CCC
СЕРТИФИКАТ
№ ОС–4–СП–0666

Мультиплексор MC04

Блоки MC04-SWI/C000

Промышленные управляемые коммутаторы серии SWI/C000

Техническое описание и инструкция по эксплуатации.

г.Пермь

Введение 4
1.2 Назначение 4
1.3 Область применения 4
1.4 Функциональные возможности 4
1.5 Основные параметры 5
1.6 Монтаж оборудования 6
1.6.1 Монтаж оборудования на Din-рейку. 6
1.6.2 Монтаж оборудования на стену. 7
1.7 Конструктивное исполнение 9
2. Управление коммутатором с помощью технологии Web 17
2.1 О управлении с помощью технологии Web 17
2.2 Начало работы 17
2.3 Системная информация. [System information] 18
2.4 Лицевая панель [Front Panel] 19
2.5 Основные настройки [Basic Setting] 20
2.5.1 Настройка коммутатора [Switch Setting] 20
2.5.2 Установка пароля администратора [Admin Password] 21
2.5.3 Настройка параметров IP протокола коммутатора [IP Setting] 21
2.5.4 Настройка протокола SNTP [SNTP(Time)] 22
2.5.5 Настройка протокола LLDP 23
2.5.6 Автоматическое обновление программного обеспечения [Auto Provision] 24
2.5.7 Резервное копирование и восстановление [Backup & Restore] 25
2.5.8 Обновление встроенного программного обеспечения [Upgrade Firmware] 26
2.6 DHCP сервер 27
2.6.1 Настройка DHCP сервера [Setting] 28
2.6.2 Клиенты DHCP-сервера [DHCP server – Client List] 29
2.6.3. Привязка выдачи IP адресов к портам коммутатора [Port and IP Binding] 29
2.7 Настройка Портов [Port Setting] 30
2.7.1 Настройка портов [Port Control] 30
2.7.2 Состояние порта [Port Status] 31
2.7.3 Ограничение скорости порта [Rate Limit] 31
2.7.4 Агрегация каналов [Port Trunk] 32
2.7.4.1 Настройка агрегации каналов [Port Trunk - Setting] 32
2.7.4.2 Агрегация каналов – состояние [Port Trunk - Status] 33
2.8 Резервирование [Redundancy] 34
2.8.1 Протокол резервирования Redundant Ring 35
2.8.2 RSTP 37
2.8.2.1 Настройка RSTP [RSTP Setting] 38
2.9 VLAN 40
2.9.1 Настройка VLAN [VLAN Setting] 42
2.9.2 Отображение VLAN [VLAN Table] 44
2.10 SNMP 45
2.10.1 Настройка SNMP агента [SNMP – Agent Setting] 47
2.10.2 Настройка сообщений Trap [Trap Setting] 48
2.11 Приоритизация трафика [Traffic Prioritization] 49
2.11.1 Приоритизация трафика на основе портов [Port-based Priority] 51
2.11.2 COS/802.1p 52
2.11.3 TOS/DSCP 53
2.12 Multicast 54
2.12.1 IGMP Snooping 55
2.12.2 Фильтрация IGMP [Multicast Filtering] 56

2.13 Безопасность [Security] 58
2.13.1 IP Security 58
2.13.2 Port Security 59
2.13.3 MAC Blacklist 60
2.13.4 802.1x 60
2.13.4.1 Radius Server 61
2.13.4.2 Port Auth Setting 64
2.13.4.3 Port Auth State 64
2.14 Сигнализация 65
2.14.1 Аварийная сигнализация [Warning] 65
2.14.2 Сигнализация об ошибках системы [System warning] 65
2.14.2.1 настройка протокола Syslog [Syslog Setting] 66
2.14.2.2 Настройка SMTP [SMTP Setting] 67
2.14.2.3 Выбор события аварий [Event Selection] 68
2.15 наблюдение и диагностика [Monitor and Diag] 69
2.15.1 MAC Address Table 69
2.15.2 Статистика порта [Port Statistic] 70
2.15.3 Зеркалирование портов [Port Monitoring] 71
2.15.4 Локальный лог событий [System Event Log] 72
2.16 Сохранение конфигурации [Save Configuration] 72
2.17 Заводские установки [Factory Default] 73
2.18 Перезагрузка коммутатора [System Reboot] 73

1. Введение

Данное техническое описание и инструкция по эксплуатации предназначены для изучения функциональных возможностей, параметров и правил эксплуатации промышленных управляемых коммутаторов серии SWI/C000.

1.2 Назначение

Промышленные управляемые коммутаторы серии SWI/C000 – полностью управляемые промышленные коммутаторы, специально разработанные для индустриального применения в жестких промышленных условиях. Гигабитные порты и ряд функций заложенных в коммутаторы серии SWI/C000 позволяют строить высокопроизводительную сеть именно на промышленных объектах: построение виртуальных сетей (VLAN), управление группами пользователей (IGMP), управление приоритетом передачи данных, фильтрация трафика и многое другое.

1.3 Область применения

Нефтегазовая, энергетическая, транспортная, добывающая и другие отрасли

1.4 Функциональные возможности

• Время восстановления кольца по технологии S-Ring < 10 мс (до 250 устройств в кольце)
• MSTP/RSTP/STP(IEEE 802.1s/w/D)
• IGMP snooping - фильтрация группового (multicast) трафика
• LACP (Link Aggregation Control Protocol) для объединения каналов
• Поддержка протокола SNMP v1/v2/v3 для управления и контроля
• Поддержка протокола RMON – для контроля трафика
• Уведомление о событиях с помощью Syslog, Email, SNMP Trap, и релейного выхода
• Отключение порта при попытке доступа с неавторизованного MAC-адреса
• Централизованное управление и контроль с помощью Web, Telnet, Console, SNMP v1/v2/v3
• Тройное резервирование питания
• удобная комбинация1 0/100Base-T(X), 100Base- FX, 1000Base-T, 1000Base-SX, и 1000Base-LX портов в составе коммутаторов
• RS-232 порт (разъем RJ-45)
• Наличие портов с P.S.E (инжекторы PoE)
• Релейный выход
• Рабочая температура: от -40º до +70º
• Прочный металлический корпус (без вентиляторов) IP-30
• Монтаж на DIN-рейку и панель

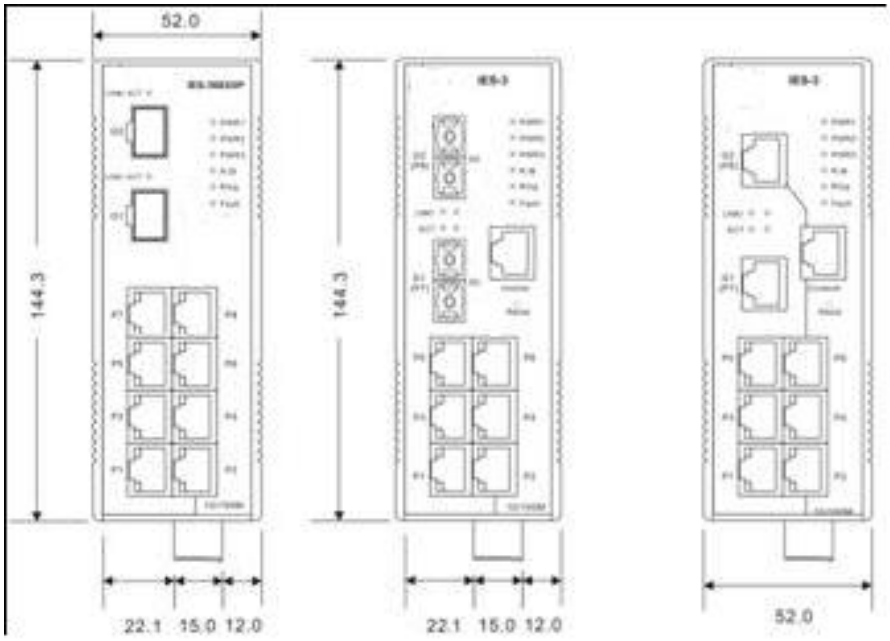
Свойства коммутатора
• Пропускная способность (Switching bandwidth) – 5.6 Гб/с
• Задержка передачи кадра – 7 мкс
• Таблица – 8192 MAC адресов
• 4 уровня приоритизации трафика

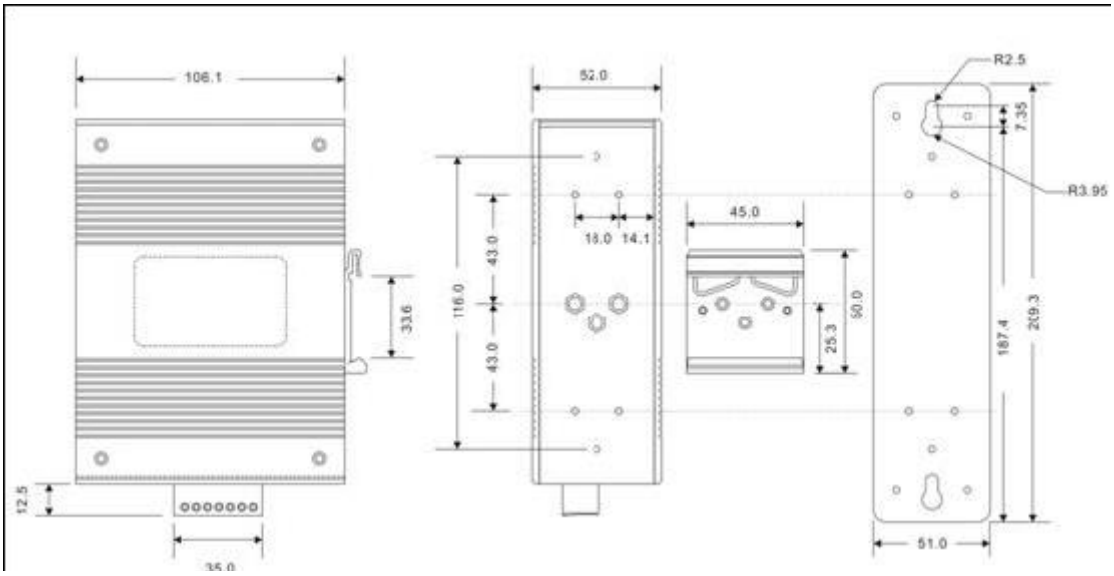
• Максимальное количество VLAN – 4096
• IGMP групп – 1024
• Ограничение скорости порта пользователем
• Поддержка протокола RADIUS
• поддержка TOS/Diffserv

1.5 Основные параметры

• Питание с возможностью резервирования (2 входа на 7-pin разъеме 12~48В DC 1 разъем типа jack 12~45В DC)
• Рабочая температура: от -40º до +70ºС
• Температура хранения: от-40º до +85ºС
• Влажность: 5% - 95%
• Корпус: IP-30
• 10/100/1000Base-T(X) порт
• 10/100Base-T(X) порт
• 100Base-FX порт
• 1000Base-X порт
• 1000Base-X SFP порт
• Консольный порт: 9600bps, 8, N, 1
• Размеры (ШхГхВ) мм: 52x108x144

Размеры (мм)



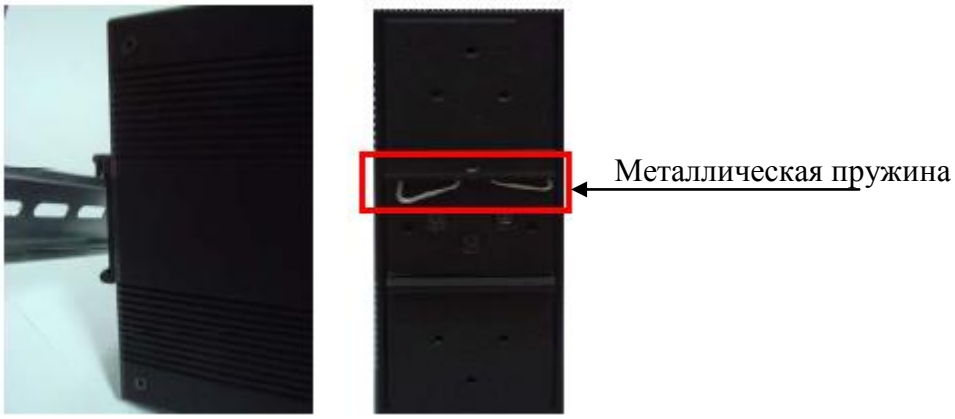


1.6 Монтаж оборудования

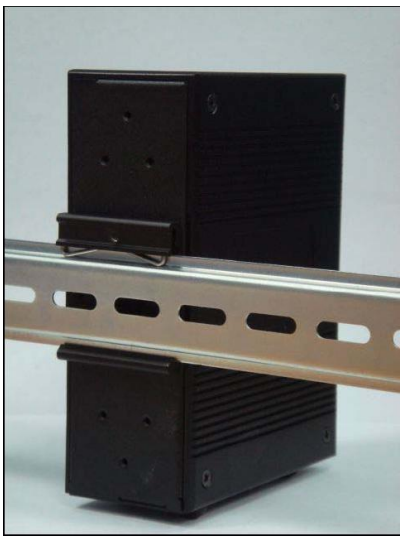
1.6.1 Монтаж оборудования на Din-рейку.

Каждый коммутатор имеет крепление на задней панели для монтажа на Din-рейку.

Шаг 1: наклонив коммутатор, зацепите металлическую пружину за Din-рейку.



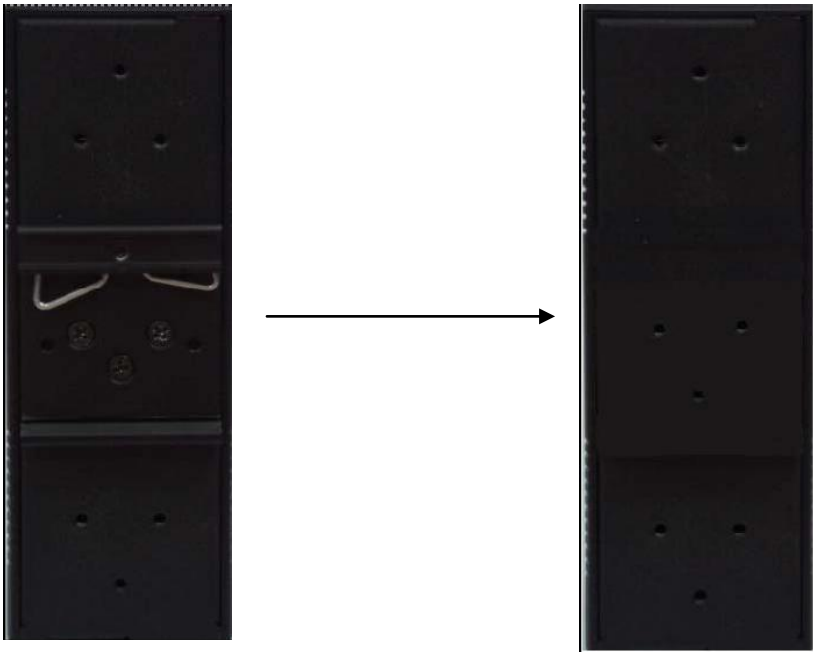
Шаг 2: защелкните нижний край крепления.



1.6.2 Монтаж оборудования на стену.

Каждый коммутатор имеет в комплекте поставки металлическую планку для крепления на стену.

Шаг 1: удалите Din-реечное крепление с задней панели, выкрутив винты



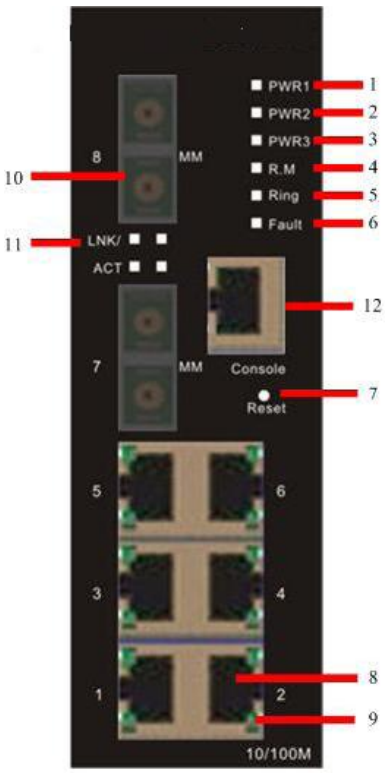
Шаг 2: Прикрепите металлическую планку к коммутатору с помощью 6 винтов (поставляются в комплекте)

Шаг 3: установите коммутатор на стену

1.7 Конструктивное исполнение

Порт	Описание
10/100 RJ-45 Fast Ethernet порт	6 10/100Base-T(x) RJ-45 Fast Ethernet портов с авто определением скорости Скорость: авто Дуплекс: авто Flow control: выключен
Gigabit RJ-45 порт	2 1000Base-TX порта для SWI-3062GT
Оптический порт (Fiber port)	2 1000BaseX порта для SWI-3062GF 2 100BaseFX порта для SWI-3062FX 2 1000BaseX SFP порта для SWI-3082GP
Console	Порт RS-232 с разъемом RJ-45
Reset	При нажатии на кнопку в течении 2-3 секунд коммутатор перезагрузится При нажатии кнопки более 5 секунд коммутатор перезагрузится с заводскими настройками

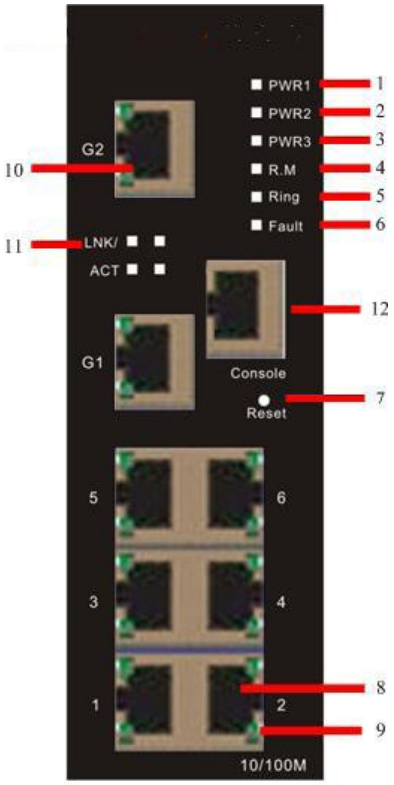
SWI/C062FX



1 - Светодиодный индикатор PWR1 – если питание подключено к разъему PWR1, то горит зеленым светом
2 - Светодиодный индикатор PWR2 – если питание подключено к разъему PWR2, то горит зеленым светом
3 - Светодиодный индикатор PWR3 – если питание подключено к разъему PWR3, то горит зеленым светом
4 – Светодиодный индикатор R.M. (Ring Master) – если горит, то это значит, что коммутатор является главным коммутатором в кольце S-Ring
5 - Светодиодный индикатор Ring – если горит, то это значит, что кольцо S-Ring активировано

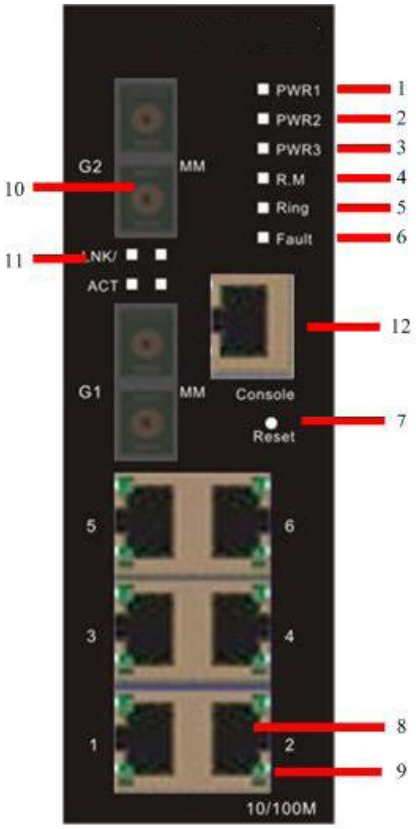
6 - Светодиодный индикатор Fault – если горит, то это значит, что произошла авария
7 – Кнопка перезагрузки – удерживание в течение 3 секунд приводит к перезагрузке, если удерживать 5 секунд, то коммутатор вернется к заводским настройкам
8 – 10/100Base(X) Ethernet порт
9 – Светодиодный индикатор состояния порта
10 – 100BaseFX оптический порт
11 – Светодиодный индикатор оптического порта.
12 – Консольный порт

SWI/C082GT и SWI/C080



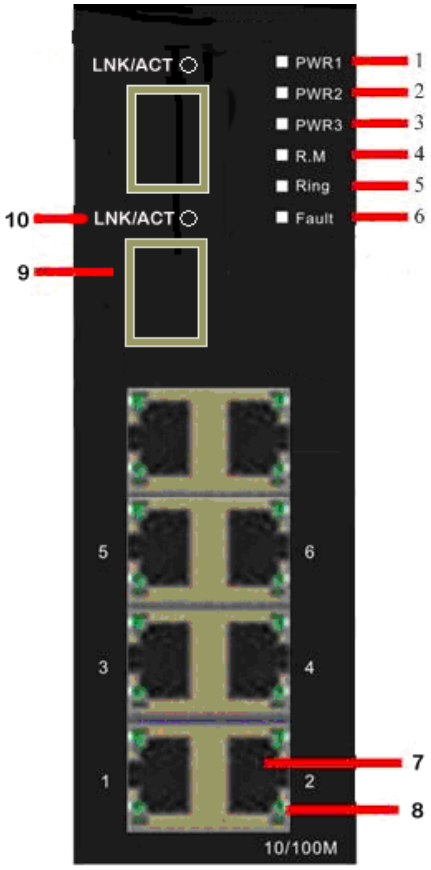
1 - Светодиодный индикатор PWR1 – если питание подключено к разъему PWR1, то горит зеленым светом
2 - Светодиодный индикатор PWR2 – если питание подключено к разъему PWR2, то горит зеленым светом
3 - Светодиодный индикатор PWR3 – если питание подключено к разъему PWR3, то горит зеленым светом
4 – Светодиодный индикатор R.M. (Ring Master) – если горит, то это значит, что коммутатор является главным коммутатором в кольце S-Ring
5 - Светодиодный индикатор Ring – если горит, то это значит, что кольцо S-Ring активировано
6 - Светодиодный индикатор Fault – если горит, то это значит, что произошла авария
7 – Кнопка перезагрузки – удерживание в течение 3 секунд приводит к перезагрузке, если удерживать 5 секунд, то коммутатор вернется к заводским настройкам
8 – 10/100Base(X) Ethernet порт
9 – Светодиодный индикатор состояния порта
10 – 1000Base-T Ethernet порт (SWI-3062GT), 10/100Base-T порт (SWI-3080)
11 - Светодиодный индикатор состояния порта
12 – Консольный порт

SWI/C062GF



1 - Светодиодный индикатор PWR1 – если питание подключено к разъему PWR1, то горит зеленым светом
2 - Светодиодный индикатор PWR2 – если питание подключено к разъему PWR2, то горит зеленым светом
3 - Светодиодный индикатор PWR3 – если питание подключено к разъему PWR3, то горит зеленым светом
4 – Светодиодный индикатор R.M. (Ring Master) – если горит, то это значит, что коммутатор является главным коммутатором в кольце S-Ring
5 - Светодиодный индикатор Ring – если горит, то это значит, что кольцо S-Ring активировано
6 - Светодиодный индикатор Fault – если горит, то это значит, что произошла авария
7 – Кнопка перезагрузки – удерживание в течение 3 секунд приводит к перезагрузке, если удерживать 5 секунд, то коммутатор вернется к заводским настройкам
8 – 10/100Base(X) Ethernet порт
9 – Светодиодный индикатор состояния порта
10 – 1000BaseX оптический порт
11 – Светодиодный индикатор оптического порта.
12 – Консольный порт (RJ-45)

SWI/C082GP



1 - Светодиодный индикатор PWR1 – если питание подключено к разъему PWR1, то горит зеленым светом
2 - Светодиодный индикатор PWR2 – если питание подключено к разъему PWR2, то горит зеленым светом
3 - Светодиодный индикатор PWR3 – если питание подключено к разъему PWR3, то горит зеленым светом
4 – Светодиодный индикатор R.M. (Ring Master) – если горит, то это значит, что коммутатор является главным коммутатором в кольце S-Ring
5 - Светодиодный индикатор Ring – если горит, то это значит, что кольцо S-Ring активировано
6 - Светодиодный индикатор Fault – если горит, то это значит, что произошла авария
7 - 10/100Base(X) Ethernet порт
8 - Светодиодный индикатор состояния порта
9 – 100Base-FX/1000BaseX SFP порт
10- Светодиодный индикатор состояния оптического порт (SFP)

Значение светодиодных индикаторов расположенных на лицевой панели

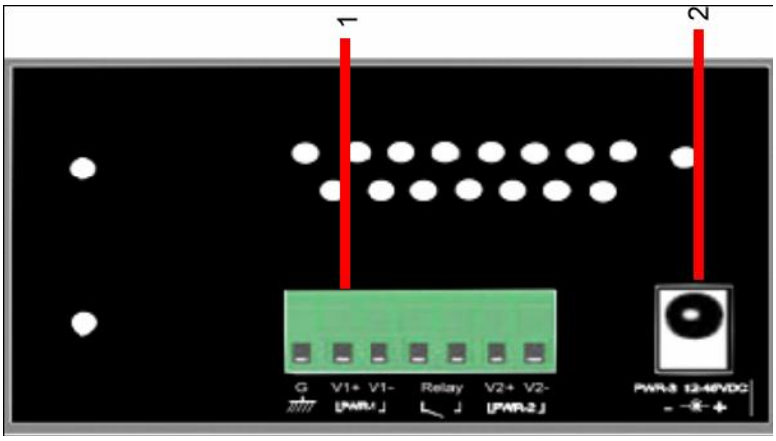
Светодиодный индикатор	Цвет	Состояние	Описание
PWR1	зеленый	Горит постоянно	Питание подключено к модулю 1
PWR2	зеленый	Горит постоянно	Питание подключено к модулю 2
PWR3	зеленый	Горит постоянно	Питание

			подключено к разъему jack
R.M	зеленый	Горит постоянно	коммутатор является главным коммутатором в кольце S-Ring
Ring	зеленый	Горит постоянно	Кольцо S-Ring включено и все линки работают
		Медленно мигает	Один из линков кольца отключен
		Быстро мигает	-
Fault	желтый	Горит постоянно	Релйный выход Отключение питания или отключился один из портов
10/100Base-T(X) Fast Ethernet порт			
LNK	зеленый	Горит постоянно	Порт включен
ACT	зеленый	мигает	Передача данных
Full Duplex	желтый	Горит постоянно	Порт работает в режиме полный дуплекс
Gigabit Ethernet порт			
ACT	зеленый	мигает	Передача данных
LNK	желтый	Горит постоянно	Линк поднят
Оптический порт			
ACT	зеленый	мигает	Передача данных
LNK	желтый	Горит постоянно	Линк поднят
SFP			
LNK	Зеленый	Горит постоянно	Линк поднят
ACT	зеленый	Горит постоянно	Передача данных

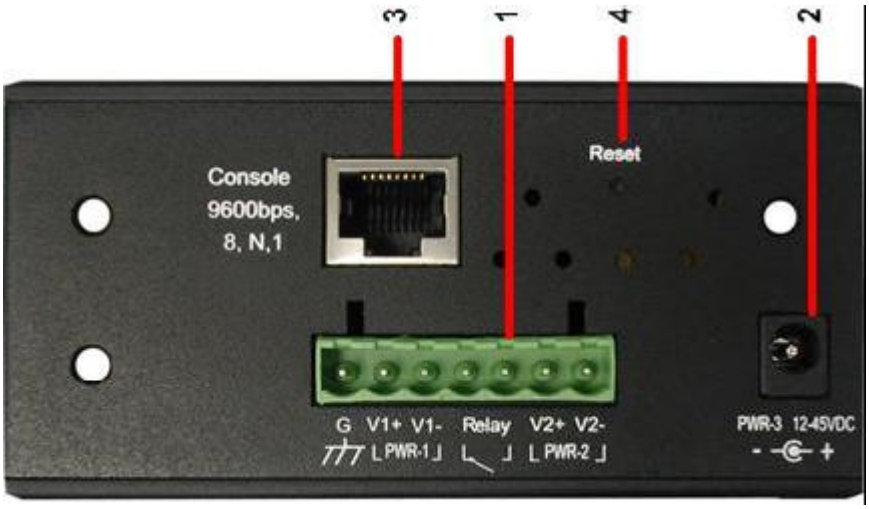
Нижняя панель

Нижняя панель SWI/C062GF/GT/FX-C080

1 – 7 контактная группа: PWR1, PWR2 (12-48VDC) и релейный выход (1A@24VDC)
2- разъем питания типа jack PWR3

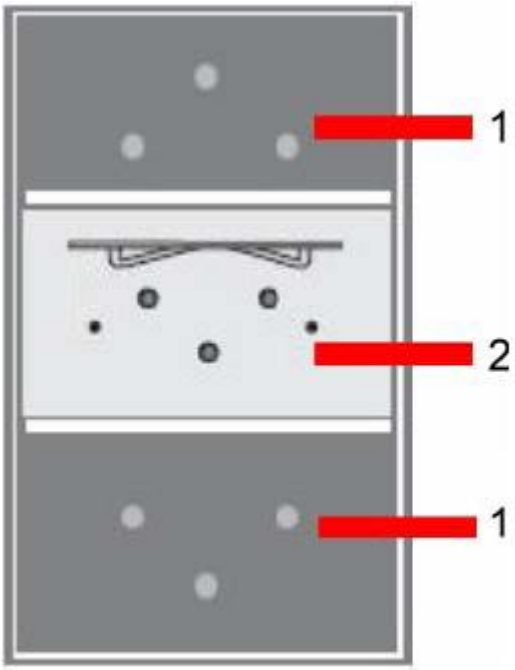


Нижняя панель SWI/C082GP



1 – 7 контактная группа: PWR1, PWR2 (12-48VDC) и релейный выход (1A@24VDC)
2 - разъем питания типа jack PWR3
3 – Консольный порт
4 - Кнопка перезагрузки – удерживание в течение 3 секунд приводит к перезагрузке, если удерживать 5 секунд, то коммутатор вернется к заводским настройкам

Задняя панель



1 – отверстия с резьбой для крепления металлической планки
2 – крепление для монтажа на DIN-рейку.

Разъемы и кабели

Коммутаторы SWI/C062FX, SWI/C062GF имеют оптические порты с SC коннекторами. Пожалуйста помните, что TX порт коммутатора A должен быть соединен с RX портом коммутатора B

Для модуля SFP необходимы оптические кабели с разъемом LC.

Консольный кабель

Для управления коммутаторами может быть использован последовательный порт RS(232) – консольный порт.

PC (male)	RS-232 DB9 female	DB9 - RJ 45
Pin #2 RD	Pin #2 TD	Pin #2
Pin #3 TD	Pin #3 RD	Pin #3
Pin #5 GD	Pin #5 GD	Pin #5

2. Управление коммутатором с помощью технологии Web

2.1 О управлении с помощью технологии Web

Web сайт HTML загружен во флэш-память коммутатора, которая находится на плате CPU. Web сайт позволяет вам легко управлять коммутатором с помощью стандартного web-браузера (такой как Microsoft Internet Explorer 5.0 или позже), где бы вы не находились в сети.

Замечание: по умолчанию в IE 5.0 или более поздних версиях не включены Java Апплеты. Вам необходимо в настройках браузера включить возможность использовать Java Апплеты.

2.2 Начало работы

Подсоедините кабель RJ45 к любому порту коммутатора. Убедитесь, что коммутатор доступен в сети (есть ping с ПК к адресу 192.168.10.1). Запустите на ПК Интернет-браузер. В строке «Адрес» Интернет-браузера введите 192.168.10.1 и нажмите ввод. Появится окно Web-управления. Введите имя пользователя admint и пароль admin (см. рис.1). После этого появится окно Web-управления коммутатора.

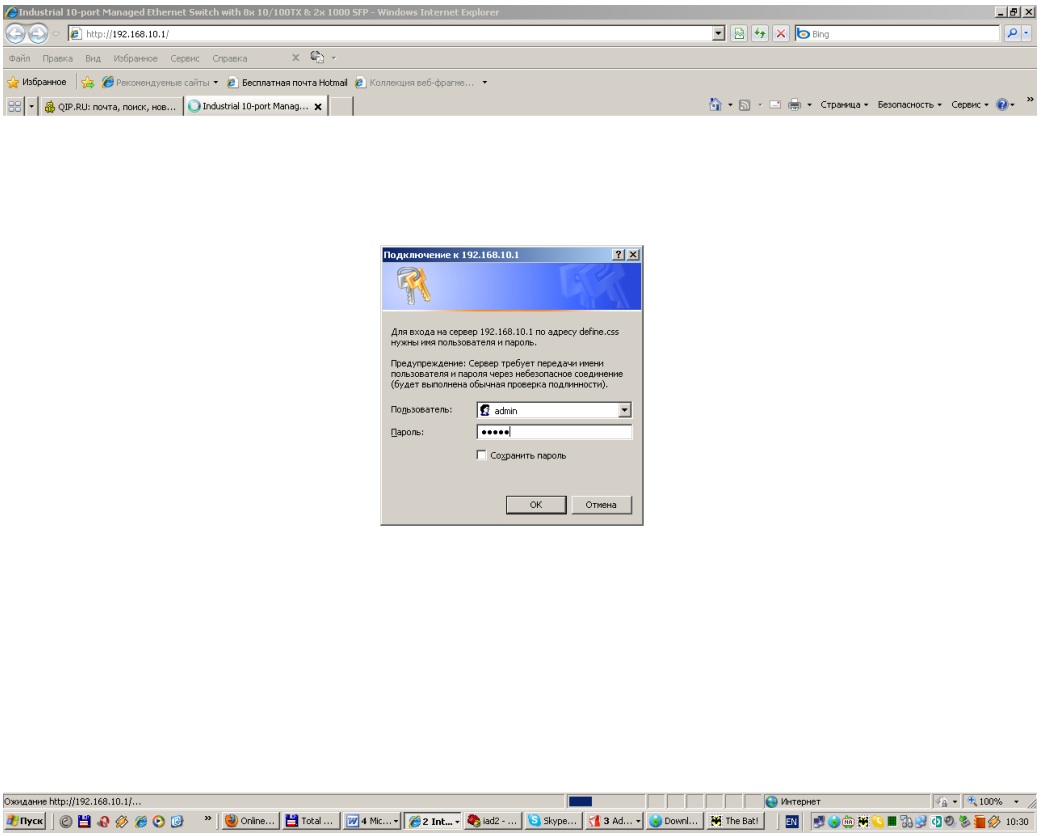
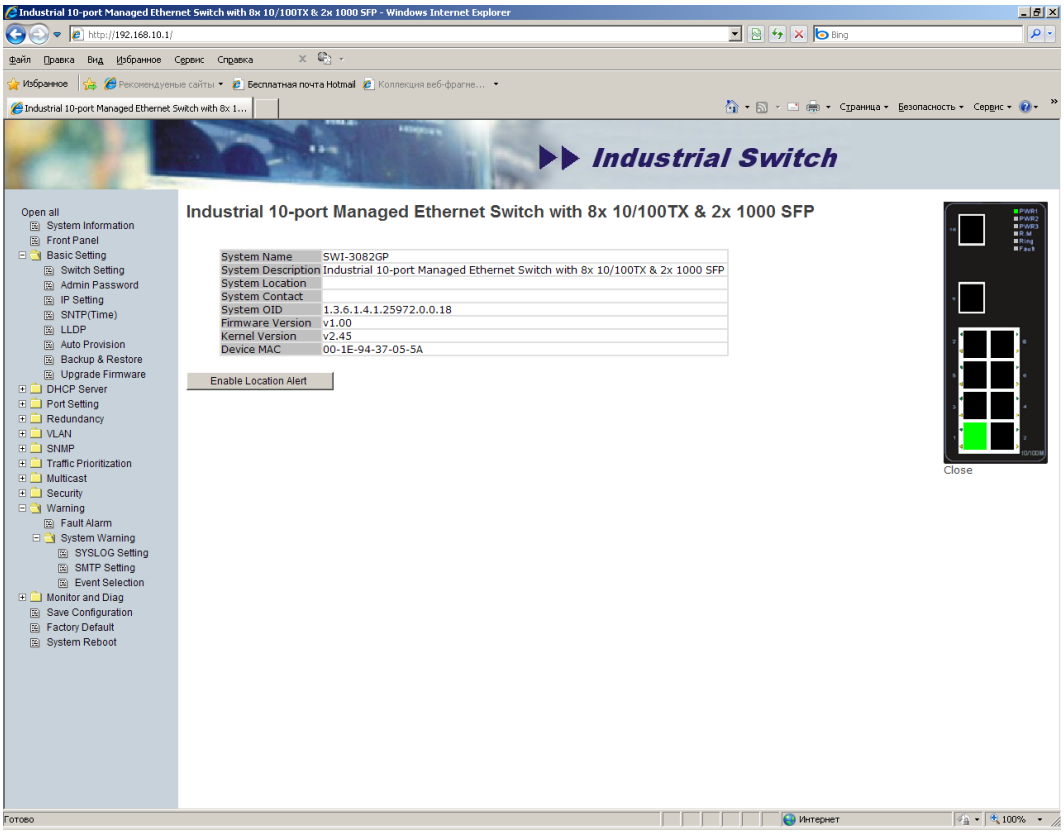


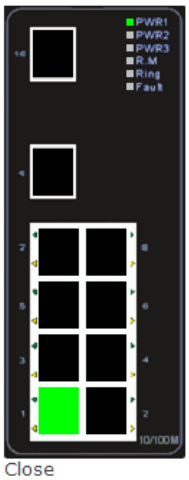
Рис.1

2.3 Системная информация. [System information]



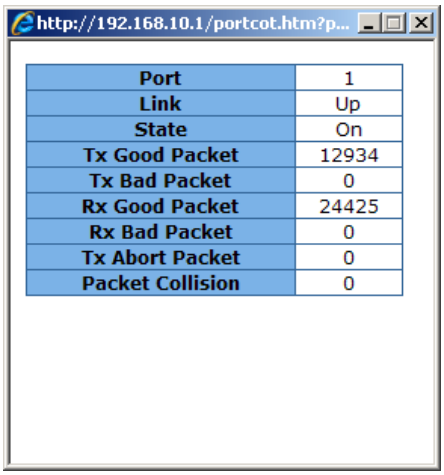
На этой странице отображается информация, которая настраивается на странице Настройка коммутатора [Basic Setting]→[Switch Setting].
После нажатия кнопки Enable Location Alert светодиодные индикаторы PWR1, PWR2, PWR3, Fault начнут мигать вместе. После нажатия кнопки Disable Location Alert мигать индикаторы перестанут. Сделано это для того, чтобы физически обозначить коммутатор на месте (если в одном месте большое количество установленных коммутаторов, то не всегда можно определить каким именно коммутатором ты в данный момент управляешь)

2.4 Лицевая панель [Front Panel]



Close

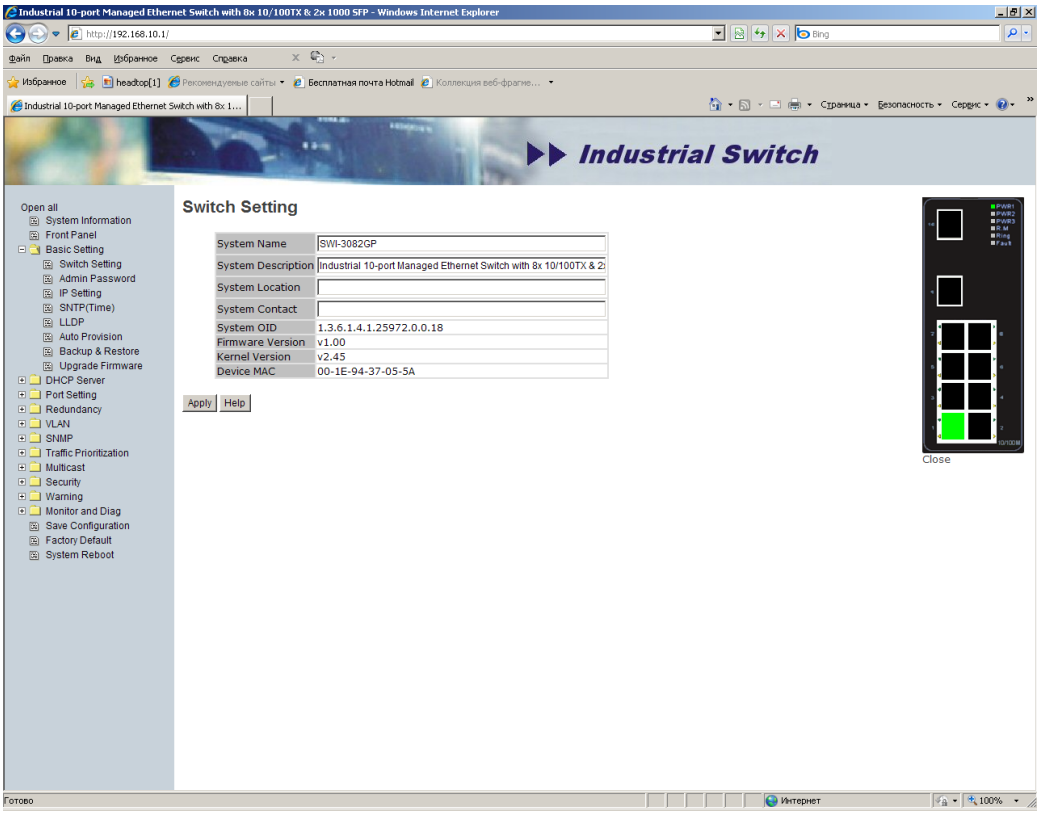
На странице [System information] также отображается реальное состояние лицевой панели коммутаторов серии SWI/C000. Зеленом цветом обозначаются активные порты Кликнув левой кнопкой «мыши» на любой порт, можно посмотреть его состояние и статистику.



Port	1
Link	Up
State	On
Tx Good Packet	12934
Tx Bad Packet	0
Rx Good Packet	24425
Rx Bad Packet	0
Tx Abort Packet	0
Packet Collision	0

2.5 Основные настройки [Basic Setting]

2.5.1 Настройка коммутатора [Switch Setting]



Описание параметров

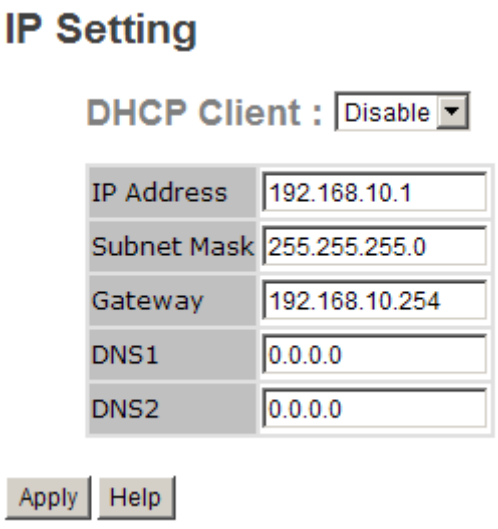
Параметр	Оисание
System Name	Системное название коммутатора. Любое слово – максимальная длина 64 байта
System Description	Описание коммутатора.
System Location	Описания физического размещения коммутатора. Любы слова максимальная длина 64 байта
System Contact	Имя ответственного человека или название организации
System OID	Системный идентификатор объекта
Firmware Version	Версия программного обеспечения
Kernel Version	Версия ядра программного обеспечения
MAC Address	Уникальный MAC адрес коммутатора.

2.5.2 Установка пароля администратора [Admin Password]

Описание параметров

Параметр	Описание
User name	Имя пользователя (по умолчанию “**admin**”)
New Password	Новый пароль (по умолчанию “**admin**”)
Confirm password	Подтверждение пароля.
Apply	Нажмите “**Apply**” чтобы активировать изменения.

2.5.3 Настройка параметров IP протокола коммутатора [IP Setting]

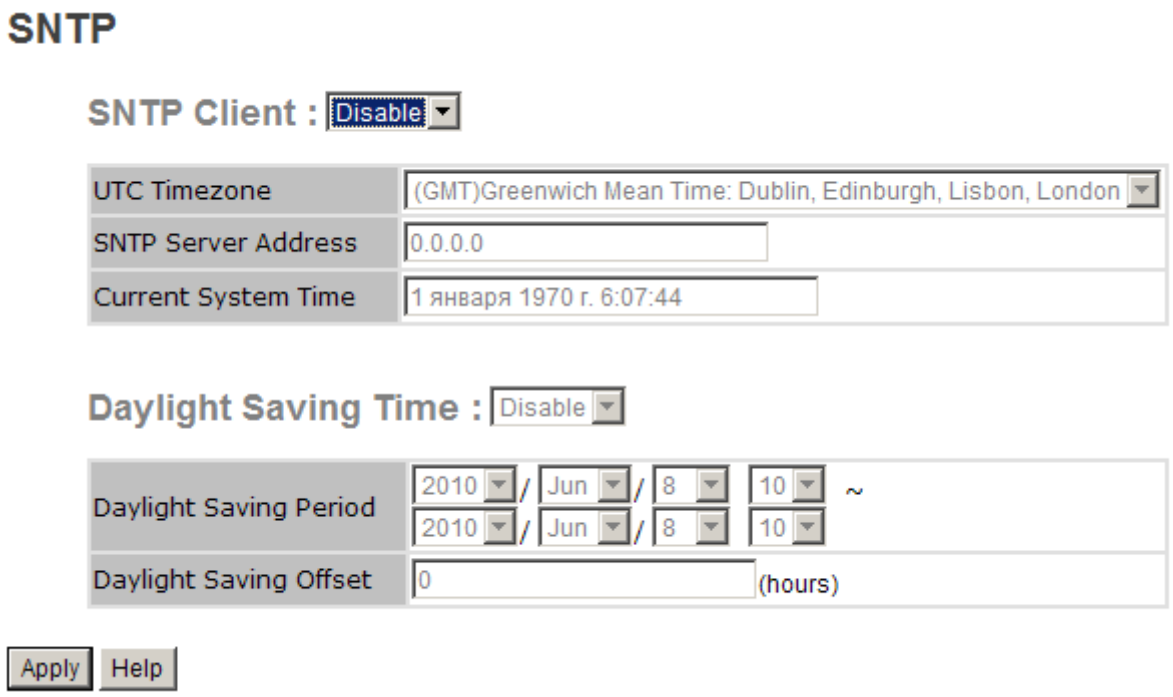


Описание параметров

Парметр	Описание
DHCP Client	активирует (Enable) и деактивирует DHCP клиента на коммутаторе. Когда DHCP клиент активирован, коммутатор получает IP адрес от сетевого DHCP сервера. После того как вы активируете DHCP клиент, IP адрес коммутатора по умолчанию заменится на адрес, который будет получен от DHCP сервера.
IP Address	IP адрес коммутатора, Если DHCP клиент активирован, то вам не надо устанавливать IP адрес. В этой строке будет показан адрес, который коммутатору выдаст DHCP клиент. По умолчанию IP адрес – 192.168.10.1
Subnet Mask	Маска подсети. Если DHCP клиент активирован, то вам не надо устанавливать маску подсети
Gateway	IP Адрес основного сетевого шлюза. По умолчанию - 192.168.10.254
DNS1	IP адрес основного DNS сервера
DNS2	IP адрес дополнительного DNS сервера
Apply	Нажмите “**Apply**”, чтобы активировать конфигурацию

2.5.4 Настройка протокола SNTP [SNTP(Time)]

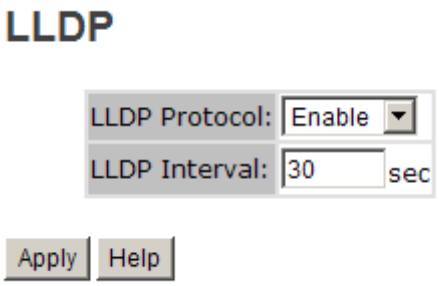
SNTP (Simple Network Time Protocol) – протокол, с помощью которого коммутатор синхронизирует свои часы с внешним сервером.



Описание параметров

Параметр	Описание
SNTP Client	Активирует (Enable) или деактивирует (Disable) SNTP клиента.
Daylight Saving Time	Активирует переход на летнее время. Если вы включаете эту функцию, то необходимо указать период действия летнего времен в строке Daylight Saving period
UTC Time zone	Часовые пояса UTC - Universal Coordinated Time всеобщее скоординированное время
SNTP Server Address	IP адрес SNTP сервера
Current System Time	Показывает текущее время коммутатора.
Daylight Saving Period	Время начала и конца действия летнего времени.
Daylight Saving Offset	Количество часов, на которое смещается время
Apply	Нажмите Apply, чтобы активировать новую конфигурацию

2.5.5 Настройка протокола LLDP



Link Layer Discovery Protocol (**LLDP**) - протокол канального уровня, позволяющий сетевому оборудованию оповещать локальную сеть о своем существовании и характеристиках, а также собирать такие же оповещения, поступающие от соседнего оборудования. Протокол формально утвержден как IEEE standard 802.1AB-2005, в мае 2005 года, и является независимым от производителей сетевого оборудования заменой их патентованным протоколам, таким как Cisco Discovery Protocol, Extreme Discovery Protocol, Foundry Discovery Protocol и Nortel Discovery Protocol.

Применение:
Информация собранная посредством LLDP накапливается в устройствах, и может быть запрошена посредством SNMP. Таким образом, топология сети, в которой используется LLDP, может быть получена с управляющего компьютера, посредством последовательного обхода и опроса каждого устройства, на предмет собранной им информации. При этом получаемая информация содержит:

- имя устройства и его описание (описательные поля *system name* и её *description* в настройках сетевого оборудования)
- имя порта и его описание (*port name* и *description*)

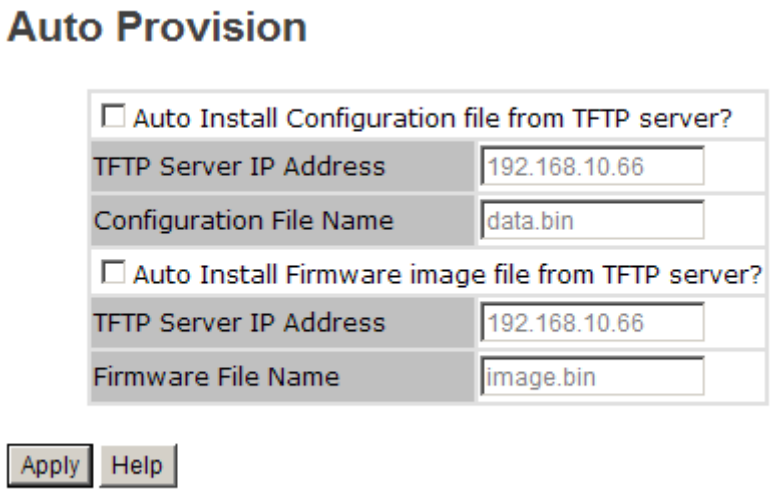
- имя VLAN
- IP-адрес устройства, по которому оно доступно для управления (запросов) по протоколу SNMP
- функции устройства - коммутация, маршрутизация и т.п.
- информация о MAC/PHY
- MDI power
- параметры объединения каналов (*link aggregation*)

Используя эту информацию, и опрашивая MIB базы данных обнаруженных устройств, системы управления могут динамически моделировать и отслеживать состояния локальных сетей передачи данных (LAN), а также строить их визуальные схемы для пользователей и администраторов.

Описание параметров

Параметр	описание
LLDP Protocol	Активировать и деактивировать LLDP протокол
LLDP Interval	Интервал отправки LLDP пакетов (по умолчанию 30 секунд)
Apply	Нажмите Apply, чтобы активировать конфигурацию.

2.5.6 Автоматическое обновление программного обеспечения [Auto Provision]



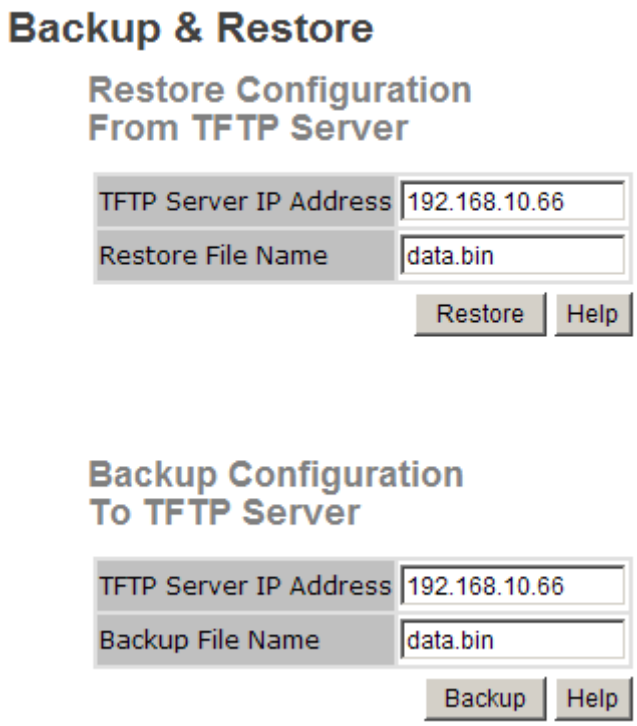
Функция [Auto Provision] позволяет автоматически обнавлять програмное обеспечение [firmware] и файл конфигурации с помощью TFTP сервера. После того как вы перезагрузите коммутатор, он автоматически загрузит файлы с TFTP сервера. До перезагрузки коммутатора убидитесь, что TFTP сервер готов и на нем находятся нужные файлы.

Описание параметров

Auto Install Configuration File from TFTP server?	Если отметить этот параметр, то коммутатор будет автоматически загружать конфигурационный файл
TFTP Server IP Address	IP адрес TFTP сервера

Configuration File Name	Имя конфигурационного файла
Auto Install Firmware image file from TFTP server?	Если отметить этот параметр, то коммутатор будет автоматически загружать образ программного обеспечения
Firmware File Name	Имя файла программного обеспечения

2.5.7 Резервное копирование и восстановление [Backup & Restore]



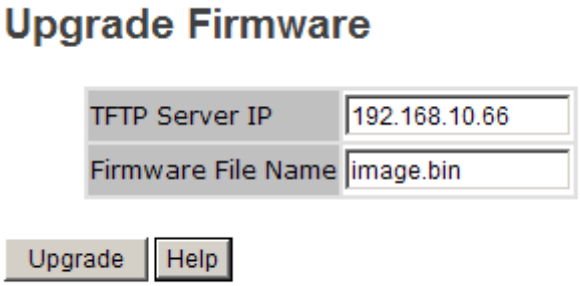
Вы можете сохранить конфигурацию коммутатора с помощью протокола TFTP [Backup] на сервер и загрузить конфигурацию с сервера в коммутатор [Restore]

Описание параметров

Параметр	описание
TFTP Server IP Address	IP адрес TFTP сервера
Restore File Name	Имя конфигурационного файла.
Restore	Нажмите “**restore**” чтобы записать конфигурационный файл в EEPROM.
Buckup File Name	Имя конфигурационного файла.
Backup	Нажмите “**backup**” чтобы сохранить файл на сервер

2.5.8 Обновление встроенного программного обеспечения [Upgrade Firmware]

С помощью этой функции вы можете обновлять программное обеспечение коммутатора. Перед обновлением убедитесь, что образ программного обеспечения находится на TFTP сервере. После того как программное обеспечение было загружено в коммутатор, его необходимо перезагрузить.



Описание параметров

Параметр	Описание
TFTP Server IP	IP адрес TFTP сервера
Firmware File Name	Имя файла программного обеспечения
Upgrade	Нажмите **Upgrade,** чтобы загрузить файл

2.6 DHCP сервер

DHCP (англ. *Dynamic Host Configuration Protocol* - протокол динамической конфигурации узла) - это сетевой протокол, позволяющий компьютерам автоматически получать IP-адрес и другие параметры, необходимые для работы в сети TCP/IP. Данный протокол работает по модели «клиент-сервер». Для автоматической конфигурации компьютер - клиент на этапе конфигурации сетевого устройства обращается к т.н. *серверу DHCP*, и получает от него нужные параметры. Сетевой администратор может задать диапазон адресов, распределяемых сервером среди компьютеров. Это позволяет избежать ручной настройки компьютеров сети и уменьшает количество ошибок. Протокол DHCP используется в большинстве крупных (и не очень) сетей TCP/IP.

Распределение IP-адресов

Протокол DHCP предоставляет три способа распределения IP-адресов:

- *Ручное распределение.* При этом способе сетевой администратор сопоставляет аппаратному адресу (обычно MAC-адресу) каждого клиентского компьютера определённый IP-адрес. Фактически, данный способ распределения адресов отличается от ручной настройки каждого компьютера лишь тем, что сведения об адресах хранятся централизованно (на сервере DHCP), и потому их проще изменять при необходимости.
- *Автоматическое распределение.* При данном способе каждому компьютеру на постоянное использование выделяется произвольный свободный IP-адрес из определённого администратором диапазона.
- *Динамическое распределение.* Этот способ аналогичен автоматическому распределению, за исключением того, что адрес выдаётся компьютеру не на постоянное пользование, а на определённый срок. Это называется *арендой адреса*. По истечении срока аренды IP-адрес вновь считается свободным, и клиент обязан запросить новый (он, впрочем, может оказаться тем же самым).

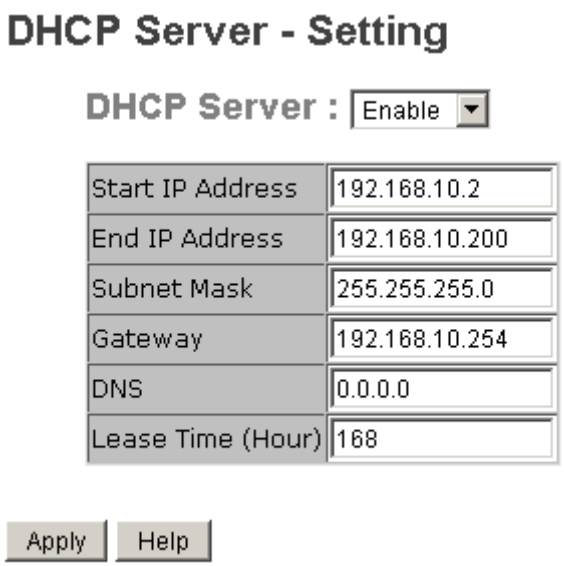
Помимо IP-адреса, DHCP также может сообщать клиенту дополнительные параметры, необходимые для нормальной работы в сети. Эти параметры называются *опциями DHCP*. Список стандартных опций можно найти в RFC 2132.

Некоторыми из наиболее часто используемых опций являются:

- IP-адрес маршрутизатора по умолчанию;
- маска подсети;
- адреса серверов DNS;
- имя домена DNS.

2.6.1 Настройка DHCP сервера [Setting]

В промышленные коммутаторы SWI/C000 встроены функции DHCP-сервера.

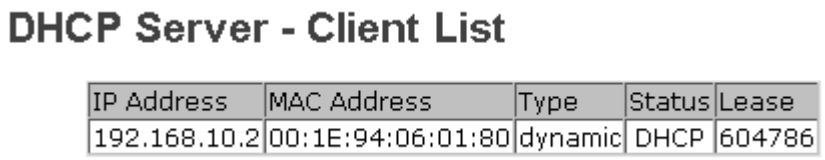


Описание параметров

Параметр	Описание
DHCP Server	Включает [Enable] или выключает [Disable] функции DHCP-сервера. Enable – коммутатор будет DHCP-сервером в локальной сети
Start IP Address	Начальный IP-адрес динамического диапазона IP-адресов. Пример: необходимо выдавать IP-адреса в диапазоне с 192.168.1.100 до 192.169.1.200. **Start IP Address** – 192.168.1.100
End IP Address	Конечный IP-адрес динамического диапазона IP-адресов. Пример: необходимо выдавать IP-адреса в диапазоне с 192.168.1.100 до 192.169.1.200. **End IP Address** – 192.168.1.200
Subnet Mask	Маска подсети, которая будет выдаваться динамически клиентам
Gateway	Сетевой шлюз, который будет выдаваться динамически клиентам.
DNS	IP-адрес DNS-сервера, который будет выдаваться динамически клиентам
Lease Time (Hour)	Срок аренды выданного IP-адреса (часы). По истечении срока аренды IP-адрес вновь считается свободным, и клиент обязан запросить новый
Apply	Нажмите **Apply** чтобы активировать конфигурацию

2.6.2 Клиенты DHCP-сервера [DHCP server – Client List]

Когда функции DHCP-сервера включены, то коммутатор собирает информацию о клиентах и отображает на этой странице.

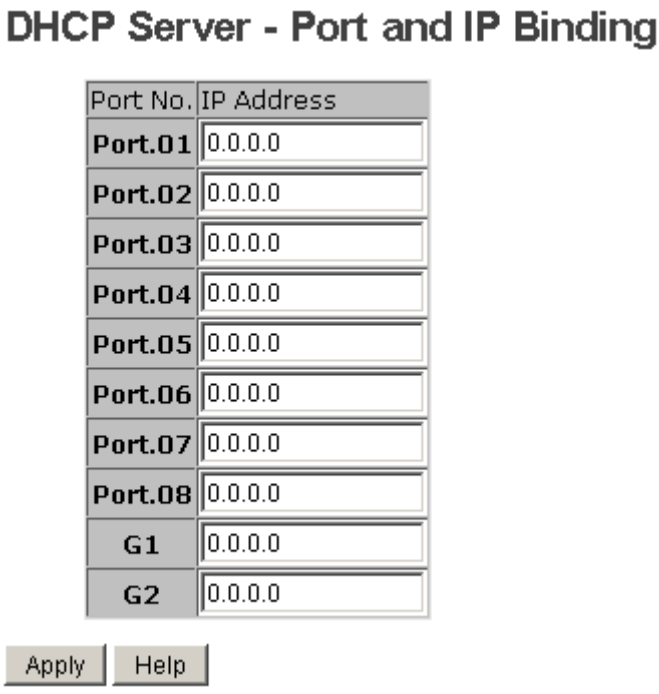


Описание параметров

Параметр	Описание
IP Address	IP адрес клиента, который он получил
MAC Address	MAC адрес клиента
Type	Способ получения IP адреса
Status	
Lease	Срок аренды в секундах

2.6.3. Привязка выдачи IP адресов к портам коммутатора [Port and IP Binding]

Вы можете «привязать» IP адрес из назначенного вами динамического диапазона к определенному порту. Когда сетевое устройство подсоединяется к порту и запрашивает IP адрес, то ему всегда выдается IP адрес, который «привязан» к данному порту.



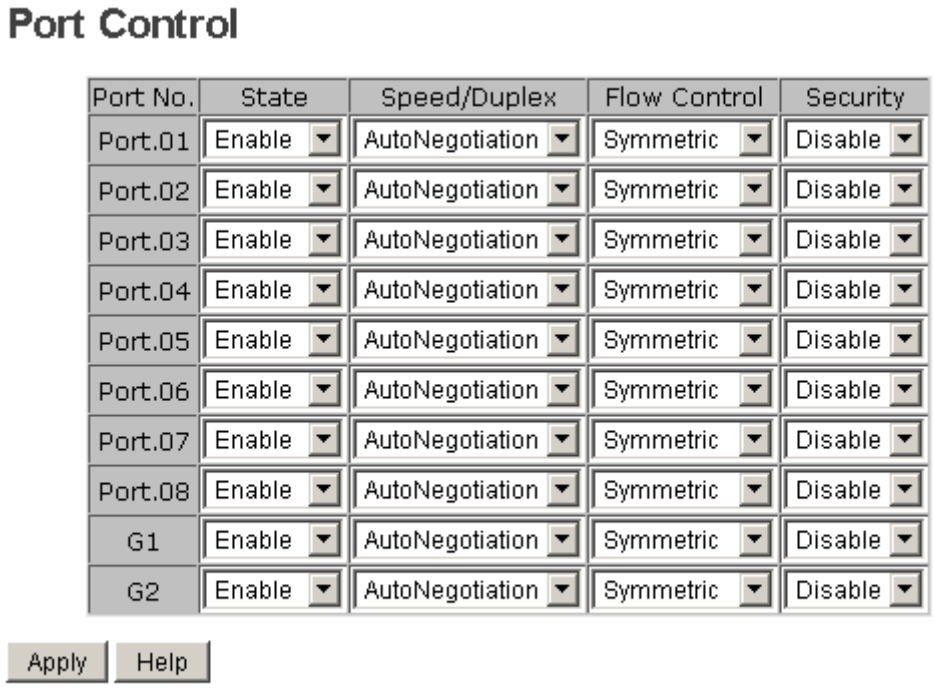
Если в колонке IP Address стоит 0.0.0.0, то это значит, что IP адрес не назначен.

2.7 Настройка Портов [Port Setting]

На этой странице настраиваются физические параметры портов

2.7.1 Настройка портов [Port Control]

С помощью этой страницы настраивается состояние порта, скорость, безопасность и т.п.



Описание параметров

Параметр	Описание
Port NO.	Номер порта, который настраиваете.
State	Состояние порта **Enable** – порт включен и готов к работе. **Disable –** порт выключен
Speed/Duplex	Устанавливается скорость и режим работы портов. **AutoNegotiation** – автоопределение режима работы
Flow Control	Включение режима работы IEEE 802.3x Flow control. **Symmetric** – режим работы Flow Control. Если оба соединенных порта поддерживают работу Flow Control в полном объеме, то эта функция включается. Если один из портов не поддерживает эту функцию, то она будет неактивна. **Asymmetric –** Flow control всегда включен вне зависимости от второго порта. **Disable** – функция Flow control выключена.
Security	**Enable –** включить функцию безопасности порта. Принцип работы: при включении этой функции коммутатор обрабатывает только фреймы, которые пришли на данный порт и содержат MAC адреса указанные на странице **Security ->Port Security.**
Apply	Нажмите “**Apply**” чтобы применить новую конфигурацию.

2.7.2 Состояние порта [Port Status]

На данной странице отображается 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
Port.05	100TX	Down	Enable	N/A	N/A
Port.06	100TX	Down	Enable	N/A	N/A
Port.07	100TX	UP	Enable	100 Full	Disable
Port.08	100TX	Down	Enable	N/A	N/A
G1	SFP	Down	Enable	N/A	N/A
G2	SFP	Down	Enable	N/A	N/A

2.7.3 Ограничение скорости порта [Rate Limit]

Rate Limit

Port No.	Ingress Limit Frame Type	Ingress	Egress
Port.01	All	0 kbps	0 kbps
Port.02	All	0 kbps	0 kbps
Port.03	All	0 kbps	0 kbps
Port.04	All	0 kbps	0 kbps
Port.05	All	0 kbps	0 kbps
Port.06	All	0 kbps	0 kbps
Port.07	All	0 kbps	0 kbps
Port.08	All	0 kbps	0 kbps
G1	All	0 kbps	0 kbps
G2	All	0 kbps	0 kbps

Rate range is from 100 kbps to 102400 kbps (i.e. 100Mbps) for mega-ports, or 256000 kbps (i.e. 250Mbps) for giga-ports. Zero means no limit.

Apply Help

На этой странице настраивается ограничение входящей исходящей скорости передачи информации на портах. А также вид служебного трафика, который необходимо ограничить.

Описание параметров

Параметр	Описание
Ingress Limit Frame Type	Тип входящего трафика который необходимо ограничить. **All** – весь трафик. **Broadcast/Multicast/Flooded Unicast** – весь служебный трафик (широковещательный, групповой, и юникастовый трафик). **Broadcast/Multicast –** широковещательный и групповой трафик. **Broadcast only** – только широковещательный трафик. Ограничение по типу трафика касается **только входящего трафика Ingress.**
Ingress	Ограничение входящего трафика. От 100 кб/с до 102400 кб/с (100 Мб/с) с шагом 1 кб/с (1024кб/с – 1Мб/с) Для Гигабитных портов от 100 кб/с до 256000 кб/с (250 Мб/с)
Egress	Ограничение исходящего трафика. От 100 кб/с до 102400 кб/с (100 Мб/с) с шагом 1 кб/с (1024кб/с – 1Мб/с) Для Гигабитных портов от 100 кб/с до 256000 кб/с (250 Мб/с)
Apply	Нажмите “**Apply**” чтобы применить новую конфигурацию

2.7.4 Агрегация каналов [Port Trunk]

Агрегирование каналов — технология, которая позволяет объединить несколько физических каналов в один логический. Такое объединение позволяет увеличивать пропускную способность канала и увеличить надежность канала. Агрегирование каналов может быть настроено как между двумя коммутаторами, так и между коммутатором и сервером.

Чтобы Port Trunk работал правильно, физические порты-члены Port Trunk должны иметь одинаковые свойства, перечисленные ниже:

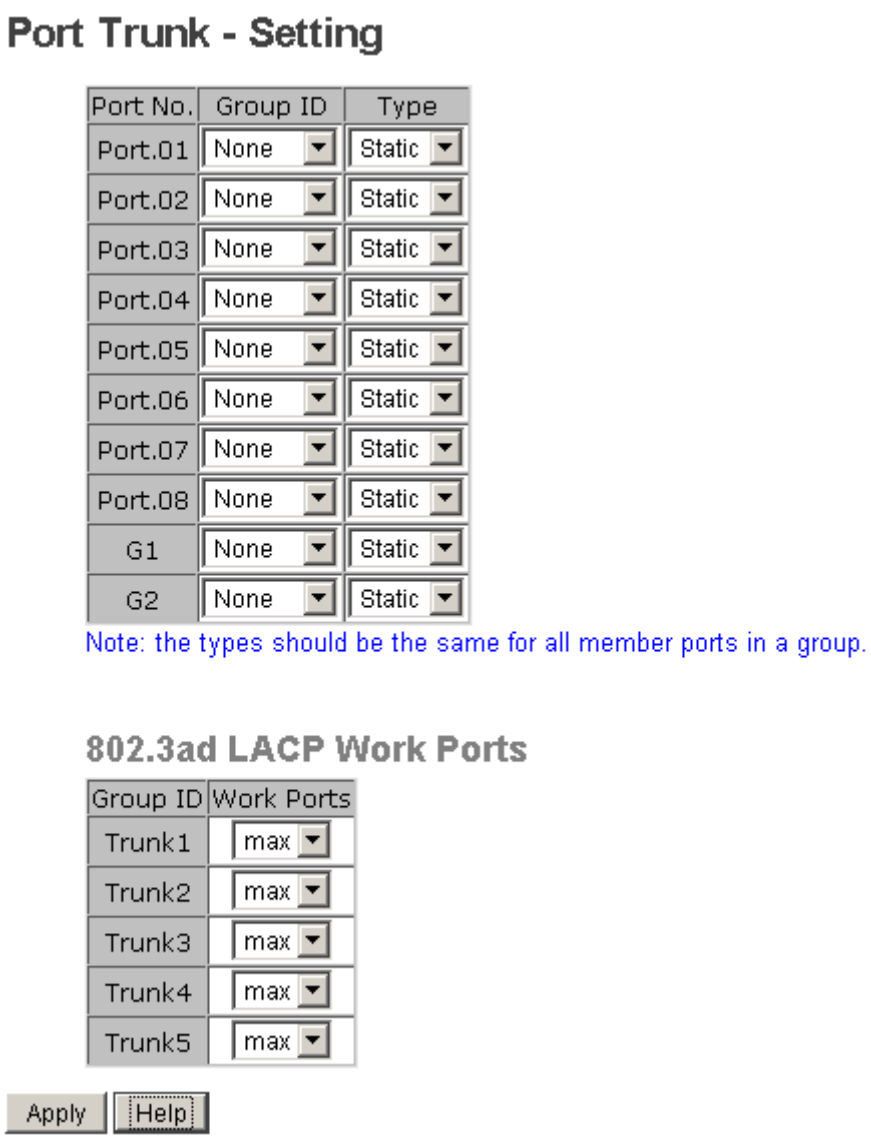
- Все порты должны работать в режиме полного дуплекса.
- Все порты должны работать на одной и той же скорости.
- Все порты должны быть портами доступа, они должны принадлежать одному и тому же VLAN, либо все должны быть магистральными (тегированными) портами.

Агрегация порта тесно связана с аппаратными средствами коммутатора. Коммутатор допускает агрегацию физических портов любых двух коммутаторов, максимально поддерживается 5 групп портов по 4 порта в каждой группе.

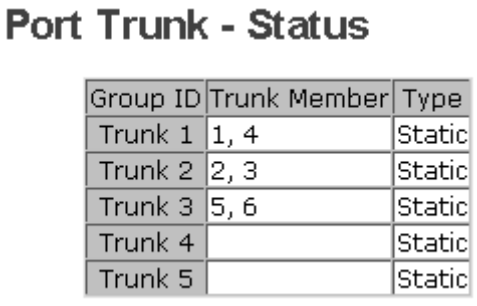
2.7.4.1 Настройка агрегации каналов [Port Trunk - Setting]

Описание параметров

Параметр	Описание
Group ID	Номер транка (группы) к которому будет принадлежать данный порт.
Type	Выбираете тип агрегации каналов или статический (static) или с помощью протокола LACP (IEEE 802.3ad)
Work ports	Установка количества портов в одном транке (группе)
Apply	Нажмите “**Apply**” чтобы применить новую конфигурацию .



2.7.4.2 Агрегация каналов – состояние [Port Trunk - Status]



На этой странице отображается состояние агрегации каналов.

Описание параметров

Параметр	Описание параметра
Group ID	Номер транка (группы)
Trunk Member	Номера портов, которые принадлежат транку
Type	Тип транка. Статический или LACP

2.8 Резервирование [Redundancy]

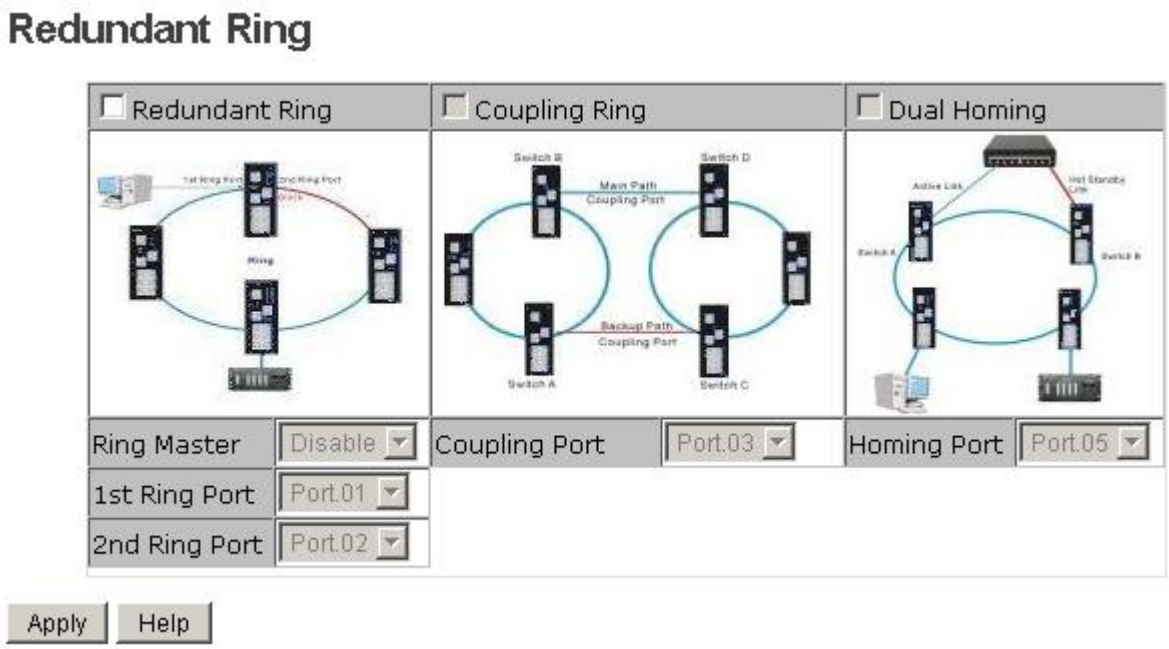
Для обеспечения защиты каналов связи от единичного отказа необходимо их резервировать. Резервирование неизбежно ведет к возникновению кольцевых участков сети - замкнутых маршрутов. Стандарт Ethernet, предусматривает только древовидную топологию и не допускает кольцевых, так как это приводит к зацикливанию пакетов.

Современные коммутаторы, как правило, поддерживают дополнительный протокол Spanning Tree Protocol (STP, IEEE 802.1d), который позволяет создавать кольцевые маршруты в сетях Ethernet. Постоянно анализируя конфигурацию сети, STP автоматически выстраивает древовидную топологию, переводя избыточные коммуникационные линии в резерв. В случае нарушения целостности построенной таким образом сети (обрыв связи, например), STP в считанные секунды включает в работу необходимые резервные линии, восстанавливая древовидную структуры сети. Этот протокол не требует первичной настройки и работает автоматически.

Более мощная разновидность данного протокола - Rapid Spanning Tree Protocol (RSTP, IEEE 802.1w), позволяющая снизить время перестройки сети до нескольких миллисекунд. Протоколы STP и RSTP позволяют создавать произвольное количество избыточных линий связи и являются обязательным функционалом для промышленных коммутаторов, применяемых в резервированных сетях.

Для некоторых промышленных приложения время перестройки топологии сети стандартных протоколов слишком велико. Поэтому был разработан фирменный протокол резервирования Redundant Ring**.** Время перестройки до 150мс при 250 устройств в цепи.

2.8.1 Протокол резервирования Redundant Ring



Данная технология позволяет объединить коммутаторы по схемам: кольцо [Redundant Ring], объединение колец [Coupling Ring] и двойное подключение [Dual Homing].

Самая простая и наиболее используемая топология – кольцо. Все коммутаторы объединяются в кольцо, в котором один коммутатор назначается менеджером кольца [Ring Master]. Задача менеджера – блокирование передачи данных по одному из направлений и постоянная рассылка тестовых пакетов для проверки целостности кольца. Блокировка замыкающей линии связи позволяет избежать возникновения коллизии, описанной в стандартном протоколе IEEE 802.3 Ethernet. При этом данные продолжают свободно проходить между узлами логически по линейной топологии. Менеджер кольца рассылает специальные тестовые пакеты в обоих направлениях и ждет их возвращения по кругу. По их потере менеджер определяет разрыв кольца и активизирует заблокированную линию для передачи данных. Таким образом, при возникновении неполадок в любом месте кольца оно становится линейной структурой.

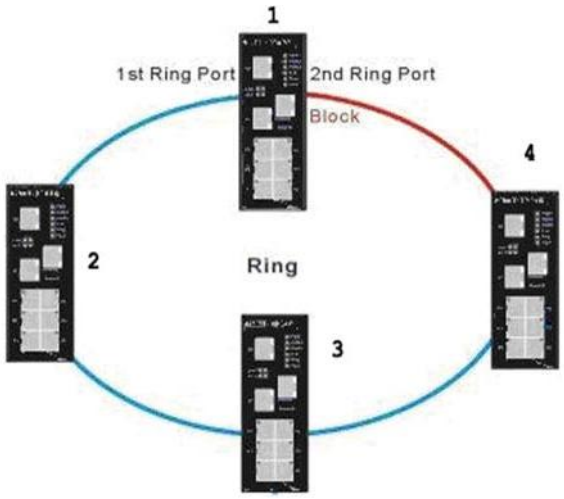
Замечание: Перед тем как включать коммутаторы в кольцо, необходимо настроить на них протокол резервирования, дабы избежать физических петлей.

Описание параметров

Параметр	Описание
Redundant Ring	Отметьте для активации функции резервирования. У **всех** коммутаторов в кольце **должна** быть включена эта функция
Ring Master	Выберите **Enable** чтобы сделать коммутатор менеджером кольца. Только один коммутатор может быть менеджером. Если у двух и более коммутаторов активирована эта функция, то менеджером кольца

	становиться коммутатор, который имеет наименьший MAC адрес. Остальные становятся резервными менеджерами кольца.
1st Ring Port	Если коммутатор менеджер кольца, то это основной [primary] порт (порт к которому присоединен основной неблокируемый линк). Если это простой член кольца, то это порт который присоединен к кольцу.
2nd Ring Port	Если коммутатор менеджер кольца, то это резервный [backup] порт (порт к которому присоединен блокируемый линк) Если это простой член кольца, то это порт который присоединен к кольцу.

Пример построения кольца:



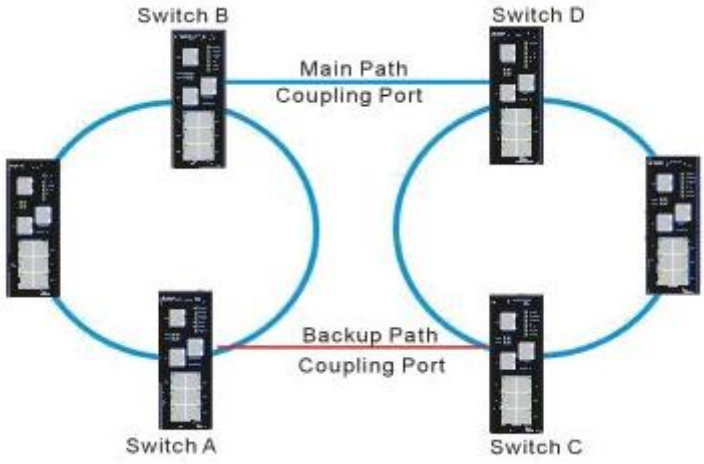
Пусть кольцо состоит из четырех коммутаторов. Коммутатор 1 является менеджером кольца. В настройках 1 коммутатора включаем [Redundant Ring], затем [Ring Master]. Выбираем порты, которые будут включены в кольцо и указываем их в строках **1st Ring Port и 2nd Ring Port. 2nd Ring Port** это порт, к которому будет подключен логически блокируемый линк. На 2, 3, и 4 коммутаторах включаем [Redundant Ring] и в строках **1st Ring Port и 2nd Ring Port. 2nd Ring Port** указываем порты**,** которыми они будут подключатся в кольцо. После этого подсоединяем линки. Если все настроено корректно, то на менеджере кольца будет постоянно гореть сведодиоды R.M и Ring, а на остальных коммутаторах будет постоянно гореть светодиод Ring.

Замечание: подсоединяйте линки кольца только к тем портам, которые указаны в строках 1st Ring Port и 2nd Ring Port. 2nd Ring Port, иначе кольцо не будет работать.

Coupling Ring – дублированное соединение колец.

В некоторых системах бывает неудобно соединять все устройства в одно большое резервированное кольцо в силу того, что некоторые устройства расположены достаточно далеко друг от друга. Топология Coupling Ring дает возможность разделить устройства распределенной системы на небольшие группы и создать небольшие резервированные кольца, соединенные друг с другом.

Принцип действия Coupling Ring: из двух линий связи соединяющих два кольца активной остается только одна. Резервная линия [Backup Path] активизируется во время сбоя основной линии [Main Path].



В организации Coupling Ring участвуют всегда 4 коммутатора. Два из одного кольца и два из другого. Если в одном кольце функция Coupling Ring будет включена более чем у двух коммутаторов, то Coupling Ring работать не будет. Также не рекомендуется включать функцию Coupling Ring в коммутаторе, который является менеджером кольца, так как это вызовет очень большую нагрузку на коммутатор.

Для того чтобы включить Coupling Ring в коммутаторе, необходимо отметить **[Coupling Ring].** Затем необходимо выбрать порт, который будет соединять два кольца, и отметить его в строке **[Coupling Port].** Все это проделать у оставшихся трех коммутаторов. Смотрите рисунок. Основная и резервная линия определятся автоматически. Коммутатор, у которого будет наименьший MAC адрес, организует резервную линию [backup path]

Dual Homing – двойное подключение. С помощью этой функции, возможно подключить кольцо к обычному коммутатору с помощью двух линков RSTP. Только два коммутатора в кольце могут поддерживать функцию Dual Homing. Для включения этой функции необходимо отметить Dual Homing в выбранных коммутаторах, а так же выбрать в этих коммутаторах порты, которыми они будут соединятся с обычным коммутатором [Homing Port].

Замечание: в коммутаторе одновременно могут работать только два вида протоколов резервирования. Либо RSTP либо Redundant Ring.

2.8.2 RSTP

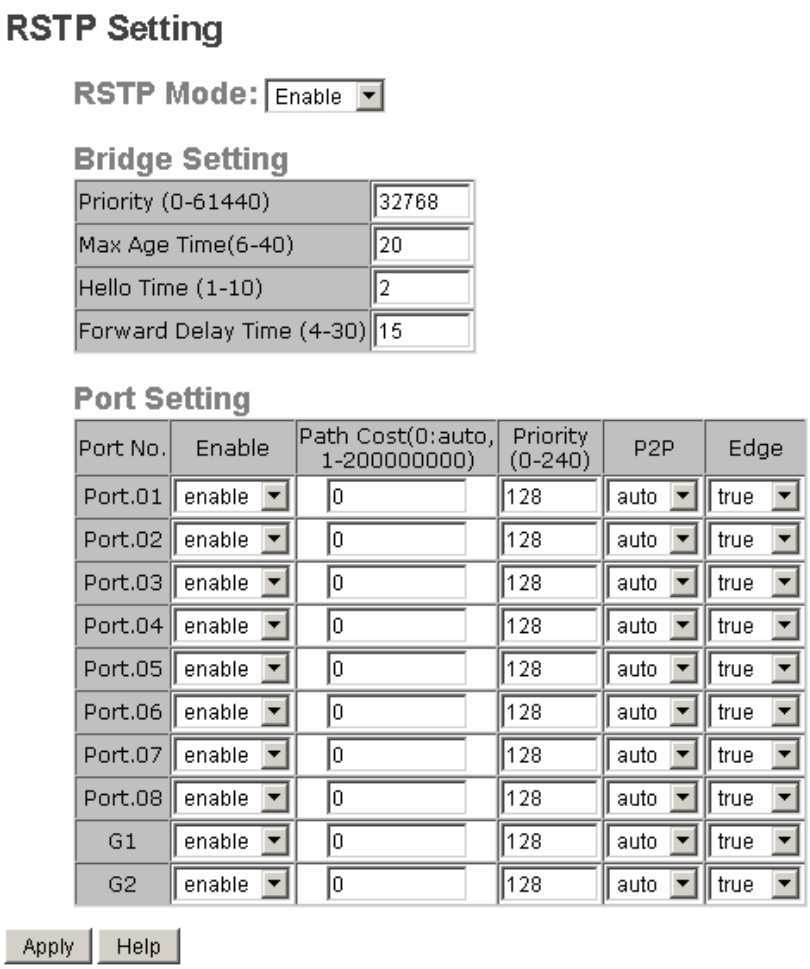
RSTP (*Rapid STP*, англ. *Rapid spanning tree protocol, быстрый протокол разворачивающегося дерева*), он же IEEE 802.1W - ускоренная версия протокола STP, использующегося для исключения петель (исключения дублирующих маршрутов) в соединениях коммутаторов Ethernet с дублирующими линиями.

По сравнению с STP уменьшилось время построения топологии, исключена поддержка разделяемой среды передачи данных (коаксиального кабеля).

Принцип работы в общих чертах похож на STP: выбирается корневой коммутатор (англ. *root switch*), к которому, каждый из участвующих в построении дерева коммутатор, ищет кратчайший маршрут (с учётом пропускной способности канала) через соседние коммутаторы (или напрямую). Линии, не попавшие в маршрут, переводятся в режим ожидания и не используются для передачи данных. пока работают основные линии. В случае выхода из строя основных линий, ожидающие линии используются для построения альтернативной топологии, после чего одна из линий становится активной, а остальные продолжают находиться в режиме ожидания.

Протоколы RSTP и STP обратно совместимы.

2.8.2.1 Настройка RSTP [RSTP Setting]



Описание параметров

Параметр	Описание
RSTP mode	необходимо активировать протокол RSTP [Enable] прежде чем настраивать параметры RSTP.
Priority (0-61440)	Приоритет коммутатора (Bridge Priority). Устанавливается с шагом 4096. Коммутатор с меньшей величиной имеет более высокий приоритет. После того, как вы поменяли приоритет, необходимо перезагрузить коммутатор. Параметр влияет на выбор корневого коммутатора (root bridge) и на его идентификатор (ID Bridge).
Max Age (6-40)	Количество секунд ожидания приема RSTP сообщения об конфигурации, после этого коммутатор сам высылает сообщение о реконфигурации.
Hello Time (1-10)	Период рассылки BPDU сообщений (по умолчанию 2 секунды)
Forwarding Delay Time (4-30)	Задержка перехода состояний портов Из состояния прослушивания (Listening) и обучения (Learning) в состояние пердача (Forwarding). (по умолчанию 15 секунд.)
Path Cost (1-200000000)	Стоимость пути к другому коммутатору, который присоединен к этому порту.
Priority (0-240)	Цена порта. Параметр влияет, какой порт будет заблоктрован в сети. Шаг - 16

Admin P2P	Некоторые сообщения протокола RSTP зависят от того, что соединен ли соответствующий порт только с одним коммутатором (соединение точка-точка P2P) или он может быть соединен с 2 ти более коммутаторами (разделяемая среда передачи). Этот параметр позволяет вручную настраивать соединение. True – соединение P2P. False – соединение не P2P.
Admin Edge	Эту опцию можно включить, если интерфейс подсоединен к оконечному сегменту локальной сети LAN или к конечному узлу. Так как конечные узлы не могут вызвать зацикливания перенаправления, они могут напрямую переходить к STP состоянию передачи пакетов. Указание конечных портов обеспечивает более быстрое взаимодействие таких устройств, как рабочие станции и серверы; сохраняет текущие базы данных пересылок, что снижает объем пересылки пакетов, необходимых для перестройки адресных таблиц во время перенастройки структуры; не вынуждает протокол STP инициировать перенастройку сети, когда интерфейс меняет состояние; а также преодолевает другие проблемы тайм-аута, связанные с настройкой протокола STP. Тем не менее, следует помнить, что конечный порт может быть включен только для портов, подсоединенных к конечным узлам локальной сети. Для того, чтобы сконфигурировать порт как edge port выберите True.

2.9 VLAN

Виртуальной сетью VLAN (Virtual LAN) называют группу узлов сети, образующих домен широковещательного трафика (Broadcast Domain).

При создании локальной сети на основе коммутатора, несмотря на возможность использования пользовательских фильтров по ограничению трафика, все узлы сети представляют собой единый широковещательный домен, то есть широковещательный трафик передается всем узлам сети. Таким образом, коммутатор изначально не ограничивает широковещательный трафик, а сами сети, построенные по указанному принципу, именуются плоскими.

Виртуальные сети образуют группу узлов сети, в которой весь трафик, включая и широковещательный, полностью изолирован на канальном уровне от других узлов сети. Это означает, что передача кадров между узлами сети, относящимися к различным виртуальным сетям, на основании адреса канального уровня невозможна (хотя виртуальные сети могут взаимодействовать друг с другом на сетевом уровне с использованием маршрутизаторов).

Изолирование отдельных узлов сети на канальном уровне с использованием технологии виртуальных сетей позволяет решать одновременно несколько задач. Во-первых, виртуальные сети способствуют повышению производительности сети, локализуя широковещательный трафик в пределах виртуальной сети и создавая барьер на пути широковещательного шторма. Коммутаторы пересылают широковещательные пакеты (а также пакеты с групповыми и неизвестными адресами) внутри виртуальной сети, но не между виртуальными сетями. Во-вторых, изоляция виртуальных сетей друг от друга на канальном уровне позволяет повысить безопасность сети, делая часть ресурсов для определенных категорий пользователей недоступной

До появления общепризнанного стандарта по организации виртуальных сетей IEEE 802.1Q каждый производитель сетевого оборудования использовал собственную технологию организации VLAN. Такой подход имел существенный недостаток - технологии одного производителя были несовместимы с технологиями других фирм. Поэтому при построении виртуальных сетей на базе нескольких коммутаторов необходимо было использовать только оборудование от одного производителя. Принятие стандарта виртуальных сетей IEEE 802.1Q позволило преодолеть проблему несовместимости, однако до сих пор существуют коммутаторы, которые либо не поддерживают стандарт IEEE 802.1Q, либо, кроме возможности организации виртуальных сетей по стандарту IEEE 802.1Q, предусматривают и иные технологии.

Существует несколько способов построения виртуальных сетей, но сегодня в коммутаторах главным образом реализуется технология группировки портов или используется спецификация IEEE 802.1Q.

Виртуальные сети на основе группировки портов (Port-based) обычно реализуются в так называемых Smart-коммутаторах или в управляемых коммутаторах - как дополнение к возможности организации VLAN на базе стандарта IEEE 802.1Q.

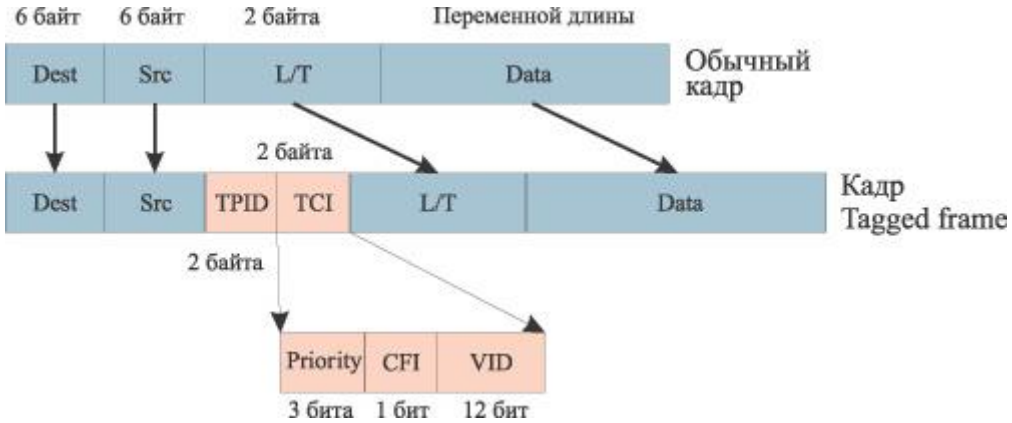
Данный способ создания виртуальных сетей достаточно прост и, как правило, не вызывает проблем. Каждый порт коммутатора приписывается к той или иной виртуальной сети, то есть порты группируются в виртуальные сети. Решение о продвижении сетевого пакета в этой сети основывается на MAC-адресе получателя и ассоциированного с ним порта. Если к порту, которому назначена принадлежность к определенной виртуальной сети, например к VLAN#1, подключить ПК пользователя, то этот ПК автоматически будет принадлежать сети VLAN#1. Если же к данному порту подключается коммутатор, то все порты этого коммутатора также будут принадлежать VLAN#1

При использовании технологии группировки портов один и тот же порт может быть одновременно приписан к нескольким виртуальным сетям, что позволяет реализовывать

разделяемые ресурсы между пользователями различных виртуальных сетей. Например, чтобы реализовать совместный доступ к сетевому принтеру или к файл-серверу пользователей виртуальных сетей VLAN#1 и VLAN#2, тот порт коммутатора, к которому подключается сетевой принтер или файл-сервер, нужно приписать одновременно к сетям VLAN#1 и VLAN#2

При наличии развитой сетевой инфраструктуры, насчитывающей множество коммутаторов, более эффективным решением создания виртуальных сетей будет технология IEEE 802.1Q. В виртуальных сетях, основанных на стандарте IEEE 802.1Q, информация о принадлежности передаваемых Ethernet-кадров к той или иной виртуальной сети встраивается в сам передаваемый кадр. Таким образом, стандарт IEEE 802.1Q определяет изменения в структуре кадра Ethernet, позволяющие передавать информацию о VLAN по сети.

К кадру Ethernet добавляется метка (Tag) длиной 4 байта — такие кадры называют кадрами с метками (Tagged frame). Дополнительные биты содержат информацию по принадлежности кадра Ethernet к виртуальной сети и о его приоритете.



Добавляемая метка кадра включает в себя двухбайтовое поле TPID (Tag Protocol Identifier) и двухбайтовое поле TCI (Tag Control Information). Поле TCI, в свою очередь, состоит из полей Priority, CFI и VID. Поле Priotity длиной 3 бита задает восемь возможных уровней приоритета кадра. Поле VID (VLAN ID) длиной 12 бит является идентификатором виртуальной сети. Эти 12 бит позволяют определить 4096 различных виртуальных сетей, однако идентификаторы 0 и 4095 зарезервированы для специального использования, поэтому всего в стандарте 802.1Q возможно определить 4094 виртуальные сети. Поле CFI (Canonical Format Indicator) длиной 1 бит зарезервировано для обозначения кадров сетей других типов (Token Ring, FDDI), передаваемых по магистрали Ethernet, и для кадров Ethernet всегда равно 0.

Порты коммутатора, поддерживающие VLAN'ы, (с некоторыми допущениями) можно разделить на два множества:

1. Тегированные порты (или транковые порты, *trunk-порты*).
2. Нетегированные порты (или порты доступа, *access-порты*);

Тегированные порты нужны для того, чтобы через один порт была возможность передать несколько VLAN'ов и, соответственно, получать трафик нескольких VLAN'ов на один порт. Информация о принадлежности трафика VLAN'у, как было сказано выше, указывается в специальном теге. Без тега коммутатор не сможет различить трафик различных VLAN'ов.

Если порт нетегированный в каком-то VLAN'е, то трафик этого VLAN передается без тега. Нетегированным порт может быть только в одном VLAN.

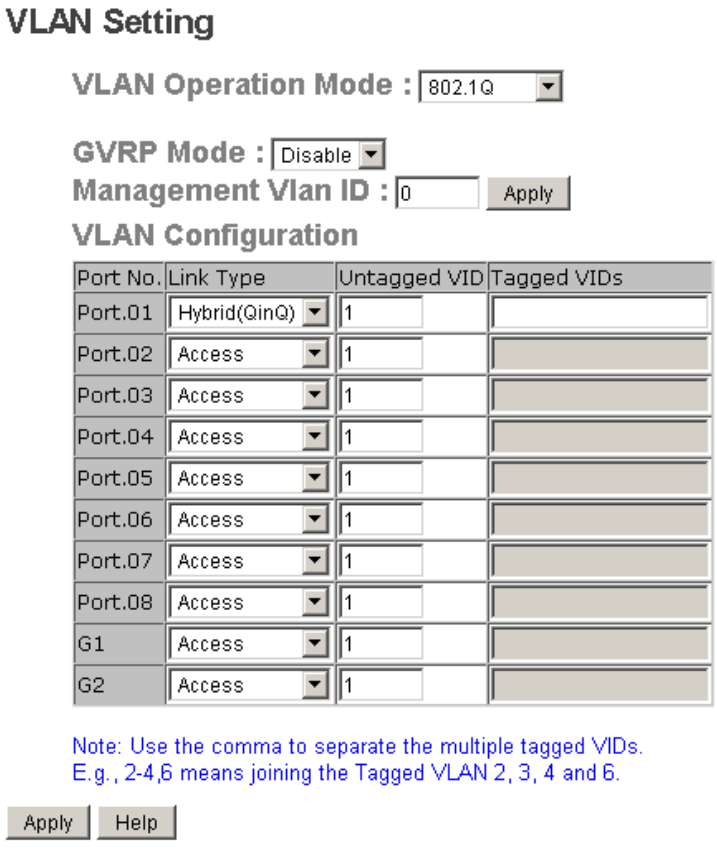
Обычно, по умолчанию все порты коммутатора считаются нетегированными членами VLAN#1. В процессе настройки или работы коммутатора они могут перемещаться в другие VLAN'ы.

Рассмотренные примеры виртуальных сетей относились к так называемым статическим виртуальным сетям (Static VLAN), в которых все порты настраиваются вручную, что хотя и весьма наглядно, но при развитой сетевой инфраструктуре является довольно рутинным делом. Кроме того, при каждом перемещении пользователей в пределах сети приходится производить перенастройку сети с целью сохранения их членства в заданных виртуальных сетях, а это, конечно, крайне нежелательно.

Существует и альтернативный способ конфигурирования виртуальных сетей, а создаваемые при этом сети называются динамическими виртуальными сетями (Dynamic VLAN). В таких сетях пользователи могут автоматически регистрироваться в сети VLAN, для чего служит специальный протокол регистрации GVRP (GARP VLAN Registration Protocol). Этот протокол определяет способ, посредством которого коммутаторы обмениваются информацией о сети VLAN, чтобы автоматически зарегистрировать членов VLAN на портах во всей сети.

Все коммутаторы, поддерживающие функцию GVRP, могут динамически получать от других коммутаторов (и, следовательно, передавать другим коммутаторам) информацию VLAN о регистрации, включающую данные об элементах текущей VLAN, о порте, через который можно осуществлять доступ к элементам VLAN и т.д. Для связи одного коммутатора с другим в протоколе GVRP используется сообщения GVRP BPDU (GVRP Bridge Protocol Data Units). Любое устройство с поддержкой протокола GVPR, получающее такое сообщение, может динамически подсоединяться к той сети VLAN, о которой оно оповещено.

2.9.1 Настройка VLAN [VLAN Setting]



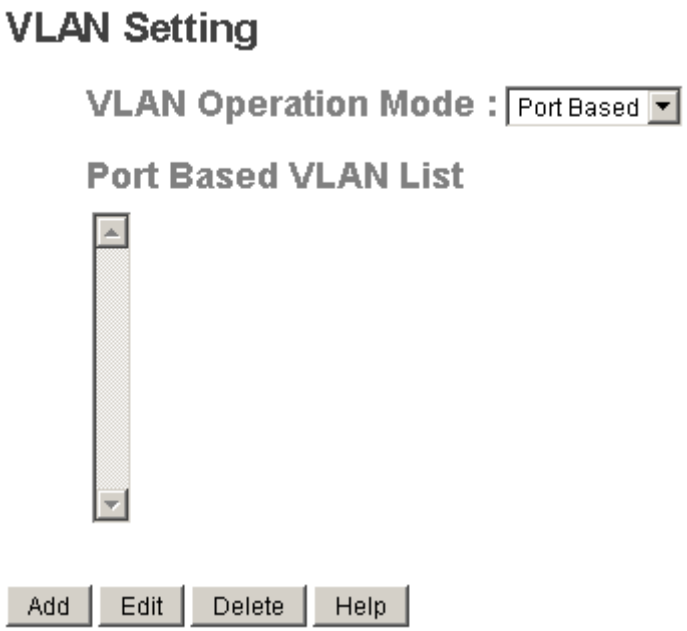
По умолчанию все порты коммутатора находятся в VLAN#1 (Default VLAN). Default VLAN удалить нельзя.

Описание параметров

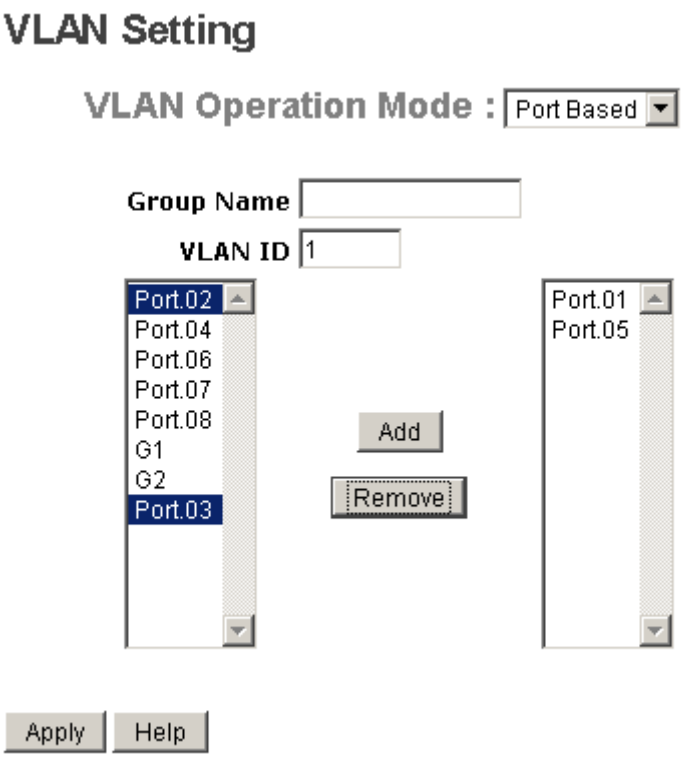
Параметр	Описание
VLAN Operation Mode	Указываете режим работы VLAN. Disable – выключить, 802.1Q – режим работы по протоколу IEEE 802.1, Port Based – VLAN на основе портов.
GVRP Mode	Enable/Disable включить/выключить функцию GVRP.
Management VLAN ID	Назначить VLAN для управления коммутатором. Прежде чем назначит этот VLAN необходимо присвоить ему какой-нибудь порт, иначе вы не сможете управлять коммутатором. Диапазон (1-4094)
Link Type	Существует 4 типа линков: **Access Link** – нетегированный линк. Позволяет объединять порты в один VLAN. Один Access Link может быть только в одном VLAN. **1QTrunk** – тегированный линк. Позволяет установить порт в 1, 2 и больше VLAN'ов. Трафик из такого порта выходит тегированный. **Hybrid** – позволяет порту находится в одном нетегированном VLAN и в нескольких тегированных. **QinQ** – инкапсуляция пользовательского VLAN в магистральный VLAN
Untagged VID	VLAN ID для нетегированного трафика. Например: номер VLAN для Access потров Диапазон (1-4094)
Tagged VIDs	Номера VLAN для тегированного трафика. Например для транковых портов. Разделение разных VID через запятую. Например: 5,6,7. или 2,5-7 это значит 2,5,6,7. Если порты имеют одинаковый VID, то это значит что они находятся в одном VLAN

Настройка Port Based VLAN

Выберите в строке **VLAN Operation Mode** тип VLAN **Port Based.** Откроется страница настройки



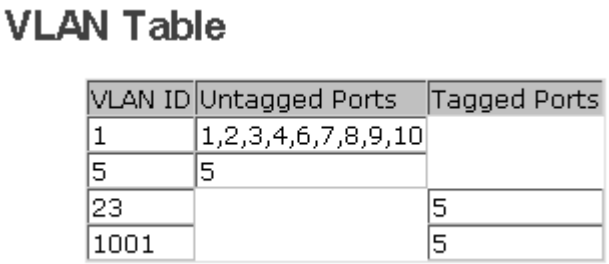
Нажмите кнопку **Add.** Откроется страница конфигурации портов



В строке **Group Name** указывается название Vlan. В строке **VLAN ID** соответственно указывается ID нового VLAN (1-4094). В левом столбце выбираем порты, которые будут участвовать в новом VLAN, затем нажимаем кнопку **Add** и выбранные порты перемещаются в левый столбец – они принадлежат новой VLAN. Нажимаем кнопку **Apply,** чтобы применить конфигурацию.

После того как вы выбрали Port Based VLAN обычные 802.1Q VLAN работать не будут. Трафик будет передаваться только в пределах одной Vlan ID. Все не выбранные порты будут находиться в Default VLAN#1.

2.9.2 Отображение VLAN [VLAN Table]



На этой странице отображается существующие VLAN и порты, которые принадлежат им.

2.10 SNMP

Протокол SNMP (Simple Network Management Protocol) является простым протоколом управления сетью, он широко используется для управления компьютерными сетями. SNMP - это развивающийся протокол.

Первой версией SNMP была версия SNMP v1 [RFC1157], она нашла применение у множества производителей, выбравших этот протокол из-за его простоты и легкости реализации. SNMP v2c - улучшенная версия SNMP v1, она поддерживает управление сетью на разных уровнях; в версии SNMP v3 улучшена безопасность за счет добавления режима USM (User-based Security Mode) и модели управления доступом VACM (View-based Access Control Model).

Протокол SNMP обеспечивает простой способ обмена сетевой управляющей информацией между двумя точками сети. При SNMP применяется механизм опроса очереди сообщений и передача сообщений по протоколу UDP (протокол транспортного уровня, не требующий установления соединения). Поэтому он хорошо поддерживается существующими компьютерными сетями.

При протоколе SNMP применяется режим станции-агента. В этой структуре имеется две части: NMS (Network Management Station - Станция управления сетью) и Агент. NMS - это рабочая станция, на которой функционирует программа-клиент SNMP. Для управления сетью она является ядром. Агент - это серверное программное обеспечение, функционирующее на устройствах, которыми требуется управлять. NMS управляет всеми объектами управления через Агентов. Коммутатор поддерживает функции Агента.

Связь между NMS и Агентом осуществляется в режиме Клиент/Сервер путем обмена стандартными сообщениями. NMS посылает запрос, а Агент отвечает на него. Существует семь типов сообщений SNMP:

- Get-Request
- Get-Response
- Get-Next-Request
- Get-Bulk-Request
- Set-Request
- Trap
- Inform-Request

NMS посылает запросы Агенту при помощи сообщений Get-Request, Get-Next-Request, Get-Bulk-Request и Set-Request. Агент, приняв эти запросы отвечает на них сообщением Get-Response. В некоторых специальных ситуациях, например, когда порты сетевых устройств находятся в состоянии включения или выключения (Up/Down), либо при изменении топологии сети, Агенты могут посылать на NMS сообщения Trap, чтобы информировать ее о нештатных событиях. Кроме того, на NMS может быть задан режим оповещения о нештатных событиях путем включения функции RMON. При наступлении нештатного события Агенты будут посылать сообщения Trap, либо создавать отчет о событии (в зависимости от настроек). Для связи между NMS при многоуровневом управлении сетью в основном используются сообщения Inform-Request.

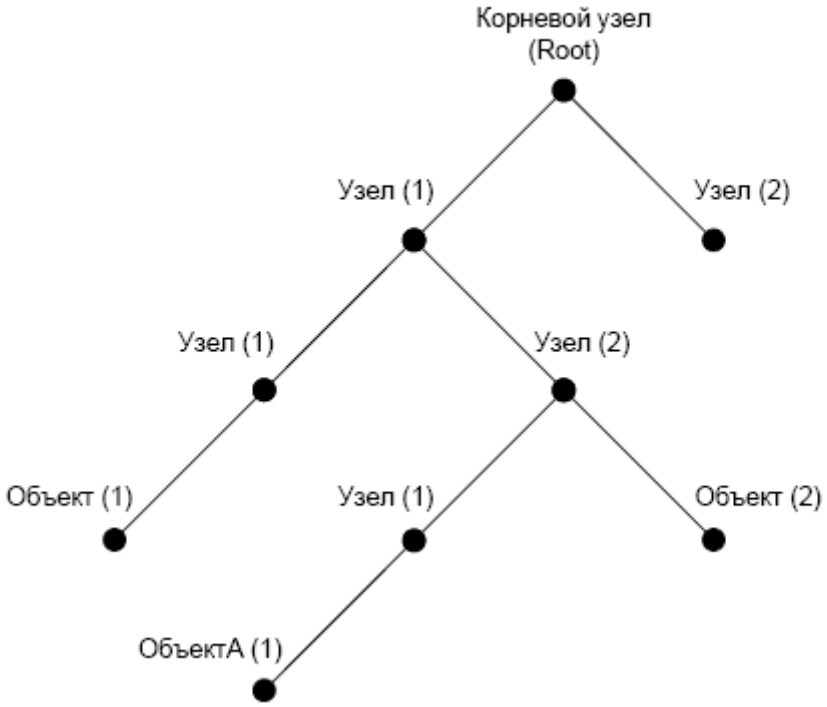
Режим USM гарантирует безопасную передачу за счет применения эффективного алгоритма шифрования и аутентификации. В режиме USM осуществляется шифрование сообщений в соответствии с паролем, введенным пользователем. Этот механизм гарантирует невозможность просмотра сообщения в процессе передачи. Аутентификация в режиме USM гарантирует невозможность изменения сообщения в процессе передачи. В

режиме USM применяется криптозащита DES-CBC. При аутентификации используются алгоритмы шифрования HMAC-MD5 и HMAC-SHA.

Для классификации прав доступа пользователей используется модель VACM. В соответствии с этой моделью пользователи с одинаковыми правами доступа объединяются в одну группу. Пользователи не могут выполнять операции, которые им не разрешены.

Начальные сведения о MIB

Информация управления сетью, становящаяся доступной от NMS структурируется и организуется в базе данных управляющей информации (MIB - Management Information Base). В MIB определена информация, которая может быть доступна протоколам управления сетью. Информация классифицирована по уровням и структурам. Предопределенная управляющая информация может быть получена из мониторинга сетевых устройств. В стандарте ISO ASN.1 (Abstract Syntax Notation One) для MIB определена древовидная структура. Каждая MIB организует всю доступную информацию в этой древовидной структуре. Каждый узел дерева имеет OID (Object Identifier - идентификатор объекта) и краткое описание узла. OID представляет собой набор целых чисел, разделенных точками. Он определяет узел и может использоваться для поиска узла в древовидной структуре MIB



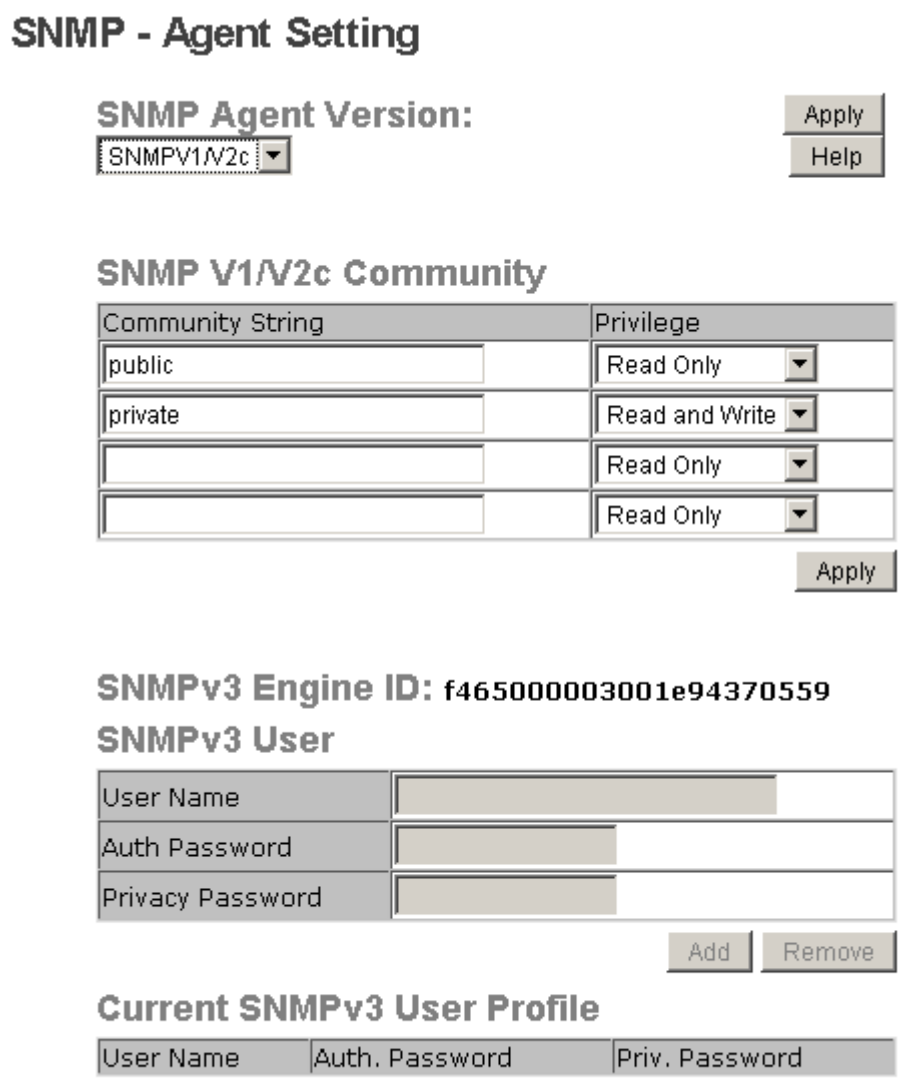
На этом рисунке OID объекта A является 1.2.1.1. NMS может отыскать этот объект по его уникальному OID и получить стандартные переменные объекта. MIB определяет набор стандартных переменных для контролируемых сетевых устройств следуя этой структуре.

Если необходим просмотр информации переменных Агента MIB, в NMS должно функционировать программное обеспечение просмотра MIB. MIB в Агенте обычно состоит из общедоступной MIB и частной MIB. Общедоступная MIB обычно содержит общедоступную управляющую информацию сети, доступную всем NMS. Частная MIB содержит специальную информацию, которая может просматриваться и контролироваться изготовителями.

MIB-I [RFC1156] была первой реализацией общедоступной MIB протокола SNMP, впоследствии она была заменена на MIB-II [RFC1213]. MIB-II является расширением MIB-I, поддерживает OID дерева MIB в MIB-I. MIB-II поддерживает суб-деревья, называемые группами. Объекты в этих группах охватывают все области функционала сетевого управления. NMS получает управляющую информацию сети, посещая MIB Агента SNMP.

Коммутатор может функционировать, как Агент SNMP и поддерживать как SNMP v1/v2c, так и SNMP v3.

2.10.1 Настройка SNMP агента [SNMP – Agent Setting]



Описание параметров

Параметр	Описание параметра
SNMP Agent Version	Коммутатор поддерживает 3 версии протокола SNMP. SNMPV1/V2 используют для аунтентификации доступа к объектам название сообщества (Community). По умолчанию записаны два Community – public и private. Public – только для чтения. Private – для чтения и записи. SNMPV3 использует для аунтентификации, чтения и записи алгоритмы MD5 и DES.
SNMP V1/V2	Указываете название сообщества (Community) 32 знака и их

Community	права (чтение и запись). Если не хотите добавлять сообщества, то оставляете строки пустыми
SNMPV3 User	Если вы выбрали SNMPV, то вам необходимо установить профиль пользователя SNMP (SNMP User). Может быть 8 разных профилей в коммутаторе. Для того чтобы создать профиль необходимо установить: Имя пользователя [User Name] – 16 знаков Пароль [Auth Password] – 16 знаков. Персональный пароль [Privacy Password] – 16 знаков (может отличатся от Auth Password)
Current SNMPv3 User Profile	Показывает все существующие профили пользователей
Apply	Нажмите кнопку **Apply,** чтобы применить новую конфигурацию

2.10.2 Настройка сообщений Trap [Trap Setting]

Менеджер системных сообщений [Trup Server] – это сервер, который получает системные сообщения и предупреждения сгенерированные коммутатором. Если в коммутаторе не задан Trup Server, то никаких системных сообщений передаваться не будет. Для того чтобы задать Trup Server на коммутаторе, необходимо задать IP адрес и Community сервера, а также версию SNMP протокола.

Системные сообщения: пропадание питания, отключение порта и т.п.

Описание параметров.

Параметр	Описание
Server IP	IP адрес Trup Server, который принимает системные сообщения
Community	Community для аунтентификации
Trap Version	Версия протокола SNMP
Add	Добавить профиль.
Remove	Удалить профиль.

2.11 Приоритизация трафика [Traffic Prioritization]

Некоторые виды трафика важно передавать по сети без задержек, например, видео в реальном времени при проведении видеоконференций или трафик IP-телефонии. Для того, чтобы обеспечить необходимое качество обслуживания такого трафика (Quality of Service - QoS), коммутаторы SWI/C000 поддерживают технологию приоритизации трафика.

Анализируя содержимое заголовка кадра Ethernet или IP-пакета, коммутатор получает информацию о необходимом для данного приложения классе обслуживания (Class of Service – CoS) и помещает данные в соответствующую очередь выходного порта. Таких очередей 4. Каждая выходная очередь имеет свой приоритет обслуживания. Очередь с наивысшим приоритетом обслуживается первой, с низшим приоритетом – последней.

Физическое устройство классического коммутатора можно упрощенно представить следующим образом: пакет приходит на входной порт, обрабатывается механизмом коммутации, который решает, куда направить пакет, и попадает в аппаратные очереди выходного порта. Аппаратные очереди представляет собой быструю память, хранящую пакеты перед тем, как они попадут непосредственно на выходной порт. Далее, согласно определенному механизму обработки, пакеты извлекаются из очередей и покидают коммутатор. Изначально очереди равноправны и именно механизм обработки очередей (Scheduling) определяет приоритизацию. Обычно каждый порт коммутатора содержит ограниченное число очередей: 2, 4 и так далее .

В общих чертах настройка приоритизации заключается в следующем:

1. Изначально очереди равноправны. Поэтому предварительно необходимо их настроить, то есть определить очередность (или пропорциональность объема) их обработки. Чаще всего это делается привязкой приоритетов 802.1P к очередям.

2. Необходимо сконфигурировать обработчик очередей (Scheduler). Чаще всего используются взвешенный циклический алгоритм (Weighted Round Robin WRR) или строгая очередь приоритетов (Strict Priority Queuing).

3. Назначение приоритета поступающим пакетам: по входному порту, по CoS или, в случае дополнительных возможностей (Layer 3 switch), по каким-то полям IP.

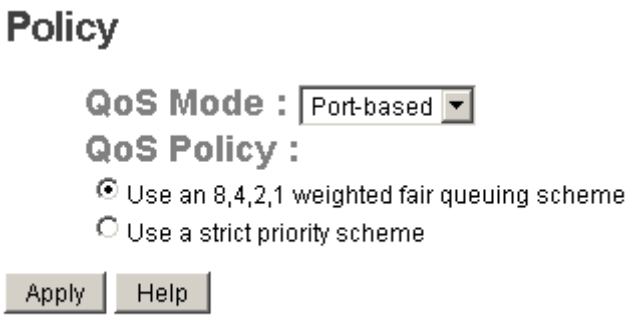
Работает все это следующим образом:

1. Пакет попадает в коммутатор. Если это обычный Ethernet пакет (клиентский Access Port), то он не имеет меток приоритета и таковая может выставляться коммутатором, например, по номеру входного порта, если это нужно. Если входной порт транковый (802.1Q), то пакет может нести метку приоритета и коммутатор может ее принять или заменить на необходимую. В любом случае пакет на данном этапе попал в коммутатор и имеет необходимую разметку COS.

2. После обработки процессом коммутации пакет в соответствии с меткой приоритета CoS направляется классификатором (Classify) в соответствующую очередь выходного порта. Например, критический трафик попадает в высокоприоритетную, а менее важный в низкоприоритетную очереди.

3. Механизм обработки (Scheduling) извлекает пакеты из очередей согласно их приоритетам. Из высокоприоритетной очереди за единицу времени будет выдано на выходной порт больше пакетов, чем из низкоприоритетной.

Приоритизация трафика включает в себя 3 вида – на основе портов [Port Based], 802.1p/COS (Clacc of Service описывается в IEEE 802.1p. приоритет определяется на канальном уровне), TOS/DSCP (Type of Service. Приоритет определяется на сетевом уровне).



В строке [QoS Mode] устанавливается, какой вид приоритизации трафика вы будете использовать.

Port Based – приоритет трафика определяется портом.

COS only - приоритет трафика определяется COS

TOS only - приоритет трафика определяется TOS

COS first – приоритет трафика определяется COS и TOS, но COS разделяет трафик первым.

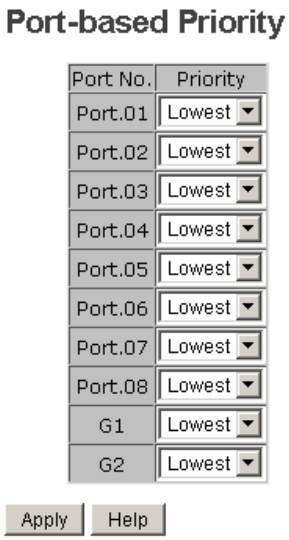
TOS first - приоритет трафика определяется COS и TOS, но TOS разделяет трафик первым.

QoS Policy

Use an 8,4,2,1 weighted fair queuing scheme – пакеты с разным приоритетом обрабатываюся коммутатором в соотношении 8:4:2:1. Например: коммутатор в одну еденицу времени будет обрабатывать 8 пакетов с высоким приоритетом (High), 4 пакета со средним приоритетом (Middle), 2 пакета с низким приоритетом (Low) и 1 пакет с низшим приоритетом (Lowest).

Use a strict priority scheme – пакеты с более высоким приоритетом будут передаваться первыми, до тех пор пока очередь высокоприоритетных пакетов не станет пустой (строгая очередь приоритетов).

2.11.1 Приоритизация трафика на основе портов [Port-based Priority]

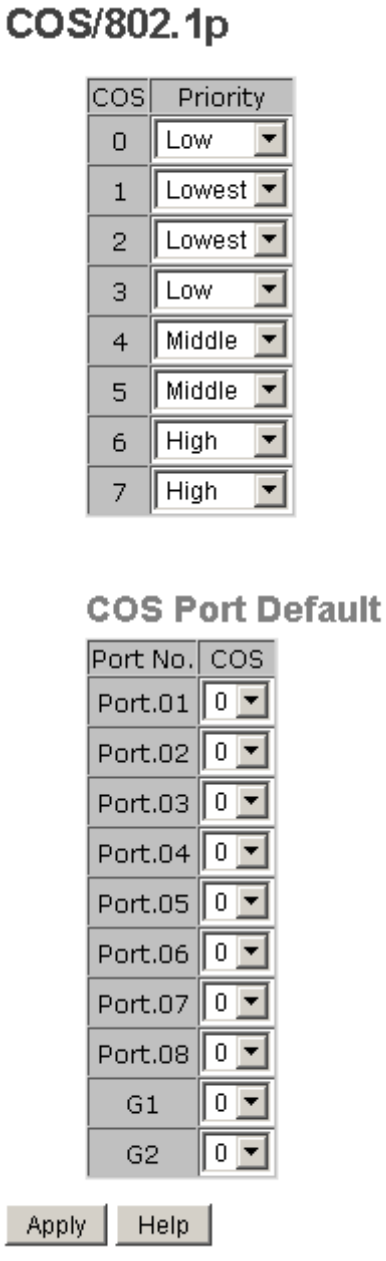


Каждому порту коммутатора назначается одна из 4 очередей приоритета: высокая (High), средняя (Middle), низкая (Low) и наименьшая (Lowest).

2.11.2 COS/802.1p

Коммутаторы Ethernet (Layer 2) используют протоколы канального уровня. Протокол Ethernet в чистом виде не поддерживает поле приоритета. Поэтому на Ethernet портах (Access Port) возможна лишь внутренняя (по отношению к коммутатору) классификация по номеру входящего порта и отсутствует какая-либо маркировка.

Более гибким решением является использование стандарта IEEE 802.1P, который разрабатывался совместно с 802.1Q. Иерархия отношений здесь следующая: 802.1D описывает технологию мостов и является базовой для 802.1Q и 802.1P. 802.1Q описывает технологию виртуальных сетей (VLAN), а 802.1P обеспечение качества обслуживания. В целом, включение поддержки 802.1Q (транк с виланами), автоматически дает возможность использования 802.1P (см главу 2.9 VLAN). Согласно стандарту используются 3 бита в заголовке второго уровня, которые называются Class of Service (COS). Таким образом, COS может принимать значения от 0 до 7.



Описание параметров

Параметр	Описание
COS/802.1p	COS (Class Of Service) или 802.1P. Приоритет определяется 3 битам в заголовке приоритет поля Tag 802.1Q. COS принимает значения от 0 до 7. Необходимо каждому значениюCOS выставить соответствие 4 очередей приоритета: High, Middle, Low, and Lowest.
COS Port Default	Когда входящий пакет не имеет VLAN Tag (нетегированный пакет) его приоритет выставляется в зависимости от входящего порта.Вам необходимо задать каждому порту значение COS

2.11.3 TOS/DSCP

Коммутаторы SWI/C000 могут оперировать IP пакетами, в которых под цели маркировки предусмотрено соответствующее поле в заголовке - IP Type of Service (ToS) размером один байт. ToS может быть заполнен классификатором IP Precedence или DSCP в зависимости от задачи. IP precedence (IPP) имеет размерность 3 бита (принимает значения 0-7). DSCP относится к модели DiffServ и состоит из 6 бит (значения 0-63).

TOS/DSCP

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

Apply Help

Описание параметров

Параметр	Описание
TOS/DSCP	Каждому значению DSCP присваивается одна из очередей приоритета: High, Middle, Low, and Lowest
Apply	Нажмите “**Apply**” чтобы активировать конфигурацию

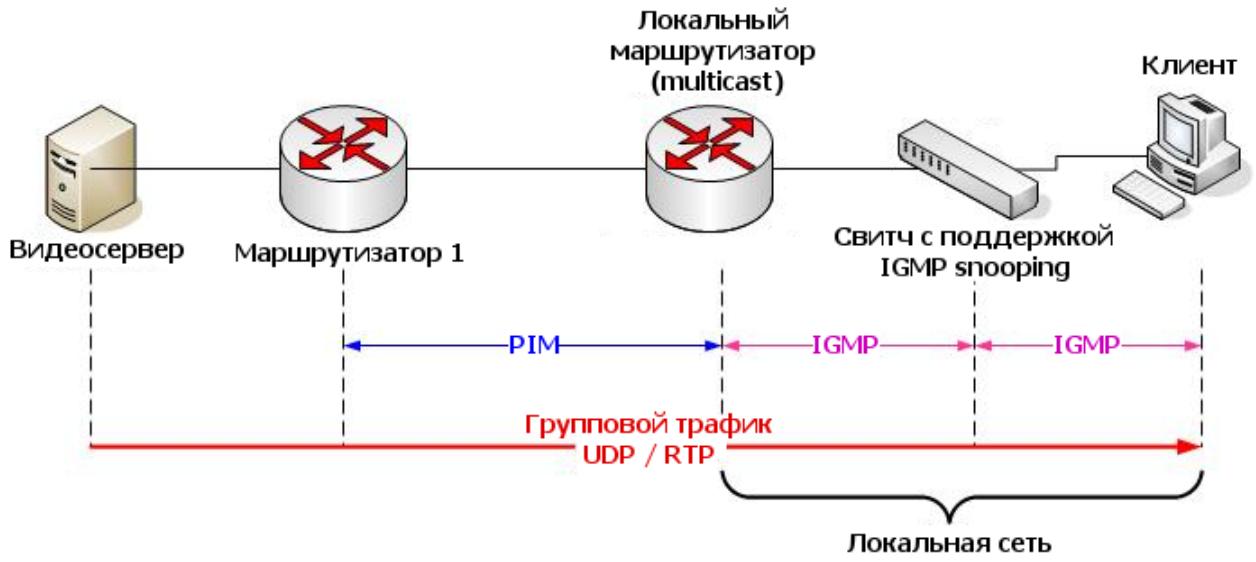
2.12 Multicast

IGMP (*Internet Group Management Protocol* - протокол управления группами Интернета) - протокол управления групповой (multicast) передачей данных в сетях, основанных на протоколе IP. IGMP используется маршрутизаторами и IP-узлами для организации сетевых устройств в группы.

Этот протокол является частью спецификации групповой передачи пакетов в IP-сетях. IGMP расположен выше сетевого уровня, хотя, по сути, действует не как транспортный протокол. Он во многом аналогичен ICMP для односторонней передачи. IGMP может использоваться для поддержки потокового видео и онлайн-игр, для этих типов приложений он позволяет использовать сетевые ресурсы более эффективно. IGMP уязвим к некоторым атакам, и брандмауэры обычно позволяют пользователю отключить этот протокол, если в нем нет необходимости.

IGMP используется только в сетях IPv4, так как в IPv6 групповая передача пакетов реализована по-другому.

Сеть, предоставляющая услуги групповой передачи данных (например, видео) с использованием IGMP, может иметь следующую базовую архитектуру:



IGMP используется клиентским компьютером и соседними коммутаторами для соединения клиента и локального маршрутизатора, осуществляющего групповую передачу. Далее между локальным и удаленным маршрутизаторами используется протокол Protocol Independent Multicast (PIM), с его помощью групповой трафик направляется от видеосервера к многочисленным клиентам групповой передачи.

Согласно Request for Comments (RFC), документу сообщества Internet Engineering Task Force (IETF), существует три версии IGMP. IGMPv1 определен в RFC 1112, IGMPv2 — в RFC 2236 и IGMPv3 — в RFC 3376.

Основным улучшением в IGMPv3 относительно IGMPv2 является поддержка фильтрации IP-адресов. С помощью этого механизма узел может сообщить, с каких адресов он хочет получать пакеты, а с каких нет.

Протокол IGMP реализован в виде серверной и клиентской частей, первая из которых выполняется на маршрутизаторе, вторая — в узле сети, получающем групповой трафик. Клиент посылает уведомление о принадлежности к какой-либо группе локальному маршрутизатору, в это время маршрутизатор находится в ожидании уведомлений и периодически рассылает клиентам запросы.

В IPv4 адрес мультивещания позволяет устройству отправлять пакеты определенной группе хостов(группе мультивещания) в отличной подсети. IP-адрес мультивещания определяет группу получателей трафика, а не конкретный хост. В качестве IP-адреса мультивещания используют IP-адреса класса D (224.0.0.0 – 239.255.255.255). некоторые адреса зарезервированы IANA для особых целей.

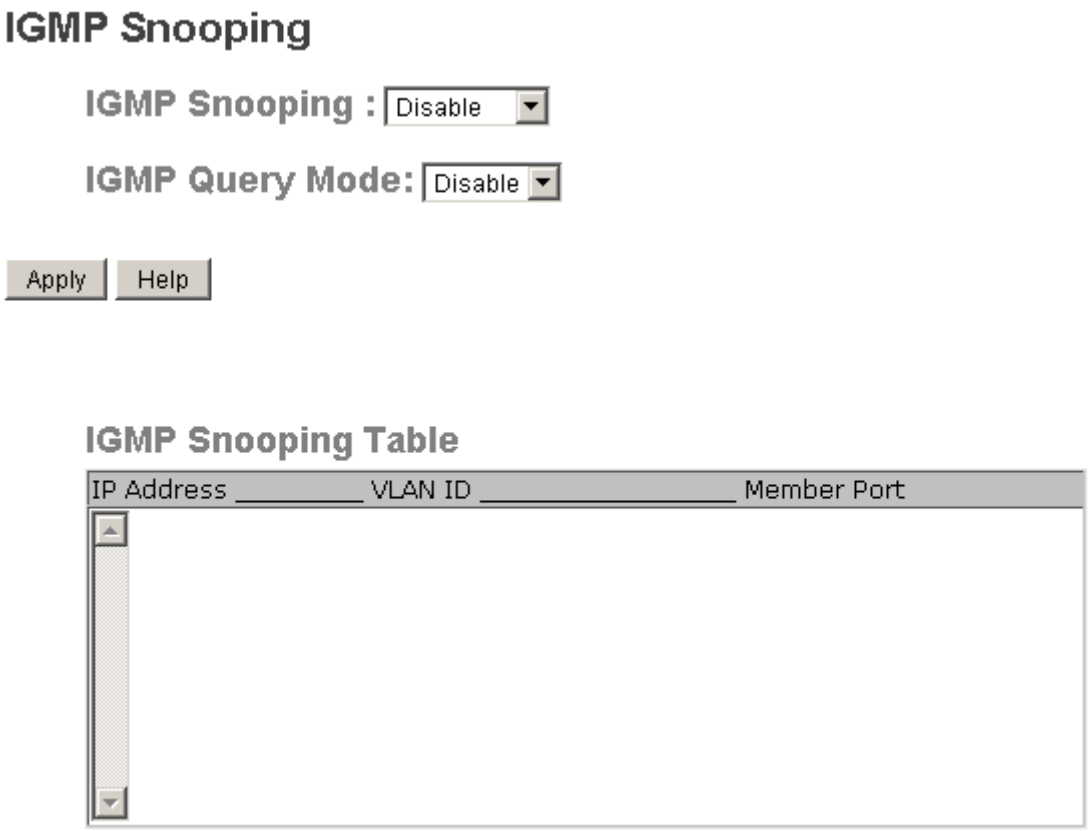
2.12.1 IGMP Snooping

IGMP snooping - процесс отслеживания сетевого трафика IGMP, который позволяет сетевым устройствам канального уровня (свитчам) отслеживать IGMP обмен между *потребителями* и *поставщиками* (маршрутизаторами) многоадресного (multicast) IP трафика, формально происходящий на более высоком (сетевом) уровне. Эта функциональность доступна в коммутаторах серии SWI/C000 но всегда требует отдельного включения и настройки.

После включения IGMP snooping, коммутатор начинает анализировать все IGMP пакеты между подключенными к нему *компьютерами-потребителями* и *маршрутизаторами-поставщиками* multicast трафика. Обнаружив IGMP запрос *потребителя* на подключение к *multicast группе*, коммутатор включает *порт*, к которому тот подключен, в список ее членов (для *ретрансляции* группового трафика). И наоборот - услышав запрос 'IGMP Leave' (покинуть), удаляет соответствующий порт из списка группы.

Querier -- это маршрутизатор (коммутатор), который отвечает за отправку multicast трафика в сегмент. Querier становится маршрутизатор (коммутатор) у которого меньше IP-адрес.

Эта роль выбирается с помощью IGMP, так как могут использоваться различные протоколы маршрутизации multicast трафика. Если используются разные протоколы на маршрутизаторах (коммутаторах), которые передают трафик в одну сеть, то маршрутизаторы (коммутаторы) не смогут обнаружить друг друга

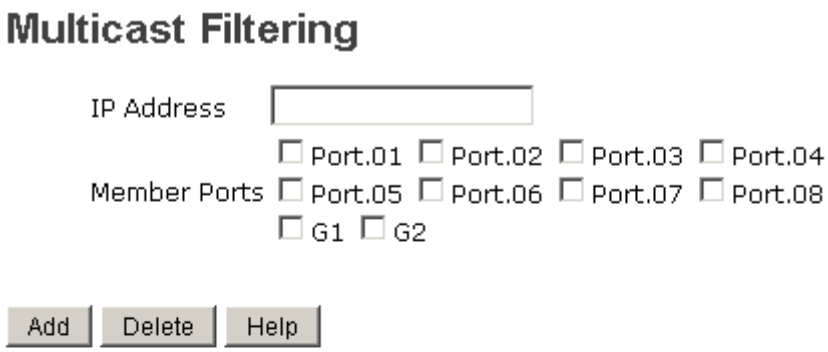


Описание параметров

Параметр	Описание.
IGMP Snooping	Включить выключить функцию IGMP snooping.
IGMP Query Mode	Enable – коммутатор становится Querier сети (устанавливается если например видеосервер включается непосредственно в этот коммутатор) Может быть только один IGMP querier в IGMP приложениях. Auto - Querier выбирается автоматически (по наименьшему IP адресу)
IGMP Snooping Table	Отображение существующих multicast групп
Apply	Нажмите “**Apply**” чтобы активировать новую конфигурацию.

2.12.2 Фильтрация IGMP [Multicast Filtering]

Функция фильтрации IGMP позволяет определять, к каким группам IGMP сможет присоединяться абонент на порту. Таким образом можно контролировать предоставление функций Multicasting (например рассылку контента) конкретным пользователям.



Описание параметров

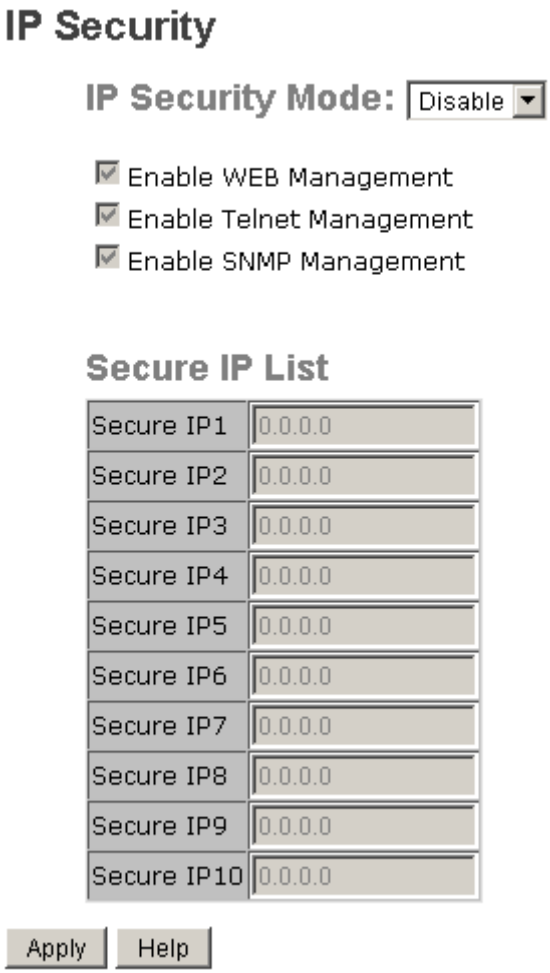
Параметр	Описание.
IP Address	Введите IP адрес мультикастовой группы в диапазоне 224.0.0.0 – 239.0.0.0
Member Ports	Отметьте порты, чтобы включить их в определенную группу.
Add	Нажмите чтобы добавить профиль в Multicast Filtering table
Delete	Удалить профиль из Multicast Filtering table

2.13 Безопасность [Security]

В коммутаторах серии SWI/C000 используются пять функций обеспечения безопстности: ограничение доступа к коммутатору по IP адресу (IP Security), ограничение по порту коммутатора (Port Security), по MAC адресу, по времени жизни записи MAC адреса в коммутаторе (MAC address Aging), а так же применение функций протокола 802.3x

2.13.1 IP Security

Функция IP Security позволяет включить/выключить управление коммутатором по протоколам WEB, Telnet, SNMP. А также может ограничить доступ к управлению коммутатору по IP адресам (только с указанных IP адресов возможно управлять коммутатором).



Описание параметров

Параметр	Описание
IP security MODE	Включает/Выключает функцию IP security .
Enable WEB Management	Включает управление по WEB.

Enable Telnet Management	Включает управление по Telnet.
Enable SNMP Management	Включает управление по SNMP.
Secure IP List	Назначает IP адреса, с которых возможно управление коммутатором

2.13.2 Port Security

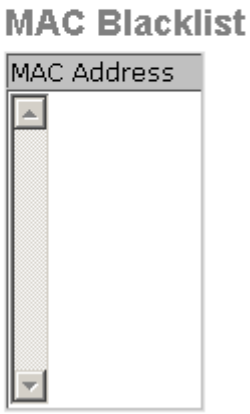
Функция Port Security «привязывает» MAC адреса к определенному порту коммутатора. Если на странице Port Control (см. главу 2.7.1 Port Control) включена функция Security на определенном порту, то порт будет обрабатывать фреймы, содержащие указанные MAC адреса.

Описание параметров

Параметр	Описание
MAC Address	Введите MAC адрес (например 001122334455).
Port NO.	Выберите порт коммутатора.
Add	Нажмите кнопку Add чтобы добавить информацию
Delete	Нажмите кнопку Delete чтобы удалить отмеченную информацию в Port Security List

2.13.3 MAC Blacklist

Функция MAC Blacklist (Черный список) позволяет исключить трафик, который предназначен определенным MAC адресам. То есть устройство с этим MAC адресом не получит ни одного фрейма.



Описание параметров

Параметр	Описание
MAC Address	Введите MAC адрес, чтобы добавить в MAC Blacklist (Черный список) в формате 001122334455.
Add	Нажмите Add чтобы добавить адрес в Blacklist (Черный список).

2.13.4 802.1x

Механизм аутентификации портов позволяет проверять права доступа клиентов к портам коммутатора с использованием внешнего сервера (сервера аутентификации). Коммутаторы серии SWI/C000 поддерживают метод аутентификации с помощью протокола IEEE 802.1x.

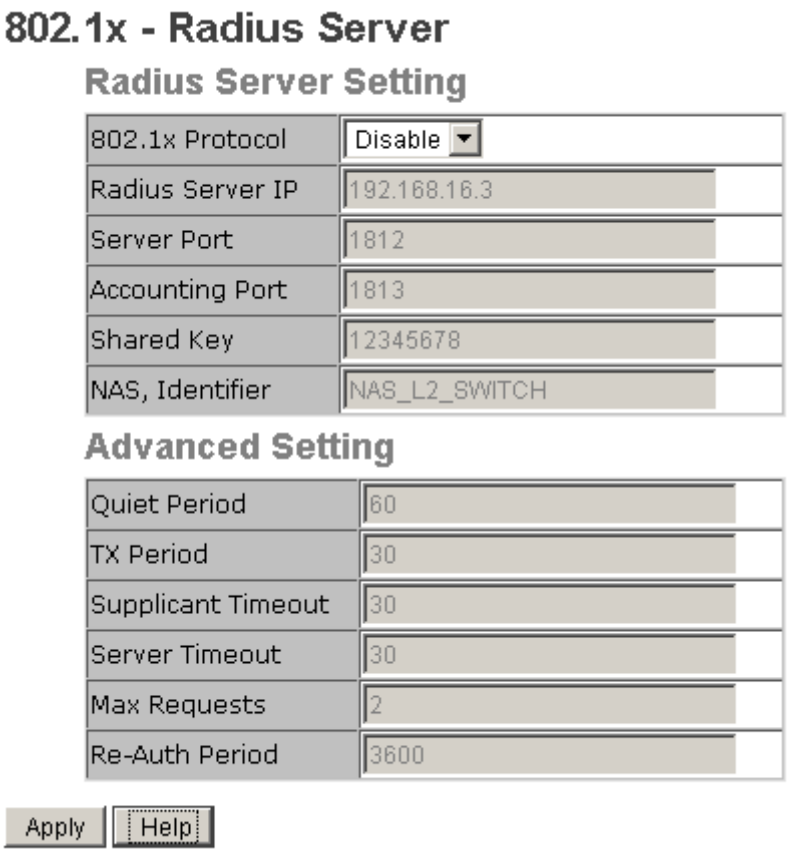
IEEE 802.1x – предусматривает проверку прав доступа к портам на сервере аутентификации с использованием имени пользователя и пароля, предоставленных пользователю.

Проверка прав пользователя осуществляется с использованием протокола RADIUS (Remote Authentication Dial In User Service, RFC 2138, 2139)

Процесс проверки прав пользователя, подключающегося к порту с активированным механизмом аутентификации IEEE 802.1x, показан на рисунке. Данный коммутатор запрашивает у клиента информацию для входа в систему в виде имени пользователя и пароля. После получения от клиента параметров входа в систему коммутатор отправляет

запрос аутентификации на сервер RADIUS. Сервер RADIUS проверяет, обладает ли данный клиент правом доступа к порту. Коммутатор в данном случае выступает как NAS (Network Access Server) сервер доступа.

2.13.4.1 Radius Server



Описание параметров

Параметр	Описание
Radius Server Setting	
Radius Server IP	Введите IP адрес RADIUS сервера.
Server port	UDP порт используемый Radius сервером для аутентификации (по умолчанию 1812).
Account port	UDP порт используемый Radius сервером для аккаунтинга (по умолчанию 1813) (**Accounting** (учёт) — слежение за потреблением сетевых ресурсов пользователем.)
Shared Key	Ключ используемый коммутатором и Radius сервером для аутентификации друг с другом.
NAS, Identifier	Идентификатор коммутатора, для аутентификации коммутатора с Radius сервером.
Advanced Setting	
Quiet Period	«Период молчания» интервал времени между неудачной аутентификацией и новой попыткой аутентификации супликанта (supplicant) и аутентификатором сети (по умолчанию 60 секунд)

Tx Period	Время которое коммутатор ждет пред отправкой нового фрейма EAPOL PDU (по умолчанию 30 секунд)
Supplicant Timeout	Время ожидания между сообщениями EAP между супликантом и аутентификаторм. (по умолчанию 30 секунд)
Server Timeout	Время ожидание ответа коммутатором ответа от Radius сервера на запрос аутентификации (по умолчанию 30 секунд)
Max Requests	Количество попыток аутентификации клиента до тех пор пока порт станет неавторизирован (по умолчанию 2)
Re-Auth Period	Период времени, после которого, клиент должен заново пройти аутентификацию. (не должен быть равным 0. по умолчанию 3600 секунд)

2.13.4.2 Port Auth Setting

На этой странице настраивается режим авторизации портов

802.1x - Port Authorize Mode

Port No.	Port Authorize Mode
Port.01	Accept
Port.02	Accept
Port.03	Accept
Port.04	Accept
Port.05	Accept
Port.06	Accept
Port.07	Accept
Port.08	Accept
G1	Accept
G2	Accept

Apply Help

Описание параметров

Параметр	Описание
Port Authorized Mode	**Reject:** порт «жестко» устанавливается в режим «неавторизован». **Accept:** порт «жестко» устанавливается в режим «авторизован» Authorize: состояние порта определяется протоколом 802.1x **Disable:** порт не участвует в процедуре аутентификации по протоколу 802.1x

2.13.4.3 Port Auth State

На этой странице отображается состояние авторизации портов

802.1x - Port Authorize State

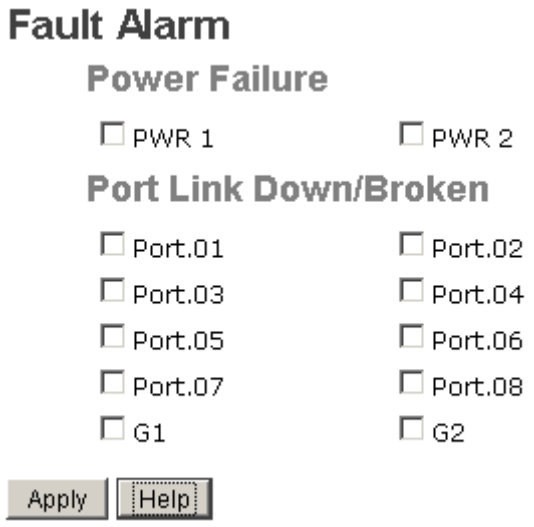
Port No.	Port Authorize State
Port.01	Accept
Port.02	Accept
Port.03	Accept
Port.04	Accept
Port.05	Accept
Port.06	Accept
Port.07	Accept
Port.08	Accept
G1	Accept
G2	Accept

2.14 Сигнализация

Функции сигнализации очень важны при управлении и обслуживании коммутатора. Коммутатор может сигнализировать о каком-либо событии или ошибки с помощью протокола SYSLOG, SMTP или релейного выхода. Сигнализация позволяет вам наблюдать состояние коммутатора на удаленном «сайте». Когда произойдет определенное событие, коммутатор пошлет сообщение на Syslog сервер, пошлет e-mail сообщение и сработает релейный выход (замигает светодиот Fault).

2.14.1 Аварийная сигнализация [Warning]

Когда произойдет выбранное вами аварийное событие, то светодиод Fault и



релейный выход буду сигнализировать об этом.

Описание параметров

Параметр	Описание
Power Failure	Отметьте источник питания PWR1 и PWR2.
Port Link Down/Broken	Отметьте физические порты коммутатора. Если пропадет линк одного из низ, аварийная сигнализация оповестит об этом.
Apply	Нажмите “**Apply**” чтобы применить новую конфигурацию.

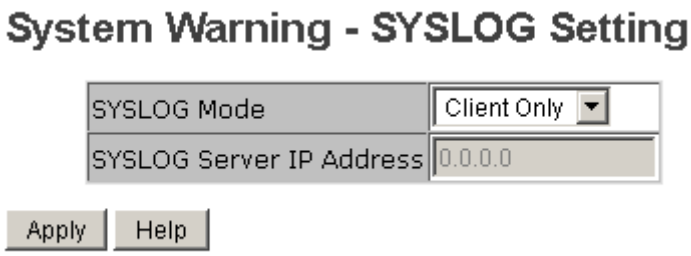
2.14.2 Сигнализация об ошибках системы [System warning]

Коммутатор может передавать уведомления о своих системных неисправностях с помощью Syslog и E-mail. Вы можете выбрать из списка аварию и способ передачи сообщения о ней.

2.14.2.1 настройка протокола Syslog [Syslog Setting]

syslog — стандарт отправки сообщений о происходящих в системе событиях (логов), использующийся в компьютерных сетях, работающих по протоколу IP. Протокол syslog прост: отправитель посылает короткое текстовое сообщение, размером меньше 1024 байт получателю сообщения. Сообщения могут отправляться как по UDP, так и по TCP. Syslog используется для удобства администрирования и обеспечения информационной безопасности.

Он реализован под множество платформ и используется в множестве устройств. Поэтому, использование syslog позволяет обеспечить сбор информации с разных мест и хранение её в едином репозитории. (RFC 3164 3195)

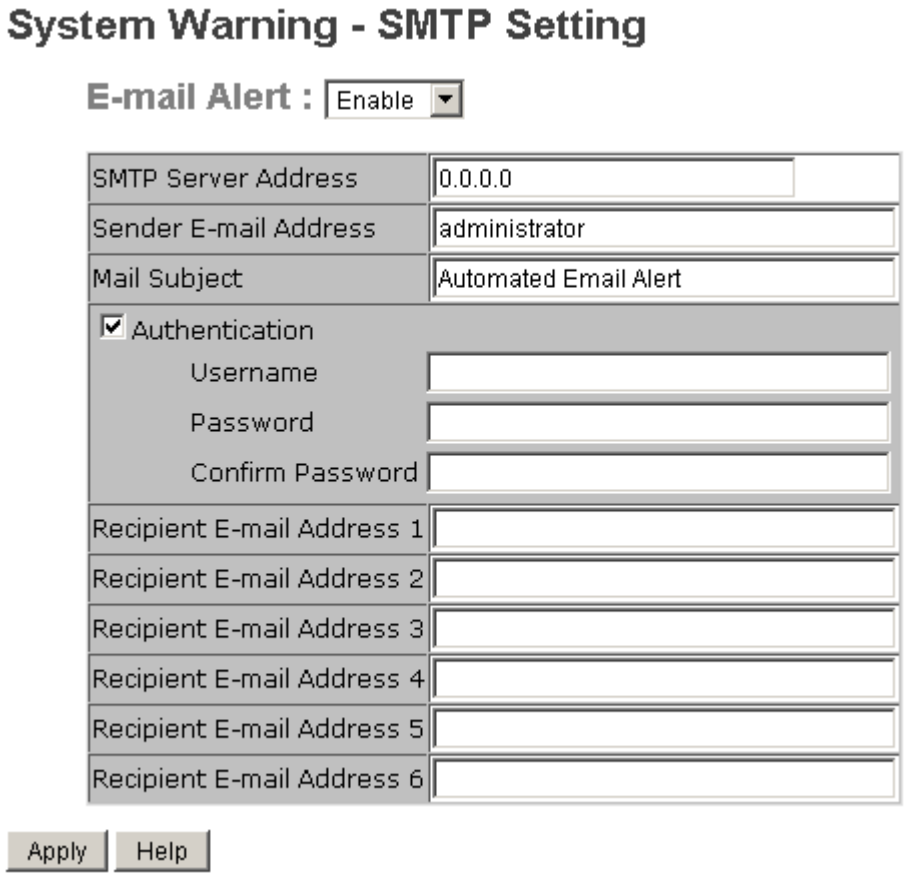


Описание параметров

Параметр	Описание
SYSLOG Mode	**Disable:** выключить функцию SYSLOG. **Client Only:** отправляет сообщение только в локальный лог (его можно посмотреть на странице System Event Log коммутатора) **Server Only:** Отправляет сообщение только на удаленный сервер Syslog. **Both:** отправляет сообщение и в локальный лог и на удаленный сервер
SYSLOG Server IP Address	IP адрес удаленного Syslog сервера.
Apply	Нажмите “**Apply**” чтобы активировать новую конфигурацию.

2.14.2.2 Настройка SMTP [SMTP Setting]

SMTP – (Simple Mail Transfer Protocol) протокол передачи e-mail сообщений по сети RFC 821.

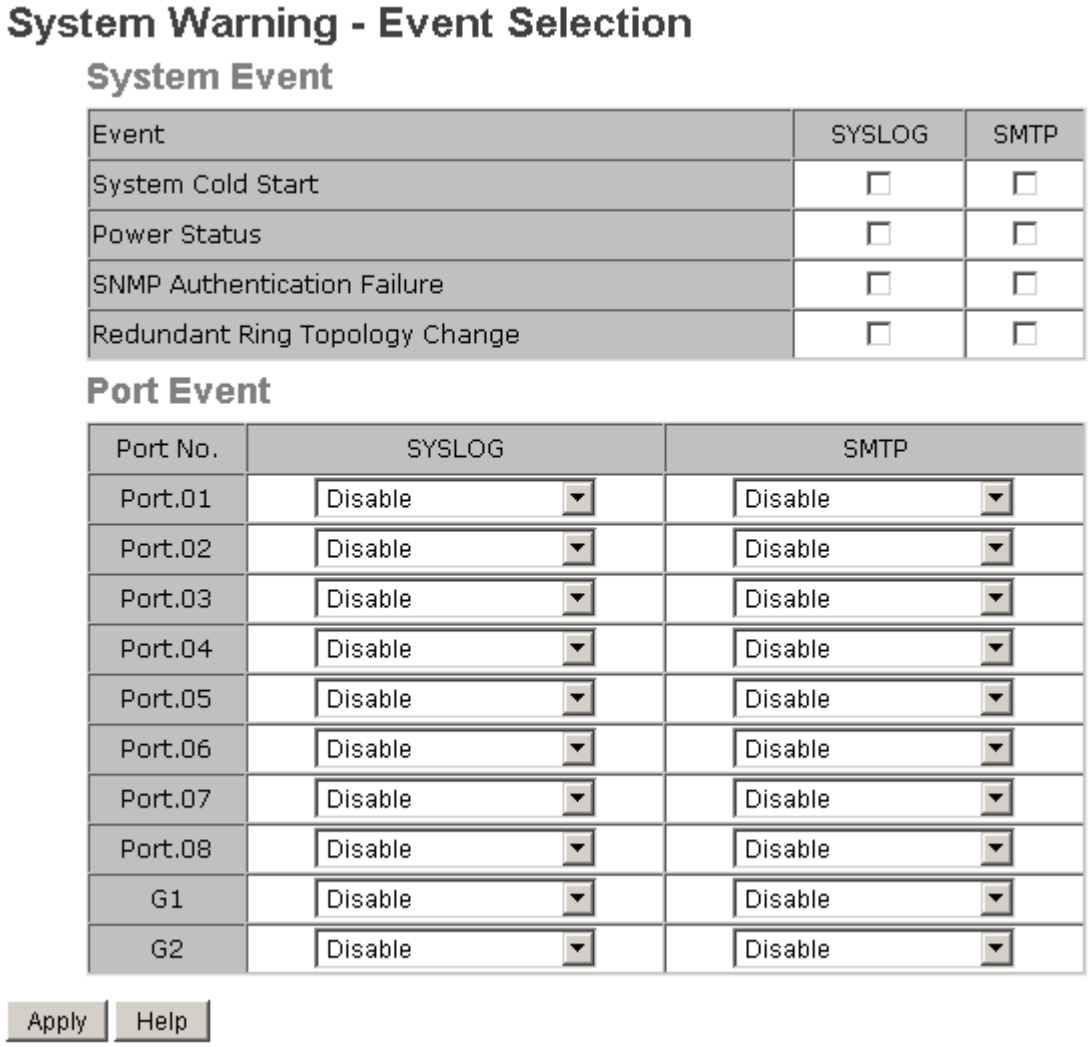


Описание параметров

Параметр	Описание
E-mail Alert	Включить/выключить оповещение об аварийных событиях с помощью e-mail.
SMTP Server Address	IP адрес почтового сервера или его доменное имя.
Sender E-mail Address	Почтовый адрес от имени которого отправляются e-mail сообщения
Mail Subject	Тема письма
Authentication	Параметры аутентификации на SMTP сервере. Если это необходимо **Username:** имя пользователя. **Password:**. пароль **Confirm Password:** подтверждение пароля
Recipient E-mail Address	Почтовые адреса получателей сообщения. Может быть 6 получателей.
Apply	Нажмите “**Apply**” чтобы активировать новую конфигурацию

2.14.2.3 Выбор события аварий [Event Selection]

Существует два метода оповещения об аварии: с помощью SMTP и Syslog. Выберите аварийное событие и метод сообщения о нем. Замечание: необходимо включить поддержку протоколов Syslog и SMTP, чтобы это окно стало активным.



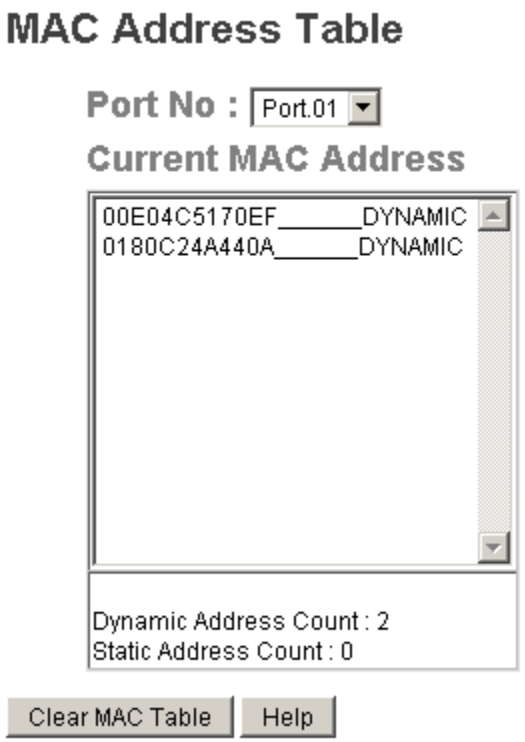
Описание параметров

System Event	
System Cold Start	Сообщение при перезагрузке коммутатора
Power Status	Сообщение, когда питание пропало или появилось
SNMP Authentication Failure	Сообщение, когда аутентификация SNMP неудачна
Redundant Ring Topology Change	Сообщение, когда изменилось состояние порта.
Port Event SYSLOG / SMTP Event	Сообщение, когда пропал или появился линк на выбранном порту

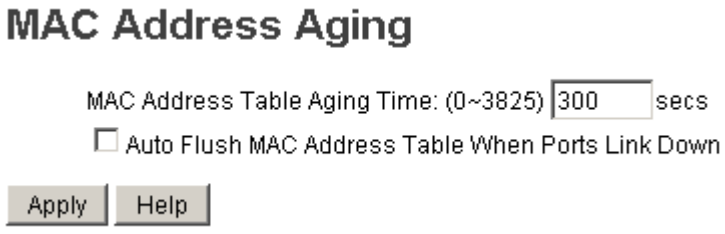
2.15 наблюдение и диагностика [Monitor and Diag]

С помощью специальных инструментов, которыми обладают коммутаторы серии SWI/C000, можно отслеживать и диагностировать состояние и проблемы коммутатора.

2.15.1 MAC Address Table



Коммутатор выводит таблицу MAC адресов принадлежащую конкретному порту. Кнопкой Clear Mac Table Ьщжно очистить таблицу.



На коммутаторе можно задать время жизни записи о MAC адресе в таблице (по умолчанию 300 секунд)

Также можно настроить автоматическую очистку таблицы MAC Адресов при выключении физического линка (отметьте Auto Flush MAC Address Table When Ports Link Down)

2.15.2 Статистика порта [Port Statistic]

На этой странице показанных несколько счетчиков для каждого порта

Port Statistics

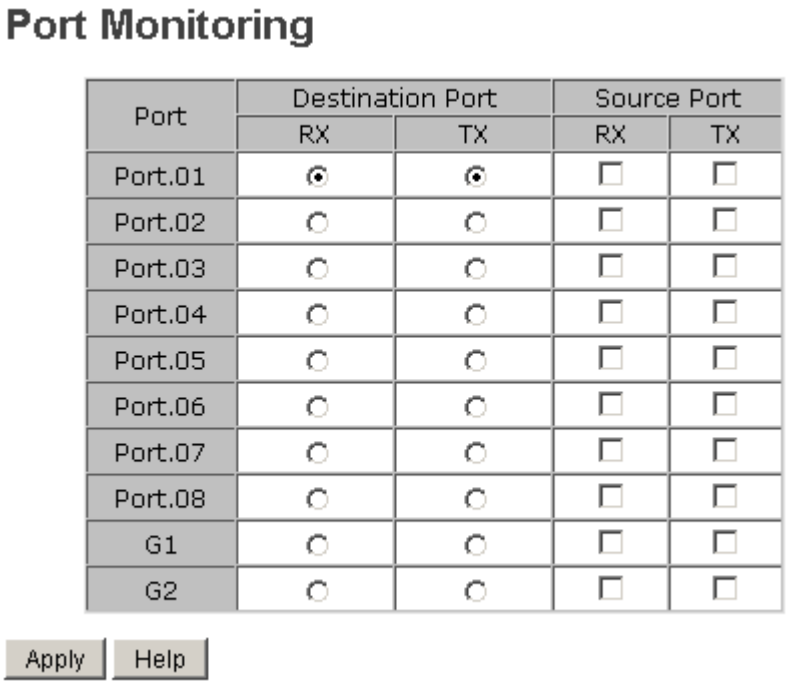
Port	Type	Link	State	TX Good Packet	TX Bad Packet	RX Good Packet	RX Bad Packet	TX Abort Packet	Packet Collision
Port.01	100TX	Up	Enable	1390454	0	1320007	0	0	0
Port.02	100TX	Up	Enable	448	0	1387772	0	0	0
Port.03	100TX	Down	Enable	0	0	0	0	0	0
Port.04	100TX	Down	Enable	0	0	0	0	0	0
Port.05	100TX	Down	Enable	0	0	0	0	0	0
Port.06	100TX	Down	Enable	0	0	0	0	0	0
Port.07	100TX	Down	Enable	0	0	0	0	0	0
Port.08	100TX	Down	Enable	0	0	0	0	0	0
G1	SFP	Down	Enable	0	0	0	0	0	0
G2	SFP	Down	Enable	0	0	0	0	0	0

Clear Help

Описание параметров

Параметр	Описание
Type	Показывает скорость порта и тип порта.
Link	Статус линка
State	Показывает включен или выключен порте.
TX GOOD Packet	Количество целых пакетов посланных портом.
TX Bad Packet	Количество битых пакетов посланных портомt.
RX GOOD Packet	Количество целых пакетов принятых портом.
RX Bad Packet	Количество битых пакетов принятых портом
TX Abort Packet	Количество пакетов остановленных портом.
Packet Collision	Количество обнаруженных коллизий на этом порту.
Clear	Обнуление всех счетчиков

2.15.3 Зеркалирование портов [Port Monitoring]



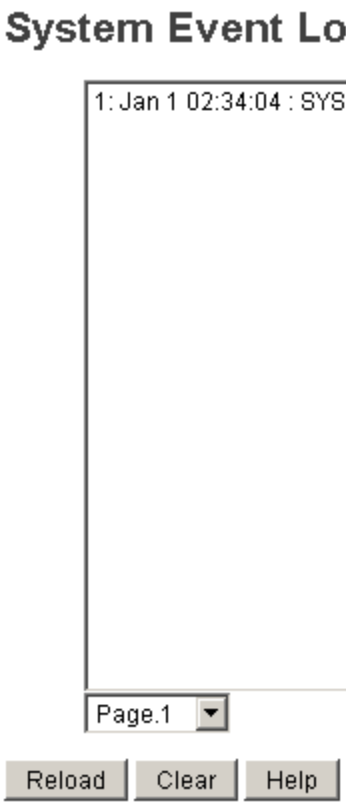
С помощью этой функции можно отслеживать пакеты приходящие на определенные порты.

Описание параметров

Параметр	Описание
Destination Port	Порт который принимает копии пакетов
Source Port	Порт, который необходимо мониторить. Отметьте, что необходимо мониторить прием или передачу пакетов или все вместе. Не выбирайте слишком много портов для мониторинга. ЭТО СОЗДАЕТ БОЛЬШУЮ НАГРУЗКУ НА КОММУТАТОР
TX	Пакеты отправленные портом.
RX	Пакеты принимаемые портом..

2.15.4 Локальный лог событий [System Event Log]

Если включено ведение локального лога (см **2**.14.2.1 настройка протокола Syslog [Syslog Setting]) то на этой странице будут отображаться события. Которые произошли в системе.



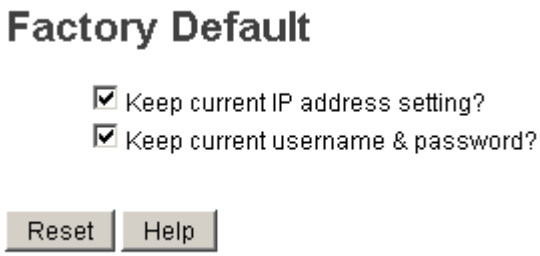
Описание параметров

параметр	описание
Page	Выберите страницу лога.
Reload	Получить новейшие событие.
Clear	Очистить лог.

2.16 Сохранение конфигурации [Save Configuration]

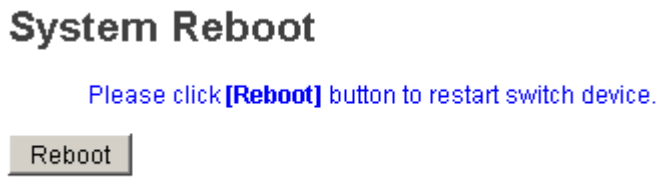
Для того чтобы сохранить конфигурацию в постоянной flash памяти, необходимо нажать кнопку Save на этой странице, инече при перезагрузке все несохраненные данные будут утеряны.

2.17 Заводские установки [Factory Default]



В коммутаторе есть возможность вернуться к настройкам по умолчанию. Нажмите кнопку Reset, и коммутатор перезагрузится с настройками по умолчанию. Если вы хотите сохранить сетевые настройки коммутатора, отметьте «Keep current IP address setting?».Если вы хотите сохранить имя пользователя и пароль для доступа к управлению коммутатора. Отметьте «Keep current username & password?».

2.18 Перезагрузка коммутатора [System Reboot]



Нажмите кнопку Reboot для перезагрузки коммутатора