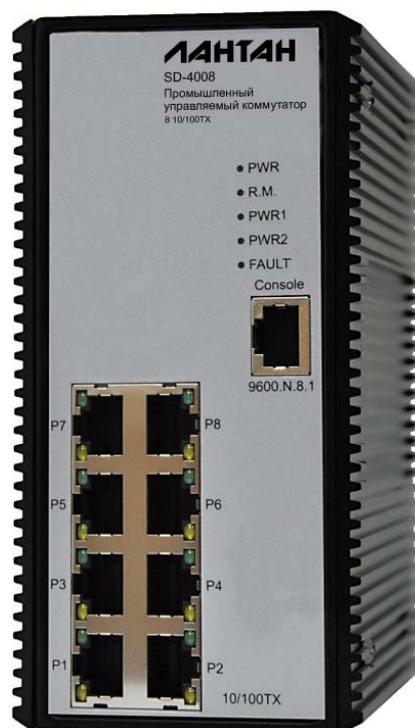


# ЛАНТАН

---

## SD-4008

### 8 10/100TX Управляемый Промышленный Коммутатор



### Руководство пользователя

## Предупреждение FCC

Это оборудование было протестировано и признано соответствующим ограничениям для цифровых устройств **Class-A**, согласно части 15 правил **FCC** (Федеральной комиссии связи США). Эти ограничения разработаны для обеспечения достаточной защиты от вредных помех в жилых помещениях. Данное оборудование генерирует, использует и может излучать радиоволны. Они могут вызывать помехи для радиосвязи, если оборудование не установлено и не используется в соответствии с настоящими инструкциями.

Тем не менее, нет гарантии, что помехи не будут возникать в каждом конкретном случае. Если это оборудование вызывает помехи для радио или телевизионного приема, что можно определить путем включения и выключения оборудования, пользователь может попытаться устранить помехи одним или несколькими из следующих способов:

- Переориентировать или переместить приемную антенну.
- Увеличить расстояние между оборудованием и приемником
- Подключить оборудование к розетке в цепи, отличной от той, к которой подключен приемник.
- Обратится в техническую поддержку или к специалистам по радио / ТВ за помощью

## Предупреждение CE Mark

Это продукт **Class-A**. В бытовых условиях это изделие может вызывать радиопомехи, в этом случае пользователь обязан принять адекватные меры.

## Оглавление

Глава 1. Введение.....	1
1.1. Свойства оборудования.....	1
1.2. Свойства программного обеспечения.....	3
1.3. Комплект поставки.....	4
Глава 2. Описание устройства .....	5
2.1 Физические размеры .....	5
2.2 Лицевая панель .....	5
2.3 Нижняя панель.....	5
2.4 Диагностические светодиоды (LED) .....	6
Глава 3. Монтаж устройства .....	7
3.1 Пошаговые действия по монтажу.....	7
3.2 Крепление на DIN-рейку .....	8
3.3 Настенный монтаж Коммутатора.....	9
3.4 Подключение питания .....	10
3.5 Подключение контакта сигнализирующего об ошибке .....	11
3.6 Подключение кабелей .....	12
3.7 Приложение <i>Pro-Ring2s</i> .....	13
Глава 4. Управление с консоли.....	14
4.1 Соединение с портом консоли ( <i>Console Port</i> ).....	14
4.2 Назначение контактов.....	14
4.3 Вход в интерфейс Консоли .....	15
4.4 Управление при помощи команд <i>CLI</i> .....	16
Глава 5. Web - Управление .....	17
5.1 Кратко об Web - управлении.....	17
5.2 Подготовка к Web - управлению .....	17
5.3 Вход в систему .....	18
5.4 Система.....	19
5.4.1 Основная информация о Коммутаторе: <i>General – Switch Information</i> .....	19

5.4.2 Ресурсы: <i>General – Asset</i> .....	19
5.4.3 Средняя Загрузка ЦПУ: <i>General – CPU Load Average</i> .....	20
<b>5.5 Время: <i>Time - SNTP</i> .....</b>	<b>21</b>
<b>5.6 Учетная запись: <i>Account - Admin</i>.....</b>	<b>23</b>
<b>5.7 IP адресация: <i>IP Addressing – IPV4</i> .....</b>	<b>24</b>
<b>5.8 Журнал Системы: <i>Syslog</i> .....</b>	<b>25</b>
5.8.1 Настройка Журнала Системы: <i>Syslog Configuration</i> .....	25
<b>5.9 Настройка SNMP: <i>SNMP Configuration</i>.....</b>	<b>26</b>
5.9.1 Агент: <i>SNMP - Agent</i> .....	26
5.9.2 Настройка ловушек SNMP: <i>SNMP Trap Configuration</i> .....	27
<b>5.10 Реле тревог: <i>System Alert - Relay Alarm</i> .....</b>	<b>28</b>
5.10.1 Системные тревоги: <i>System Alert – SMTP</i> .....	28
5.10.2 Системные тревоги – События: <i>System Alert – Event</i> .....	30
<b>5.11 Сервер <i>DHCP</i>.....</b>	<b>31</b>
5.11.1 Конфигурация сервера: <i>DHCP Server</i> .....	31
5.11.2 Таблица клиента - <i>Client Table</i> .....	32
5.11.3 Привязки - <i>IP Bindings</i> .....	32
<b>5.12 Настройка порта: <i>Port – Configuration</i>.....</b>	<b>33</b>
<b>5.13 Состояние порта - <i>Port Status</i>.....</b>	<b>34</b>
<b>5.13 Статистика порта - <i>Port Statistics</i>.....</b>	<b>34</b>
<b>5.15 Тревоги на порту - <i>Port – Port Alert</i>.....</b>	<b>35</b>
<b>5.16 Настройка пределов скорости - <i>Rate Control –Rate Limit</i>.....</b>	<b>36</b>
<b>5.17 Настройка агрегирования - <i>Aggregation – Configuration</i> .....</b>	<b>37</b>
5.17.1 Настройка - <i>Configuration</i> .....	38
5.17.2 Состояние агрегации - <i>Aggregator – Status</i> .....	39
<b>5.18 Дерево Соединений – <i>Spanning Tree</i>.....</b>	<b>40</b>
5.18.1 Настройки RSTP (RSTP Setting) .....	40
5.18.2 Информация о RSTP - <i>RSTP Information</i> .....	42
<b>5.19 Механизм кольца <i>Pro-Ring II S</i>.....</b>	<b>43</b>
<b>5.20 Поддержка мультиадресного обмена - <i>Multicast Support</i> .....</b>	<b>44</b>

5.20.1 Слежение за сетевым трафиком - <i>IGMP Snooping</i> .....	44
5.20.2 Статическая фильтрация адресов - <i>Static Filtering</i> .....	45
<b>5.21 Протокол <i>LLDP</i></b> .....	<b>46</b>
5.21.1 Настройка протокола LLDP - <i>LLDP Configuration</i> .....	46
5.22.1 Соседние порты - <i>LLDP Neighbors</i> .....	46
<b>5.23 База данных фильтрации – <i>Filtering Data Base</i></b> .....	<b>47</b>
5.23.1 Настройка Базы данных фильтрации .....	47
5.23.2 Динамическая таблица MAC-адресов - <i>Dynamic MAC table</i> .....	47
<b>5.24 Виртуальная сеть - <i>VLAN</i></b> .....	<b>48</b>
5.24.1. Настройка сети - <i>VLAN Configuration</i> .....	48
5.24.2 Состояние коммутатора - <i>Switch Status</i> .....	50
<b>5.25 Качество обслуживания - <i>QoS</i></b> .....	<b>51</b>
5.25.1 Общие настройки - <i>Global Settings</i> .....	51
5.25.2 Приоритеты порта - <i>Port Priority</i> s.....	52
5.25.3 Отображение класса обслуживания на очереди - <i>COS Mapping to Queue</i> .....	52
5.25.4 Отображение кода дифференцированных служб на очереди – <i>DSCP mapping to queue</i> ....	53
<b>5.26. Зеркальное отображение порта - <i>Port Mirroring</i></b> .....	<b>54</b>
<b>5.27. Защита - <i>Security</i></b> .....	<b>55</b>
5.27.1 Настройка Защиты источников IP - <i>IP Source Guard - Configuration</i> .....	55
5.27.2 Защита по IP - <i>IP Source Guard – Static Table</i> .....	56
5.27.3 Аутентификация - <i>802.1X/Radius</i> .....	57
5.27.3.1 Настройка - <i>Configuration</i> .....	57
5.27.3.2 Настройки порта - <i>Port Setting</i> .....	58
5.27.3.3 Состояние порта - <i>Port Status</i> .....	59
5.27.4 Фильтрация по MAC-адресам - <i>MAC Filtering</i> .....	60
5.27.5 Защита порта - <i>Port Security</i> .....	60
<b>5.28. Обслуживание - <i>Maintenance</i></b> .....	<b>61</b>
5.28.1 Сохранить настройки - <i>Save Configuration</i> .....	61
5.28.2 Перезапуск устройства - <i>Restart Device</i> .....	61
5.28.3 Фабричные настройки по умолчанию - <i>Factory Defaults</i> .....	61
5.28.4 Обновление фирменного ПО - <i>Firmware Upgrade</i> .....	62

5.28.5 Экспорт/Импорт - <i>Export/Import</i> .....	63
5.28.6 Диагностика - <i>Diagnostics</i> : Пингование - <i>Ping</i> .....	64
<b>Диагностика - Troubleshooting</b> .....	<b>65</b>
<b>Приложение А—Назначение контактов RJ-45</b> .....	<b>66</b>
<b>Приложение В — Список команд</b> .....	<b>69</b>
<i>Switch Setting Commands Set</i> – Настройка Коммутатора .....	69
<i>Admin Password Commands Set</i> – Команды администратора.....	70
<i>IP Setting Commands Set</i> –Настройки IP .....	70
<i>SNTP Commands Set</i> – Команды работы с SNTP .....	71
<i>LLDP Commands Set</i> – Команды работы с LLDP.....	72
<i>Backup &amp; Restore</i> – Резервирование и восстановление.....	72
<i>Upgrade Firmware</i> – Обновление Фирменного ПО .....	72
<i>DHCP Server Commands Set</i> - Работа с сервером DHCP.....	73
<i>Port Control Commands Set</i> – Управление портом .....	74
<i>Port Status Commands Set</i> – Состояние порта.....	75
<i>Rate Limit Commands Set</i> – Настройка пределов скоростей .....	76
<i>Trunk Commands Set</i> –Управление «Стволом».....	77
<i>PRO-RING IIS Commands Set</i> – Управление кольцом PRO-RING IIS.....	78
<i>RSTP Commands Set</i> – Управление RSTP.....	79
<i>VLAN Commands Set</i> – Управление виртуальной сетью.....	80
<i>SNMP Commands Set</i> – Команды SNMP .....	82
<i>Traffic Prioritization Commands Set</i> – Приоритеты трафика .....	83
<i>IGMP Commands Set</i> – Команды IGMP .....	84
<i>Multicast Static Filtering Table Commands Set</i> – Мультиадресная Фильтрация .....	85
<i>IP Security Commands Set</i> – Защита IP .....	86
<i>Port Security Commands Set</i> – Защита порта .....	86
<i>MAC Blacklist Commands Set</i> – Черный список MAC-адресов .....	87
<i>802.1x Commands Set</i> – Команды 802.1x .....	88
<i>Fault Alarm Commands Set</i> – Реле ошибок.....	89
<i>System Warning Commands Set</i> – Системные предупреждения .....	90
<i>Mac Address Table Commands Set</i> – Таблица MAC - адресов .....	91

<i>Port Statistics Commands Set</i> – Статистика порта .....	92
<i>Port Monitoring Commands Set</i> – Мониторинг порта .....	92
<i>System Event Log Commands Set</i> – Архив системных событий .....	92
<i>Ping Commands Set</i> - Пингование .....	92
<i>Loading Average Commands Set</i> – Средняя загрузка .....	93
<i>Factory Default Commands Set</i> – Заводские настройки .....	93
<i>System Reboot Commands Set</i> – Перезагрузка системы .....	93
<i>Logout Commands Set</i> - Выход .....	93



# Глава 1. Введение

**8-ми портовый 10 / 100TX Управляемый Промышленный Коммутатор** представляет собой экономически эффективное решение и отвечает высоким требованиям по надежности, необходимым для промышленных применений. Использование оптоволоконного порта может увеличить расстояние соединения, что увеличивает гибкость структуры сети и её производительность

## 1.1. Свойства оборудования

<b>Стандарты</b>	IEEE 802.3 10Base-T Ethernet IEEE 802.3u 100Base-TX/ FX IEEE802.3x Flow Control and Back Pressure IEEE802.3ad Port trunk with LACP IEEE802.1d Spanning Tree/ IEEE802.1w Rapid Spanning Tree IEEE802.1p Class of Service IEEE802.1Q VLAN Tag IEEE 802.1x User Authentication (Radius) IEEE802.1ab LLDP
<b>Архитектура Коммутатора</b>	Системная плата (Switching Fabric): 1.6Gbps Пропускная пакетная способность (Full-Duplex): 8.3Mpps @64bytes
<b>Скорость передачи</b>	14,880pps - Порт Ethernet 148,800pps - Порт Fast Ethernet 1,488,000pps - Порт Gigabit Fiber Ethernet
<b>Буфер пакета</b>	1Mbits
<b>MAC адрес</b>	8К (таблица MAC адресов)
<b>Флэш ROM</b>	4Mbytes
<b>DRAM</b>	32Mbytes

<b>Коннекторы</b>	10/100TX: 8 портов RJ-45 с функцией Auto MDI/MDI-X RS-232: тип RJ-45
<b>Сетевой кабель</b>	10Base-T: 2-пары UTP/STP Cat. 3, 4, 5/ 5E кабель EIA/TIA-568 100 Ом (100m) 100Base-TX: 2-пары UTP/STP Cat. 5/ 5E кабель EIA/TIA-568 100 Ом (100m)
<b>Протокол</b>	CSMA/CD
<b>Светодиоды</b>	На модуле: Питание (Зеленый), Питание 1 (Зеленый), Питание 2 (Зеленый), Ошибка (Красный), Мастер (Зеленый), FWD - пересылка (Зеленый); На каждом порту: Link/Activity(Зеленый), Full duplex/Collision (Янтарный)
<b>Питание</b>	Внешнее питание: Пост. ток 12~48В, Резервное питание: Пост. ток 12~48В
<b>Потребление питания</b>	7.86 Вт при полной нагрузке
<b>Рабочая влажность</b>	От 5% до 95% (Без конденсации)
<b>Рабочая температура</b>	-40°C ~ 75°C
<b>Температура хранения</b>	-40°C ~ 85°C
<b>Размеры корпуса</b>	IP-30, 74мм (Ш) x 105мм (Г) x 152мм (В)
<b>Монтаж</b>	DIN рейка, проушины для настенного крепления (опция)
<b>EMI - эмиссия</b>	FCC Class A, CE EN61000-4-2, CE EN61000-4-3, CE EN-61000-4-4, CE EN61000-4-5, CE EN61000-4-6, CE EN61000-4-8, CE EN61000-4-11, CE EN61000-4-12, CE EN61000-6-2, CE EN61000-6-4
<b>Безопасность</b>	UL, cUL, CE/EN60950-1
<b>Тест стабильности</b>	IEC60068-2-32 (Падение), IEC60068-2-27 (Удар), IEC60068-2-6 (Вибрация)

## 1.2. Свойства программного обеспечения

<b>Management-Управление</b>	SNMP v1 v2c, v3/ Web/Telnet/CLI
<b>SNMP MIB (база управляющей информации)</b>	RFC 1215 Trap, RFC1213 MIBII, RFC 1157 SNMP MIB, RFC 1493 Bridge MIB, RFC 2674 VLAN MIB, RFC 1643 , RFC 1757, RSTP MIB, Private MIB, LLDP MIB
<b>VLAN</b>	Port Based VLAN IEEE 802.1Q Tag VLAN (256 ввода)/ VLAN ID (До 4К, VLAN ID может быть присвоен от 1 до 4094.) GVRP (256 Групп)
<b>Port Trunk с LACP</b>	LACP Port Trunk: 4 Trunk групп /Максимально 4 trunk элемента
<b>LLDP</b>	Поддерживает LLDP, позволяя коммутатору оповещать (advertise) о своей идентификации и возможностях по LAN
<b>Spanning tree - связующее дерево</b>	IEEE802.1d <i>spanning tree</i> IEEE802.1w <i>rapid spanning tree</i> .
<b>Pro-Ring2s</b>	Поддерживает Pro-Ring2s. Поддерживает резервирование и время восстановления менее 20ms
<b>Quality of Service</b>	Качество обслуживания, определяемое портом, Tag и IPv4 Type of service (ToS), IPv4 Different Service (DS)
<b>Class of Service</b>	Поддерживает IEEE802.1p категорию обслуживания, каждый порт обеспечивает 4 приоритета очередей
<b>Port Security</b>	Поддерживает 100 вводов MAC адресов для статических MAC и другие 100 для фильтров MAC
<b>Port Mirror</b>	Поддерживает 3 типа зеркалирования: "RX, TX и Оба пакета".
<b>IGMP</b>	Поддерживает IGMP snooping v1,v2 – отслеживание 256многоадресных групп и запросов IGMP
<b>IP Security</b>	Поддерживает 10 IP адресов, которые имеют разрешение на доступ к управлению коммутатором, и предотвращает не санкционированный доступ.
<b>Login Security</b>	Поддерживает аутентификацию IEEE802.1X Authentication/RADIUS
<b>Bandwidth Control (Управление полосой частот)</b>	Поддерживает фильтр входящих пакетов(ingress packet) и ограничения на выходящие пакеты (egress packet). Управление скоростью выходящих пакетов поддерживает все типы пакетов и пределы скоростей 100К~102400Kbps(10/100). Комбинации настроек фильтра входящих пакетов: Broadcast/Multicast/Unknown Unicast пакеты; Broadcast/Multicast пакеты; Broadcast пакеты только и Все пакеты. Скоростью пакетов packet может быть настроена в диапазоне 100К~102400Kbps(10/100)
<b>Flow Control</b>	Поддерживает Flow Control для Full-duplex и Back Pressure для Half-duplex
<b>System Log</b>	Поддерживает запись в Системный архив (System log) и Сервер Удаленного Системного архива (Remote system log server)
<b>SMTP</b>	Поддерживает SMTP Server и 6 учетных записей e-mail для получения сообщений тревоги (event alert)
<b>Relay Alarm</b>	Содержит один релейный выход для сигнализации отказа порта, пропадания питания. Реле коммутирует ток: 1A @ DC24V
<b>SNMP Trap (Сообщения ловушек)</b>	1. Topology Change - Изменение топологии сети 2. Power Trap - Нарушения питания 3. MAC-Violation – Ошибки MAC адресов

<b>DHCP</b>	Содержит DHCP Client/ DHCP Server/ Port и IP Binding (связывание)
<b>DNS</b>	Обеспечивает свойства DNS Client и поддерживает Primary и Secondary DNS Server
<b>SNTP</b>	Поддерживает SNTP для синхронизации системного времени в Internet
<b>Firmware Update</b>	Поддерживает TFTP обновление Фирменного ПО, TFTP резервирование и восстановление.
<b>Configuration Upload/Download</b>	Поддерживает двоичный формат файла конфигурации для быстрой инсталляции системы.
<b>ifAlias</b>	Каждый порт позволяет импортировать 128bits из буквенной строки из слова на интерфейсе SNMP и CLI

### 1.3. Комплект поставки

Пожалуйста, ознакомьтесь с перечнем комплекта поставки, приведенным ниже, для последующей проверки комплектности поставки.

- ❖ 8 10/100TX Управляемый Промышленный Коммутатор – 1 шт.
- ❖ Руководство пользователя – 1 шт.
- ❖ Вставляемый клеммный блок – 1 шт.
- ❖ Монтажные пластины – 2 шт.
- ❖ Кабель RJ-45 - DB9-Female – 1шт.

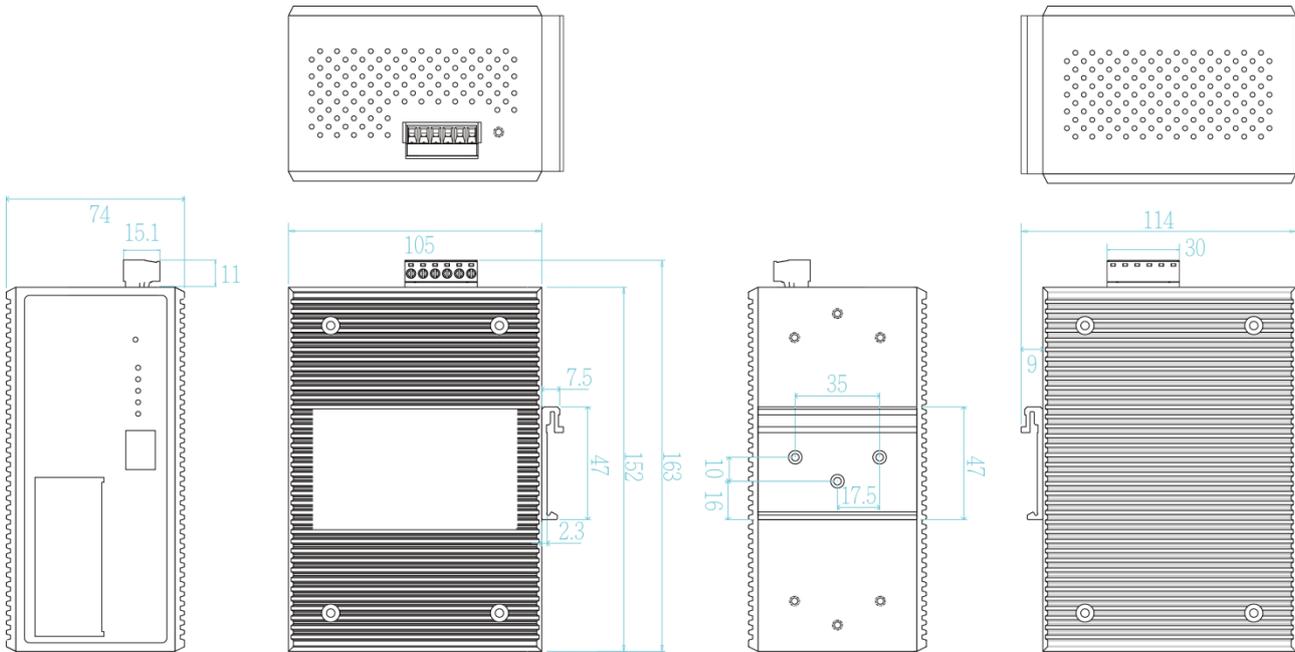
Если какой-либо компонент поврежден или отсутствует, то обратитесь к Вашему местному дилеру за поддержкой.

## Глава 2. Описание устройства

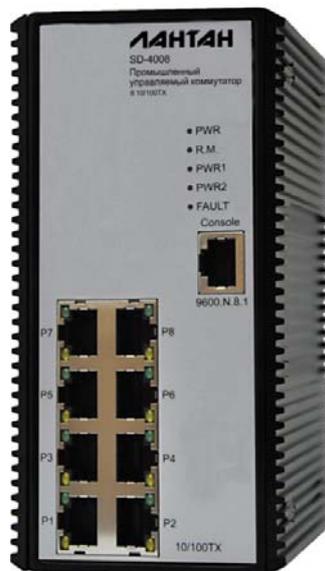
В этой главе приведено описание Промышленного коммутатора, спецификации, информация по подключению и монтажу.

### 2.1 Физические размеры

74мм x 105мм x 152мм (Ш x Г x В)

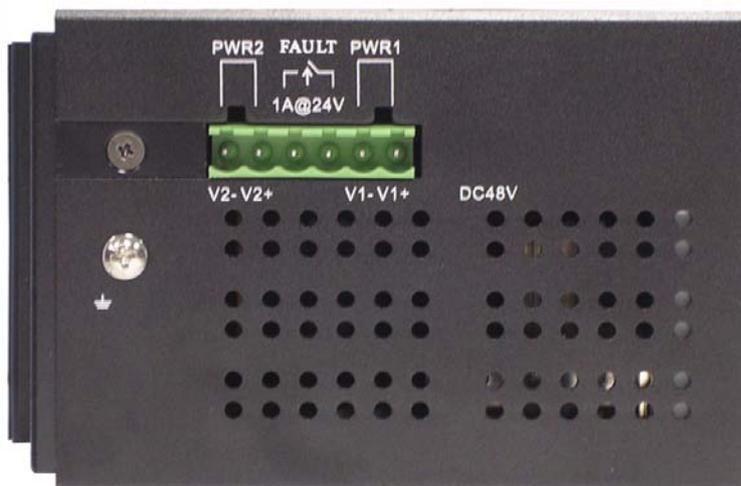


### 2.2 Лицевая панель



*Лицевая панель Промышленного Коммутатора*

### 2.3 Нижняя панель



Нижняя панель Промышленного Коммутатора

## 2.4 Диагностические светодиоды (LED)

LED	Цвет	Состояние	Значение
PWR	Green	Вкл.	Питание Коммутатора включено.
		Выкл.	Нет питания
R.M.	Green	Вкл.	Коммутатор является Главным (master) группы <b>Pro-Ring2s</b>
		Выкл.	Коммутатор не является Главным (master) группы <b>Pro-Ring2s</b>
PWR1	Green	Вкл.	Питание <b>Power 1</b> активно
		Выкл.	Питание <b>Power 1</b> не активно
PWR2	Green	Вкл.	Питание <b>Power 2</b> активно
		Выкл.	Питание <b>Power 2</b> не активно
FAULT	Red	Вкл.	Ошибка питания или порта
		Выкл.	Нет ошибок
P1 ~ P8	Green	Вкл.	Обнаружено сетевое устройство.
		Мигание	Порт передает или получает пакеты от TX устройства.
		Выкл.	Нет присоединенных устройств
	Amber	Вкл.	Порт в режиме полный дуплекс.
		Мигание	Наблюдается «Collision of Packets» - столкновение Пакетов.
		Выкл.	Порт в режиме полудуплекс или нет присоединенных устройств
FWD (P1~P8)	Green	Вкл.	Подключенное устройство использует питание по сети «Power over Ethernet» на порту.
		Выкл.	Нет подключенных устройств или отказ прохождения питания (power forwarding)

## **Глава 3. Монтаж устройства**

В этой главе, приведено описание монтажа Промышленного коммутатора на DIN-рейке или стене и способы его подключения.

### **3.1 Пошаговые действия по монтажу**

1. Распакуйте Промышленный коммутатор.
2. Проверьте, закреплено ли приспособление для монтажа «DIN-Rail» на Индустриальном Коммутаторе. Если «DIN-Rail» не смонтировано, прочтите следующий раздел главы: *Крепление на DIN-рейку*.
3. Если пользователь будет использовать настенный монтаж Промышленного Коммутатора, прочтите раздел этой главы: *Настенный монтаж Коммутатора*.
4. Закрепите Промышленный коммутатор на направляющей DIN-Rail или на стене.
5. Подключите питание на Промышленный коммутатор. Обратитесь к разделу: *Подключение питания*. Светодиод питания на коммутаторе загорится. Обратитесь к разделу: *Диагностические светодиоды(LED)*.
6. Подготовьте кабель категории 5 (витые пары) для подключения к сети Ethernet.
7. Вставьте одну сторону кабеля (категории 5) с коннектором RJ-45 в порт Ethernet коммутатора (RJ-45 порт) а другую сторону этого кабеля с коннектором RJ-45 в порт Ethernet сетевого устройства, например: Коммутатора ПК или Сервера. Светодиод порта UTP (RJ-45) на Промышленном коммутаторе загорится при подключении кабеля к сетевому устройству. Обратитесь к разделу: *Диагностические светодиоды(LED)*.

Когда все соединения установлены, и светодиоды всех устройств показывают нормальное состояние, установка Промышленного Коммутатора завершена.

---

**[ПРИМЕЧАНИЕ]** Убедитесь, что подключенные сетевые устройства поддерживают MDI / MDI-X. Если они не поддерживают, используйте перекрестный кабель (кроссовер).

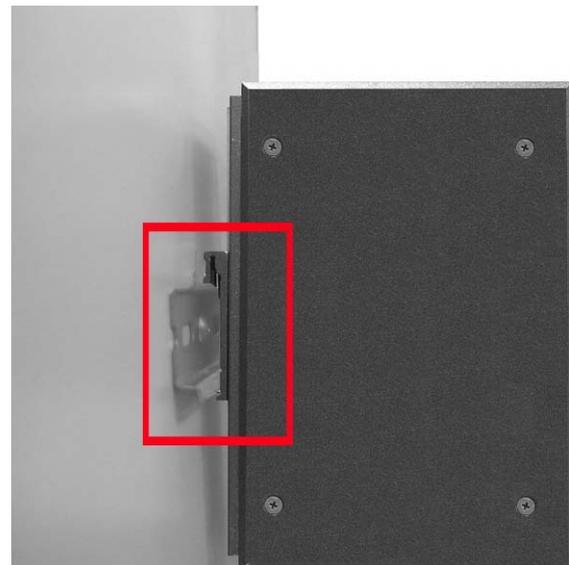
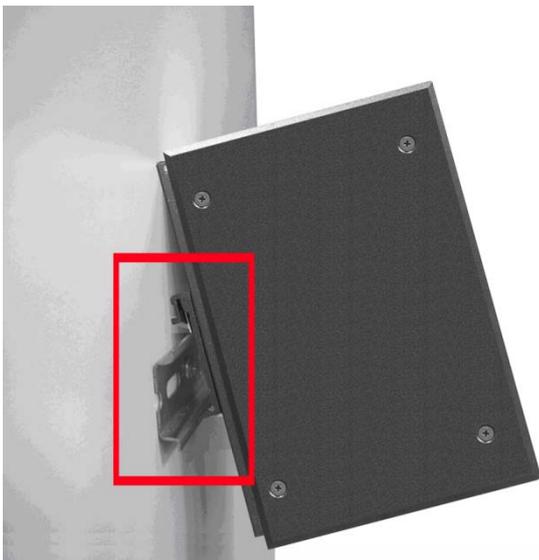
---

### 3.2 Крепление на DIN-рейку

Приспособление для монтажа «DIN-Rail» закреплено на Промышленном Коммутаторе при изготовлении. Если «DIN-Rail» не смонтировано на Промышленном Коммутаторе, обратитесь к следующим фотографиям, чтобы установить «DIN-Rail» на Коммутаторе. Выполните следующие шаги, чтобы смонтировать Промышленный коммутатор на направляющую DIN-рейку.



1. Во-первых, установите верхнюю часть «DIN-Rail» в направляющую.
2. Затем, легко нажмите на корпус, чтобы защелкнуть «DIN-Rail» на направляющей DIN рейке.



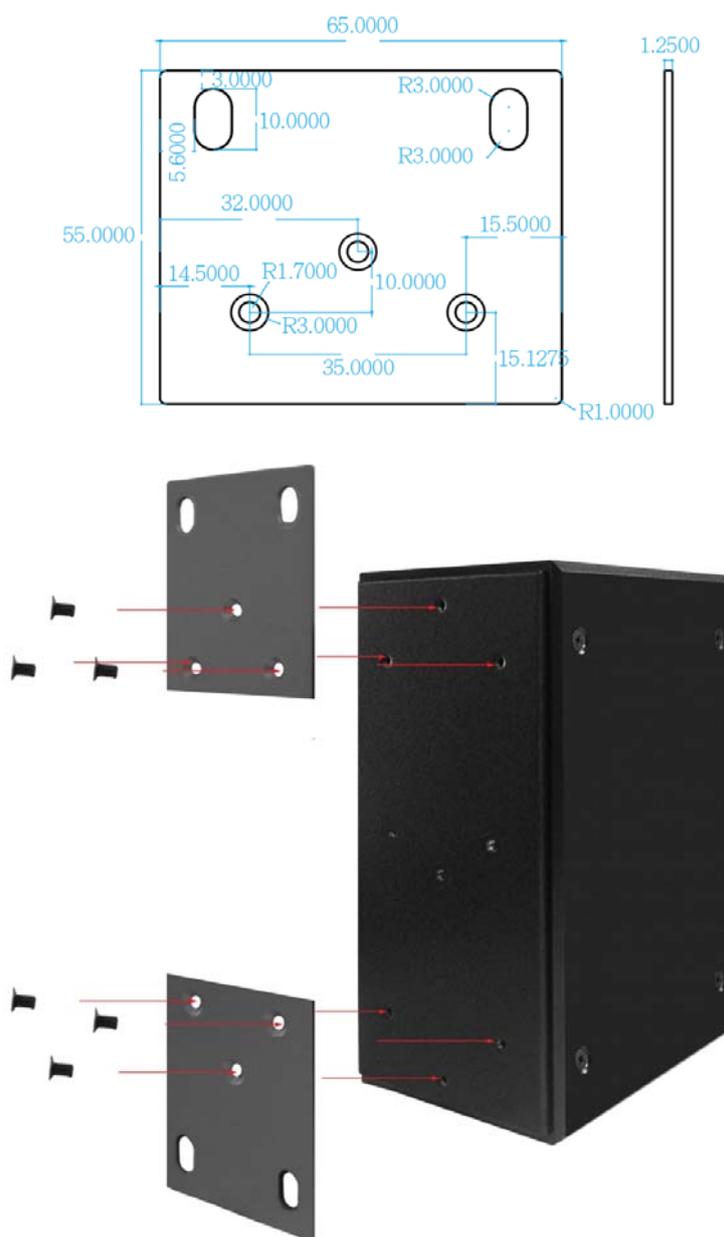
3. Убедитесь, что «DIN-Rail» Коммутатора закрепилась на направляющей.
4. Чтобы снять Коммутатор с направляющей сделайте эти действия в обратном направлении.

### 3.3 Настенный монтаж Коммутатора

Выполните следующие действия, чтобы прикрепить Промышленный коммутатор с пластинами для настенного крепления к стене:

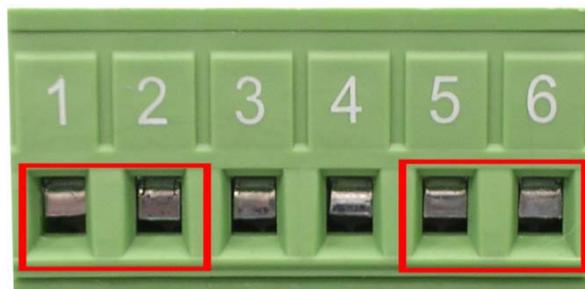
1. Снимите DIN-рейку с Промышленного коммутатора; не потеряйте винты при удалении DIN-рейки.
2. Поместите пластину настенного монтажа на задней панели Промышленного коммутатора.
3. Используя винты, закрепите пластины на Промышленном коммутаторе.
4. Используя отверстия в углах пластины настенного монтажа, повесьте Промышленный коммутатор на стене.
5. Чтобы снять пластины настенного монтажа, сделайте эти действия в обратном направлении.

**ПРИМЕЧАНИЕ:** Набор для крепления на стене приобретается отдельно.

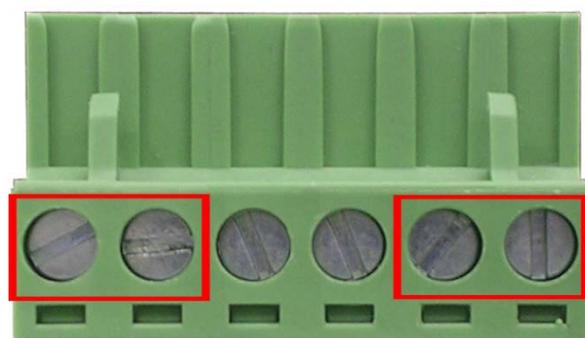


### 3.4 Подключение питания

Для подключения питания выполните следующие шаги:



1. Вставьте провода питания Постоянного тока (DC) в контакты **1** и **2** для «**Power 2**», или в **5** и **6** для «**Power 1**»



2. Закрепите провода от выпадания, подтянув винты.

---

**[ПРИМЕЧАНИЕ]** Калибр проводов для клеммной колодки должны быть в диапазоне между 12 ~ 24 AWG (0.25 – 4.0 мм кв)

---

### 3.5 Подключение контакта сигнализирующего об ошибке

Контакты сигнализации неисправности находятся в середине клеммного блока, как показано на рисунке. Когда Коммутатор обнаружит состояние сбоя питания или ошибку порта связи (доступно для управляемой модели), разрывает цепь контактов. На следующем рисунке показан пример подключения проводов к контактам сигнализации неисправности.

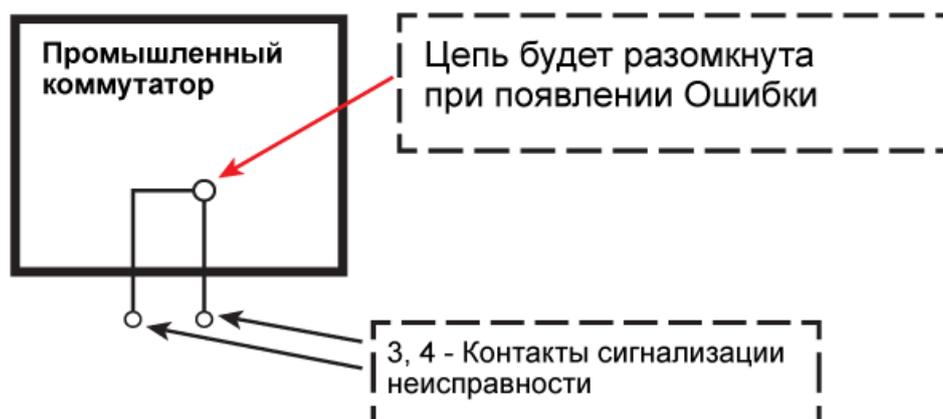


Вставьте провода в контакты сигнализации об ошибке «*fault alarm contacts*».

---

**[ПРИМЕЧАНИЕ]** Калибр проводов для клеммной колодки должны быть в диапазоне между 12 ~ 24 AWG (0.25 – 4.0 мм кв)

---

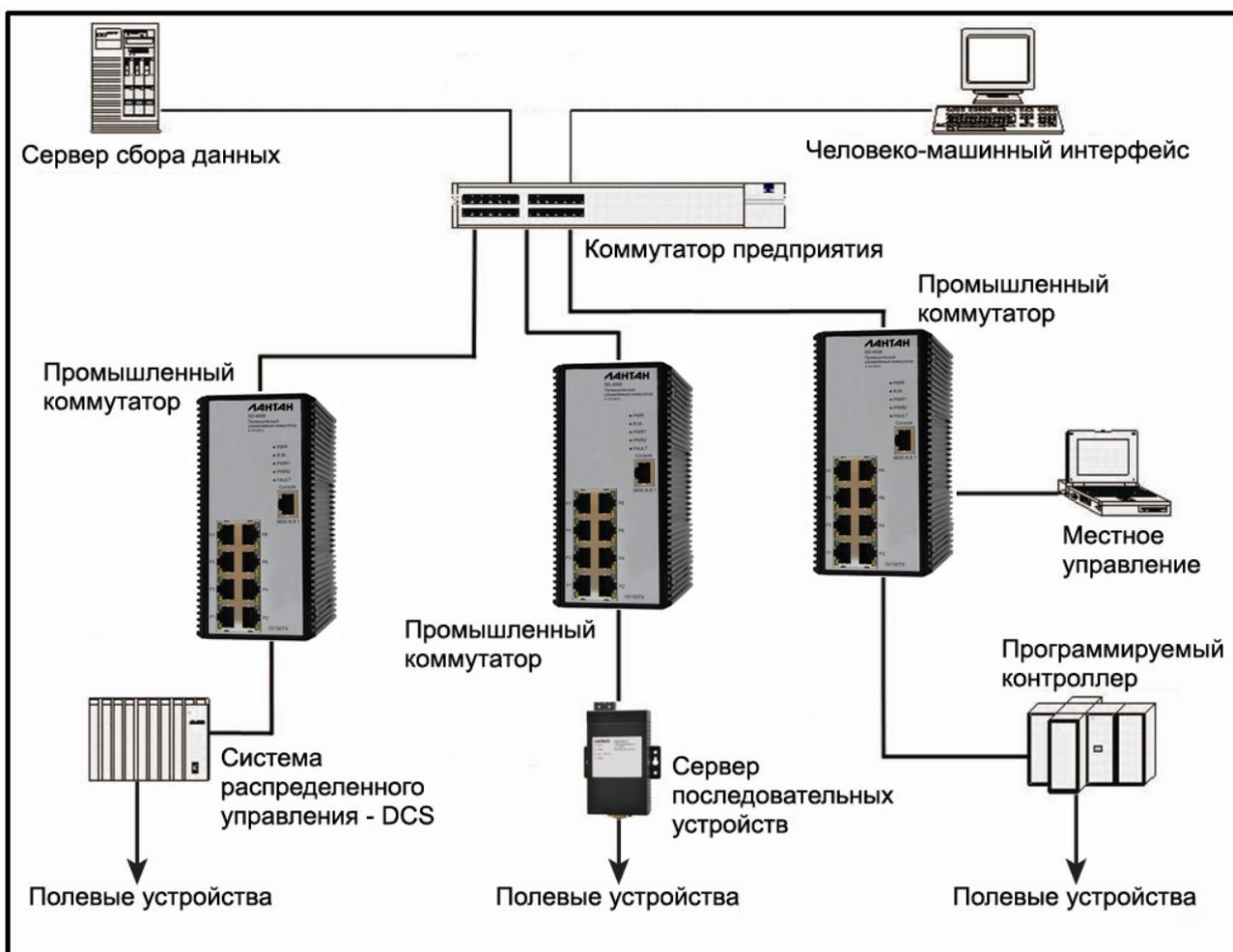


### 3.6 Подключение кабелей

Используйте четыре витые пары Категории 5 или выше для соединения с портом RJ-45. Кабели между коммутатором и другими участниками соединений (коммутаторы, концентраторы, рабочие станции и т.д.) должен быть не длиннее 100 метров (328 футов.).

В этой главе приведены некоторые примеры приложений, чтобы помочь пользователю понять возможности применения функции Промышленного коммутатора.

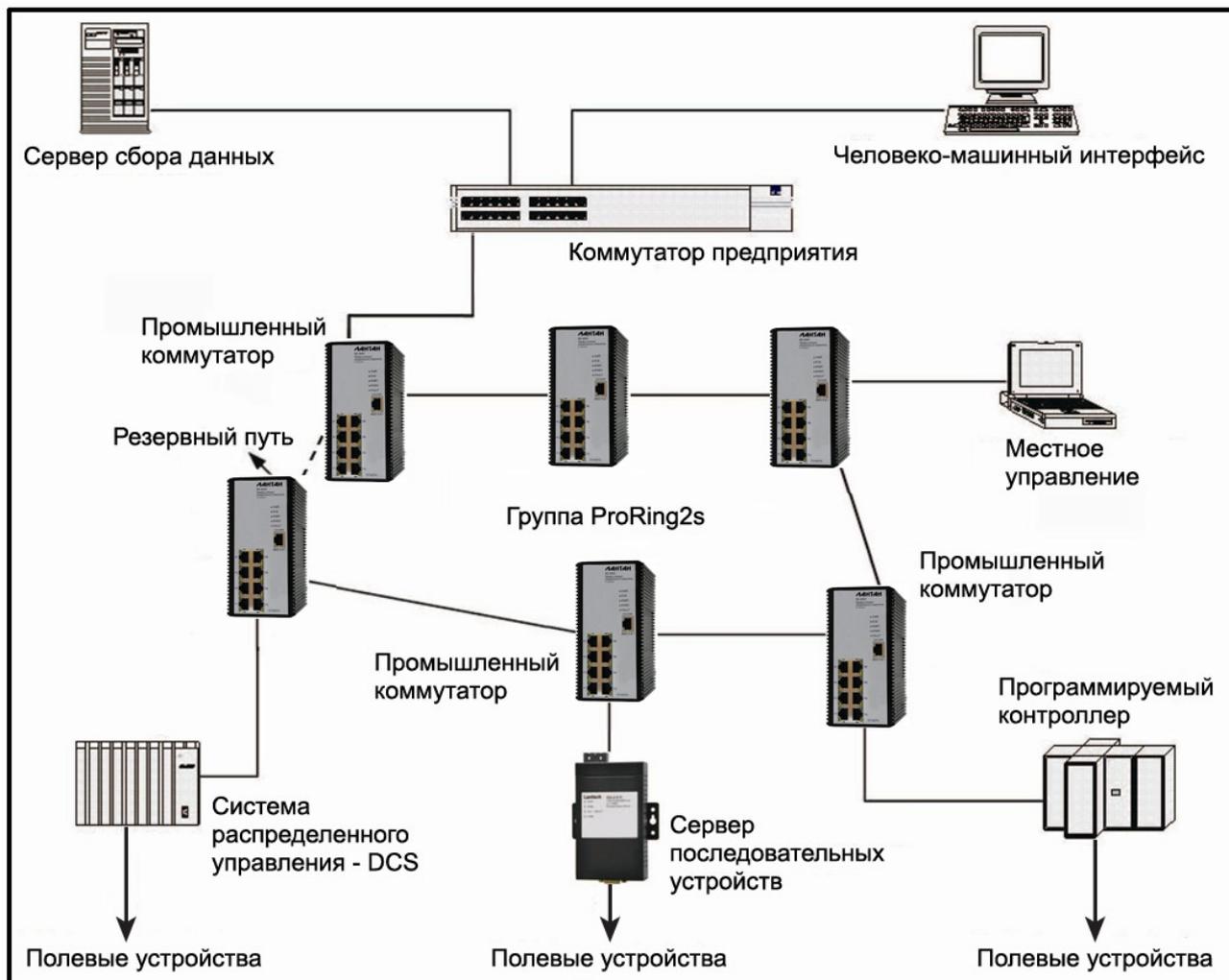
Один из примеров приложения с использованием Промышленного коммутатора, показан ниже:



### 3.7 Приложение *Pro-Ring2s*

**Pro-Ring II** является новым Кольцевым механизмом для Промышленных коммутаторов Lantech и Лантан, в которых устранена необходимость предварительной установке **Master switch** - Главного коммутатора (как это было в старом Pro-Ring) и использованы более безопасные топологии для защиты сети, чем ранее. **Pro-Ring II** работает как закольцованная цепь - Ring Chain, чтобы уменьшить риск отключения *Master switch*, при этом настройка становится гораздо легче.

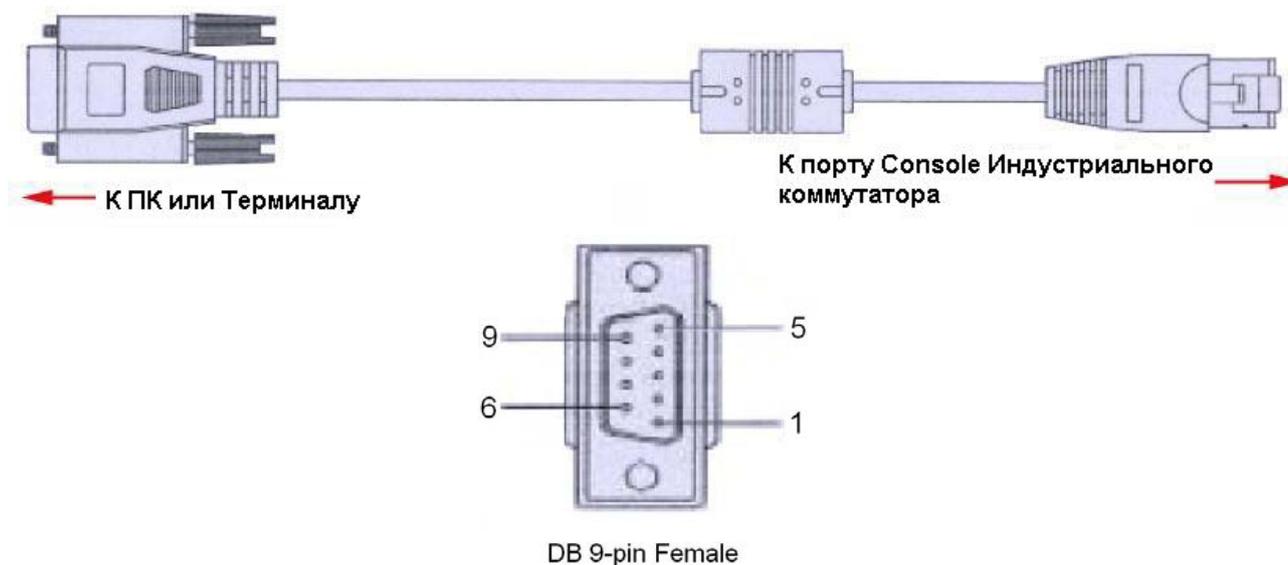
Pro-Ring II обратно совместим со старыми системами Pro-Ring с понижением классификации схем колец.



## Глава 4. Управление с консоли

### 4.1 Соединение с портом консоли (*Console Port*)

Прилагаемый кабель, на одном конце которого коннектор RS-232, а на другом конце коннектор RJ-45. Соедините коннектор RS-232 с разъемом ПК или терминала, а другой конец RJ-45 подсоедините к порту «**Console**» коммутатора. Подключенный терминал или компьютер должен поддерживать функцию эмуляции терминала.



### 4.2 Назначение контактов

DB9 Connector	RJ-45 Connector
Не подсоединен	1 Оранжевый / Белый
<b>2</b>	<b>2 Оранжевый</b>
<b>3</b>	<b>3 Зеленый/Белый</b>
Не подсоединен	4 Голубой
<b>5</b>	<b>5 Голубой/Белый</b>
Не подсоединен	6 Зеленый
Не подсоединен	7 Коричневый / Белый
Не подсоединен	8 Коричневый

### 4.3 Вход в интерфейс Консоли

Когда соединение между Коммутатором и ПК готово, включите компьютер и запустите программу эмуляции терминала или **Hyper Terminal** и настройте параметры связи, чтобы они соответствовали следующим характеристикам порта «Console» по умолчанию:

**Baud Rate: 9600 bps**

**Data Bits: 8**

**Parity: none**

**Stop Bit: 1**

**Flow control: None**



Окно настройки параметров коммуникации

Закончив настройку, нажмите «OK». Когда появится пустой экран, нажмите клавишу **Enter**, чтобы появилось окно входа. Введите «**root**» (значение по умолчанию) в качестве имени пользователя и пароля (используйте клавишу **Enter** для переключения), затем нажмите **Enter** и появится Главное меню управления консоли. Ниже показан экран входа в систему

```
User Name : root
Password  : ****
```

Интерфейс «Console login»

## 4.4 Управление при помощи команд *CLI*

Система поддерживает управление от консоли с помощью команд **CLI**. После того, как Вы вошли в систему, Вы увидите командную строку. Чтобы войти в интерфейс управления CLI, введите команду Разрешить - "**enable**".

```
switch>e  
switch#
```

*Интерфейс команд CLI*

## Глава 5. Web - Управление

В этой главе описаны настройка и функции **Web-Based** управления

### 5.1 Кратко об Web - управлении

Во флэш-памяти на плате ЦПУ Коммутатора размещен встроенный **HTML Web -caйм**, который предлагает расширенные функции управления и позволяет пользователям управлять Коммутатором из любой точки сети через стандартные браузеры, такие как *Microsoft Internet Explorer*.

Управление при помощи Веб-интерфейса (*Web-Based Management*) поддерживает **Internet Explorer версии 6.0** или более поздней версии. И оно применяется в *Java Applets* для снижения нагрузки на сеть, повышения скорости доступа и представляет простой экран просмотра.

### 5.2 Подготовка к Web - управлению

Перед использованием Веб-управления, установите Промышленный коммутатор в сети и убедитесь, что какой-либо из компьютеров в сети может подключиться к Индустриальному коммутатору через Веб-браузер.

Значения сетевых настроек Промышленного коммутатора по умолчанию перечислены ниже:

- IP Address: **192.168.16.1**
- Subnet Mask: **255.255.255.0**
- Default Gateway: **192.168.16.254**
- User Name: **root**
- Password: **root**

## 5.3 Вход в систему

1. Запустите Internet Explorer на ПК
2. Введите "HTTP: //" + " IP-адрес коммутатора", а затем нажмите кнопку "Enter".



3. Сразу появится экран входа - «Login»
4. Введите Имя пользователя и Пароль. Имя пользователя и Пароль по умолчанию те же самые «root»
5. Нажмите клавишу **Enter** или кнопку **OK**, появится главный экран управления веб-интерфейса.



Экран «Login»

## 5.4 Система

### 5.4.1 Основная информация о Коммутаторе: *General – Switch Information*

Здесь пользователь может найти системное имя, описание, местоположение и данные для контакта с персоналом для идентификации Коммутатора. В таблице показаны поля (только для чтения), содержащие основную информацию о Коммутаторе.

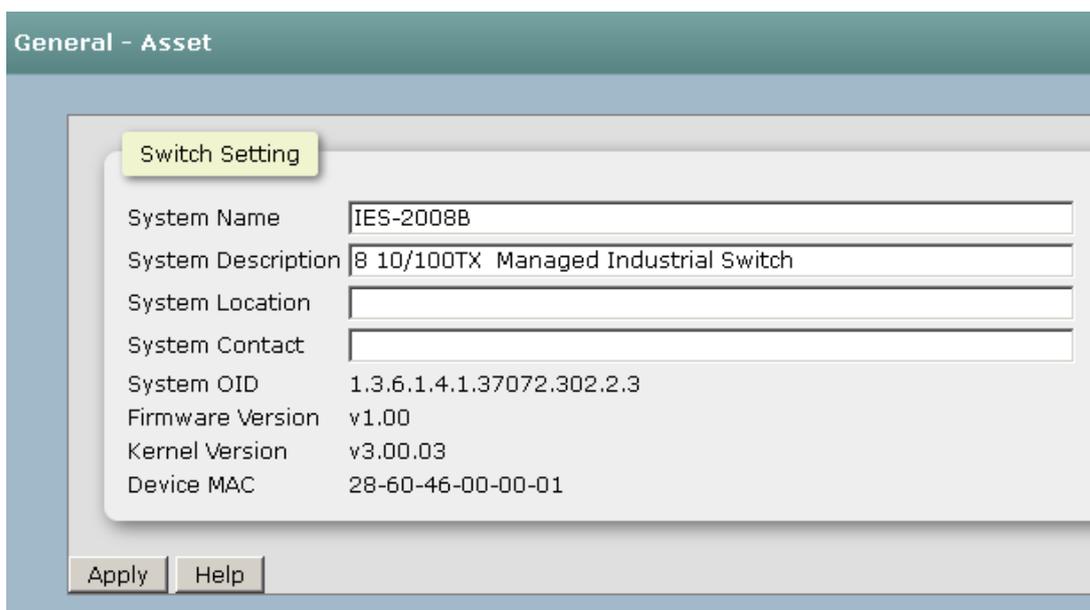
- **System Name:** Присвоенное системное имя Коммутатора (максимальная длина 64 байта).
- **System Description:** Описание Коммутатора.
- **System Location:** Присвоенное физическое местоположение Коммутатора (максимальная длина 64 байта).
- **System Contact:** Имя контактного лица или организации.
- **System OID:** Идентификатор SNMP OID Коммутатора.
- **Firmware Version:** Показывает версию прошивки коммутатора
- **Kernel Version:** Отображает версию программного ядра.
- **MAC Address:** Отображает уникальный аппаратный адрес, присвоенный производителем.

**General - Switch Information**

Switch Information	
System Name	IES-2008B
System Description	8 10/100TX Managed Industrial Switch
System Location	
System Contact	
System OID	1.3.6.1.4.1.37072.302.2.3
Firmware Version	v1.00
Kernel Version	v3.00.03
Device MAC	28-60-46-00-00-01
System Time	1970年1月1日 上午 12:15:47

### 5.4.2 Ресурсы: *General – Asset*

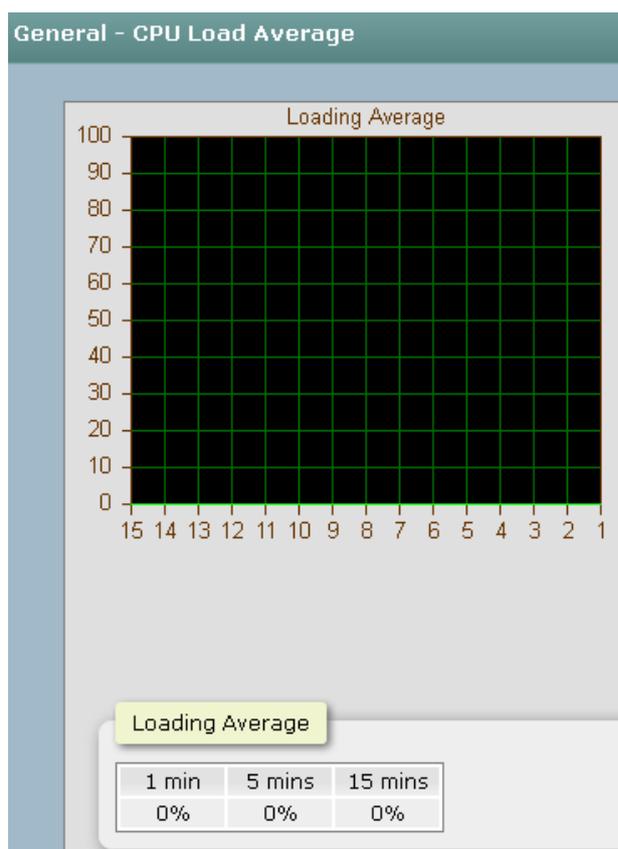
Здесь Вы можете изменить Имя системы, Описание, Местоположение и Контакты



Интерфейс настроек Коммутатора «Switch settings»

### 5.4.3 Средняя Загрузка ЦПУ: *General – CPU Load Average*

Если пользователь беспокоится о том, что "Может быть мой Коммутатор обрабатывает слишком много сетевых пакетов и поэтому пропускная способность сети уменьшается?". В этом случае можно использовать этот дисплей, чтобы увидеть степень загрузки центрального процессора коммутатора.



## 5.5 Время: *Time - SNTP*

SNTp (*Simple Network Time Protocol*) представляет собой упрощенную версию интернет-протокола NTP, который используется для синхронизации часов реального времени в компьютерах.

Потому что, как правило, время на разных станциях узла может отличаться, в программах обмена данными, работающих на этих узлах, это вызвало бы нежелательный эффект (переходы вперед и назад). Коммутатор предоставляет комплексные механизмы для доступа к национальному времени и частоте распространения услуг, организации синхронизации времени в подсети и применения локального времени в каждой участвующей точке подсети.

Летнее время (DST) это соглашение о переводе часов предназначенное, чтобы лучше использовать дневной свет. Обычно часы переводятся вперед на один час в начале весны и переводятся назад осенью.

- **SNTp Client:** Включение / выключение функции SNTp, чтобы получить время с сервера SNTp.
- **UTC Timezone:** Универсальное Координированное Время (*Universal Time Coordinated*). Установите зону часового пояса местоположения Коммутатора. В таблице на следующей странице перечислены различные временные зоны для справки
- **SNTp Sever Address:** IP-адрес сервера SNTp. Вы можете назначить IP-адрес местного сервера сетевого времени или IP-адрес сервера времени Интернет
- **Daylight Saving Time:** Используется для включения / выключения функции сохранения дневного света (периода и смещения). Пользователь может настроить: Daylight Saving Period и Daylight Saving Offset.
- **Daylight Saving Period:** введите даты начала и конца Летнего времени в формате: 'YYYYMMDD' и 'HH: MM '(оставьте пробел между 'YYYYMMDD' и 'HH: MM')
  - YYYYMMDD: восьмизначное число: год / месяц / день.
  - HH: MM: пятизначное число (включая двоеточие) час / минута.

Например, наберите '20070701 2:00' и '20071104 2:04' в два поля, соответственно, которые будут указывать, что DST начинается в 2:00 утра 11 марта 2007 и заканчивается в 2:00 утра 4 ноября 2007 года.

- **Daylight Saving Offset:** Для не американских и не европейских стран, укажите суммарное время экономии дневного света. Для этого, введите в соответствующем поле число минут в диапазоне от 0 до 720. То есть, Вы можете установить смещение до 12 часов
- Нажмите кнопку **Apply** - Применить, чтобы настройки вступили в силу (см. рисунок через страницу).

<b>Местная зона времени</b>	<b>Отличие от UTC</b>	<b>Время в 12:00 UTC</b>
November Time Zone	- 1 час	11
Oscar Time Zone	-2 часа	10
ADT - Atlantic Daylight	-3 часа	9
AST - Atlantic Standard EDT - Eastern Daylight	-4 часа	8
EST - Eastern Standard CDT - Central Daylight	-5 часов	7
CST - Central Standard MDT - Mountain Daylight	-6 часов	6
MST - Mountain Standard	-7 часов	5
PDT - Pacific Daylight		
PST - Pacific Standard ADT - Alaskan Daylight	-8 часов	4
ALA - Alaskan Standard	-9 часов	3
HAW - Hawaiian Standard	-10 часов	2
Nome, Alaska	-11 часов	1
CET - Central European FWT - French Winter MET - Middle European MEWT - Middle European Winter SWT - Swedish Winter	+1 час	13
EET - Eastern European, USSR Zone 1	+2 часа	14
BT - Baghdad, USSR Zone 2	+3 часа	15
ZP4 - USSR Zone 3	+4 часа	16
ZP5 - USSR Zone 4	+5 часов	17
ZP6 - USSR Zone 5	+6 часов	18
WAST - West Australian Standard	+7 часов	19
CCT - China Coast, USSR Zone 7	+8 часов	20
JST - Japan Standard, USSR Zone 8	+9 часов	21
EAST - East Australian Standard	+10 часов	22
GST - Guam Standard, USSR Zone 9		
IDLE - International Date Line NZST - New Zealand Standard NZT - New Zealand	+12 часов	Полночь

Time - SNTP

SNTP Client Setting

SNTP Client

UTC Timezone

SNTP Server Address

Daylight Saving Setting

Daylight Saving Time

Daylight Saving Period  /  /   ~  
 /  /

Daylight Saving Offset  (hours)

Интерфейс настройки SNTP «SNTP Configuration»

## 5.6 Учетная запись: Account - Admin

В целях безопасности Веб-управления измените Имя пользователя и Пароль

- **User name:** Введите Новое имя пользователя (По умолчанию: 'root')
- **New Password:** Введите Новый пароль (По умолчанию: 'root')
- **Confirm password:** Повторите Ввод Нового пароля
- И затем, нажмите **Apply** – Применить.

Account - Admin

Username & Password

User Name

New Password

Confirm Password

## 5.7 IP адресация: *IP Addressing – IPV4*

Коммутатор является сетевым устройством, которому необходимо назначить IP-адрес для того, чтобы идентифицироваться в сети. Пользователи должны выбрать способ присвоения IP-адреса Коммутатору.

- **DHCP Client:** Включить или выключить функцию *DHCP Client*. Когда функция *DHCP Client* включена, IP-адрес Коммутатору будет присвоен сетевым сервером DHCP. IP-адрес по умолчанию будет заменен IP-адресом, назначенным DHCP сервером. После того, как пользователь нажимает кнопку **Apply** - Применить, появится окно с сообщением о том, что при включении функции *DHCP Client*, текущий IP-адрес будет потерян и пользователь должен найти новый IP-адрес на сервере DHCP.
- **IP Address:** IP-адрес коммутатора, используемый в сети. Если функция *DHCP Client* включена, то коммутатор настроен, как клиент DHCP и сетевой сервер DHCP назначит IP-адреса коммутатору и отобразит его в этой колонке. Если функция *DHCP Client*, отключена, пользователь должен назначить IP-адрес вручную. IP-адрес по умолчанию: 192.168.16.1 .
- **Subnet Mask:** маска подсети IP-адреса. Если функция *DHCP Client* отключена, пользователь должен назначить маску подсети в этом поле колонки.
- **Gateway:** Сетевой шлюз коммутатора. Если функция *DHCP Client* отключена, пользователь должен назначить шлюз в этом поле колонки. По умолчанию Шлюз: 192.168.16.254.
- **DNS1:** Присвоенный основной (первичный) DNS IP-адрес.
- **DNS2:** Присвоенный вторичный DNS IP-адрес.
- Затем, нажмите кнопку **Apply** – Применить.

IP Addressing - IPV4

IP Setting

DHCP Client: Disable

IP Address: 192.168.16.2

Subnet Mask: 255.255.255.0

Gateway: 192.168.16.254

DNS1: 0.0.0.0

DNS2: 0.0.0.0

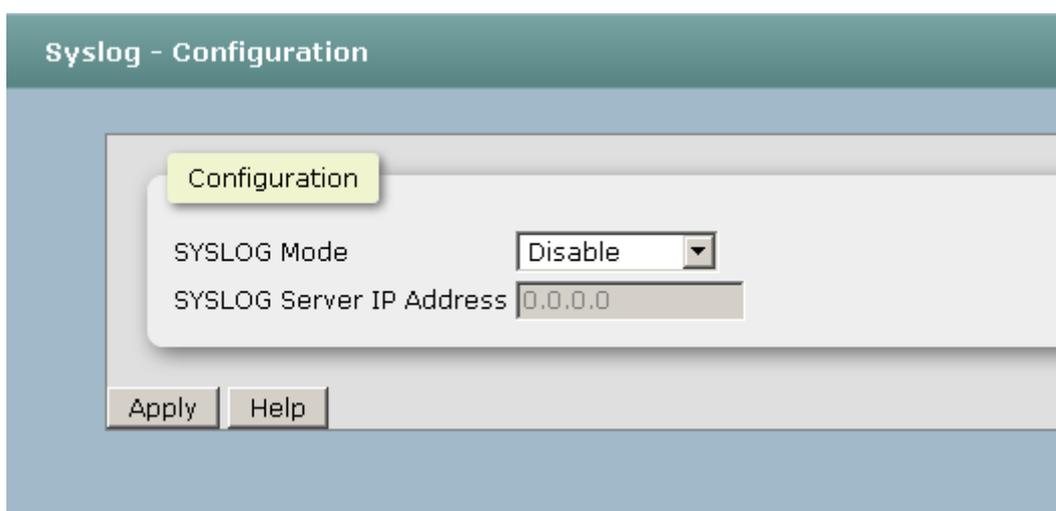
Apply Help

Интерфейс «IP Addressing»

## 5.8 Журнал Системы: Syslog

На этой странице пользователю может решить, отправлять ли журнал событий системы (system event log), и выбрать Режим (*Mode*), в котором журнал событий будет передаваться: только клиенту, только серверу, или клиенту и серверу. Какие виды журнала событий будут посылаться клиенту / серверу зависит от настроек в **Event Configuration**. Есть четыре типа событий для публикации в журнале событий: **Device Cold Start, Authentication Failure, X-Ring Topology Change, Port Event** (Холодный запуск устройства, Ошибка проверки подлинности, Изменение топологии X-кольца и События на порту).

### 5.8.1 Настройка Журнала Системы: Syslog Configuration



Интерфейс настройки журнала «Syslog Configuration»

- **Syslog Mode:** Выберите режим системного журнала - **Client Only**, **Server Only**, или **Both**. **Client Only** (Только Клиенту) означает, что журнал событий будет передаваться только на этот интерфейс Коммутатора, с другой стороны **Server Only** (Только серверу) означает, что системный журнал будет отправлен только удаленному серверу системного журнала с назначенным IP-адресом. Если режим установлен в **Both** (В оба адреса), журнал системных событий будут отправлен на удаленный сервер и данный интерфейс.
- **Syslog Server IP Address:** Когда режим "Syslog Mode" установлен, как **Server Only / Both**, пользователь должен назначить IP-адрес сервера системного журнала, по которому журнал будет отправлен.
- Убедитесь в том, что выбранный режим является правильным, и нажмите кнопку **Apply** – Применить, чтобы настройка вступила в силу.

## 5.9 Настройка SNMP: *SNMP Configuration*

Простой протокол сетевого управления (Simple Network Management Protocol) SNMP это протокол, разработанный для управления узлами IP-сети (серверами, рабочими станциями, маршрутизаторами, коммутаторами, концентраторами и т.д.). SNMP позволяет сетевым администраторам управлять работой сети, находить и решать проблемы сети и планировать развитие сети. Системы управления сетью узнают о проблемах по получению сообщений «traps» ловушек или уведомления об изменениях от сетевых устройств, реализующих SNMP.

### 5.9.1 Агент: *SNMP - Agent*

- **SNMP Mode:** Выберите версию SNMP (**V1 / V2c** или **V3**), которую Вы хотите использовать и нажмите кнопку **Change** - Изменить, чтобы перейти к выбранному режиму версии SNMP.
- **SNMP V1V2c Community:** Здесь вы можете определить новую строку сообщества и удалить нежелательные строки сообществ:
  - **Community String:** Заполните строку имени сообщества.
  - **Privilege: Read only** (Только чтение). Разрешает запросы со строкой имени сообщества для отображения информации MIB-объекта.  
**Read/write** (Чтение / запись). Разрешает запросы со строкой имени сообщества для отображения информации MIB-объекта и настройки объектов MIB.
- Нажмите, **Apply** –применить

Community String	Privilege
public	Read Only
private	Read and Write
	Read Only
	Read Only

Интерфейс «SNMP Agent Configuration»

## 5.9.2 Настройка ловушек SNMP: *SNMP Trap Configuration*

**Trap manager** (Менеджер ловушек) – это станция управления, которая принимает сообщения - *trap messages*, генерируемые Коммутатором. Если не определен никакой *Trap manager*, ловушки не будут использованы. Чтобы определить Станцию управления в качестве *Trap manager*, назначьте IP-адрес, введите строку SNMP сообщества и выберите *Trap*-версию SNMP.

- **Server IP:** Введите IP-адрес *Trap manager*.
- **Community:** Введите строку сообщества для *Trap* – станции.
- **Trap Version:** Выберите тип *Trap*-версии -**v1** или **v2c** SNMP.
- Нажмите кнопку **Add** – Добавить.
- Для удаления строки сообщества, выберите строку сообщества, указанную в текущем Менеджере и нажмите кнопку Удалить – **Remove**.

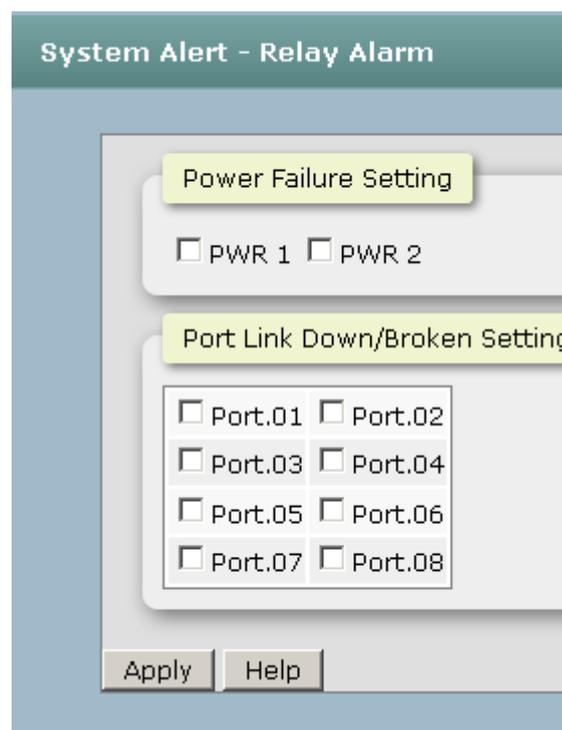
The screenshot shows a web-based configuration interface for SNMP traps. The title bar reads "SNMP - Trap". Below the title bar, there are two main panels. The first panel, titled "Trap Server Setting", contains three input fields: "Server IP", "Community", and "Trap Version". The "Trap Version" field has two radio buttons, "v1" (which is selected) and "v2c". Below these fields is an "Add" button. The second panel, titled "Trap Server Profile", contains a table with three columns: "Server IP", "Community", and "Trap Version". The table is currently empty. Below the table is a "Remove" button. At the bottom left of the interface is a "Help" button.

Интерфейс «Trap Managers»

## 5.10 Реле тревог: **System Alert - Relay Alarm**

Функция Реле аварийной сигнализации (**Fault Relay Alarm**) обеспечивает сигнализацию нарушений электроснабжения и ошибок порта: Пропадание соединения / обнаружение обрыва (**Port Link Down/Broken**). Когда на обоих входах: вход питания 1 и вход питание 2, установлены флажки-галочки (PWR 1 / PWR 2), то светодиодный индикатор неисправности (FAULT LED) будет загораться при отказе на одном из входов питания. Так же и при ошибках на портах (**Port Link Down/Broken**) светодиод FAULT LED будет загораться; если был установлен флажок-галочка рядом с соответствующим портом (Port.01 - Port.08). В разделе «Подключение контакта сигнализирующего об ошибке» приведена схема соединений для обнаружения неисправности.

- **Power Failure Setting:** Установите флажок в соответствующем поле, чтобы включить функцию индикации ошибки (FAULT LED) на панели при пропадании питания.
- **Port Link Down/Broken Setting:** Установите флажок в соответствующем поле, чтобы включить функцию индикации ошибки (FAULT LED) на панели при пропадании соединения / обнаружении обрыва.



Интерфейс «Fault Relay Alarm»

### 5.10.1 Системные тревоги: **System Alert – SMTP**

Simple Mail Transfer Protocol - Простой протокол передачи почты (SMTP) является стандартом для передачи электронной почты по сети. Вы можете настроить IP сервера SMTP, тему сообщения, отправителя, почтовый аккаунт, пароль и адрес получателя электронной почты, которому будет послано сообщение о тревоге. Есть пять типов событий: Device Cold Start, Authentication Failure, X-Ring Topology Change, Port Event (Холодный запуск устройства, Ошибки идентификации, Изменение топологии X-кольца, События на Порту), которые могут быть использованы, как сигнал тревоги. Кроме того, эта функция обеспечивает механизм аутентификации (опознания) в том числе аутентификацию, при которой клиент регистрируется на SMTP-сервер в процессе отправки сообщения о тревоге электронной почтой.

- **Email Alert:** Если эта функция включена, пользователь может настроить детали отправки уведомлений электронной почтой в SMTP-сервер, когда произойдет событие.
- **SMTP Server IP:** IP-адрес почтового сервера (Эта функция будет доступна, если функция *Email Alert* включена)
- **Sender Email Address (E-mail адрес Отправителя):** Введите псевдоним (*alias*) коммутатора в полный адрес электронной почты, например `switch101@123.com`, чтобы указать, откуда пришло сообщение.
- **Mail Subject:** Введите тему сообщения E-mail.
- **Authentication:** После пометки галочкой этого поля, будут показаны поля учетной записи электронной почты, пароля, подтверждения пароля. Настройте учетную запись электронной почты и пароль для идентификации, для регистрации коммутатора на SMTP-сервере.
- **Mail Account:** Учетная запись электронной почты, например, `johnadmin`, для получения сообщений по электронной почте. Это должна быть существующая на почтовом сервере учетная запись электронной почты.
- **Password:** Пароль для учетной записи электронной почты.
- **Confirm Password:** Подтверждение пароля.
- **Rcpt e-mail Address 1 ~ 6 (Адреса получателей):** Вы можете, также, записать в соответствующие поля до 6 учетных записи электронной почты получателей сообщений по электронной почте.
- Нажмите кнопку **Apply** - Применить, чтобы настройки вступили в силу.

**System Alert - SMTP**

**SMTP Setting**

E-mail Alert :

SMTP Server Address

Sender E-mail Address

Mail Subject

Authentication

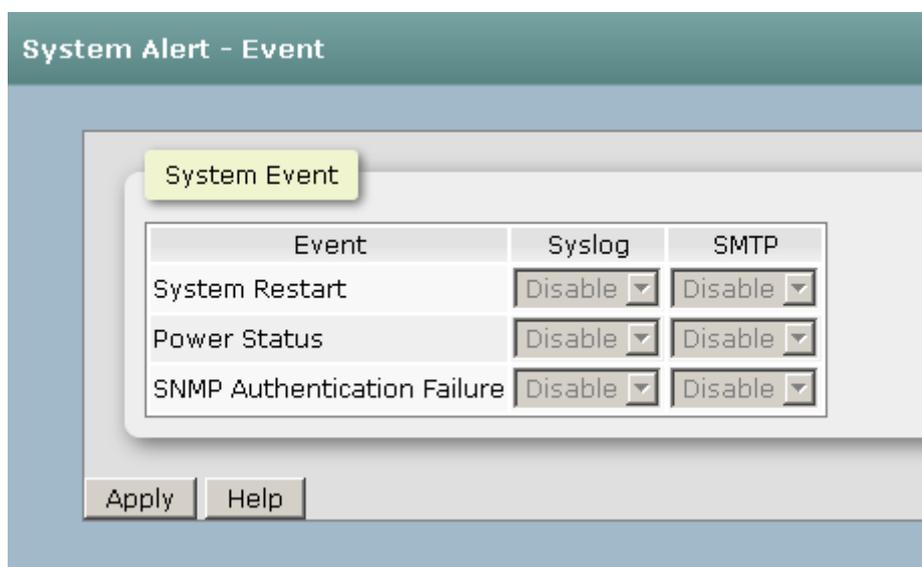
**Recipient E-mail Setting**

E-mail Address 1	<input type="text"/>
E-mail Address 2	<input type="text"/>
E-mail Address 3	<input type="text"/>
E-mail Address 4	<input type="text"/>
E-mail Address 5	<input type="text"/>
E-mail Address 6	<input type="text"/>

### 5.10.2 Системные тревоги – События: *System Alert – Event*

После пометки в поле **Syslog / SMTP**, запись о событии / сообщение E-mail о тревоге будет отправляться в сервер системного журнала и SMTP сервер, соответственно. Кроме того, запись о событии на Порту/ сообщение E-mail о тревоге (связь установлена, связь пропала, или оба события) могут быть отправлены на сервер системного журнала / SMTP-сервер, соответственно, при настройке условия запуска.

- **System event:** Выбор системных событий: Есть 3 типа событий - Холодный старт устройства, Ошибка идентификации, Изменение топологии X-кольца. Поля для пометок не доступны, если не активированы в первую очередь - режим **Syslog Client Mode** в закладке **Configuration Syslog** и **Email Alert** в закладке **Configuration SMTP**.
  - **System Restart:** Когда устройство выполняет холодный старт, то система пересылает запись о событии / сообщение E-mail в системный журнал / SMTP-сервер.
  - **Power Status:** Когда потребляемая мощность по PoE нестабильная, система пересылает запись о событии / сообщение E-mail в системный журнал / SMTP-сервер, соответственно.
  - **SNMP Authentication Failure:** Когда не удастся SNMP-аутентификации, система выдаст запись события / сообщение E-mail в системный журнал / SMTP-сервер, соответственно.



Интерфейс «Event Configuration»

## 5.11 Сервер *DHCP*

DHCP – это аббревиатура Dynamic Host Configuration Protocol (Протокол динамического конфигурирования хоста – узла). Этот протокол используется для назначения динамических IP-адресов устройствам в сети. При динамической адресации Устройство может иметь различные IP-адреса при каждом подключении к сети. В некоторых системах IP-адрес устройства может быть изменен даже в то время, когда устройство все еще подключено. DHCP также поддерживает смешение статических и динамических IP-адресов. Динамическая адресация упрощает администрирование сети, так как программа отслеживает IP-адреса, не требуя управления от администратора. Это означает, что новый компьютер может быть добавлен к сети без ручного назначения уникального IP-адреса.

Система содержит функцию ***DHCP Server***. При включении функции ***DHCP Server***, система коммутатора будет настроена, как сервер DHCP.

### 5.11.1 Конфигурация сервера: *DHCP Server*

- **DHCP Server:** Включение или отключение функции DHCP Server. *Enable* - Коммутатор будет DHCP-сервером в локальной сети.
- **Start IP Address:** Введите в IP-адрес. Нижний IP адрес является началом динамического диапазона IP-адресов. Например, динамический IP-адрес находится в диапазоне между 192.168.16.100~ 192.168.16.200. 192.168.16.100 является нижним IP адресом.
- **End IP Address:** Введите в IP-адрес. Верхний IP- адрес является концом динамического диапазона IP-адресов. Например, динамический IP-адрес, находится в диапазоне между 192.168.16.100 ~192.168.16.200. 192.168.16.200 является верхним IP адресом.
- **Subnet Mask:** Введите маску подсети.
- **Gateway:** Введите IP-адрес шлюза в сети.
- **DNS:** Введите имя домена сервера IP-адрес в сети.
- **Lease Time (Час):** Это период времени, через который система восстанавливает назначение динамического IP-адреса, чтобы убедиться в том, что динамический IP-адрес не был занят в течение длительного времени или что сервер не знает, что динамический IP свободный.
- А потом, нажмите кнопку ***Apply*** - Применить.



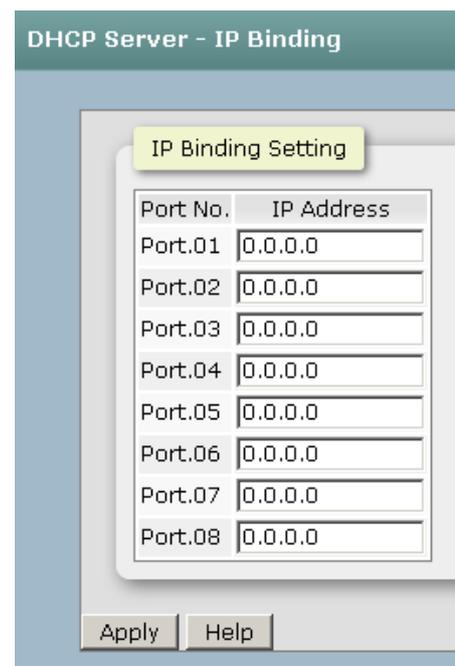
### 5.11.2 Таблица клиента - *Client Table*

Когда функция **DHCP Server** включена, система будет собирать информацию о DHCP-клиенте, включая назначенный IP-адрес, MAC-адрес, тип назначения IP, статус и время аренды (*lease time*).



### 5.11.3 Привязки - *IP Bindings*

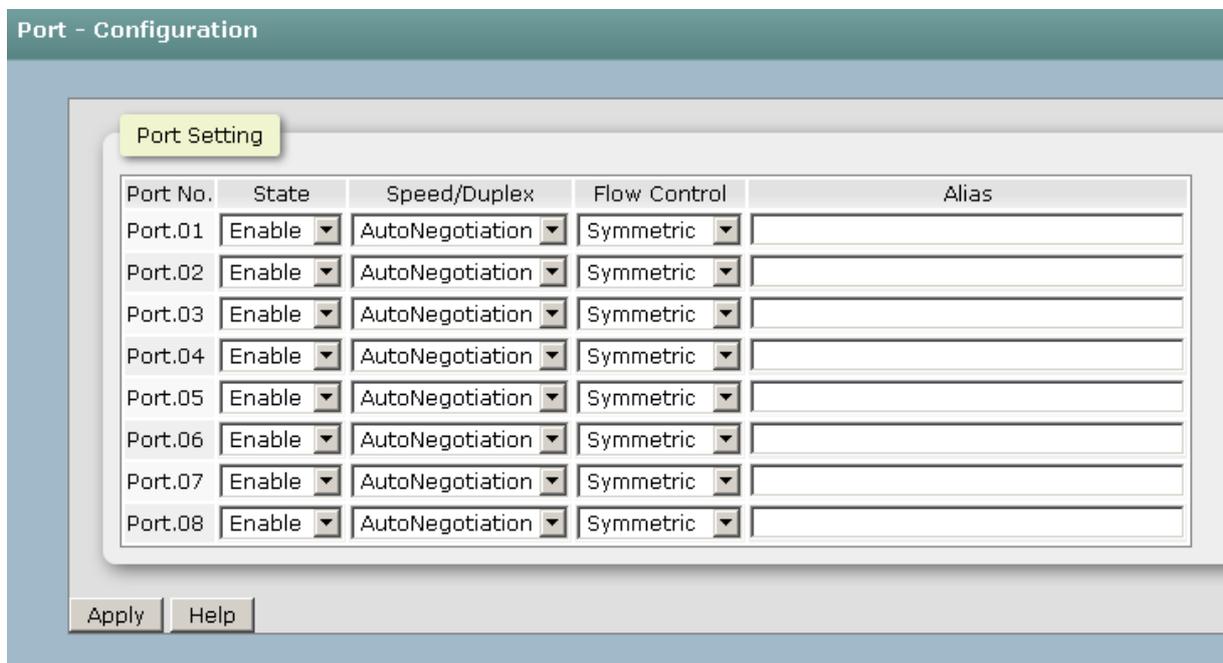
Связывают динамический IP-адрес с портом для подключения клиента. Пользователю разрешено заполнить каждый столбец порта одним конкретным IP-адресом. Когда устройство подключается к порту и запрашивает присвоение IP-адреса, система присвоит IP-адрес, привязанный к порту



## 5.12 Настройка порта: Port – Configuration

В окне **Port – Configuration** Вы можете настроить параметры каждого порта для управления параметрами соединения и статусом каждого порта (см. список ниже).

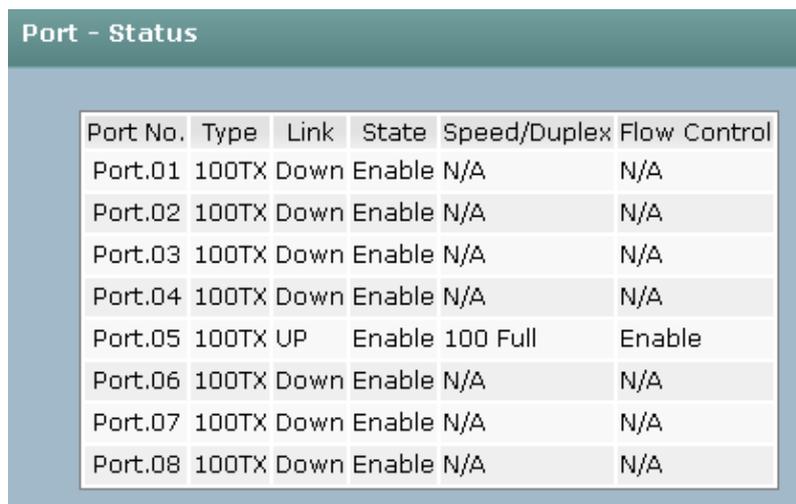
- **Port No.:** Номер порта, который вы хотите настроить.
- **State:** Текущее состояние порта. Порт может быть установлен в режим отключенный или включенный. Если состояние порта установлено, как "Disable", он не будет получать или отправлять никакие пакеты.
- **Speed/Duplex:** Можно настроить, как «auto» или задать скорость и тип передачи вручную.
- **Flow Control:** Управление потоком данных: Настоящий пункт определяет - будет или нет принимающий узел создавать обратную связь с посылающим узлом. Если эта функция включена, то, как только передающее устройство превысит входную скорость приема данных, приемное устройство будет посылать кадр PAUSE (паузы), который остановит передачу отправителю на определенный период времени. При отключении функции, принимающее устройство будет отбрасывать пакеты, если их слишком много для обработки
- **Aliases:** Описание для каждого порта, чтобы менеджер мог узнать устройства, подключенные к каждому порту, оно будет показано утилитой NMS (Network Management System).
- Нажмите кнопку **Apply** - Применить, чтобы настройки вступили в силу.



Интерфейс «Port Configuration»

## 5.13 Состояние порта - *Port Status*

В этом окне отображено состояние настроек портов



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	UP	Enable	100 Full	Enable
Port.06	100TX	Down	Enable	N/A	N/A
Port.07	100TX	Down	Enable	N/A	N/A
Port.08	100TX	Down	Enable	N/A	N/A

## 5.14 Статистика порта - *Port Statistics*

В окне *Port Statistics* отображается текущая статистическая информация, которая показывает состояние передачи пакетов в режиме реального времени для каждого порта. Пользователь может использовать эту информацию для планирования сети, проверки и обнаружения проблем, когда происходят столкновения, связанные с интенсивным обменом (*heavy traffic*).

- **Port:** Номер порта.
- **Type:** Отображает тип текущей скорости на порту.
- **Link:** Состояние связи: 'Up' – рабочее или 'Down' - простой.
- **State:** Настраивается в окне управления портом. Когда состояние - Отключено, порт не будет передавать или получать никаких пакетов.
- **Tx Good Packet:** Число переданных хороших пакетов через этот порт.
- **Tx Bad Packet:** Число плохих пакетов переданных через этот порт (в том числе отсеянных по размеру [меньше чем 64 октетов], большого размера, с ошибками CRC, фрагменты и сбойные (*Jabbers*) пакеты).
- **Rx Good Packet:** Число полученных хороших пакетов через этот порт
- **Rx Bad Packet:** Число полученных через этот порт плохих пакетов (в том числе отсеянных по размеру [меньше чем 64 октетов], большого размера, с CRC ошибками, фрагменты и сбойные (*Jabbers*) пакеты).
- **Tx Abort Packet:** Число прерванных при передаче пакетов.
- **Packet Collision:** Число столкновений пакетов.
- **Packet Dropped:** Число сброшенных пакетов.
- **Rx Bcast Packet:** Число широковещательных (*broadcast*) пакетов.
- **Rx Mcast Packet:** Число групповых (*multicast*) пакетов.
- Нажмите кнопку **Clear** - Очистить, чтобы очистить показания всех счетчиков.

Port - Port Statistic

Port	Type	Link	State	TX Good Packet	TX Bad Packet	RX Good Packet	RX Bad Packet	TX Abort Packet	Packet Collision	Drop Packet	RX Bcast Packet	RX Mcast Packet	TX Mcast Packet
Port.01	100TX	Down	Enable	0	0	0	0	0	0	0	0	0	0
Port.02	100TX	Down	Enable	0	0	0	0	0	0	0	0	0	0
Port.03	100TX	Down	Enable	0	0	0	0	0	0	0	0	0	0
Port.04	100TX	Down	Enable	0	0	0	0	0	0	0	0	0	0
Port.05	100TX	Up	Enable	3677	0	6910	0	0	0	0	8	0	43
Port.06	100TX	Down	Enable	0	0	0	0	0	0	0	0	0	0
Port.07	100TX	Down	Enable	13	0	73	0	0	0	0	58	2	13
Port.08	100TX	Down	Enable	0	0	0	0	0	0	0	0	0	0

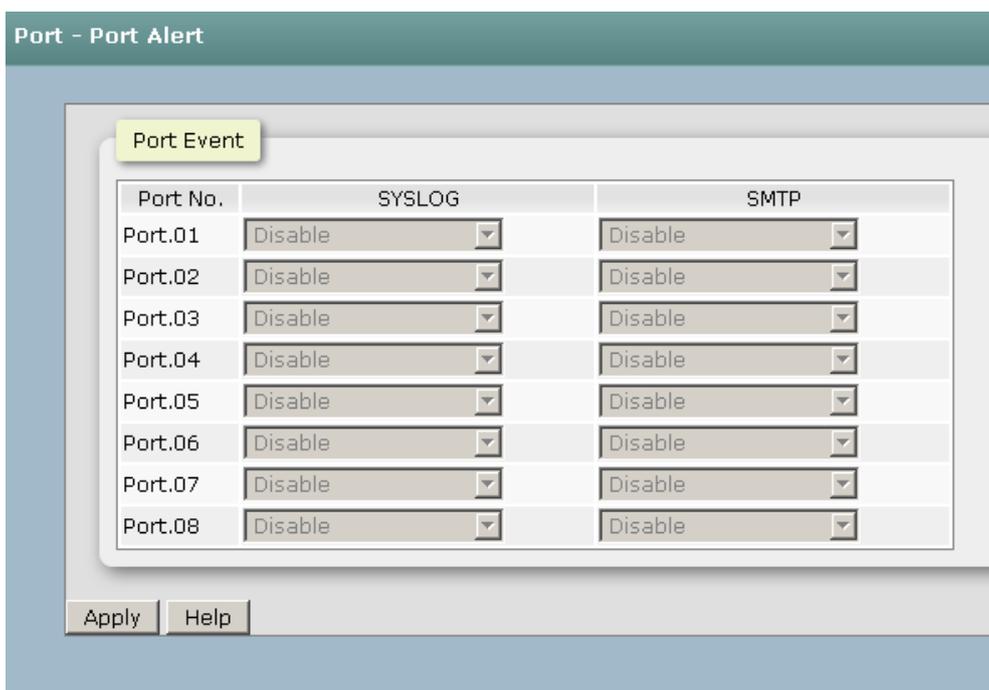
Clear Help

Интерфейс «Port Statistics»

## 5.15 Тревоги на порту - *Port – Port Alert*

После пометки в поле **Syslog / SMTP**, запись о событии / сообщение E-mail о тревоге будет отправляться в сервер системного журнала и SMTP сервер, соответственно. Кроме того, запись о событии на Порту/ сообщение E-mail о тревоге (связь установлена, связь пропала, или оба события) могут быть отправлены на сервер системного журнала / SMTP-сервер соответственно, при настройке условия запуска.

- **Выбор системных событий:** Есть 3 типа событий - Холодный старт устройства, Ошибка идентификации, Изменение топологии X-кольца. Поля для пометок не доступны, если сначала не активирован режим - **Syslog Client Mode** в закладке **Configuration** и **E-mail Alert** в закладке **SMTP Configuration**.
  - **Device cold start:** Когда устройство выполняет холодный старт, то система выдает запись о событии / сообщение по электронной почте в системный журнал / SMTP-сервер соответственно.
  - **Authentication Failure:** Когда не удастся идентификация SNMP, система выдает запись о событии / сообщение по электронной почте в системный журнал / SMTP-сервер соответственно.
  - **MAC Violation:** Когда нарушен MAC-адрес, система выдает запись о событии / сообщение по электронной почте в системный журнал / SMTP-сервера соответственно.
- **Port event selection:** Для доступа к пунктам выпадающего меню, сначала необходимо активировать режим - **Syslog Client Mode** в закладке **Configuration** и **E-mail Alert** в закладке **SMTP Configuration**. Пункты выпадающего меню: **Link UP**, **Link Down**, **Link UP & Link Down**. Если пункт деактивирован сообщений по соответствующему событию не будет посылаться в системный журнал / SMTP-сервер.
  - **Link UP:** Система выдает сообщение только при активации соединения.
  - **Link Down:** Система выдает сообщение только при отказе соединения.
  - **Link UP & Link Down:** Система выдает сообщение при активации и отказе соединения.

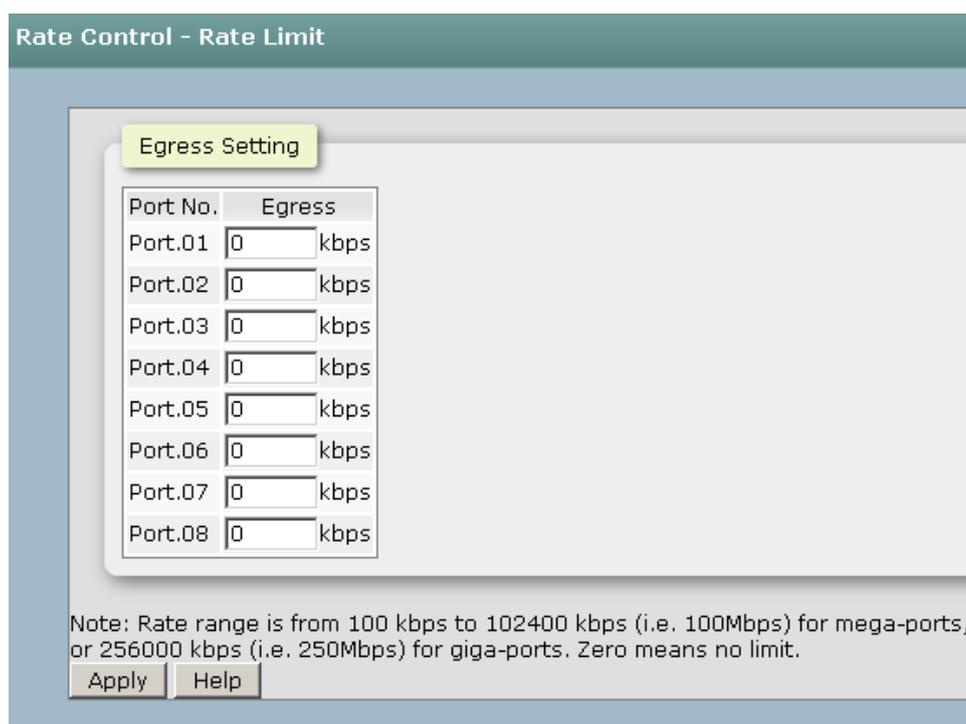


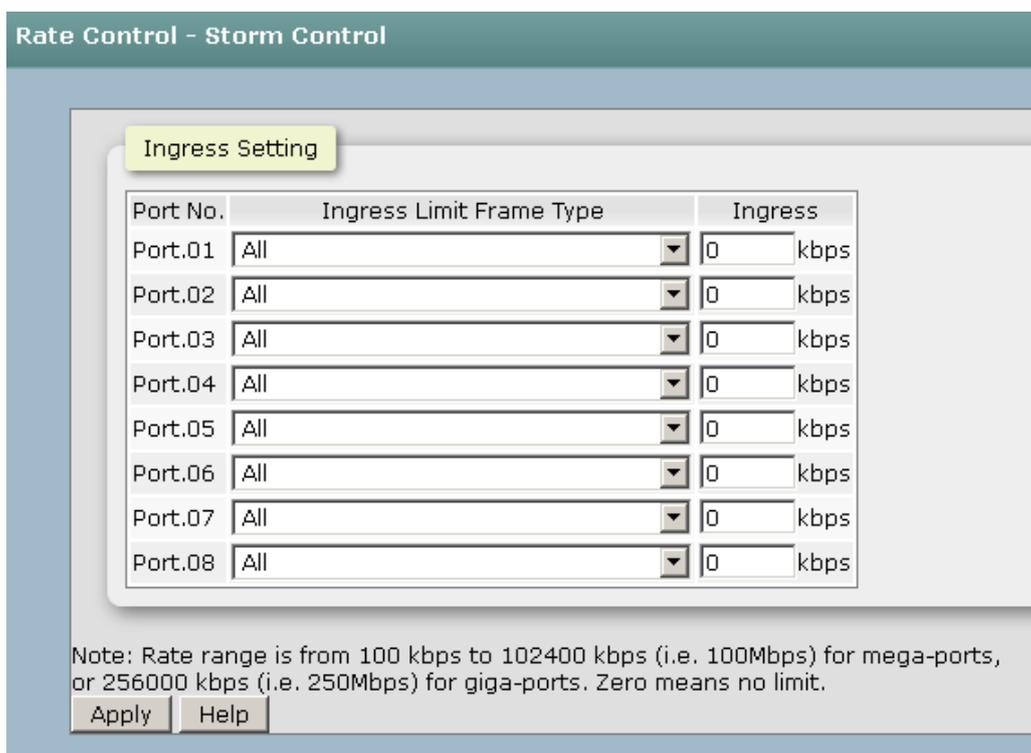
## 5.16 Настройка пределов скорости - *Rate Control –Rate Limit*

Вы можете настроить скорость полосы пропускания каждого порта и тип ограничения кадров (*frame*).

Все порты поддерживают управление скоростью на выходе порта (**Egress**). Например, если порт 1 является 10Мбит-ным портом, пользователи могут установить регрессивную скорость на выходе порта (**Egress**) 1Мбит, 500Кбит. Коммутатор будет выдавать на выход пакеты с регрессивной скоростью.

- А потом, нажмите кнопку **Apply** - Применить.





- **Storm Control:** выберите тип входных кадров, который хотите отфильтровать. Есть четыре типа кадров для выбора
  - **All** - Все
  - **Broadcast/Multicast/Flooded Unicast** - Широковещательные / многоадресные / Переполненные индивидуальные.
  - **Broadcast/Multicast** - Широковещательные / многоадресные /
  - **Broadcast only** – Только широковещательные.

Типы пакетов: **Broadcast/Multicast/Flooded Unicast**, **Broadcast/Multicast**, **Broadcast Only**, доступны только для входных кадров (*Ingress frames*). Скорость исходящих (*Egress rate*) относится ко всем типам кадров.

- А потом, нажмите кнопку **Apply** – Применить.

## 5.17 Настройка агрегирования - *Aggregation – Configuration*

Объединение портов - **Port trunking** - это комбинирование нескольких портов или сетевых кабелей для расширения скорости соединения за пределы возможностей одного порта или одного сетевого кабеля. Для объединения нескольких физических портов и образования единого логического канала используется **Link Aggregation Control Protocol** (Протокол Агрегации управления каналами (LACP)), который представляет собой протокол Слой 2, в соответствии с IEEE 802.3ad. Все порты логического канала или так называемого логического агрегатора работают на одной и той же скорости соединения и для LACP-операций требуется полнодуплексный режим (*full-duplex*).

### 5.17.1 Настройка - *Configuration*

- **Group ID:** Для выбора есть 5 магистральных групп - **Trunk groups**. Назначьте "**Group ID**" для магистральной группы.
- **TYPE:** При выборе **LACP**, магистральные группы используют LACP. Порт, который присоединяется к магистральной группе LACP соединительных линий, должен сначала «договорится» с портами-членами группы. Заметьте, что магистральная группа, в том числе порты-члены, разделенные между собой двумя коммутаторами, имеет возможность включения функции LACP для двух коммутаторов. Если функция LACP отключена, магистральная группа линий является статической магистральной группой (**Static trunk group**). Преимущество отключения LACP в том, что порт присоединяется к магистральной группе без «рукопожатий» с портами-членами; но порты-члены не знают, что они объединены вместе и формируют логическую магистральную группу (*logic trunk group*).
- **Work ports:** Это поле столбца позволяет пользователю выбрать общее количество активных портов (до четырех). В группе - **LACP static trunk group**, например Вы назначаете четыре порта членами магистральной группы, чьи столбцы *Work ports* могут иметь две настройки; излишние порты служат запасными/резервными портами и могут быть агрегированы, при отказе рабочих портов. Если это **Static trunk group** (не- LACP), число рабочих порты должно равняться общему количеству портов членов группы
- Нажмите кнопку **Apply** – Применить.

**Port Setting**

Port No.	Group ID	Type
Port.01	None	Static
Port.02	None	Static
Port.03	None	Static
Port.04	None	Static
Port.05	None	Static
Port.06	None	Static
Port.07	None	Static
Port.08	None	Static

Note: the types should be the same for all member ports in a group.

**802.3ad LACP Work Ports**

Group ID	Work Ports
Trunk1	max
Trunk2	max
Trunk3	max
Trunk4	max

Apply Help

Интерфейс «Port Trunk—Aggregator Setting»(четыре порта добавлены с активацией LACP)

### 5.17.2 Состояние агрегации - *Aggregator – Status*

Вы можете проверить настройки агрегации порта в окне - **Status**.

**Aggregation - Status**

Group ID	Trunk	Member	Type
Trunk 1			Static
Trunk 2			Static
Trunk 3			Static
Trunk 4			Static

## 5.18 Дерево Соединений – *Spanning Tree*

Протокол **Rapid Spanning Tree Protocol (RSTP)** является развитием протокола **Spanning Tree Protocol (STP)** и предусматривает более быстрое преобразование (конвергенцию) связующего дерева после изменения топологии. Система поддерживает, также, и протокол STP. Система автоматически определяет под управлением какого протокола (STP или RSTP) работает подключенное устройство.

### 5.18.1 Настройки RSTP - *RSTP Setting*

Эта Веб-страница предоставляет интерфейс конфигурации порта для RSTP. Вы можете назначить больший или меньший приоритет для каждого порта. **Rapid Spanning Tree** будет держать порт с высоким приоритетом в состоянии пересылки (*forwarding state*) и блокировать другие порты, чтобы гарантировать отсутствие петли в локальной сети.

- **RSTP mode:** Пользователь должен включить функцию RSTP, до настройки соответствующих параметров.
- **Priority:** Коммутатор с наименьшим значением имеет наивысший приоритет и выбран в качестве корневого (*root*). Если значение изменено, пользователь должен перезагрузить коммутатор. Значение должно быть кратно 4096 в соответствии со стандартным правилом протокола.
- **Max Age:** Число секунд ожидания коммутатором получения конфигурационного сообщения **Spanning Tree Protocol**, прежде чем начать попытку реконфигурации. Введите значение от 6 до 40.
- **Hello Time:** Время, которое управляет переключатель, чтобы отправить пакет BPDU, для проверки текущего состояния RSTP. Введите значение от 1 до 10.
- **Forward Delay Time:** Число секунд ожидания портом, перед переходом от *Rapid Spanning-Tree Protocol learning* и слушающего состояния в состоянии пересылки (*forwarding state*). Введите значение от 4 до 30.
- **Enable:** Выберите порт, который Вы хотите включить в RSTP.
- **Path Cost:** Стоимость пути до другого моста (*bridge*) от этого передающего моста в указанный порт. Введите число от 1 до 200 млн.
- **Priority:** Решите, какой порт следует заблокировать, установив его приоритет как самый низкий. Введите число от 0 до 240. Значение приоритета должно быть кратно 16.
- **P2P:** Быстрые переходы состояний возможны в рамках RSTP в зависимости от того, должен ли порт быть подключен только к другому мосту (т.е. он обслуживается с сегментом LAN точка-точка), или он может быть подключен к двум или более мостам (т.е. он обслуживается совместно используемым сегментом LAN). Эта функция позволяет манипулировать статусом «P2P» административно.

«**True**» означает, что порт рассматривается, как соединение «точка-точка» - *point-to-point link*.

«**False**» означает, что порт рассматривается в качестве соединения общего использования - *shared link*.

«**Auto**» означает, что тип связи определяется автоматическим согласованием между двумя точками (*Peer*).

- **Edge:** Порт, подключенный непосредственно к конечным станциям, не создает замкнутую петлю в сети. Для настройки порта в качестве краевого (*Edge*) порта установите статус порта "**True**".
- Нажмите кнопку **Apply** – Применить.

**RSTP - RSTP Setting**

**RSTP Mode**

**Bridge Setting**  
 Priority (0-61440)   
 Max Age Time(6-40)   
 Hello Time (1-10)   
 Forward Delay Time (4-30)

**Port Setting**

Port No.	Enable	Path Cost(0:auto, 1-200000000)	Priority (0-240)	P2P	Edge
Port.01	<input type="text" value="enable"/>	<input type="text" value="0"/>	<input type="text" value="128"/>	<input type="text" value="auto"/>	<input type="text" value="true"/>
Port.02	<input type="text" value="enable"/>	<input type="text" value="0"/>	<input type="text" value="128"/>	<input type="text" value="auto"/>	<input type="text" value="true"/>
Port.03	<input type="text" value="enable"/>	<input type="text" value="0"/>	<input type="text" value="128"/>	<input type="text" value="auto"/>	<input type="text" value="true"/>
Port.04	<input type="text" value="enable"/>	<input type="text" value="0"/>	<input type="text" value="128"/>	<input type="text" value="auto"/>	<input type="text" value="true"/>
Port.05	<input type="text" value="enable"/>	<input type="text" value="0"/>	<input type="text" value="128"/>	<input type="text" value="auto"/>	<input type="text" value="true"/>
Port.06	<input type="text" value="enable"/>	<input type="text" value="0"/>	<input type="text" value="128"/>	<input type="text" value="auto"/>	<input type="text" value="true"/>
Port.07	<input type="text" value="enable"/>	<input type="text" value="0"/>	<input type="text" value="128"/>	<input type="text" value="auto"/>	<input type="text" value="true"/>
Port.08	<input type="text" value="enable"/>	<input type="text" value="0"/>	<input type="text" value="128"/>	<input type="text" value="auto"/>	<input type="text" value="true"/>

### 5.18.2 Информация о RSTP - RSTP Information

На этой Веб-странице приводится информация о порте и коммутаторе в RSTP.

**RSTP - RSTP Information**

**Root Bridge Information**

Bridge ID	N/A
Root Priority	N/A
Root Port	N/A
Root Path Cost	N/A
Max Age Time	N/A
Hello Time	N/A
Forward Delay Time	N/A

**Port Information**

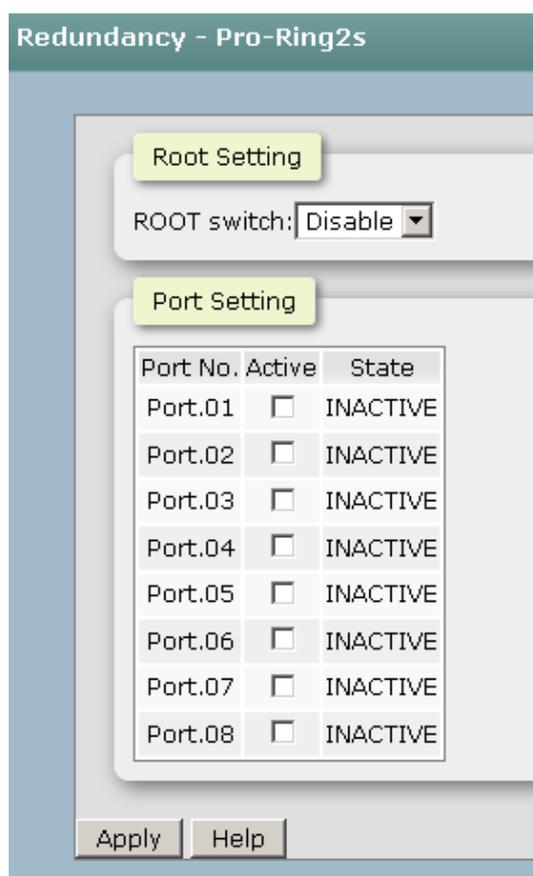
Port	Path Cost	Port Priority	OperP2P	OperEdge	STP Neighbor	State	Role
------	-----------	---------------	---------	----------	--------------	-------	------

*Интерфейс «RSTP System Configuration»*

## 5.19 Механизм кольца *Pro-Ring II S*

**Pro-Ring IIs** - это новый механизм Кольца для коммутаторов Lantech и Лантан, который защищает сеть при помощи гибкой топологии лучше, чем ранее. *Pro-Ring IIs* работает, как одно кольцо - **Single Ring** и как множество колец - **Multiple Ring**, чтобы восстановить разорванное кольцо менее чем за 20 мс в сети, содержащей до 50 коммутаторных узлов.

- **Root Switch:** Чтобы включить функцию X-Ring, сначала нужно установить Коммутаторы в Режим *Enable* или *Backup*. "**Enable**" - Включить, означает, что этот Коммутатор будет играть роль корневого коммутатора, "**Backup**" – Резерв, означает, что этот Коммутатор возьмёт на себя роль корневого коммутатора, при отказе первоначального корневого коммутатора.
- **Port setting:** Порт, который Вы хотите использовать в Ring-топологии кольцо, обычно устанавливаются, как **G1** и **G2**. Для решений с избыточностью, такими, как связанные кольца (*Couple ring*) и двойное подключение (Dual homing), если Вы не уверены, какой порт необходимо Включить - *Enable*, просто выберите все порты, которые ответственны за восходящие линии связи.
- А потом, нажмите кнопку **Apply** - Применить, чтобы настройки вступили в силу.



Интерфейс «RSTP Port Configuration»

## 5.20 Поддержка мультиадресного обмена - *Multicast Support*

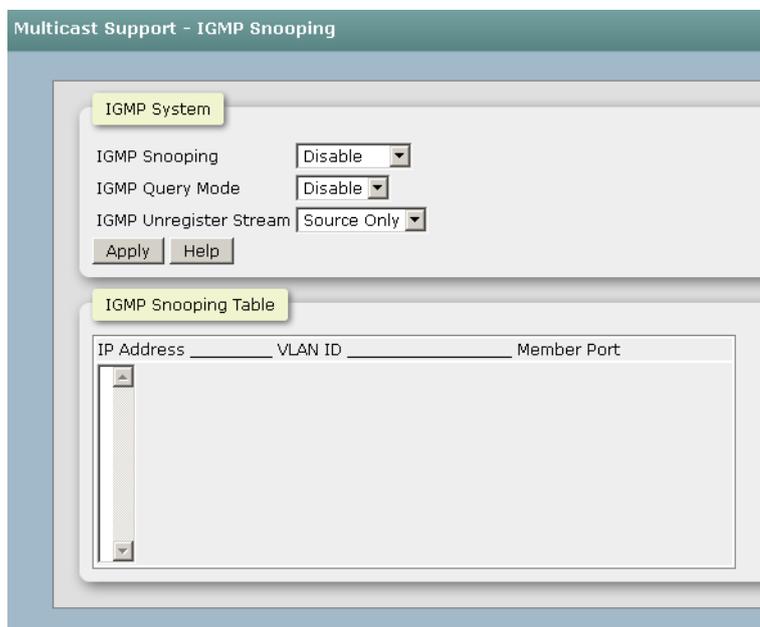
Интернет протокол управления группами - Internet Group Management Protocol (IGMP) является внутренним протоколом комплекта Интернет Протоколов (IP). IGMP управляет многоадресным (групповым) трафиком с помощью коммутаторов, маршрутизаторов и хостов (узлов), которые поддерживают IGMP. Активация IGMP позволяет портам обнаруживать запросы IGMP, пакеты отчетов и управлять многоадресным трафиком, проходящим через коммутатор. У IGMP есть три основных типа сообщения, показанные в таблице:

Message - Сообщение	Описание
<b>Query - Запрос</b>	Сообщение, посланное источником (IGMP роутером или коммутатором) запрашивающее ответ от каждого хоста, принадлежащего мультиадресной группе ( <i>multicast group</i> ).
<b>Report - Отчет</b>	Сообщение, посланное хостом (узлом) источнику, показывающее, что узел хочет быть или является членом группы, указанной в этом отчете ( <i>report message</i> ).
<b>Leave Group – Уход из группы</b>	Сообщение, посланное хостом (узлом) источнику, показывающее, что узел перестает быть членом указанной мультиадресной группы.

### 5.20.1 Слежение за сетевым трафиком - *IGMP Snooping*

Поддержку коммутатором мультиадресного IP Вы можете включить, активируя протокол IGMP на Веб-странице расширенных настроек, после этого появится информационное окно «IGMP Snooping». Диапазон мультиадресных (групповых) IP адресов от 224.0.0.0 до 239.255.255.255.

- **IGMP Protocol:** Включение / отключение протокола IGMP.
- **IGMP Query:** Включение / отключение функции запросов IGMP. Информация о запросах IGMP будет отображаться в разделе состояния IGMP.
- **IGMP Unregister Stream:** Позволяет коммутатору узнать, как обрабатывать мультиадресный поток данных, который не был зарегистрирован в запросе *IGMP Query*.
- Нажмите кнопку **Apply** - Применить.



### 5.20.2 Статическая фильтрация адресов - *Static Filtering*

Мультиадресные (*Multicast*) сообщения похожи на широковещательные (*Broadcasts*), они отправляются ко всем конечным станциям (*end stations*) в сети LAN или VLAN. Мультиадресная фильтрация является функцией, с которой конечная станция может получить многоадресный трафик, если подключенные порты были включены в указанную группу многоадресной рассылки. При использовании многоадресной фильтрации, сетевые устройства направляют многоадресный трафик только на порты, которые подключены к зарегистрированным конечным станциям.

- **IP Address:** Назначьте IP-адрес многоадресной группы в диапазоне от **224.0.0.0 ~ 239.255.255.255**.
- **Member Ports:** Поставьте флажки рядом с номерами портов, чтобы включить их в качестве портов-членов определенной многоадресной группы IP-адресов.
- Нажмите кнопку **Add** - Добавить, чтобы добавить новый фильтр многоадресной рассылки в поле, или выберите фильтр и нажмите кнопку **Delete**, чтобы удалить фильтр.

The screenshot shows a web-based configuration interface titled "Multicast Support - Static Filtering". It is divided into two main sections:

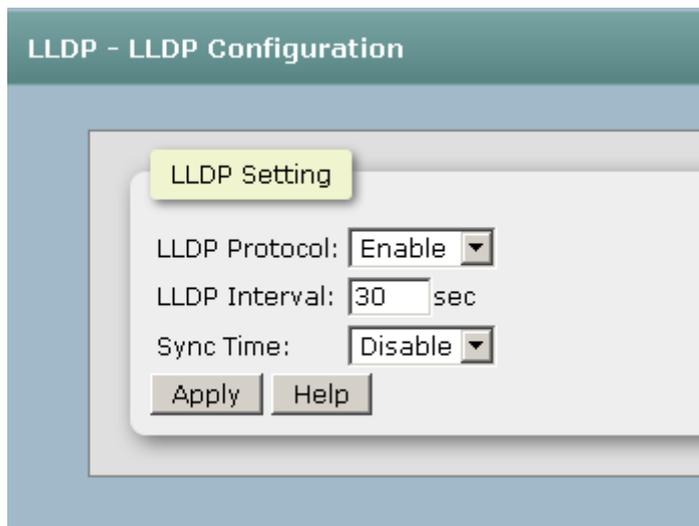
- Filtering Setting:** This section contains an "IP Address" input field. Below it, there are eight checkboxes labeled "Member Ports" from "Port.01" to "Port.08". At the bottom of this section are three buttons: "Add", "Delete", and "Help".
- Multicast Filtering List:** This section contains a table with two columns: "IP Address" and "Member Ports". The table is currently empty, with a vertical scrollbar on the left side.

## 5.21 Протокол *LLDP*

Link Layer Discovery Protocol (LLDP) определяется стандартом IEEE 802.1ab-2009 и является новым стандартным протоколом канального уровня, который обеспечивает решение для проблем конфигурации, вызванных расширением Локальных сетей. LLDP определяет стандартный метод, которым сетевые Ethernet-устройства (такие как, коммутаторы, маршрутизаторы и беспроводные точки доступа LAN) оповещают о своем существовании и характеристиках другие узлы сети и хранения информации, которую они получают от соседних устройств. LLDP работает на всех системах связи 802. Протокол работает над слоем канального уровня, позволяя двум системам, работающим на различных протоколах сетевого уровня, узнать друг о друге.

### 5.21.1 Настройка протокола LLDP - *LLDP Configuration*

- **LLDP Protocol:** Откройте меню выбора, чтобы включить или отключить функцию LLDP.
- **LLDP Interval:** Установите интервал посылки оповещения коммутатора к другим узлам.
- **Sync Time:** Укажите, как долго будет коммутатор синхронизировать информацию LLDP .
- Нажмите кнопку **Apply** - Применить.



Интерфейс «LLDP»

### 5.22.1 Соседние порты - *LLDP Neighbors*

Это окно информирует о «соседних» портах - **Port Neighbor** при помощи протокола LLDP.



## 5.23 База данных фильтрации – *Filtering Data Base*

Используйте таблицу MAC – адресов для обеспечения безопасности порта.

### 5.23.1 Настройка Базы данных фильтрации

- **MAC Address Configuration:**  
Установите **Aging time** - время старения MAC-адресов в таблице и определить автоматически или нет очищать таблицу MAC-адресов при отказе порта.
- **Port Setting:** Укажите, какой порт будет управлять таблицей MAC-адресов.
- Нажмите кнопку **Apply** - Применить.

Filtering Data Base - Configuration

MAC Address Configuration

MAC Address Table Aging Time: (0~3825)  secs

Auto Flush MAC Address Table When Ports Link Down

Apply

Port Setting

Port No.	Security
Port.01	Disable
Port.02	Disable
Port.03	Disable
Port.04	Disable
Port.05	Disable
Port.06	Disable
Port.07	Disable
Port.08	Disable

Apply

Help

### 5.23.2 Динамическая таблица MAC-адресов - *Dynamic MAC table*

Вы можете следить за состоянием таблицы MAC-адресов при помощи этой функции

Filtering Data Base - Dynamic MAC Table

MAC Table List

Port No :

Current MAC Address

Dynamic Address Count : 0  
Static Address Count : 0

Clear MAC Table Help

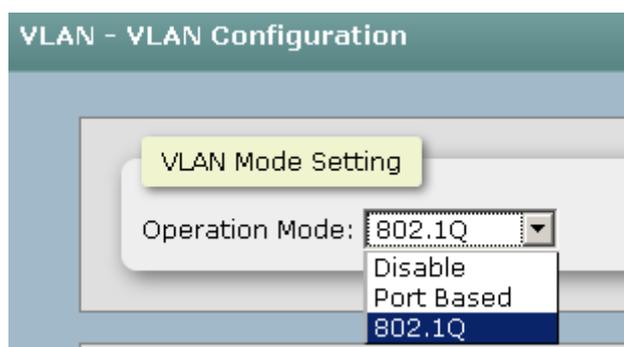
## 5.24 Виртуальная сеть - VLAN

Виртуальная локальная сеть (VLAN) это логическая группировка сети, ограниченная широковещательным доменом (*broadcast domain*), который позволяет изолировать сетевой трафик, так что только члены одной VLAN будут получать трафик из той же сети VLAN. В принципе, создание VLAN на коммутаторе логически эквивалентно пересоединению группы сетевых устройств к другому коммутатору *Layer 2*. Тем не менее, все сетевые устройства по-прежнему подключены к одному коммутатору физически.

Коммутатор поддерживает **Port-based** и **802.1Q (tagged-based)** VLAN. В конфигурации по умолчанию режим VLAN является "**Disable**" - Отключен.

### 5.24.1. Настройка сети - VLAN Configuration

- **Operation Mode** (Режим работы): Введите MAC-адрес порта, который должен постоянно пересылать трафик, независимо от активности сетевого устройства



- **802.1Q VLAN Setting:** Включите режим GVRP и определите ID Management VLAN. GVRP (Generic VLAN Registration Protocol) является протоколом, который облегчает управление виртуальными локальными сетями (VLAN) в рамках более крупной сети. GVRP соответствует спецификации IEEE 802.1Q, которая определяет метод пометки кадров (*tagging*) с конфигурационными данными VLAN. Это позволяет сетевым устройствам динамически обмениваться информацией о конфигурации VLAN с другими устройствами.

- **Port Setting:** Выберите порт, который Вы хотите настроить.
- **Link Type:** Есть 4 типа соединений:
  1. **Access Link:** Сегмент, который обеспечивает путь соединения одной или нескольких станций с VLAN-известным устройством. *Access Port* (Порт доступа), подключенный к *Access Link*, имеет непомеченный (*untagged*) VID (также называемый PVID). После того как кадр без тега попадает в Порт доступа, коммутатор вставит четырех байтовый тег в кадр. Содержание последних 12-ти бит тега является непомеченным VID. Когда этот кадр отправляется через любой Порта доступа той же PVID, коммутатор удалит теги из кадра, чтобы восстановить его так, как было первоначально. Порты той же непомеченной VID рассматриваются, как те же самые члены группы VLAN.

Примечание: Так как Порт доступа не понимает помеченные кадры, поле колонка *Tagged VID* не доступна.

2. **Trunk Link:** Сегмент, который обеспечивает путь соединения для одного или нескольких VLAN-известных устройств (коммутаторов). *Trunk Port* (Магистральный Порт), подключенный к **Trunk Link**, понимает помеченные кадры, которые используются для связи между сетями VLAN с помощью коммутаторов. Какие кадры из указанных VID будут переданы зависит от значений в поле колонки «*Tagged VID*». Пожалуйста, вставляйте запятую между двумя VID.

Примечание: Магистральный порт не вставляет тег в немаркированный кадр, и поэтому поле колонки «*Untagged VID*» не доступно. Не нужно набирать "1" в поле «*Tagged VID*». Магистральный порт будет пересылать кадры VLAN 1. Магистральный порт должен быть подключен к «*trunk/hybrid*» порту другого коммутатора. Помеченные VID двух портов должны быть одинаковыми.

3. **Hybrid Link:** Сегмент, который состоит из **Access Link** и **Trunk Link**. Гибридный порт имеет свойства Портов доступа и Магистральных портов. Гибридный порт имеет PVID принадлежащий конкретной VLAN, и он также передает указанные помеченные кадры для целей VLAN-коммуникации с помощью коммутаторов.
4. **QinQ (Double Tag VLAN) configuration:** *Double Tag VLAN* является еще одним механизмом, применяемый в сети Metro LAN, который может сохранить **IP v4 -адреса** резидентных групп подсетей VLAN (порт пользователя) в VLAN (хост) и, используя IP-адрес шлюза по умолчанию, *Double Tag VLAN* использует (*sharing*) ту же маску подсети. *Double Tag VLAN* в L2 обеспечивает повышение безопасности между пользователем, по дис-связи между суб-сетей VLAN, даже если они находится в той же LAN и имеют ту же маску подсети. И что еще лучше, настройка более простая, чем присвоение каждой VLAN (как port- based VLAN) пользователю.

**Примечания:** 1. Не нужно набирать "1" в поле «Tagged VID». Гибридный порт будет пересылать кадры VLAN 1.

2. Магистральный порт должен быть подключен к магистральному / гибричному Порту другого Коммутатора. Помеченные VID двух портов должны быть одинаковыми.

- **UNTAGGED VID:** Это поле столбца доступно, когда *Link Type - Link Access u Hybrid Link*. Назначьте номер в диапазоне от 1 до 4094.
- **Tagged VID:** Это поле столбца доступно, когда *Link Type - Trunk Link u Hybrid Link*. Назначьте номер в диапазоне от 1 до 4094.
- Нажмите кнопку **Apply** - Применить, чтобы настройки вступили в силу.

Вы можете увидеть на экране тип связи, информацию о непомеченных VID, и помеченных VID на каждом порту в приведенной ниже таблице

**VLAN - VLAN Configuration**

**VLAN Mode Setting**  
Operation Mode:

**802.1Q VLAN Setting**  
GVRP Mode :   
Management VLAN ID :

**Port Setting**

Port No.	Link Type	Untagged VID	Tagged VIDs
Port.01	Access	<input type="text" value="1"/>	
Port.02	Access	<input type="text" value="1"/>	
Port.03	Access	<input type="text" value="1"/>	
Port.04	Access	<input type="text" value="1"/>	
Port.05	Access	<input type="text" value="1"/>	
Port.06	Access	<input type="text" value="1"/>	
Port.07	Access	<input type="text" value="0"/>	
Port.08	Access	<input type="text" value="1"/>	

### 5.24.2 Состояние коммутатора - **Switch Status**

В этой функции Вы можете увидеть состояние настроек VLAN,

**VLAN - Switch Status**

VLAN ID	Untagged Ports	Tagged Ports
1	1,2,3,4,5,6,7,8	

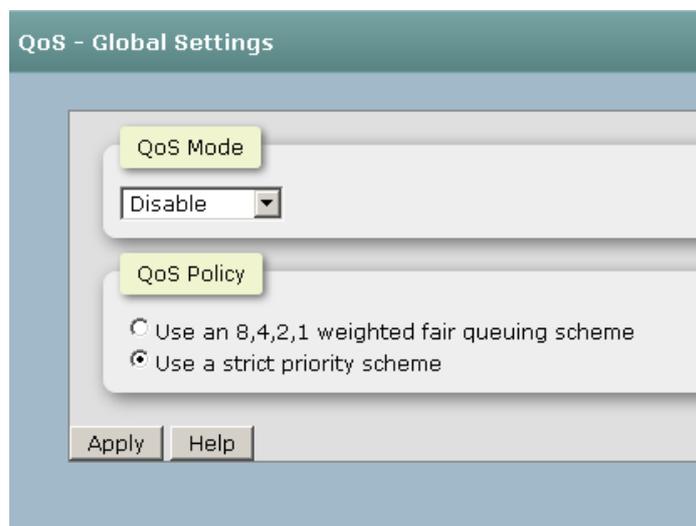
## 5.25 Качество обслуживания - QoS

Качество обслуживания (**Quality of Service - QoS**) - это способность обеспечить различный приоритет различным приложениям, пользователям или потокам данных, или гарантировать определенный уровень пропускной способности потока данных. Гарантии QoS важны, когда пропускная способность сети недостаточна, особенно для потоковых мультимедиа-приложений в режиме реального времени (таких как Voice Over IP или видеоконференции, так как эти приложения часто требуют фиксированную скорость передачи бит и чувствительны к задержкам), и в сетях, где ёмкость является ограниченным ресурсом, например, в сотовой коммуникации. При отсутствии перегрузок в сети, применять механизмы QoS не требуется.

### 5.25.1 Общие настройки - *Global Settings*

Здесь вы можете выбрать, какую использовать схему очередей: «8-4-2-1» или схему строгих приоритетов, или выберите тип приоритета для настройки *Qos Policy*.

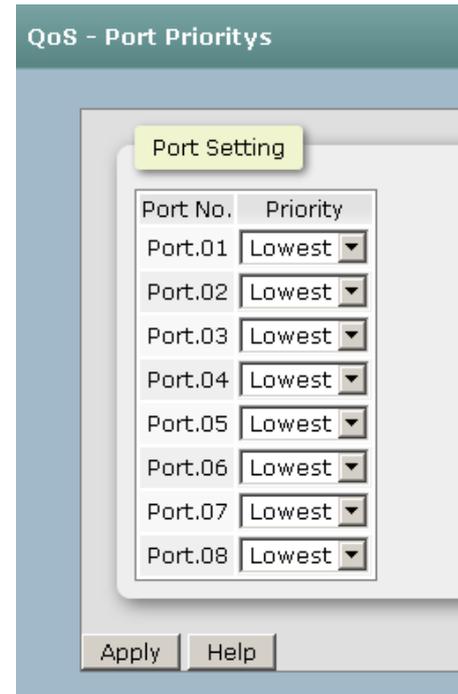
- **Qos Policy:** Выберите правило политики *Qos Policy*.
  - **Using the 8,4,2,1 weight fair queue scheme** (Использовать весовую 8,4,2,1 схему очередей): Коммутатор будет следовать 8: 4: 2: 1 приоритетам скорости обработки очередей (от очереди с высоким приоритетом к очереди с низким приоритетом). Например, во время работы система будет обрабатывать одновременно 1 кадр из самой низкой очереди, 2 кадра из низкой очереди, 4 кадра из средней очереди, и 8 кадров из высокой очереди в соответствии с правилом 8,4,2,1.
  - **Use a strict priority scheme** (Использовать схему строгих приоритетов): Всегда кадры высшей очереди будут обрабатываться первыми, кроме момента, когда более высшая очередь пуста.
  - **Priority Type:** Есть 5 типов приоритет для выбора: **Port-based, TOS only, COS only, TOS first, u TOS first. Disable** - Отключить – означает, что тип приоритета не выбран.
- Нажмите кнопку **Apply** - Применить, чтобы настройки вступили в силу.



### 5.25.2 Приоритеты порта - *Port Priority*

Настройка уровня приоритета индивидуальна для каждого порта. При выборе в ниспадающем меню типа приоритета **PriorityType** пункта **Port-based**, будет доступна настройка политики очереди для каждого порта.

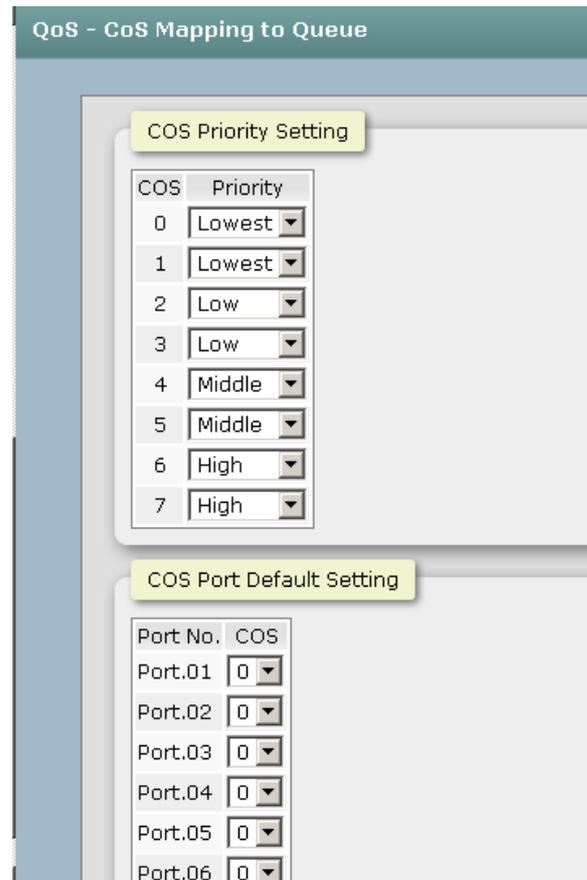
- **Port x:** У каждого порта есть 4 уровня приоритета: High, Middle, Low, Lowest (Высокий, Средний, Низкий, Самый низкий), которые можно установить.
- Нажмите кнопку **Apply** - Применить, чтобы настройки вступили в силу.



### 5.25.3 Отображение класса обслуживания на очереди - *COS Mapping to Queue*

Настройка уровня приоритета COS (Класса обслуживания). При выборе в ниспадающем меню типа приоритета **PriorityType** пункта **COS only/COS first**, будет доступна настройка политики очереди для каждого порта.

- **COS priority:** Настройка уровня приоритета COS 0 ~ 7- High, Middle, Low, Lowest (Высокий, Средний, Низкий, Самый низкий).
- Нажмите кнопку **Apply** - Применить.



### 5.25.4 Отображение кода дифференцированных служб на очереди – *DSCP mapping to queue*

Настройка приоритета DSCP (*Differentiated Services Code Point*). При выборе в ниспадающем меню типа приоритета **Priority Type** пункта **DSCP only/ DSCP first**, будет доступна настройка политики очереди для каждого порта.

- **DSCP Priority:** Система обеспечивает 0 ~ 63 уровней приоритета DSCP. Каждый уровень имеет 4 типа приоритета: High, Middle, Low, Lowest (Высокий, Средний, Низкий, Самый низкий). Значение по умолчанию: **Самый низкий приоритет для каждого уровня**. При получении пакета IP, система будет проверять значение уровня DSCP в IP-пакете. Например, пользователь установил уровень DSCP 25, как Высокий, то система будет проверит значение DSCP принятого IP-пакета. Если значение DSCP полученного IP-пакета составляет 25 (приоритет = Высокий), тогда пакет будет иметь Самый высокий приоритет.
- Нажмите кнопку **Apply** – Применить, чтобы настройки вступили в силу.

QoS - DSCP Mapping to Queue

Priority Setting

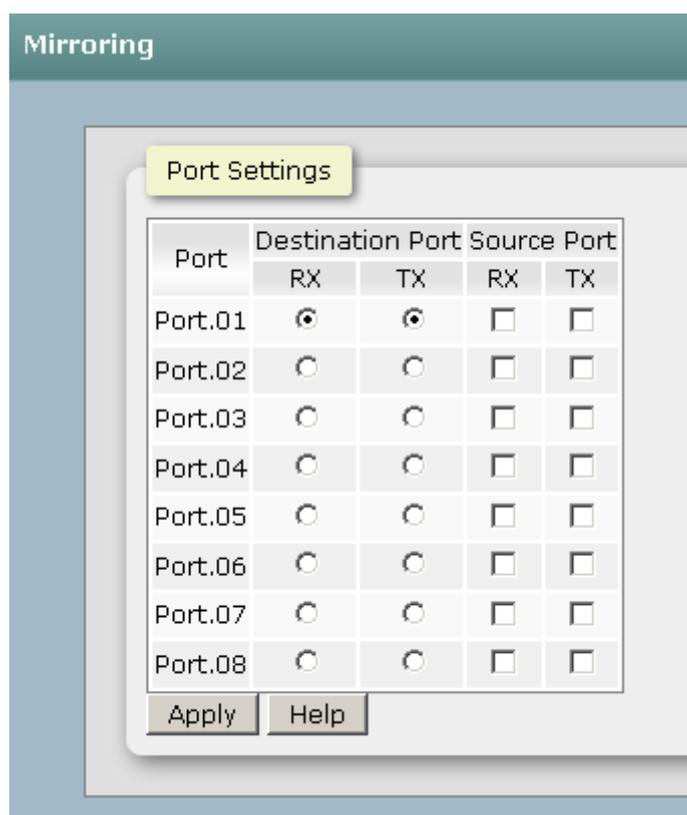
DSCP	0	1	2	3	4	5	6	7
Priority	Lowest							
DSCP	8	9	10	11	12	13	14	15
Priority	Lowest							
DSCP	16	17	18	19	20	21	22	23
Priority	Low							
DSCP	24	25	26	27	28	29	30	31
Priority	Low							
DSCP	32	33	34	35	36	37	38	39
Priority	Middle							
DSCP	40	41	42	43	44	45	46	47
Priority	Middle							
DSCP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

Apply Help

## 5.26 Зеркальное отображение порта - *Port Mirroring*

Зеркалирование портов является способом мониторинга трафика в коммутируемых сетях. Трафик, проходящий через порты можно контролировать на одном указанном порту (*Destination Port*), на который будет дублироваться входящий и исходящий трафик портов-источников (*Source Port*) для мониторинга.

- **Destination Port** (Порт назначения): Только один порт может быть выбран, как порт назначения (зеркалом) для мониторинга трафика RX и TX портов-источников. Или используйте один из двух портов для мониторинга только трафика RX, а другой только для трафика TX. Пользователь может соединить зеркальный порт с анализатором локальной сети или *Netxray*.
- **Source Port** (Порт источник): Порты, которые пользователь хочет контролировать. Трафик всех контролируемых портов будет скопирован в зеркальном порту (*Destination Port*). Пользователь может выбрать для мониторинга несколько портов-источников, устанавливая флажки в полях и RX или TX.
- Затем, нажмите кнопку **Apply** - Применить.



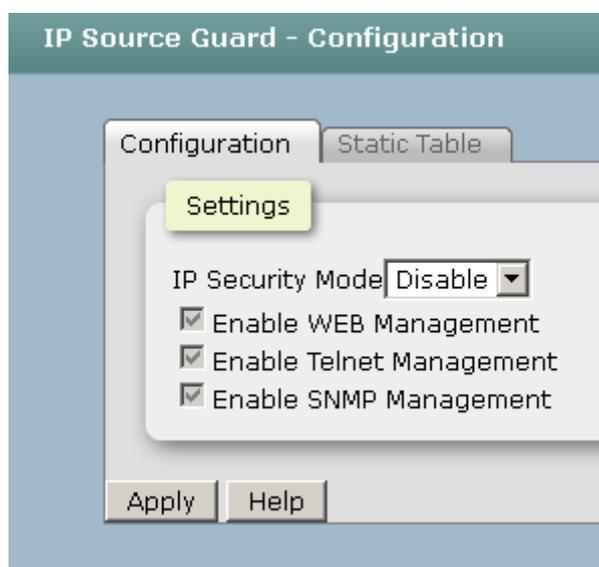
## 5.27 Защита - Security

При помощи этой функции Вы можете блокировать доступ неавторизованным клиентам.

### 5.27.1 Настройка Защиты источников IP - *IP Source Guard - Configuration*

Для защиты системы управления коммутатора, функция **IP Source Guard** позволяет назначить 10 конкретных IP-адресов, которые будут иметь разрешение на доступ к управлению переключателем при помощи HTTP и сервисов Telnet. Цель – ограничить число IP-адресов так, чтобы только уполномоченному персоналу / устройству было позволено осуществлять управление коммутатором.

- **IP Security Mode:** Поставив флажок выбора в поле режима **Enable, Enable HTTP Server, Enable Telnet Server**, Вы сделаете доступными поля десяти безопасных IP-адресов. Если не сделать этого, то эти поля останутся серыми.
- **Enable HTTP Server:** После установки флажка в этом поле, устройства, IP-адреса которых совпадают с одним из десяти IP-адресов в таблице безопасности **Security IP1 ~ IP10**, получают разрешение на доступ к этому коммутатору с помощью HTTP.
- **Enable Telnet Server:** После установки флажка в этом поле, устройства, IP-адреса которых совпадают с одним из десяти IP-адресов в таблице безопасности **Security IP1 ~ IP10**, получают разрешение на доступ к этому коммутатору с помощью служб Telnet.
- **Enable SNMP Management:** После установки флажка в этом поле, устройства, IP-адреса которых совпадают с одним из десяти IP-адресов в таблице безопасности **Security IP1 ~ IP10**, получают разрешение на доступ к этому коммутатору с помощью служб SNMP.



### 5.27.2 Защита по IP - *IP Source Guard – Static Table*

- **Security IP 1 ~ 10:** Система позволяет пользователю назначить до 10 конкретных IP-адресов для доступа. Только эти 10 IP-адресов могут получить доступ и управлять коммутатором через службы HTTP / Telnet после включения режима - **IP Security Mode**.
- Затем, нажмите кнопку **Apply** - Применить, чтобы настройки вступили в силу.

---

**[Примечание]** Не забывайте выполнить действие “Save Configuration” - Сохранить настройки, в противном случае новые настройки будут потеряны при отключении питания коммутатора.

---

The screenshot displays the 'IP Source Guard - Configuration' window. It features two tabs: 'Configuration' and 'Static Table', with 'Static Table' being the active tab. A yellow highlight is placed on the 'IP List Settings' section. This section contains a table with 10 rows, each labeled 'Secure IP' followed by a number from 1 to 10. Each row has a corresponding text input field containing the IP address '0.0.0.0'. At the bottom of the window, there are two buttons: 'Apply' and 'Help'.

Secure IP	IP Address
Secure IP1	0.0.0.0
Secure IP2	0.0.0.0
Secure IP3	0.0.0.0
Secure IP4	0.0.0.0
Secure IP5	0.0.0.0
Secure IP6	0.0.0.0
Secure IP7	0.0.0.0
Secure IP8	0.0.0.0
Secure IP9	0.0.0.0
Secure IP10	0.0.0.0

### 5.27.3 Аутентификация - 802.1X/Radius

Протокол IEEE 802.1x является спецификацией аутентификации, которая предохраняет клиента от доступа к беспроводным точкам доступа или проводным коммутаторам, без идентифицирования (авторизации), по имени пользователя и паролю, проверяемых сервером аутентификации (таким, как сервер RADIUS).

После включения функции IEEE 802.1X, можно настроить параметры этой функции.

#### 5.27.3.1 Настройка - Configuration

- **IEEE 802.1x Protocol:** Включить или отключить протокол 802.1x.
- **Radius Server IP:** Назначение IP-адреса RADIUS Server.
- **Server Port:** Присвоение UDP-адреса порту назначения (*destination port*) для запросов по аутентификации к указанному RADIUS Server.
- **Accounting Port:** Присвоение UDP-адреса порту для учета запросов к указанному RADIUS Server.
- **Shared Key:** Установка ключа шифрования для использования во время сеансов аутентификации с указанным сервером RADIUS. Этот ключ должен соответствовать ключу шифрования, используемого на сервере RADIUS.
- **NAS, Identifier:** Установка идентификатора клиента RADIUS.
- **Quiet Period:** Установка периода времени, в течение которого порт не пытается запрашивать просителя (*supplicant*).
- **TX Period:** Установка периода ожидания порта до повторной передачи следующего EAPOL PDU во время сессии аутентификации.
- **Supplicant Timeout:** Установка периода ожидания коммутатором ответа от просителя (*supplicant*) на запрос EAP (*Extensible Authentication Protocol*).
- **Server Timeout:** Установка периода ожидания коммутатором ответа сервера на запрос об аутентификации.
- **Max Requests:** Установка числа попыток аутентификации, после которого произойдет переход в тайм-аут, если проверка не прошла, и сеанс аутентификации закончен.
- **Reauth period:** Установка периода времени, через который подключенные клиенты, должны быть переидентифицированы (*re-authenticated*).
- Нажмите **Apply** – Применить.

802.1x/Radius - Configuration

**Radius Server Setting**

802.1x Protocol: Disable

Radius Server IP: 192.168.16.3

Server Port: 1812

Accounting Port: 1813

Shared Key: 12345678

NAS, Identifier: NAS\_L2\_SWITCH

**Advanced Setting**

Quiet Period: 60

TX Period: 30

Supplicant Timeout: 30

Server Timeout: 30

Max Requests: 2

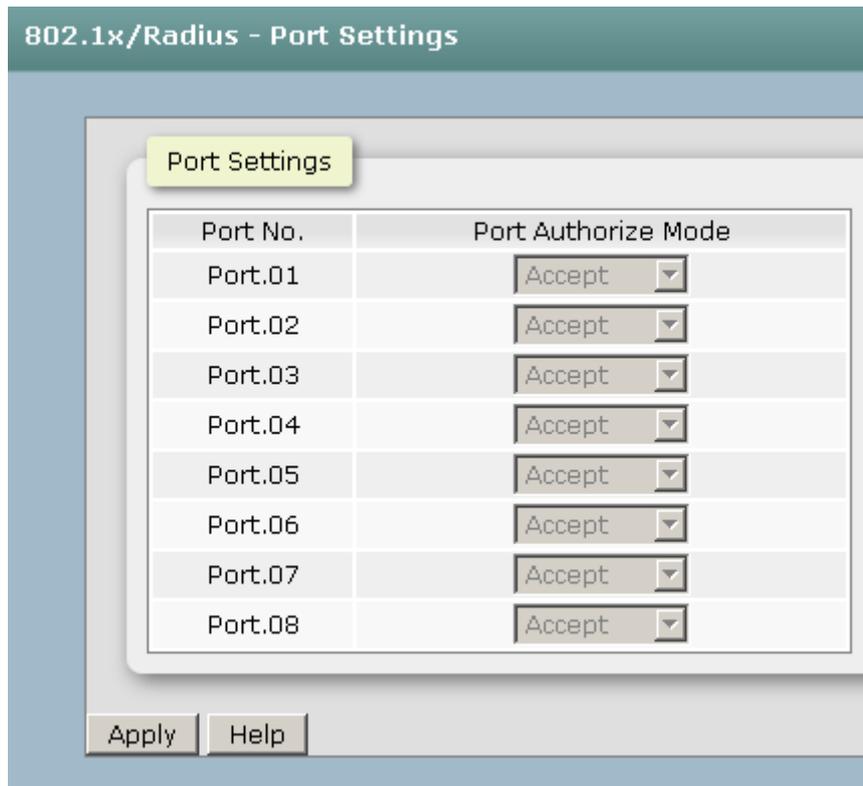
Re-Auth Period: 3600

Apply Help

### 5.27.3.2 Настройки порта - *Port Setting*

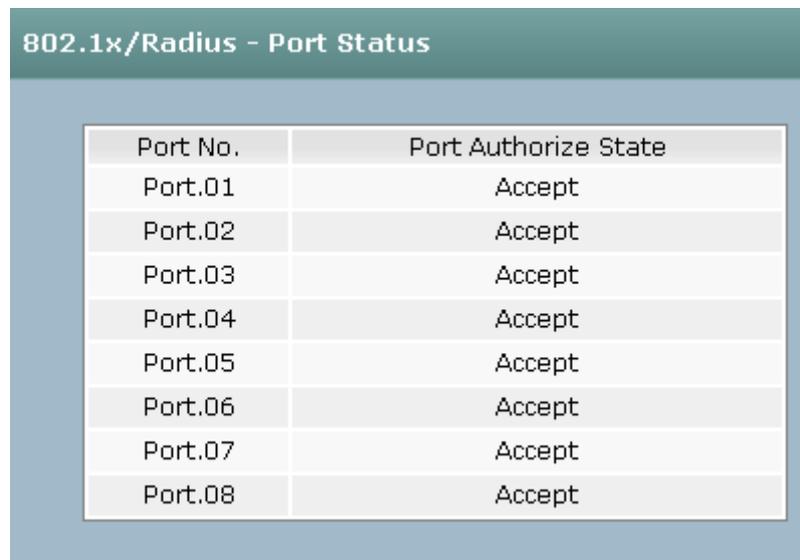
Для каждого порта можно настроить состояние аутентификации в соответствии с Протоколом 802.1x. Состояние может быть: *Disable*, *Accept*, *Reject*, *Authorize* (Отключить, Принять, Отклонить, Разрешить).

- **Reject:** Указанный порт необходимо сохранить в неавторизованном состоянии.
- **Accept:** Указанный порт необходимо сохранить в авторизованном состоянии.
- **Authorize:** Указанный порт установлен в авторизованное состояние или в неавторизованное состояние в соответствии с итогами обмена сообщениями об аутентификации между *Supplicant* (Просителем) и сервером аутентификации.
- **Disable:** Указанный порт работает без соблюдения Протокола 802.1x.
- Нажмите кнопку **Apply** - Применить.



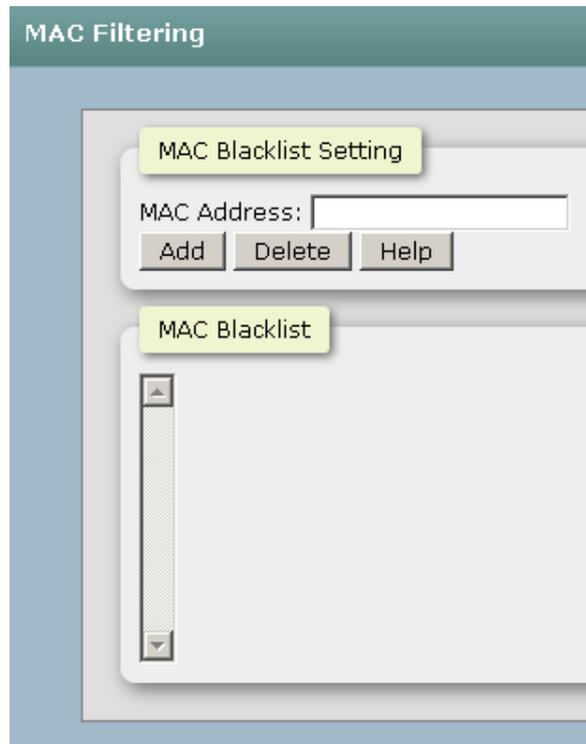
### 5.27.3.3 Состояние порта - *Port Status*

При помощи этой функции Вы можете узнать состоянии Авторизации порта.



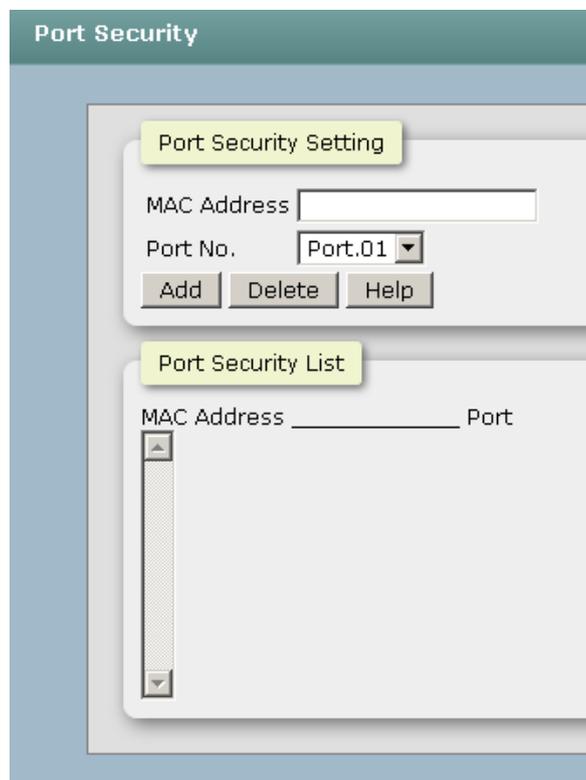
### 5.27.4 Фильтрация по MAC-адресам - *MAC Filtering*

При помощи этой функции Вы можете блокировать не авторизованные коммутаторы по MAC-адресу.



### 5.27.5 Защита порта - *Port Security*

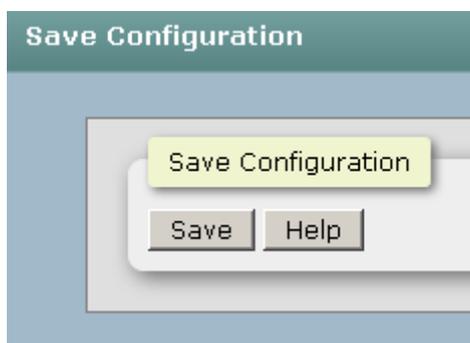
При помощи этой функции Вы можете блокировать не авторизованные порты по MAC-адресу.



## 5.28. Обслуживание - *Maintenance*

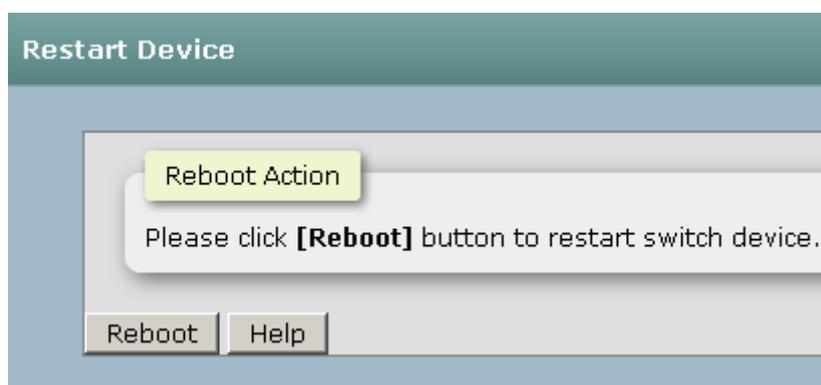
### 5.28.1 Сохранить настройки - *Save Configuration*

Сохраняйте текущие настройки коммутатора.....



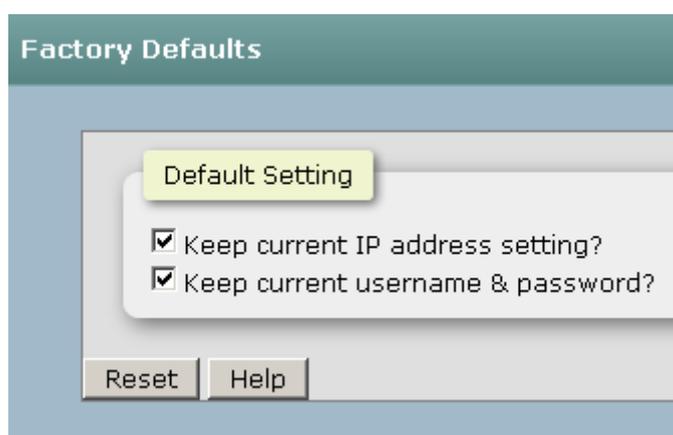
### 5.28.2 Перезапуск устройства - *Restart Device*

Делайте «Warm» - Теплый пуск коммутатора.



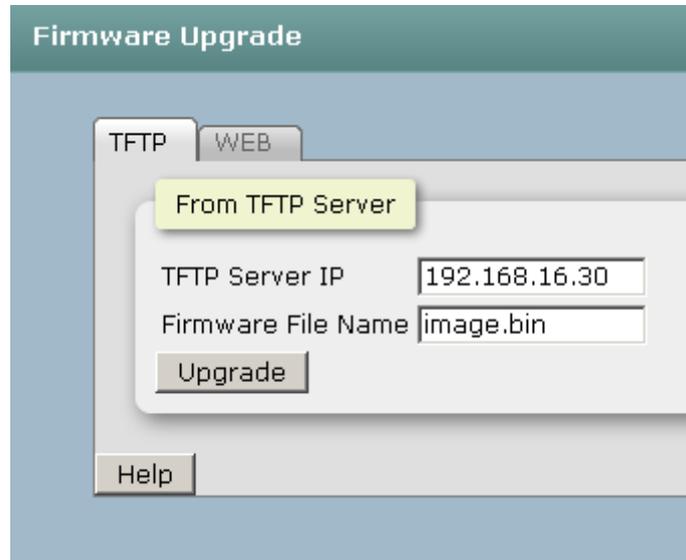
### 5.28.3 Фабричные настройки по умолчанию - *Factory Defaults*

Восстановление настроек по умолчанию - *Default Settings*. Нажмите "**Reset**", чтобы сбросить все настройки к значениям по умолчанию.

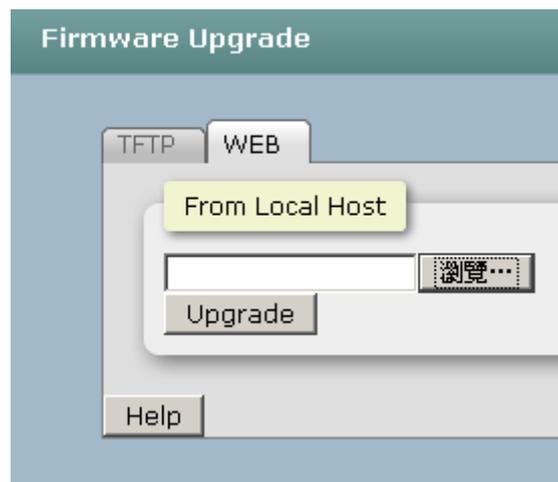


#### 5.28.4 Обновление фирменного ПО - *Firmware Upgrade*

- **TFTP Server IP Address:** Введите IP-адрес своего TFTP сервера.
- **Firmware File Name:** Введите имя файла имиджа прошивки для обновления.
- Нажмите Upgrade



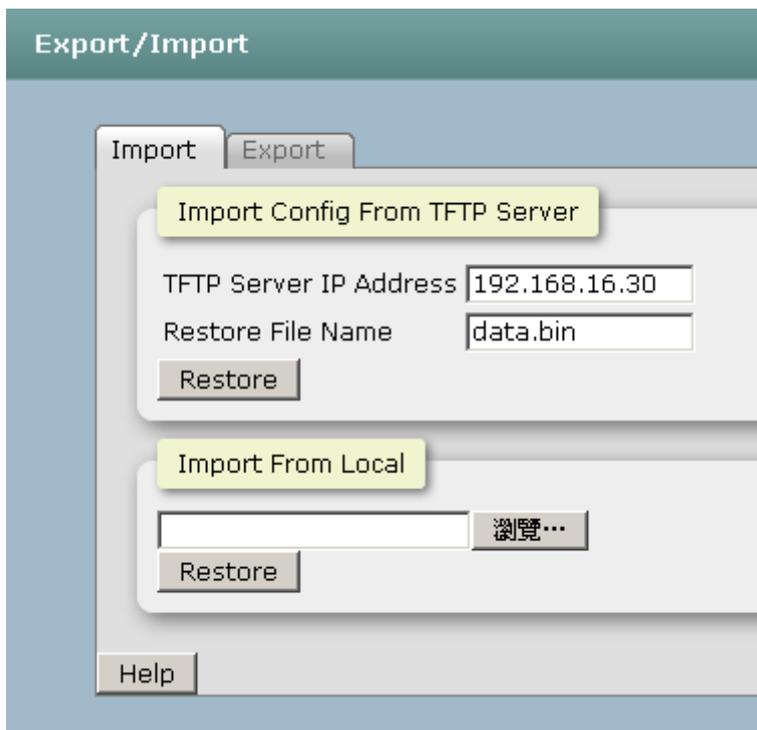
Вы также можете найти прошивку на вашем жестком диске для веб-обновления



### 5.28.5 Экспорт/Импорт - *Export/Import*

Вы можете восстановить предыдущую резервную конфигурацию с сервера TFTP для восстановления настроек. Прежде чем сделать это, необходимо сначала найти имидж-файл на сервере TFTP и коммутатор загрузит обратно флэш-изображение.

- **TFTP Server IP Address:** Введите IP- адрес о TFTP сервера
- **Restore File Name:** Введите правильное имя файла для восстановления.
- Нажмите кнопку **Restore** - Восстановить



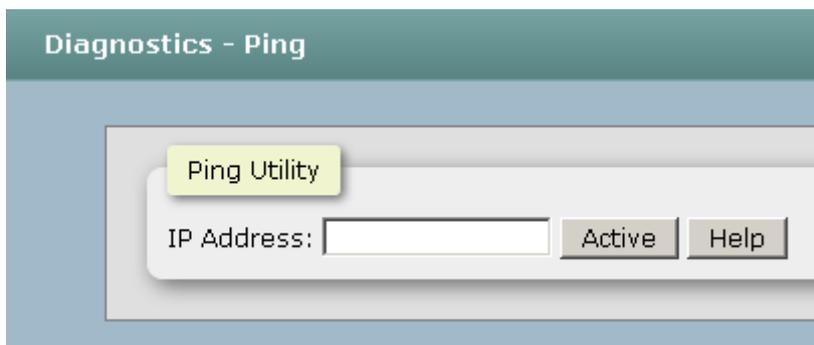
Вы можете создать резервную копию текущей конфигурации флэш-памяти на сервере TFTP для восстановления конфигурации позже. Это поможет вам избежать бесполезной траты времени на настройку параметров с помощью резервного копирования конфигурации.

- **TFTP Server IP Address:** Введите IP- адрес о TFTP сервера
- **Backup File Name:** Введите имя файла.
- Нажмите **Backup** - Резервное копирование



### 5.28.6 Диагностика – *Diagnostics*: Пингование - *Ping*

При помощи этой функции Вы можете «пинговать» - обнаруживать другие устройства сети.



## Диагностика - Troubleshooting

- Убедитесь в том, что Вы используете соответствующий шнур / адаптер (DC 24-48V). Не используйте адаптер питания с выходом с напряжением выше, чем 48 В постоянного тока. Это может привести к повреждению устройства.
- Выберите нужный UTP / STP кабель для построения сети пользователя. Используйте кабели с коннекторами RJ-45 (неэкранированная витая пара (UTP) или экранированная витая пара (STP)), в зависимости от типа разъема коммутатора: 100Ω кабель категорий 3, 4 или 5 для соединений 10 Мбит, 100Ω кабель категории 5 для соединений 100 Мбит, или 100Ω кабель категории 5e / выше для соединений 1000 Мбит. Длина любого соединения кабелем с витой парой не должна превышать 100 метров (328 футов).
- **Диагностические светодиодные индикаторы (LED):** Работа Коммутатора легко контролируется с помощью индикаторов на лицевой панели. Они оказывают помощь в выявлении проблем, с которыми может столкнуться пользователь и нахождении возможных решений проблем.
- Если индикатор питания не горит, когда шнур питания подключен, возможно, проблема в кабеле питания. Проверьте надежность соединений с электрической розеткой. Если проблем остается, обратитесь в сервисный центр.
- Если светодиодные индикаторы в норме и подключенные кабели являются правильными, но пакеты не могут передаваться, проверьте пользовательские настройки или статус Ethernet устройств системы.

## Приложение А—Назначение контактов RJ-45

Порты **UTP / STP** автоматически определяют соединения **Fast Ethernet** (10Base-T / 100Base-TX), или соединения **Gigabit Ethernet** (10Base-T / 100Base-TX / 1000Base-T). **Auto MDI / MDIX** означает, что коммутатор может подключаться к другому коммутатору или рабочей станции без изменения типа кабеля (прямой или перекрестный). Далее показаны схемы прямых и перекрестных кабелей.

- **10 / 100BASE-TX х контактов**

С кабелями 10 / 100BASE-TX, контакты 1 и 2 используются для передачи данных, и контакты 3 и 6 для приема данных.

- **RJ-45 Назначение контактов**

Pin Number	Assignment
1	Tx+
2	Tx-
3	Rx+
6	Rx-

---

**[Примечание]** Знаки "+" и "-" представляют полярность проводов, составляющих каждую пару.

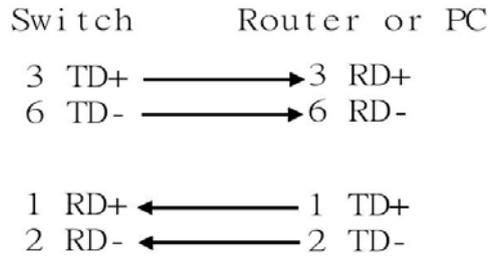
---

В приведенной таблице показано расположение контактов портов 10 / 100BASE-TX MDI и MDI-X..

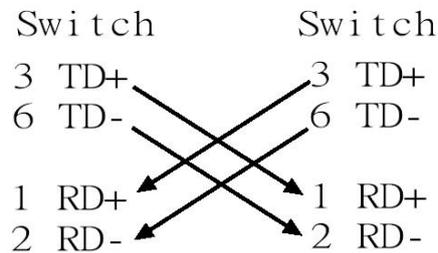
Pin Number	MDI-X Signal Name	MDI Signal Name
1	Receive Data plus (RD+)	Transmit Data plus (TD+)
2	Receive Data minus (RD-)	Transmit Data minus (TD-)
3	Transmit Data plus (TD+)	Receive Data plus (RD+)
6	Transmit Data minus (TD-)	Receive Data minus (RD-)

▪ **Схемы кабелей 10/100Base-TX**

На следующих двух рисунках приведены схемы кабелей 10/100Base-TX



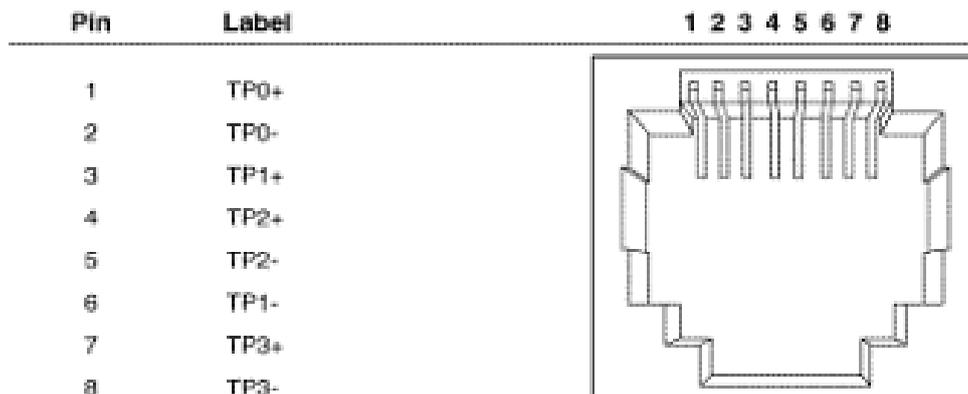
*Схема прямого кабеля (Straight through)*



*Схема перекрестного кабеля (Crossover)*

▪ **Контакты коннекторов 10/100/1000 Base-TX**

В таблице и на рисунке показано назначение и расположение контактов коннектора RJ-45 10/100/1000 Ethernet



▪ Схемы кабелей 10/100/1000Base-TX

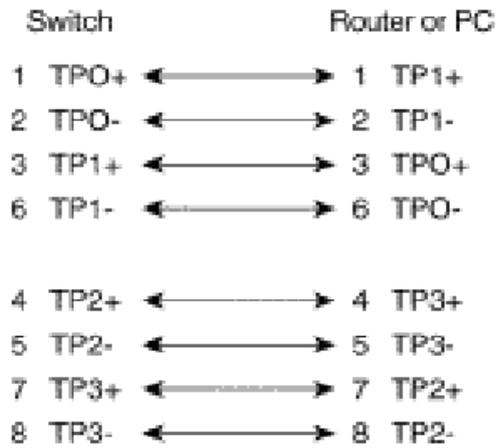


Схема прямого кабеля (Straight through)

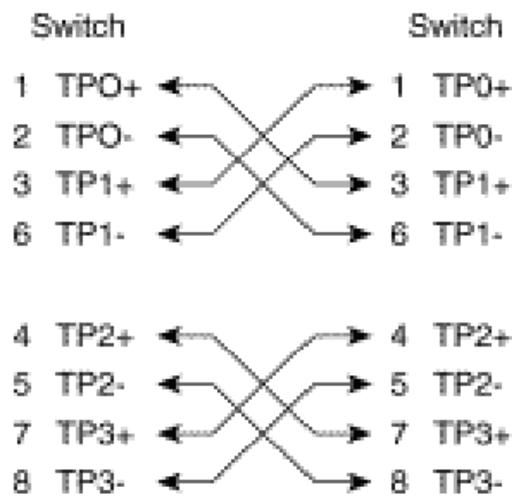


Схема перекрестного кабеля (Crossover)

## Приложение В — Список команд

### Список Наборов Команд - Commands Set List

User EXEC (Пользовательская) -----E

Privileged EXEC (Привилегированная)-----P

Global configuration (Глобальная настройка) -----G

VLAN database (База данных сети)-----V

Interface configuration (Настройка интерфейса) -----I

Команды	Уро- вень	Описание	Пример
<b>enable</b>	<b>E</b>	Войти в режим <i>Privileged EXEC</i>	switch> <b>enable</b>
<b>quit</b>	<b>E</b>	Logout command line shell	switch> <b>quit</b>
<b>show</b>	<b>E</b>	Показать <i>Switch configuration</i>	switch> <b>show config</b>
<b>uptime</b>	<b>E</b>	Показать <i>System up time</i>	switch> <b>uptime</b>
<b>disable</b>	<b>P</b>	Выйти из режима <i>Privileged EXEC</i>	switch>enable switch# <b>disable</b>
<b>configure</b>	<b>P</b>	Войти в режим <i>Global configuration</i>	switch>enable switch# <b>configure</b>
<b>end</b>	<b>G</b>	Выйти из режима <i>Global configuration</i>	switch>enable switch(config)# <b>end</b>
<b>exit</b>	<b>G</b>	Выйти из режима <i>Global configuration</i>	switch>enable switch(config)# <b>exit</b>

### Switch Setting Commands Set – Настройка Коммутатора

Команды	Уро- вень	Описание	Пример
<b>show terminal</b>	<b>P</b>	Show console information	switch>enable switch# <b>show terminal</b>
<b>system name</b> [System Name]	<b>G</b>	Configure system name	switch>enable switch#configure switch(config)# <b>system name xxx</b>
<b>system location</b> [System Location]	<b>G</b>	Set switch system location string	switch>enable switch#configure switch(config)# <b>system location xxx</b>
<b>system Описание</b> [System Описание]	<b>G</b>	Set switch system Описание string	switch>enable switch#configure switch(config)# <b>system description xxx</b>
<b>system contact</b> [System Contact]	<b>G</b>	Set switch system contact window string	switch>enable switch#configure switch(config)# <b>system contact xxx</b>
<b>show system-info</b>	<b>E</b>	Show system information	switch> <b>show system-info</b>

**Admin Password Commands Set – Команды администратора**

Команды	Уро- вень	Описание	Пример
<b>admin username</b> [Username]	<b>G</b>	Changes a login username. (maximum 10 words)	switch>enable switch#configure switch(config)# <b>admin username xxxxxx</b>
<b>admin password</b> [Password]	<b>G</b>	Specifies a password (maximum 10 words)	switch>enable switch#configure switch(config)# <b>admin password xxxxxx</b>
<b>show admin</b>	<b>P</b>	Show administrator information	switch>enable switch# <b>show admin</b>

**IP Setting Commands Set –Настройки IP**

Команды	Уро- вень	Описание	Пример
<b>ip address</b> [Ip-address] [Subnet- mask] [Gateway]	<b>G</b>	Configure the IP address of switch	switch>enable switch#configure switch(config)# <b>ip address 192.168.1.1 255.255.255.0 192.168.1.254</b>
<b>ip dhcp</b>	<b>G</b>	Enable DHCP client function of switch	switch>enable switch#configure switch(config)#ip dhcp
<b>show ip</b>	<b>P</b>	Show IP information of switch	switch>enable switch# <b>show ip</b>
<b>no ip dhcp</b>	<b>G</b>	Disable DHCP client function of switch	switch>enable switch#configure switch(config)#no ip dhcp

**SNTP Commands Set – Команды работы с SNTP**

Команды	Уро- вень	Описание	Пример
<b>sntp enable</b>	<b>G</b>	Enable SNTP function	switch>enable switch#configure switch(config)# <b>sntp enable</b>
<b>sntp ip</b> [IP]	<b>G</b>	Set SNTP server IP, if SNTP function is inactive, this command can't be applied.	switch>enable switch#configure switch(config)# <b>sntp ip 192.168.16.1</b>
<b>sntp timezone</b> [Timezone] Format: [1~63]	<b>G</b>	Set timezone index, use "show sntp timezone" command to get more information of index number	switch>enable switch#configure switch(config)# <b>sntp timezone 22</b>
<b>sntp daylight</b>	<b>G</b>	Enable daylight saving time, if SNTP function is inactive, this command can't be applied.	switch>enable switch#configure switch(config)# <b>sntp daylight</b>
<b>sntp daylight-period</b> [Start time] [End time] Format:[yyyymmdd- hh:mm]	<b>G</b>	Set period of daylight saving time, if SNTP function is inactive, this command can't be applied. Parameter format: [yyyymmdd-hh:mm]	switch>enable switch#configure switch(config)# <b>sntp daylight-period 20120808-01:01 20120809-01:01</b>
<b>sntp daylight-offset</b> [Minute]	<b>G</b>	Set offset of daylight saving time, if SNTP function is inactive, this command can't be applied.	switch>enable switch#configure switch(config)# <b>sntp daylight-offset 60</b>
<b>show sntp</b>	<b>P</b>	Show SNTP information	switch>enable switch# <b>show sntp</b>
<b>show sntp timezone</b>	<b>P</b>	Show index number of time zone list	switch>enable switch# <b>show sntp timezone</b>
<b>no sntp</b>	<b>G</b>	Disable SNTP function	switch>enable switch#configure switch(config)# <b>no sntp</b>
<b>no sntp daylight</b>	<b>G</b>	Disable daylight saving time	switch>enable switch#configure switch(config)# <b>no sntp daylight</b>

**LLDP Commands Set – Команды работы с LLDP**

Команды	Уро- вень	Описание	Пример
<b>lldp enable</b>	<b>G</b>	Enable LLDP function	switch>enable switch#configure switch(config)# <b>lldp enable</b>
<b>lldp interval</b> [TIME sec]	<b>G</b>	Configure LLDP interval	switch>enable switch#configure switch(config)# <b>lldp interval 1800</b>
<b>lldp synctime</b> [enable disable]	<b>G</b>	Enable/disable LLDP sync time	switch>enable switch#configure switch(config)# <b>lldp synctime enable</b>
<b>show lldp</b>	<b>P</b>	Show LLDP information	switch>enable switch# <b>show lldp</b>
<b>no lldp</b>	<b>G</b>	Disable LLDP	switch>enable switch#configure switch(config)# <b>no lldp</b>

**Backup & Restore – Резервирование и восстановление**

Команды	Уро- вень	Описание	Пример
<b>tftp [server IP]</b> <b>backup [file name]</b>	<b>G</b>	Save configuration to TFTP and need to specify the IP of TFTP server and the file name of image.	switch>enable switch#configure switch(config)# <b>tftp 192.168.16.120 backup 123.bin</b>
<b>tftp [server IP]</b> <b>restore [file name]</b>	<b>G</b>	Get configuration from TFTP server and need to specify the IP of TFTP server and the file name of image.	switch>enable switch#configure switch(config)# <b>tftp 192.168.16.120 restore 123.bin</b>

**Upgrade Firmware – Обновление Фирменного ПО**

Команды	Уро- вень	Описание	Пример
<b>tftp [server IP]</b> <b>upgrade [file name]</b>	<b>G</b>	Upgrade firmware by TFTP and need to specify the IP of TFTP server and the file name of image.	switch>enable switch#configure switch(config)# <b>tftp 192.168.16.120 upgrade image.bin</b>

**DHCP Server Commands Set - Работа с сервером DHCP**

Команды	Уровень	Описание	Пример
<b>dhcpserver enable</b>	<b>G</b>	Enable DHCP Server	switch>enable switch#configure switch(config)# <b>dhcpserver enable</b>
<b>dhcpserver lowip</b> [Low IP]	<b>G</b>	Configure low IP address for IP pool	switch>enable switch#configure switch(config)# <b>dhcpserver lowip 192.168.1.100</b>
<b>dhcpserver highip</b> [High IP]	<b>G</b>	Configure high IP address for IP pool	switch>enable switch#configure switch(config)# <b>dhcpserver highip 192.168.1.200</b>
<b>dhcpserver subnetmask</b> [Subnet mask]	<b>G</b>	Configure subnet mask for DHCP clients	switch>enable switch#configure switch(config)# <b>dhcpserver subnetmask 255.255.255.0</b>
<b>dhcpserver gateway</b> [Gateway]	<b>G</b>	Configure gateway for DHCP clients	switch>enable switch#configure switch(config)# <b>dhcpserver gateway 192.168.1.254</b>
<b>dhcpserver dnsip</b> [DNS IP]	<b>G</b>	Configure DNS IP for DHCP clients	switch>enable switch#configure switch(config)# <b>dhcpserver dnsip 192.168.1.1</b>
<b>dhcpserver leasetime</b> [Hours.]	<b>G</b>	Configure lease time (Hours.)	switch>enable switch#configure switch(config)# <b>dhcpserver leasetime 1</b>
<b>dhcpserver ipbinding</b> [IP address]	<b>I</b>	Set static IP for DHCP clients by port	switch>enable switch#configure switch(config)#interface fastEthernet 2 switch(config-if)# <b>dhcpserver ipbinding 192.168.1.1</b>
<b>show dhcpserver configuration</b>	<b>P</b>	Show configuration of DHCP server	switch>enable switch# <b>show dhcpserver configuration</b>
<b>show dhcpserver clients</b>	<b>P</b>	Show client entries of DHCP server	switch>enable switch# <b>show dhcpserver clients</b>
<b>show dhcpserver ip-binding</b>	<b>P</b>	Show IP-Binding information of DHCP server	switch>enable switch# <b>show dhcpserver ip-binding</b>
<b>no dhcpserver</b>	<b>G</b>	Disable DHCP server function	switch>enable switch#configure switch(config)# <b>no dhcpserver</b>

**Port Control Commands Set – Управление портом**

Команды	Уро- вень	Описание	Пример
<b>interface fastEthernet</b> [Portid]	<b>G</b>	Choose the port for modification.	switch>enable switch#configure switch(config)# <b>interface fastEthernet 2</b>
<b>state</b> [enable disable]	<b>I</b>	Use the state interface configuration command to specify the state mode of operation for Ethernet ports. Use the disable form of this command to disable the port.	switch>enable switch#configure switch(config)#interface fastEthernet 2 switch(config-if)# <b>state disable</b>
<b>duplex</b> [full   half]	<b>I</b>	Use the duplex configuration command to specify the duplex mode of operation for Fast Ethernet.	switch>enable switch#configure switch(config)#interface fastEthernet 2 switch(config-if)# <b>duplex full</b>
<b>speed</b> [10 100 1000 auto]	<b>I</b>	Use the speed configuration command to specify the speed mode of operation for Fast Ethernet., the speed can't be set to 1000 if the port isn't a giga port	switch>enable switch#configure switch(config)#interface fastEthernet 2 switch(config-if)# <b>speed 100</b>
<b>flowcontrol mode</b> [symmetric asymmetric]	<b>I</b>	Configure flow control	switch>enable switch#configure switch(config)#interface fastEthernet 2 switch(config-if)# <b>flowcontrol mode asymmetric</b>
<b>no flowcontrol</b>	<b>I</b>	Disable flow control of interface	switch>enable switch#configure switch(config)#interface fastEthernet 2 switch(config-if)# <b>no flowcontrol</b>
<b>security enable</b>	<b>I</b>	Enable security of interface	switch>enable switch#configure switch(config)#interface fastEthernet 2 switch(config-if)# <b>security enable</b>
<b>no security</b>	<b>I</b>	Disable security of interface	switch>enable switch#configure switch(config)#interface fastEthernet 2 switch(config-if)# <b>no security</b>
<b>show dhcpserver configuration</b>	<b>P</b>	Show configuration of DHCP server	switch>enable switch# <b>show dhcpserver configuration</b>

**Port Control Commands Set - продолжение**

Команды	Уро- вень	Описание	Пример
<b>auto-sfp</b> [Enable Disable]	<b>G</b>	Enable/disable to auto detect 100/1000 SFP	switch>enable switch#configure switch(config)# <b>auto-sfp disable</b>
<b>alias</b> [name]	<b>I</b>	Set port alias name	switch>enable switch#configure switch(config)#interface fastEthernet 2 switch(config-if)# <b>alias 1111</b>
<b>show interface configuration</b>	<b>I</b>	show interface configuration status	switch>enable switch#configure switch(config)#interface fastEthernet 2 switch(config-if)# <b>show interface configuration</b>

**Port Status Commands Set – Состояние порта**

Команды	Уро- вень	Описание	Пример
<b>show interface status</b>	<b>I</b>	show interface actual status	switch>enable switch#configure switch(config)#interface fastEthernet 2 switch switch (config-if)# <b>show interface status</b>

**Rate Limit Commands Set – Настройка пределов скоростей**

Команды	Уро- вень	Описание	Пример
<b>ratelimit type all</b>	I	Set interface ingress limit frame type to “accept all frame”	switch>enable switch#configure switch(config)#interface fastEthernet 2 switch(config-if)# <b>ratelimit type all</b>
<b>ratelimit type broadcast-multicast-flooded-unicast</b>	I	Set interface ingress limit frame type to “accept broadcast, multicast, and flooded unicast frame”	switch>enable switch#configure switch(config)#interface fastEthernet 2 switch(config-if)# <b>ratelimit type broadcast-multicast-flooded-unicast</b>
<b>ratelimit type broadcast-multicast</b>	I	Set interface ingress limit frame type to “accept broadcast and multicast frame”	switch>enable switch#configure switch(config)#interface fastEthernet 2 switch(config-if)# <b>ratelimit type broadcast-multicast</b>
<b>ratelimit type broadcast- only</b>	I	Set interface ingress limit frame type to “only accept broadcast frame”	switch>enable switch#configure switch(config)#interface fastEthernet 2 switch(config-if)# <b>ratelimit type broadcast-only</b>
<b>ratelimit in [kbps]</b>	I	Set interface input bandwidth. zero means no limit.	switch>enable switch#configure switch(config)#interface fastEthernet 2 switch(config-if)# <b>ratelimit in 160</b>
<b>ratelimit out [kbps]</b>	I	Set interface output bandwidth. Rate Range is from 100 kbps to 102400 kbps or to 256000 kbps for giga ports, and zero means no limit.	switch>enable switch#configure switch(config)#interface fastEthernet 2 switch(config-if)# <b>ratelimit out 160</b>
<b>show ratelimit</b>	I	Show interfaces bandwidth control	switch>enable switch#configure switch(config)#interface fastEthernet 2 switch(config-if)# <b>show ratelimit</b>

**Trunk Commands Set – Управление «Стволом»**

Команды	Уро- вень	Описание	Пример
<b>aggregator priority</b> [1~65535]	<b>G</b>	Set port group system priority	switch>enable switch#configure switch(config)# <b>aggregator priority 22</b>
<b>aggregator group</b> [GroupID] [Port- list] <b>lACP workp</b> [Workport]	<b>G</b>	Assign a trunk group with LACP active. [GroupID] :1~3 [Port-list]:Member port list, This parameter could be a port range(ex.1-4) or a port list separate by a comma(ex.2, 3, 6) [Workport]: The amount of work ports, this value could not be less than zero or be large than the amount of member ports	switch>enable switch#configure switch(config)# <b>aggregator group 1 1-4 lACP workp 2</b> or switch(config)# <b>aggregator group 2 1,4,3 lACP workp 3</b>
<b>aggregator activityport</b> [Group ID] [Port Numbers]	<b>G</b>	Set activity port	switch>enable switch#configure switch(config)# <b>aggregator activityport 1 2</b>
<b>aggregator group</b> [GroupID] [Port- list] <b>no lACP</b>	<b>G</b>	Assign a static trunk group. [GroupID] :1~3 [Port-list]:Member port list, This parameter could be a port range(ex.1-4) or a port list separate by a comma(ex.2, 3, 6)	switch>enable switch#configure switch(config)# <b>aggregator group 1 2-4 no lACP</b> or switch(config)# <b>aggregator group 1 3,1,2 no lACP</b>
<b>show aggregator</b>	<b>P</b>	Show the information of trunk group	switch>enable switch# <b>show aggregator 1</b> or switch# <b>show aggregator 2</b> or switch# <b>show aggregator 3</b>
<b>no aggregator lACP</b> [GroupID]	<b>G</b>	Disable the LACP function of trunk group	switch>enable switch#configure switch(config)# <b>no aggregator lACP 1</b>
<b>no aggregator group</b> [GroupID]	<b>G</b>	Remove a trunk group	switch>enable switch#configure switch(config)# <b>no aggregator group 1</b>

**PRO-RING IIS Commands Set – Управление кольцом PRO-RING IIS**

Команды	Уро- вень	Описание	Пример
<b>prorstp enable</b>	<b>I</b>	Enable PRO-RING IIS for this interface	switch>enable switch#configure switch(config)#interface fastEthernet 2 switch(config-if)# <b>prorstp enable</b>
<b>prorstp-root</b> [disable enable ba ckup]	<b>G</b>	Configure PRO-RING IIS ROOT	switch>enable switch#configure switch(config)# <b>prorstp-root enable</b>
<b>no prorstp</b>	<b>I</b>	Disable PRO-RING IIS for this interface	switch>enable switch#configure switch(config)#interface fastEthernet 2 switch(config-if)# <b>no prorstp</b>
<b>no prorstp</b>	<b>G</b>	Disable PRO-RING IIS for all interfaces	switch>enable switch#configure switch(config)# <b>no prorstp</b>
<b>show prorstp</b>	<b>P</b>	Show PRO-RING IIS configuration	switch>enable switch# <b>show prorstp</b>

**RSTP Commands Set – Управление RSTP**

Команды	Уро- вень	Описание	Пример
<b>rstp enable</b>	<b>G</b>	Enable RSTP	switch>enable switch#configure switch(config)# <b>rstp enable</b>
<b>rstp priority</b> [0~61440]	<b>G</b>	Configure RSTP bridge priority parameter	switch>enable switch#configure switch(config)# <b>rstp priority 4096</b>
<b>rstp max-age</b> [6~40]	<b>G</b>	Configure RSTP max age parameter	switch>enable switch#configure switch(config)# <b>rstp max-age 6</b>
<b>rstp hello-time</b> [1~10]	<b>G</b>	Configure RSTP hello time parameter.	switch>enable switch#configure switch(config)# <b>rstp hello-time 1</b>
<b>rstp forward-time</b> [4~30]	<b>G</b>	Configure RSTP forward time parameter.	switch>enable switch#configure switch(config)# <b>rstp forward-time 4</b>
<b>rstp path-cost</b> [0:auto,1-200000000]	<b>I</b>	Path cost on this interface	switch>enable switch#configure switch(config)#interface fastEthernet 2 switch(config-if)# <b>rstp path-cost 20</b>
<b>rstp port-priority</b> [0-240]	<b>I</b>	Port priority on this interface.	switch>enable switch#configure switch(config)#interface fastEthernet 2 switch(config-if)# <b>rstp port-priority 16</b>
<b>rstp admin-p2p</b> [Auto True False]	<b>I</b>	Admin P2P on this interface.	switch>enable switch#configure switch(config)#interface fastEthernet 2 switch(config-if)# <b>rstp admin-p2p false</b>
<b>rstp admin-edge</b> [True False]	<b>I</b>	Admin Edge on this interface	switch>enable switch#configure switch(config)#interface fastEthernet 2 switch(config-if)# <b>rstp admin-edge false</b>
<b>rstp admin-non-stp</b> [True False]	<b>I</b>	Admin NonSTP on this interface	switch>enable switch#configure switch(config)#interface fastEthernet 2 switch(config-if)# <b>rstp admin-non-stp false</b>
<b>show rstp</b>	<b>G</b>	Show RSTP information.	switch>enable switch# <b>show rstp</b>
<b>no rstp</b>	<b>G</b>	Disable RSTP.	switch>enable switch#configure switch(config)# <b>no rstp</b>

**VLAN Commands Set – Управление виртуальной сетью**

Команды	Уро- вень	Описание	Пример
<b>vlan database</b>	<b>P</b>	Enter VLAN configure mode	switch>enable switch# <b>vlan database</b>
<b>vlanmode</b> [portbase  802.1q   disable  gvrp]	<b>V</b>	To set switch VLAN mode.	switch>enable switch#vlan database switch(vlan)# <b>vlanmode portbase</b> or switch(vlan)# <b>vlanmode 802.1q</b> or switch(vlan)# <b>vlanmode disable</b> or switch(vlan)# <b>vlanmode gvrp</b>
<b>Ported based VLAN configuration</b>			
<b>vlan port-based grpname</b> [Group Name] <b>grp-id</b> [GroupID] <b>port</b> [PortNumbers]	<b>V</b>	Add new port based VALN	switch>enable switch#vlan database switch(vlan)# <b>vlan port-based grpname test grp-id 2 port 2-4</b> or switch(vlan)# <b>vlan port-based grpname test grp-id 2 port 2,3,4</b>
<b>show vlan</b> [GroupID] or <b>show vlan</b>	<b>V</b>	Show VLAN information	switch>enable switch#vlan database switch(vlan)# <b>show vlan 2</b>
<b>no vlan</b> [VID]	<b>V</b>	Delete port base group ID	switch>enable switch#vlan database switch(vlan)# <b>no vlan 2</b>
<b>IEEE 802.1Q VLAN</b>			
<b>vlan 8021q mnt-vid</b> [VID]	<b>V</b>	Configure management VID (0 is disabled)	switch>enable switch#vlan database switch(vlan)# <b>vlan 8021q mnt-vid 22</b>
<b>vlan 8021q name</b> [GroupName] <b>vid</b> [VID]	<b>V</b>	Change the name of VLAN group, if the group didn't exist, this command can't be applied.	switch>enable switch#vlan database switch(vlan)# <b>vlan 8021q name test vid 22</b>
<b>vlan 8021q port</b> [PortNumber] <b>access-link untag</b> [UntaggedVID]	<b>V</b>	Assign a access link for VLAN by port, if the port belong to a trunk group, this command can't be applied.	switch>enable switch#vlan database switch(vlan)# <b>vlan 8021q port 3 access-link untag 22</b>
<b>vlan 8021q port</b> [PortNumber] <b>trunk-link tag</b> [TaggedVID List]	<b>V</b>	Assign a trunk link for VLAN by port, if the port belong to a trunk group, this command can't be applied.	switch>enable switch#vlan database switch(vlan)# <b>vlan 8021q port 3 trunk-link tag 2,3,6,99</b> or switch(vlan)# <b>vlan 8021q port 3 trunk-link tag 3-20</b>
<b>vlan 8021q port</b> [PortNumber] <b>hybrid-link untag</b> [UntaggedVID] <b>tag</b> [TaggedVID List]	<b>V</b> can't be applied.	Assign a hybrid link for VLAN by port, if the port belong to a trunk group, this command	switch>enable switch#vlan database switch(vlan)# <b>vlan 8021q port 3 hybrid-link untag 4 tag 3,6,8</b> or switch(vlan)# <b>vlan 8021q port 3 hybrid-link untag 5 tag 6-8</b>

**VLAN Commands Set - IEEE 802.1Q VLAN - продолжение**

Команды	Уро- вень	Описание	Пример
<b>vlan 8021q port</b> [PortNumber] <b>hybrid-link-qinq</b> <b>untag</b> [UntaggedVID] <b>tag</b> [TaggedVID List]	<b>V</b>	Assign a qinq link for VLAN by port, if the port belong to a trunk group, this command can't be applied.	switch>enable switch#vlan database switch(vlan)# <b>vlan 8021q port 3 hybrid-link-qinq untag 4 tag 3,6,8</b> or switch(vlan)# <b>vlan 8021q port 3 hybrid-link-qinq untag 5 tag 6-8</b>
<b>vlan 8021q</b> <b>aggregator</b> [PortNumber] <b>access-link untag</b> [UntaggedVID]	<b>V</b>	Assign a access link for VLAN by trunk group	switch>enable switch#vlan database switch(vlan)# <b>vlan 8021q aggregator 3 access-link untag 33</b>
<b>vlan 8021q</b> <b>aggregator</b> [PortNumber] <b>trunk-link tag</b> [TaggedVID List]	<b>V</b>	Assign a trunk link for VLAN by trunk group	switch>enable switch#vlan database switch(vlan)# <b>vlan 8021q aggregator 3 trunk-link tag 2,3,6,99</b> or switch(vlan)# <b>vlan 8021q aggregator 3 trunk-link tag 3-20</b>
<b>vlan 8021q</b> <b>aggregator</b> [PortNumber] <b>hybrid-link untag</b> [UntaggedVID] <b>tag</b> [TaggedVID List]	<b>V</b>	Assign a hybrid link for VLAN by trunk group	switch>enable switch#vlan database switch(vlan)# <b>vlan 8021q aggregator 3 hybrid-link untag 4 tag 3,6,8</b> or switch(vlan)# <b>vlan 8021q aggregator 3 hybrid-link untag 5 tag 6-8</b>
<b>vlan 8021q</b> <b>aggregator</b> [PortNumber] <b>hybrid-link-qinq</b> <b>untag</b> [UntaggedVID] <b>tag</b> [TaggedVID List]	<b>V</b>	Assign a qinq link for VLAN by trunk group	switch>enable switch#vlan database switch(vlan)# <b>vlan 8021q aggregator 3 hybrid-link-qinq untag 4 tag 3,6,8</b> or switch(vlan)# <b>vlan 8021q aggregator 3 hybrid-link-qinq untag 5 tag 6-8</b>
<b>show vlan</b> [GroupID] or <b>show vlan</b>	<b>V</b>	Show VLAN information	switch>enable switch#vlan database switch(vlan)# <b>show vlan 2</b>
<b>no vlan</b> [GroupID]	<b>V</b>	Delete port base group ID	switch>enable switch#vlan database switch(vlan)# <b>no vlan 2</b>

**SNMP Commands Set – Команды SNMP**

Команды	Уро- вень	Описание	Пример
<b>snmp agent-mode</b> [v1v2c v3]	<b>G</b>	Select the agent mode of SNMP	switch>enable switch#configure switch(config)# <b>snmp agent-mode v1v2c</b>
<b>snmp community-strings</b> [Community] <b>right</b> [RO/RW]	<b>G</b>	Add SNMP community string.	switch>enable switch#configure switch(config)# <b>snmp community-strings public right rw</b>
<b>Snmp trap server</b> [IP address] <b>community</b> [Community-string] <b>trap-version</b> [v1 v2c]	<b>G</b>	Configure SNMP server host information and community string	switch>enable switch#configure switch(config)# <b>snmp trap server 192.168.1.120 community public trap-version v2c</b>
<b>snmp snmpv3-user</b> [UserID] <b>password</b> [Authentication Password] [Privacy Password]	<b>G</b>	Create a SNMPv3 user profile	switch>enable switch#configure switch(config)# <b>snmp snmpv3-user root password 123 123</b>
<b>no snmp community-strings</b> [Community]	<b>G</b>	Disable SNMP community strings function	switch>enable switch#configure switch(config)# <b>no snmp community-strings public</b>
<b>no snmp trap server</b> [IP Address]	<b>G</b>	Remove SNMP trap setting	switch>enable switch#configure switch(config)# <b>no snmp trap server 192.168.1.120</b>
<b>no snmp snmpv3-user password</b> [Authentication Password] [Privacy Password]	<b>G</b>	Remove SNMPv3 user profile	switch>enable switch#configure switch(config)# <b>no snmp snmpv3-user root password 123 123</b>

**Traffic Prioritization Commands Set – Приоритеты трафика**

Команды	Уро- вень	Описание	Пример
<b>qos prioritytype</b> [port-based cos-only tos-only cos-first tos-first]	<b>G</b>	Setting of QOS priority type	switch>enable switch#configure switch(config)# <b>qos prioritytype port-base</b>
<b>qos policy</b> [weighted-fair strict]	<b>G</b>	Select QOS policy scheduling	switch>enable switch#configure switch(config)# <b>qos policy weighted-fair</b>
<b>qos priority portbased</b> [Port] [lowest low middle high]	<b>G</b>	Configure Port-based Priority	switch>enable switch#configure switch(config)# <b>qos priority portbased 1 low</b>
<b>qos priority cos</b> [Priority][lowest low middle high]	<b>G</b>	Configure COS Priority	switch>enable switch#configure switch(config)# <b>qos priority cos 0 middle</b>
<b>qos priority cosportdefault</b> [Port][Priority]	<b>G</b>	Configure COS Port default	switch>enable switch#configure switch(config)# <b>qos priority cosportdefault 1 1</b>
<b>qos priority tos</b> [Priority][lowest low middle high]	<b>G</b>	Configure TOS Priority	switch>enable switch#configure switch(config)# <b>qos priority tos 3 high</b>
<b>show qos</b>	<b>P</b>	Displays the information of QoS configuration	switch>enable switch#configure switch# <b>show qos</b>
<b>no qos</b>	<b>G</b>	Disable QoS function	switch>enable switch#configure switch(config)#no qos

**IGMP Commands Set – Команды IGMP**

Команды	Уро- вень	Описание	Пример
<b>igmp enable</b>	<b>G</b>	Enable IGMP snooping function	switch>enable switch#configure switch(config)# <b>igmp enable</b>
<b>igmp query</b> [auto/fource]	<b>G</b>	Configure IGMP query mode	switch>enable switch#configure switch(config)# <b>igmp query auto</b>
<b>igmp unregister</b> [flooding/blocking/so urceonly]	<b>G</b>	Configure IGMP unregister stream	switch>enable switch#configure switch(config)# <b>igmp unregister flooding</b>
<b>igmp last-query- count</b> [1~2 sec.]	<b>G</b>	Configure Last Member Query Count	switch>enable switch#configure switch(config)# <b>igmp last-query- count 1</b>
<b>igmp last-query- interval</b> [1~250 tenths of a sec.]	<b>G</b>	Configure Last Member Query Interval	switch>enable switch#configure switch(config)# <b>igmp last-query- interval 100</b>
<b>igmp query-interval</b> [1~250 sec.]	<b>G</b>	Configure Query Interval	switch>enable switch#configure switch(config)# <b>igmp query-interval 100</b>
<b>query-response- interval</b> [1~250 tenths of a sec.]	<b>G</b>	Configure Query Response Interval	switch>enable switch#configure switch(config)# <b>igmp query- response-interval 100</b>
<b>show igmp configuration</b>	<b>P</b>	Show IGMP configuration.	switch>enable switch# <b>show igmp configuration</b>
<b>show igmp table</b>	<b>P</b>	Show IGMP snooping table.	switch>enable switch# <b>show igmp table</b>
<b>no igmp</b>	<b>G</b>	Disable IGMP snooping function	switch>enable switch#configure switch(config)# <b>no igmp</b>
<b>no igmp query</b>	<b>G</b>	Disable IGMP query	switch>enable switch#configure switch(config)# <b>no igmp query</b>

**Multicast Static Filtering Table Commands Set – Мультиадресная Фильтрация**

Команды	Уро- вень	Описание	Пример
<b>multicast-filtering</b> [IP_addr]	<b>I</b>	Configure multicast filtering entry of interface.	switch>enable switch#configure switch(config)#interface fastEthernet 2 switch(config)# <b>multicast-filtering 225.100.100.100</b>
<b>no multicast-filtering</b> [IP_addr]	<b>I</b>	Remove multicast filtering entry of interface	switch>enable switch#configure switch(config)#interface fastEthernet 2 switch(config-if)# <b>no multicast-filtering 225.100.100.100</b>
<b>show multicast-filtering</b>	<b>P</b>	Show multicast filtering table	switch>enable switch# <b>show multicast-filtering</b>

**IP Security Commands Set – Защита IP**

Команды	Уро- вень	Описание	Пример
<b>security enable</b>	<b>G</b>	Enable IP security function	switch>enable switch#configure switch(config)# <b>security enable</b>
<b>security http</b>	<b>G</b>	Enable IP security of HTTP server	switch>enable switch#configure switch(config)# <b>security http</b>
<b>security telnet</b>	<b>G</b>	Enable IP security of telnet server	switch>enable switch#configure switch(config)# <b>security telnet</b>
<b>security snmp</b>	<b>G</b>	Enable IP security of SNMP server	switch>enable switch#configure switch(config)# <b>security snmp</b>
<b>security ip [Index(1..10)] [IP Address]</b>	<b>G</b>	Set the IP security list	switch>enable switch#configure switch(config)# <b>security ip 1 192.168.1.55</b>
<b>show security</b>	<b>P</b>	Show the information of IP security	switch>enable switch# <b>show security</b>
<b>no security</b>	<b>G</b>	Disable IP security function	switch>enable switch#configure switch(config)# <b>no security</b>
<b>no security http</b>	<b>G</b>	Disable IP security of HTTP server	switch>enable switch#configure switch(config)# <b>no security http</b>
<b>no security telnet</b>	<b>G</b>	Disable IP security of telnet server	switch>enable switch#configure switch(config)# <b>no security telnet</b>
<b>no security snmp</b>	<b>G</b>	Disable IP security of SNMP server	switch>enable switch#configure switch(config)# <b>no security snmp</b>

**Port Security Commands Set – Защита порта**

Команды	Уро- вень	Описание	Пример
<b>mac-address-table static hwaddr [HW-Addr]</b>	<b>I</b>	Configure MAC address entry of interface (static).	switch>enable switch#configure switch(config)#interface fastEthernet 2 switch(config-if)# <b>mac-address-table static hwaddr 000012345678</b>
<b>show mac-address-table static</b>	<b>P</b>	Show MAC address table (static)	switch>enable switch# <b>show mac-address-table static</b>
<b>no mac-address-table static hwaddr [HW-Addr]</b>	<b>I</b>	Remove an entry of MAC address table of interface (static)	switch>enable switch#configure switch(config)#interface fastEthernet 2 switch(config-if)# <b>no mac-address-table static hwaddr 000012345678</b>

**MAC Blacklist Commands Set – Черный список MAC-адресов**

Команды	Уро- вень	Описание	Пример
<b>mac-address-table filter hwaddr [HW-Addr]</b>	<b>G</b>	Configure MAC address entry of interface (filter)	switch>enable switch#configure switch(config)# <b>mac-address-table filter hwaddr 000012348678</b>
<b>show mac- address-table filter</b>	<b>P</b>	Show MAC address table (filter).	switch>enable switch# <b>show mac-address-table filter</b>
<b>no mac-address- table filter hwaddr [HW-Addr]</b>	<b>G</b>	Remove an entry of  MAC address table (filter)	switch>enable  switch#configure switch(config)# <b>no mac-address-table filter hwaddr 000012348678</b>

**802.1x Commands Set – Команды 802.1x**

Команды	Уро- вень	Описание	Пример
<b>8021x enable</b>	<b>G</b>	Enable IEEE802.1x function	switch>enable switch#configure switch(config)# <b>8021x enable</b>
<b>8021x system radiusip</b> [Radius Server IP]	<b>G</b>	Use the 802.1x system radius IP global configuration command to change the radius server IP.	switch>enable switch#configure switch(config)# <b>8021x system radiusip 192.168.1.1</b>
<b>8021x system serverport</b> [Port Number]	<b>G</b>	Use the 802.1x system server port global configuration command to change the radius server port	switch>enable switch#configure switch(config)# <b>8021x system serverport 1815</b>
<b>8021x system accountport</b> [Port Number]	<b>G</b>	Use the 802.1x system account port global configuration command to change the accounting port	switch>enable switch#configure switch(config)# <b>8021x system accountport 1816</b>
<b>8021x system sharedkey</b> [SharedKey]	<b>G</b>	Use the 802.1x system share key global configuration command to change the shared key value.	switch>enable switch#configure switch(config)# <b>8021x system sharedkey 123456</b>
<b>8021x system nasid</b> [NAS ID]	<b>G</b>	Use the 802.1x system nasid global configuration command to change the NAS ID	switch>enable switch#configure switch(config)# <b>8021x system nasid test1</b>
<b>8021x misc quietperiod</b> [Seconds]	<b>G</b>	Use the 802.1x misc quiet period global configuration command to specify the quiet period value of the switch.	switch>enable switch#configure switch(config)# <b>8021x misc quietperiod 10</b>
<b>8021x misc txperiod</b> [Seconds]	<b>G</b>	Use the 802.1x misc TX period global configuration command to set the TX period.	switch>enable switch#configure switch(config)# <b>8021x misc txperiod 5</b>
<b>8021x misc supptimeout</b> [Seconds]	<b>G</b>	Use the 802.1x misc supp timeout global configuration command to set the supplicant timeout.	switch>enable switch#configure switch(config)# <b>8021x misc supptimeout 20</b>
<b>8021x misc servertimeout</b> [Seconds]	<b>G</b>	Use the 802.1x misc server timeout global configuration command to set the server timeout.	switch>enable switch#configure switch(config)# <b>8021x misc servertimeout 20</b>
<b>8021x misc maxrequest</b> [number]	<b>G</b>	Use the 802.1x misc max request global configuration command to set the MAX requests.	switch>enable switch#configure switch(config)# <b>8021x misc maxrequest 3</b>
<b>8021x misc reauthperiod</b> [Seconds]	<b>G</b>	Use the 802.1x misc reauth period global configuration command to set the reauth period.	switch>enable switch#configure switch(config)# <b>8021x misc reauthperiod 3000</b>
<b>8021x portstate</b> [disable   reject   accept   authorize]	<b>I</b>	Use the 802.1x port state interface configuration command to set the state of the selected port.	switch>enable switch#configure switch(config)#interface fastethernet 3 switch(config-if)# <b>8021x portstate authorize</b>

**Команды 802.1x - продолжение**

Команды	Уро- вень	Описание	Пример
<b>show 8021x</b>	<b>P</b>	Displays a summary of the 802.1x properties and also the port sates.	switch>enable switch# <b>show 8021x</b>
<b>no 8021x</b>	<b>G</b>	Disable 802.1x function	switch>enable switch#configure switch(config)# <b>no 8021x</b>

**Fault Alarm Commands Set – Реле ошибок**

Команды	Уро- вень	Описание	Пример
<b>fault-relay power</b> [number] [enable/disable]	<b>G</b>	Configure Relay Alarm for Power Failure	switch>enable switch#configure switch(config)# <b>fault-relay power 1 enable</b>
<b>fault-relay</b> [enable/disable]	<b>I</b>	Configure Relay Alarm for Port Link Down/Broken	switch>enable switch#configure switch(config)#interface fastEthernet 1 switch(config-if)# <b>fault-relay enable</b>
<b>show fault-relay</b>	<b>P</b>	Show Fault Relay Alarm setting	switch>enable switch# <b>show fault-relay</b>
<b>no fault-relay</b>	<b>G</b>	Disable Fault Relay Alarm function	switch>enable switch#configure switch(config)# <b>no fault-relay</b>

**System Warning Commands Set – Системные предупреждения**

Команды	Уровень	Описание	Пример
<b>systemlog mode</b> [client server both]	<b>G</b>	Specified the log mode	switch>enable switch#configure switch(config)# <b>syslog mode both</b>
<b>systemlog ip</b> [IP address]	<b>G</b>	Set System log server IP address.	switch>enable switch#configure switch(config)# <b>syslog ip 192.168.1.100</b>
<b>show syslog</b>	<b>P</b>	Show SYSLOG configuration and log table.	switch>enable switch#configure switch# <b>show syslog</b>
<b>no syslog</b>	<b>G</b>	Disable systemlog function	switch>enable switch#configure switch(config)# <b>no syslog</b>
<b>smtp enable</b>	<b>G</b>	Enable SMTP function	switch>enable switch#configure switch(config)# <b>smtp enable</b>
<b>smtp serverip</b> [IP address]	<b>G</b>	Configure SMTP server IP	switch>enable switch#configure switch(config)# <b>smtp serverip 192.168.1.5</b>
<b>smtp sender</b> [sendername]	<b>G</b>	Configure sender of mail	switch>enable switch#configure switch(config)# <b>smtp sender test01</b>
<b>smtp subject</b> [subject]	<b>G</b>	Configure subject of mail	switch>enable switch#configure switch(config)# <b>smtp subject alarm</b>
<b>smtp authentication</b>	<b>G</b>	Enable SMTP authentication	switch>enable switch#configure switch(config)# <b>smtp authentication</b>
<b>smtp account</b> [account]	<b>G</b>	Configure authentication account	switch>enable switch#configure switch(config)# <b>smtp account John</b>
<b>smtp password</b> [password]	<b>G</b>	Configure authentication password	switch>enable switch#configure switch(config)# <b>smtp password 1234</b>
<b>smtp rcptemail</b> [Index] [Email address]	<b>G</b>	Configure Rcpt e-mail Address	switch>enable switch#configure switch(config)# <b>smtp rcptemail 1 Alert@test.com</b>
<b>show smtp</b>	<b>P</b>	Show the information of SMTP	switch>enable switch# <b>show smtp</b>
<b>no smtp</b>	<b>G</b>	Disable SMTP function	switch>enable switch#configure switch(config)# <b>no smtp</b>
<b>event device-restart</b> [Syslog SMTP Both]	<b>G</b>	Set device restart event type	switch>enable switch#configure switch(config)# <b>event device-restart both</b>
<b>event authentication-failure</b> [Sysog SMTP Both]	<b>G</b>	Set Authentication failure event type	switch>enable switch#configure switch(config)# <b>event authentication-failure both</b>

**Системные предупреждения - продолжение**

Команды	Уровень	Описание	Пример
<b>event syslog</b> [Link-UP Link-Down Both]	I	Set port event for SYSLOG	switch>enable switch#configure switch(config)#interface fastethernet 3 switch(config-if)# <b>event syslog both</b>
<b>event smtp</b> [Link-UP Link-Down Both]	I	Set port event for SMTP	switch>enable switch#configure switch(config)#interface fastethernet 3 switch(config-if)# <b>event smtp both</b>
<b>show event</b>	P	Show event selection	switch>enable switch# <b>show event</b>
<b>no event device-restart</b> [Syslog SMTP Both]	G	Disable device restart event type	switch>enable switch#configure switch(config)# <b>no event device-restart both</b>
<b>no event authentication-failure</b> [Syslog SMTP Both]	G	Disable Authentication failure event typ	switch>enable switch#configure switch(config)# <b>no event authentication-failure both</b>
<b>no event syslog</b>	I	Disable port event for system log	switch>enable switch#configure switch(config)#interface fastethernet 3 switch(config-if)# <b>no event syslog</b>
<b>no event smtp</b>	I	Disable port event for SMTP	switch>enable switch#configure switch(config)#interface fastethernet 3 switch(config-if)# <b>no event smtp</b>

**Mac Address Table Commands Set – Таблица MAC - адресов**

Команды	Уровень	Описание	Пример
<b>show mac-address-table</b>	I	Show MAC address table	switch>enable switch#configure switch(config)#interface fastethernet 2 switch(config-if)# <b>show mac-address-table</b>
<b>show mac-address-table all</b>	P	Show MAC address table (all)	switch>enable switch# <b>show mac-address-table all</b>
<b>no mac-address-table</b>	G	Remove dynamic entry of MAC address table	switch>enable switch#configure switch(config)# <b>no mac-address-table</b>
<b>agingtime</b> [seconds 0~3825 steps 15]	G	Configure mac address table aging time	switch>enable switch#configure switch(config)# <b>agingtime 30</b>
<b>auto-flush</b> [enable disable]	G	Auto flush mac address table when ports link down	switch>enable switch#configure switch(config)# <b>auto-flush enable</b>

**Port Statistics Commands Set – Статистика порта**

Команды	Уровень	Описание	Пример
<b>show interface accounting</b>	I	show interface statistic counter	switch>enable switch#configure switch(config)#interface fastEthernet 2 switch switch (config-if)# <b>show interface accounting</b>
<b>no accounting</b>	I	Clear interface accounting information	switch>enable switch#configure switch(config)#interface fastEthernet 2 switch(config-if)# <b>no accounting</b>

**Port Monitoring Commands Set – Мониторинг порта**

Команды	Уровень	Описание	Пример
<b>monitor destination</b> [RX TX Both]	I	Configure destination port of monitor function	switch>enable switch#configure switch(config)#interface fastEthernet 2 switch(config-if)# <b>monitor destination rx</b>
<b>monitor source</b> [RX TX Both]	I	Configure destination port of monitor function	switch>enable switch#configure switch(config)#interface fastEthernet 2 switch(config-if)# <b>monitor source rx</b>
<b>show monitor</b>	P	Show port monitor information	switch>enable switch# <b>show monitor</b>
<b>show monitor</b>	I	Show port monitor information	switch>enable switch#configure switch(config)#interface fastEthernet 2 switch(config-if)# <b>show monitor</b>
<b>no monitor</b>	I	Disable source port of monitor function	switch>enable switch#configure switch(config)#interface fastEthernet 2 switch(config-if)# <b>no monitor</b>

**System Event Log Commands Set – Архив системных событий**

Команды	Уровень	Описание	Пример
<b>show syslog</b>	P	Show SYSLOG configuration and log table.	switch>enable switch# <b>show syslog</b>

**Ping Commands Set - Пингование**

Команды	Уровень	Описание	Пример
<b>ping</b> [ip]	E	Ping function	switch> <b>ping 192.168.16.1</b>

**Loading Average Commands Set – Средняя загрузка**

Команды	Уровень	Описание	Пример
<b>loadavg</b>	<b>E</b>	Show system load average	switch> <b>loadavg</b>
<b>event loadavg</b> [Systemlog SMTP Both]	<b>G</b>	Set system load average event type	switch>enable switch#configure switch(config)# <b>event loadavg both</b>

**Factory Default Commands Set – Заводские настройки**

Команды	Уровень	Описание	Пример
<b>default</b> [keepip keepadmin both]	<b>G</b>	Restore to factory default configuration	switch>enable switch#configure switch(config)# <b>default both</b>

**System Reboot Commands Set – Перезагрузка системы**

Команды	Уровень	Описание	Пример
<b>reload</b>	<b>G</b>	Reboot switch	switch>enable switch#configure switch(config)# <b>reload</b>

**Logout Commands Set - Выход**

Команды	Уровень	Описание	Пример
<b>logout</b>	<b>E</b>	Logout command line shell	switch> <b>logout</b>