

# LTV NSG-7204P-01

4-портовый Ethernet-коммутатор



## Инструкция пользователя

Версия 1.0



[www.ltv-cctv.ru](http://www.ltv-cctv.ru)

Благодарим за приобретение нашего продукта. В случае возникновения каких-либо вопросов, связывайтесь с продавцом оборудования.

Данная инструкция подходит для Ethernet-коммутатора LTV NSG-7204P-01.

Сведения, представленные в данном руководстве, верны на момент опубликования. Производитель оставляет за собой право в одностороннем порядке без уведомления потребителя вносить изменения в изделия для улучшения их технологических и эксплуатационных параметров. Вид изделий может незначительно отличаться от представленного на фотографиях. Обновления будут включены в новую версию данной инструкции. Мы своевременно вносим изменения.

# СОДЕРЖАНИЕ

<b>1. ВВЕДЕНИЕ</b> .....	<b>6</b>
<b>2. ОПИСАНИЕ</b> .....	<b>7</b>
2.1. Внешний вид .....	7
<b>3. УСТАНОВКА</b> .....	<b>9</b>
3.1. Комплект поставки.....	9
3.2. Монтаж на DIN-рейку.....	9
3.3. Монтаж на стену .....	9
3.4. Подключение кабелей .....	10
3.4.1. Подключение устройств .....	10
3.4.2. Подключение кабеля для конфигурирования .....	10
3.4.3. Подключение кабеля электропитания .....	10
3.5. Рекомендации по установке .....	11
3.6. Рекомендации по электромагнитной совместимости .....	11
<b>4. КОНФИГУРИРОВАНИЕ</b> .....	<b>12</b>
4.1. Требуемое оборудование.....	12
4.2. Настройка сетевого подключения .....	12
4.2.1. Присвоение статического IP-адреса компьютеру.....	12
4.2.2. Проверка сетевого подключения .....	14
4.3. Веб-интерфейс .....	15
4.3.1. Аутентификация .....	15
4.3.2. Основные кнопки .....	16
4.3.3. Конфигурация по умолчанию .....	16
4.3.4. Время ожидания пользователя .....	17
4.3.5. Сохранение конфигурации .....	17
4.3.6. Восстановление конфигурации .....	17
4.3.7. Выход.....	17
<b>5. РАБОТА С ВЕБ-ИНТЕРФЕЙСОМ</b> .....	<b>18</b>
5.1. Меню System Status .....	18
5.2. Меню Port setting .....	18
5.2.1. Раздел Port setting .....	18
5.2.2. Раздел Rate Limit .....	20
5.3. Меню PoE .....	21
5.4. Меню VLAN .....	22
5.4.1. Раздел Port VLAN settings.....	22
5.4.2. Раздел VLAN forward list .....	24
5.5. Меню QoS.....	25
5.5.1. Раздел QoS setting .....	25
5.5.2. Раздел DSCP settings.....	26
5.6. LACP.....	27
5.6.1. Раздел TRUNK.....	27
5.6.2. Раздел FastRing .....	27
5.6.3. Раздел RSTP .....	29
5.7. Меню Port Security.....	32
5.7.1. Раздел Static address lock .....	32
5.7.2. Раздел 802.1X certification.....	33
5.8. Меню Network management .....	35
5.8.1. Раздел SNMP setting .....	35
5.8.2. Раздел Email alarm .....	36
5.8.3. Раздел Port mirror .....	37
5.8.4. Раздел IGMP Snooping.....	38
5.9. Меню Network Statistics.....	39
5.9.1. Раздел Packet statistics .....	39
5.9.2. Раздел MAC Address .....	40
5.10. Меню System Management .....	41

5.10.1. Раздел IP address .....	41
5.10.2. Раздел User management.....	41
5.10.3. Раздел Log information .....	42
5.10.4. Раздел File management .....	43
5.10.5. Раздел Alarm management.....	44
<b>6. ОБЖИМ КАБЕЛЯ ВИТОЙ ПАРЫ .....</b>	<b>46</b>
<b>7. УСТРАНЕНИЕ НЕИСПРАВНОСТЕЙ.....</b>	<b>47</b>
<b>8. ГАРАНТИЯ И ОГРАНИЧЕНИЯ .....</b>	<b>48</b>
<b>9. СПЕЦИФИКАЦИЯ .....</b>	<b>49</b>

## Предупреждения

- Для безопасной и правильной эксплуатации устройства перед началом работы с ним внимательно ознакомьтесь инструкцией.
- Перед чисткой устройства обесточьте его. Не используйте мокрую ткань или жидкости при чистке устройства.
- Данное устройство предназначено для эксплуатации только внутри помещений. Не используйте устройство под дождем или во влажной среде. При попадании посторонних предметов или жидкостей внутрь корпуса устройства немедленно выключите его и вызовите для осмотра квалифицированного специалиста.
- Не эксплуатируйте устройство в запыленных помещениях. Избыточная пыль в устройстве может привести к накоплению электростатического заряда, который негативно влияет на срок службы устройства и может привести к коммуникационным сбоям.
- Устройство должно использоваться только с тем типом источника питания, который указан в спецификации. Перед подключением устройства необходимо проверить напряжение электропитания. При длительном неиспользовании устройства отключите его от источника электропитания.
- Устройство должно эксплуатироваться вдали от мощных радиочастотных передатчиков, радаров и прочих источников высокочастотного электромагнитного излучения.
- При наличии сильных электромагнитных помех подключайте к устройству экранированные кабели.
- Кабели, подключенные к устройству, старайтесь по возможности прокладывать в помещении. Это позволит избежать перегрузок по напряжению и току.
- Во избежание поражения электрическим током не открывайте корпус устройства, даже если оно обесточено.
- Аксессуары, поставляемые с данным устройством, (в том числе кабели электропитания, блоки питания и т. д.) не предназначены для использования с другими устройствами.
- Для отвода избыточного тепла необходимо оставлять достаточно места для вентиляции оборудования, установленного в шкафах и стойках. Предпочтительно использовать активные системы охлаждения.
- При установке оборудования в шкафы и стойки необходимо удостовериться, что они выдержат его вес.
- Рекомендуется устанавливать оборудование в шкафы и стойки с заземлением.

# 1. Введение

LTV NSG-7204P-01 – управляемый Ethernet-коммутатор в промышленном исполнении с 4 портами Gigabit Ethernet, каждый из которых поддерживает подачу питания PoE / PoE+. Также в этом Ethernet-коммутаторе присутствует 2 порта uplink Gigabit Ethernet: формата SFP, в которые можно устанавливать разнообразные оптоволоконные SFP-модули. 4 основных порта поддерживают стандарты питания IEEE 802.3af и 802.3at с автоматическим обнаружением и определением класса питаемых устройств PoE и выдают до 30 Вт на каждый порт суммарной мощности до 150 Вт. Кроме того, первый порт поддерживает подачу питания 4PPoE с мощностью до 60 Вт, что позволяет подключать к нему PTZ IP-видеокамеры с высоким энергопотреблением.

## Основные особенности

- 4 порта 10/100/1000 Мбит/с (автоматическое определение MDI/MDIX)
- 2 порта uplink 1000 Мбит/с для модулей SFP
- Поддержка PoE, PoE+ (IEEE 802.3af, IEEE 802.3at) до 30 Вт на порт
- Поддержка 4PPoE до 60 Вт на первом порту
- Светодиодная индикация нагрузки PoE
- Управление распределением мощности PoE
- Управление через веб-интерфейс, VLAN, QoS, FastRing, RSTP, SNMP, IGMP Snooping, зеркалирование портов, отправка тревожных сообщений
- Протокол FastRing, время восстановления 20 мс
- Поддержка резервного источника питания
- Промышленное исполнение, безвентиляторная конструкция
- Быстрая установка, удобный монтаж на стену, на стол, на рейку DIN
- Грозозащита, защита от электростатических разрядов, высокая помехоустойчивость

**ВНИМАНИЕ:** Дальность передачи зависит от используемого кабеля. Для достижения максимальной дальности передачи рекомендуется стандартный кабель витой пары категории 5е/6.

## 2. Описание

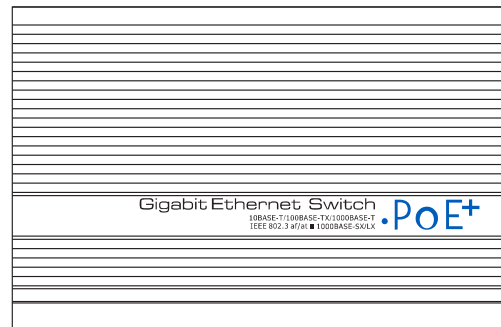
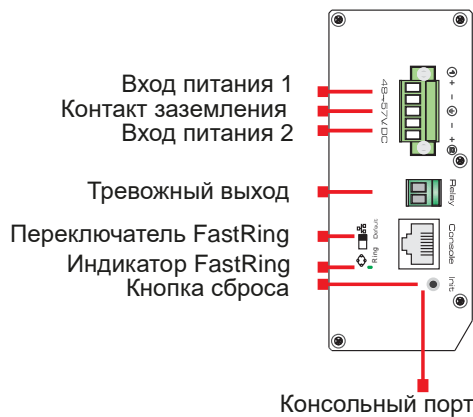
### 2.1. Внешний вид



Рис. 2.1. Внешний вид

На передней панели коммутатора расположены 4 основных порта Ethernet с поддержкой питания PoE и 2 порта uplink. Входы питания, контакт заземления, переключатель FastRing, тревожный выход и консольный порт находятся на левой панели.

#### Левая панель



#### Передняя панель

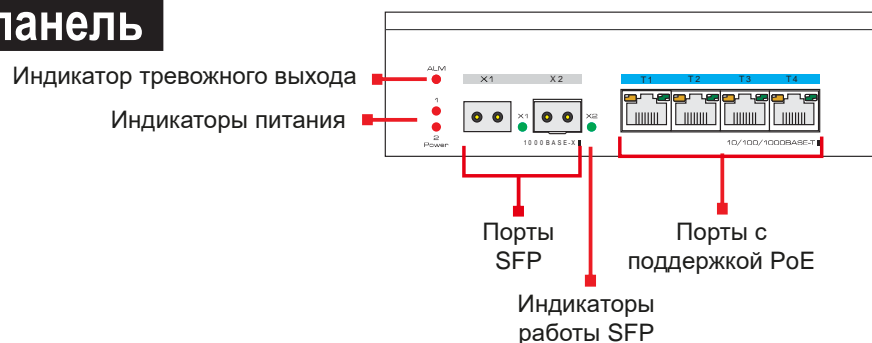
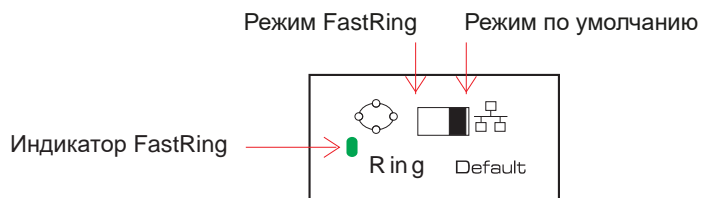


Рис. 2.2. Расположение разъемов и индикаторов



В режиме FastRing порты SFP X1 и X2 формируют кольцо FastRing

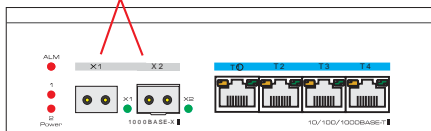


Рис. 2.3. Включение и выключение режима FastRing

**ВНИМАНИЕ:** Грозозащита возможна только при правильном заземлении устройства. Для заземления используйте провод калибра 20 AWG или более толстый, который подключается к контакту заземления коммутатора.



## 3. Установка

Для данного коммутатора предусмотрены следующие варианты установки: настольный, настенный и на DIN-рейку.

### 3.1. Комплект поставки

Перед установкой проверьте комплект поставки устройства. При неполной комплектации свяжитесь с продавцом.

Наименование	Количество
4-портовый Ethernet-коммутатор	1 шт.
Блок питания	1 шт.
Набор крепежных аксессуаров	1 шт.
Инструкция пользователя	1 шт.

Прежде чем приступить к установке обесточьте подключаемое оборудование, иначе вы можете его повредить. Заземление и грозозащита значительно повышают защищенность коммутатора.

### 3.2. Монтаж на DIN-рейку

1. Прикрепите винтами к коммутатору кронштейн для монтажа на DIN-рейку.

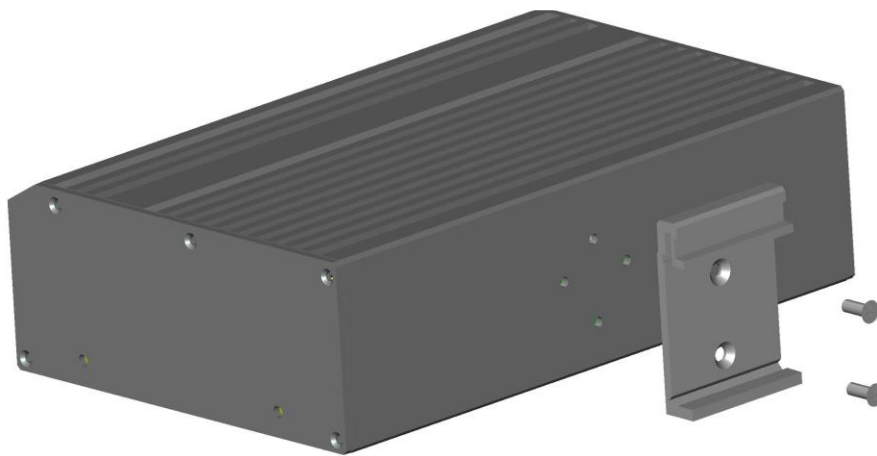


Рис. 3.1. Крепление кронштейна для монтажа на DIN-рейку

2. Установите коммутатор на DIN-рейку.

### 3.3. Монтаж на стену

Также вы можете установить коммутатор на прочную стену.

1. Прикрепите винтами к коммутатору кронштейны для монтажа на стену.



Рис. 3.2. Крепление кронштейнов для монтажа на стену

2. Установите коммутатор на стену.

## 3.4. Подключение кабелей

### 3.4.1. Подключение устройств

Для подключения компьютеров и других устройств к портам коммутатора используйте кабели витой пары с прямым или перекрестным обжимом.

### 3.4.2. Подключение кабеля для конфигурирования

Используйте кабель витой пары, чтобы подключить компьютер для конфигурирования к любому порту коммутатора кроме консольного порта.

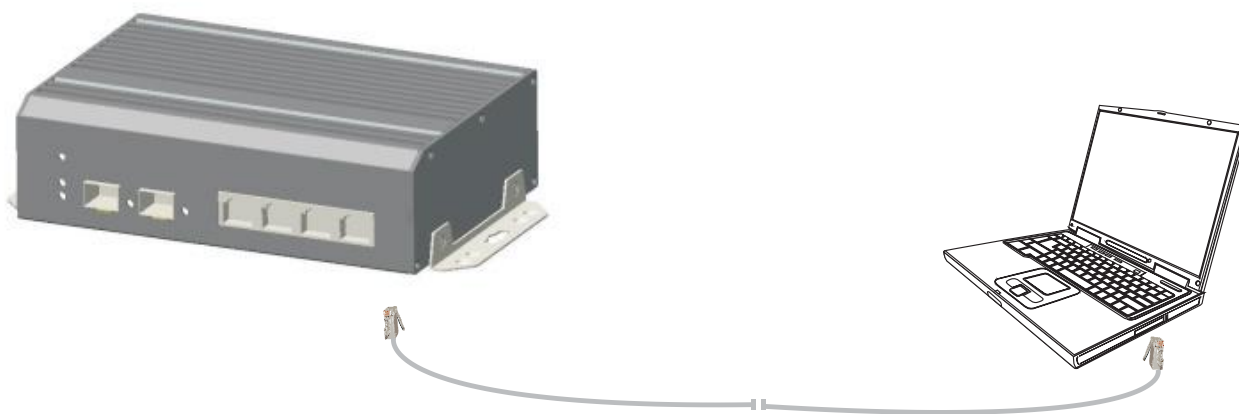


Рис. 3.3. Подключение кабеля для конфигурирования

### 3.4.3. Подключение кабеля электропитания

1. Подключите красный провод блока питания к контакту + и черный провод к контакту – разъема электропитания коммутатора, как показано на Рис. 3.4. Закрепите отверткой провода в контактной колодке.

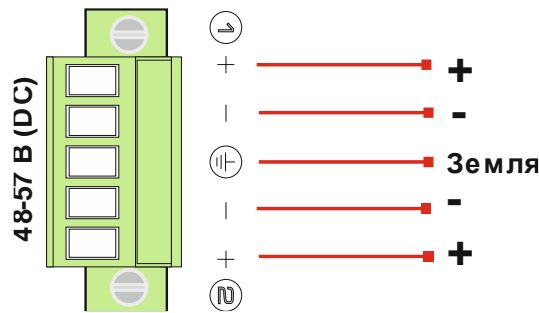


Рис. 3.4. Назначение контактов разъема электропитания

2. Включите питание. При правильном подключении загорится индикатор питания.

### 3.5. Рекомендации по установке

Коммутатор предназначен для эксплуатации внутри помещений. Независимо от варианта монтажа следует учитывать следующие требования.

- Необходимо оставлять зазоры более 10 см по бокам от корпуса устройства для нормального охлаждения.
- В помещении для установки коммутатора должна быть хорошая вентиляция.
- Поверхность, на которую устанавливается коммутатор, должна выдерживать его вес вместе с аксессуарами.
- Стойки и столы для установки коммутатора должны иметь заземление.

### 3.6. Рекомендации по электромагнитной

#### совместимости

Во время работы коммутатор может подвергнуться внешнему электромагнитному воздействию. Следует учитывать следующие рекомендации по электромагнитной совместимости.

- Коммутатор следует устанавливать вдали от мощных радиопередатчиков, радаров и высокочастотных устройств.
- При необходимости используйте экранированные кабели.

## 4. Конфигурирование

### 4.1. Требуемое оборудование

Для конфигурирования коммутатора необходим компьютер с установленным Ethernet-адаптером. Подключите Ethernet-адаптер компьютера кабелем витой пары к любому порту коммутатора кроме консольного. Порт коммутатора, который используется для конфигурирования должен принадлежать к VLAN, в которой разрешено конфигурирование (по умолчанию VLAN1).

### 4.2. Настройка сетевого подключения

Когда вы подключаетесь к коммутатору в первый раз, вы можете использовать приведенные в таблице сетевые настройки по умолчанию.

<b>IP-адрес</b>	192.168.1.200
<b>Маска подсети</b>	255.255.255.0

IP-адреса компьютера и коммутатора должны находиться в одном сегменте IP-сети. Данное устройство не умеет самостоятельно назначать статический IP-адрес компьютеру, который используется для конфигурирования, поэтому эту процедуру необходимо выполнить вручную. Настройка сетевого подключения дана на примере операционной системы Windows 7. Для настройки сетевого подключения выполните следующие действия.

#### 4.2.1. Присвоение статического IP-адреса компьютеру

1. Вручную назначьте IP-адрес компьютера. IP-адрес компьютера должен находиться в одном сегменте сети с IP-адресом видеокamеры по умолчанию. В **Панели управления** откройте **Центр управления сетями и общим доступом**. Нажмите **Подключение по локальной сети** для перехода к следующему окну.

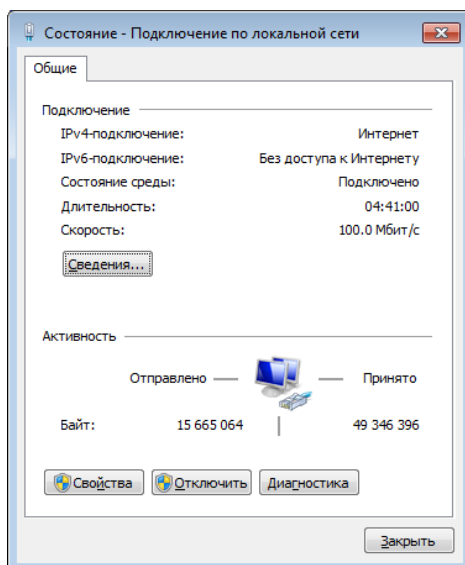


Рис. 4.1. Подключение по локальной сети

2. В появившемся окне нажмите кнопку **Свойства**. Выберите версию интернет протокола **Протокол Интернета версии 4 (TCP/IP)**. Далее нажмите кнопку **Свойства**, чтобы сконфигурировать сетевые параметры протокола **TCP/IP** для данного компьютера. На закладке **Основные** введите IP-адрес (используйте значение из диапазона 192.168.1.1...192.168.1.254, кроме 192.168.1.200) и маску подсети (255.255.255.0). Значения адресов DNS-серверов вы можете оставить пустым либо указать реальные IP-адреса. Нажмите **ОК**, чтобы выйти и применить сетевые настройки.

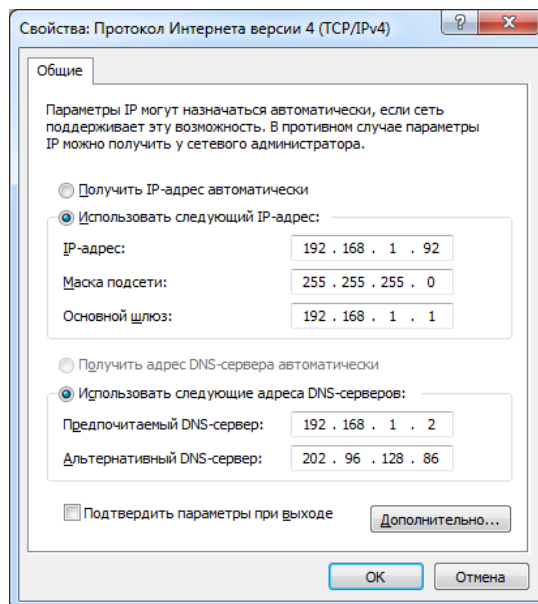


Рис. 4.2. Настройки TCP/IP

**ВНИМАНИЕ:** Если компьютер, который используется для конфигурирования коммутатора, настроен подключаться к сети через прокси-сервер, то это нужно отключить. В **Панели управления** откройте **Свойства браузера** и выберите вкладку **Подключения**. Щелкните мышью на кнопке **Настройка сети** и снимите галочку с пункта **Использовать прокси-сервер для локальных подключений**.

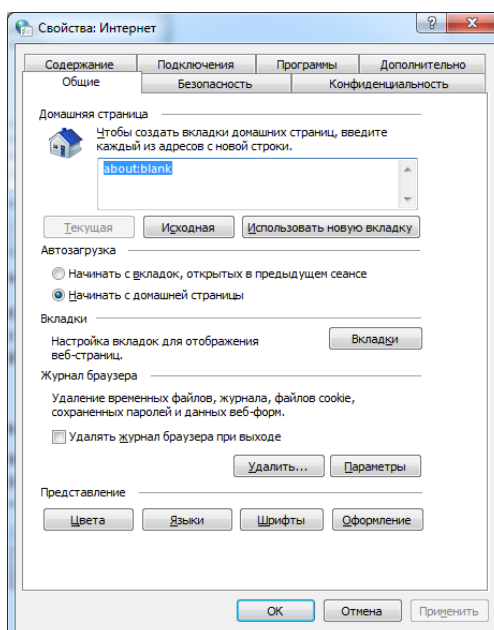


Рис. 4.3. Свойства браузера

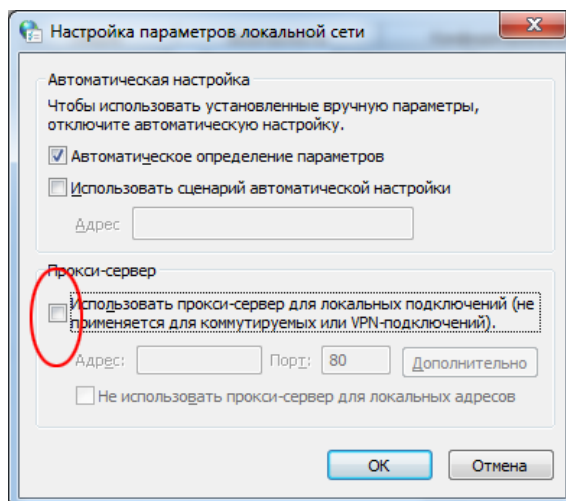


Рис. 4.4. Отключение прокси-сервера

### 4.2.2. Проверка сетевого подключения

1. Нажмите кнопку **Пуск**, в строке поиска наберите **cmd** и нажмите кнопку **Enter**, чтобы открыть окно командной строки.

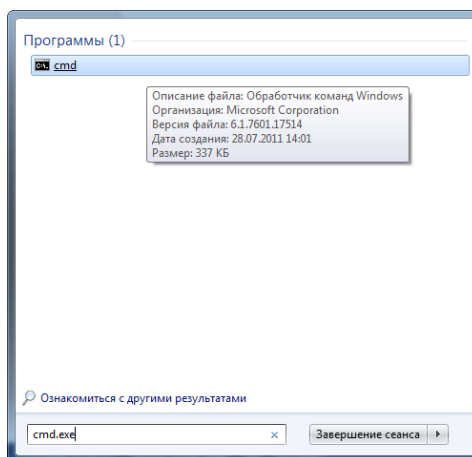


Рис. 4.5. Запуск окна командной строки

2. В окне командной строки введите команду **ping 192.168.1.200** и нажмите кнопку **Enter**. Если сетевое подключение настроено правильно, то коммутатор выдаст примерно такой ответ, как на Рис. 4.6. В противном случае проверьте сетевые настройки и работоспособность оборудования.

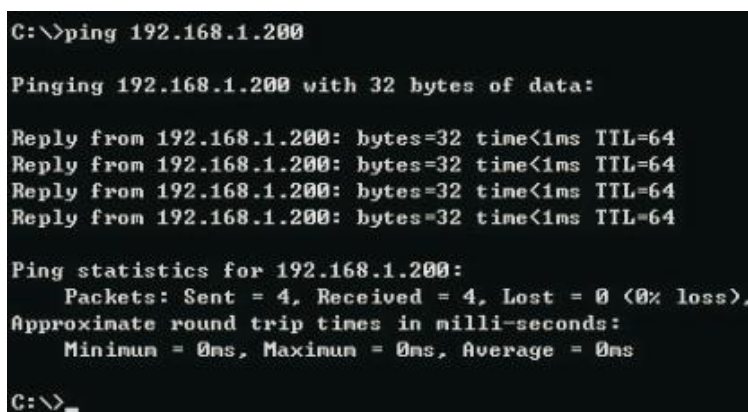


Рис. 4.6. Окно командной строки

Чтобы проверить правильность настройки сетевого подключения к коммутатору выполните следующие действия.

1. Проверьте физическое соединение между компьютером и коммутатором. Используйте при проверке другой кабель витой пары и подключите его к другому порту коммутатора (кроме консольного порта). Убедитесь, что загорелся соответствующий данному порту индикатор соединения.
2. Проверьте у компьютера настройки TCP/IP. IP-адрес компьютера должен быть 192.168.1.x (x находится в диапазоне 1...254, кроме 200, так как это IP-адрес самого коммутатора и он будет с ним конфликтовать), маска подсети – 255.255.255.0.

## 4.3. Веб-интерфейс

Для работы с веб-интерфейсом коммутатора рекомендуются следующие веб-браузеры: Internet Explorer 7 (и выше), Firefox, Chrome 11.

### 4.3.1. Аутентификация

Для аутентификации пользователя необходимо знать имя пользователя, пароль, IP-адрес коммутатора. Значения по умолчанию приведены в следующей таблице.

<b>IP-адрес</b>	192.168.1.200
<b>Маска подсети</b>	255.255.255.0
<b>Имя администратора</b>	admin
<b>Пароль администратора</b>	admin

Откройте веб-браузер, в его адресной строке введите IP-адрес коммутатора и нажмите кнопку **Enter**, чтобы открыть окно аутентификации (Рис. 4.7).

Authentication Required

The server http://192.168.1.184:80 requires a username and password. The server says: Managed Switch.

User Name:

Password:

Log In Cancel

Рис. 4.7. Окно аутентификации

После ввода правильного имени пользователя и пароля и нажатия кнопки **Log In** в веб-браузере, появится веб-интерфейс.

System status	
World time zone	(GMT+08:00) China, Hong Kong, Australia Western
	<input type="checkbox"/> Auto adjust DST
Time allocation	<input checked="" type="radio"/> Local time <input type="radio"/> Use NTP
NTP server	<input type="text"/> (Optional)
System time	06/08/2017 10:55:50
PC time	06/08/2017 10:55:43 <input type="button" value="update time to switch"/>
Device name	<input type="text"/>
Contact information	<input type="text"/>
Contact address	<input type="text"/>
MAC address	c4:08:80:00:01:11
Hardware version	v0.1
Software version	1.0.1a_M6P_B1M_T1
Running time	00:04:33
CPU temperature	31.5°C

Рис. 4.8. Веб-интерфейс

#### 4.3.2. Основные кнопки

Назначение основных кнопок веб-интерфейса указано в следующей таблице.

Кнопка	Функция
<b>Help</b>	Открыть справку по текущей странице веб-интерфейса
<b>Apply</b>	Подтвердить введенные значения и подтвердить ввод информации
<b>Cancel</b>	Отменить введенные значения
<b>Return</b>	Вернуться на предыдущую страницу
<b>New page</b>	Открыть новой страницей
<b>Select all</b>	Выбрать все порты на текущей странице
<b>Refresh</b>	Обновить данные на текущей странице
<b>Delete all</b>	Удалить все выбранные пункты в данном разделе

#### 4.3.3. Конфигурация по умолчанию

В следующей таблице перечислены основные параметры конфигурации коммутатора и их значения по умолчанию, которые оптимальны в большинстве случаев. Вы можете изменить эти значения, если они не соответствуют условиям эксплуатации.

	Параметр	Значение по умолчанию
<b>System</b>	<b>Username / password</b>	admin/admin
	<b>IP Address</b>	IP Address : 192.168.1.200 Subnet Mask : 255.255.255.0
	<b>MAC address table aging time</b>	300 Seconds
<b>Port</b>	<b>Ports Status</b>	Enable
	<b>Ports Speed Rate</b>	Auto-negotiation
	<b>Port duplex mode</b>	Auto-negotiation



	<b>Flow Control</b>	Open
	<b>Trunking</b>	Port does not converge
	<b>Port Speed Limitation</b>	No limitation for Speed
	<b>Port Link Type</b>	Access
<b>VLAN</b>	<b>Management VLAN</b>	VLAN 1
	<b>VLAN Function Mode</b>	Port-based VLAN
<b>MAC Binding</b>		No Binding
<b>RSTP</b>	<b>RSTP Function</b>	Close
<b>Network Management</b>	<b>SNMP</b>	Close

#### 4.3.4. Время ожидания пользователя

Если пользователь не проявляет никакой активности в веб-интерфейсе, по истечении некоторого времени сеанс работы будет автоматически завершен и пользователю будет заново выведено окно авторизации. Для продолжения работы необходимо будет снова ввести пароль. По умолчанию время ожидания пользователя составляет 5 минут.

#### 4.3.5. Сохранение конфигурации

Нажмите кнопку **Backup** для сохранения файла конфигурации. В дальнейшем вы сможете восстановить конфигурацию настроек вашего коммутатора, используя сохраненный файл с расширением cfg.

#### 4.3.6. Восстановление конфигурации

Нажмите кнопку **Browse** и выберите ранее сохраненный файл конфигурации с расширением cfg. Нажмите кнопку **Recover** для восстановления конфигурации. Конфигурации настроек будет восстановлена и вступит в силу после автоматической перезагрузки коммутатора.

#### 4.3.7. Выход

Нажмите кнопку **Exit**, чтобы выйти из веб-интерфейса. После этого появится окно авторизации с предложением ввести имя пользователя и пароль.

## 5. Работа с веб-интерфейсом

### 5.1. Меню System Status

В меню **System Status** собраны системные параметры и настройки коммутатора. Они перечислены в таблице ниже.

Параметр	Описание
<b>Word Time Zone</b>	Здесь вы можете выбрать различные часовые пояса и включить автоматический переход на летнее/зимнее время.
<b>Time Configuration</b>	Вы можете настроить время вручную или синхронизировать его с NTP-сервером
<b>NTP Server</b>	Протокол NTP используется для автоматической синхронизации сетевых устройств. Введите IP-адрес NTP-сервера, чтобы активировать синхронизацию.
<b>System Time</b>	Текущее системное время устройства
<b>PC Time</b>	Текущее системное время компьютера
<b>Device Name</b>	Имя коммутатора
<b>Contacts</b>	Контакты системного администратора устройства
<b>Contact Address</b>	Адрес системного администратора устройства
<b>MAC Address</b>	Уникальный MAC-адрес устройства в шестнадцатеричном формате
<b>Hardware, Software Version</b>	Версия программного и аппаратного обеспечения устройства
<b>Running Time</b>	Время непрерывной работы коммутатора. После перезагрузки время обнуляется.

### 5.2. Меню Port setting

#### 5.2.1. Раздел Port setting

Здесь вы можете получить информацию об основных параметрах портов и их текущем статусе, а также можете включить или отключить порт, установить скорость обмена данными (**Port speed**), включить или выключить контроль потока данных (**Flow control**), выбрать режим дуплексного соединения (**Duplex mode**).

Подробное описание настроек портов дано в следующей таблице.

Параметр	Описание
<b>Port Enable</b>	Устанавливает статус порта. Если порт отключен ( <b>Disable</b> ), коммутация для данного порта не осуществляется. По умолчанию порт включен ( <b>Enable</b> ).

<b>Port rate</b>	Устанавливает скорость обмена данными для данного порта. Доступны следующие значения: 10 Мбит/с ( <b>10Mbit/s</b> ), 100 Мбит/с ( <b>100Mbit/s</b> ), 1000 Мбит/с ( <b>1000Mbit/s</b> ), автоматически ( <b>Auto negotiation</b> ). По умолчанию установлено автоматическое определение скорости передачи данных ( <b>Auto negotiation</b> ), то есть коммутатор автоматически согласовывает с подключенным к данному порту устройством максимальную скорость обмена данными.
<b>Duplex mode</b>	Устанавливает режим дуплексного соединения для данного порта. Доступны следующие значения: полнодуплексный ( <b>Full duplex</b> ), полудуплексный ( <b>Half duplex</b> ), автоматический ( <b>Auto negotiation</b> ). По умолчанию установлен автоматический режим.
<b>Flow control</b>	Включает или выключает функцию контроля передачи данных. Если у обоих соединенных между собой коммутаторов включен контроль передачи данных, то в случае переполнения буфера данных у одного из них другой получает об этом сообщение и временно прекращает передачу данных или снижает скорость передачи данных. Данная функция позволяет избежать потери пакетов и обеспечивает нормальную работу сетевых служб. Функция контроля передачи данных включена по умолчанию.

### Пример

В качестве примера установим для портов с 1 по 10 скорость передачи данных 100 Мбит/с в полудуплексном режиме и отключим для них контроль передачи данных. Для этого необходимо выполнить следующие действия.

1. В поле диапазона портов (**Port range**) введите порты T1...X2 или отметьте их напрямую в списке портов.
2. Выберите скорость обмена данными (**Port rate**) в выпадающем списке 100 Мбит/с (**100M**).
3. Выберите режим дуплексного соединения (**Duplex mode**) в выпадающем списке полудуплексный (**Half duplex**).
4. Отключите (**Disable**) функцию контроля передачи данных (**Flow control**).
5. Нажмите кнопку **OK**, чтобы применить изменения или кнопку **Save**.

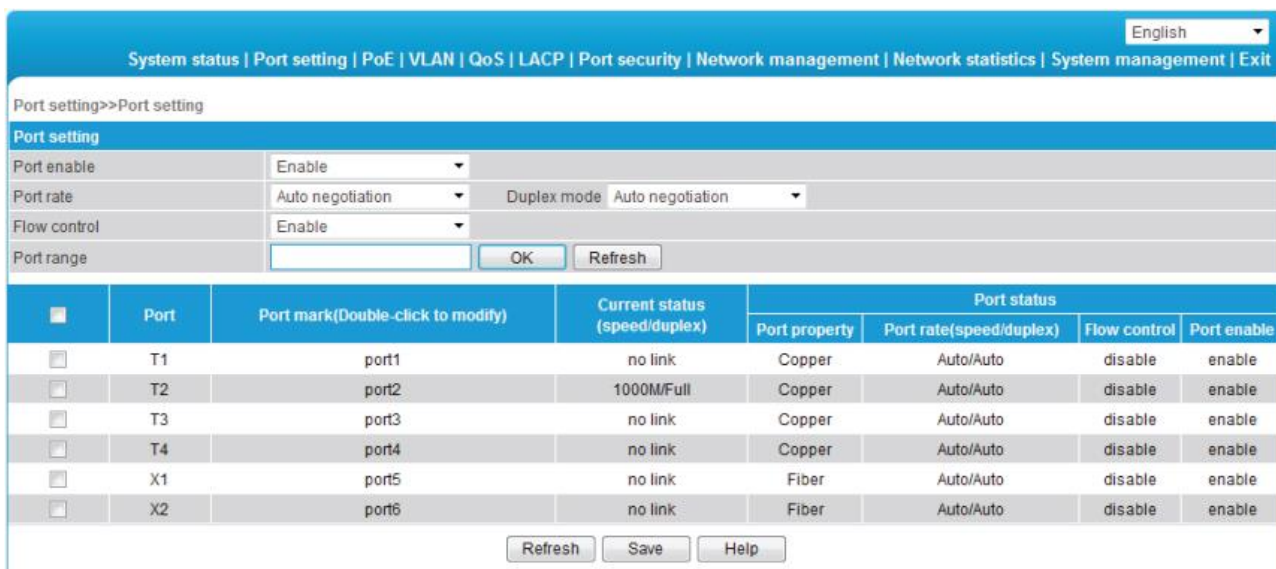


Рис. 5.1. Раздел настроек портов

### 5.2.2. Раздел Rate Limit

В этом разделе меню можно ограничивать скорость передачи данных для каждого порта коммутатора. Пользователь может устанавливать ограничение скорости входящей и нисходящей передачи данных или отключить ограничение. Можно выбирать значения от 64 Кбит/с до 1000 Мбит/с.

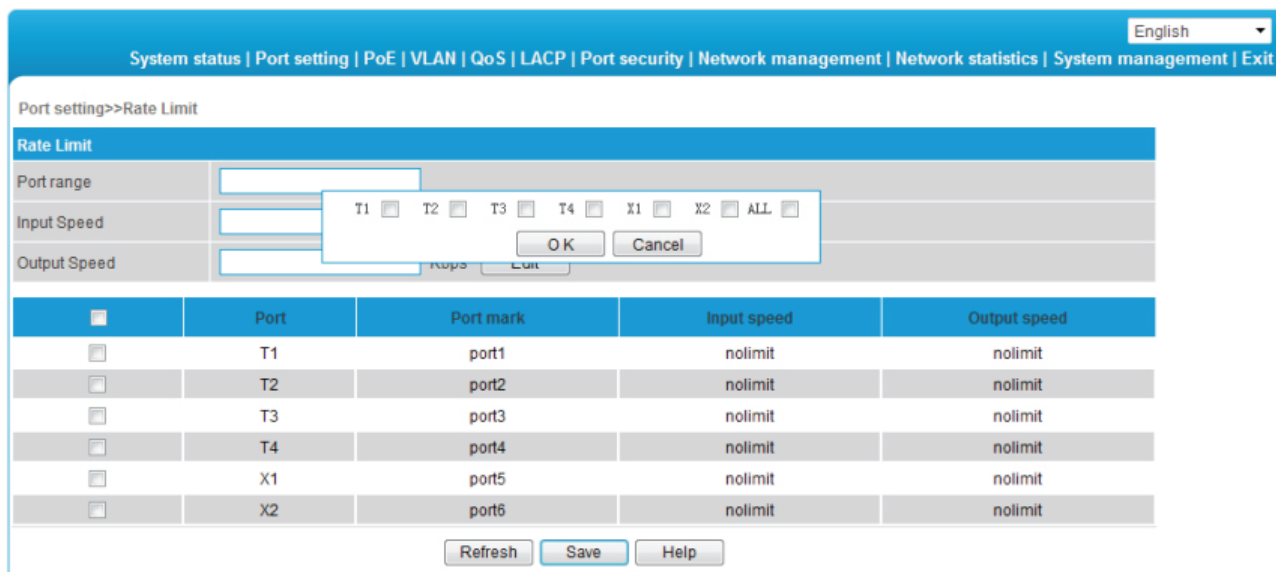


Рис. 5.2. Ограничение скорости передачи

Ограничение скорости касается всех типов трафика (unicast, multicast, broadcast). Если скорость передачи данных превысит пороговое значение, коммутатор будет отбрасывать пакеты либо воспользуется функцией контроля передачи данных, чтобы снизить скорость передачи данных у другого коммутатора.

Параметр	Описание
<b>Port range</b>	Порты, к которым нужно применить ограничение.
<b>Input Speed</b>	Максимальная скорость входящей передачи данных.
<b>Output Speed</b>	Максимальная скорость исходящей передачи данных.

## Пример

В качестве примера установим для портов с T1 по T4 ограничение скорости передачи данных 50 Мбит/с в полудуплексном режиме и отключим для них контроль передачи данных. Для этого необходимо выполнить следующие действия.

1. Перейдите в раздел меню **Rate Limit**.
2. Отметьте порты с T1 по T4, введите ограничение скорости 50 (Мбит/с).
3. Нажмите кнопку **Apply**, чтобы применить изменения или **Save** для сохранения.

## 5.3. Меню PoE

В меню управления электропитанием PoE вы можете включить или отключить его, настроить общую мощность PoE, максимальную перегрузку, резерв мощности и т. п.

Описание основных параметров дано в таблице ниже.

Параметр	Описание
<b>Power provided</b>	Общая мощность PoE, которая зависит от мощности встроенного блока питания и не должна ее превышать.
<b>Overload limit</b>	Встроенный блок питания допускает кратковременные перегрузки по мощности. Вы можете установить предельное значение в диапазоне 0%~10%, по умолчанию установлено 5%. Если энергопотребление превысит установленный предел перегрузки по мощности, коммутатор начнет отключать порты в соответствии с их приоритетом.
<b>Reserved rate</b>	Резерв мощности, который не участвует в распределении мощности между портами, но задействуется при перегрузке. По умолчанию установлено 15% от общей мощности. Чем больше это значение, тем меньше риск перегрузки, но тем меньше доступной мощности для распределения между портами, и наоборот – чем меньше резерв мощности, тем выше риск перегрузки.
<b>Consumed</b>	Показывает текущее энергопотребление.
<b>Remaining</b>	Показывает доступную для распределения между портами мощность, которая рассчитывается как общая мощность - резерв мощности – потребляемая на данный момент портами мощность. Обратите внимание, что при подключении к коммутатору нового оборудования с питанием PoE ему будет выделена мощность в соответствии с классом PoE, а не фактическим энергопотреблением. Например, если доступная мощность составляет 20 Вт, коммутатор не сможет выделить мощность на тот порт, к которому подключается устройство с классом энергопотребления 25.5 Вт, даже если реальное энергопотребление составляет всего 10 Вт.
<b>Reserved</b>	Показывает зарезервированную под перегрузку мощность в Вт.
<b>Provided</b>	Показывает общую мощность.
<b>Priority</b>	Предусмотрено три уровня приоритетов: <b>Low</b> (низкий), <b>Middle</b> (средний), <b>High</b> (высокий). В случае перегрузки по мощности отключение портов будет происходить в соответствии с приоритетом. В первую очередь отключаются порты с низким приоритетом.
<b>Power limit</b>	Максимальная мощность для данного порта. При превышении данного значения порт автоматически отключается.

<b>On/ Off</b>	Включение и отключение электропитания PoE.
<b>Apply</b>	Сохраняет заданные приоритет и максимальную мощность для выбранных портов.

**ВНИМАНИЕ:**

- Не изменяйте без необходимости значение доступной мощности PoE. Если это значение превысит мощность встроенного блока питания, он может выйти из строя. Если это значение меньше мощности встроенного блока питания, ее не удастся полностью распределить между портами коммутатора.
- Каждый порт поддерживает максимальную выходную мощность 30 Вт. Даже если выбрано значение, превышающее 30 Вт, выходная мощность составит 30 Вт. (Исключение составляет первый порт – T1. В режиме 4PoE++ он может выдать до 60 Вт и совместим с устройствами LTV, Dahua и Hikvision).

The screenshot displays the PoE configuration page. At the top, there is a navigation bar with links: System status | Port setting | PoE | VLAN | QoS | LACP | Port security | Network management | Network statistics | System management | Exit. The language is set to English.

**PoE**

**Power setting (Be careful for modification)**

Power provided: 150 W | Overload limit: 5 % | Reserved rate: 0 % | [OK]

**Power status**

Consumed: 0 W | Remaining: 150 W | Reserved: 0 W | Provided: 150 W

**Port status and control**

Port range: [ ] | Priority: Low | Power limit: [ ] W (0-60W) | [ON] [OFF] [OK]

	Port	Port mark	Consumed (W)	Setting		
				Power limit (W)	Priority	Port status
<input type="checkbox"/>	T1	port1	0	60	Low	close
<input type="checkbox"/>	T2	port2	0	30	Low	close
<input type="checkbox"/>	T3	port3	0	30	Low	close
<input type="checkbox"/>	T4	port4	0	30	Low	close

[Refresh] [Help]

Рис. 5.3. Управление питанием PoE

## 5.4. Меню VLAN

VLAN – виртуальная (логическая) локальная сеть. В коммутируемых сетях виртуальные локальные сети позволяют реализовать сегментацию и предоставляют необходимую организационную гибкость. Сети VLAN дают возможность группировать устройства в пределах одной физической локальной сети. Группа устройств в составе VLAN обменивается данными так, как если бы они были подключены к широковещательному домену. Сети VLAN основаны на логических, а не физических соединениях. Коммутатор поддерживает два способа организации работы VLAN: по порту или по идентификатору VLAN, определенному в протоколе IEEE802.1Q.

### 5.4.1. Раздел Port VLAN settings

Здесь вы можете видеть настройки VLAN для всех портов коммутатора и настроить такие параметры как тип порта (**Link type**), VLAN ID по умолчанию (**Default VLAN ID**), передача пакетов VLAN (**VLAN forward list**), удаление VLAN ID (**VLAN untagged mark list**).

Описание основных параметров дано в таблице ниже.

Параметр	Описание
<b>Link Type</b>	Существует два типа портов: <b>Access:</b> порт принадлежит только одной сети VLAN (Default VLAN). По умолчанию всем портам присвоен этот тип. <b>Trunk:</b> порт принадлежит нескольким сетям VLAN и может принимать и отправлять пакеты VLAN с разрешенными VLAN ID.
<b>Default VLAN ID</b>	Идентификатор VLAN по умолчанию (обычно в диапазоне от 1 до 4094, также называется PVID или native VLAN). Идентификатор VLAN по умолчанию назначается всем пакетам, приходящим на данный порт. Ethernet-кадр не может существовать в коммутаторе без метки VLAN, поэтому коммутатор назначает метку Default VLAN всем кадрам без метки.
<b>VLAN forward list</b>	Передача пакетов сети или сетей с указанным(и) VLAN разрешена на выбранных портах. Пакеты с другими метками VLAN будут отброшены.
<b>VLAN untagged mark list</b>	Все пакеты из данной сети или данных сетей VLAN будут обработаны как пакеты без меток (коммутатор поместит их в сеть VLAN по умолчанию). Кроме того, коммутатор удалит в исходящих пакетах указанные метки VLAN.

VLAN>>Port VLAN

Port range:

Link type: Direct connect terminal

Default VLAN ID:

VLAN forwarding list:

Vlan-untagged mark list:  OK

<input type="checkbox"/>	Port	Port mark	Link type	Default VLAN ID	VLAN forwarding list	Vlan-untagged mark list
<input type="checkbox"/>	T1	port1	Access	1		
<input type="checkbox"/>	T2	port2	Access	1		
<input type="checkbox"/>	T3	port3	Access	1		
<input type="checkbox"/>	T4	port4	Access	1		
<input type="checkbox"/>	X1	port5	Access	1		
<input type="checkbox"/>	X2	port6	Access	1		

Refresh Save Help

Рис. 5.4. Настройки VLAN

### ВНИМАНИЕ:

- VLAN ID может принимать значения в диапазоне 1...4094.
- Список разрешенных VLAN ID должен содержать только существующие VLAN.

Тип порта	Обработка полученных пакетов		Процедура обработки VLAN ID
	Полученные пакеты без VLAN ID	Полученные пакеты с VLAN ID	
<b>Access</b>	К пакету без метки добавляется VLAN ID по умолчанию.	Если VLAN ID полученного пакета совпадает с VLAN ID по умолчанию, то пакет принимается, в противном случае он отбрасывается.	Перед отправкой пакета из него удаляется VLAN ID.
<b>Trunk</b>	К пакету без метки добавляется VLAN ID по умолчанию.	Коммутатор сравнивает VLAN ID полученного пакета со списком разрешенных VLAN ID. Если они совпадают, пакет пропускается, в противном случае отбрасывается.	Если VLAN ID исходящего пакета совпадает с VLAN ID по умолчанию, VLAN ID удаляется из пакета. Если они различаются, то коммутатор проверяет VLAN ID исходящего пакета со списком разрешенных VLAN ID и при совпадении отправляет пакет, в противном случае отбрасывает.

### 5.4.2. Раздел VLAN forward list

В данном разделе вы можете посмотреть сконфигурированные VLAN, их описание и порты, которые в них участвуют.

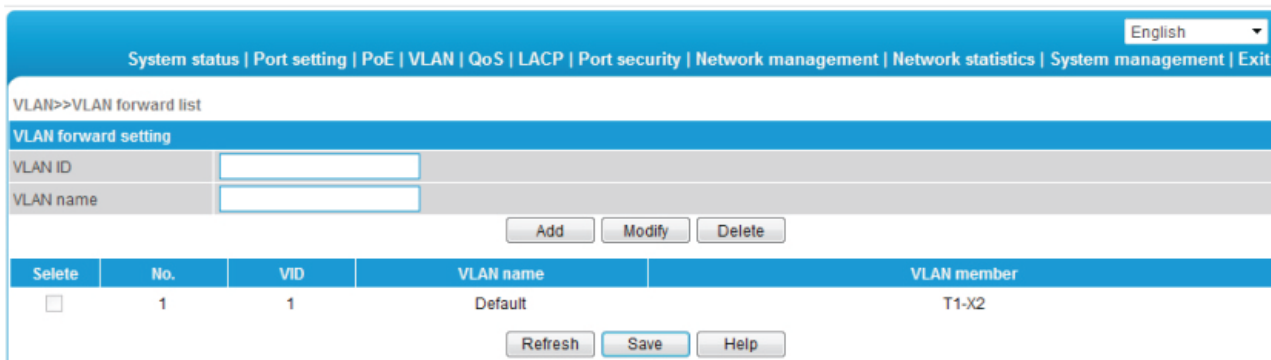


Рис. 5.5. Таблица VLAN

Описание основных параметров дано в таблице ниже.

Параметр	Описание
<b>VLAN ID</b>	VLAN ID
<b>VLAN Name</b>	Имя VLAN



## 5.5. Меню QoS

QoS (Quality of Service, качество обслуживания) – общая концепция, которая рассматривает все сервисы в терминах спроса и предложения и используется для приоритезации трафика. QoS оценивает возможности того или иного сервиса по отношению к ключевым требованиям, таким как задержка, фазовый сдвиг и коэффициент потери пакетов.

В спецификациях IEEE, посвященных приоритезации трафика для коммутаторов и других сетевых устройств, перечислено восемь классов трафика, из которых Класс 7 имеет высший приоритет и зарезервирован для передачи данных управления сетью, таких как обновления таблиц протоколов OSPF (Open Shortest Path First) и RIP (Routing Information Protocol). Классы 6 и 5 могут быть задействованы для передачи голосовых данных, видео и другого трафика, чувствительного к задержкам. Классы с 4 по 1 предназначены для трафика, менее чувствительного к задержкам, например, данные протокола FTP. Класс 0, присваиваемый по умолчанию, придерживается концепции «лучшее из возможного» (негарантированный класс качества, то есть качество не гарантируется, но поддерживается лучшее из того, что осталось после обслуживания всех остальных классов).

### 5.5.1. Раздел QoS setting

В разделе QoS settings вы можете изменить настройки функции QoS и протокола 802.1p. Описание основных параметров дано в таблице ниже.

Параметр	Описание
QoS setting	Включить ( <b>Enable</b> ) или выключить ( <b>Disable</b> ) функцию QoS. По умолчанию выключена.
802.1p QoS setting	Включить ( <b>Enable</b> ) или выключить ( <b>Disable</b> ) функцию изменения приоритетов. Позволяет переназначать приоритеты по умолчанию.
802.1p mark range	Введите класс или классы приоритетов (например, 2,5-7), которые необходимо переназначить.
Priority	Выберите класс приоритета (от 0 до 7), на который необходимо переназначить.

The screenshot shows the 'QoS setting' configuration page. At the top, there is a navigation bar with links: System status | Port setting | PoE | VLAN | QoS | LACP | Port security | Network management | Network statistics | System management | Exit. The language is set to English. The main content area is titled 'QoS>>QoS setting' and contains the following settings:

- QoS setting:** Radio buttons for 'Enable' (selected) and 'Disable'.
- 802.1p QoS setting:** Radio buttons for 'Enable' (selected) and 'Disable'.
- 802.1p mark range:** An empty text input field.
- Priority:** A dropdown menu showing '0' and an 'OK' button.

Below the settings is a table for mapping 802.1p marks to priorities:

802.1pMark	Priority	802.1pMark	Priority	802.1pMark	Priority	802.1pMark	Priority
0	0	1	1	2	2	3	3
4	4	5	5	6	6	7	7

At the bottom of the table are three buttons: 'Refresh', 'Save', and 'Help'.

Рис. 5.6. Переназначение приоритетов

### Пример

В качестве примера присвоим Классам 6 и 7 низший приоритет.

1. Включите **QoS settings** и **802.1p QoS setting**.
2. Введите в поле **802.1p mark range** значение 6-7.
3. Выберите в выпадающем списке **Priority** значение 0.
4. Нажмите кнопку **Save**, чтобы применить изменения.

**ВНИМАНИЕ:** Коммутатор для работы с приоритетами трафика использует алгоритм WRR (Weighted Round Robin, взвешенный циклический алгоритм), которые организует очереди передачи пакетов. Для каждого потока пакетов формируется своя очередь в контроллере сетевого интерфейса. Алгоритм WRR упрощает совместное использование доступной пропускной способности очередями передачи. Он присваивает очередям определенные веса, и затем это значение используется для выделения каждой очереди части доступной пропускной способности. Благодаря этому алгоритму каждая очередь обслуживается в нужном порядке и передает строго ограниченный объем данных, после чего алгоритм переходит к обслуживанию следующей очереди или к очереди с наивысшим приоритетом. Чем выше значение, тем выше приоритет.

### 5.5.2. Раздел DSCP settings

Здесь вы можете переназначить приоритеты QoS для 6-битного кода DSCP (Differentiated Services Code Point). Описание основных параметров дано в таблице ниже.

Параметр	Описание
<b>DSCP/TOS QoS setting</b>	Включить ( <b>Enable</b> ) или выключить ( <b>Disable</b> ) функцию изменения приоритетов DSCP. Позволяет переназначать приоритеты по умолчанию.
<b>DSCP mark range</b>	Ввод кода (диапазона кодов) DSCP. Значения должны принадлежать 6-битному диапазону 0...63.
<b>DSCP priority</b>	Выберите класс приоритета (от 0 до 7), на который необходимо переназначить.

System status | Port setting | PoE | VLAN | QoS | LACP | Port security | Network management | Network statistics | System management | Exit

QoS>>DSCP/TOS QoS

DSCP/TOS QoS setting:  Enable  Disable

DSCP mark range:

DSCP priority:

DSCPMark	Priority	DSCPMark	Priority	DSCPMark	Priority	DSCPMark	Priority
0	0	1	0	2	0	3	0
4	0	5	0	6	0	7	0
8	1	9	1	10	1	11	1
12	1	13	1	14	1	15	1
16	2	17	2	18	2	19	2
20	2	21	2	22	2	23	2
24	3	25	3	26	3	27	3

Рис. 5.7. Переназначение приоритетов DSCP

### Пример

В качестве примера присвоим кодам DSCP 0...16 высший приоритет.

1. Включите функцию изменения приоритетов DSCP (**DSCP/TOS QoS setting**).
2. В поле **DSCP mark range** введите значение 0-16. Выберите в выпадающем списке **DSCP priority** значение 7.
3. Нажмите кнопку **Set**, чтобы применить изменения или **Save** – чтобы применить и сохранить.

**ВНИМАНИЕ:** При одновременном использовании протокола 802.1p и кодов DSCP, приоритет имеет DSCP.

## 5.6. LACP

### 5.6.1. Раздел TRUNK

Группа TRUNK объединяет несколько физических портов для создания общего высокоскоростного канала передачи данных. Такой подход используется для обеспечения отказоустойчивости и расширения полосы пропускания. Независимо от уровня модели OSI, на котором осуществляется агрегирование каналов, нагрузка может распределяться по всем портам, хотя это не всегда происходит. Большинство методов агрегирования каналов обеспечивает также и отказоустойчивость. Агрегирование каналов осуществляется на уровне IP, когда несколько сетевых интерфейсов получают общий IP-адрес, или на уровне MAC, когда они получают один общий MAC-адрес. Кроме того, у каждого сетевого интерфейса может быть и свой собственный адрес.

**ВНИМАНИЕ:** Настройки всех портов, входящих в состав группы TRUNK, должны полностью совпадать. Это касается таких настроек, как скорость передачи данных, работа в дуплексном режиме и т. п.

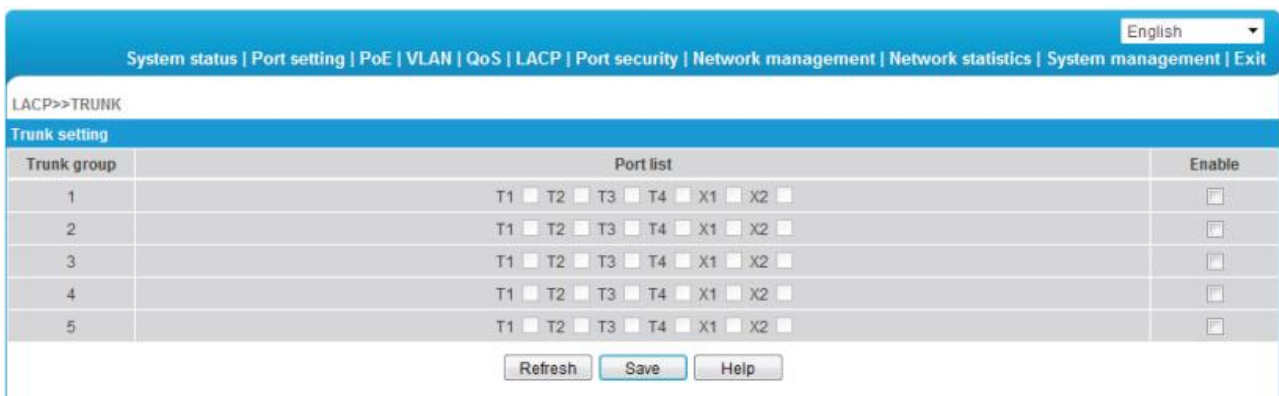
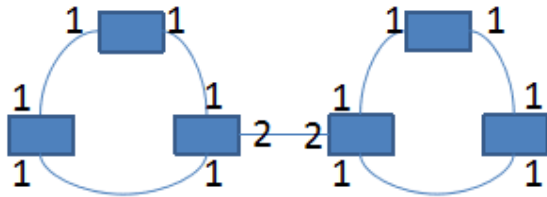
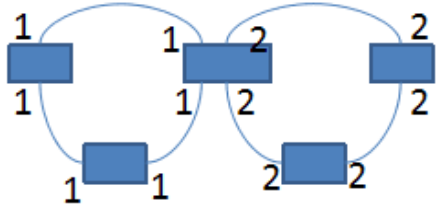


Рис. 5.8. Агрегирование каналов

### 5.6.2. Раздел FastRing

Протокол FastRing разработан с целью предотвращения петель маршрутизации при соединении коммутаторов в кольцевой топологии. Один коммутатор выбирается в качестве главного и блокирует один из своих портов, а со второго порта отправляет по кольцу служебные пакеты. Как только служебные пакеты перестают приходить на заблокированный порт, коммутатор его разблокирует.

Описание основных параметров дано в таблице ниже.

Параметр	Описание
<b>FastRing</b>	Включение ( <b>Enable</b> ) или отключение ( <b>Disable</b> ) протокола FastRing. По умолчанию отключен.
<b>Group</b>	Группа FastRing. Можно сконфигурировать две группы.
<b>ID</b>	Идентификационный номер группы.
<b>Port</b>	Выбор портов, на которых будет включен протокол FastRing.
<b>Double</b>	<p>Режим используется для связи двух колец между соседними коммутаторами. Применяется в том случае, когда нужно, чтобы устройства из двух разных колец могли «видеть» друг друга.</p>  <p style="text-align: right;">Double</p>
<b>Coupling</b>	<p>В данном режиме два кольца, настроенные на коммутаторе, будут изолированы друг от друга.</p>  <p style="text-align: right;">Coupling</p>

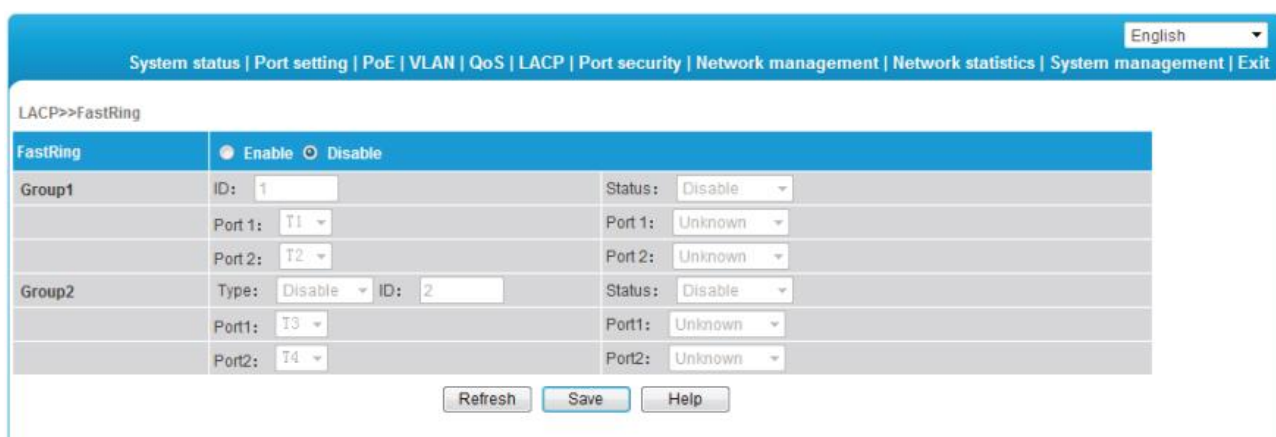


Рис. 5.9. Настройки FastRing

**ВНИМАНИЕ:** Прежде чем приступить к настройке FastRing, убедитесь, что переключатель FastRing на корпусе коммутатора находится в положении по умолчанию, так как в противном случае настройка FastRing невозможна, а кольцо FastRing будет сформировано на оптоволоконных портах uplink.

Настройки всех портов, входящих в состав группы TRUNK, должны полностью совпадать. Это касается таких настроек, как скорость передачи данных, работа в дуплексном режиме и т. п.

### 5.6.3. Раздел RSTP

#### Применение

Протокол STP (Spanning Tree Protocol, протокол разворачивающегося дерева) создавался в соответствии со стандартом IEEE 802.1D. Он разрабатывался для устранения петель маршрутизации. Устройства, поддерживающие этот протокол, обмениваются между собой пакетами для обнаружения петель маршрутизации в сети и блокируют при необходимости некоторые порты. Такой подход в итоге позволяет избавиться инфраструктуру сети от петель маршрутизации. Благодаря этому предотвращается неконтрольное размножение пакетов и их бесконечная циркуляция в петле маршрутизации, которые негативно влияют на производительность коммутатора. В узком значении протокол STP сводится к определению, данному в стандарте IEEE 802.1D. В более широком смысле под ним подразумевают как стандарт IEEE 802.1D, так и разнообразные усовершенствованные и дополненные версии, такие как протокол RSTP (Rapid Spanning Tree Protocol).

#### Базовая концепция

- Корневой мост (Root bridge)

Концепция корневого моста подразумевает, что в структуре сети, которая имеет вид дерева, протокол STP определяет корень, который может быть только один и выбирается при изменении топологии сети, то есть корневым мостом не является фиксированным.

- Стоимость пути (Path cost)

Это значение используется в STP для выбора оптимального порта для передачи данных. После вычисления стоимости пути для каждого из портов коммутатора для передачи пакета выбирается порт с наименьшей стоимостью пути, а избыточные порты блокируются, чтобы не создавать петель маршрутизации.

- Роль порта (для протокола RSTP)

- Корневой порт (**Root Port**) – это порт, который используется для передачи пакетов к корневому мосту. Каждый не корневой мост имеет только один корневой порт, имеющий минимальную стоимость пути.
- Назначенный порт (**Designated Port**) – это не корневой порт, который используется для передачи пакетов в сетевой сегмент.
- Альтернативный порт (**Alternate Port**) – это активный порт, который не является альтернативным путем к корневому коммутатору, отличающимся от основного.
- Запасной порт (**Backup Port**) – это запасной путь в сегмент.

- Состояние порта

- Передача (**Forwarding**): пакеты пересылаются, только корневой или назначенный порт могут иметь такой статус.
  - Обучение (**Learning**): коммутатор создает таблицу MAC-адресов в соответствии с полученными (но не пересланными) пакетами.
  - Отбрасывание (**Discarding**): Отбрасываются все пакеты BPDU, пользовательские пакеты не пересылаются.
- **Назначенные мосты и назначенные порты**

Их описание дано в таблице ниже.

Классификация	Назначенный мост	Назначенный порт
<b>Для оборудования</b>	Мост, который передает пакеты BPDU и к которому напрямую подключены другие мосты.	Порт, используемый назначенным мостом, для передачи пакетов BPDU на данный мост.
<b>Для сети</b>	Мост, назначенный ответственным за передачу пакетов BPDU в сетевой сегмент.	Порт, используемый назначенным мостом, для передачи пакетов BPDU в сетевой сегмент.

## Описание RSTP

RSTP (Rapid Spanning Tree Protocol, быстрый протокол разворачивающегося дерева) представляет собой оптимизированную версию STP. Он назван быстрым потому, что при назначении портов корневыми или назначенными сократилось время перехода в состояние передач и таким образом значительно ускорилось восстановление топологии сети.

**ВНИМАНИЕ:** В протоколе RSTP для обеспечения быстрого переключения на новый корневой порт необходимо, чтобы старый корневой порт прекратил передачу пакетов и исходящий назначенный порт начал передачу пакетов.

В протоколе RSTP для обеспечения быстрого подключения назначенного порта он должен быть либо портом Edge, либо P2P. В первом случае назначенный порт может сразу перейти в состояние передачи. Во втором случае порт обменивается данными и с подключенным к нему устройством и согласовывает переход в состояние передачи пакетов.

В интерфейсе настройки протокола RSTP вы можете видеть служебную информацию протокола и состояние портов (Рис. 5.10).

Описание основных параметров дано в таблице ниже.

Параметр	Описание
<b>Device priority</b>	Приоритет для данного моста. Идентификатор моста (Bridge ID) складывается из приоритета и MAC-адреса моста. Корневым назначается мост с наименьшим идентификатором.
<b>Sending message interval</b>	Интервал между рассылкой пакетов BPDU

<b>Maximum message lifetime</b>	Время жизни пакета BPDU, полученного мостом от другого моста
<b>Changing port status delay</b>	Задержка переключения порта в состояние передачи из состояния прослушивания или обучения
<b>Path expenditure</b>	Стоимость пути для данного порта
<b>Port priority</b>	Приоритет порта. По умолчанию имеет значение 128
<b>Point to point port</b>	Порт P2P используется для соединения мостов между собой. В RSTP для портов P2P предусмотрен специальный алгоритм согласования для быстрого переключения статуса порта.
<b>Edge port</b>	Порт Edge используется для подключения периферийных устройств, таких как компьютеры, IP-видеокамеры. Если порты, к которым подключены такие периферийные устройства, сразу сконфигурировать как Edge, то они сразу перейдут в состояние передачи пакетов, пропустив состояние обучения.
<b>RSTP information</b>	Информация о текущем состоянии протокола RSTP и портов.

System status | Port setting | PoE | VLAN | QoS | LACP | Port security | Network management | Network statistics | System management | Exit

English

LACP->RSTP

RSTP setting  Enable  Disable

Device priority: 32768

Sending message interval: 2 second (1-10)

Maximum message lifetime: 5 second (6-40)

Changing port status delay: 4 second (4-30)

Network bridge information: RSTP

Modify configuration

Path expenditure	Port priority	Point to point port	Edge port
0	128	No	Yes

Port range:

<input type="checkbox"/>	Port	Port mark	Path expenditure	Port priority	Point to point port	Edge port
<input type="checkbox"/>	T1	port1	automatic detection	128	NO	NO
<input type="checkbox"/>	T2	port2	automatic detection	128	NO	NO
<input type="checkbox"/>	T3	port3	automatic detection	128	NO	NO
<input type="checkbox"/>	T4	port4	automatic detection	128	NO	NO
<input type="checkbox"/>	X1	port5	automatic detection	128	NO	NO
<input type="checkbox"/>	X2	port6	automatic detection	128	NO	NO

Рис. 5.10. Настройки RSTP

## Пример

Настройте для коммутаторов А, В, С функцию RSTP, чтобы избежать возникновения сетевого шторма.

1. Включите для коммутаторов А, В, С функцию RSTP.

2. В поле диапазона портов (**Port range**) введите порты T1...X2 или отметьте их напрямую в списке портов. Введите нужные значения (**Bridge Priority, Hello timer, Maximum Age, Forward Delay**) или оставьте их по умолчанию.
3. Значение стоимости пути (**Path Expenditure**) выставьте равным 0 (автоматически).
4. Приоритет порта (**Port Priority**) должен быть равным 128 (по умолчанию).
5. В поле **P2P Port** выберите **Yes**.
6. В поле **Edge Port** выберите **No**.
7. Нажмите кнопку **Save**, чтобы сохранить изменения.

**ВНИМАНИЕ:** После настройки протокола RSTP, нажмите кнопку **RSTP Information**, чтобы проверить информацию о портах и корневом мосте. Время обновления информации составляет примерно 30 с.

## 5.7. Меню Port Security

### 5.7.1. Раздел Static address lock

Функция связывания порта с MAC-адресом предназначена для обеспечения дополнительной безопасности и гарантирует, что к выбранному порту могут подключиться только устройства с указанными MAC-адресами.

Описание основных параметров дано в таблице ниже.

Параметр	Описание
<b>MAC Address</b>	MAC-адрес сетевого устройства, которое привязывается к порту. Привязка работает до тех пор, пока MAC-адрес не будет удален и не истечет время обновления.
<b>VLAN ID</b>	Соответствующий порту номер VLAN ID
<b>Port</b>	Порт, с которым осуществляется связывание указанного выше MAC-адреса.

Рис. 5.11. Связывание порта с MAC-адресом

**ВНИМАНИЕ:** Данная функция относится к набору инструментов безопасности!

- Не используйте в качестве MAC-адреса широковещательный адрес.
- Не используйте в качестве MAC-адреса зарезервированные адреса, такие как локальные MAC-адреса.



- Для портов, которые добавлены в группу TRUNK, не допускается использование функции связывания порта с MAC-адресом.

### 5.7.2. Раздел 802.1X certification

Стандарт IEEE 802.1X определяет протокол контроля доступа и аутентификации, который ограничивает права неавторизованных устройств, подключенных к коммутатору. Сервер аутентификации проверяет каждое устройство перед тем, как оно сможет воспользоваться сервисами, которые предоставляет ему коммутатор. Пока устройство, подключенное к данному порту, не было аутентифицировано, он остается в неавторизованном состоянии и коммутатор пропускает через него только пакеты IEEE 802.1X.

В стандарте IEEE 802.1X определено три основных элемента:

- запрашивающее устройство (**Supplicant**) – устройство, запрашивающее аутентификацию;
- сервер аутентификации (**Authentication server**) – обычно RADIUS-сервер, который производит фактическую аутентификацию;
- аутентификатор (**Authenticator**) – сетевое устройство, находящееся между запрашивающим устройством и сервером аутентификации и предоставляющее доступ в сеть, обычно коммутатор или точка доступа.

The screenshot displays the configuration page for IEEE 802.1X certification. It includes a navigation bar at the top with options like 'System status', 'Port setting', and 'Exit'. The main content is divided into 'Global setting' and 'Port setting' sections.

**Global setting:**

- Enable/Disable:  Enable,  Disable
- Timing update certification: 3600 Second [60 - 40,000,000]
- Radius server:  Local,  Remote
- Radius server setting: IP address [ ], Share secret key [ ]
- Server port setting: Billing server port [ ] [0 - 65535], Certification server port [ ] [0 - 65535]

**Port setting:**

Port range	Control mode		Port control method		Maximum user quantity
	Control mode	Port control method	Control mode	Control method	Maximum user quantity
[ ] [ ]	Authorized-force	MAC Based	Authorized-force	MAC Based	[ ]

**Table of Port Settings:**

Port	Port mark	Setting status		
		Control mode	Control method	Maximum user quantity
1	port1	Authorized-force	MAC Based	4096
2	aaaaaaport2	Authorized-force	MAC Based	4096
3	port3	Authorized-force	MAC Based	4096
4	port4ssss	Authorized-force	MAC Based	4096
5	port5	Authorized-force	MAC Based	4096
6	SSSSSSport6	Authorized-force	MAC Based	4096
7	port7	Authorized-force	MAC Based	4096

Рис. 5.12. Аутентификация IEEE 802.1X

Описание основных параметров дано в таблице ниже.

Параметр	Описание
<b>Global setting</b>	Включение ( <b>Enable</b> ) или отключение ( <b>Disable</b> ) протокола 802.1X. По умолчанию отключен.
<b>Timing update certification</b>	Таймер повторного запроса аутентификации. Используется для повышения уровня безопасности.

<b>Radius Server</b>	Можно использовать встроенный ( <b>Local</b> ) или внешний ( <b>Remote</b> ) RADIUS-сервер. При использовании встроенного сервера аутентификацию будут проходить только те запрашивающие устройства, которые смогут предоставить комбинацию имени пользователя и пароля, занесенные в базу данных встроенного RADIUS-сервера. При использовании внешнего сервера необходимо указать его IP-адрес и номера портов.
<b>Radius server setting / IP address</b>	IP-адрес внешнего RADIUS-сервера.
<b>Radius server setting / Shared secret key</b>	Пароль внешнего RADIUS-сервера.
<b>Server port setting / Billing server port</b>	Порт биллинга (учета) внешнего RADIUS-сервера. По умолчанию порт 1813.
<b>Server port setting / Certification server port</b>	Порт внешнего RADIUS-сервера. По умолчанию порт 1812.
<b>Port setting / Control mode</b>	Выбор режима контроля портов.
<b>Port setting / Port control method</b>	В данной версии поддерживается только один режим контроля портов – по MAC-адресу ( <b>MAC Based</b> ).
<b>Port setting / Maximum user quantity</b>	Максимальное количество пользователей (в диапазоне 1...4096).

### Пример

Для портов T1-T4 установим автоматический режим контроля портов и максимальное количество пользователей равным 8.

1. Включите протокол RADIUS (кнопка **Enable**).
2. В диапазоне портов (**Port range**) введите T1-T4.
3. Выберите автоматический режим контроля портов (**Auto** в поле **Port Control method**).
4. Установите максимальное количество пользователей (**Maximum user quantity**) равным 8.
5. Нажмите кнопку **Save**, чтобы сохранить изменения.

### ВНИМАНИЕ:

- Между запрашивающим устройством и аутентификатором поддерживается только протокол MD5. Другие типы хэширования не поддерживаются.
- Неправильная настройка сервера учета приведет к тому, что запрашивающее устройство не сможет пройти аутентификацию.
- Для всех устройств, подключаемых к коммутатору, должны быть настроены учетные записи на RADIUS сервере или локальные учетные записи, иначе они не смогут получить доступ к коммутатору.

## 5.8. Меню Network management

### 5.8.1. Раздел SNMP setting

Протокол SNMP используется для отслеживания состояния сетевых устройств и управления ими. С его помощью администраторы сети могут оперативно получать информацию о любом устройстве в сети и быстро находить в ней сбои, а также планировать развитие сети и получать отчеты.

В SNMP определены три основных элемента:

- управляемое устройство (**Managed device**) – сетевое устройство, поддерживающее протокол управления SNMP;
- агент (**Agent**) – программное обеспечение, выполняющееся на управляемом устройстве;
- Система сетевого управления (**Network Management System, NMS**) — программное обеспечение, взаимодействующее с сетевыми устройствами для поддержки комплексной структуры данных, отражающей состояние сети.

В разделе **SNMP settings** вы можете включить или отключить протокол SNMP и настроить его.

Описание основных параметров дано в таблице ниже.

Параметр	Описание
<b>SNMP setting</b>	Включение ( <b>Enable</b> ) или отключение ( <b>Disable</b> ) протокола SNMP. По умолчанию отключен.
<b>SNMP gateway</b>	IP-адрес станции сетевого управления, куда будут отправляться пакеты SNMP.
<b>SNMP version</b>	Версия протокола SNMP, поддерживаются версии v1, v2, v3.
<b>Read-only community name</b>	Имя SNMP-сообщества с правами только на чтение (операции типа GET). По умолчанию <b>public</b> .
<b>Read-write community name</b>	Имя SNMP-сообщества с правами на чтение и запись (операции типа GET и SET). По умолчанию <b>private</b> .
<b>User name</b>	Имя пользователя учетной записи, которое используется для аутентификации.
<b>Identity authentication</b>	Алгоритм расчета хеш-функции.
<b>Encryption protocol</b>	Протокол шифрования.
<b>Read-write method</b>	Права доступа для учетной записи: только чтение ( <b>Read only</b> ) – пользователю доступен только мониторинг, чтение и запись ( <b>Read-write</b> ) пользователю доступны мониторинг и управление.
<b>Verify password</b>	Пароль пользователя.
<b>Encrypted password</b>	Ключ шифрования.

**ВНИМАНИЕ:**

Имя SNMP-сообщества используется для определения типа отношений между агентом и системой сетевого управления. Если имя SNMP-сообщества не опознается устройством, то пакеты будут отбрасываться. Вы можете использовать стандартное имя SNMP-сообщества (**public** или **private**) или задать свое собственное.

Рис. 5.13. Настройки SNMP

**5.8.2. Раздел Email alarm**

Коммутатор ведет журнал событий и может быть сконфигурирован для отправки сообщений по электронной почте определенным пользователем получателям. Кроме того, он периодически отправляет и весь журнал событий.

Описание основных параметров дано в таблице ниже.

Параметр	Описание
<b>Email alarm</b>	Включение ( <b>Enable</b> ) или отключение ( <b>Disable</b> ) функции отправки сообщений электронной почты. По умолчанию отключена.
<b>Mail server</b>	IP-адрес почтового сервера, который осуществляет отправку сообщений по протоколу SMTP.
<b>Mail accountant</b>	Имя пользователя для подключения к почтовому серверу.
<b>Mail password</b>	Пароль пользователя для подключения к почтовому серверу.
<b>Receiver address</b>	Адрес получателя сообщений.
<b>Mail reply address</b>	Адрес, на который должны приходить ответы.
<b>Mail interval</b>	Интервал отправки сообщений на почтовый сервер.

Рис. 5.14. Отправка записей журнала по электронной почте

## Пример

Настроим отправку сообщений с почтового адреса [1234@mail.ru](mailto:1234@mail.ru) на адрес [5678@mail.ru](mailto:5678@mail.ru).

1. Включите функцию отправки сообщений (кнопка **Enable** в поле **Email alarm**).
2. Введите smtp.mail.ru в поле **Mail server**.
3. Введите почтовый адрес [1234@mail.ru](mailto:1234@mail.ru) в поле **Mail accountant**
4. Введите пароль в поле **Mail password**
5. Введите почтовый адрес получателя [5678@mail.ru](mailto:5678@mail.ru) в поле **Receiver address**.
6. Введите ответный адрес, если требуется в поле **Mail reply address**.
7. Установите интервал отправки сообщений 12 часов (**12 hours**) в поле **Mail interval**.
8. Нажмите кнопку **Save**, чтобы сохранить изменения.

**ВНИМАНИЕ:** Некоторые почтовые сервера требуют, чтобы ответный адрес совпадал с адресом отправителя.

### 5.8.3. Раздел Port mirror

Функция зеркалирования портов дублирует поток данных на заданный порт. Она используется для анализа и мониторинга данных. Коммутатор поддерживает множественное зеркалирование, то есть дублирование потока данных с нескольких портов на один порт. Кроме того, пользователь может выбрать направление трафика для мониторинга.

Описание основных параметров дано в таблице ниже.

Параметр	Описание
<b>Port mirror</b>	Включение ( <b>Enable</b> ) или отключение ( <b>Disable</b> ) функции зеркалирования портов. По умолчанию отключена.
<b>Monitor port</b>	Порт мониторинга, с которого дублируются пакеты.
<b>Mirror port</b>	Порт зеркалирования, на который дублируются пакеты с портов мониторинга.
<b>Data collection</b>	Выбор направления трафика: в обоих направлениях ( <b>All date</b> ), входящий трафик ( <b>Input data</b> ), исходящий трафик ( <b>Output data</b> ).

System status | Port setting | PoE | VLAN | QoS | LACP | Port security | Network management | Network statistics | System management | Exit

English

Network management>>Port mirror

Port mirror  Enable  Disable

Monitor port

Mirror port

Data collection  All data  Input data  Output data

No.	Monitor port	Mirror port	Data collection
1			Input data
2			Output data

Рис. 5.15. Зеркалирование портов

## Пример

В качестве примера выполним зеркалирование входящего трафика с порта T3 на порт T2.

1. Включите функцию зеркалирования (кнопка **Enable** в поле **Port mirror**).
2. Укажите порт T3 в качестве порта мониторинга (**Monitor port**).
3. Укажите порт T2 в качестве порта зеркалирования (**Mirror port**).
4. Укажите в качестве направления мониторинга только входящие пакеты (**Input data**).
5. Нажмите кнопку **Save**, чтобы сохранить изменения.

### ВНИМАНИЕ:

- Эта функция используется только для тестирования и выявления сбоев. При обычной эксплуатации она должна быть отключена, чтобы не создавать дополнительной нагрузки на процессор коммутатора.
- Функция зеркалирования обрабатывает пакеты только с корректной контрольной суммой и не умеет обрабатывать пакеты с ошибками.
- Для того чтобы сменить порт зеркалирования или порт мониторинга, введите нужные значения в соответствующие поля и нажмите кнопку **Edit**.

### 5.8.4. Раздел IGMP Snooping

Функция отслеживания трафика IGMP оптимизирует обмен пакетами многоадресного трафика. Коммутаторы анализируют трафик IGMP и, вместо того чтобы ретранслировать его на все порты широковещательного домена (или VLAN), отправляет его только на те порты, к которым подключены устройства, явно затребовавшие этот трафик. Это позволяет коммутаторам исключать такой трафик из потоков, направляемых через порты, к которым не подключены его потребители, тем самым существенно снижая нагрузку на сеть.

Описание основных параметров дано в таблице ниже.

Параметр	Описание
<b>IGMP snooping function</b>	Включение ( <b>Enable</b> ) или отключение ( <b>Disable</b> ) функции отслеживания трафика IGMP. По умолчанию отключена.
<b>IGMP inquiry</b>	Включение ( <b>Enable</b> ) или отключение ( <b>Disable</b> ) функции опроса членов многоадресной группы. По умолчанию отключена.
<b>IGMP inquiry interval</b>	Интервал опроса членов многоадресной группы.
<b>Group members life time</b>	Максимальная длительность сохранения устройства в многоадресной группе с того момента, как оно перестало отвечать.
<b>Static multicast MAC address</b>	Статический MAC-адрес для многоадресной трансляции.
<b>VLAN ID</b>	VLAN ID для многоадресной трансляции.
<b>Port range</b>	Порты, которые участвуют в многоадресной трансляции.

Рис. 5.16. Отслеживание трафика IGMP

## 5.9. Меню Network Statistics

### 5.9.1. Раздел Packet statistics

В этом разделе можно посмотреть информацию по полученным (**Received frame**) и отправленным пакетам (**Sent frame**) для каждого порта. Обновление информации осуществляется кнопкой **Refresh**, сброс статистики – кнопкой **Reset**.

Описание основных параметров дано в таблице ниже.

Параметр	Описание
<b>Singlecast package</b>	Количество одноадресных пакетов.
<b>Multicast package</b>	Количество многоадресных пакетов.
<b>Broadcast package</b>	Количество широковещательных пакетов.
<b>Error package</b>	Количество пакетов с ошибками.

System status   Port setting   PoE   VLAN   QoS   LACP   Port security   Network management   Network statistics   System management   Exit								
Network statistics>>Flow statistics								
Port	Sent frame				Received frame			
	Singlecast package	Multicast package	Broadcast package	Error package	Singlecast package	Multicast package	Broadcast package	Error package
1	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0

Рис. 5.17. Статистика трафика

### 5.9.2. Раздел MAC Address

MAC-адрес (Media Access Control) – аппаратный идентификатор устройства в сети Ethernet. Коммутаторы пересылают пакеты, используя MAC-адреса, которые помещаются в их заголовках. MAC-адреса уникальны, что гарантирует правильность пересылки нужному адресату. Каждый коммутатор ведет таблицу MAC-адресов, в которой они сопоставлены с его портами. Когда коммутатор получает пакет, он может либо отбросить его, либо переслать его на нужный порт в соответствии с таблицей MAC-адресов. MAC-адреса в таблице разделяются на динамические (автоматически привязанные коммутатором к определенному порту) и статические (вручную привязанные коммутатором к определенному порту через команду).

Описание основных параметров дано в таблице ниже.

Параметр	Описание
<b>Inquiry by physical port</b>	Фильтр информации о MAC-адресах по порту.
<b>Inquiry by MAC address type</b>	Фильтр информации о MAC-адресах по типу MAC-адреса: <ul style="list-style-type: none"> <li>• все типы (<b>All type</b>),</li> <li>• динамические (<b>Dynamic MAC address</b>),</li> <li>• статические (<b>Static MAC address</b>).</li> </ul>



No.	Source address	VLAN ID	Type	Port	Process mode
1	20:4E:7F:89:DB:97	1	Dynamic	28	forward
2	00:24:8C:95:AD:4C	1	Dynamic	28	forward
3	50:E5:49:AF:46:97	1	Dynamic	28	forward
4	54:04:A6:D5:BB:6F	1	Dynamic	28	forward
5	14:DA:E9:93:02:64	1	Dynamic	28	forward
6	00:0C:29:29:D2:60	1	Dynamic	28	forward
7	00:1F:29:9A:88:E6	1	Dynamic	28	forward

Рис. 5.18. Таблица MAC-адресов

## 5.10. Меню System Management

### 5.10.1. Раздел IP address

Здесь вы можете ввести IP-адрес коммутатора и сконфигурировать прочие настройки протокола IP для коммутатора.

Описание основных параметров дано в таблице ниже.

Параметр	Описание
<b>Access</b>	Выберите тип IP-адреса: статический ( <b>Static IP</b> , настройки протокола IP задаются вручную), или динамический ( <b>Dynamic IP</b> , настройки протокола IP получаются автоматически от DHCP-сервера).
<b>IP address</b>	IP-адрес.
<b>Subnet mask</b>	Маска подсети.
<b>Default gateway</b>	Шлюз по умолчанию.
<b>DNS address</b>	IP-адрес DNS-сервера.

Access	Static IP	Dynamic IP
IP address	192.168.1.184	
Subnet mask	255.255.255.0	
Default gateway	192.168.1.1	
DNS address	202.96.134.133	

Рис. 5.19. Настройки протокола IP

### 5.10.2. Раздел User management

В этом разделе вы можете сконфигурировать права пользователей.

Рис. 5.20. Конфигурирование прав пользователей

Описание основных параметров дано в таблице ниже.

Параметр	Описание
<b>User index</b>	Номер-идентификатор пользователя. Предусмотрено три номера ( <b>1, 2, 3</b> ), которые вы можете выбрать в выпадающем меню. Номер 1 зарезервирован за администратором номер 2 или 3 могут быть как администратором, так и простым пользователем.
<b>Visit level</b>	Уровень <b>Administrator</b> имеет доступ ко всем настройкам и может их изменять. Уровень <b>Customer</b> имеет ограниченный доступ к настройкам.
<b>User name</b>	Имя пользователя.
<b>Input password</b>	Пароль.
<b>Confirm password</b>	Подтверждение пароля.

**ВНИМАНИЕ:** Пользователь с уровнем пользователя, в отличие от администратора, не имеет доступа к настройкам аутентификации, учетных записей пользователей, SNMP, сохранения или восстановления конфигурации и сброса к заводским настройкам.

**ВНИМАНИЕ:**

- Если вы забыли имя пользователя или пароль, то для их восстановления нужно обратиться к администратору сети.
- При совпадении имен действительным будет считаться комбинация имени и пароля имеющая меньший идентификатор.
- Поддерживается до трех пользователей, при этом первого пользователя с правами администратора удалить невозможно.

### 5.10.3. Раздел Log information

В этом разделе вы можете просмотреть системный журнал. В нем фиксируются ошибки, уведомления и прочие события, которые помогают отслеживать работу коммутатора. Также можно включить отправку записей журнала на удаленный сервер (**Remote log server**), загрузить журнал с коммутатора на компьютер (**Download**) или удалить журнал. В системном журнале регистрируются следующие события:

- перезапуск коммутатора,
- включение/выключение порта,

- статус питания PoE,
- информация об аутентификации пользователей,
- информация о сетевом шторме,
- системные действия и операции,
- информация о синхронизации с NTP-сервером,
- прочая системная информация.

Описание основных параметров дано в таблице ниже.

Параметр	Описание
<b>Remote log server</b>	Включение ( <b>Enable</b> ) или отключение ( <b>Disable</b> ) функции отправки записей журнала на удаленный сервер. По умолчанию отключена.
<b>Log Server Address</b>	IP-адрес удаленного сервера, на который будут отсылаться записи системного журнала.
<b>Record lowest grade</b>	Записи в системном журнале имеют восемь уровней. Здесь выбирается нижний уровень, ниже которого записи не будут отсылаться на удаленный сервер.
<b>Information processing</b>	Загрузка системного журнала с коммутатора на компьютер в формате syslog.cfg (кнопка <b>Download</b> ). Удаление записей из системного журнала (кнопка <b>Delete</b> ).

System management >> Log information

Remote log server  Enable  Disable

Log server address  Record lowest grade

Information processing

No.	Type	Time	Event
1	LINK	2014-11-06 13:21:30	Port G0/28 Link Up!
2	CONFIG	2014-11-07 16:30:45	User login successful - IP:217.23.89.110 Name:admin
3	CONFIG	2014-11-07 16:28:25	System time is changed as Local - IP:217.23.89.110 Name:admin
4	CONFIG	2014-11-10 11:24:20	User login successful - IP:192.168.1.16 Name:admin
5	CONFIG	2014-11-11 10:12:46	User login successful - IP:192.168.1.16 Name:admin
6	CONFIG	2014-11-11 10:37:51	User login successful - IP:192.168.1.16 Name:admin
7	CONFIG	2014-11-11 16:38:06	User login successful - IP:192.168.1.16 Name:admin
8	CONFIG	2014-11-19 09:30:46	User login successful - IP:192.168.1.16 Name:admin
9	CONFIG	2014-11-19 09:47:51	User login successful - IP:192.168.1.16 Name:admin

Previous Current page / Total pages 1/1 Next

Refresh Save Help

Рис. 5.21. Системный журнал

#### 5.10.4. Раздел File management

В данном разделе вы можете сохранить или восстановить настройки коммутатора, выполнить обновление прошивки и сброс на заводские настройки.

Описание основных параметров дано в таблице ниже.

Параметр	Описание
<b>Configuration backup</b>	Сохранение настроек в конфигурационном файле на компьютер в формате *.cfg.
<b>Configuration recover</b>	Восстановление настроек из конфигурационного файла.
<b>Select update file</b>	Обновление прошивки коммутатора.
<b>Restore factory defaults</b>	Сброс на заводские настройки.
<b>System reboot</b>	Перезагрузка коммутатора.

**ВНИМАНИЕ:**

- При обновлении прошивки не выключайте питание коммутатора! Настоятельно рекомендуется подключать коммутатор к источнику бесперебойного питания при обновлении прошивки.
- При перезагрузке не забывайте сохранять изменения в настройках коммутатора, иначе они будут потеряны.

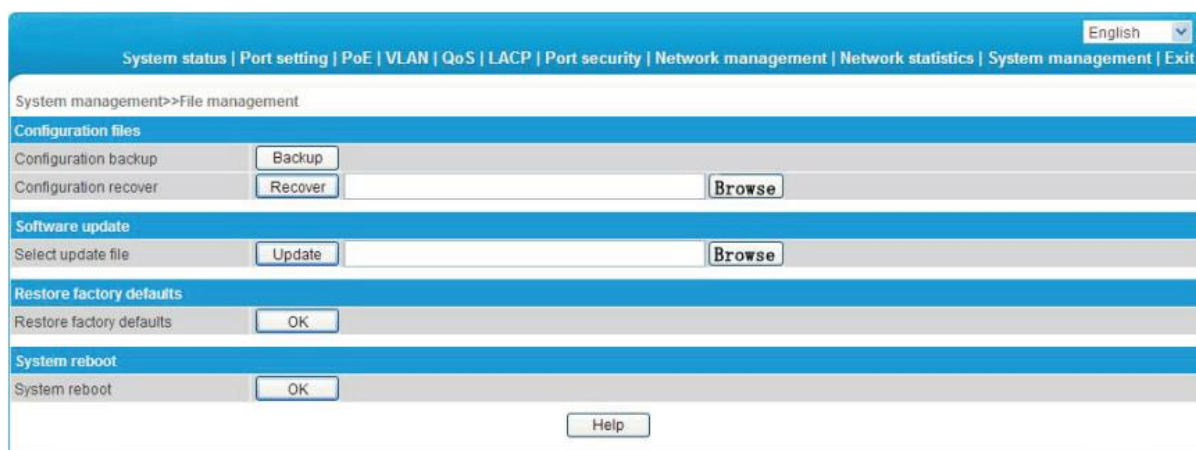


Рис. 5.22. Работа с конфигурационными файлами: обновление прошивки и сброс на заводские настройки

**5.10.5. Раздел Alarm management**

Данный раздел используется для конфигурирования тревожного выхода.

Описание основных параметров дано в таблице ниже.

Параметр	Описание
<b>Alarm</b>	Включение ( <b>Enable</b> ) или отключение ( <b>Disable</b> ) управления тревожным выходом. По умолчанию отключено.
<b>Alarm type</b>	Конфигурировании нормального состояния тревожного выхода. Он может быть нормально открытым ( <b>Normal Open</b> ) или нормально замкнутым ( <b>Normal Close</b> ).
<b>Power Supply</b>	Переключение тревожного выхода при пропадании напряжения на любом входе питания.
<b>Port Network</b>	Переключение тревожного выхода при включении или выключении выбранного порта или любого порта.
<b>Port PoE</b>	Переключение тревожного выхода при пропадании питания PoE на выбранном или любом порту.

English ▾

System status | Port setting | PoE | VLAN | QoS | LACP | Port security | Network management | Network statistics | System management | Exit

System management>>Alarm management

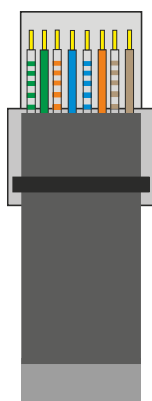
Alarm		<input type="radio"/> Enable <input checked="" type="radio"/> Disable
1.Alarm Type		<input checked="" type="radio"/> Normal Open <input type="radio"/> Normal Close
<input checked="" type="checkbox"/> 2.Power Supply	Triggering Condition: Either power supply is powered down	
<input checked="" type="checkbox"/> 3.Port Network	Triggering Condition: Network of ports get from ON to OFF	All <input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> 4.Port PoE	Triggering Condition: PoE power supply of ports get from ON to OFF	All <input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/>

Рис. 5.23. Конфигурирование тревожного выхода

## 6. Обжим кабеля витой пары

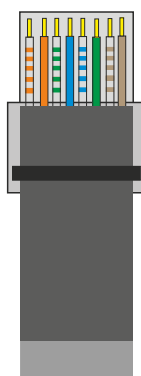
Для обжима кабеля витой пары вам потребуется следующее оборудование: обжимные клещи, тестер локальной сети. Порядок разводки проводов кабеля витой пары должны соответствовать стандарту EIA/TIA 568A или EIA/TIA 568B.

1. Удалите защитную изоляцию на 2 см от конца кабеля витой пары и выведите 4 пары проводов.
2. Разделите 4 пары проводов кабеля и выпрямите их.
3. Выведите 8 проводов кабеля в соответствии со стандартом EIA/TIA 568A или EIA/TIA 568B.
4. Обрежьте выведенные 8 проводов кабеля, чтобы их длина составила 1.5 см.
5. Вставьте 8 проводов в вилку RJ-45, чтобы каждый из них касался соответствующего контакта в вилке.
6. Используйте обжимные клещи, чтобы обжать вилку RJ-45.
7. Повторите предыдущие шаги, чтобы обжать кабель с другого конца.
8. Используйте тестер локальной сети для проверки работоспособности кабеля.



Контакт	Цвет
1	бело-зеленый
2	зеленый
3	бело-оранжевый
4	синий
5	бело-синий
6	оранжевый
7	бело-коричневый
8	коричневый

Рис. 6.1. Разводка проводов по стандарту EIA/TIA 568A



Контакт	Цвет
1	бело-оранжевый
2	оранжевый
3	бело-зеленый
4	синий
5	бело-синий
6	зеленый
7	бело-коричневый
8	коричневый

Рис. 6.2. Разводка проводов по стандарту EIA/TIA 568B

**ВНИМАНИЕ:** Если один конец кабеля обжат согласно стандарту EIA/TIA568A, то и другой конец кабеля должен быть обжат согласно стандарту EIA/TIA568A. Если один конец кабеля обжат согласно стандарту EIA/TIA568B, то и другой конец кабеля должен быть обжат согласно стандарту EIA/TIA568B.

## 7. Устранение неисправностей

В случае неисправности оборудования выполните следующие действия.

- Убедитесь, что оборудование установлено в соответствии с данной инструкцией.
- Проверьте кабели сети Ethernet. Они должны соответствовать стандарту EIA/TIA 568A или EIA/TIA 568B.
- Каждый порт с поддержкой питания PoE имеет максимальную мощность 30 Вт. Не подключайте к этим портам оборудование, которое требует большей мощности.
- Замените оборудование аналогичным коммутатором Ethernet с поддержкой PoE, чтобы удостовериться, что оборудование вышло из строя.
- Свяжитесь с продавцом, если не удалось устранить неисправность.

## 8. Гарантия и ограничения

На сетевое оборудование LTV распространяется гарантия 2 года с момента приобретения. Ознакомиться с условиями гарантийного обслуживания вы можете на веб-сайте <http://www.ltv-cctv.ru>.



## 9. Спецификация

Модель		LTV NSG-7204P-01
Сеть	Порты	4x RJ45 (10/100/1000 Мбит/с) 2x SFP uplink (1000 Мбит/с)
	Максимальная дальность передачи	100 м (все порты кроме SFP)
	Внутренняя пропускная способность	24 Гбит/с
	Скорость передачи пакетов	8900000 пакетов/с
	Размер буфера пакетов	4 Мбит
	Размер таблицы MAC-адресов	8192
	Стандарты	IEEE 802.3, 802.3u, 802.3ab, 802.3z, 802.3x, 802.1Q, 802.1p, 802.3ad, 802.1D, 802.1X
	Протоколы	VLAN, QoS, DSCP, FastRing, RSTP, RADIUS, SNMP (v1, v2, v3), IGMP, Telnet Веб-интерфейс: UDP, TCP, IP, HTTP
PoE	Порты	4x (802.3af, 802.3at)
	Общая мощность	150 Вт
	Максимальная мощность на порт	60 Вт (порт 1), 30 Вт (порты 2-4)
Защита	Импульсные скачки напряжения	Уровень 4 (IEC61000-4-4)
	Электростатические разряды	Уровень 4, 8 кВ / 10 кВ (IEC61000-4-2)
	Радиочастотное электромагнитное поле	Уровень 4 (IEC61000-4-3)
	Кондуктивные помехи	Уровень 3 (IEC61000-4-6)
	Грозозащита	Уровень 4 (IEC61000-4-5)
Физические параметры	Питание	48-57 В (DC), ≤20 Вт (блок питания в комплекте)
	Исполнение	Промышленное
	Рабочая температура	-40°C...+75°C
	Размеры	159x110x46.5мм
	Вес	1.5 кг

## О бренде LTV

Торговая марка LTV принадлежит торговому дому ЛУИС+ и известна на российском рынке с 2004 года. Линейка оборудования LTV - это полнофункциональный набор устройств, оптимальных по соотношению «цена/качество», ассортимент которых постоянно пополняется, следуя новым тенденциям на рынке CCTV и создавая их. Марка LTV представлена во всех основных подгруппах оборудования для создания систем видеонаблюдения любой сложности: видеокамеры, сменные объективы, видеорегистраторы, мониторы, сетевое оборудование, кожухи и аксессуары.

Предлагаем посетить профильный сайт, посвященный оборудованию торговой марки LTV <http://www.ltv-cctv.ru>. Здесь вы можете найти полезную техническую информацию, скачать инструкции, а также получить последнюю версию каталога оборудования. Если у вас возникнут технические вопросы, наши специалисты всегда будут рады помочь вам.

Спасибо за то, что приобрели оборудование LTV!

