математический расчет STP.
<b>Apply</b>	Нажмите Apply, чтобы активировать настройки

### MSTP - Instance Setting

Instance	State	VLANs	Priority (0-61440)
1	Enable	1-4094	32768

**Priority must be a multiple of 4096.**

Apply

Рис. MSTP Instance

В таблице описаны основные поля:

Поле	Описание
Instance	Установите номер MST instance. От 1 до 15
State	Включить или отключить MST instance
VLANs	Установите соответствие между VLAN и instance
Proprietary (0-61440)	Значение используется для идентификации корневого устройства. Устройство с самым низким значением имеет самый высокий приоритет и выбирается как корневой. Если значение изменяется, вам следует перезагрузить коммутатор. Согласно стандартному правилу протокола, значение должно быть кратным 4096
Apply	Нажмите Apply, чтобы активировать настройки

## MSTP - Instance Port

Instance: CIST ▾

Port	Priority (0-240)	Path Cost (1-200000000, 0:Auto)
Port.01 ▲		
Port.02 ▢		
Port.03	128	0
Port.04		
Port.05 ▼		

Priority must be a multiple of 16

Apply

Рис. MSTP Instance Port

В таблице описаны основные поля:

Поле	Описание
<b>Instance</b>	Введите информацию об instance, за исключением CIST
<b>Port</b>	Выберите порт, который хотите настроить
<b>Priority (0-240)</b>	Решите, какой порт должен быть заблокирован по приоритету. Введите значение от 0 до 240. Значение приоритета должно быть кратно 16
<b>Path Cost (1-200000000)</b>	Стоимость пути на указанном порту. Введите значение от 1 до 200000000
<b>Apply</b>	Нажмите Apply, чтобы активировать настройки

## 5.1.6. Групповая рассылка

### 5.1.6.1. IGMP snooping

Протокол IGMP используется IP хостами для регистрации их участия в динамической многоадресной рассылке. Существует 3 версии IGMP: v1, v2 и v3. Их спецификации представлены соответственно в RFC 1112, 2236 и 3376. IGMP Snooping совершенствует работу сетей, передающих многоадресный трафик. Протокол уменьшает объемы трафика, обеспечивая его доставку только туда, где он требуется.

**IGMP Snooping**

IGMP Snooping :

IGMP Query Mode:

IGMP Snooping Table

IP Address	VLAN ID	Member Port
230.0.0.20	1	Port.07

Рис. IGMP snooping

В таблице описаны основные поля:

Поле	Описание
<b>IGMP Snooping</b>	Включить/отключить IGMP Snooping
<b>IGMP Query Mode</b>	Можно определить коммутатор как IGMP querier. В сети может быть только один IGMP querier. Режим Auto означает, что querier будет устройство с минимальным IP адресом.
<b>IGMP Snooping Table</b>	Показать список групповых рассылок
<b>Help</b>	Показать справку
<b>Apply</b>	Нажмите Apply, чтобы активировать настройки

### 5.1.6.2 MVR

Функция MVR необходима для предоставления возможности устройствам в одном VLAN получать multicast трафик из других VLAN.

**MVR**

MVR Mode:  ▾

MVR VLAN:

Port	Type	Immediate Leave
Port.01	<input type="text" value="Inactive"/> ▾	<input type="checkbox"/>
Port.02	<input type="text" value="Inactive"/> ▾	<input type="checkbox"/>
Port.03	<input type="text" value="Inactive"/> ▾	<input type="checkbox"/>
Port.04	<input type="text" value="Inactive"/> ▾	<input type="checkbox"/>
Port.05	<input type="text" value="Inactive"/> ▾	<input type="checkbox"/>
Port.06	<input type="text" value="Inactive"/> ▾	<input type="checkbox"/>
Port.07	<input type="text" value="Inactive"/> ▾	<input type="checkbox"/>

Рис. IGMP snooping

В таблице описаны основные поля:

Поле	Описание
<b>MVR Mode</b>	Включить или выключить режим MVR
<b>MVR VLAN</b>	Настройка VLAN для MVR
<b>TYPE</b>	Выбрать тип порта: inactive, Receiver, Source
<b>Immediate Leave</b>	Включить или выключить функцию Immediate leave

### 5.1.6.3. Статическая фильтрация группового трафика

Static Multicast Filtering - это система, в которой конечный узлы получают данные только в том случае, если они зарегистрировались в специальных группах. С такой фильтрацией, сетевые устройства будут пересылать групповой трафик только на зарегистрированные адреса.



### Static Multicast Filtering

Multicast IP Address :

Member Ports :

Port.01    Port.02    Port.03    Port.04  
 Port.05    Port.06    Port.07    Port.08  
 G1    G2

	IP Address	Member Ports
<input type="checkbox"/>	230.0.0.6	Port.04, Port.05

Рис. Статическая фильтрация группового трафика

В таблице описаны основные поля:

Поле	Описание
<b>IP Address</b>	Назначьте мультикастовой группе IP адрес из диапазона 224.0.0.0 - 239.255.255.255
<b>Member Ports</b>	Щелкните галочку рядом с номером порта для включения их в группу.
<b>Add</b>	Добавить группу фильтрации
<b>Delete</b>	Удалить запись
<b>Help</b>	Показать помощь

## 5.1.7. Конфигурация портов

### 5.1.7.1. Управление портами

С помощью этой функции вы можете регулировать статус, скорость, дуплекс, управление потоком и безопасность порта.

### Port Control

Port No.	State	Speed/Duplex	Flow Control	Security
Port.01	Enable	AutoNegotiation	Symmetric	Disable
Port.02	Enable	AutoNegotiation	Symmetric	Disable
Port.03	Enable	AutoNegotiation	Symmetric	Disable
Port.04	Enable	AutoNegotiation	Symmetric	Disable
Port.05	Enable	AutoNegotiation	Symmetric	Disable
Port.06	Enable	AutoNegotiation	Symmetric	Disable
Port.07	Enable	AutoNegotiation	Symmetric	Disable
Port.08	Enable	AutoNegotiation	Symmetric	Disable
Port.09	Enable	AutoNegotiation	Symmetric	Disable

Рис. Управление портами

В таблице описаны основные поля:

Поле	Описание
Port NO.	Номер порта
Speed/Duplex	Вы можете установить режим автоматического согласования, 100 full, 100 half, 10 full, 10 half
Flow Control	Поддерживает симметричный и асимметричный режим, чтобы избежать потери пакета при возникновении перегрузки.
Security	Поддерживает функцию безопасности портов. При включении функции порт прекращает динамически запоминать MAC адреса
Apply	Нажмите Apply, чтобы активировать настройки

### 5.1.7.2. Состояние портов

Эта информация показывает текущее состояние портов.

### Port Status

Port No.	Type	Link	State	Speed/Duplex	Flow Control
Port.01	100TX	Down	Enable	N/A	N/A
Port.02	100TX	Down	Enable	N/A	N/A
Port.03	100TX	Down	Enable	N/A	N/A
Port.04	100TX	Down	Enable	N/A	N/A

Рис. Состояние портов

### 5.1.7.3. Наименование порта

Пользователь может определить имя каждого порта, а так же настраивать их.

**Port Alias**

Port No.	Port Alias
Port.01	<input type="text"/>
Port.02	<input type="text"/>
Port.03	<input type="text"/>
Port.04	<input type="text"/>
Port.05	<input type="text"/>

Рис. Наименование порта

### 5.1.7.4. Ограничение скорости

С помощью этой функции вы можете ограничить передачу данных на всех портах, включая широковещательную, многоадресную и одноадресную передачу. Вы также можете выбрать значения Ingress (входящий) или Egress (исходящий), чтобы ограничить скорость передачи трафика, получаемого или передаваемого.

**Rate Limit**

Port No.	Ingress Limit Frame Type	Ingress	Egress
Port.01	All <input type="text"/>	0 kbps	0 kbps
Port.02	All <input type="text"/>	0 kbps	0 kbps
Port.03	All <input type="text"/>	0 kbps	0 kbps
Port.04	All <input type="text"/>	0 kbps	0 kbps
Port.05	All <input type="text"/>	0 kbps	0 kbps

Рис. Ограничение скорости

В таблице описаны основные поля:

Поле	Описание
<b>Ingress Limit Frame Type</b>	Выбор из режимов: “All”, “Broadcast only”, “Broadcast/Multicast”, или “Broadcast/Multicast/Flooded Unicast”
<b>Ingress</b>	Получаемые портом данные
<b>Egress</b>	Отправляемые портом данные
<b>Apply</b>	Нажмите Apply, чтобы активировать настройки

### 5.1.7.5. Транки

#### Port Trunk - Setting

Вы можете выбрать статический транк или 802.3ad LACP для того, чтобы объединять физические связи в логическую связь для увеличения пропускной способности.

**Port Trunk - Setting**

Port No.	Group ID	Type
Port.01	None	Static
Port.02	None	Static
Port.03	None	Static
Port.04	None	Static
Port.05	None	Static
Port.06	None	Static
Port.07	None	Static
Port.08	None	Static
Port.09	None	Static
Port.10	None	Static
Port.11	None	Static
Port.12	None	Static
Port.13	None	Static
Port.14	None	Static
Port.15	None	Static
Port.16	None	Static
Port.17	None	Static

802.3ad LACP Work Ports

Group ID	Work Ports
Trunk1	max
Trunk2	max
Trunk3	max
Trunk4	max
Trunk5	max
Trunk6	max
Trunk7	max
Trunk8	max
Trunk9	max
Trunk10	max
Trunk11	max
Trunk12	max

Apply Help

Рис. Port Trunk – Setting

В таблице описаны основные поля:

Поле	Описание
<b>Group ID</b>	Выберите порт, который будет присоединён к транку.
<b>Type</b>	Поддерживает статический транк и 802.3ad LACP
<b>Work Port</b>	Выберите количество активных портов в динамической группе LACP. По умолчанию, используется максимально количество портов. Если число отлично от максимального, будут задействованы неактивные порты из динамической группы.
<b>Apply</b>	Нажмите Apply, чтобы активировать настройки

### Транк – Статус

Вы можете проверить статус транка.

### Port Trunk - Status

Group ID	Trunk Member	Type
Trunk 1	N/A	Static
Trunk 2	N/A	Static
Trunk 3	N/A	Static
Trunk 4	N/A	Static
Trunk 5	N/A	Static

Рис. Гранк – Статус

#### 5.1.7.6. Loop Guard

Эта функция защищает от кольцевой атаки, когда порт получает кольцевой пакет. В таком случае, порт автоматически станет неактивным.

### Loop Guard

Port No.	Active	Port State
Port.01	<input type="checkbox"/>	Enable
Port.02	<input type="checkbox"/>	Enable
Port.03	<input type="checkbox"/>	Enable

Рис. Loop Guard

В таблице описаны основные поля:

Поле	Описание
Active	Включение или выключение функции на порту
Port Status	Статус работы порта

#### 5.1.8. VLAN

Виртуальная локальная сеть – логическое объединение сетей, ограничивающее широковещание и позволяющее изолировать трафик сети, члены одной VLAN могут обмениваться данными друг с другом. Фактически, создание VLAN на коммутаторе эквивалентно логическому разделению устройств на разные сети. Однако, все устройства сети все еще физически подключены к одному устройству.

Коммутатор поддерживает VLAN на основе портов и 802.1Q (на основе тегов). По умолчанию, режима работы VLAN - 802.1Q.

### 5.1.8.1. Настройка VLAN

VLAN на основе тегов соответствует стандарту спецификации IEEE 802.1Q, поэтому можно создавать VLAN между устройствами разных производителей. IEEE 802.1Q VLAN использует технику вставки «тега» в Ethernet фреймы. Тег содержит идентификатор VLAN (VID), который указывает на номер VLAN.

Вы можете создать VLAN на основе тегов, а также включить или отключить GVRP протокол. Всего доступно 256 групп VLAN. При включении VLAN 802.1Q все порты коммутатора принадлежат VLAN по умолчанию, VID которой 1. VLAN по умолчанию нельзя удалить.

GVRP — сетевой протокол, позволяющий устройству локальной сети сообщить соседним устройствам, что оно желает принять пакеты для одной или нескольких VLAN. Главная цель GVRP — позволить коммутаторам автоматически обнаружить информацию о VLAN, которая иначе должна была бы быть вручную сконфигурирована в каждом коммутаторе.

**VLAN Setting**

VLAN Operation Mode : 802.1Q ▾

GVRP Mode : Disable ▾

Management VLAN ID : 0

Port VLAN Setting

Port No.	Link Type	PVID	Untagged VIDs	Tagged VIDs
Port.01	Access ▾	1	1	
Port.02	Access ▾	1	1	
Port.03	Access ▾	1	1	

Рис. Настройка VLAN

В таблице описаны основные поля:

Поле	Описание
<b>VLAN Operation Mode</b>	Настройка режима работы VLAN: выключена, на основе портов, 802.1Q

<b>GVRP Mode</b>	Включить/отключить функцию GVRP
<b>Management VLAN ID</b>	Management VLAN ID - это номер VLAN, через который устройство можно настраивать. Доступ к настройке коммутатора может предоставляться только для устройств в этом VLAN
<b>Link Type</b>	Есть 3 вида соединений: Access Link: присвоение портам своих VID. Trunk Link: расширенная версия Access Link; присваивания разных VID одному порту Hybrid Link: доступны Access Link и Trunk Link Hybrid (QinQ) Link: включает режим QinQ; позволяет вставить дополнительный тег во VLAN фрейм.
<b>Untagged VID</b>	Установите VLAN ID по умолчанию, которое будет использовано при поступлении нетегированных данных на этот порт. Интервал от 1 до 4094.
<b>Tagged VIDs</b>	Установите VID, данные которых будут передаваться с устройства.
<b>Apply</b>	Нажмите Apply, чтобы активировать настройки

### 5.1.8.2. Настройка VLAN на основе портов

Трафик передается на порты членов той же VLAN группы. В режиме работы VLAN по портам, пакеты в одной группе передаются без ограничения типов.

Заметьте, что все невыбранные порты будут отображены как принадлежащие к другой VLAN. Если включена VLAN на основе порта, VLAN тегирование использоваться не будет.

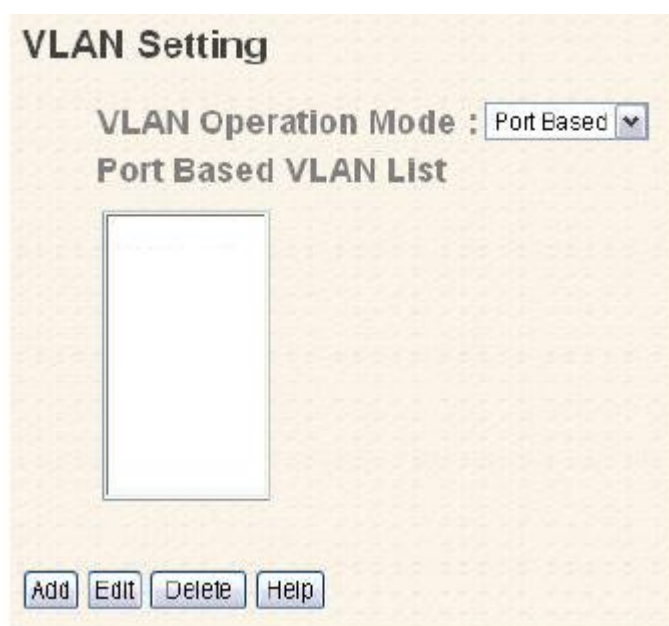




Рис. Настройка VLAN на основе портов

В таблице описаны основные поля:

Поле	Описание
<b>Add</b>	Нажмите Add, чтобы добавить VLAN
<b>Edit</b>	Изменить существующий VLAN
<b>Delete</b>	Удалить существующий VLAN
<b>Help</b>	Показать справку

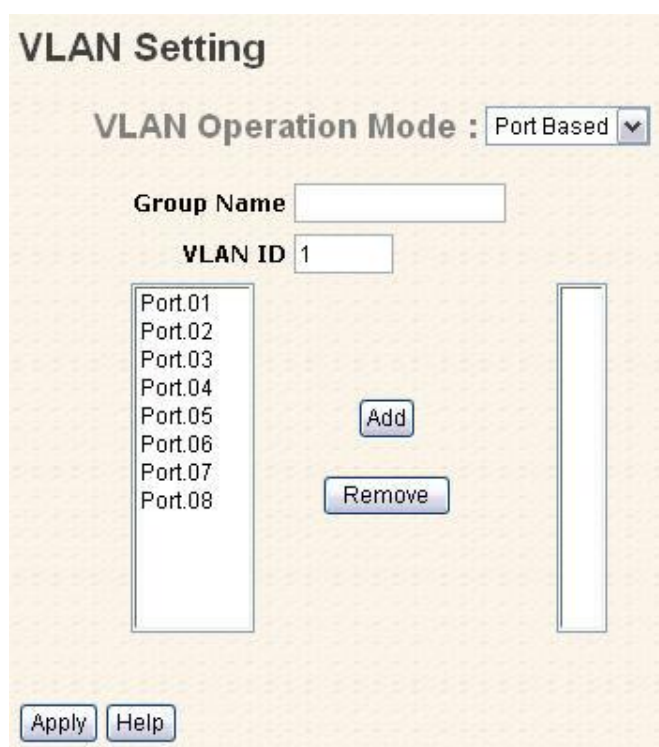


Рис. Установка VLAN

В таблице описаны основные поля:

Поле	Описание
<b>Group Name</b>	Имя группы VLAN
<b>VLAN ID</b>	Введите VLAN ID
<b>Add</b>	Выберите порт для подключения к группе VLAN
<b>Remove</b>	Удалить порт из группы VLAN
<b>Apply</b>	Нажмите Apply, чтобы активировать настройки

Help	Показать справку
------	------------------

### 5.1.9. Приоритезация трафика

Приоритезация трафика включает 3 режима: на основе порта, 802.1p/COS и TOS/DSCP. С помощью этой функции можно разделить трафик на 4 класса для разной обработки. SWM-240 поддерживают 4 очереди по приоритету.

#### 5.1.9.1 Qos policy

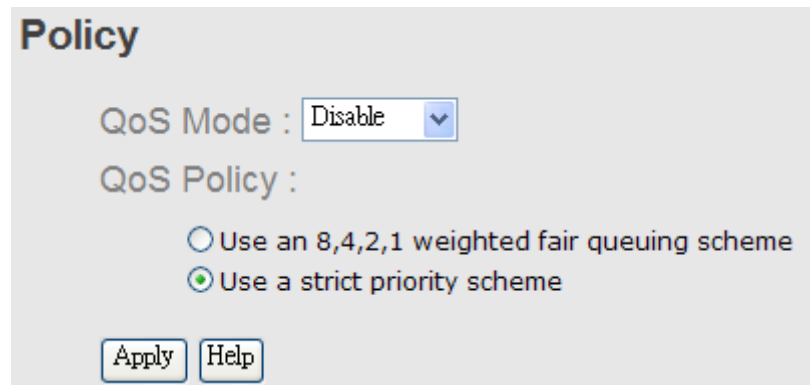


Рис. Приоритезация трафика

В таблице описаны основные поля:

Поле	Описание
<b>QoS Mode</b>	Port-base: Приоритет определяется входным портом COS only: Приоритет определяется только COS TOS only: Приоритет определяется только TOS COS first: Приоритет определяется COS и TOS, но в первую очередь COS TOS first: Приоритет определяется COS и TOS, но в первую очередь TOS
<b>QoS Policy</b>	Использование схемы взвешенной справедливой очереди 8,4,2,1: очереди будут следовать соотношению 8:4:2:1 для передачи пакетов по очереди, от высшей к низшей. Например: За одну единицу времени передаются 8 пакетов высшей приоритетности, 4 пакета средней приоритетности, 2 пакета низкой приоритетности и один пакет низшей приоритетности. Использовать строгую приоритетную очередь: Пакеты высшей приоритетности всегда передаются первыми, пока они не закончатся. То есть, сначала передаются все пакеты высшего приоритета; после того, как они закончились, могут передаваться пакеты более низкого приоритета и так далее.
<b>Apply</b>	Нажмите Apply, чтобы активировать настройки
<b>Help</b>	Показать справку

### 5.1.9.2 Port-base priority

**Port-based Priority**

Port No.	Priority
Port.01	Lowest
Port.02	Lowest
Port.03	Lowest
Port.04	Lowest
Port.05	Lowest
Port.06	Lowest
Port.07	Lowest
Port.08	Lowest

Рис. Port-based Priority

В таблице описаны основные поля:

Поле	Описание
<b>Port base Priority</b>	Назначьте порту приоритетную очередь. Можно назначить 4 очереди: высокая, средняя, низкая и низшая.
<b>Help</b>	Показать справку
<b>Apply</b>	Нажмите Apply, чтобы активировать настройки

### 5.1.9.3 COS/802.1p

COS/802.1p		COS Port Default	
<b>COS</b>	<b>Priority</b>	<b>Port No.</b>	<b>COS</b>
0	Lowest	Port.01	0
1	Lowest	Port.02	0
2	Low	Port.03	0
3	Low	Port.04	0
4	Middle	Port.05	0
5	Middle	Port.06	0
6	High	Port.07	0
7	High		

Рис. COS/802.1p

В таблице описаны основные поля:

Поле	Описание
<b>COS/802.1p</b>	COS (Класс обслуживания) известен как 802.1p. Он описывает процесс определения приоритета пакета с помощью поля приоритета пользователя в теге 802.1Q VLAN. Значение приоритета принимают значения от 0 до 7, что проецируется на 4 очереди: высокая, средняя, низкая и низшая.
<b>COS Port Default</b>	Если у входного пакета отсутствует VLAN тег, исходное значение приоритета определяется входным портом.
<b>Help</b>	Показать справку
<b>Apply</b>	Нажмите Apply, чтобы активировать настройки

#### 5.1.9.4 TOS/DSCP

**TOS/DSCP**

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

Apply Help

Рис. TOS/DSCP интерфейс

В таблице описаны основные поля:

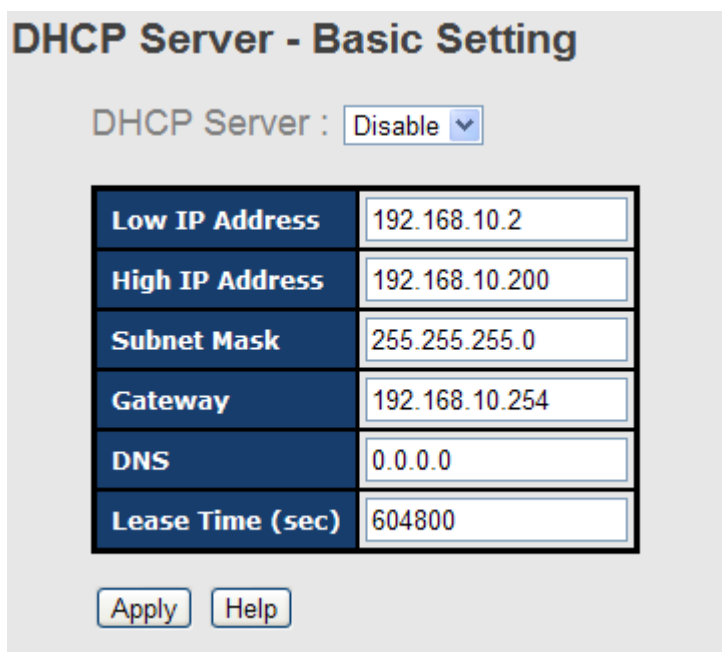
Поле	Описание
<b>TOS/DSCP</b>	TOS (Тип обслуживания) – поле в IP заголовке пакета. Поле TOS также используется в дифференцированном обслуживании (DiffServ) и называется

	DSCP (Differentiated Services Code Point). С помощью этого поля можно указать приоритет пакета, его значение может быть от 0 до 63. Значения DSCP проецируются на 4 очереди приоритетности: высокая, средняя, низкая и низшая.
<b>Help</b>	Показать справку
<b>Apply</b>	Нажмите Apply, чтобы активировать настройки

## 5.1.10. DHCP сервер

### 5.1.10.1. DHCP сервер – Установка

Коммутатор может быть DHCP сервером.



**DHCP Server - Basic Setting**

DHCP Server :

<b>Low IP Address</b>	<input type="text" value="192.168.10.2"/>
<b>High IP Address</b>	<input type="text" value="192.168.10.200"/>
<b>Subnet Mask</b>	<input type="text" value="255.255.255.0"/>
<b>Gateway</b>	<input type="text" value="192.168.10.254"/>
<b>DNS</b>	<input type="text" value="0.0.0.0"/>
<b>Lease Time (sec)</b>	<input type="text" value="604800"/>

Рис. DHCP сервер – Установка

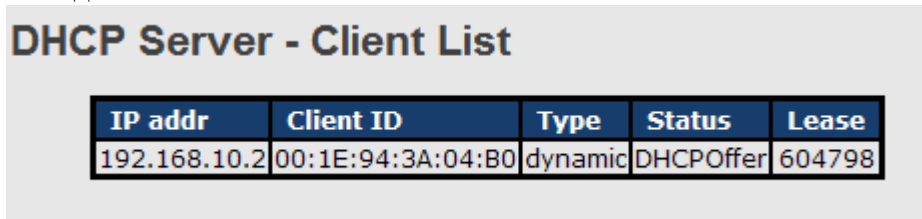
В таблице описаны основные поля:

Поле	Описание
<b>DHCP Server</b>	Включение или выключение функции DHCP сервера. При включении коммутатор будет DHCP сервером в вашей локальной сети.
<b>Start IP Address</b>	Первый адрес в диапазоне присваиваемых IP адресов. Например, если необходим диапазон от 192.168.1.100 до 192.168.1.200, то указать нужно 192.168.1.100

<b>End IP Address</b>	Последний адрес в диапазоне присваиваемых IP адресов. Например, если необходим диапазон от 192.168.1.100 до 192.168.1.200, то указать нужно 192.168.1.200
<b>Subnet Mask</b>	Маска подсети для присваиваемых IP адресов
<b>Gateway</b>	Сетевой шлюз вашей сети
<b>DNS</b>	IP адрес DNS сервера
<b>Lease Time (Hour)</b>	Время (в часах), на которое выдаётся адрес. Нужно на случай, если адрес освободится, так как иначе сервер не узнает об этом.
<b>Apply</b>	Нажмите Apple, чтобы активировать настройки

### 5.1.10.2. DHCP сервер – список устройств

При включении функции DHCP, устройство будет собирать информацию с DHCP клиентов и выведет ее в этом окне.



IP addr	Client ID	Type	Status	Lease
192.168.10.2	00:1E:94:3A:04:B0	dynamic	DHCP Offer	604798

Рис. DHCP сервер – список устройств

### 5.1.10.3. DHCP сервер – Закрепление IP адресов за портами

Вы можете назначить определённый IP адрес, который входит в интервал назначенного динамического IP. Устройство, подключившись к порту, запрашивает динамический IP; система назначает IP адрес, назначенный ранее подключенному устройству.

**DHCP Server - Port and IP Binding**

Port	IP
Port.01	192.168.10.123
Port.02	0.0.0.0
Port.03	0.0.0.0
Port.04	0.0.0.0
Port.05	0.0.0.0

Рис. DHCP сервер – Закрепление IP адресов за портами

#### 5.1.10.4. DHCP сервер - агент DHCP

DHCP агент перенаправляет DHCP сообщения между клиентами и серверами DHCP, находящимися в разных подсетях. Для этого, устройство использует Option 82 для внедрения информации в пакеты, передаваемые на DHCP сервер, и, в соответствии с Option 82, извлекая информацию из ответов, во время пересылки их к DHCP клиенту.

**DHCP Relay Agent**

Mode :  ▾

DHCP Server IP Address

1st Server IP	<input type="text" value="0.0.0.0"/>	VID	<input type="text" value="1"/>
2nd Server IP	<input type="text" value="0.0.0.0"/>	VID	<input type="text" value="1"/>
3rd Server IP	<input type="text" value="0.0.0.0"/>	VID	<input type="text" value="1"/>
4th Server IP	<input type="text" value="0.0.0.0"/>	VID	<input type="text" value="1"/>

DHCP Option 82 Remote ID

Type	<input type="text" value="IP"/> ▾
Value	<input type="text" value="192.168.10.1"/>
Display	<input type="text" value="COA80A01"/>

DHCP Option 82 Circuit-ID Table

Port No.	Circuit-ID	Option 82
Port.01	000400010001	<input type="checkbox"/>
Port.02	000400010002	<input type="checkbox"/>
Port.03	000400010003	<input type="checkbox"/>
Port.04	000400010004	<input type="checkbox"/>
Port.05	000400010005	<input type="checkbox"/>
Port.06	000400010006	<input type="checkbox"/>

В таблице описаны основные поля:

Поле	Описание
<b>DHCP Relay</b>	Включение или выключение функции
<b>DHCP Server IP Address and VID</b>	Выберите IP адрес и VID DHCP сервера. Если вы оставите “0.0.0.0”, значит сервер не активен.
<b>DHCP Option 82 Remote ID</b>	Идентификатор удалённого сервера. Поддерживается 4 типа: IP, MAC, Client-ID и Other.
<b>DHCP Option 82 Circuit-ID Table</b>	Локальный идентификатор последовательности, необходимый DHCP агенту для отправки ответа обратно к клиенту.
<b>Apply</b>	Применить

### 5.1.11. SNMP

Простой протокол управления сетями (SNMP) – протокол, разработанный для управления узлами (серверами, рабочими станциями, роутерами, коммутаторами, концентраторами и т.д.) в IP сети. SNMP позволяет администраторам сети управлять производительностью сети, находить и решать проблемы сети и планировать ее расширение. Системы управления сетями узнают о проблеме, получая trap-сообщения и уведомления об изменениях от устройств сети, поддерживающих SNMP.

#### 5.1.11.1. SNMP - Настройка агента

Вы можете настроить информацию, связанную с SNMP агентом с помощью опции Agent Setting.



### SNMP - Agent Setting

SNMP Agent Version

### SNMP V1/V2c Community

Community String	Privilege
<input type="text" value="public"/>	Read Only
<input type="text" value="private"/>	Read and Write
<input type="text"/>	Read Only
<input type="text"/>	Read Only

Рис. SNMP - Настройка агента

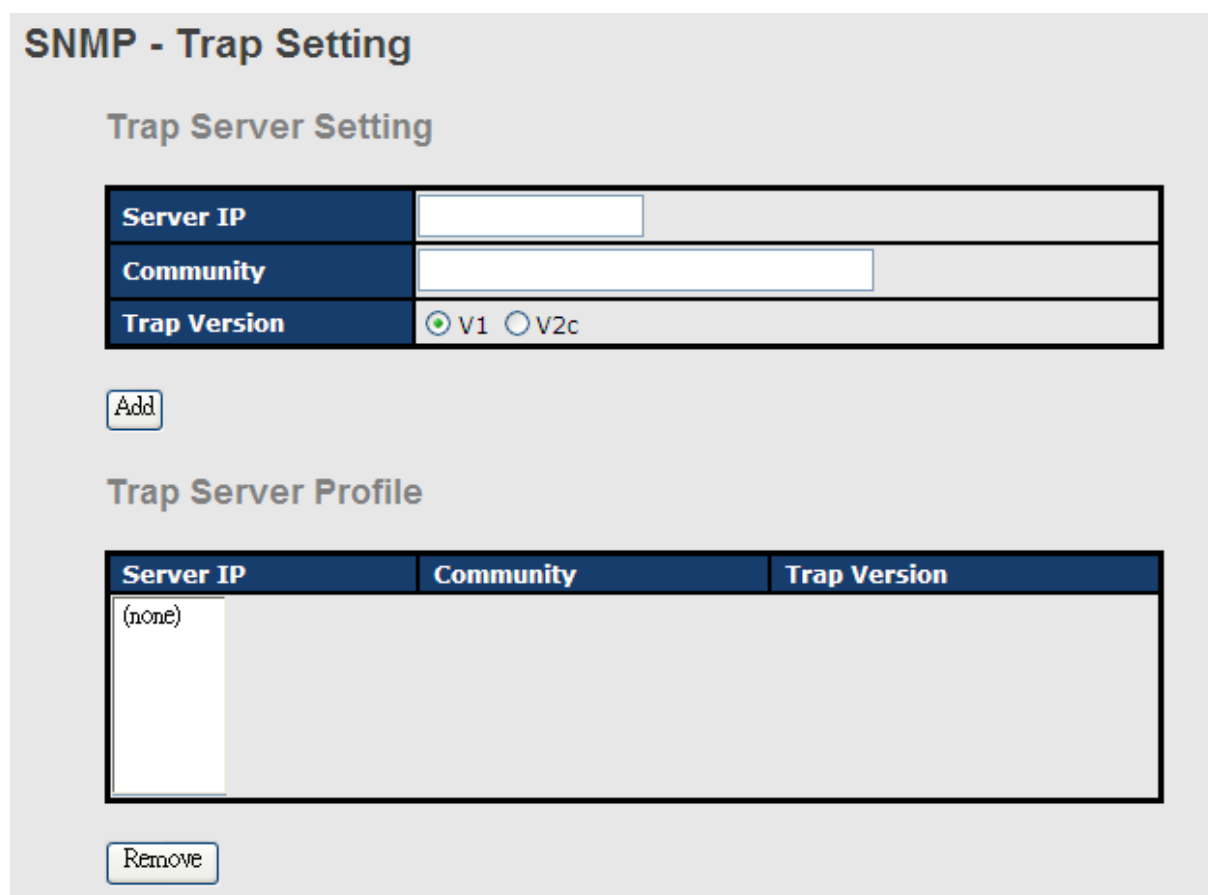
В таблице описаны основные поля:

Поле	Описание
<b>SNMP – Agent Version</b>	Поддерживаются 3 версии SNMP: SNMPV1/SNMPV2c и SNMPV3. SNMPV1 SNMPV2c агент для аутентификации проверяет на соответствие community string. SNMPv3 запрашивает уровень аутентификации с шифрованием данных MD5 или DES.
<b>SNMP V1/V2c Community</b>	Следует указать SNMP Community. Поддерживаются 4 соотношения «Community String/Privilege». Каждая Community String может содержать максимум 32 символа. Чтобы удалить Community String, оставьте поле пустым.
<b>SNMP V3 User</b>	<p>Если выбран SNMP V3, для аутентификации необходимо указать пользователя SNMPv3. Пароль (Auth Password) зашифрован по MD5, а конфиденциальный пароль (Privacy Password) по DES. Максимальное количество пользователей SNMPv3 – 8, максимальное количество символов в имени пользователя и пароле – 16.</p> <p>Если выбран SNMPv3 agent, можно:</p> <ol style="list-style-type: none"> <li>1 Ввести только имя пользователя SNMPv3</li> <li>2 Ввести только имя пользователя и пароль SNMPv3</li> <li>3 Ввести только имя пользователя, пароль и конфиденциальный пароль SNMPv3, который может отличаться от основного пароля</li> </ol> <p>Чтобы удалить текущий профиль пользователя:</p> <ol style="list-style-type: none"> <li>1 Введите имя пользователя SNMPv3, которое хотите удалить</li> </ol>

	2 Нажмите кнопку Remove
<b>Current SNMPv3 User Profile</b>	Показать все профили пользователей SNMPv3
<b>Apply</b>	Нажмите Apply, чтобы активировать настройки
<b>Help</b>	Показать справку

### 5.1.11.2. SNMP - Настройка SNMP traps

Trap сервер – это станция управления, получающая trap-сообщения - сигналы системы, сгенерированные коммутаторами. Если trap сервер не задан, trap-сообщения не генерируются. Укажите trap сервер - введите IP адрес сервера и Community String.



**SNMP - Trap Setting**

**Trap Server Setting**

<b>Server IP</b>	<input type="text"/>
<b>Community</b>	<input type="text"/>
<b>Trap Version</b>	<input checked="" type="radio"/> V1 <input type="radio"/> V2c

**Trap Server Profile**

Server IP	Community	Trap Version
(none)		

Рис. SNMP - Настройка SNMP traps

В таблице описаны основные поля:

Поле	Описание
<b>Server IP</b>	IP адрес сервера для отправки trap-сообщений

<b>Community</b>	Community string для аутентификации
<b>Trap Version</b>	Версия Trap поддерживает V1 и V2c
<b>Add</b>	Добавить trap сервер
<b>Remove</b>	Удалить trap сервер
<b>Help</b>	Показать справку

### 5.1.11.3. SNMPv3

**NMP - SNMPv3 Setting**

SNMPv3 Engine ID: f465000003001e940a002b

**Context Table**

Context Name :

**User Table**

Current User Profiles : <input type="button" value="Remove"/>	New User Profile : <input type="button" value="Add"/>	
(none)	User ID:	<input type="text"/>
	Authentication Password:	<input type="text"/>
	Privacy Password:	<input type="text"/>

**Group Table**

Current Group content : <input type="button" value="Remove"/>	New Group Table: <input type="button" value="Add"/>	
(none)	Security Name (User ID):	<input type="text"/>
	Group Name:	<input type="text"/>

Current Access Tables : <input type="button" value="Remove"/>	New Access Table : <input type="button" value="Add"/>	
(none)	Context Prefix:	<input type="text"/>
	Group Name:	<input type="text"/>
	Security Level:	<input type="radio"/> NoAuthNoPriv. <input type="radio"/> AuthNoPriv. <input type="radio"/> AuthPriv.
	Context Match Rule	<input type="radio"/> Exact <input type="radio"/> Prefix
	Read View Name:	<input type="text"/>
	Write View Name:	<input type="text"/>
	Notify View Name:	<input type="text"/>

### MIBView Table

Current MIBTables : <input type="button" value="Remove"/>	New MIBView Table : <input type="button" value="Add"/>	
(none)	View Name:	<input type="text"/>
	SubOid-Tree:	<input type="text"/>
	Type:	<input type="radio"/> Excluded <input type="radio"/> Included

**Note:**

Any modification of SNMPv3 tables might cause MIB accessing rejection. Please take notice of the causality between the tables before you modify these tables.

Поле	Описание
<b>Context Table</b>	Настройка контекстной таблицы SNMPv3. Выберите название для таблицы.
<b>User Table</b>	1. Настройки пользовательской таблицы SNMPv3 2. User ID: введите имя пользователя. 3. Authentication Password: введите пароль 4. Privacy Password: введите секретный пароль 5. Нажмите "Add" для добавления значения 6. Нажмите Remove для удаления значения
<b>Group Table</b>	1. Настройка групповой таблицы SNMPv3 2. Security Name (User ID): сопоставьте имя пользователя, которое вы ввели в пользовательской таблице 3. Group Name: Введите название группы 4. Нажмите "Add" для добавления значения 5. Нажмите Remove для удаления значения

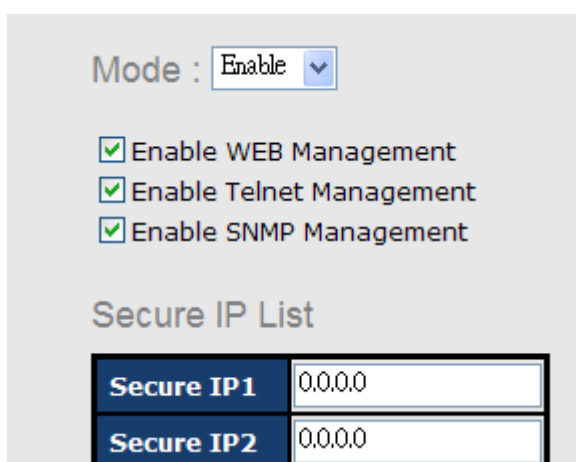
<b>Access Table</b>	<ol style="list-style-type: none"> <li>1. Настройка таблицы доступа SNMPv3</li> <li>2. Context Prefix: выберите контекстное имя</li> <li>3. Group Name: выберите группу</li> <li>4. Security Level: выберите уровень безопасности</li> <li>5. Context Match Rule: выберите контекстное правило.</li> <li>6. Read View Name: Выберите имя чтения.</li> <li>7. Write View Name: Выберите имя записи.</li> <li>8. Notify View Name: выберите имя оповещения.</li> <li>9. Нажмите “Add” для добавления значения</li> <li>10. Нажмите Remove для удаления значения</li> </ol>
<b>MIBview Table</b>	<ol style="list-style-type: none"> <li>1. Настройка таблицы MIB view</li> <li>2. ViewName: Выберите имя</li> <li>3. Sub-Oid Tree: Заполните Sub OID</li> <li>4. Type: выберите тип - исключающий или включающий.</li> <li>5. Нажмите “Add” для добавления значения</li> <li>6. Нажмите Remove для удаления значения</li> </ol>
<b>Help</b>	Показать файл помощи

## 5.1.12. Безопасность

5 разделов помогут улучшить безопасность коммутатора: IP Security, Port Security, MAC Blacklist и MAC address Aging и протокол 802.1x.

### 5.1.12.1. Безопасность IP

IP Security может включать или отключать функцию удаленного управления устройством через WEB или Telnet, или SNMP. К тому же, IP Security может ограничивать доступ к управлению указанными IP адресами. Только с этих IP адресов можно будет удаленно управлять коммутатором.



The screenshot shows a configuration window for IP Security. At the top, there is a 'Mode' dropdown menu set to 'Enable'. Below it are three checked checkboxes: 'Enable WEB Management', 'Enable Telnet Management', and 'Enable SNMP Management'. Under the heading 'Secure IP List', there are two rows of input fields. The first row is labeled 'Secure IP1' and the second 'Secure IP2', both with the value '0.0.0.0' entered in the adjacent text boxes.

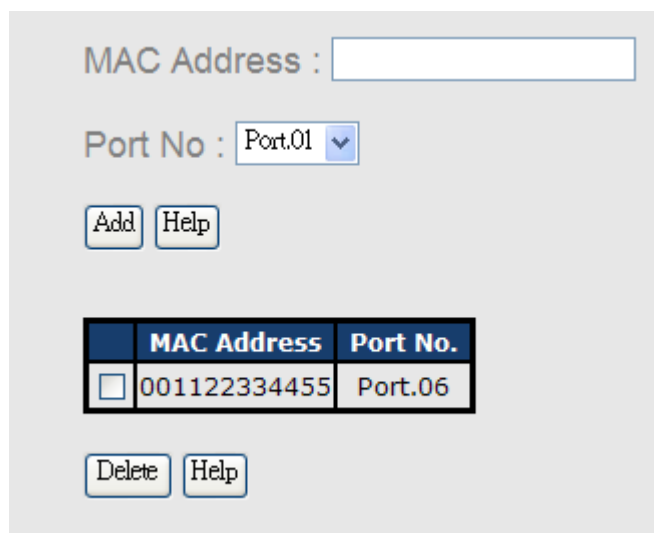
Рис. Безопасность IP

В таблице описаны основные поля:

Поле	Описание
<b>IP Security Mode</b>	Включить или отключить функцию IP безопасности
<b>Enable WEB Management</b>	Нажмите для включения функции управления через веб-браузер
<b>Enable Telnet Management</b>	Нажмите для включения функции управления через Telnet
<b>Enable SNMP Management</b>	Нажмите для включения функции управления через SNMP
<b>Apply</b>	Нажмите Apply, чтобы активировать настройки
<b>Help</b>	Показать справку

### 5.1.12.2. Безопасность портов

Функция безопасности портов позволяет добавлять статические MAC адреса в таблицу коммутации. При включении функции Port Security на странице Port Control, будут передаваться только кадры с данных адресов, все остальные будут отбрасываться.



MAC Address :

Port No : Port.01 ▼

	MAC Address	Port No.
<input type="checkbox"/>	001122334455	Port.06

Рис. Безопасность портов

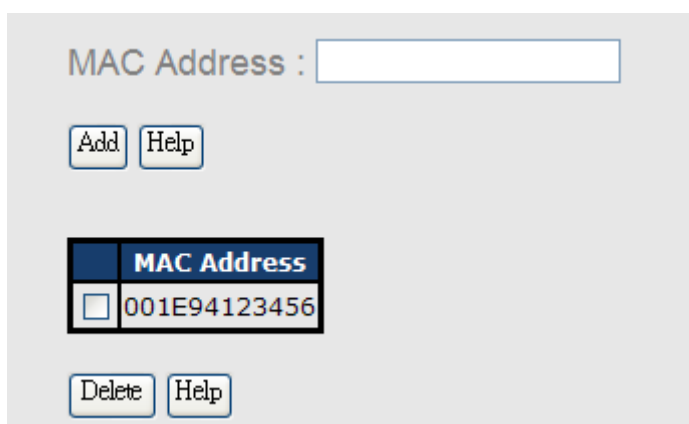
В таблице описаны основные поля:

Поле	Описание
<b>MAC Address</b>	Введите MAC адрес для указанного порта
<b>Port NO.</b>	Выберите порт коммутатора

<b>Add</b>	Добавьте запись
<b>Delete</b>	Удалить запись
<b>Help</b>	Показать справку

### 5.1.12.3. Черный список MAC адресов

Функция MAC Blacklist позволяет фильтровать трафик, передающийся на MAC адреса из списка. Любые пакеты, передающиеся на эти MAC адреса, будут отброшены.



The screenshot shows a web interface for configuring a MAC blacklist. At the top, there is a label 'MAC Address :' followed by an empty text input field. Below this are two buttons: 'Add' and 'Help'. In the center, there is a table with a dark blue header 'MAC Address'. The table contains one row with a checkbox on the left and the MAC address '001E94123456' on the right. Below the table are two more buttons: 'Delete' and 'Help'.

Рис. Черный список MAC адресов

В таблице описаны основные поля:

Поле	Описание
<b>MAC Address</b>	Введите MAC адрес, который будет добавлен в чёрный список MAC адресов
<b>Port NO.</b>	Выберите порт коммутатора
<b>Add</b>	Добавить запись
<b>Delete</b>	Удалить запись
<b>Help</b>	Показать справку

### 5.1.12.4. 802.1x

#### 802.1x – Radius сервер

802.1x позволяет централизованно управлять правами для аутентификации и авторизации. Обратитесь к стандарту IEEE 802.1X - Port Based Network Access Control.

### 802.1x - Radius Server

Radius Server Setting

<b>802.1x Protocol</b>	Enable <input type="button" value="v"/>
<b>Radius Server IP</b>	192.168.16.3
<b>Server Port</b>	1812
<b>Accounting Port</b>	1813
<b>Shared Key</b>	12345678
<b>NAS, Identifier</b>	NAS_L2_SWITCH

Advanced Setting

<b>Quiet Period</b>	60
<b>TX Period</b>	30
<b>Supplicant Timeout</b>	30
<b>Server Timeout</b>	30
<b>Max Requests</b>	2
<b>Re-Auth Period</b>	3600

Рис. 802.1x – Radius сервер

В таблице описаны основные поля:

Поле	Описание
<b>Radius Server Setting</b>	
<b>Radius Server IP</b>	IP адрес сервера аутентификации
<b>Server Port</b>	Установите номер UDP порта, используемого сервером для аутентификации
<b>Account port</b>	Установите номер UDP порта для запросов учетных записей на указанном Radius сервере.
<b>Shared key</b>	Ключ, совместно используемый коммутатором и сервером аутентификации
<b>NAS, Identifier</b>	Строка, используемая для идентификации коммутатора



Advanced Setting	
<b>Quiet Period</b>	Установите интервал времени между ошибкой аутентификации и новой попыткой
<b>Tx Period</b>	Установите время, в течение которого коммутатор будет ожидать ответ на EAP запрос до повторной отправки запроса на сервер
<b>Supplicant Timeout</b>	Установите время, в течение которого коммутатор будет ожидать ответ на EAP запрос от клиента
<b>Server Timeout</b>	Установите время, в течение которого коммутатор будет ожидать ответ на запрос аутентификации с Radius сервера
<b>Max Requests</b>	Установите максимальное количество попыток отправки данных запрашивающему устройству
<b>Re-Auth Period</b>	Установите интервал времени, после которого подключённые клиенты должны быть повторно аутентифицированы
<b>Apply</b>	Нажмите Apply, чтобы активировать настройки
<b>Help</b>	Показать справку

### 802.1x - Режим авторизации по портам

Здесь вы можете настроить режим 802.1x авторизации для каждого порта.

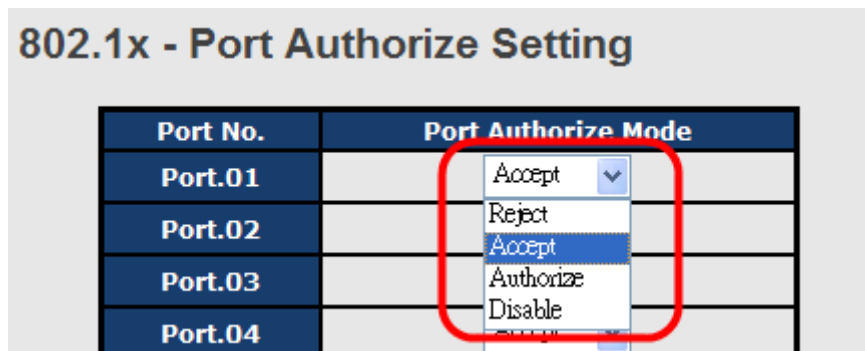


Рис. 802.1x - Режим авторизации по портам

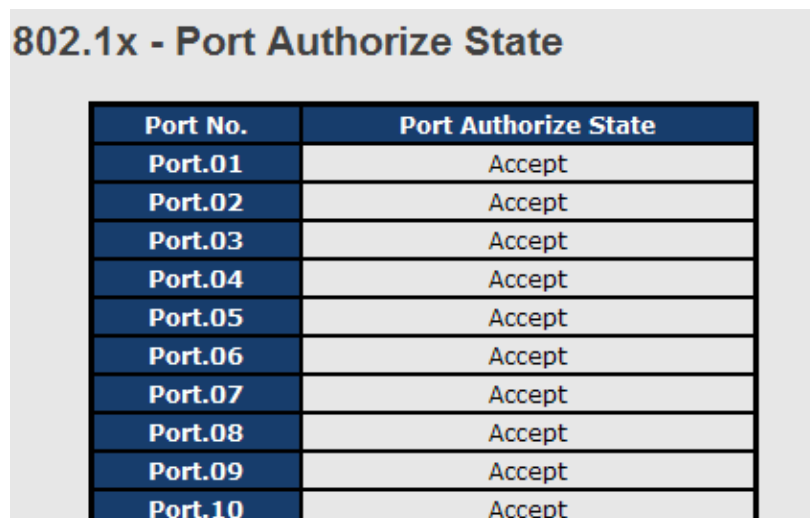
В таблице описаны основные поля:

Поле	Описание
<b>Port Authorized Mode</b>	<p>Режимы авторизации:</p> <ul style="list-style-type: none"> <li>● Reject: на этом порту авторизация запрещена</li> <li>● Ассепт: на этом порту авторизация обязательна</li> <li>● Authorize: состояние этого порта определяется настройками 802.1x аутентификации</li> </ul>

	<ul style="list-style-type: none"> <li>● Disable: этот порт не будет участвовать в 802.1x</li> </ul>
<b>Apply</b>	Нажмите Apply, чтобы применить настройки
<b>Help</b>	Показать справку

### 802.1x - Состояние авторизации по портам

На данной странице отображается состояние авторизации 802.1x по портам



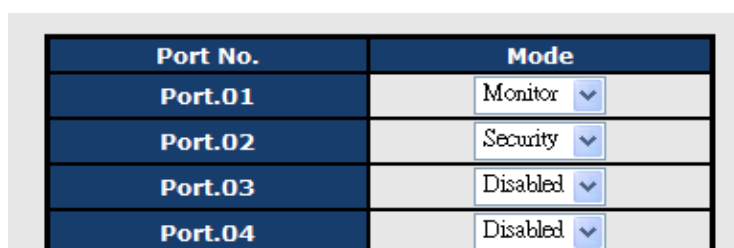
Port No.	Port Authorize State
Port.01	Accept
Port.02	Accept
Port.03	Accept
Port.04	Accept
Port.05	Accept
Port.06	Accept
Port.07	Accept
Port.08	Accept
Port.09	Accept
Port.10	Accept

Рис. 802.1x - Состояние авторизации по портам

### 5.1.12.5 IP Guard

#### IP Guard – Port Setting

IP Guard - интеллектуальная функция, используемая для обеспечения безопасности устройства и блокирует указанные IP адреса (или не разрешённые вручную), не давая им доступа в сеть.



Port No.	Mode
Port.01	Monitor
Port.02	Security
Port.03	Disabled
Port.04	Disabled

Рис. IP Guard – Port Setting

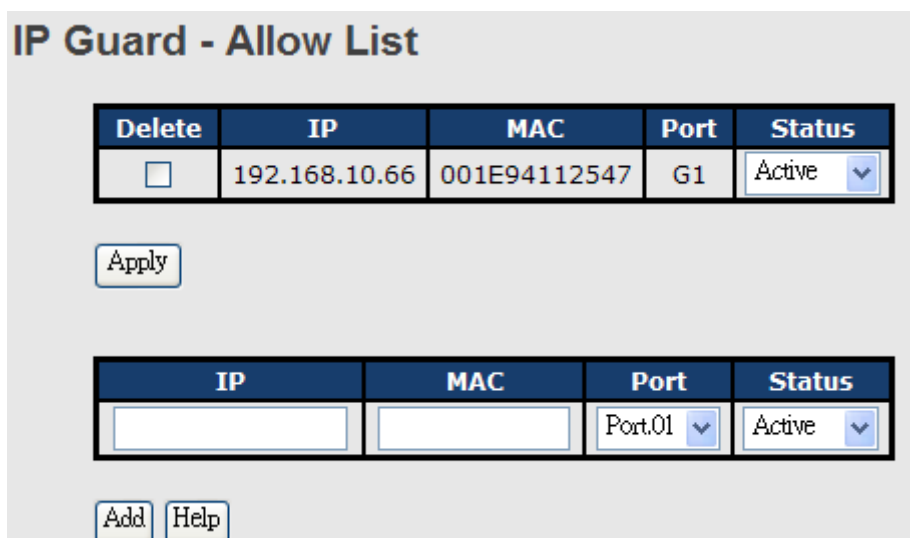
В таблице описаны основные поля:

Поле	Описание
<b>Mode</b>	<ul style="list-style-type: none"> <li>- Disable mode: функция полностью отключена.</li> <li>- Monitor mode: функция отключена, но отслеживает</li> </ul>

	IP трафик. - Security mode: функция включена, нелегальные IP будут заблокированы.
<b>Apply</b>	Применить
<b>Help</b>	Показать справку

### IP Guard – Allow List

Здесь вы можете настроить белый список IP адресов для IP Guard.



**IP Guard - Allow List**

Delete	IP	MAC	Port	Status
<input type="checkbox"/>	192.168.10.66	001E94112547	G1	Active

Apply

IP	MAC	Port	Status
<input type="text"/>	<input type="text"/>	Port.01	Active

Add Help

Рис. IP Guard – Allow List

В таблице описаны основные поля:

Поле	Описание
<b>IP</b>	Разрешённый IP адрес
<b>MAC</b>	Разрешённый MAC адрес
<b>Port</b>	Разрешённый порт
<b>Status</b>	Вы можете как разрешить указанному трафику передаваться, так и наоборот, запретить. Active: Разрешить IP трафик Suspend: Блокировать IP трафик
<b>Delete</b>	Если вы хотите удалить запись, нажмите здесь и нажмите Apply.

### IP Guard – Super-IP List

На этой странице вы можете выбрать Super-IP. Эти адреса будут обладать специальным приоритетом, который не будет ограничен MAC адресом или портом.

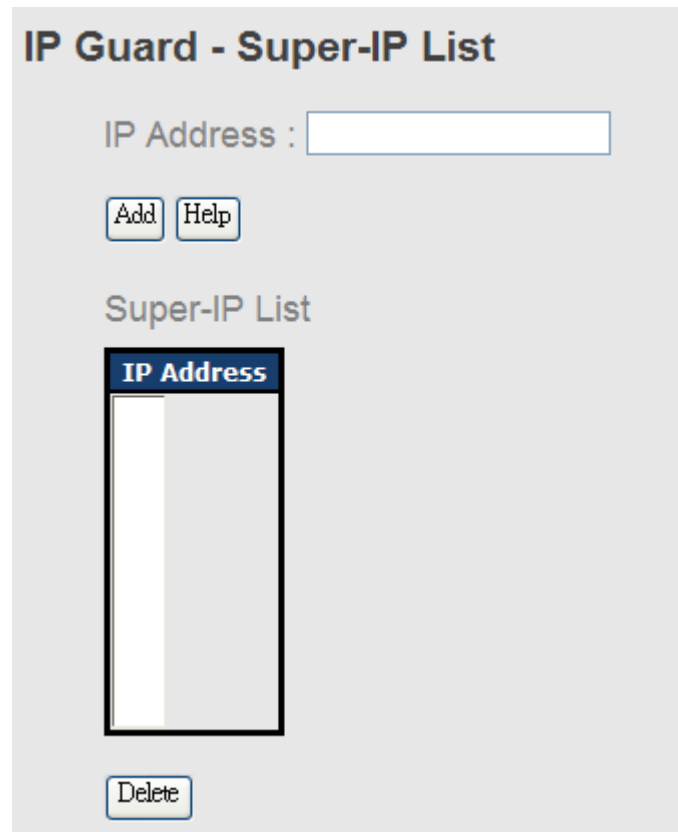
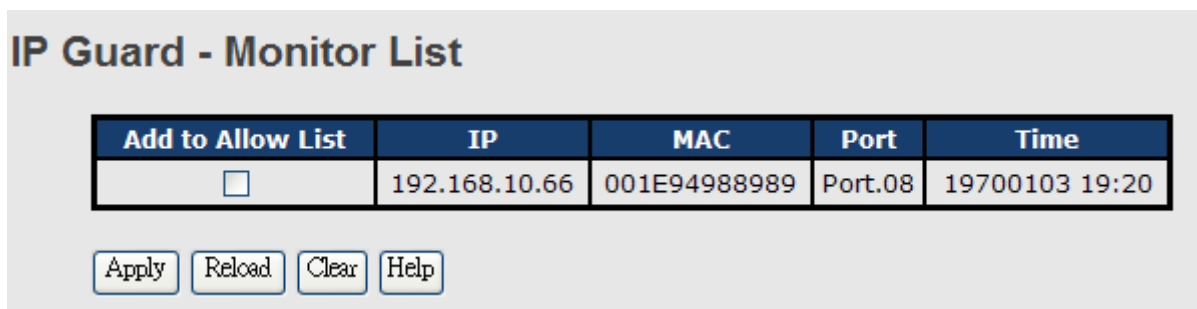


Рис. IP Guard – Super-IP List

### IP Guard – Super-IP List



Add to Allow List	IP	MAC	Port	Time
<input type="checkbox"/>	192.168.10.66	001E94988989	Port.08	19700103 19:20

Рис. IP Guard – Super-IP List

В таблице описаны основные поля:

Поле	Описание
IP	Разрешённый IP адрес
MAC	Разрешённый MAC адрес
Port	Разрешённый порт

Time	Время записи
------	--------------

### 5.1.13. Оповещения

Функция оповещения очень важна для управления коммутатором. Вы можете получать оповещения от коммутатора с помощью системного журнала, E-Mail и сигнального реле. Это позволяет вам удаленно следить за состоянием коммутатора. При возникновении событий, на ваш назначенный сервер, E-Mail или сигнальное реле будет посылаться оповещения.

#### Защитное реле

Когда возникает любое из выбранных событий, загорится Fault светодиод и электрическое реле просигнализирует в то же время.

**Fault Relay Alarm**

Power Failure

PWR 1       PWR 2

Port Link Down/Broken

Port.01       Port.02  
 Port.03       Port.04  
 Port.05       Port.06  
 Port.07       Port.08  
 Port.09       Port.10  
 Port.11       Port.12  
 Port.13       Port.14  
 Port.15       Port.16  
 Port.17       Port.18  
 Port.19       Port.20  
 Port.21       Port.22  
 Port.23       Port.24

#### Настройка журнала событий

SYSLOG - это протокол передачи уведомлений о событиях через сеть. Обратитесь к RFC 3164 – Протокол BSD SYSLOG

**SYSLOG Setting**

<b>Syslog Mode</b>	Both
<b>Syslog Server IP Address</b>	192.168.10.66

Apply Help

Рис. Настройка журнала событий

В таблице описаны основные поля:

Поле	Описание
<b>Syslog Mode</b>	Режимы SysLog: <ul style="list-style-type: none"> <li>• Disable: отключение SYSLOG</li> <li>• Client Only: ведение локального протокола</li> <li>• Server Only: ведение протокола на удалённом SYSLOG сервере</li> <li>• Both: оба варианта</li> </ul>
<b>Syslog Server IP Address</b>	IP адрес SYSLOG сервера
<b>Apply</b>	Нажмите Apply, чтобы применить настройки
<b>Help</b>	Показать справку

### Настройка SMTP

SMTP – это простой протокол передачи почты. Это протокол для передачи e-mail через Internet. Обратитесь к RFC 821

### SMTP Setting

E-mail Alert:  ▾

SMTP Server IP Address :	<input type="text" value="192.168.10.66"/>
Mail Subject :	<input type="text" value="Automated Email Alert"/>
Sender :	<input type="text" value="test mail"/>
<input type="checkbox"/> Authentication	
Rcpt e-mail Address 1 :	<input type="text" value="test@192.168.10.66"/>
Rcpt e-mail Address 2 :	<input type="text"/>
Rcpt e-mail Address 3 :	<input type="text"/>
Rcpt e-mail Address 4 :	<input type="text"/>

Рис. Настройка SMTP

В таблице описаны основные поля:

Поле	Описание
<b>E-mail Alarm</b>	Включить или отключить передачу оповещений системы по E-Mail
<b>Sender E-mail Address</b>	IP адрес SMTP сервера
<b>Mail Subject</b>	Тема письма
<b>Authentication</b>	Username: имя пользователя Password: пароль Confirm Password: повторите пароль
<b>Receipient E-mail Address</b>	E-Mail адрес получателя. Поддерживает до 6 получателей по почте.
<b>Apply</b>	Нажмите Apply, чтобы применить настройки
<b>Help</b>	Показать справку

### Выбор событий

Syslog и SMTP – два способа оповещения, поддерживаемых системой. Проверьте соответствующее поле, чтобы включить способ оповещения о системных событиях, который вы хотите выбрать. Обратите внимание, что нельзя поставить галочку если SYSLOG или SMTP отключены.

**Event Selection**

System Event

Event Type	Syslog	SMTP
Device cold start	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Device warm start	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Authentication failure	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Ring topology change	<input type="checkbox"/>	<input checked="" type="checkbox"/>

Port Event

Port	Syslog	SMTP
Port.01	Link Down <input type="button" value="v"/>	Disable <input type="button" value="v"/>
Port.02	Disable <input type="button" value="v"/>	Link Up & Link Down <input type="button" value="v"/>

Рис. Выбор событий

В таблице описаны основные поля:

Поле	Описание
<b>System Event</b>	
<b>System Cold Start</b>	Оповещение при перезапуске системы
<b>Power Status</b>	Оповещение при подключении или отключении питания
<b>SNMP Authentication Failure</b>	Оповещение при ошибке SNMP аутентификации
<b>Sy-Ring topology change</b>	Оповещение при изменении в топологии Sy-Ring
<b>Port Event SYSLOG/SMTP event</b>	Отключено Включение порта Отключение порта Включение и отключение порта
<b>Apply</b>	Нажмите Apply, чтобы применить настройки
<b>Help</b>	Показать справку

## 5.1.14. Мониторинг и диагностика

### 5.1.14.1. Журнал событий



Если включено ведение локального журнала, то он появится в этой таблице.

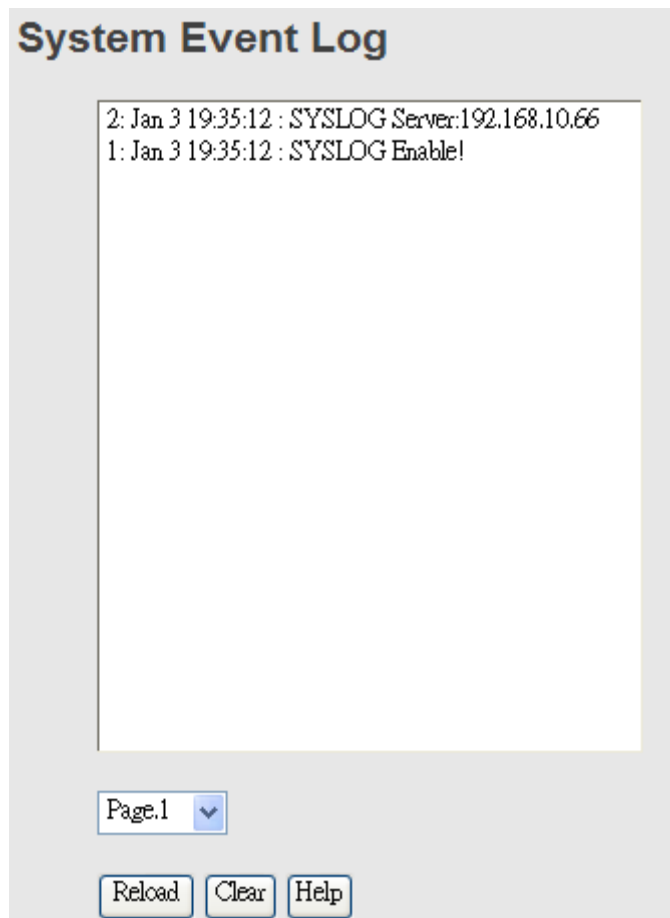


Рис. Журнал событий

В таблице описаны основные поля:

Поле	Описание
Page	Выберите номер страницы журнала
Reload	Отображение последних событий и обновления этой страницы
Clear	Очистить журнал
Help	Показать справку

#### 5.1.14.2. Таблица MAC адресов

Обратитесь к IEEE 802.1 D Секция 7.9. Таблица MAC адресов определяет, куда данный фрейм с данными MAC адресами отправления и назначения будет отправлен.

### MAC Address Table

Port No. :

Type	MAC Address	Port No.
Static	001122334455	Port.06
Dynamic	001E94988989	Port.08
Static	01005E000006	Port.05

Dynamic Address Count : 1  
Static Address Count : 2

### MAC Address Aging Setting

MAC Address Aging Time:

Auto Flush Table When Ports Link Down:

MAC Address Auto Learning:

Рис. Таблица MAC адресов

В таблице описаны основные поля:

Поле	Описание
<b>MAC Address Table Aging Time</b>	Установить период старения MAC адресов в таблице. Значение – от 0 до 3825. По умолчанию – 300 секунд.
<b>Auto Flush MAC Address Table When ports Link Down</b>	Включить эту функцию
<b>Apply</b>	Нажмите Apply, чтобы активировать настройки
<b>Help</b>	Показать справку

### 5.1.14.3. Статистика портов

Эта страница отображает текущую статистику на всех портах.

## Port Overview

Port No.	Type	Link	State	TX Good Packet	TX Bad Packet	RX Good Packet	RX Bad Packet	TX Abort Packet	Packet Collision
Port.01	100TX	Down	Forwarding	0	0	0	0	0	0
Port.02	100TX	Down	Forwarding	0	0	0	0	0	0
Port.03	100TX	Down	Forwarding	0	0	0	0	0	0
Port.04	100TX	Down	Forwarding	0	0	0	0	0	0

Рис. Статистика портов

В таблице описаны основные поля:

Поле	Описание
Type	Показать скорость передачи данных и тип носителя
Link	Показать статус соединения
State	Состояние портов: включены или отключены
TX Good Packet	Количество корректных пакетов, отправленных через этот порт
TX Bad Packet	Количество битых пакетов, отправленных через этот порт
RX Good Packet	Количество корректных пакетов, полученных через этот порт
RX Bad Packet	Количество битых пакетов, полученных через этот порт
TX Abort Packet	Количество пакетов, отброшенных на этом порту
Packet Collision	Количество обнаруженных коллизий
Clear	Очистить все показатели
Help	Показать справку

#### 5.1.14.4 Счётчики портов

Эта страница отображает набор счётчиков для каждого порта. Кнопка “Clear” обнуляет все счётчики.

Port No. :

<b>InGoodOctetsLo</b>	<b>InGoodOctetsHi</b>	<b>InBadOctets</b>	<b>OutFCSErr</b>
0	0	0	0
<b>InUnicasts</b>	<b>Deferred</b>	<b>InBroadcasts</b>	<b>InMulticasts</b>
0	0	0	0
<b>Octets64</b>	<b>Octets127</b>	<b>Octets255</b>	<b>Octets511</b>
0	0	0	0
<b>Octets1023</b>	<b>OctetsMax</b>	<b>OutOctetsLo</b>	<b>OutOctetsHi</b>
0	0	0	0
<b>OutUnicasts</b>	<b>Excessive</b>	<b>OutMulticasts</b>	<b>OutBroadcasts</b>
0	0	0	0
<b>Single</b>	<b>OutPause</b>	<b>InPause</b>	<b>Multiple</b>
0	0	0	0
<b>Undersize</b>	<b>Fragments</b>	<b>Oversize</b>	<b>Jabber</b>
0	0	0	0
<b>InMACRcvErr</b>	<b>InFCSErr</b>	<b>Collisions</b>	<b>Late</b>
0	0	0	0

Рис. Счётчики портов

В таблице описаны основные поля:

Поле	Описание
<b>InGoodOctetsLo</b>	Младшие 32 бита счётчика InGoodOctets. Сумма длин всех правильных Ethernet кадров.
<b>InGoodOctetsHi</b>	Старшие 32 бита счётчика InGoodOctets. Сумма длин всех правильных Ethernet кадров.
<b>InBadOctets</b>	Сумма длин всех битых пакетов
<b>OutFCSErr</b>	Количество кадров, переданных с неправильным FCS. Если кадр изменяется во время передачи (например, к нему прибавляют или удаляют тег), сначала проверяется его FCS. Если оригинальная FCS невалидна, новая FCS создаётся тоже невалидной и этот счётчик увеличивается на 1.
<b>InUnicasts</b>	Количество правильных кадров с юникастовыми MAC адресами.
<b>Deferred</b>	Общее число переданных кадров, которые не содержали ошибок, но были остановлены из-за занятости канала. Применим только в режиме half-duplex.
<b>InBroadcasts</b>	Количество правильных кадров с бродкастовым адресом

	назначения
<b>InMulticasts</b>	исло правильных кадров с мультикастовыми адресами назначения.
<b>Octets64</b>	Количество кадров, полученных и переданных, с длиной ровно 64 октета, включая те что с ошибками.
<b>Octets127</b>	Количество кадров, полученных и переданных, с длиной от 65 до 127 октетов, включая те что с ошибками.
<b>Octets255</b>	Количество кадров, полученных и переданных, с длиной от 128 до 255 октетов, включая те что с ошибками.
<b>Octets511</b>	Количество кадров, полученных и переданных, с длиной от 256 до 511 октетов, включая те что с ошибками.
<b>Octets1023</b>	Количество кадров, полученных и переданных, с длиной от 512 до 1023 октетов, включая те что с ошибками.
<b>OctetsMax</b>	Количество кадров, полученных и переданных, с длиной от 1024 до максимального числа октетов, включая те что с ошибками.
<b>OutOctetsLo</b>	Младшие 32 бита счётчика OutOctets. Сумма длин всех Ethernet кадров, отосланных с этого MAC.
<b>OutOctetsHi</b>	Старшие 32 бита счётчика OutOctets. Сумма длин всех Ethernet кадров, отосланных с этого MAC.
<b>OutUnicasts</b>	Количество отосланных кадров с юникастовым типом MAC адреса назначения.
<b>Excessive</b>	Количество кадров, отброшенных при достижении 16 последовательных коллизий. Счётчик работает только при half-duplex и только если DiscardExcessive выставлен в 1.
<b>OutBroadcasts</b>	Количество отосланных кадров с бродкастовым типом MAC адреса назначения.
<b>Single</b>	Количество успешно переданных кадров, с которыми произошла ровно одна коллизия. Счётчик работает только при half-duplex.
<b>OutPause</b>	Количество корректных кадров Flow Control, которые были отосланы.
<b>InPause</b>	Количество корректных кадров Flow Control, которые были получены.

<b>Multiple</b>	Количество успешно переданных кадров, с которыми произошло больше одной коллизии. Счётчик работает только при half-duplex.
<b>Undersize</b>	Общее число полученных кадров, чья длина менее 64 октетов, но с правильным FCS.
<b>Fragments</b>	Общее число полученных кадров, чья длина менее 64 октетов и с неправильным FCS.
<b>Oversize</b>	Общее число полученных кадров, чья длина более максимальной величины кадра, но с правильным FCS.
<b>Jabber</b>	Общее число полученных кадров, чья длина более максимальной величины кадра и с неправильным FCS.
<b>InMACRcvErr</b>	Общее количество полученных кадров, полученных с RxErr сигналом от PHY.
<b>InFCSErr</b>	Общее количество полученных кадров, у которых ошибка в CRC, но не посчитанных в Fragments, Jabber или RxErr.
<b>Collisions</b>	Количество коллизий, которые не посчитаны в Single, Multiple, Excessive или в Late. Счётчик работает только при half-duplex.
<b>Late</b>	Количество коллизий, обнаруженных после 512-го бит-тайма во время передачи кадра. Счётчик работает только при half-duplex.

#### 5.1.14.5. Мониторинг портов

Мониторинг портов может осуществляться за исходящим (TX), входящим (RX) или и тем и другим трафиком. TX мониторинг копируют данные, которые исходят из выбранного исходного TX порта (source port) на выбранный TX порт назначения. RX мониторинг также копирует данные, входящие в выбранные исходные порты и отправляет их на выбранный порт назначения. Отметим, что данные только копируются, все кадры также уходят к адресату, которому они предназначались.

### Port Monitoring

Port No.	Destination Port		Source Port	
	RX	TX	RX	TX
Port.01	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input type="checkbox"/>	<input type="checkbox"/>
Port.02	<input type="radio"/>	<input type="radio"/>	<input type="checkbox"/>	<input type="checkbox"/>
Port.03	<input type="radio"/>	<input type="radio"/>	<input type="checkbox"/>	<input type="checkbox"/>
Port.04	<input type="radio"/>	<input type="radio"/>	<input type="checkbox"/>	<input type="checkbox"/>

Рис. Мониторинг портов

В таблице описаны основные поля:

Поле	Описание
<b>Destination Port</b>	Порт получит копию фрейма от порта отправителя для мониторинга
<b>Source Port</b>	Мониторинг порта. Поставьте галочку на TX или RX
<b>TX</b>	Входящие данные
<b>RX</b>	Исходящие данные
<b>Apply</b>	Нажмите Apply, чтобы применить настройки
<b>Clear</b>	Очистить все поля (отключение функции мониторинга)
<b>Help</b>	Показать справку

#### 5.1.14.6. Мониторинг трафика

Здесь вы можете настроить мониторинг трафика устройства. Если трафика слишком много, устройство сделает запись в журнале или отошлёт письмо по электронной почте.

### Traffic Monitor

Port No.	Monitored-Counter	Time-Interval (1~300s)	Increasing-Quantity
Port.01	RX Octet	3	1000
Port.02	RX Broadcast	3	1000
Port.03	RX Multicast	3	1000
Port.04	RX Unicast	3	1000
Port.05	RX Non-Unicast	3	1000
Port.06	Disable	3	1000

Рис. Мониторинг трафика

В таблице описаны основные поля:

Поле	Описание
<b>Monitored –Counter</b>	Выберите тип мониторинга.
<b>Time-Interval</b>	Выберите интервал.
<b>Increasing – Quantity</b>	Выберите предельное количество трафика для оповещения.
<b>Event Alarm</b>	Выберите тип оповещения (SysLog или SMTP).

### 5.1.14.7. Ping

Функция Ping позволяет коммутатору посылать ICMP пакеты для проверки удаленных узлов.

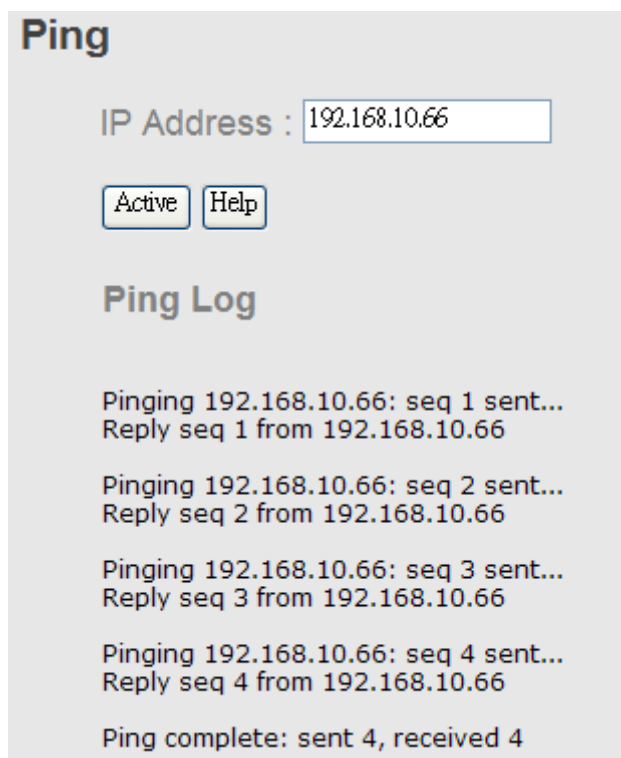


Рис. Ping

В таблице описаны основные поля:

Поле	Описание
<b>IP Address</b>	Введите IP адрес, который хотите диагностировать
<b>Active</b>	Нажмите Active, чтобы отправить ICMP пакеты



### 5.1.15. Сохранение конфигурации

При любых изменениях настроек нужно нажать «Сохранение настроек», чтобы сохранить текущие данные настроек в постоянную flash-память. Иначе, текущие настройки будут удалены при выключении или перезагрузке системы.



Рис. Сохранение конфигурации

В таблице описаны основные поля:

Поле	Описание
Save	Сохранить все настройки
Help	Показать справку

### 5.1.16. Сброс настроек



Рис. Сброс настроек

Для того, чтобы вернуть коммутатор к заводским настройкам, нажмите Reset. Вы можете выбрать «Keep current IP address setting» и «Keep current username & password», чтобы не допустить сброс IP адреса и имени пользователя и пароля.

### 5.1.17. Перезагрузка системы



Рис. Интерфейс перезагрузки системы

## 6. Командная строка

### 6.1. Управление с помощью командной строки

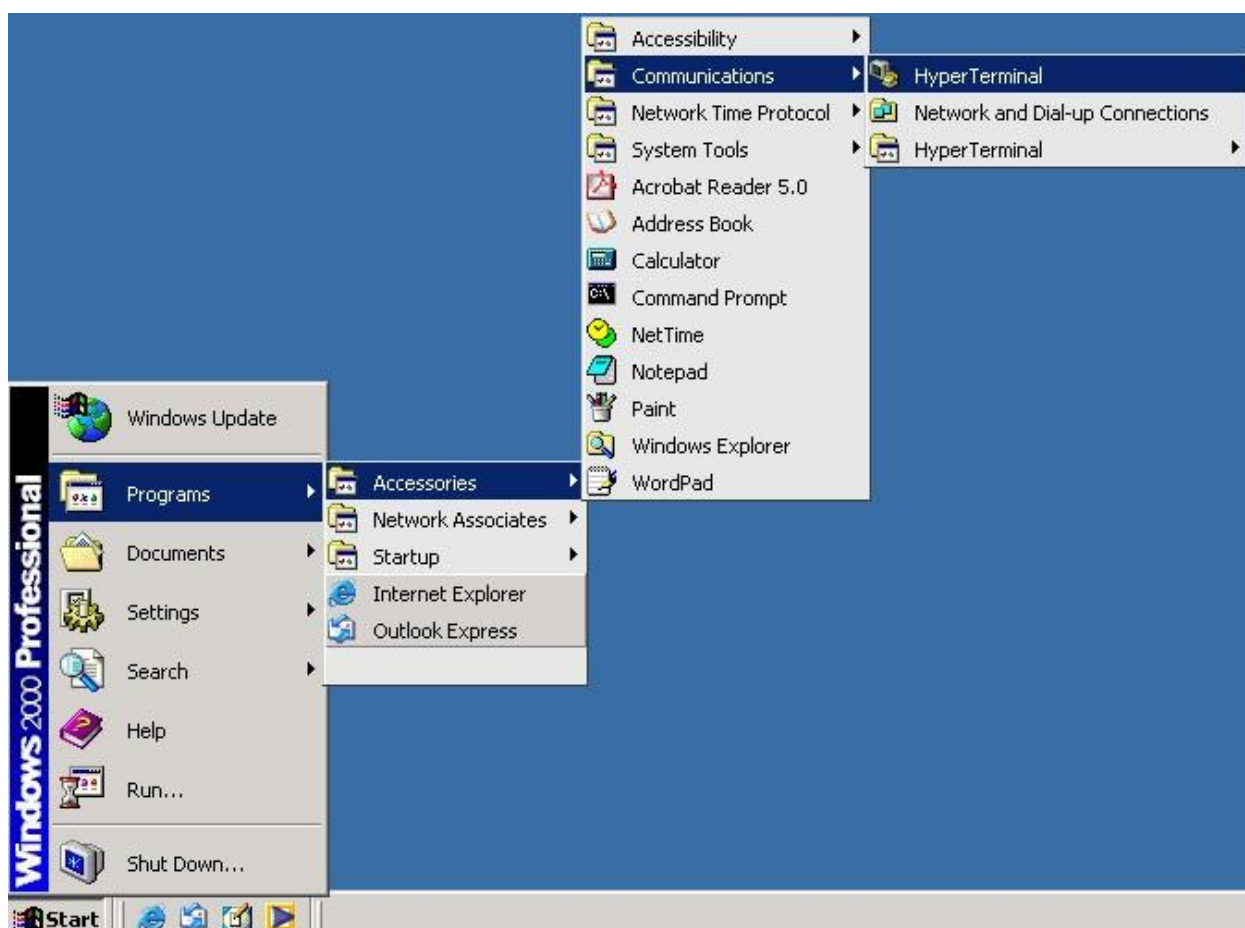
Кроме web-управления, SWM-240 также поддерживают управление с помощью командной строки. Вы можете использовать консоль или Telnet для управления коммутатором.

#### Управление с помощью командной строки через последовательный консольный RS-232 порт (9600, 8, none, 1, none)

Для настройки с помощью последовательного консольного RS-232 порта используйте кабель RJ45 к DB9-F (DB-9 «мама»), чтобы подключить консольный RS-232 порт коммутатора с COM портом вашего компьютера.

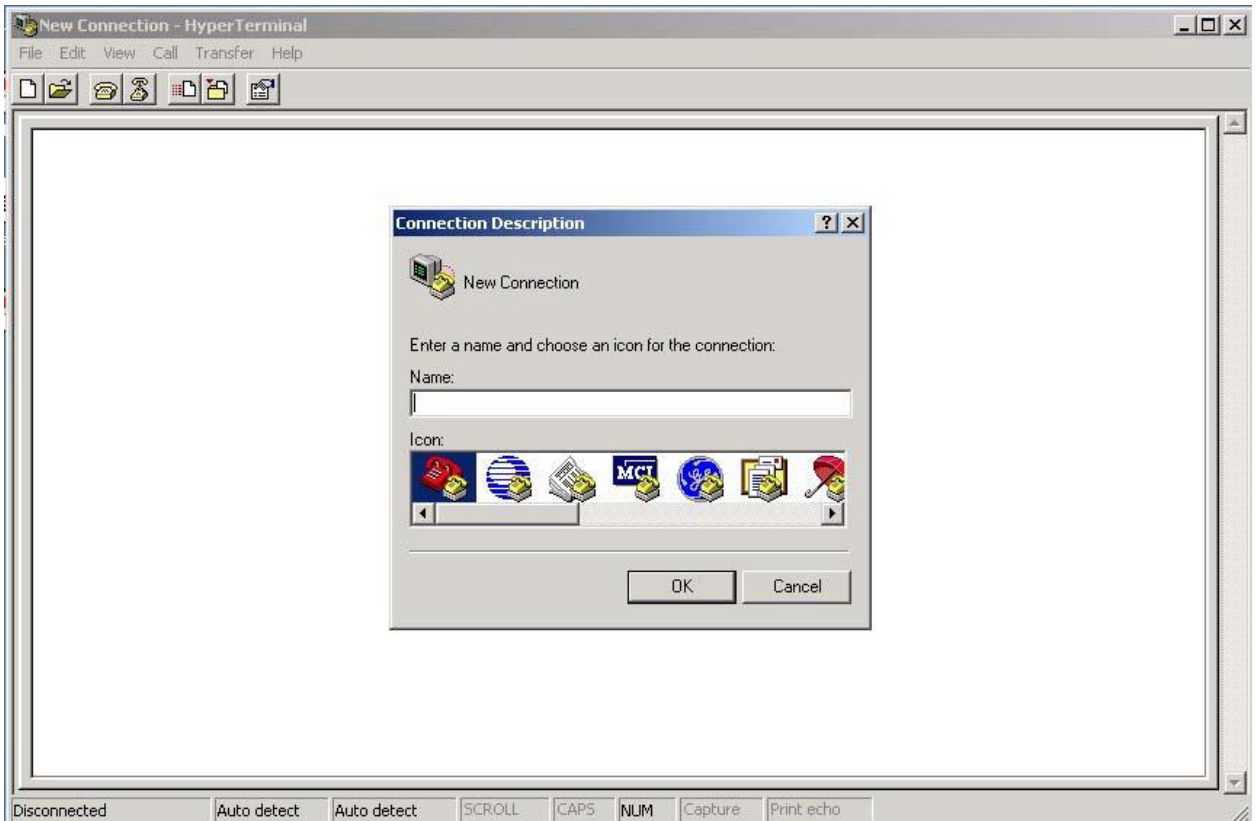
Для того, чтобы получить доступ к консоли через последовательный RS-232 кабель:

Шаг 1. На рабочем столе Windows выберите Пуск > Программы > Стандартные > Связь > Hyper Terminal

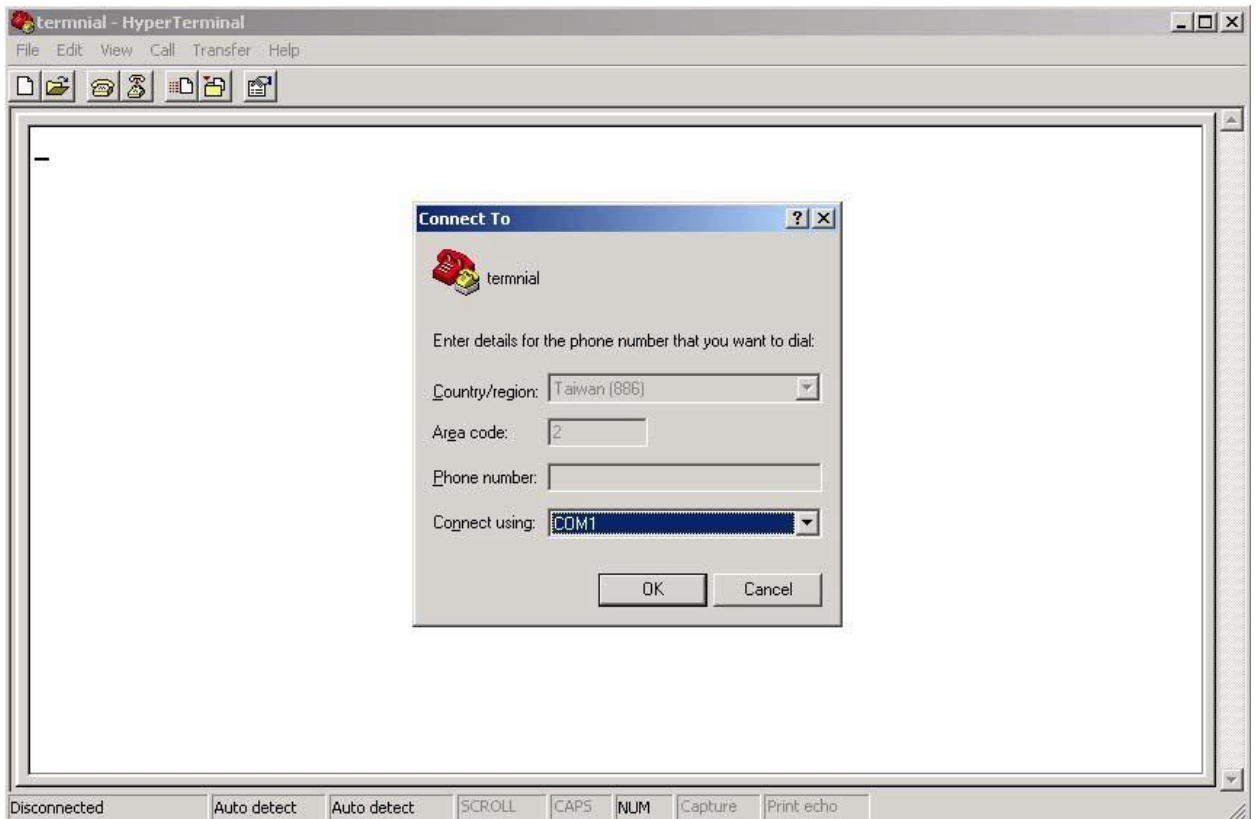


Можно использовать любой другой эмулятор терминала, такой как Putty.

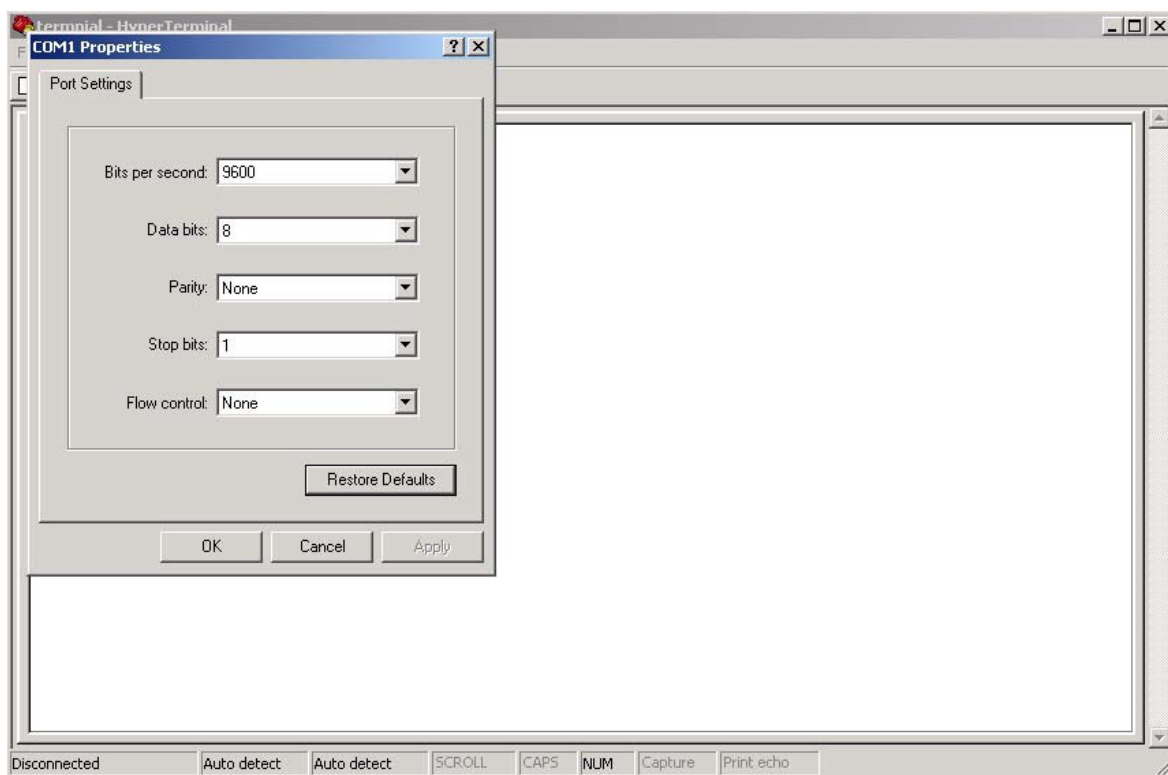
Шаг 2. Введите имя для нового соединения



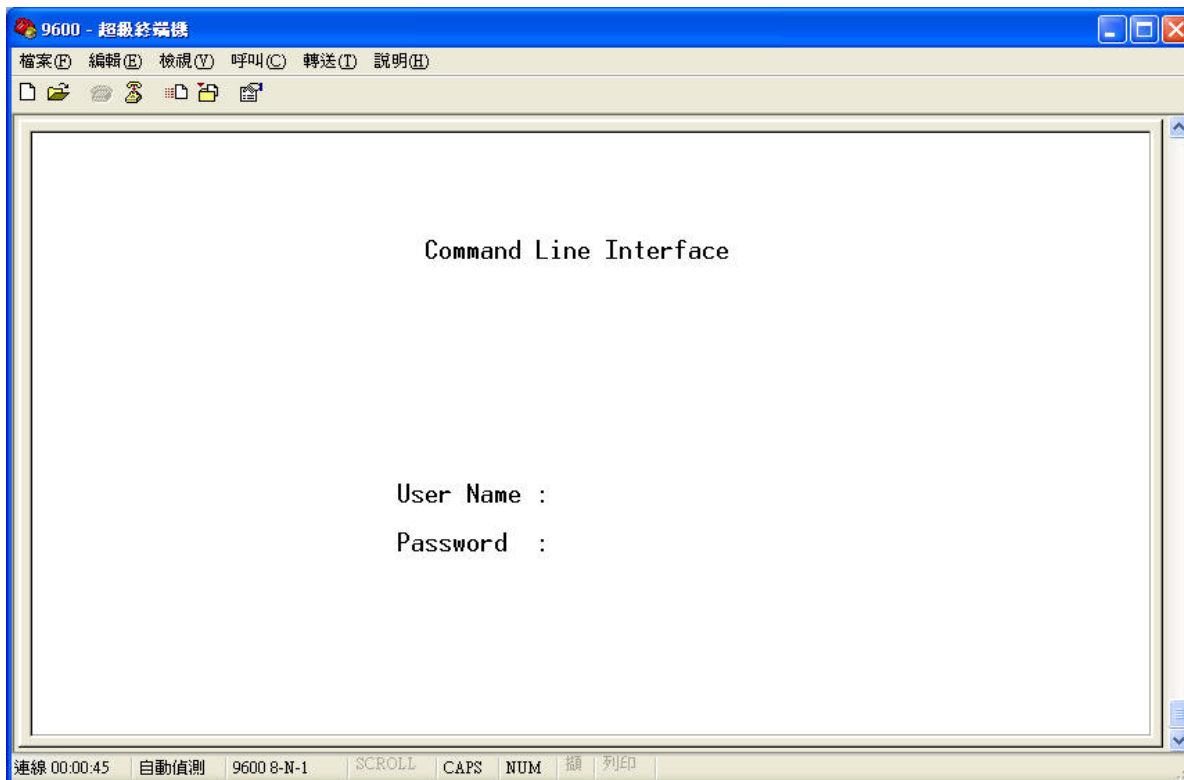
Шаг 3. Выберите номер COM порта для его использования



Шаг 4. Настройка свойств COM порта. 9600 для бит в секунду, 8 для бит данных, None для четности, 1 для стоповых битов и none для управления потоком.



Шаг 5. Появится окно входа в систему. Введите имя пользователя и пароль (пароль такой же, как и для Web браузера), затем нажмите enter.



## Управление через Telnet

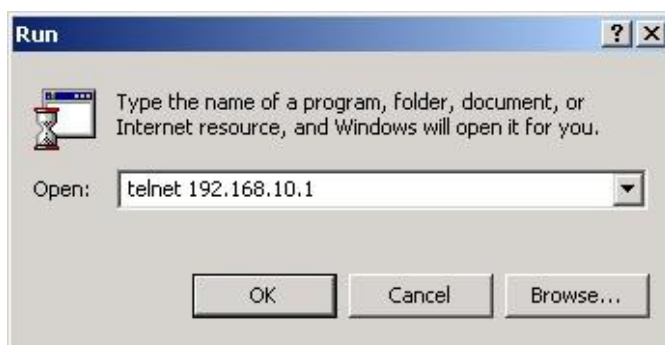
Пользователи могут использовать Telnet для настройки коммутаторов.

Значения по умолчанию:

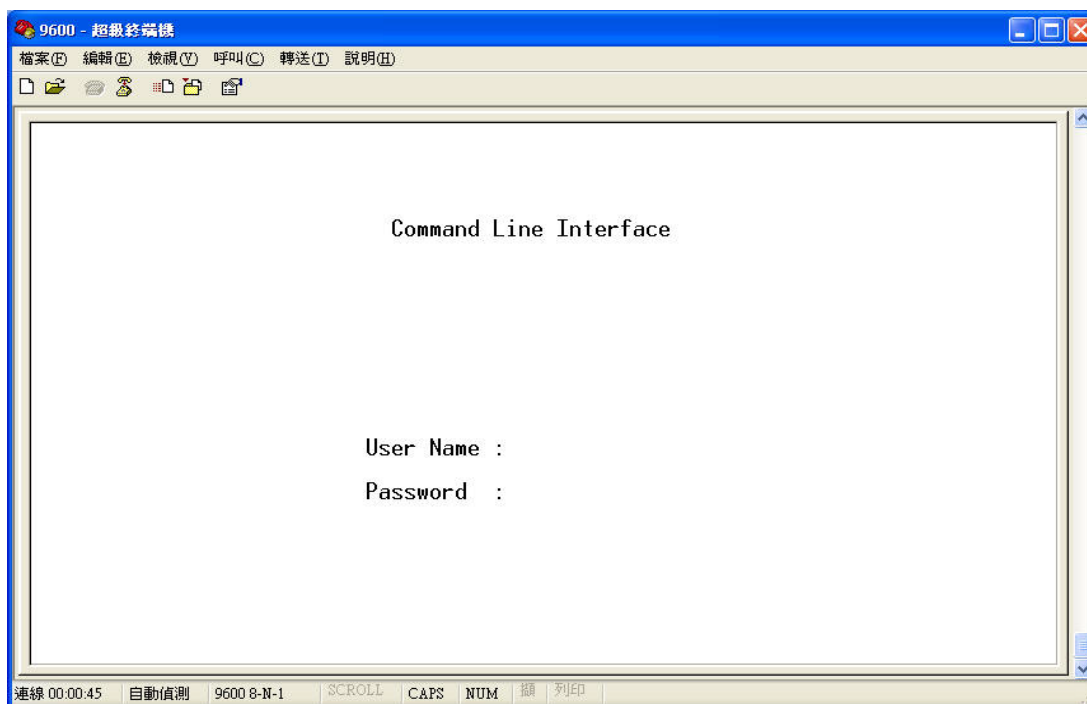
- IP адрес: 192.168.10.1
- Subnet Mask: 255.255.255.0
- Default Gateway: 192.168.10.254
- User Name: admin
- Password: admin

Для того, чтобы получить доступ к консоли Telnet:

Шаг 1. Набрать telnet \*IP адрес коммутатора\* из командной строки windows (или любой аналог)



Шаг 2. Появится окно входа в систему. Введите имя пользователя и пароль (пароль такой же, как и для Web браузера), затем нажмите enter.



## Уровень команд

Режимы	Доступ	Строка ввода	Выход	О режиме
User EXEC	Начните работу с коммутатором	switch>	Введите <b>logout</b> или <b>quit</b> .	Число команд, доступных в режиме пользователя, ограничено. Используйте этот режим для <ul style="list-style-type: none"> <li>• Входа в другой режим</li> <li>• Отображения информации о системе</li> </ul>
Privileged EXEC	Введите команду <b>enable</b> , когда пользователь находится в режиме User EXEC	switch#	Введите <b>disable</b> для выхода	Привилегированный режим. Используется для: <ul style="list-style-type: none"> <li>• Просмотра развёрнутой информации о системе</li> <li>• сохранения настроек</li> </ul>
Global configuration	Введите команду <b>configure</b> , находясь в Privileged EXEC	switch(config)#	Для выхода в привилегированный режим, введите <b>exit</b> или <b>end</b>	Используйте этот режим, чтобы настроить параметры, применяющиеся ко всему коммутатору
VLAN database	Введите команду <b>vlan database</b> , находясь в Privileged EXEC	switch(vlan)#	Для выхода в привилегированный режим, введите <b>exit</b>	Используйте этот режим чтобы настроить параметры VLAN
Interface configuration	Введите команду <b>interface</b> (с выбранным интерфейсом), находясь в режиме global configuration	switch(config-if)#	Для выхода в global configuration mode, введите <b>exit</b> . Для выхода в privileged EXEC введите <b>end</b> .	Используйте этот режим, чтобы настроить параметры Ethernet портов.

Символ уровня команды

Режим	Символ уровня команды
User EXEC	E
Privileged EXEC	P
Global configuration	G
VLAN database	V
Interface configuration	I

## 6.2. Список команд - системные команды

Команды SWM-240	Уровень	Описание	Пример
<b>show config</b>	E	Показать настройки коммутатора	switch>show config
<b>show terminal</b>	P	Показать информацию о консоли	switch#show terminal
<b>write memory</b>	P	Сохранить настройки на постоянную память (Flash)	switch#write memory
<b>system name</b> [System Name]	G	Указать имя системы	switch(config)#system name xxx
<b>system location</b> [System Location]	G	Указать местоположение коммутатора	switch(config)#system location xxx
<b>system description</b> [System Description]	G	Указать описание коммутатора	switch(config)#system description xxx
<b>system contact</b> [System Contact]	G	Указать связанные с коммутатором контакты	switch(config)#system contact xxx
<b>show system-info</b>	E	Показать информацию о системе	switch>show system-info
<b>ip address</b> [Ip-address] [Subnet-mask] [Gateway]	G	Настроить IP адрес коммутатора	switch(config)#ip address 192.168.1.1 255.255.255.0 192.168.1.254
<b>ip dhcp</b>	G	Включить функцию DHCP	switch(config)#ip dhcp

		клиента	
<b>show ip</b>	P	Показать IP коммутатора	switch#show ip
<b>no ip dhcp</b>	G	Выключить DHCP	switch(config)#no ip dhcp
<b>reload</b>	G	Выполнить «холодную» перезагрузку	switch(config)#reload
<b>default</b>	G	Сбросить настройки до заводских	Switch(config)#default
<b>admin username [Username]</b>	G	Изменить имя пользователя администратора (максимум 10 символов)	switch(config)#admin username xxxxxx
<b>admin password [Password]</b>	G	Указать пароль администратора (максимум 10 символов)	switch(config)#admin password xxxxxx
<b>show admin</b>	P	Показать информацию об администраторе	switch#show admin
<b>dhcpserver enable</b>	G	Включить DHCP сервер	switch(config)#dhcpserver enable
<b>dhcpserver lowip [Low IP]</b>	G	Настроить начальный IP адрес для пула IP адресов	switch(config)# dhcpserver lowip 192.168.1.1
<b>dhcpserver highip [High IP]</b>	G	Настроить конечный IP адрес для пула IP адресов	switch(config)# dhcpserver highip 192.168.1.50
<b>dhcpserver subnetmask [Subnet mask]</b>	G	Указать маску подсети для DHCP клиентов	switch(config)#dhcpserver subnetmask 255.255.255.0
<b>dhcpserver gateway [Gateway]</b>	G	Указать шлюз для DHCP клиентов	switch(config)#dhcpserver gateway 192.168.1.254
<b>dhcpserver dnsip [DNS IP]</b>	G	Указать IP адрес DNS сервера для DHCP клиентов	switch(config)# dhcpserver dnsip 192.168.1.1
<b>dhcpserver leasetime [Hours]</b>	G	Настроить время, на которое выдается IP адрес (в час)	switch(config)#dhcpserver leasetime 1
<b>dhcpserver ipbinding</b>	I	Указать статический IP для	switch(config)#interface fastEthernet 2



[IP address]		DHCP клиентов на определённом порту	switch(config-if)#dhcpserver ipbinding 192.168.1.1
show dhcpserver configuration	P	Показать настройки DHCP сервера	switch#show dhcpserver configuration
show dhcpserver clients	P	Показать данные о DHCP клиентах	switch#show dhcpserver clients
show dhcpserver ip-binding	P	Показать информацию о назначенных через DHCP IP адресах	switch#show dhcpserver ip-binding
no dhcpserver	G	Отключить DHCP сервер	switch(config)#no dhcpserver
security enable	G	Включить защиту IP	switch(config)#security enable
seGcurity http	G	Включить IP защиту HTTP сервера	switch(config)#security http
sePcurity telnet	G	Включить IP защиту telnet сервера	switch(config)#security telnet
security ip [Index(1..10)] [IP Address]	G	Определить список безопасных IP	switch(config)#security ip 1 192.168.1.55
show security	P	Показать информацию о доверенных IP адресах устройства	switch#show security
no security	G	Отключить функцию IP безопасности устройства	switch(config)#no security
no security http	G	Отключить IP защиту на HTTP сервере	switch(config)#no security http
no security telnet	G	Отключить IP защиту на telnet сервере	switch(config)#no security telnet

### 6.3. Список команд – команды портов

Команды SWM-240	Уровень	Описание	Пример
interface fastEthernet [Portid]	G	Выберите порт для настройки	switch(config)#interface fastEthernet 2
duplex [full   half]	I	Выбрать дуплексный режим работы для Fast	switch(config)#interface fastEthernet 2

		Ethernet	switch(config-if)#duplex full
<b>speed</b> [10 100 1000 auto]	<b>I</b>	Указать скорость работы порта. Скорость не может быть равна 1000, если порт не является гигабитным.	switch(config)#interface fastEthernet 2 switch(config-if)#speed 100
<b>flowcontrol mode</b> [Symmetric Asymmetric]	<b>I</b>	Настройка контроля за потоком.	switch(config)#interface fastEthernet 2 switch(config-if)#flowcontrol mode Asymmetric
<b>no flowcontrol</b>	<b>I</b>	Отключить контроля за потоком	switch(config-if)#no flowcontrol
<b>security enable</b>	<b>I</b>	Включить защиту интерфейса	switch(config)#interface fastEthernet 2 switch(config-if)#security enable
<b>no security</b>	<b>I</b>	Отключить защиту интерфейса	switch(config)#interface fastEthernet 2 switch(config-if)#no security
<b>bandwidth type all</b>	<b>I</b>	Включить режим обработки входящих кадров “принимать все”	switch(config)#interface fastEthernet 2 switch(config-if)#bandwidth type all
<b>bandwidth type broadcast-multicast-flooded-unicast</b>	<b>I</b>	Включить режим обработки входящих кадров “принимать широковещательные, групповые и избыточные одноадресные”	switch(config)#interface fastEthernet 2 switch(config-if)#bandwidth type broadcast-multicast-flooded-unicast
<b>bandwidth type broadcast-multicast</b>	<b>I</b>	Включить режим обработки входящих кадров “принимать широковещательные и групповые”	switch(config)#interface fastEthernet 2 switch(config-if)#bandwidth type broadcast-multicast
<b>bandwidth type broadcast-only</b>	<b>I</b>	Включить режим обработки входящих	switch(config)#interface fastEthernet 2

		кадров “принимать только широкоэвещательные”	switch(config-if)#bandwidth type broadcast-only
<b>bandwidth in [Value]</b>	<b>I</b>	Указать входящую пропускную способность. Интервал скорости – от 100 кбит/с до 102400 кбит/с для гигабитных портов, и 0 - без ограничений.	switch(config)#interface fastEthernet 2 switch(config-if)#bandwidth in 100
<b>bandwidth out [Value]</b>	<b>I</b>	Указать исходящую пропускную способность. Интервал скорости – от 100 кбит/с до 102400 кбит/с или 256000 кбит/с для гигабитных портов, и 0 - без ограничений.	switch(config)#interface fastEthernet 2 switch(config-if)#bandwidth out 100
<b>show bandwidth</b>	<b>I</b>	Показать ограничения на пропускную способность	switch(config)#interface fastEthernet 2 switch(config-if)#show bandwidth
<b>state [Enable   Disable]</b>	<b>I</b>	Определить статус работы Ethernet портов. Чтобы отключить порт, введите disable.	switch(config)#interface fastEthernet 2 switch(config-if)#state Disable
<b>show interface configuration</b>	<b>I</b>	Показать настройки порта	switch(config)#interface fastEthernet 2 switch(config-if)#show interface configuration
<b>show interface status</b>	<b>I</b>	Показать фактическое состояние порта	switch(config)#interface fastEthernet 2 switch(config-if)#show interface status
<b>show interface accounting</b>	<b>I</b>	Показать статистику порта	switch(config)#interface fastEthernet 2 switch(config-if)#show
<b>no accounting</b>	<b>I</b>	Очистить статистику	switch(config)#interface fastEthernet 2 switch(config-if)#no accounting

#### 6.4. Список команд – команд транков

Команды SWM-240	Уровень	Описание	Пример
<b>aggregator priority</b> [1to65535]	<b>G</b>	Определить приоритет для транка	switch(config)#aggregator priority 22
<b>aggregator activityport</b> [Port Numbers]	<b>G</b>	Определить активный порт	switch(config)#aggregator activityport 2
<b>aggregator group</b> [GroupID] [Port-list] lacp workp [Workport]	<b>G</b>	Назначить группу агрегируемых портов LACP [GroupID]: от 1 до 3 [Port-list]: список портов в в группе. Этот параметр может быть диапазоном (например, 1-4) или перечислением (2, 3, 6) [Workport]: Количество рабочих портов, значение должно быть не меньше 0 или больше, чем количество портов в группе	switch(config)#aggregator group 1 1-4 lacp workp 2 or switch(config)#aggregator group 2 1,4,3 lacp workp 3
<b>aggregator group</b> [GroupID] [Port-list] nolacp	<b>G</b>	Назначить статическую транковую группу [GroupID]: 1-3 [Port-list]: список портов в в группе. Этот параметр может быть диапазоном (например, 1-4) или перечислением (2, 3, 6)	switch(config)#aggregator group 1 2-4 nolacp или switch(config)#aggregator group 1 3,1,2 nolacp
<b>show aggregator</b>	<b>P</b>	Показать информацию об агрегированных портах	switch#show aggregator
<b>no aggregator lacp</b> [GroupID]	<b>G</b>	Отключить функцию LACP для агрегированной группы	switch(config)#no aggregator lacp 1
<b>no aggregator group</b> [GroupID]	<b>G</b>	Удалить агрегированную группу	switch(config)#no aggregator group 2

## 6.5. Список команд – команды VLAN

Команды SWM-240	Уровень	Описание	Пример
<b>vlan database</b>	P	Вход в режим настройки VLAN	switch#vlan database
<b>vlan [8021q   gvrp]</b>	V	Выбор режима VLAN	switch(vlan)# vlanmode 802.1q или switch(vlan)# vlanmode gvrp
<b>no vlan [VID]</b>	V	Отключить группу VLAN (по VID)	switch(vlan)#no vlan 2
<b>no gvrp</b>	V	Отключить GVRP	switch(vlan)#no gvrp
<b>IEEE 802.1Q VLAN</b>			
<b>vlan 8021q port [PortNumber] access-link untag [UntaggedVID]</b>	V	Назначить VLAN порту. Эту команду нельзя применить, если порт принадлежит к агрегируемой группе	switch(vlan)#vlan 802.1q port 3 access-link untag 33
<b>vlan 8021q port [PortNumber] trunk-link tag [TaggedVID List]</b>	V	Назначить транковое соединение для VLAN через порт. Эту команду нельзя применить, если порт принадлежит к агрегируемой группе	switch(vlan)#vlan 8021q port 3 trunk-link tag 2,3,6,99 или switch(vlan)#vlan 8021q port 3 trunk-link tag 3-20
<b>vlan 8021q port [PortNumber] hybrid-link untag [UntaggedVID] tag [TaggedVID List]</b>	V	Назначить гибридное соединение для VLAN через порт. Эту команду нельзя применить, если порт принадлежит к транковой группе	switch(vlan)# vlan 8021q port 3 hybrid-link untag 4 tag 3,6,8 или switch(vlan)# vlan 8021q port 3 hybrid-link untag 5 tag 6-8
<b>vlan 8021q aggregator [TrunkID] access-link untag [UntaggedVID]</b>	V	Назначить VLAN агрегируемой группе	switch(vlan)#vlan 8021q aggregator 3 access-link untag 33
<b>vlan 8021q aggregator</b>	V	Назначить транковое соединение для VLAN через агрегируемую	switch(vlan)#vlan 8021q aggregator 3

[TrunkID] trunk-link tag [TaggedVID List]		группу	trunk-link tag 2,3,6,99 or switch(vlan)#vlan 8021q aggreator 3 trunk-link tag 3-20
vlan 8021q aggreator [PortNumber] hybrid-link untag [UntaggedVID] tag [TaggedVID List]	V	Назначить гибридное соединение для VLAN через агрегируемую группу	switch(vlan)# vlan 8021q aggreator 3 hybrid-link untag 4 tag 3,6,8 or switch(vlan)# vlan 8021q aggreator 3 hybrid-link untag 5 tag 6-8
show vlan [VID] or show vlan	V	Показать информацию о VLAN	switch(vlan)#show vlan 23

## 6.6. Список команд - команды Spanning Tree

Команды SWM-240	Уровень	Описание	Пример
spanning-tree enable	G	Включить STP	switch(config)#spanning-tree enable
spanning-tree priority [0to61440]	G	Настроить параметры приоритетов STP	switch(config)#spanning-tree priority 32767
spanning-tree max-age [seconds]	G	Задать интервал, через который будут отправляться команды от корневого узла ко всем остальным. Если коммутатор не получит BPDU сообщение от корневого коммутатора за данный интервал, он инициализирует перестроение дерева STP.	switch(config)# spanning-tree max-age 15
spanning-tree hello-time [seconds]	G	Использовать команду для изменения интервала между hello BPDU	switch(config)#spanning-tree hello-time 3
spanning-tree	G	Определите длительность стадии	switch(config)#

<b>forward-time</b> [seconds]		ожидания для логического дерева. Эта стадия определяет длительность стадий прослушивания и обучения, которые предшествуют стадии передачи данных.	spanning-tree forward-time 20
<b>stp-path-cost</b> [1to200000000]	<b>I</b>	Установить стоимость пути для конкретного интерфейса. Эта стоимость используется как метрика при построении или перестроении логического дерева.	switch(config)#interface fastEthernet 2 switch(config-if)#stp-path-cost 20
<b>stp-path-priority</b> [Port Priority]	<b>I</b>	Установить приоритет конкретного интерфейса. Приоритетность связи влияет на выбор корневого коммутатора.	switch(config)#interface fastEthernet 2 switch(config-if)# stp-path-priority 127
<b>stp-admin-p2p</b> [Auto True False]	<b>I</b>	Приоритет P2P STP на этом интерфейсе	switch(config)#interface fastEthernet 2 switch(config-if)# stp-admin-p2p Auto
<b>stp-admin-edge</b> [True False]	<b>I</b>	Приоритет Edge STP на этом интерфейсе	switch(config)#interface fastEthernet 2 switch(config-if)# stp-admin-edge True
<b>stp-admin-non-stp</b> [True False]	<b>I</b>	Приоритет NonSTP STP на этом интерфейсе	switch(config)#interface fastEthernet 2 switch(config-if)# stp-admin-non-stp False
<b>Show spanning-tree</b>	<b>E</b>	Показать статистику STP	switch>show spanning-tree
<b>no spanning-tree</b>	<b>G</b>	Отключить STP	switch(config)#no spanning-tree

## 6.7. Список команд - команды QoS

Команды SWM-240	Уровень	Описание	Пример
<b>qos policy</b> [weighted-fair strict]	<b>G</b>	Выбрать тип QOS	switch(config)#qos policy weighted-fair
<b>qos prioritytype</b>	<b>G</b>	Указать тип	switch(config)#qos

[port-based cos-only tos-only cos-first tos-first]		приоритетности QOS	prioritytype
<b>qos priority portbased</b> [Port] [lowest low middle high]	<b>G</b>	Настройка приоритетности на основе порта	switch(config)#qos priority portbased 1 low
<b>qos priority cos</b> [Priority][lowest low middle high]	<b>G</b>	Настройка COS приоритета	switch(config)#qos priority cos 22 middle
<b>qos priority tos</b> [Priority][lowest low middle high]	<b>G</b>	Настройка TOS приоритетности	switch(config)#qos priority tos 3 high
<b>show qos</b>	<b>P</b>	Показать информацию о настройках QOS	switch>show qos
<b>no qos</b>	<b>G</b>	Отключить функцию QOS	switch(config)#no qos

## 6.8. Список команд - команды IGMP

Команды SWM-240	Уровень	Описание	Пример
<b>igmp enable</b>	<b>G</b>	Включить функцию IGMP snooping	switch(config)#igmp enable
<b>Igmp-query auto</b>	<b>G</b>	Указать режим автоматических IGMP запросов	switch(config)#Igmp-query auto
<b>Igmp-query force</b>	<b>G</b>	Указать форсированный режим IGMP запросов	switch(config)#Igmp-query force
<b>show igmp configuration</b>	<b>P</b>	Показать настройки IGMP snooping	switch#show igmp configuration
<b>show igmp multi</b>	<b>P</b>	Показать подробно таблицу записей IGMP snooping	switch#show igmp multi
<b>no igmp</b>	<b>G</b>	Отключить функцию IGMP snooping	switch(config)#no igmp
<b>no igmp-query</b>	<b>G</b>	Отключить IGMP запросы	switch#no igmp-query



## 6.9. Список команд - команды MAC

Команды SWM-240	Уровень	Описание	Пример
<b>mac-address-table static hwaddr [MAC]</b>	<b>I</b>	Настройка таблицы MAC адресов (статических)	switch(config)#interface fastEthernet 2 switch(config-if)#mac-address-table static hwaddr 000012345678
<b>mac-address-table filter hwaddr [MAC]</b>	<b>G</b>	Настройка таблицы MAC адресов (фильтр)	switch(config)#mac-address-table filter hwaddr 000012348678
<b>show mac-address-table</b>	<b>P</b>	Показать таблицу MAC адресов	switch#show mac-address-table
<b>show mac-address-table static</b>	<b>P</b>	Показать таблицу статических MAC адресов	switch#show mac-address-table static
<b>show mac-address-table filter</b>	<b>P</b>	Показать таблицу фильтрации MAC адресов	switch#show mac-address-table filter
<b>no mac-address-table static hwaddr [MAC]</b>	<b>I</b>	Удалить запись из таблицы статических MAC адресов	switch(config)#interface fastEthernet 2 switch(config-if)#no mac-address-table static hwaddr 000012345678
<b>no mac-address-table filter hwaddr [MAC]</b>	<b>G</b>	Удалить запись из таблицы фильтрации MAC адресов	switch(config)#no mac-address-table filter hwaddr 000012348678
<b>no mac-address-table</b>	<b>G</b>	Удалить динамическую запись из таблицы MAC адресов	switch(config)#no mac-address-table

## 6.10. Список Commands Set - Набор команд SNMP

Команды SWM-240	Уровень	Описание	Пример
<b>snmp agent-mode</b>	<b>G</b>	Выберите режим SNMP	switch(config)#snmp agent-

[v1v2c   v3]		agent	mode v1v2c
<b>snmp-server host</b> [IP address] <b>community</b> [Community-string] <b>trap-version</b> [v1 v2c]	<b>G</b>	Введите данные SNMP сервера и community string	switch(config)#snmp-server host 192.168.10.50 community public trap-version v1 (remove) Switch(config)#no snmp-server host 192.168.10.50
<b>snmp community-strings</b> [Community-string] <b>right</b> [RO RW]	<b>G</b>	Настроить права community string	switch(config)#snmp community-strings public right RO or switch(config)#snmp community-strings public right RW
<b>snmp snmpv3-user</b> [User Name] <b>password</b> [Authentication Password] [Privacy Password]	<b>G</b>	Настроить профиль пользователя для SNMPv3 агента. Поле с паролем может быть пустым.	switch(config)#snmp snmpv3-user test01 password AuthPW Pri
<b>show snmp</b>	<b>P</b>	Показать настройки SNMP	switch#show snmp
<b>show snmp-server</b>	<b>P</b>	Показать информацию о trap-сервере	switch#show snmp-server
<b>no snmp community-strings</b> [Community]	<b>G</b>	Удалить указанную community string	switch(config)#no snmp community-strings public
<b>no snmp snmpv3-user</b> [User Name] <b>password</b> [Authentication Password] [Privacy Password]	<b>G</b>	Удалить указанного пользователя SNMPv3 агента. Поле с паролем может быть пустым.	switch(config)# no snmp snmpv3-user test01 password AuthPW PrivPW
<b>no snmp-server host</b> [Host-address]	<b>G</b>	Удалить данные SNMP сервера	switch(config)#no snmp-server 192.168.10.50

### 6.11. Список команд - команды «зеркалирования» портов

Команды SWM-240	Уровень	Описание	Пример
<b>monitor rx</b>	<b>G</b>	Выбрать порт назначения для мониторинга входящего трафика	switch(config)#monitor rx
<b>monitor tx</b>	<b>G</b>	Выбрать порт назначения для мониторинга исходящего трафика	switch(config)#monitor tx
<b>show monitor</b>	<b>P</b>	Показать информацию о мониторинге портов	switch#show monitor
<b>monitor [RX TX Both]</b>	<b>I</b>	Выбрать исходный порт мониторинга	switch(config)#interface fastEthernet 2 switch(config-if)#monitor RX
<b>show monitor</b>	<b>I</b>	Показать информацию о мониторинге выбранного порта	switch(config)#interface fastEthernet 2 switch(config-if)#show monitor
<b>no monitor</b>	<b>I</b>	Отключить функцию мониторинга порта	switch(config)#interface fastEthernet 2 switch(config-if)#no monitor

### 6.12. Список команд - команды 802.1x

Команды SWM-240	Уровень	Описание	Пример
<b>8021x enable</b>	<b>G</b>	Включить 802.1x протокол	switch(config)# 8021x enable
<b>8021x system radiousip [IP address]</b>	<b>G</b>	Указать IP адрес Radius сервера	switch(config)# 8021x system radiousip 192.168.1.1
<b>8021x system serverport [port ID]</b>	<b>G</b>	Изменить порт Radius сервера	switch(config)# 8021x system serverport 1815
<b>8021x system</b>	<b>G</b>	Изменить порт авторизации	switch(config)# 8021x

<b>accountport</b> [port ID]			system accountport 1816
<b>8021x system sharekey</b> [ID]	<b>G</b>	Изменить значение разделяемого ключа	switch(config)# 8021x system sharekey 123456
<b>8021x system nasid</b> [words]	<b>G</b>	Изменить NAS идентификатор	switch(config)# 8021x system nasid test1
<b>8021x misc quietperiod</b> [sec.]	<b>G</b>	Указать значение Quiet period (интервал между ошибкой аутентификации и новой попыткой) для коммутатора	switch(config)# 8021x misc quietperiod 10
<b>8021x misc txperiod</b> [sec.]	<b>G</b>	Указать TX интервал	switch(config)# 8021x misc txperiod 5
<b>8021x misc supportimeout</b> [sec.]	<b>G</b>	Указать время, в течение которого коммутатор будет ожидать ответ на EAP запрос от клиента	switch(config)# 8021x misc supportimeout 20
<b>8021x misc servertimeout</b> [sec.]	<b>G</b>	Указать время, в течение которого коммутатор будет ожидать ответ на запрос аутентификации с Radius сервера	switch(config)#8021x misc servertimeout 20
<b>8021x misc maxrequest</b> [number]	<b>G</b>	Указать максимальное количество попыток отправки запроса	switch(config)# 8021x misc maxrequest 3
<b>8021x misc reauthperiod</b> [sec.]	<b>G</b>	Указать интервал времени, после которого подключённые клиенты должны быть повторно аутентифицированы	switch(config)# 8021x misc reauthperiod 3000
<b>8021x portstate</b> [disable   reject   accept   authorize]	<b>I</b>	Указать статус выбранных портов	switch(config)#interface fastethernet 3 switch(config-if)#8021x portstate accept
<b>show 8021x</b>	<b>E</b>	Показать свойства 802.1x, а также статусы портов	switch>show 8021x
<b>no 8021x</b>	<b>G</b>	Отключить функцию 802.1x	switch(config)#no 8021x

### 6.13. Список команд - команды TFTP

Команды SWM-240	Уровень	Описание	Пример
<b>backup</b> <b>flash:backup_cfg</b>	<b>G</b>	Сохранить настройки на TFTP сервере; необходимо указать IP адрес TFTP сервера и имя файла	switch(config)#backup flash:backup_cfg
<b>restore</b> <b>flash:restore_cfg</b>	<b>G</b>	Получить настройки с TFTP сервера; необходимо указать IP адрес TFTP сервера и имя файла	switch(config)#restore flash:restore_cfg
<b>upgrade</b> <b>flash:upgrade_fw</b>	<b>G</b>	Обновить прошивку с TFTP сервера; необходимо указать IP адрес TFTP сервера и имя файла	switch(config)#upgrade flash:upgrade_fw

### 6.14. Список команд - команды SYSLOG, SMTP, EVENT

Команды SWM-240	Уровень	Описание	Пример
<b>systemlog ip</b> [IP address]	<b>G</b>	Указать IP адрес сервера журнала событий	switch(config)# systemlog ip 192.168.1.100
<b>systemlog mode</b> [client server both]	<b>G</b>	Указать режим syslog	switch(config)# systemlog mode both
<b>show systemlog</b>	<b>E</b>	Показать журнал событий	Switch>show systemlog
<b>show systemlog</b>	<b>P</b>	Показать информацию о клиенте и сервере syslog	switch#show systemlog
<b>no systemlog</b>	<b>G</b>	Отключить ведение журнала событий	switch(config)#no systemlog
<b>smtp enable</b>	<b>G</b>	Включить функцию SMTP	switch(config)#smtp enable
<b>smtp serverip</b> [IP address]	<b>G</b>	Настроить IP адрес SMTP сервера	switch(config)#smtp serverip 192.168.1.5
<b>smtp authentication</b>	<b>G</b>	Включить SMTP аутентификацию	switch(config)#smtp authentication

<b>smtp account</b> [account]	<b>G</b>	Настроить аккаунт SMTP	switch(config)#smtp account User
<b>smtp password</b> [password]	<b>G</b>	Установить пароль SMTP	switch(config)#smtp password
<b>smtp rcptemail</b> [Index] [Email address]	<b>G</b>	Указать e-mail адрес получателя	switch(config)#smtp rcptemail 1 <u>Alert@test.com</u>
<b>show smtp</b>	<b>P</b>	Показать информацию об SMTP	switch#show smtp
<b>no smtp</b>	<b>G</b>	Отключить функцию SMTP	switch(config)#no smtp
<b>event device-cold-start</b> [Systemlog SMTP Both]	<b>G</b>	Включить оповещение о перезагрузке	switch(config)#event device-cold-start both
<b>event authentication- failure</b> [Systemlog SMTP Both]	<b>G</b>	Включить оповещение о провале аутентификации	switch(config)#event authentication-failure both
<b>event Sy-Ring-topology- change</b> [Systemlog SMTP Both]	<b>G</b>	Включить оповещение об изменении в кольцевой топологии	switch(config)#event ring-topology-change both
<b>event systemlog</b> [Link-UP Link- Down Both]	<b>I</b>	Включить оповещения о событиях интерфейсов для системного журнала	switch(config)#interface fastethernet 3 switch(config-if)#event systemlog both
<b>event smtp</b> [Link-UP Link- Down Both]	<b>I</b>	Включить оповещения о событиях интерфейсов для SMTP	switch(config)#interface fastethernet 3 switch(config-if)#event smtp both
<b>show event</b>	<b>P</b>	Показать отслеживаемые события	switch#show event
<b>no event device-cold- start</b>	<b>G</b>	Выключить оповещение о перезагрузке	switch(config)#no event device-cold-start
<b>no event authentication-</b>	<b>G</b>	Выключить оповещение о	switch(config)#no event

<b>failure</b>		провале аутентификации	authentication-failure
<b>no event Sy-Ring-topology-change</b>	<b>G</b>	Выключить оповещение об изменении в кольцевой топологии	switch(config)#no event ring-topology-change
<b>no event systemlog</b>	<b>I</b>	Выключить оповещения о событиях интерфейсов для системного журнала	switch(config)#interface fastethernet 3 switch(config-if)#no event systemlog
<b>no event smpt</b>	<b>I</b>	Выключить оповещения о событиях интерфейсов для SMTP	switch(config)#interface fastethernet 3 switch(config-if)#no event smtp

### 6.15. Список команд - команды SNTP

Команды SWM-240	Уровень	Описание	Пример
<b>sntp enable</b>	<b>G</b>	Включить функцию SNTP	switch(config)#sntp enable
<b>sntp daylight</b>	<b>G</b>	Включить опцию перехода между зимним и летним временем. Эту команду нельзя применить, если SNTP функция неактивна.	switch(config)#sntp daylight
<b>sntp daylight-period</b> [Start time] [End time]	<b>G</b>	Указать начало и окончание периода летнего времени. Эту команду нельзя применить, если SNTP функция неактивна. Формат параметра: [уууymmdd-hh:mm]	switch(config)# sntp daylight-period 20060101-01:01 20060202-01-01
<b>sntp daylight-offset</b> [Minute]	<b>G</b>	Указать разницу, на которую смещаются стрелки часов. Эту команду нельзя применить, если SNTP функция неактивна.	switch(config)#sntp daylight-offset 3
<b>sntp ip</b> [IP]	<b>G</b>	Указать IP адрес SNTP сервера. Эту команду нельзя применить, если	switch(config)#sntp ip 192.169.1.1

		SNTP функция неактивна.	
<b>sntp timezone</b> [Timezone]	<b>G</b>	Выбрать номер часового пояса. Используйте команду “show sntp timezone”, чтобы получить больше информации о номерах часовых поясов	switch(config)#sntp timezone 22
<b>show sntp</b>	<b>P</b>	Показать информацию о SNTP	switch#show sntp
<b>show sntp timezone</b>	<b>P</b>	Показать список индексов часовых поясов	switch#show sntp timezone
<b>no sntp</b>	<b>G</b>	Отключить функцию SNTP	switch(config)#no sntp
<b>no sntp daylight</b>	<b>G</b>	Отключить функцию перевода стрелок часов	switch(config)#no sntp daylight

### 6.16. Список команд - команды Sy-Ring

Команды SWM-240	Уровень	Описание	Пример
<b>Ring enable</b>	G	Включить Sy-Ring	switch(config)# ring enable
<b>Ring master</b>	G	Сделать устройство корневым в кольце	switch(config)# ring master
<b>Ring couplering</b>	G	Включить Ring coupling	switch(config)# ring couplering
<b>Ring dualhoming</b>	G	Включить Dual Homing	switch(config)# ring dualhoming
<b>Ring ringport</b> [1st Ring Port] [2nd Ring Port]	G	Выбор 1-го и 2-го Ring портов	switch(config)# ring ringport 7 8
<b>Ring couplingport</b> [Coupling Port]	G	Выбор coupling port	switch(config)# ring couplingport 1
<b>Ring controlport</b> [Control Port]	G	Выбор control port	switch(config)# ring controlport 2



<b>Ring homingport</b> [Dual Homing Port]	G	Выбор dual homing порта	switch(config)# ring homingport 3
<b>show Ring</b>	P	Показать информацию об Sy-Ring	switch#show ring
<b>no Ring</b>	G	Отключить Sy-Ring	switch(config)#no ring
<b>no Ring master</b>	G	Отменить назначение корневым коммутатором в кольце	switch(config)# no ring master
<b>no Ring couplering</b>	G	Отключить Ring Coupling	switch(config)# no ring couplering
<b>no Ring dualhoming</b>	G	Отключить Dual Homing	switch(config)# no ring dualhoming