

MOXA EtherDevice Switch

Руководство пользователя управляемых коммутаторов

Девятое издание, сентябрь 2015

MOXA Networking Co., Ltd.

Тел.: +886-2-2910-1230

Факс: +886-2-2910-1231

www.moxa.com

Официальный дистрибьютор в России

ООО «Ниеншанц-Автоматика»

www.nnz-ipc.ru www.moxa.ru

sales@moxa.ru

support@moxa.ru



© 2015 Moxa Inc. All rights reserved.

Руководство пользователя управляемых коммутаторов MOXA

Программные продукты, описанные в данном руководстве, поставляются по лицензионному соглашению и могут использоваться только в соответствии с условиями этого соглашения.

Авторские права

Авторское право © 2006 г. MOXA Networking Co., Ltd.

Все права защищены.

Воспроизведение в любой форме без разрешения запрещено.

Торговые марки

MOXA - зарегистрированная торговая марка MOXA Group.

Все другие торговые или зарегистрированные марки, упомянутые в настоящем руководстве, принадлежат соответствующим производителям.

Дополнение

Компания MOXA оставляет за собой право вносить изменения и дополнения в данное руководство без предварительного уведомления потребителя.

Не предоставляя гарантий, данное руководство не ограничивает потребителя в решении специфических задач. MOXA оставляет за собой право в любое время изменять и/или модифицировать продукцию и/или программное обеспечение, описанные в данном руководстве. Информация в данном руководстве является точной и надежной. Тем не менее, MOXA не несет ответственности за использование информации, содержащейся в настоящем руководстве, а также за любые нарушения прав третьих лиц, возникших в результате использования данной информации.

Настоящее Руководство может содержать типографские ошибки.

Информация, содержащаяся в настоящем руководстве, периодически корректируется; все изменения могут быть включены в новые издания настоящего руководства.

Оглавление

1. Введение.....	6
2. Начало работы с коммутатором.....	7
<i>Настройка с помощью последовательной консоли (115200, None, 8, 1, VT100)</i>	8
<i>Настройка через Telnet-консоль</i>	10
<i>Настройка через web-обозреватель</i>	12
<i>Отключение доступа через Telnet и web-обозреватель</i>	13
3. Основные функции.....	14
<i>Базовые настройки</i>	15
<i>System Identification (Идентификация системы)</i>	15
<i>Password (Пароль)</i>	17
<i>Accessible IP List (Разрешенные IP-адреса)</i>	17
<i>Port Settings (Настройки портов)</i>	18
<i>Network Parameters (Параметры сети)</i>	20
<i>GARP Timer Parameters (Параметры таймера GARP)</i>	23
<i>System Time Settings (Настройки системного времени)</i>	24
<i>IEEE 1588 PTP</i>	26
<i>Turbo Ring DIP Switch (DIP-переключатель Turbo Ring)</i>	31
<i>System File Update (Обновление системных настроек)</i>	32
<i>Restart (Перезагрузка)</i>	35
<i>Reset to Factory Default (Сброс к заводским настройкам)</i>	35
<i>Loop Protection (Защита от образования петель)</i>	35
<i>Использование функции Port Trunking</i>	36
<i>Концепция Port Trunking</i>	36
<i>Port Trunking Settings (Настройка функции Port Trunking)</i>	37
<i>Настройка протокола SNMP</i>	38
<i>SNMP Read/Write Settings (Настройки Чтения/Записи SNMP)</i>	40
<i>Trap Settings (Настройка SNMP Trap)</i>	41
<i>Private MIB information (Информация о частной MIB)</i>	43
<i>Использование технологии питания PoE (только для моделей с PoE)</i>	43
<i>Тип 1</i>	43
<i>Тип 2</i>	47
<i>Назначение приоритета трафика</i>	58
<i>Концепция приоритезации трафика</i>	58
<i>Настройка приоритезации трафика</i>	61

Использование виртуальных сетей Virtual LAN	66
Виртуальные сети VLAN	66
Примеры приложений, использующих VLAN	69
Настройка виртуальной сети VLAN	70
QinQ Setting (Настройка функции QinQ)	72
VLAN Table (Таблица VLAN)	73
Фильтрация многоадресного трафика	74
Концепция фильтрации многоадресного трафика	74
Настройка IGMP Snooping	77
Current Active IGMP Streams (Активные потоки IGMP)	80
Static Multicast MAC Addresses (Статические многоадресные MAC-адреса)	81
Настройка протокола GMRP	82
Таблица GMRP	83
Multicast Filtering Behavior (Алгоритм фильтрации многоадресных рассылок)	83
Контроль пропускной способности по портам	84
Настройка управления пропускной способностью	84
Безопасность	88
User Login Authentication – User Login Settings (Вход в систему с помощью имени пользователя – Настройка входа в систему)	88
User Login Authentication – Auth Server Setting (Вход в систему с помощью имени пользователя – Настройка сервера аутентификации)	89
Сертификат проверки подлинности сервера	89
Управление доступом к порту	90
Static Port Lock (Статическая блокировка порта)	90
Стандарт IEEE 802.1X	90
Configuring Static Port Lock (Настройка статической блокировки порта)	91
Настройка стандарта IEEE 802.1X	91
Автоматические предупреждения	95
Настройка предупреждений по e-mail	95
Настройка предупреждений через релейный выход	98
Использование функции Line-Swap-Fast-Recovery	100
Установка IP-адреса устройства	100
Automatic “Set Device IP” by DHCP/BootP/RARP (Автоматическая настройка функции «Set Device IP» с помощью DHCP/BootP/RARP-сервера)	102
Настройка функции DHCP Relay Agent	102
Диагнос	105
тика	105
Зеркалирование порта (Mirror Port)	105

<i>Ping</i>	106
<i>Функция LLDP</i>	106
Использование функции мониторинга	107
<i>Мониторинг коммутатора</i>	107
<i>Мониторинг портов</i>	108
<i>Мониторинг SFP-модулей</i>	109
Использование таблицы MAC-адресов	109
Использование списка управления доступом (ACL)	110
<i>Концепция функции ACL</i>	110
<i>Установка и настройка списка управления доступом</i>	112
Использование журнала событий	116
Использование функции Syslog	117
Использование протоколов HTTPS/SSL	118
4. Утилита настроек коммутатора EDS	119
<i>Начало работы с Конфигуратором EDS</i>	120
<i>Широковещательный поиск</i>	120
<i>Поиск по IP-адресу</i>	121
<i>Обновление микропрограммного обеспечения</i>	121
<i>Изменение IP-адреса</i>	122
<i>Экспорт настроек</i>	122
<i>Импорт настроек</i>	123
<i>Разблокировка сервера</i>	124
5. MIB-группы	126
6. Поддержка MOXA в Интернет	127

Введение

Благодарим Вас за выбор управляемого Ethernet-коммутатора компании Moxa. Данное руководство поможет Вам подключить данный коммутатор к Ethernet-устройствам, используемыми в Вашей промышленной сети.

Руководство разделено на две основные части:

- **Глава 2: Начало работы с коммутатором**

В данной главе подробно описан процесс установки коммутатора Moxa. Есть три варианта доступа к параметрам коммутатора: последовательная консоль, Telnet-консоль и web-консоль.

- **Глава 3: Основные функции**

В данной главе описывается, как получить доступ к различным функциям управления, мониторинга и администрирования. Эти функции могут быть доступны через последовательную консоль, Telnet-консоль и web-консоль. Web-консоль является наиболее удобным способом настройки коммутатора Moxa. В этой главе мы используем web-консоль для того, чтобы познакомить Вас с функциями управляемого Ethernet-коммутатора Moxa.

Начало работы с коммутатором

В данной главе подробно описан процесс установки коммутатора Муха в первый раз. Есть три способа управления коммутатором: последовательная консоль, Telnet-консоль и web-консоль. Если Вы не знаете IP-адрес коммутатора Муха, Вы можете открыть последовательную консоль, подключив коммутатор к СОМ-порту компьютера с помощью консольного кабеля. Соединение через Telnet или web-обозреватель позволяет получить доступ к коммутатору по сети Ethernet или Internet.

В данной главе раскрыты следующие темы:

- **Настройка с помощью последовательной консоли (115200, None, 8, 1, VT100)**
- **Настройка с помощью Telnet-консоли**
- **Настройка с помощью web-консоли**
- **Отключение доступа через Telnet и web-обозреватель**

Настройка с помощью последовательной консоли (115200, None, 8, 1, VT100)

Примечание:

- Вы не можете одновременно подключиться к коммутатору и через последовательную, и через Telnet-консоль.
- Вы можете одновременно подключиться к коммутатору через web-консоль и другую консоль (Telnet или последовательную). Тем не менее, мы настоятельно рекомендуем НЕ делать так, это позволит избежать конфликтов в управлении коммутатором.

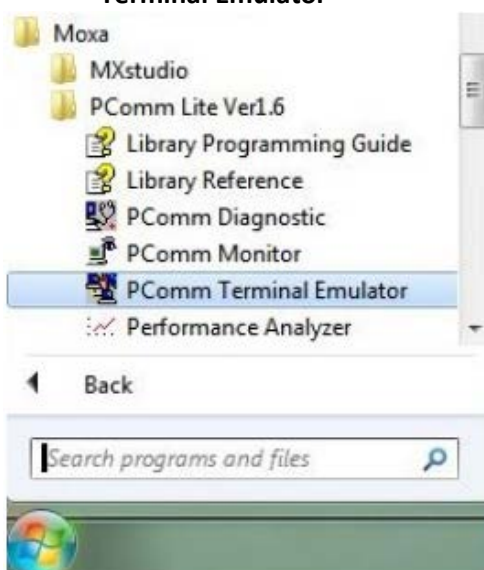
Примечание:

В качестве терминальной программы мы рекомендуем использовать ПО MOXA **PComm Terminal Emulator**, которое доступно для бесплатной загрузки на сайте компании MOXA.

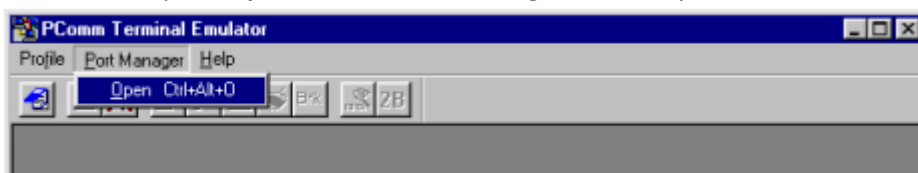
Перед началом работы с PComm Terminal Emulator подсоедините консольный порт коммутатора к COM-порту Вашего компьютера (обычно COM1 или COM2, в зависимости от настроек Вашей системы) через кабель RJ45-в-DB9-F (или RJ45-в-DB25-F).

После установки утилиты PComm Terminal Emulator выполните следующие действия для получения доступа к коммутатору через консоль RS-232:

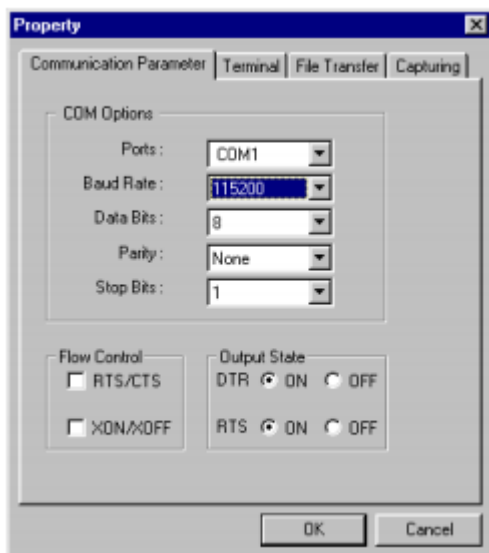
1. С рабочего стола Windows зайдите в меню **Start** → **Programs** → **Pcomm Lite Ver1.6** → **Terminal Emulator**



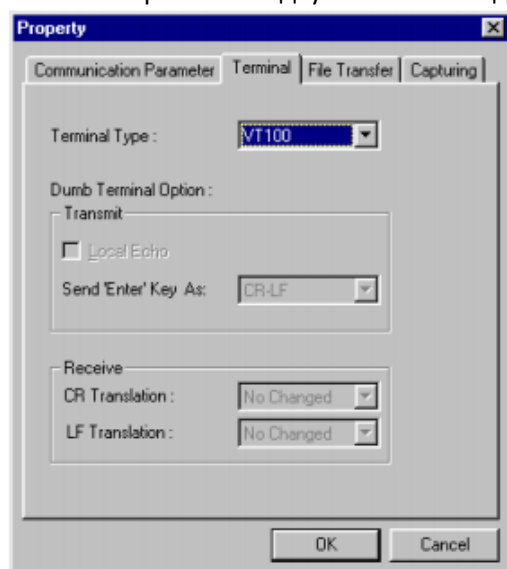
2. Выберите **Open** в меню **Port Manager** для настройки нового соединения.



3. В окне **Property** откроется вкладка **Communication Parameter**. Выберите соответствующий COM-порт для консольного управления, задайте параметры **Baud Rate – 115200, Data bits – 8, Parity – None и Stop Bits – 1**.



4. Откройте вкладку **Terminal** и задайте **Terminal Type – VT100**. Нажмите **OK**.



В окне терминала Введите **1** для выбора типа терминала **ansi/VT100**, нажмите Enter.

```
MOXA EtherDevice Switch IKS-6726
Console terminal type (1: ansi/vt100, 2: vt52) : 1
```

5. Откроется окно авторизации пользователя консоли. Нажмите **Enter** для выбора роли пользователя, выберите **admin** или **user**. Переведите курсор на поле **Console Password** и введите пароль (используется тот же пароль, что и для администрирования через web-обозреватель; оставьте поле пустым, если пароль еще не определен) и нажмите **Enter**.

```
Model : IKS-6726-T
Name : Managed Redundant Switch 02678
Location : Switch Location

Firmware Version : V2.6
Serial No : 02678
IP : 192.168.127.253
MAC Address : 00-90-E8-1B-55-24

+-----+
| Account : [admin] | user |
| Password : +-----+ |
+-----+
```

6. Загрузится главное меню (**Main Menu**) коммутатора (Примечание: для изменения настроек шрифта терминала *Psom Terminal Emulator* выберите **Font...** в меню **Edit** и установите необходимые параметры).

1. Basic Settings	- Basic settings for network and system parameter.
2. Port Trunking	- Allows multiple ports to be aggregated as a link.
3. SNMP Settings	- The settings for SNMP.
4. Comm. Redundancy	- Establish Ethernet communication redundant path.
5. Traffic Prioritization	- Prioritize Ethernet traffic to help determinism.
6. Virtual LAN	- Set up a VLAN by IEEE802.1Q VLAN or Port-based VLAN.
7. Multicast Filtering	- Enable the multicast filtering capability.
8. Bandwidth Management	- Restrict unpredictable network traffic.
9. Port Access Control	- Port access control by IEEE802.1X or Static Port Lock.
a. Auto Warning	- Warning email and/or relay output by events.
b. Line Swap	- Fast recovery after moving devices to different ports.
c. Set Device IP	- Assign IP addresses to connected devices.
d. Diagnosis	- Test network integrity and mirroring port.
e. Monitor	- Monitor a port and network status.
f. MAC Address Table	- The complete table of Ethernet MAC Address List.
g. System log	- The setting for System log, and Event log.
h. Exit	- Exit
	- Use the up/down arrow keys to select a category, and then press Enter to select. -

7. После входа в главное меню используйте следующие клавиши для перемещения курсора и выбора опций:

Клавиша	Функция
Вверх/Вниз/Влево/Вправо/Tab	Передвижение экранного курсора
Enter	Показать и выбрать опции
Пробел	Переключение между значениями
Esc	Предыдущее меню

Наст. роика через Telnet-консоль

Вы можете использовать консоль Telnet для настройки коммутатора через сеть. Для получения сетевого доступа (через Telnet или web-обозреватель) из ПК, подключенного к той же сети LAN, что и коммутатор, убедитесь, что оба находятся в одном и том же логическом сегменте. Для этого проверьте IP-адрес и маску сети Вашего ПК. По умолчанию IP-адрес коммутатора – 192.168.127.253, а маска подсети – 255.255.0.0 (для сети класса B). Если вы не измените эти значения, и маска подсети Вашего ПК 255.255.0.0, то IP-адрес компьютера должен иметь вид 192.168.xxx.xxx. Если маска подсети ПК 255.255.255.0, то его IP-адрес должен иметь вид 192.168.127.xxx.

Примечание:

Для доступа к функциям настройки коммутатора с помощью Telnet- или Web-консоли, убедитесь, что Ваш ПК и коммутатор находятся в одном и том же логическом сегменте сети.

Примечание:

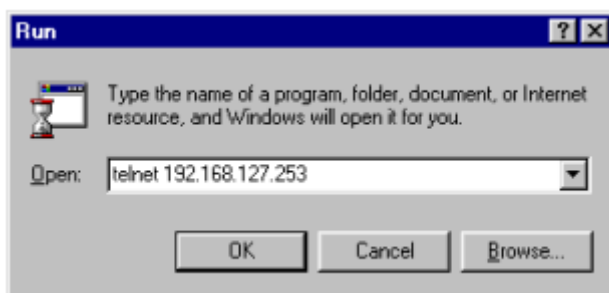
Перед осуществлением доступа через Telnet-консоль подключите один из Ethernet-портов RJ45 коммутатора к сети или непосредственно к сетевому адаптеру компьютера. Допускается использование как прямого, так и перекрестного Ethernet-кабеля. Если у Вас возникнут сложности с соединением, обратитесь к разделу «Автоматическое определение типа соединения MDI/MDI-X» настоящего руководства для получения дополнительной информации о типах Ethernet-кабелей и портов.

Примечание:

По умолчанию коммутатор MOXA имеет IP-адрес 192.168.127.253

Выполните следующие действия для получения доступа через Telnet-консоль:

1. В окне команды **Run (Пуск)** Windows введите команду **telnet** и задайте IP-адрес коммутатора.



2. Введите 1 для выбора терминала типа **ansi/VT100**, нажмите **Enter**.

```
MOXA EtherDevice Switch IKS-6726
Console terminal type (1: ansi/vt100, 2: vt52) : 1
```

3. Telnet-консоль предложит Вам войти в систему. Нажмите **Enter** для выбора аккаунта: администратора или пользователя (**admin** или **user**). С помощью клавиши «вниз» выберите поле **Password** и введите пароль, если это необходимо. Этот пароль будет использоваться для доступа через последовательную консоль, Telnet-консоль и web-обозреватель. Оставьте поле пустым, если пароль еще не определен, и нажмите **Enter**.

```
Model : IKS-6726
Name : Managed Redundant Switch 00000
Location : Switch Location

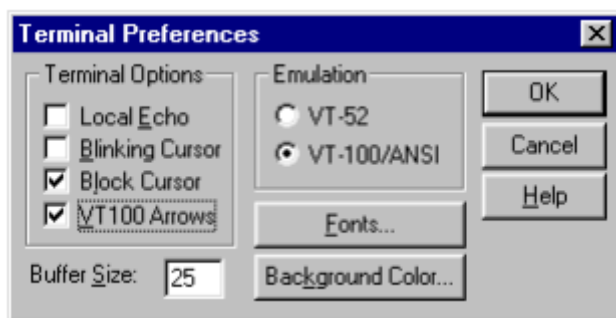
Firmware Version : V1.0
Serial No : 00000
IP : 192.168.127.253
MAC Address : 00-90-E8-00-67-26

+-----+
| Account : [admin] user |
| Password : +-----+ |
+-----+
```

4. Должно появиться главное меню (**Main Menu**) Telnet-консоли.

```
IKS-6726 series V1.0
-----
1. Basic Settings - Basic settings for network and system parameter.
2. Port Trunking - Allows multiple ports to be aggregated as a link.
3. SNMP Settings - The settings for SNMP.
4. Comm. Redundancy - Establish Ethernet communication redundant path.
5. Traffic Prioritization - Prioritize Ethernet traffic to help determinism.
6. Virtual LAN - Set up a VLAN by IEEE802.1Q VLAN or Port-based VLAN.
7. Multicast Filtering - Enable the multicast filtering capability.
8. Bandwidth Management - Restrict unpredictable network traffic.
9. Port Access Control - Port access control by IEEE802.1X or Static Port Lock.
a. Auto Warning - Warning email and/or relay output by events.
b. Line Swap - Fast recovery after moving devices to different ports.
c. Set Device IP - Assign IP addresses to connected devices.
d. Diagnosis - Test network integrity and mirroring port.
e. Monitor - Monitor a port and network status.
f. MAC Address Table - The complete table of Ethernet MAC Address List.
g. System log - The setting for System log, and Event log.
h. Exit - Exit
- Use the up/down arrow keys to select a category,
and then press Enter to select. -
```

5. Выберите в меню **Terminal** -> **Preferences...**, которое расположено в верхней части telnet-окна.
6. Должно открыться окно **Terminal Preferences**. Убедитесь, что стоит галочка **VT100 Arrows**.



7. Используйте следующие клавиши на клавиатуре, чтобы перемещаться внутри Telnet-консоли Моха:

Клавиша	Функция
Вверх/Вниз/Влево/Вправо/Tab	Передвижение экранного курсора
Enter	Показать и выбрать опции
Пробел	Переключение между значениями
Esc	Предыдущее меню

Примечание:

По внешнему виду и списку параметров Telnet-консоль аналогична последовательной консоли.

Наст. роика через web-обозреват ель

Web-интерфейс является самым удобным инструментом для настройки и мониторинга коммутатора МОХА. Для осуществления web-доступа можно использовать стандартные обозреватели, например, Internet Explorer.

Примечание:

Для доступа к функциям настройки коммутатора с помощью Telnet- или Web-консоли, убедитесь, что Ваш ПК и коммутатор находятся в одном и том же логическом сегменте сети.

Примечание:

Если коммутатор настроен для работы в виртуальных сетях VLAN, убедитесь в том, что VLAN ID компьютера соответствует параметру Management VLAN ID коммутатора.

Примечание:

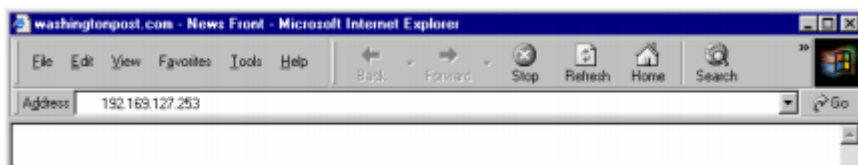
Перед осуществлением доступа через web-интерфейс или Telnet-консоль подключите один из Ethernet-портов RJ45 коммутатора к сети или непосредственно к сетевому адаптеру компьютера. Допускается использование как прямого, так и перекрестного Ethernet-кабеля.

Примечание:

По умолчанию коммутатор МОХА имеет IP-адрес 192.168.127.253

Выполните следующие действия для получения доступа через Web-обозреватель:

1. Введите IP-адрес коммутатора в Web-браузере в строке Address (Адрес) или URL. Нажмите Enter для установления соединения.



2. Откроется окно Web-консоли. Выберите аккаунт администратора или пользователя (**admin** или **user**) введите пароль (**Password**). Этот пароль будет использоваться для доступа через последовательную консоль, Telnet-консоль и web-обозреватель. Оставьте поле пустым, если пароль еще не определен, и нажмите **Enter**.



Примечание:

По умолчанию пароль в последовательной, Web- и Telnet-консоли, не задан, т.е. поле пароля пустое.

3. Возможно, для загрузки страницы администрирования придется подождать несколько секунд. Для доступа к функциям коммутатора используйте меню, располагающееся в левой части окна администрирования.



Отключение доступа через Telnet и web-обозреватель

Если Вы подключаете коммутатор к сети общего пользования и не собираетесь пользоваться функциями настройки коммутатора через сеть, мы рекомендуем отключить Telnet-консоль и web-интерфейс коммутатора. Для отключения функций настройки зайдите в меню **последовательной консоли: Basic Settings → System**, отключите Telnet- и Web-консоль как показано ниже:

```

Moxa EtherDevice Switch IKS-6726-T
Basic Settings
[System] [Password] [Accessible IP] [Port] [Network] [Time] [Backup Media]
[Restart] [Factory default] [Upgrade] [Activate] [Main menu]
System Identification
ESC: Previous menu  Enter: Select  Space bar: Toggle

Switch Name           [6726-252           ]
Switch Location       [Switch Location    ]
Switch Description    [MOXA IKS-6726-T   ]
Maintainer Contact Info [                    ]

Serial NO.            02678
Firmware Version      V2.6
MAC Address           00-90-E8-1B-55-24

Telnet Console        [Enable ]
Web Configuration     [http or https]
Web Auto-logout (s)  [0          ]
  
```

Основные функции

В этой главе описывается процесс получения доступа к основным функциям настройки, мониторинга и администрирования коммутатора. Предусмотрено три способа получения доступа к управлению коммутатором: последовательная консоль, Telnet-консоль и web-обозреватель. Доступ через последовательную консоль осуществляется локально путем подсоединения коммутатора к COM-порту компьютера через консольный кабель. Настройка через последовательную консоль удобна в тех случаях, если IP-адрес коммутатора неизвестен. Доступ к коммутатору по сети Ethernet или Internet осуществляется через Telnet-консоль или web-обозреватель.

Доступ через web-обозреватель – это наиболее удобный для пользователя способ настройки коммутатора MOXA. Основные процедуры настройки управляемого коммутатора будут представлены в этой главе на примере доступа через web-интерфейс. В целом, отличия между технологиями управления через последовательную консоль, Telnet и web очень невелики.

В этой главе будет рассмотрено:

- **Базовые настройки (Basic Settings)**
- **Защита от образования петель**
- **Использование функции Port Trunking**
- **Настройка SNMP**
- **Использование технологии питания по PoE (только для моделей с PoE)**
- **Использование приоритизации трафика**
- **Виртуальные сети VLAN**
- **Фильтрация широковещательного трафика**
- **Управление пропускной способностью по портам**
- **Безопасность**
- **Авторизационный сертификат**
- **Ограничение доступа по портам**
- **Автоматические предупреждения**
- **Технология Line-Swap-Fast-Recovery**
- **Назначение IP-адресов подключенным устройствам**
- **Диагностика**
- **Мониторинг**
- **Таблица MAC-адресов**
- **Управление доступом**
- **Журнал событий**
- **Системный журнал**
- **Использование HTTPS/SSL**

Базовые настройки

Базовые настройки (Basic Settings) – это набор базовых параметров, необходимых администраторам для работы с коммутаторами MOXA.

System Identification (Идентификация системы)

Параметры, заданные в разделе идентификация системы (system identification), будут отображены в верхней части web-обозревателя и будут включены в e-mail сообщения о сбоях системы. Настройка этих параметров позволит быстрее идентифицировать различные коммутаторы, работающие в сети.

System Identification

Switch Name	Managed Redundant Switch 00000
Switch Location	Switch Location
Switch Description	IKS-G6824
Maintainer Contact Info	
Web Configuration	http or https
Web Auto-logout (s)	0
Age Time (s)	300
CPU Loading (past 5 seconds)	9 %
CPU Loading (past 30 seconds)	10 %
CPU Loading (past 5 minutes)	10 %
Free Memory	60061004
Jumbo Frame	Disable
Jumbo Frame MAX (bytes)	9000

Activate

Switch Name (Имя коммутатора)

Параметр	Описание	Значение по умолчанию
Макс.30 символов	Данный параметр описывает роль, которую выполняет коммутатор. Например, Factory Switch 1.	Managed Redundant Switch [серийный номер коммутатора]

Switch Location (Местоположение коммутатора)

Параметр	Описание	Значение по умолчанию
Макс.80 символов	Данный параметр описывает местоположение коммутатора. Например, production line 1.	Switch Location

Switch Description (Описание коммутатора)

Параметр	Описание	Значение по умолчанию
Макс.30 символов	Данный параметр описывает более подробную информацию о коммутаторе.	Нет

Maintainer Contact Info (Информация об администраторе)

Параметр	Описание	Значение по умолчанию
Макс.30 символов	Данный параметр содержит контактную информация о лице, осуществляющем поддержку устройства.	Нет

Web Auto-logout (S) (Автоматический выход из Web-консоли (секунды))

Параметр	Описание	Значение по умолчанию
60-86400 (секунд)	Отключить или продлить время автоматического выхода из Web-консоли.	0 (отключен)

Age Time (S) (Время хранения записи в таблице MAC-адресов (секунды))

Параметр	Описание	Значение по умолчанию
15-3825 (секунд)	Время хранения записи о MAC-адресе в таблице коммутатора Моха. По истечении заданного промежутка времени запись об адресе удаляется, и данные не будут передаваться строго на указанный порт.	300

CPU Loading (Загрузка процессора)

Параметр	Описание	Значение по умолчанию
Только чтение	Объем использования процессора в течение последних 5 секунд, 30 секунд, 5 минут.	Нет

Free Memory (Свободная память)

Параметр	Описание	Значение по умолчанию
Только чтение	Текущая загрузка памяти на коммутаторе.	Нет

Jumbo Frame (поддержка Jumbo Frame)

Параметр	Описание	Значение по умолчанию
Включен	Включает поддержку кадров Jumbo Frame на коммутаторе.	Выключен
Выключен	Выключает поддержку кадров Jumbo Frame.	

Jumbo Frame MAX (bytes) (Максимальное количество байт в кадре Jumbo Frame)

Параметр	Описание	Значение по умолчанию
1522-9000	Максимальная длина кадра Jumbo Frame.	9000

Примечание:

Функция Jumbo Frame поддерживается только в коммутаторах серии IKS-G6000 и ICS-G7000.

Password (Пароль)

Коммутатор Моха обеспечивает два уровня доступа. Пользователь **admin** имеет возможность полностью производить конфигурирование и изменение настроек коммутатора, **user** имеет только возможность чтения параметров и не может вносить никаких изменений.



Внимание!

По умолчанию пароль для коммутатора не задан. Если администратором был задан пароль, то его необходимо будет вводить при каждой загрузке последовательной консоли, Telnet-консоли или web-обозревателя.

Account (Учетная запись)

Параметр	Описание	Значение по умолчанию
Admin	Учетная запись admin позволяет изменять все параметры коммутатора.	admin
User	Учетная запись user позволяет только просматривать параметры коммутатора.	

Password (Пароль)

Параметр	Описание	Значение по умолчанию
Old password (Старый пароль, макс. 16 символов)	Для смены пароля введите текущий пароль.	Нет
New password (Новый пароль, макс. 16 символов)	Задайте новый пароль.	Нет
Retype password (Повтор пароля, макс.16 символов)	Повторите ввод нового пароля для проверки правильности введенных данных.	Нет

Accessible IP List (Разрешенные IP-адреса)

Коммутаторы Моха используют функцию фильтрации по IP-адресам для контроля доступа.



Вы можете добавлять или удалять IP-адреса для ограничения доступа к коммутатору. Когда включен список доступных IP-адресов, только адресам из списка будет разрешен доступ к коммутатору Моха. Каждая запись IP-адреса и маски подсети могут использоваться для различных ситуаций:

- **Предоставление доступа хосту с определенным IP-адресом**

Например, введите IP-адрес 192.168.1.1 с маской подсети 255.255.255.255 для доступа только к адресу 192.168.1.1.

- **Предоставление доступа любому хосту указанной подсети**

Например, введите IP-адрес 192.168.1.0 с маской подсети 255.255.255.0 для доступа со всех IP-адресов подсети в соответствии с указанной комбинацией IP-адреса/маски подсети.

- **Предоставление доступа для всех хостов**

Убедитесь, что список разрешенных IP-адресов выключен. Снимите флажок с поля **Enable the accessible IP list**.

В таблице ниже показаны примеры конфигурирования списка разрешенных IP-адресов:

Разрешенные хосты	Формат ввода
Any host (Любой хост)	Снять флажок «Enable the accessible IP list»
192.168.1.120	192.168.1.120 / 255.255.255.255
192.168.1.1 ~ 192.168.1.254	192.168.1.0 / 255.255.255.0
192.168.0.1 ~ 192.168.255.254	192.168.0.0 / 255.255.0.0
192.168.1.1 ~ 192.168.1.126	192.168.1.0 / 255.255.255.128
192.168.1.129 ~ 192.168.1.254	192.168.1.128 / 255.255.255.128

Port Settings (Настройка портов)

Port Settings (Настройка Ethernet-порта)

Настройки параметров порта нужны для того, чтобы дать пользователю возможность контролировать доступ к порту и скорость передачи данных, управлять потоком и настраивать тип порта (MDI или MDIX).



Enable (Включить)

Параметр	Описание	Значение по умолчанию
Включен	Разрешает передачу данных по порту.	Enabled (включен)
Выключен	Немедленно прекращает передачу данных по порту.	



Внимание!

Если Ethernet-устройство или сегмент сети, подключенные к порту, наносят вред остальной сети, возможность деактивации передачи данных через порт в **Basic Settings/Port** позволяет администратору немедленно отключить прохождение трафика через этот порт.

Description (Описание)

Параметр	Описание	Значение по умолчанию
Тип среды передачи данных	Отображает тип среды передачи данных по каждому порту	Нет

Name (Имя)

Параметр	Описание	Значение по умолчанию
Макс.63 символа	Задаёт имя данному порту, помогая администратору видеть различия между портами. Например, PLC 1.	Нет

Speed (Скорость передачи данных по порту)

Параметр	Описание	Значение по умолчанию
Auto	Позволяет порту использовать протокол IEEE 802.3u для согласования скорости с подключенными устройствами. Порт и подключенные устройства самостоятельно определяют оптимальную скорость обмена данными.	Auto
1G-Full	Выберите одну из	

100M-Full	фиксированных скоростей передачи, если по какой-то причине функция автоматического согласования auto negotiation не может быть использована.	
100M-Half		
10M-Full		
10M-Half		

FDX Flow Ctrl (Контроль потока Full Duplex)

Этот параметр разрешает или запрещает возможность контроля потока данных в случае, если поле Speed (скорость передачи данных по порту) имеет значение "auto". Конечный результат будет определен автоматически между коммутатором Моха и подключенными устройствами.

Параметр	Описание	Значение по умолчанию
Включен	Включает возможность контроля потока при работе устройства в режиме скорости Auto.	Выключен
Выключен	Отключает возможность контроля потока при работе устройства в режиме скорости Auto.	

MDI/MDIX

Параметр	Описание	Значение по умолчанию
Auto	Позволяет порту автоматически определять тип портов подключенных устройств и соответственно изменять свой тип порта.	Auto
MDI	Используйте значения MDI или MDIX, если возникают трудности с определением типа порта с помощью функции автоматического согласования auto negotiation.	
MDIX		

Network Parameters (Параметры сети)

Настройка сетевых параметров позволяет пользователям задавать параметры адресов IPv4 и IPv6 для настройки доступа к коммутатору через сеть. Коммутаторы Моха поддерживают адреса IPv4 и IPv6 и могут управляться с помощью каждого из них.

Смысл каждого параметра расшифрован ниже:



IPv4

Настройки IPv4 включают в себя IP-адрес коммутатора и маску подсети, а также IP-адрес шлюза по умолчанию. Кроме того, есть поля для указания IP-адреса 1-го и 2-го сервера DNS.

Auto IP Configuration (Автоматическая настройка IP-адреса)

Параметр	Описание	Значение по умолчанию
Disable (Выключен)	Задание IP-адреса коммутатора вручную.	Disable (Выключен)
By DHCP (с помощью DHCP)	IP-адрес коммутатора будет назначен автоматически DHCP-сервером.	
By BootP (с помощью BootP)	IP-адрес коммутатора будет назначен автоматически сетевым BootP-сервером.	

Switch IP Address (IP-адрес коммутатора)

Параметр	Описание	Значение по умолчанию
IP-адрес коммутатора Моха	Задаёт IP-адрес коммутатора в сети TCP/IP.	192.168.127.253

Switch Subnet Mask (Маска подсети)

Параметр	Описание	Значение по умолчанию
Маска подсети коммутатора	Определяет типа сети, к которой подключен коммутатор (например, 255.255.0.0 для сети класса B, 255.255.255.0 для сети класса C).	255.255.255.0

Default Gateway (Шлюз по умолчанию)

Параметр	Описание	Значение по умолчанию
IP-адрес шлюза по умолчанию	IP-адрес шлюза, соединяющего LAN с внешней сетью.	Нет

DNS IP Address (IP-адрес DNS-сервера)

Параметр	Описание	Значение по умолчанию
IP-адрес первого DNS-сервера	IP-адрес DNS-сервера Вашей сети. После задания IP-адреса	Нет

	DNS-сервера Вы можете вводить URL коммутатора EDS (например, www.PT.company.com) в браузере вместо введения IP-адреса.	
IP-адрес второго DNS-сервера	IP-адрес DNS-сервера Вашей сети. Коммутатор будет пытаться работать со вторым DNS-сервером в случае отсутствия соединения с первым	Нет

DHCP Retry Periods (Периоды повтора запросов к DHCP-серверу)

Параметр	Описание	Значение по умолчанию
1-30	Пользователь может вручную настроить периоды повтора запросов к DHCP-серверу.	1

DHCP Retry Times (Интервалы повторов запросов к DHCP-серверу)

Параметр	Описание	Значение по умолчанию
0-65535	Пользователь может вручную настроить интервалы повторов запросов к DHCP-сервера.	0

IPv6

Настройки адреса IPv6 включают в себя два типа адресов: адрес Link-Local Unicast и адрес Global Unicast. Адрес Link-Local делает коммутатор доступным через IPv6 для всех устройств, подключенных к той же локальной подсети. Для подключения к сети большего размера с несколькими сегментами тип адреса коммутатора должен быть Global Unicast.

Global Unicast Address Prefix (Prefix Length: 64 bits) (Префикс адреса Global Unicast, макс.длина префикса – 64 бита)

Параметр	Описание	Значение по умолчанию
Префикс адреса Global Unicast	Значение префикса должно соответствовать RFC 2373 "IPv6 Addressing Architecture," ("Адресация архитектуры IPv6"), используя 16-битные шестнадцатеричные значения, разделенные двоеточиями на 8 частей. Одно двойное двоеточие можно использовать в адресе, чтобы указать нужное количество нулей, необходимое для заполнения неопределенного поля.	Нет

Global Unicast Address (Адрес Global Unicast)

Параметр	Описание	Значение по умолчанию
----------	----------	-----------------------

Нет	Отображение адреса Global Unicast IPv6. Сетевую часть адреса Global Unicast можно настроить, указав префикс Global Unicast и используя ID интерфейса EUI-64 в младших 64 битах. Host-часть адреса Global Unicast автоматически генерируется с использованием модифицированной EUI-64 формы идентификатора интерфейса (MAC-адреса коммутатора)	Нет
-----	---	-----

Link-Local Address (Адрес Link-Local)

Параметр	Описание	Значение по умолчанию
Нет	Сетевая часть локального адреса – FE80, а часть хоста локального адреса автоматически генерируется с использованием модифицированной EUI-64 формы идентификатора интерфейса (MAC-адреса коммутатора)	Нет

Neighbor Cache

IPv6 Address	Link Layer (MAC) Address	State
fe80::290:e0ff:fe0e:e02	00-90-e8-0e-0e-02	Reachable

Neighbor Cache (таблица соседних устройств)

Параметр	Описание	Значение по умолчанию
Нет	Информация, содержащаяся в таблице соседних устройств, включает в себя IPv6-адреса смежных узлов, их адреса Link-Layer и информацию о текущем состоянии записей.	Нет

GARP Timer Parameters (Параметры таймера GARP)

Базовый протокол регистрации атрибутов (GARP) обеспечивает общую структуру сети, он описан в стандарте IEEE 802.1. Технология GARP определяет архитектуру, правила функционирования, состояния устройств, а также переменные для регистрации и отмены регистрации значений атрибутов.

Параметры таймера GARP обмениваются путем создания приложений с помощью GVRP (Протокол регистрации VLAN GARP) для установки свойств таймера.

Обратите внимание, что Вам необходимо установить одинаковые значения таймера GARP на всех коммутаторах 2-го уровня, чтобы убедиться в том, что система работает корректно.

Join Time (время join-сообщения)

Параметр	Описание	Значение по умолчанию
Нет	Определяет период времени join-сообщения	200

Leave Time (время leave-сообщения)

Параметр	Описание	Значение по умолчанию
Нет	Определяет период времени Leave-сообщения	600

Leaveall Time (время leaveall-сообщения)

Параметр	Описание	Значение по умолчанию
Нет	Определяет период времени Leaveall-сообщения	10000

Примечание:

Параметр Leave Time должен быть минимум в два раза больше, чем параметр Join Time, а Leaveall Time – больше, чем Leave Time.

System Time Settings (Настройки сист. много времени)

Коммутатор Моха имеет функцию установки системного времени на основе информации, полученной от NTP-сервера, а также может принимать дату и время, заданные пользователем. Благодаря этому такие функции, как автоматическое сообщение о событии по e-mail, содержат информацию о точном времени наступления события.

Примечание:

Коммутаторы Моха не обладают часами реального времени. Пользователь должен устанавливать актуальные дату и время после каждой перезагрузки устройства, особенно, если отсутствует связь с NTP-сервером или Интернет-соединение.

Current Time (Текущее время)

Параметр	Описание	Значение по умолчанию
Заданное пользователем текущее время	Этот параметр позволяет задать местное время в 24-часовом формате.	Нет

Current Date (Текущая дата)

Параметр	Описание	Значение по умолчанию
Заданная пользователем текущая дата	Этот параметр позволяет задать текущую дату в формате год/месяц/число.	Нет

Daylight Saving Time (Переход на летнее время)

Настройки перехода на летнее время используются для автоматического перехода, соответствующего стандартам страны.

Start Date (Дата начала)

Параметр	Описание	Значение по умолчанию
Заданная пользователем дата начала	Данный параметр определяет дату перехода на летнее время.	Нет

End Date (Дата окончания)

Параметр	Описание	Значение по умолчанию
Заданная пользователем дата окончания	Данный параметр определяет дату окончания летнего времени.	Нет

Offset (Количество часов при переводе времени)

Параметр	Описание	Значение по умолчанию
Заданное пользователем количество часов	Данный параметр определяет количество часов, на которое время должно быть переведено вперед при переходе на летнее время.	Нет

System Up Time (Продолжительность работы системы)

Отображает продолжительность работы коммутатора (в секундах) со времени последнего «холодного» запуска.

Time Zone (Часовой пояс)

Параметр	Описание	Значение по умолчанию
Заданный пользователем часовой пояс	Позволяет осуществлять перевод времени из Гринвича (GMT) в местное время.	GMT (Greenwich Mean Time)

Примечание:

Изменение часового пояса приведет к изменению текущего времени. Настройте часовой пояс до

настройки времени.

Time Server IP/Name (IP-адрес/имя сервера времени)

Параметр	Описание	Значение по умолчанию
IP-адрес/имя 1ого сервера времени	IP-адрес или доменное имя (например, 192.168.1.1 или time.stdtime.gov.tw или time.nist.gov)	Нет
IP-адрес/имя 2ого сервера времени	Коммутатор будет пытаться работать со 2ым сервером времени в случае отсутствия соединения с 1ым.	

Time Protocol (Протокол передачи времени)

Параметр	Описание	Значение по умолчанию
NTP	NTP (протокол сетевого времени) необходим для синхронизации времени с несколькими серверами времени. Точность составляет до 50 мс.	
SNTP	С SNTP (простой протокол сетевого времени) процесс синхронизации проще, чем с NTP. Точность времени – до 1 секунды, подходит для приложений, нетребовательных к точности времени.	

Enable NTP/SNTP Server (Включение NTP/SNTP сервера)

Параметр	Описание	Значение по умолчанию
Включен/выключен	Включает функциональные возможности сервера SNTP/NTP для клиентов.	Выключен

IEEE 1588 PTP

Информация для данного раздела взята с сайта NIST (<http://ieee1588.nist.gov/intro.htm>)

«Измерение времени должно происходить в соответствии с Протоколом синхронизации точного времени для сетевых измерительных систем и систем управления (стандарт IEEE 1588-2008) с целью синхронизации часов реального времени, установленных в компонентах системы автоматизации электроэнергетических объектов.

Стандарт IEEE 1588 (ноябрь 2002 года) расширяет возможности применения Ethernet-сетей в системах управления, повышает производительность сетей. В последнее время все больше энергетических систем используют сильно распределенные сети, которые не могут отвечать жестким требованиям к синхронизации времени. Рассматриваемый стандарт регулирует отношения master-slave между часами и обеспечивает соблюдение конкретных требований ко времени в системах электроэнергетики. Все устройства получают информацию о времени от часов grandmaster. Протокол в первую очередь предназначен для удобного управления сетью».

Как коммутатор Ethernet влияет на синхронизацию IEEE 1588?

Информация для данного раздела взята с сайта NIST (<http://ieee1588.nist.gov/switch.htm>):

«Ethernet-коммутатор вносит задержку в несколько микросекунд при синхронизации между часами grandmaster и часами slave, соответствующими стандарту IEEE 1588. Такие задержки могут приводить к ошибкам в синхронизации. Длительность задержек зависит от конструкции коммутатора и от особенностей сетевого трафика. Эксперименты с прототипами протокола IEEE 1588 показали, что задержками можно управлять. Например, благодаря использованию статистических данных с устройств, работающих по IEEE 1588, можно выявить средние задержки, и затем их компенсировать для достижения максимальной точности синхронизации времени».

Возможно ли создание Ethernet-коммутаторов, защищенных от колебаний времени задержки?

Ethernet-коммутатор с поддержкой IEEE 1588 должен не допускать образования очереди в передаче информации. Он должен отличаться от обычного коммутатора двумя параметрами:



Часы Grandmaster:
Определяют основное
время системы

Пограничные часы
(boundary clock):
Выполняют функцию Slave
по отношению к
Grandmaster и функцию
master к своим slave-
устройствам

Обычные часы (ordinary
clock):
Выполняют функцию Slave
по отношению к master-
устройству

1. В коммутаторе должны быть реализованы функции пограничных часов (Boundary Clock) и прозрачных часов (Transparent Clock).
2. Коммутатор должен быть настроен так, чтобы передавать сообщения IEEE 1588 способом, альтернативным способу передачи обычного трафика.

Такой коммутатор будет синхронизировать часы всех устройств, подключенных к нему, с максимально возможной точностью.

Примечание:

Если модуль CM-600-4TX-PTP не установлен, то коммутатор серии EDS-600 поддерживает только программную реализацию стандарта IEEE 1588.

PTP Setting (Настройка PTP)

PTP Setting

IEEE 1588/PTP Operation
 Operation Enable PTP

IEEE 1588/PTP Configuration

Clock Mode v2 E2E BC

logSyncInterval 0 (1 sec)

logAnnounceInterval 1 (2 sec)

announceReceiptTimeout 3

logMinDelayReqInterval 0 (1 sec)

Domain Number 0 (DFLT)

Transport of PTP IPv4

priority1 128

priority2 128

clockClass 248

clockAccuracy 0x21

Timescale PTP

ARB Time 0

Leap59 False

Leap61 False

UTC Offset Valid False

UTC Offset 0

Status

Current Data Set
 Offset To Master(nsec)
 Mean Path Delay(nsec)
 Step Removed

Parent Data Set
 Parent Identity
 Grandmaster Identity
 Grandmaster clockClass
 Grandmaster clockAccuracy
 Grandmaster priority1
 Grandmaster priority2

Parent Time Data Set
 Current UTC Offset Valid
 Current UTC Offset
 Leap59
 Leap61
 Timescale
 Time Source

PTP Port Settings

Port	Port Enable	Port Status
1-1	<input type="checkbox"/> Enable	PTP_DISABLED
1-2	<input type="checkbox"/> Enable	PTP_DISABLED
1-3	<input type="checkbox"/> Enable	PTP_DISABLED
1-4	<input type="checkbox"/> Enable	PTP_DISABLED
2-1	<input type="checkbox"/> Enable	PTP_DISABLED

Activate

IEEE 1588/PTP Operation (Работа стандарта IEEE 1588/PTP)

Параметр	Описание	Значение по умолчанию
PTP включен	Включает или выключает работу IEEE 1588	Выключен

IEEE 1588/PTP Configuration (Настройка IEEE 1588/PTP)

Clock Mode (Режим часов (устанавливает режим часов коммутатора))

Параметр	Описание	Значение по умолчанию
v1 BC	Включает режим работы пограничных часов (boundary clock) IEEE 1588 v1	v1 BC
v2 E2E 2-step TC	Включает режим работы прозрачных часов (transparent clock) IEEE 1588 v2 edge-to-edge с 2-шаговым методом	
v2 E2E 1-step TC	Включает режим работы прозрачных часов (transparent clock) IEEE 1588 v2 edge-to-edge с 1-шаговым методом	
v2 P2P 2-step TC	Включает режим работы прозрачных часов (transparent clock) IEEE 1588 v2 peer-to-peer с 2-шаговым методом	
v2 E2E BC	Включает режим работы пограничных часов (boundary clock) IEEE 1588 v2 edge-to-edge	
v2 P2P BC	Включает режим работы пограничных часов (boundary clock) IEEE 1588 v2 peer-to-peer	

logSyncInterval (устанавливает временной интервал для сообщений синхронизации)

Параметр	Описание	Значение по умолчанию
0, 1, 2, 3 или 4	0 (1 с), 1 (2 с), 2 (4 с), 3 (8 с) или 4 (16 с). Поддерживается IEEE 1588 V1.	0
-3, -2, -1, 0 или 1	-3 (128 мс), -2 (256 мс), -1 (512 мс), 0 (1 с) или 1 (2 с). Поддерживается IEEE 1588 V2.	

logAnnounceInterval (устанавливает интервал отправки оповещающих сообщений)

Параметр	Описание	Значение по умолчанию
0, 1, 2, 3 или 4	0 (1 с), 1 (2 с), 2 (4 с), 3 (8 с) или 4 (16 с)	1 (2 с)

announceReceiptTimeout

Параметр	Описание	Значение по умолчанию
2, 3, 4, 5, 6, 7, 8, 9 или 10	Множитель для определения таймаута получения оповещающего сообщения по интервалу отправки оповещающего сообщения.	3

logMinDelayReqInterval

Параметр	Описание	Значение по умолчанию
0, 1, 2, 3, 4 или 5	Минимальный интервал времени отправки запроса задержки.	0 (1 с)

logMinPdelayReqInterval

Параметр	Описание	Значение по умолчанию
-1, 0, 1, 2, 3 или 4	Минимальный интервал времени отправки	0 (1 с)

	запроса задержки: -1 (512 мс), 0 (1 с), 1 (2 с), 2 (4 с), 3 (8 с) или 4 (32 с) (Доступно в режиме часов версий v2 P2P 2-step TC и v2 P2P BC)	
--	--	--

Domain Number (Номер домена)

Параметр	Описание	Значение по умолчанию
_DFLT (0), _ALT(1), _ALT(2) или _ALT(3)	Имя поддомена (IEEE 1588-2002) или номер домена (IEEE 1588-2008) в PTP-сообщении	_DFLT (0)

Transport of PTP (транспортный протокол для передачи сообщений IEEE 1588 PTP)

Параметр	Описание	Значение по умолчанию
IPv4 или 802.3/Ethernet	<ul style="list-style-type: none"> IEEE 1588 PTP V1 поддерживает только IPv4 IEEE 1588 PTP V2 поддерживает и IPv4, и IPv6 	IPv4

Preferred Master

Параметр	Описание	Значение по умолчанию
True or False (Правда или ложь)	Назначение коммутатора на роль GrandMaster	False

priority1

Параметр	Описание	Значение по умолчанию
0-255	Установка первого приоритета; 0 = наивысший приоритет, 255 = самый низкий приоритет	128

priority2

Параметр	Описание	Значение по умолчанию
0-255	Установка второго приоритета; 0 = наивысший приоритет, 255 = самый низкий приоритет	128

clockClass

Параметр	Описание	Значение по умолчанию
0-255	Данный параметр обозначает отслеживание времени или частоты, установленными часами grandmaster.	248

clockAccuracy (Точность часов)

Параметр	Описание	Значение по умолчанию
0x21	Данный параметр означает точность синхронизации с master-часами. Значение 0x21 говорит о том, что точность времени коммутатора – до 100 нс.	0x21

Timescale (шкала времени)

Параметр	Описание	Значение по умолчанию
PTP или ARB	<ul style="list-style-type: none"> Шкала времени PTP: При нормальной работе шкала времени непрерывна. Единица времени – секунда в Международной системе единиц 	PTP

	<ul style="list-style-type: none"> Шкала времени ARB: При нормальной работе период времени устанавливается во время административных работ. Период может быть сброшен во время работы. Между административными работами шкала времени непрерывна. Дополнительные административные работы могут вызвать ошибки в шкале времени. 	
--	---	--

ARB Time (время ARB)

Параметр	Описание	Значение по умолчанию
0-255	Время отсчёта (в секундах) РТР-часов	0

Leap59

Параметр	Описание	Значение по умолчанию
True or False (Правда или ложь)	Последняя минута текущего UTC-дня содержит 59 секунд. Если шкала времени не РТР, то значение будет False.	False

Leap61

Параметр	Описание	Значение по умолчанию
True or False (Правда или ложь)	Последняя минута текущего UTC-дня содержит 61 секунд. Если шкала времени не РТР, то значение будет False.	False

UTC Offset Valid

Параметр	Описание	Значение по умолчанию
True or False (Правда или ложь)	Если время смещения UTC верно, то значение будет True, если нет, то False.	False

UTC Offset

Параметр	Описание	Значение по умолчанию
0-255	Имеющееся смещение UTC (в секундах)	0

Status (состояние)

Параметр	Описание	Значение по умолчанию
N/A	Текущее состояние IEEE 1588 РТР.	N/A

PTP Port Settings (Настройка РТР-порта)

Текущие настройки РТР-порта.

Turbo Ring DIP Switch (DIP-переключатель Turbo Ring)

Раздел Turbo Ring DIP Switch позволяет пользователю отключать четвёртый DIP-переключатель, расположенный на верхней панели коммутатора. По умолчанию он включен и настроен для использования по протоколу Turbo Ring v2. Когда пользователь изменяет положение 4ого DIP-переключателя в состояние ON, на коммутаторе запустится процесс инициации протокола резервирования Turbo Ring. Ниже показано подробное описание:

Turbo Ring DIP Switch

Disable the Turbo Ring DIP Switch

1. To enable the entire set of Hardware DIP switches, uncheck the "Disable the Turbo Ring DIP Switch" option.
2. To disable the entire set of Hardware DIP switches, check the "Disable the Turbo Ring DIP Switch" option.

Set DIP switch as Turbo Ring

Set DIP switch as Turbo Ring v2

Activate

Параметр	Описание	Значение по умолчанию
Disable the Turbo Ring DIP switch (DIP-переключатель Turbo Ring выключен)	Не выбран: Протокол Turbo Ring активируется автоматически в тот момент, когда 4ый DIP-переключатель будет установлен в положение ON.	Не выбран
	Выбран: Протокол Turbo Ring не активируется автоматически в независимости от положения 4ого DIP-переключателя.	
Set DIP switch as Turbo Ring (Включить функцию Turbo Ring)	Если DIP-переключатель включен, то протокол Turbo Ring будет активирован, когда DIP-переключатель будет установлен в положение ON.	Set DIP switch as Turbo Ring v2
Set DIP switch as Turbo Ring v2 (Включить функцию Turbo Ring v2)	Если DIP-переключатель включен, то протокол Turbo Ring v2 будет активирован, когда DIP-переключатель будет установлен в положение ON.	

Примечание:

Когда 4ый DIP-переключатель (Turbo Ring) установлен в положение ON, пользователь не сможет отключить функцию Turbo Ring с помощью web-обозревателя, последовательной или Telnet-консоли.

Если Вы хотите включить VLAN и/или функцию port trunking (объединение портов) на любом из последних четырех портов коммутатора, не используйте 4ый DIP-переключатель для активации функции Turbo Ring. В таком случае используйте web-обозреватель, последовательную или Telnet-консоль для активации функции Turbo Ring.

System File Update (Обновление системных настроек)

Update System Files By Remote TFTP (Обновление системных настроек с удаленного TFTP-сервера)

Коммутатор MOXA позволяет сохранять текущие настройки коммутатора в файл на удаленный TFTP-сервер или на локальный хост. Это позволяет в дальнейшем использовать эти же параметры для других коммутаторов Moxa. Кроме того, коммутаторы Moxa поддерживают функцию загрузки настроек и микропрограммного обеспечения с удаленного TFTP-сервера или локального хоста.

Update System Files by TFTP

TFTP Server IP/Name

Configuration Files Path and Name

Firmware Files Path and Name

Log Files Path and Name

TFTP Server IP/Name (IP-адрес/имя TFTP-сервера)

Параметр	Описание	Значение по умолчанию
IP-адрес TFTP-сервера	IP-адрес или имя TFTP-сервера. Должны быть заданы до загрузки или сохранения файлов.	Нет

Configuration Files Path and Name (имя файла настроек и путь к нему)

Параметр	Описание	Значение по умолчанию
Максимально 40 символов	Имя файла настроек коммутатора и путь к нему на сервере TFTP.	Нет

Firmware Files Path and Name (имя файла микропрограммного обеспечения и путь к нему)

Параметр	Описание	Значение по умолчанию
Максимально 40 символов	Имя файла микропрограммного обеспечения коммутатора и путь к нему на сервере TFTP.	Нет

Log Files Path and Name (имя log-файла и путь к нему)

Параметр	Описание	Значение по умолчанию
Максимально 40 символов	Имя log-файла коммутатора и путь к нему на сервере TFTP.	Нет

После задания пути и имени файла нажмите **Download** для скачивания подготовленного файла с удаленного TFTP-сервера или **Upload** для помещения нужного файла на TFTP-сервер.

Update System Files from Local PC (Обновление системных настроек через локальный компьютер)



Configuration File (Файл настроек)

Для экспортирования файла настроек коммутатора нажмите **Export** и сохраните файл на локальном хосте.

Log File (Log-файл)

Для экспортирования log-файла нажмите **Export** и сохраните файл на локальном хосте.

Примечание:

Некоторые операционные системы откроют файл настроек и log-файл на web-странице. В этом случае для сохранения файла нажмите правой кнопкой мышки на кнопке **Export**.

Upgrade Firmware (Обновление микропрограммного обеспечения)

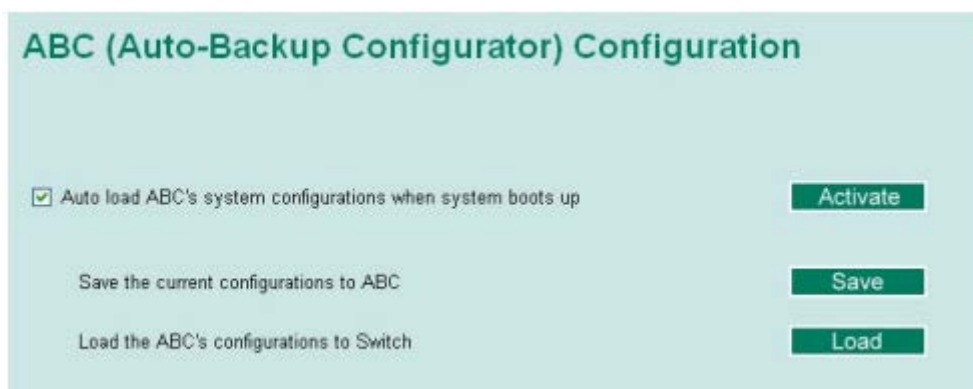
Для импортирования файла микропрограммного обеспечения в данный коммутатор нажмите **Browse** для выбора файла микропрограммного обеспечения, ранее сохраненного на Вашем ПК. Процедура обновления запустится автоматически после нажатия на **Import**.

Upload Configure Data (Загрузка файла настроек)

Для импортирования файла настроек в данный коммутатор, нажмите **Browse** для выбора файла настроек, ранее сохраненного на Вашем компьютере. Процедура обновления запустится автоматически после нажатия на **Import**.

ABC (Auto-Backup Configurator) Configuration (Обновление системных настроек с использованием устройства резервного хранения конфигурации ABC)

Для сохранения и загрузки настроек коммутатора пользователь может использовать устройства резервного хранения конфигурации ABC, подключаемые к консольному порту RS-232 коммутатора.



Restart (Перезагрузка)

Данная функция позволяет пользователям быстро перезагрузить систему (коммутатор).



Reset to Factory Default (Сброс к заводским наст. роикам)



Данная функция позволяет пользователям сбросить коммутатор к заводским настройкам. Данная функция доступна в web-обозревателе, последовательной и Telnet-консоли.

Примечание:

После восстановления заводских настроек, Вам нужно будет использовать настройки сети по умолчанию, чтобы восстановить соединение с коммутатором Мохы через Web- или Telnet-консоль.

Loop Protection (Защита от образования петель)

Коммутаторы Мохы обладают функцией защиты от образования петель: отправьте контрольное сообщение BPDU с Ethernet-порта и проверьте, вернется ли оно обратно к коммутатору. Если это произойдет, коммутатор будет автоматически блокировать Ethernet-порт для предотвращения заикливания.



Выберите Enable и нажмите **Activate** для включения защиты от образования петель.

Использование функции Port Trunking

Технология Link Aggregation (объединения линий связи) позволяет объединить несколько линий сетевой связи для получения единой группы Link Aggregation Group. MAC-клиент работает с группой так, как будто она представляет собой одну линию связи.

Функция Port Trunking в коммутаторах Moxa позволяет устройствам обмениваться данными в группах, максимальное количество групп – до 4, а максимальное количество портов в каждой группе – 8. Если одна из 8 линий связи в группе выйдет из строя, остальные 7 линий продолжат передавать данные, разделив между собой пропускную способность канала.

Функция Port trunking может быть использована для объединения коммутаторов Moxa до 8 линиями связи. Если все порты на этих двух коммутаторах работают в полнодуплексном режиме 100BaseTX, потенциальная пропускная способность соединения может составить 1600 Мбит/с.

Концепция Port Trunking

Протокол Port Trunking предоставляет следующие преимущества:

- Большую гибкость коммуникаций за счет возможности увеличить пропускную способность сети в 2 раза, в 3 раза, в 4 раза и даже до 8 раз.
- Резервирование – если одна из линий связи оборвана, трафик будет проходить через остальные линии данной группы.
- Разделение нагрузки – обмен данными с одним MAC-клиентом может осуществляться по нескольким линиям связи

Для предотвращения появления широковещательного шторма или петель в сети перед настройкой функции Port Trunking отключите все соединения по портам, которые Вы хотите добавить к транку или удалить из него. Подключите все необходимые соединения только после завершения процедуры настройки.

Если все порты на двух объединяемых коммутаторах сконфигурированы как 100BaseTX и передают данные в режиме полный дуплекс, то потенциальная пропускная способность соединения составит 1.6 Гбит/с. Это значит, что пользователь сможет до 8 раз увеличить пропускную способность сети с помощью функции Port Trunking между двумя коммутаторами Moxa.

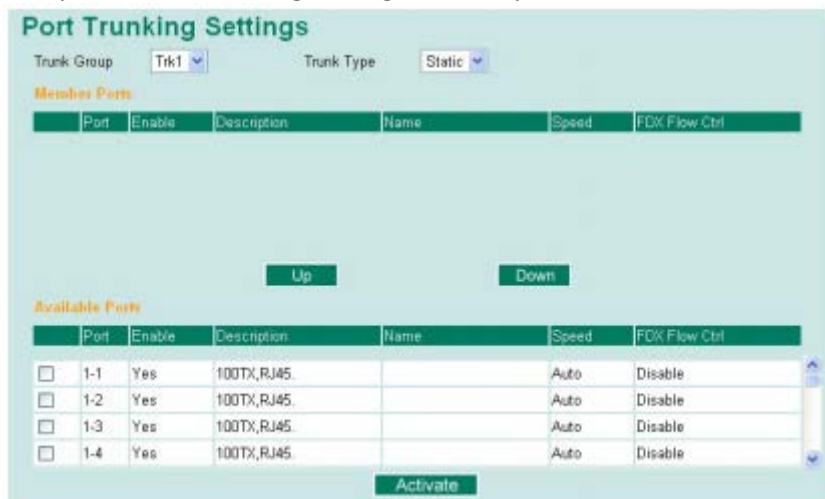
Каждый коммутатор Moxa может иметь максимум 4 транк-группы. Когда Вы активируете функцию Port Trunking, следующие настройки портов будут сброшены на заводские значения по умолчанию или отключены:

- Настройки резервирования связи будут сброшены
- Настройки 802.1Q VLAN будут сброшены
- Настройки Multicast-фильтрации будут сброшены
- Настройки блокировки портов будут сброшены и выключены
- Настройки назначения IP-адреса устройства будут сброшены
- Настройки зеркалирования портов будут сброшены

После активации функции Port Trunking Вы сможете снова настроить данные параметры для каждого транк-порта.

Port Trunking Settings (Настройка функции Port Trunking)

Настройки Port Trunking Settings используются для назначения портов в транк-группы.



Шаг 1: Выберите нужную транк-группу.

Шаг 2: Выберите тип транка: Static (статический) или LACP

Шаг 3: Выберите нужные порты из списка Available Ports (доступные порты) и нажмите **Up** для добавления в группу.

Шаг 4: Выберите нужные порты из списка Member Ports (входящие в группу порты) и нажмите **Down** для удаления из группы.

Trunk Group (Транк-группа) – максимум до 4 групп

Параметр	Описание	Значение по умолчанию
Trk1, Trk2, Trk3, Trk4 (зависит от возможностей микросхемы коммутатора, некоторые порты поддерживают только до 3 групп)	Определяет текущую транк-группу.	Trk1

Серия EDS-400A не поддерживает функцию Port Trunking. Количество транк-групп для других серий указаны ниже:

Параметр	Описание
2	EDS-505A, EDS-P506A-4PoE, EDS-516A
3	EDS-518A
4	Остальные модели

Trunk Type (Тип транка)

Параметр	Описание	Значение по умолчанию
Static (статический)	Запатентованный протокол транка, реализованный компанией Moxa	Static
LACP	Протокол LACP (IEEE 802.3ad, Link Aggregation Control Protocol).	

Available Ports/Member Ports (Доступные порты/порты транка)

Параметр	Описание	Значение по умолчанию
Member/Available Ports	Список портов в данной группе и портов,	нет

(порты транка/ доступные порты)	доступных для добавления.	
Check box (выбор порта)	Выбор порта для добавления или перемещения.	Unchecked (не выбран)
Port (Порт)	Номер порта.	нет
Port Description (Описание Порта)	Отображение типа среды передачи порта.	нет
Name (Имя порта)	Отображение имени порта.	нет
Speed (Скорость)	Отображает скорость передачи данных порта (1G-Full, 100M-Full, 100M-Half, 10M-Full или 10M-Half).	нет
FDX Flow Control (Управление Потоками FDX)	Отображает, включено ли управление потоками FDX.	нет
Up (Вверх)	Добавить выбранные доступные порты в список портов транка.	нет
Down (Вниз)	Удалить текущие порты транка и переместить их в список доступных портов.	нет

Trunk Group	Member Port	Status
Trk1 (Static)	1-1	Success
	1-2	Success
	1-3	Success

Trunk Table (Таблица транков)

Параметр	Описание
Trunk Group (Транк-группа)	Показывает транк-группу и ее тип.
Member Port (Порт транка)	Показывает, какой порт принадлежит транк-группе.
Status (Состояние)	Success (Успешно) – означает, что транк успешно функционирует. Fail (Ошибка) – оповещает о том, что в работе транка возникли ошибки

Настройка протокола SNMP

Коммутаторы Moxa поддерживают три версии протокола SNMP – SNMP V1, SNMP V2c, SNMP3. В протоколах SNMP V1 и SNMP V2 авторизация пользователей выполняется посредством «идентификатора сообщества» (community string), это значит, что доступ к операциям чтения и записи осуществляется через «идентификатор сообщества» *public* и *private* (по умолчанию). В SNMP3 используются алгоритмы аутентификации MD5 и SHA, что делает его самым надежным протоколом. Для усиления безопасности Вы также можете активировать шифрование данных.

Режимы и уровни безопасности SNMP, поддерживаемые коммутатором Moxa, приведены в таблице ниже. Выберите режим и уровень безопасности, который будет использоваться в коммуникациях между SNMP-агентом и диспетчером.

Версия протокола	Режим безопасности	Аутентификация	Шифрование данных	Метод
SNMP V1, V2c	V1, V2c Read Community (сообщество, имеющее доступ к чтению)	«идентификатор сообщества»	Нет	Выберите «идентификатор сообщества» для аутентификации.
	V1, V2c Read/Write Community (сообщество, имеющее доступ к чтению/записи)	«идентификатор сообщества»	Нет	Выберите «идентификатор сообщества» для аутентификации.
SNMP V3	No-Auth	Нет	Нет	Используйте аккаунт admin или user для доступа к объектам.
	MD5 или SHA	Аутентификация, основанная на MD5 или SHA	Нет	Обеспечивает аутентификацию на базе алгоритмов HMAC-MD5 или HMAC-SHA. Для аутентификации необходимо введение пароля, состоящего минимум из 8 символов.
	MD5 или SHA	Аутентификация, основанная на MD5 или SHA	Ключ шифрования данных	Обеспечивает аутентификацию на базе алгоритмов HMAC-MD5 или HMAC-SHA и ключ шифрования данных. Для аутентификации и шифрования необходимо введение пароля, состоящего минимум из 8 символов, и ключ шифрования данных.

Данные параметры настраиваются в окне настройки SNMP. Подробная расшифровка параметров окна настройки SNMP приведена ниже.

The screenshot shows the 'SNMP' configuration page. It is divided into several sections:

- SNMP Read/Write Settings:** Includes fields for 'SNMP Versions' (set to 'V1, V2c'), 'V1,V2c Read Community' (set to 'public'), 'V1,V2c Write/Read Community' (set to 'private'), 'Admin Auth. Type' (set to 'No-Auth'), 'Admin Data Encryption Key' (checkbox), 'User Auth. Type' (set to 'No-Auth'), and 'User Data Encryption Key' (checkbox).
- Trap Settings:** Includes fields for '1st Trap Server IP/Name', '1st Trap Community' (set to 'public'), '2nd Trap Server IP/Name', and '2nd Trap Community' (set to 'public').
- Trap Mode:** Includes a 'Trap' dropdown menu, 'Retries (1-99)' (set to 1), and 'Timeout (1-300s)' (set to 1).
- Private MIB information:** Shows 'Switch Object ID' as 'enterprise 8691.7.17' and an 'Activate' button.

SNMP Read/Write Settings (Настройка чтения/Записи SNMP)

SNMP Versions (Версия SNMP)

Параметр	Описание	Значение по умолчанию
V1, V2c, V3 или V1, V2c или только V3	Версия протокола SNMP, используемая для управления коммутатором.	V1, V2c

V1, V2c Read Community (Сообщество, имеющее доступ к чтению)

Параметр	Описание	Значение по умолчанию
Макс. 30 символов	Выберите «идентификатор сообщества» для аутентификации. Это означает, что при введении идентификатора public, SNMP-агент получит доступ ко всем объектам на уровне чтения.	Public

V1, V2c Read/Write Community (Сообщество, имеющее доступ к чтению/записи)

Параметр	Описание	Значение по умолчанию
Макс. 30 символов	Выберите «идентификатор сообщества» для аутентификации. Это означает, что при введении идентификатора private, SNMP-агент получит доступ ко всем объектам на уровне чтения и записи.	Private

Для SNMP V3 существует два уровня доступа, соответствующие различным учетным записям пользователей. **Admin** имеет доступ на уровне чтения и записи MIB-файла. **User** может только просматривать данные.

Admin Auth. Type (тип аутентификации пользователя Admin) – для SNMP V1, V2c, V3 и только V3

Параметр	Описание	Значение по умолчанию
No-Auth	Используйте аккаунт admin для доступа к объектам без аутентификации.	Нет
MD5-Auth	Обеспечивает аутентификацию на базе алгоритма HMAC-MD5. Для аутентификации необходимо введение пароля, состоящего минимум из 8 символов.	Нет
SHA-Auth	Обеспечивает аутентификацию на базе алгоритма HMAC-SHA. Для аутентификации необходимо введение пароля, состоящего минимум из 8 символов.	Нет

Admin Data Encryption Key (ключ шифрования данных пользователя Admin) – для SNMP V1, V2c, V3 и только V3

Параметр	Описание	Значение по умолчанию
Enable (Включен)	Необходим ключ шифрования данных (минимум 8 и максимум 30 символов)	Нет
Disable (Отключен)	Нет шифрования данных	Нет

User Auth. Type (тип аутентификации пользователя) – для SNMP V1, V2c, V3 и только V3

Параметр	Описание	Значение по умолчанию
No-Auth	Используйте аккаунт admin для доступа к объектам без аутентификации.	Нет
MD5-Auth	Обеспечивает аутентификацию на базе алгоритма HMAC-MD5. Для аутентификации необходимо введение пароля, состоящего минимум из 8 символов.	Нет
SHA-Auth	Обеспечивает аутентификацию на базе алгоритма HMAC-SHA. Для аутентификации необходимо введение пароля, состоящего минимум из 8 символов.	Нет

User Data Encryption Key (ключ шифрования данных пользователя) – для SNMP V1, V2c, V3 и только V3

Параметр	Описание	Значение по умолчанию
Enable (Включен)	Необходим ключ шифрования данных (минимум 8 и максимум 30 символов)	Нет
Disable (Отключен)	Нет шифрования данных	Нет

Trap Settings (Наст. ройка SNMP Trap)

Функция SNMP Trap позволяет SNMP-агенту отправлять NMS-сообщения о важных событиях. Коммутатор поддерживает два режима SNMP: режим **Trap** и режим **Inform**.


Режим SNMP Trap - TRAP

В режиме **Trap** SNMP-агент отправляет сообщения SNMPv1 trap в систему управления сетью (NMS). От системы не приходит никакого подтверждения получения сообщения, поэтому SNMP-агент не может узнать, достигло ли сообщение адресата.



Режим SNMP Trap - INFORM

Протокол SNMPv2 поддерживает механизм Inform. Когда сообщение Inform отправляется SNMP-агентом в систему управления сетью (NMS), адресат отправляет ответное сообщение (подтверждение о получении), подобно любой системе надежной отправки и получения запросов. Если SNMP-агент не получает ответа от системы управления сетью (NMS) в определенный период времени, SNMP-агент повторно отправит сообщение inform в систему управления сетью (NMS). Максимальное время ожидания составляет 300 секунд (по умолчанию – 1 с), а максимальное число повторных попыток – 99 раз (по умолчанию – 1 раз). Если SNMP-агент получил ответ от системы управления сетью (NMS), он прекратит посылать информационные сообщения.



1-st Trap Server IP/Name (IP-адрес/имя первого Trap-сервера)

Параметр	Описание	Значение по умолчанию
IP-адрес или имя	Введите IP-адрес или имя первого Trap-сервера, используемого Вашей сетью.	Нет

1-st Trap Community (Первое Trap-сообщество)

Параметр	Описание	Значение по умолчанию
Макс.30 символов	Введите «идентификатор сообщества» для аутентификации.	Public

2-nd Trap Server IP/Name (IP-адрес/имя второго Trap-сервера)

Параметр	Описание	Значение по умолчанию
IP-адрес или имя	Введите IP-адрес или имя второго Trap-сервера, используемого Вашей сетью.	Нет

2-nd Trap Community (Второе Trap-сообщество)

Параметр	Описание	Значение по умолчанию
Макс.30 символов	Введите «идентификатор сообщества» для аутентификации.	Public

Private MIB information (Информация о частной MIB)

Switch Object ID (Object ID коммутатора)

Параметр	Описание	Значение по умолчанию
Уникальный ID коммутатора Moxa	Указывает заводское значение ID коммутатора.	Зависит от модели коммутатора

Примечание: Object ID коммутатора не может быть изменен.

Использование технологии питания PoE (только для моделей с PoE)

Технология питания по сетям Ethernet (Power over Ethernet) становится все более популярной благодаря высокой степени надежности Ethernet-коммутаторов с такой технологией, предоставляющих необходимую мощность для запитываемых устройств (PD) в тех случаях, когда нет возможности установки блока питания или он не может обеспечить необходимый уровень мощности.

Получать питание по технологии PoE могут следующие основные типы устройств:

- Камеры видеонаблюдения
- Датчики ввода/вывода для систем безопасности
- Промышленные беспроводные точки доступа
- IP-телефоны

На самом деле, интеграция в единую сеть передачи данных – не редкость для видео-, голосовых и прочих данных, требующих высокой скорости передачи в промышленных условиях. Коммутаторы Moxa с PoE оснащены большим количеством дополнительных функций управления выдачей питания, что особенно ценно для критически важных Ethernet-сетей, включая сети систем безопасности. Кроме того, коммутаторы PoE Moxa поддерживают стандарт высокой мощности PoE+, возможность питания от 24 В постоянного тока и функции резервированных сетей Turbo Ring и Turbo Chain со временем восстановления до 20 мс.

В зависимости от модели коммутатора доступны два типа функций PoE:

Параметр	Поддерживаемые модели
Тип 1	EDS-P510, EDS-P506A-4PoE, IKS-6726-8PoE
Тип 2	EDS-P510A-8PoE, IKS-6728-8PoE-4GTXSFP

Тип 1

PoE Setting (Настройка PoE)

Настройки позволяют пользователю задать мощность питания по PoE, ограничить доступ к PoE-порту, ограничить мощность PoE-порта и проверять запитываемые устройства на неисправности.

Описание каждой настройки представлено ниже:



PoE Power Budget (Настройка мощности питания по PoE)

Указывает мощность питания по PoE, которая может быть представлена системой

Параметр	Описание	Значение по умолчанию
Auto (авто)	Позволяет пользователям устанавливать ограничение мощности каждого PoE-порта.	Auto
Manual (ручная)	Позволяет пользователям устанавливать предельное значение мощности, потребляемой системой.	

Port Setting (Настройка порта)

Enable (Включить)

Параметр	Описание	Значение по умолчанию
Выбран	Разрешает передачу данных и питание через порт	Выбран
Не выбран	Немедленно запрещает доступ к портам	

Power Limit (Предел мощности)

Параметр	Описание	Значение по умолчанию
Auto (авто)	Мощность, автоматически выделяемая в соответствии с классом запрашиваемого устройства.	Auto
Manual (ручная)	Позволяет пользователям устанавливать предельное значение мощности, выдаваемой портом.	

Ethernet-коммутатор PoE может контролировать состояние работы запрашиваемых устройств с использованием протокола IP. Если запрашиваемое устройство выходит из строя, коммутатор не получит от него ответ на ping-запрос, и по истечении определенного периода времени процесс аутентификации будет перезапущен. Это удобный способ обеспечения надежности сети и снижения расходов на управление.

PD Failure Check (Проверка запрашиваемых устройств на неисправности)

Параметр	Описание	Значение по умолчанию
Включен	Включает функцию проверки запрашиваемых устройств на неисправности.	Отключен
Отключен	Выключает функцию проверки запрашиваемых устройств на неисправности.	

IP (IP-адрес запрашиваемого устройства)

Параметр	Описание	Значение по умолчанию
Макс.15 символов	Установка IP-адреса запрашиваемого устройства.	Нет

Period (Частота проверки запрашиваемых устройств)

Параметр	Описание	Значение по умолчанию
Макс.5 символов	Установка частоты проверки запрашиваемых устройств.	Нет

PoE Timetabling (Таблица времени работы питания по PoE)

Обычно запрашиваемые устройства не нуждаются в питании 24 часа в сутки, 7 дней в неделю. Поэтому Ethernet-коммутаторы с PoE обладают функцией настройки времени работы для того, чтобы настраивать расписание работы каждого PoE-порта для уменьшения нагрузки на систему.



Port (Порт)

Параметр	Описание	Значение по умолчанию
Порт	Включение заранее определенного порта.	Port 1 (порт 1)

Enable

Параметр	Описание	Значение по умолчанию
Включен	Включает порт на определенный период времени.	Отключен
Отключен	Отключает порт на определенный период времени.	

Таблица времени работы в течение недели

Day (День)

Параметр	Описание	Значение по умолчанию
Включен	Включает порт в определенные дни недели.	Отключен
Отключен	Отключает порт в определенные дни недели.	

Start/End Time (Время старта/окончания работы)

Параметр	Описание	Значение по умолчанию
Время работы	Позволяет пользователю настроить время старта и окончания работы для запрашиваемых устройств.	0-24

PoE Status (Состояние PoE-портов)

PoE Status				
Port	Status	Consumption(W)	Voltage(V)	Current(mA)
1	Enable	0	0	0
2	Enable	0	0	0
3	Enable	0	0	0
4	Enable	0	0	0

Параметр	Описание
Enable/Disable Включен/выключен	Состояние PoE-порта
Consumption (W) Потребление (Вт)	Фактическая потребляемая мощность PoE-порта
Voltage (V) Напряжение (В)	Фактическое выдаваемое напряжение PoE-порта
Current (mA) Потребление тока (мА)	Фактический потребляемый ток PoE-порта

PoE Email Warning Events Settings (Настройки оповещения по Email о событиях PoE)

Так как промышленные Ethernet-сети часто территориально распределены, а боенты сети не всегда знают, что происходит в других концах сети. Это значит, что PoE-порты подключенные к запитываемым устройствам, должны оповещать администраторов сети о событиях в режиме реального времени. Даже когда инженеры центра управления находятся вне диспетчерской в течение длительного периода времени, они все равно могут быть проинформированы о возникновении события, связанного с запитываемыми устройствами. Ethernet-коммутаторы с PoE поддерживают два способа оповещения о событии: по Email и с помощью релейного выхода. Также отправлять оповещения по Email или управлять состоянием реле можно по факту изменения состояния датчиков, подключенных к цифровым входам коммутатора.

Тип Email-оповещений можно разделить на две группы: сбой питания и обрыв связи с запитываемым устройством.

PoE Email Warning Events Settings		
Port Events		
Port	Power Fail	PD-Failure
1	<input type="checkbox"/>	<input type="checkbox"/>
2	<input type="checkbox"/>	<input type="checkbox"/>
3	<input type="checkbox"/>	<input type="checkbox"/>
4	<input type="checkbox"/>	<input type="checkbox"/>

Событие	Email с оповещением будет отправлен, когда...
Сбой питания	...фактическая потребляемая мощность запитываемого устройства превышает установленный предел мощности.
Обрыв связи с запитываемым устройством	...коммутатор не получает ответ от запитываемого устройства в течение определенного периода времени.

PoE Relay Warning Events Settings (Настройки оповещения о событиях PoE с помощью реле)

Тип оповещений можно разделить на две группы: сбой питания и обрыв связи с запрашиваемым устройством.



Событие	Оповещение через реле сработает, когда...
Сбой питания	...фактическая потребляемая мощность запрашиваемого устройства превышает установленный предел мощности
Обрыв связи с запрашиваемым устройством	...коммутатор не получает ответ от запрашиваемого устройства в течение определенного периода времени.

Тип 2

PoE Setting (Настройки PoE)

Настройки позволяют пользователю управлять выходной мощностью PoE, ограничить мощность питания по PoE, произвести конфигурирование PoE-порта и проверять запрашиваемые устройства на неисправности.

Далее – описание каждого элемента настроек:



PoE System Configuration (Системные настройки PoE)

PoE power output (Выход питания PoE)

Параметр	Описание	Значение по умолчанию
Включен	Включает подачу питания на запрашиваемое устройство	Включен
Отключен	Выключает подачу питания на запрашиваемое устройство	

PoE power threshold (Порог мощности питания по PoE)

Параметр	Описание	Значение по умолчанию
30...240	Установка порога максимальной суммарной выходной мощности PoE	240

PoE threshold cutoff (Порог выключения PoE)

Параметр	Описание	Значение по умолчанию
Включен	Отключает питание запрашиваемого устройства в момент наступления заданного порога.	Отключен
Отключен	Не отключает питание запрашиваемого устройства в момент наступления заданного порога.	

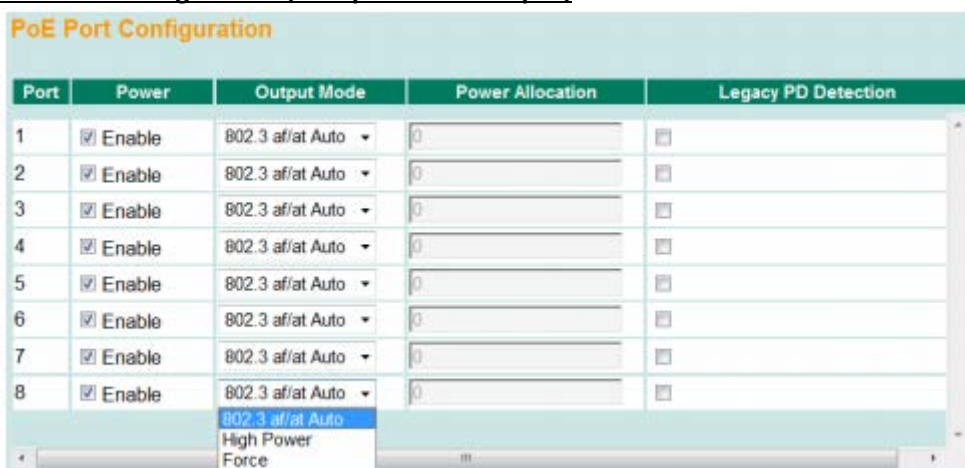
Sum of allocated power (Сумма распределенной мощности)

Параметр	Описание
Распределенная мощность	Данный параметр отражает общую сумму мощности, распределенной на все запрашиваемые устройства.

Sum of measured power (Сумма измеренной мощности)

Параметр	Описание
Измеренная мощность	Данный параметр отражает общую сумму измеряемой мощности запрашиваемых устройств.

PoE Port Configuration (Настройка PoE-порта)



Power (Питание)

Параметр	Описание	Значение по умолчанию
Включен	Позволяет осуществлять передачу данных и питания через порт	Включен
Отключен	Немедленно отключает доступ к порту	

Output Mode (Режим вывода)

Параметр	Описание	Значение по умолчанию
802.3 af/at Auto	Подача питания по протоколам IEEE 802.3 af/at. Допустимый диапазон сопротивления для запрашиваемых устройств – от 17 кОм до 29 кОм	802.3 af/at Auto
High Power	Режим «High Power» обеспечивает максимальную мощность питания устройств. Допустимый диапазон сопротивления для запрашиваемых устройств – от 17 кОм до 29 кОм, а значение распределения мощности на порт автоматически устанавливается 36 Вт.	
Force	Режим «Force» обеспечивает подачу питания к устройствам, не поддерживающим протоколы IEEE 802.3 af/at. Допустимый диапазон сопротивления для запрашиваемых устройств – от 2.4 кОм, а диапазон распределения мощности – от 0 до 36 Вт.	

Power Allocation (распределяемая мощность питания)

Параметр	Описание	Значение по умолчанию
0...36	В режиме питания Force максимальная распределяемая мощность может достигать 36 Вт	36

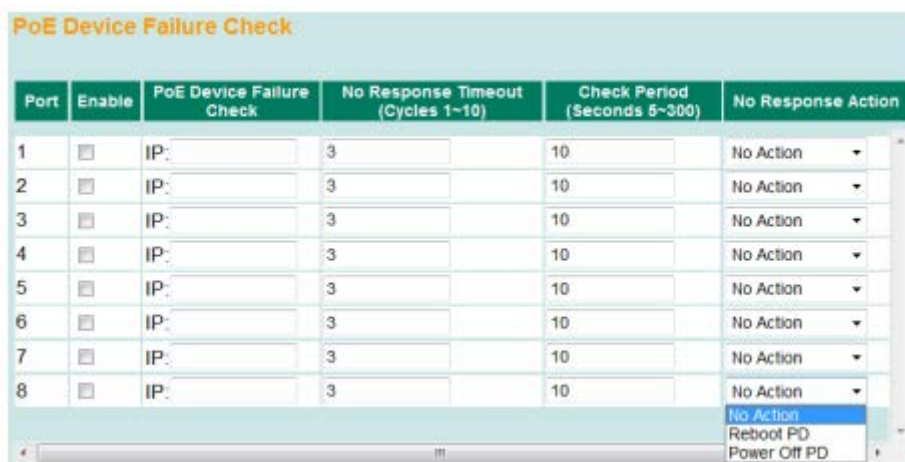
Legacy PD Detection (Обнаружение устаревших запрашиваемых устройств)

Ethernet-коммутаторы с PoE обладают функцией **Legacy PD Detection**. Когда электрическая емкость запрашиваемого устройства выше 2.7 мкФ, проверка системы с помощью функции **Legacy PD Detection** разрешает подачу питания на устройство. Если включить данную функцию, проверка запрашиваемого устройства займет от 10 до 15 секунд до момента подачи питания.

Параметр	Описание	Значение по умолчанию
Включен	Функция Legacy PD Detection включена.	Отключен
Отключен	Функция Legacy PD Detection выключена.	

PoE Device Failure Check (Проверка устройств на неисправности по PoE-сети)

Ethernet-коммутатор PoE может контролировать состояние работы запрашиваемых устройств с использованием протокола IP. Если запрашиваемое устройство выходит из строя, коммутатор не получит от него ответ на ping-запрос, и по истечении определенного периода времени процесс аутентификации будет перезапущен. Это удобный способ обеспечения надежности сети и снижения расходов на управление.



Enable (Включение)

Параметр	Описание	Значение по умолчанию
Включен	Функция проверки устройств на неисправности включена.	Включен
Отключен	Функция проверки устройств на неисправности выключена.	

PoE Device IP Address (IP-адрес запрашиваемых устройств)

Параметр	Описание	Значение по умолчанию
Макс.15 символов	Ввод IP-адреса запрашиваемых устройств	Нет

No Response Timeout (Количество циклов при ожидании ответа)

Параметр	Описание	Значение по умолчанию
1...10	Циклы проверки доступности удаленного IP-адреса.	3

Check Period (период проверки)

Параметр	Описание	Значение по умолчанию
5...300	Период проверки удаленного IP-адреса.	10

No Response Action (Действие при отсутствии ответа от устройства)

Параметр	Описание	Значение по умолчанию
No Action	Бездействие.	No Action
Reboot PD	Перезагрузка запрашиваемого устройства с помощью выключения/включения питания PoE.	
Power Off PD	Выключение запрашиваемого устройства с помощью выключения/включения питания PoE.	

PoE Timetabling (Режим работы PoE)

Обычно у запрашиваемых устройств нет необходимости работать 24 в сутки, 7 дней в неделю. Ethernet-коммутаторы с PoE позволяют пользователям настраивать режимы работы каждого PoE-порта для оптимизации затрат на питание системы.



Порт

Параметр	Описание	Значение по умолчанию
Порт	Включение заранее определенного порта.	Port 1 (порт 1)

Enable

Параметр	Описание	Значение по умолчанию
Включен	Включает порт на определенный период времени.	Отключен
Отключен	Отключает порт на определенный период времени.	

Таблица времени работы в течение недели

Day (День)

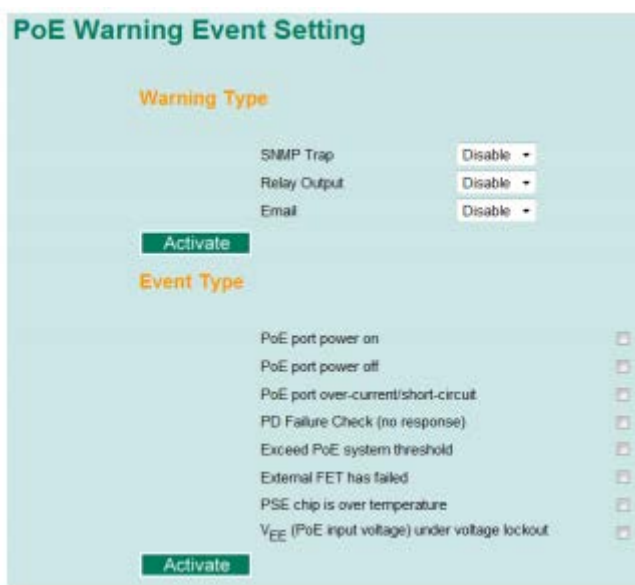
Параметр	Описание	Значение по умолчанию
Включен	Включает порт в определенные дни недели.	Отключен
Отключен	Отключает порт в определенные дни недели.	

Start/End Time (Время старта/окончания работы)

Параметр	Описание	Значение по умолчанию
Время работы	Позволяет пользователю настроить время старта и окончания работы для запрашиваемых устройств.	0-24

PoE Warning Event Setting (Настройки оповещения о событиях)

Так как промышленные Ethernet-сети часто территориально распределены, а боенты сети не всегда знают, что происходит в других концах сети. Это значит, что PoE-порты подключенные к запрашиваемым устройствам, должны оповещать администраторов сети о событиях в режиме реального времени. Даже когда инженеры центра управления находятся вне диспетчерской в течение длительного периода времени, они все равно могут быть проинформированы о возникновении события, связанного с запрашиваемыми устройствами. Ethernet-коммутаторы с PoE поддерживают несколько способов оповещения о событии: SNMP trap, Email и с помощью релейного выхода. Также отправлять оповещения по Email или управлять состоянием реле можно по факту изменения состояния датчиков, подключенных к цифровым входам коммутатора.



Warning Type (Способы оповещения о событии)

SNMP Trap

Параметр	Описание	Значение по умолчанию
Enable	Включает функцию SNMP Trap для оповещения о событиях.	Disable (отключен)
Disable	Выключает функцию SNMP Trap для оповещения о событиях.	

Relay Output (Релейный выход)

Параметр	Описание	Значение по умолчанию
Enable	Включает оповещение о событиях с помощью релейного выхода.	Disable (отключен)
Disable	Выключает оповещение о событиях с помощью релейного выхода.	

Email

Параметр	Описание	Значение по умолчанию
Enable	Включает оповещение о событиях по Email.	Disable (отключен)
Disable	Выключает оповещение о событиях по Email.	

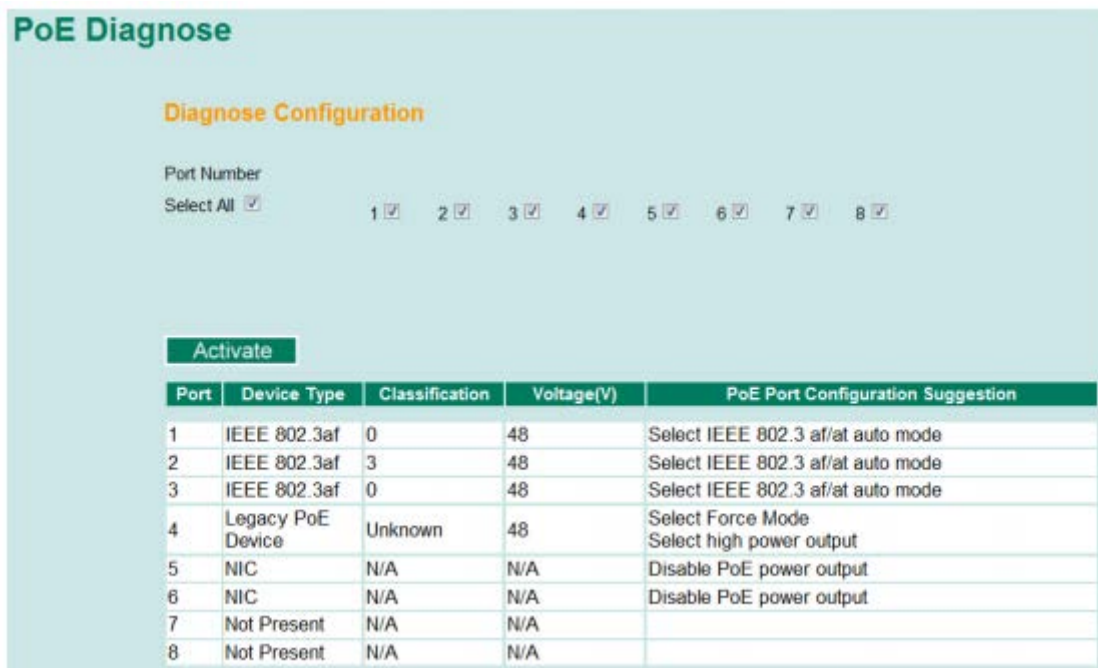
Event Type (События)

Событие	Описание
PoE port power on <i>Подача питания по PoE-порту включена</i>	Подача питания на запрашиваемое устройство.
PoE port power off <i>Подача питания по PoE-порту выключена</i>	Подача питания выключена.
PoE port over-current/short-circuit <i>Защита PoE-порта от перегрузки/короткого замыкания</i>	Ограничения по нагрузке порта: Стандарт 802.3 af – 350 мА Стандарт 802.3 at – 600 мА High Power – 720 мА Force – 600 мА
PD Failure Check (no response) When <i>Проверка запрашиваемых устройств на неисправности (отсутствие ответа на ping)</i>	Когда коммутатор не получает ответа от запрашиваемого устройств в течение определенного периода времени.
Exceed PoE system threshold <i>Превышение порога PoE-системы</i>	Когда сумма потребления питания всех запрашиваемых устройств превышает порог общей выходной мощности PoE.
External FET has failed <i>Ошибка работы полевого транзистора</i>	Когда полевой МОП-транзистор порта вышел из строя, свяжитесь с технической поддержкой Moxa.
PSE chip is over temperature <i>Повышенная температура чипа источника PoE-питания</i>	Проверьте температуру окружающей среды. Если она выше 75°C, переустановите коммутатор в соответствующей среде. Если температура ниже 75°C, свяжитесь с технической поддержкой Moxa.
VEE (PoE input voltage) under voltage lockout <i>Блокировка питания при пониженном напряжении питания коммутатора</i>	Если напряжение питания коммутатора падает ниже 44 В постоянного тока, отрегулируйте напряжение в промежутке между 46 и 57 В постоянного тока, чтобы устранить эту проблему.

Примечание:

Релейный выход не поддерживает три типа событий: **External FET has failed**, **PSE chip is over temperature** и **VEE (PoE input voltage) under voltage lockout**.

PoE Diagnose (Диагностика PoE)



Функция **PoE Diagnose** позволяет пользователям наблюдать за состоянием запрашиваемых устройств и предлагает варианты конфигурации для того, чтобы выбрать оптимальные настройки для запрашиваемых устройств.

Для диагностики запрашиваемых устройств необходимо выполнить следующие шаги:

Шаг 1: Введите номера портов, которые необходимо протестировать.

Шаг 2: Нажмите **Activate (Активировать)**.

Шаг 3: Система покажет состояние выбранных запрашиваемых устройств.

Настройка функции диагностики

Port Number (Номер порта)

Параметр	Описание	Значение по умолчанию
Включен	Добавить порт для диагностики.	Отключен
Отключен	Удалить порт из списка диагностируемых.	

Device Type (Тип устройства)

Параметр	Описание
Not Present <i>Нет соединения</i>	Нет соединения с портом коммутатора.
NIC <i>Сетевая плата компьютера</i>	Сетевая плата компьютера подключена к порту коммутатора.
IEEE 802.3 af	Запрашиваемое устройство IEEE 802.3 af подключено к порту коммутатора.
IEEE 802.3 at	Запрашиваемое устройство IEEE 802.3 at подключено к порту коммутатора.
Legacy PoE Device <i>Устаревшее устройство PoE</i>	Устаревшее запрашиваемое устройство подключено к порту коммутатора, напряжение которого слишком высоко/низко, или емкость которого слишком высока.
Unknown <i>Неизвестное устройство</i>	Неизвестное запрашиваемое устройство подключено к порту коммутатора.

Classification (Классификация)

Параметр	Описание
N/A	Нет классификации порта.
0...4	Класс от 0 до 4.
Unknown <i>Неизвестный класс</i>	Неизвестный класс порта, выше, чем класс 4.

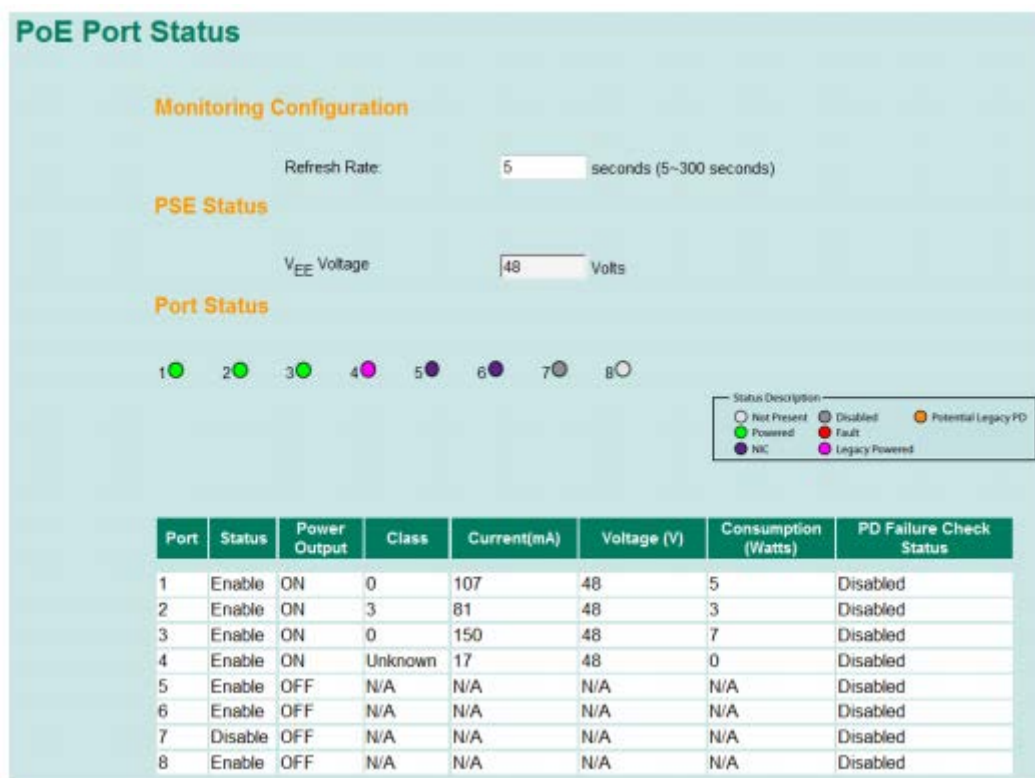
Voltage (V) – Напряжение (В)

Параметр	Описание
N/A	Нет выходного напряжение порта.
Voltage <i>Напряжение</i>	Напряжение порта.

PoE Port Configuration Suggestion (Рекомендации по настройке PoE-порта)

Параметр	Описание
Disable PoE power output <i>Отключить питание PoE</i>	При обнаружении сетевой платы компьютера или неизвестного запрашиваемого устройства, система предложит отключить подачу питания по PoE.
Enable "Legacy PD Detection" <i>Включить функцию Legacy PD Detection</i>	При обнаружении запрашиваемого устройства с более высокой емкостью, система предложит включить функцию Legacy PD Detection.
Select Force Mode <i>Включить режим Force</i>	При обнаружении запрашиваемого устройства с более высоким/низким сопротивлением или более высокой емкостью, система предложит включить режим Force.
Select IEEE 802.3 af/at auto mode <i>Включить режим 802.3 af/at Auto</i>	При обнаружении запрашиваемого устройства со стандартом IEEE 802.3 af/at, система предлагает выбрать режим 802.3 af/at Auto.
Select high power output <i>Включить высокую выходную мощность</i>	При обнаружении устройства неизвестной классификации, система предлагает выбрать высокую выходную мощность.
Raise external power supply voltage > 46VDC <i>Установить источник питания с напряжением более 46 В пост.тока</i>	При обнаружении внешнего источника питания с напряжением ниже 46 В, система предлагает повысить напряжения.
Enable PoE function for detection <i>Включить функцию PoE</i>	Система предлагает включить функцию PoE.

PoE Port Status (Состояние PoE-порта)



Настройка мониторинга

Refresh Rate (Частота обновления)

Параметр	Описание	Значение по умолчанию
5...300	Частота обновления состояния PoE-порта.	5

PSE Status (Состояние модуля питания)

VEE Voltage (Напряжение питания)

Параметр	Описание	Значение по умолчанию
Read-only (Только чтение)	Отображение выдаваемого коммутатором напряжения.	Нет

PoE Port Status (Состояние PoE-порта)

Описание состояния

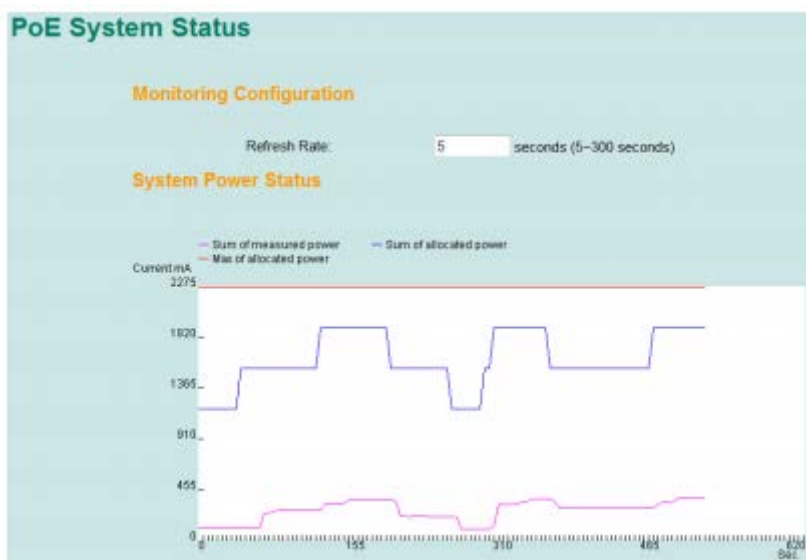
Параметр	Описание
Not Present <i>Нет соединения</i>	Нет соединения с портом коммутатора. Нет выходной мощности PoE.
Powered <i>Система питается</i>	Выдаётся питание PoE.
NIC <i>Сетевая плата компьютера</i>	Система обнаружила сетевую плату компьютера, подключенную к порту коммутатора. Нет выходной мощности PoE.
Disabled <i>Функция PoE отключена</i>	Функция PoE на порту отключена. Нет выходной мощности PoE.
Fault	В режиме Force система определила параметры запрашиваемого

<i>Ошибка</i>	устройства вне допустимого диапазона.
Legacy Powered <i>Устаревшее запитываемое устройство</i>	В режиме Force система определила устаревшее запитываемое устройство.
Potential Legacy PD <i>Потенциально устаревшее запитываемое устройство</i>	В режиме 802.3 af/at или High Power система определила потенциально устаревшее запитываемое устройство. Нет выходной мощности PoE.

Port Description (Описание порта)

Параметр	Описание
Status <i>Состояние</i>	Функция PoE включена.
Power Output <i>Выходная мощность</i>	Выходная мощность каждого PoE-порта.
Class <i>Класс</i>	Класс устройств, подключенных к каждому PoE-порту.
Current (mA) <i>Потребление тока (mA)</i>	Фактическое значение тока, потребляемого каждым PoE-портом.
Voltage (V) <i>Напряжение (V)</i>	Фактическое значение напряжения, потребляемого каждым PoE-портом.
Consumption (Watts) <i>Потребляемая мощность (Вт)</i>	Фактическое значение мощности, потребляемой каждым PoE-портом.
PD Failure Check Status <i>Состояние проверки запитываемых устройств на неисправности</i>	Состояние проверки запитываемых устройств, подключенных к каждому PoE-порту, на неисправности. Alive: Запитываемое устройство регулярно отвечает на ping-запросы. Not Alive: Запитываемое устройство не отвечает на ping-запросы. Disable: Проверка запитываемых устройств на неисправности не активирована.

PoE System Status (Состояние PoE-системы)



Monitoring Configuration (Настройка мониторинга)

Параметр	Описание	Значение по умолчанию
5...300	Частота обновления состояния PoE-системы.	5

System Power Status (Состояние системы питания)

Состояние системы питания отражает график со следующими параметрами: **Sum of measured power** (Сумма измеренных мощностей), **Sum of allocated power** (Сумма выделяемых мощностей) и **Max of allocated power** (Максимальная выделяемая мощность).

Sum of measured power (Сумма измеренных мощностей) на графике отражена розовым цветом.

Sum of allocated power (Сумма выделяемых мощностей) на графике отражена синим цветом.

Max of allocated power (Максимальная выделяемая мощность) на графике отражена красным цветом.

График отражает эти параметры на осях **Current (mA)** – Ток (мА) и **Sec. (second)** - Секунда, он обновляется с частотой обновления состояния портов.

Назначение приоритетов трафика

Функция назначения приоритета сетевым пакетам позволяет обеспечить высокое качество сервиса (Quality of Service, QoS) сети и повысить надежность доставки данных. Пользователь может назначать приоритет пакетам таким образом, чтобы наиболее важные данные доставлялись с наименьшей задержкой. Функция Quality of Service (QoS) задает ряд правил для контроля трафика. Правила определяют тип трафика и то, как коммутатор должен реагировать на прохождение через него трафика определенного типа. Коммутатор MOXA распознает как теги IEEE 802.1p/1Q CoS 2-го уровня, так и ToS теги 3-го уровня. Функция QoS повышает производительность и надежность промышленных сетей.

Концепция приоритизации трафика

Назначение приоритета сетевым пакетам позволяет добиться того, чтобы наиболее критичные ко времени доставки и наиболее важные пакеты доставлялись стабильно и с минимальной задержкой. Преимущества использования приоритизации трафика:

- Улучшение производительности сети за счет контроля над трафиком и перегрузками сети.

- Назначение приоритета для разных типов трафика. Как правило, высокий приоритет задается пакетам, критичным ко времени доставки, и данным, важным для бизнес-процессов.
- Обеспечение предсказуемой пропускной способности для мультимедийных приложений, таких как видеоконференции или передача голоса по IP (voice over IP).
- Поддержка производительности сети при росте трафика. Функция приоритезации трафика позволит избежать необходимости наращивания пропускной способности сети.

В коммутаторах Moxa приоритезация трафика построена на использовании четырех очередей трафика. Пакеты с более высоким приоритетом отсылаются по одной очереди, остальные пакеты с более низким приоритетом – по другим.

Приоритезация трафика в EDS осуществляется в соответствии с двумя стандартами маркировки и классификации пакетов:

- **Протокол IEEE 802.1D** – маркировка 2-го уровня
- **Differentiated Services (DiffServ)** – маркировка 3-го уровня

Стандарт маркировки трафика IEEE 802.1D

Маркировка трафика IEEE Std 802.1D, 1998 позволяет обеспечить высокий уровень сервиса сети (Quality of Service, QoS). Уровни сервиса трафика задаются в 4-байтном теге IEEE Std 802.1Q, который предназначен для передачи идентификатора VLAN, а также данных о приоритете пакета IEEE 802.1p. 4-байтный тег следует непосредственно после полей MAC-адреса получателя и MAC-адреса отправителя.

Маркировка трафика IEEE Std 802.1D, 1998 назначает уровень приоритета IEEE 802.1p от 0 до 7 для каждого кадра. Это определяет уровень сервиса, который данный тип трафика должен получить. В таблице ниже показаны уровни приоритета IEEE 802.1p для различных типов трафика.

Уровень приоритета IEEE 802.1p	Тип трафика IEEE 802.1D
0	Best Effort (default) <i>Негарантированный (по умолчанию)</i>
1	Background <i>Фоновый</i>
2	Standard (spare) <i>Стандартный (резервный режим)</i>
3	Excellent Effort (business critical) <i>Режим высокого качества (критически важное для бизнеса)</i>
4	Controlled Load (streaming multimedia) <i>Контролируемая загрузка (потокосная передача мультимедийных данных)</i>
5	Video (interactive media); less than 100 milliseconds of latency and jitter <i>Видео (интерактивная среда); менее 100 мс задержки</i>
6	Voice (interactive voice); less than 10 milliseconds of latency and jitter <i>Голос (интерактивная среда); менее 10 мс задержки</i>
7	Network Control Reserved traffic <i>Критичный трафик управления сетью</i>

Несмотря на то, что стандарт IEEE 802.1D является самой распространенной схемой назначения приоритетов сетевым пакетам, у него есть несколько ограничений:

- Он требует наличие дополнительного 4-байтного тега в Ethernet-кадре, что обычно является опцией в Ethernet-сети. Без этого тега схема работать не будет.
- Тег является частью заголовка IEEE 802.1Q, поэтому для того, чтобы применять QoS на 2-м уровне, вся сеть должна поддерживать тегирование IEEE 802.1Q VLAN.

- Этот стандарт поддерживается только в сетях LAN и не поддерживается в маршрутизируемых WAN соединениях, поскольку теги IEEE 802.1Q при проходе через маршрутизатор удаляются.

Стандарт маркировки трафика – Differentiated Services (DiffServ)

DiffServ DSCP – это стандарт маркировки 3-го уровня, который использует для хранения информации о приоритете пакета поле DiffServ Code Point (DSCP) в заголовке IP-протокола. DSCP является передовой технологией приоритизации пакетов, поскольку позволяет задавать сети способы назначения приоритетов различным типам трафика. DSCP использует 64 значения, которые соответствуют задаваемым пользователем уровням сервиса, что позволяет максимально эффективно управлять сетевым трафиком.

Преимущества DiffServ DSCP по сравнению с IEEE 802.1D:

- Возможность управления обработкой различных типов трафика в коммутаторе путем назначения каждому типу трафика своего уровня сетевого сервиса.
- Не требует использования дополнительных полей Ethernet-кадра.
- DSCP использует IP заголовок пакета, поэтому назначенный приоритет сохраняется не только в локальной сети, но и при передаче через Интернет.
- DSCP обратно совместим с IPV4 TOS, что позволяет работать с существующими устройствами, использующими схему назначения приоритетов TOS 3-го уровня.

Назначение приоритета трафику

Коммутатор Моха классифицирует трафик на основе 2-го уровня 7-уровневой модели OSI и назначает приоритет трафику в соответствии с информацией о приоритете, содержащейся в принимаемом кадре. Входящий трафик классифицируется на основе фрейма IEEE 802.1D и перенаправляется в очередь соответствующего приоритета в соответствии со значением уровня сервиса IEEE 802.1p, заданного в кадре. Значения уровня сервиса задаются в 4-байтном теге IEEE 802.1Q, поэтому трафик будет содержать значения приоритета 802.1p только в том случае, если сеть сконфигурирована с VLAN тегированием. Трафик проходит через коммутатор следующим образом:

- Пакет, полученный коммутатором, может содержать или не содержать тег 802.1p. Если он не содержит данный тег, то ему назначается тег 802.1p по умолчанию (обычно это 0). Либо пакет может быть маркирован новым тегом 802.1p, что приведет к тому, что все данные о старом теге 802.1p будут потеряны.
- Поскольку все уровни приоритета 802.1p соответствуют очередям трафика, то пакет, подготовленный для передачи, будет помещен в соответствующую очередь. Когда пакет окажется в голове очереди и будет готов к передаче, коммутатор определит, тегирован ли текущий выходной порт для данной VLAN. Если это так, в расширенном заголовке 802.1D будет использован новый тег IEEE 802.1p.
- Коммутатор Моха проверит пакет, полученный на входном порте, в соответствии с классификацией трафика IEEE 802.1D и назначит ему приоритет на основе значения IEEE 802.1p в данном теге. Именно это значение определяет, к какой очереди трафика будет отнесен пакет.

Очереди пакетов

Для возможности приоритизации трафика коммутатор Моха поддерживает несколько очередей пакетов. Трафик с высоким приоритетом пройдет через коммутатор, не будучи задержанным трафиком с более низким приоритетом. Когда пакет доставляется на коммутатор, на входе он подвергается определенной обработке (классификация, маркировка/ремаркировка) и сортируется в соответствующую очередь. Далее коммутатор отправляет пакеты из каждой очереди. Коммутаторы Моха поддерживают два механизма обслуживания очередей:

- Weight Fair (на основе веса очереди): Этот метод обслуживает все очереди трафика, отдавая приоритет высокоприоритетным очередям. В большинстве случаев, этот метод отдает первенство трафику с более высоким приоритетом, но в случае, если высокоприоритетный трафик превышает пропускную способность линии, прохождение низкоприоритетного трафика не блокируется.
- Strict (строгий): Этот метод первым обслуживает высокоприоритетный трафик, очередь низкоприоритетного трафика задерживается до тех пор, пока не будут переданы высокоприоритетные данные. Этот метод всегда отдает первенство трафику с высоким приоритетом.

Настройка приоритизации трафика

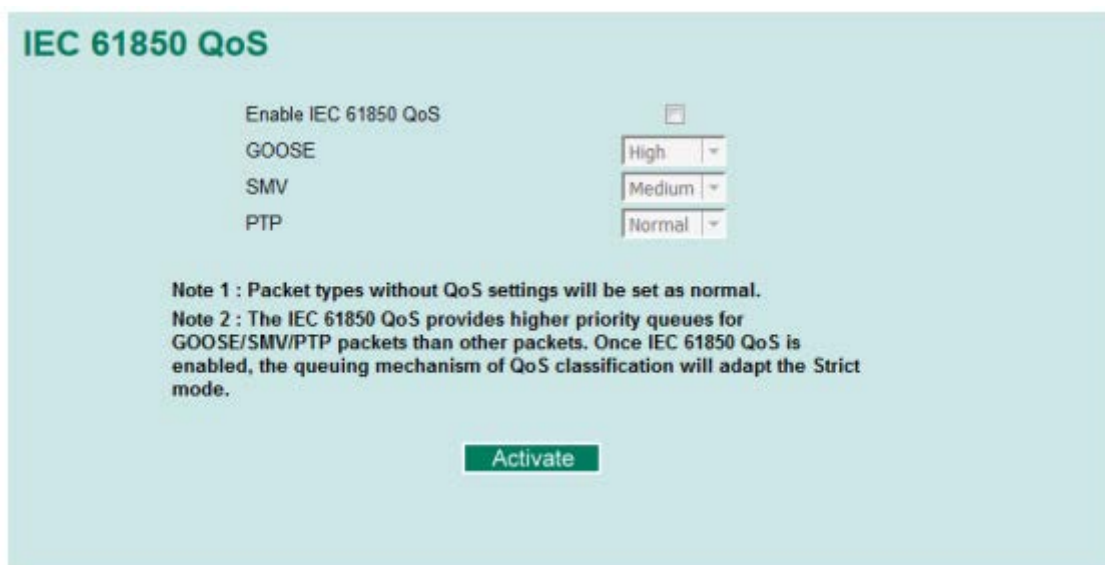
Функция Quality of Service (QoS) обеспечивает возможность приоритизации трафика для гарантии того, что важные данные доставляются последовательно и в соответствии с графиком. Для классификации сетевых пакетов коммутатор MOXA поддерживает распознавание тегов TOS 3-го уровня и IEEE 802.1p/1Q CoS 2-го уровня. Функция QoS в коммутаторах Moxa повышает производительность и детерминизм промышленной сети для критически важных приложений.

IEC 61850 QoS

Функция качества обслуживания **IEC 61850 QoS (Quality of Service)** является функцией приоритизации пакетов, которая назначает приоритеты критически важным сообщениям, отправленным по протоколам GOOSE/SMV/PTP в системах энергетических подстанций. Для сравнения, классификация QoS (QoS Classification) используется только для приоритизации сообщения на основе порта.

Модели, поддерживающие функцию

Серия PT-7728, серия PT-7828, серия PT-7728-PTP (Firmware V3.4)



Enable IEC 61850 QoS (включение приоритета пакетов)

Параметр	Описание	Значение по умолчанию
<i>Включить функцию IEC 61850 QoS</i>	Включает/выключает функцию IEC 61850 QoS	<i>Выключена</i>

Протокол GOOSE

Параметр	Описание	Значение по умолчанию
High/Medium/Normal/Low Высокий/средний/ нормальный/низкий	Приоритет пакетов протокола GOOSE: High -> Medium -> Normal -> Low (Высокий -> Средний -> Нормальный -> Низкий). Рекомендуем использовать высокий приоритет (High).	High

Протокол SMV

Параметр	Описание	Значение по умолчанию
High/Medium/Normal/Low Высокий/средний/ нормальный/низкий	Приоритет пакетов протокола SMV: High -> Medium -> Normal -> Low (Высокий -> Средний -> Нормальный -> Низкий). Рекомендуем использовать высокий приоритет (High).	Medium

Протокол RTP

Параметр	Описание	Значение по умолчанию
High/Medium/Normal/Low Высокий/средний/ нормальный/низкий	Приоритет пакетов протокола GOOSE: High -> Medium -> Normal -> Low (Высокий -> Средний -> Нормальный -> Низкий).	Normal

QoS Classification (Классификация QoS)

Существуют два типа классификации функции QoS в зависимости от модели коммутатора.

Тип	Модели коммутаторов
Тип 1 <i>Тип 1</i>	Серия EDS-400A, EDS-505A/508A/510A/G509, EDS-P506A-4PoE/P510/P510A-8PoE, серия EDS-600, IKS-G6524/G6824, серия ICS-G7000
Тип 2 <i>Тип 2</i>	EDS-516A/518A, EDS-728/828, IKS-6726/6726-8PoE/6728

Тип 1

Port	Inspect ToS	Inspect CoS	Port Priority
1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	3(Normal) ▼
2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	3(Normal) ▼
3	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	3(Normal) ▼
4	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	3(Normal) ▼
5	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	3(Normal) ▼
6	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	3(Normal) ▼
7	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	3(Normal) ▼
8	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	3(Normal) ▼

Коммутатор Моха поддерживает распознавание тегов TOS 3-го уровня и CoS 2-го уровня для классификации пакетов трафика.

Queuing Mechanism (Механизм создания очередей)

Параметр	Описание	Значение по умолчанию
Weight Fair	У коммутатора Моха есть 4 очереди приоритетов. В	Weight Fair

<i>На основе веса очереди</i>	схеме Weight Fair четырем уровням приоритета соответствуют веса 8, 4, 2, 1. Эта схема предотвращает блокировку передачи низкоприоритетных пакетов, которые будут иметь лишь небольшую задержку в обработке, по сравнению с высокоприоритетным трафиком.	
<i>Strict Строгий</i>	В схеме Strict высокоприоритетный трафик занимает выходной порт до того, пока очередь не исчерпается, и только после этого отправляются пакеты с более низким приоритетом. Эта схема может привести к блокировке передачи низкоприоритетных пакетов, зато гарантируется максимально быстрая доставка высокоприоритетных.	

Inspect TOS (Распознавание битов TOS)

Параметр	Описание	Значение по умолчанию
<i>Включен/Выключен</i>	Включает или выключает активацию распознавания коммутатором битов TOS в пакете IPV4 для определения приоритета каждого пакета.	Включен

Inspect COS (Распознавание тегов COS)

Параметр	Описание	Значение по умолчанию
<i>Включен/Выключен</i>	Включает или выключает активацию распознавания коммутатором тегов 802.1p COS в MAC-кадре для определения приоритета каждого пакета.	Включен

Port Priority (Приоритет порта)

Параметр	Описание	Значение по умолчанию
<i>Port priority Приоритет порта</i>	У коммутатора Moxa есть 4 очереди приоритетов. К каждому порту применяется определенный тип очереди: Low, normal, medium, high (низкий, нормальный, средний, высокий).	3(Normal)

Примечание:

Приоритет входящего фрейма определяется в следующем порядке:

1. Inspect TOS (распознавание TOS)
2. Inspect COS (распознавание COS)
3. Port priority (приоритет порта)

Примечание:

Администратор может активировать эти классификации индивидуально или в комбинации. К примеру, если требуется порт с высоким приоритетом, функции Inspect TOS и Inspect COS можно отключить. Это оставляет активированным только Port Highest Priority, что означает, что все входящие фреймы получают на этом порту высокий приоритет.

Тип 2



Queuing Mechanism (Механизм создания очередей)

Параметр	Описание	Значение по умолчанию
Weight Fair <i>На основе веса очереди</i>	У коммутатора Моха есть 4 очереди приоритетов. В схеме Weight Fair четырем уровням приоритета соответствуют веса 8, 4, 2, 1. Эта схема предотвращает блокировку передачи низкоприоритетных пакетов, которые будут иметь лишь небольшую задержку в обработке, по сравнению с высокоприоритетным трафиком.	Weight Fair
Strict <i>Строгий</i>	В схеме Strict высокоприоритетный трафик занимает порт выхода до того, пока очередь не исчерпается, и только после этого отправляются пакеты с более низким приоритетом. Эта схема может привести к блокировке передачи низкоприоритетных пакетов, зато гарантируется максимально быстрая доставка высокоприоритетных.	

Port Highest Priority (Наивысший приоритет порта)

Параметр	Описание	Значение по умолчанию
Enable/Disable <i>Включен/Выключен</i>	Включает или выключает определение приоритета для каждого порта.	Выключен

Inspect TOS (Распознавание битов TOS)

Параметр	Описание	Значение по умолчанию
Enable/Disable <i>Включен/Выключен</i>	Включает или выключает распознавание коммутатором битов TOS в пакете IPV4 для определения приоритета каждого пакета.	Включен

Inspect COS (Распознавание тегов COS)

Параметр	Описание	Значение по умолчанию
Enable/Disable <i>Включен/Выключен</i>	Включает или выключает распознавание коммутатором тегов 802.1p COS в MAC-кадре для определения приоритета каждого пакета.	Включен

Примечание:

Приоритет входящего фрейма определяется в следующем порядке:

1. Port Highest Priority (наивысший приоритет порта)
2. Inspect TOS (распознавание TOS)
3. Inspect COS (распознавание COS)

CoS Mapping ((привязка значений CoS к очередям приоритетов)



CoS Value and Priority Queues (Значение CoS и очереди приоритетов)

Параметр	Описание	Значение по умолчанию
High/Medium/Normal/Low <i>Высокий/средний/нормальный/низкий</i>	Распределите разные значения CoS по четырем исходящим очередям.	0: Low 1: Low 2: Normal 3: Normal 4: Medium 5: Medium 6: High 7: High

TOS/DiffServ Mapping (привязка значений TOS/DiffServ к очередям приоритетов)

Mapping Table of ToS (DSCP) Value and Priority Queues

ToS	Level	ToS	Level	ToS	Level	ToS	Level
0x00(1)	0(Low)	0x04(2)	0(Low)	0x08(3)	0(Low)	0x0C(4)	0(Low)
0x10(5)	0(Low)	0x14(6)	0(Low)	0x18(7)	0(Low)	0x1C(8)	0(Low)
0x20(9)	1(Low)	0x24(10)	1(Low)	0x28(11)	1(Low)	0x2C(12)	1(Low)
0x30(13)	1(Low)	0x34(14)	1(Low)	0x38(15)	1(Low)	0x3C(16)	1(Low)
0x40(17)	2(Normal)	0x44(18)	2(Normal)	0x48(19)	2(Normal)	0x4C(20)	2(Normal)
0x50(21)	2(Normal)	0x54(22)	2(Normal)	0x58(23)	2(Normal)	0x5C(24)	2(Normal)
0x60(25)	3(Normal)	0x64(26)	3(Normal)	0x68(27)	3(Normal)	0x6C(28)	3(Normal)
0x70(29)	3(Normal)	0x74(30)	3(Normal)	0x78(31)	3(Normal)	0x7C(32)	3(Normal)
0x80(33)	4(Medium)	0x84(34)	4(Medium)	0x88(35)	4(Medium)	0x8C(36)	4(Medium)
0x90(37)	4(Medium)	0x94(38)	4(Medium)	0x98(39)	4(Medium)	0x9C(40)	4(Medium)
0xA0(41)	5(Medium)	0xA4(42)	5(Medium)	0xA8(43)	5(Medium)	0xAC(44)	5(Medium)
0xB0(45)	5(Medium)	0xB4(46)	5(Medium)	0xB8(47)	5(Medium)	0xBC(48)	5(Medium)

Activate

ToS (DSCP) Value and Priority Queues (значение и очереди приоритетов ToS (DSCP))

Параметр	Описание	Значение по умолчанию
High/Medium/Normal/Low Высокий/средний/ нормальный/низкий	Распределите различные значения TOS по четырем исходящим очередям.	1 ~ 16: Low 17 ~ 32: Normal 33 ~ 48: Medium 49 ~ 64: High

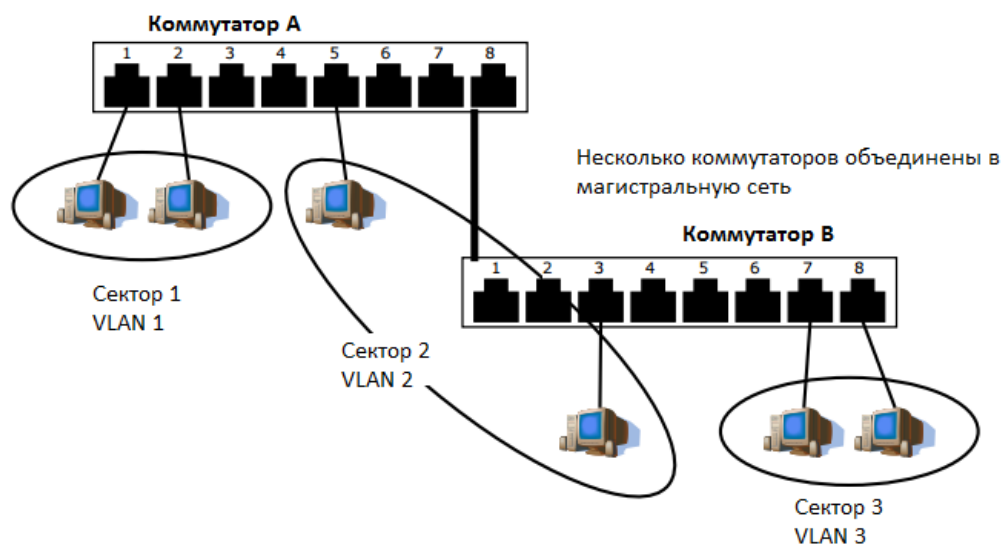
Использование вирт уальных сет ей Virtual LAN

Настройка виртуальных сетей (VLAN) на коммутаторах Моха позволит увеличить эффективность работы сети, разделяя ее на несколько логических, а не физических, сегментов. Управлять логическими подсетями гобычно гораздо легче.

Вирт уальные сет и VLAN

Виртуальная подсеть VLAN – это группа устройств, которые могут быть расположены в произвольных точках сети, но взаимодействуют друг с другом так, как будто принадлежат к одному физическому сегменту. Используя VLAN, пользователь может разбивать сеть на сегменты, не будучи ограниченными физическими соединениями, как это бывает в традиционных сетях. Как правило, сеть разделяют на сегменты по следующим параметрам:

- **По рабочим группам** – VLAN отдела маркетинга, финансов, разработки.
- **По должностным группам** – VLAN директорского состава, менеджеров, остального персонала.
- **По группам пользователей** – VLAN пользователей e-mail, пользователей мультимедийных приложений.



Преимущества VLAN

Основное преимущество виртуальных сетей в том, что они позволяют сегментировать сети гораздо более гибко, нежели традиционное физическое разделение сетей. Использование VLAN также дает следующие преимущества:

- **Облегчает перемещение устройств в сети:** Используя традиционные сети, администраторы сети тратят очень много времени на работу, связанную с перекоммутацией. Если пользователи переходят в другую подсеть, адреса хостов приходится обновлять вручную. К примеру, если компьютер маркетолога, находящийся в сети VLAN Marketing, перемещается в другой кабинет, то компьютер должен сохранить свою принадлежность к группе Marketing. С использованием VLAN потребуется лишь назначить новый порт как принадлежащий к сети VLAN Marketing. Прокладывать какие-либо новые соединения не потребуется.
- **Обеспечивает дополнительную безопасность:** устройства, принадлежащие к одной и той же VLAN, могут взаимодействовать только с устройствами той же VLAN. Если устройству из VLAN Marketing нужно установить соединение с устройством из VLAN Finance, трафик пройдет через маршрутизатор или коммутатор 3-го уровня.
- **Помогают контролировать трафик:** В традиционных сетях могут возникать перегрузки, связанные с наличием широковещательного трафика, идущего ко всем устройствам сети. VLAN повышает производительность сети, поскольку объединяет те устройства, которые логически взаимодействуют только друг с другом

VLAN в коммутаторах МОХА для стойки 19"

Коммутаторы EDS обеспечивают поддержку VLAN стандарта IEEE 802.1Q-1998. Этот стандарт позволяет трафику с нескольких устройств VLAN проходить через одно физическое соединение. Стандарт IEEE 802.1Q-1998 позволяет подключать каждый порт Вашего коммутатора к:

- Любой сети VLAN, назначенной администратором
- Нескольким сетям VLAN одновременно, с использованием тегов 802.1Q

Стандарт требует, чтобы до передачи трафика через коммутатор были определены теги 802.1Q VLAN ID для каждой сети.

Управление сетью VLAN

По умолчанию коммутатор МохА имеет только одну VLAN со следующими характеристиками:

- Имя – Management VLAN
- Тег 802.1Q VLAN ID – 1 (если требуется тегирование)

Все порты коммутатора изначально размещены в одной VLAN. Это единственная подсеть, которая позволяет программному обеспечению сетевого управления иметь доступ к коммутатору.

Взаимодействие между VLAN

Если устройствам из одной VLAN необходимо взаимодействовать с устройствами из другой VLAN, необходим маршрутизатор или коммутатор 3-го уровня. Только при подключении сетей VLAN к этим устройствам будет возможно взаимодействие между ними.

Сети VLAN: тегированное и нетегированное членство

Коммутатор Moxa поддерживает 802.1Q VLAN тегирование – систему, которая позволяет трафику нескольких VLAN проходить через одну физическую (магистральную, транковую) линию. При настройке VLAN необходимо понимать, когда требуется тегированное, а когда нетегированное членство. Это определяется следующим образом: если порт находится в одной сети VLAN, он может быть нетегированным членом, но если требуется, чтобы порт был одновременно членом нескольких VLAN, должно быть задано тегированное членство.

Порт, подключенный к хосту (например, клиентскому ПК), будет нетегированным членом одной VLAN и будет назначен **Портом доступа (Access Port)** коммутатора, в то время как соединения между коммутаторами будут тегированными членами всех VLAN и будут назначены **Транк-портами (Trunk Port)**.

Стандарт IEEE 802.1Q-1998 определяет, как VLAN работают в открытой сети с коммутацией пакетов. Сетевой пакет, отвечающий стандарту 802.1Q, несет дополнительную информацию, позволяющую коммутатору определить, к какой VLAN принадлежит порт. Если фрейм несет такую дополнительную информацию, это тегированный фрейм.

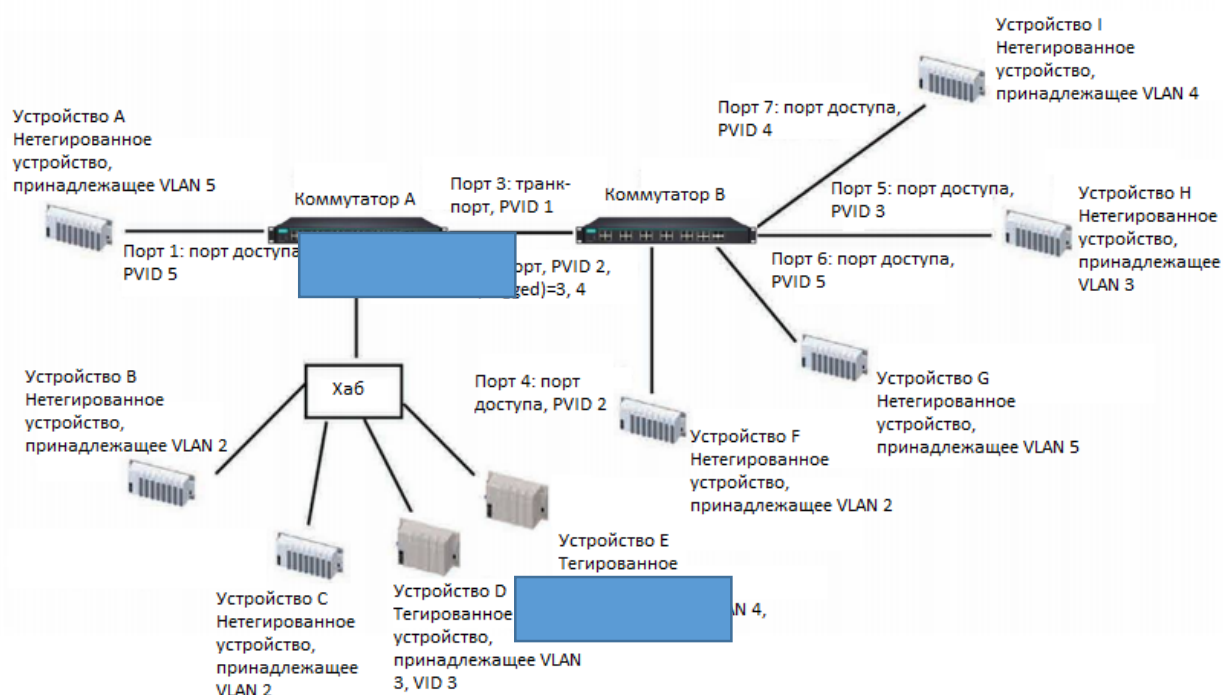
Для прохождения пакетов нескольких VLAN через одну физическую (магистральную, транк-) линию связи каждый пакет должен содержать идентификатор VLAN. Это позволяет коммутаторам определить, к какой VLAN относится каждый пакет. Для связи между сетями VLAN необходимо использовать маршрутизатор.

Коммутатор MOXA поддерживает три типа настроек портов VLAN:

- **Порт доступа (Access Port):** Порт соединения с единственным нетегированным устройством. Пользователю необходимо задать PVID порта (по умолчанию), который указывает, к какой VLAN принадлежит устройство. Когда пакет с порта доступа поступает на транк-порт (порт требует, чтобы все пакеты несли тег- информацию), коммутатор вставит PVID в этот пакет, чтобы помочь следующему коммутатору 802.1Q VLAN идентифицировать его.
- **Транк-порт (Trunk Port):** Порт соединения с LAN, состоящей из нескольких нетегированных/тегированных устройств и/или коммутаторов или хабов. Трафик транк-порта должен содержать Тег. Пользователи также могут задать PVID для транк-порта. Нетегированный пакет получит такой же VID, как и назначенный порту PVID.
- **Гибридный порт (Hybrid Port):** Порт похож на Транк-порт, за исключением того, что пользователи могут указывать теги, которые будут удалены из исходящих пакетов.

Следующий раздел показывает, как использовать разные типы портов в разных приложениях.

Примеры приложений, использующих VLAN



В данном примере:

- Порт 1 соединен с единственным нетегированным устройством, принадлежащим VLAN 5; он должен быть настроен как «порт доступа» (Access) с PVID 5.
- Порт 2 соединен с сетью LAN. Сеть содержит два нетегированных устройства, принадлежащие VLAN 2, одно тегированное устройство с VID3 и одно тегированное устройство с VID4. Порт 2 должен быть настроен как «транк-порт» с PVID2 для нетегированных устройств и Fixed VLAN (Tagged) для тегированных устройств 3 и 4. Поскольку один порт может иметь один уникальный PVID, все нетегированные устройства на одном и том же порту должны принадлежать к одной и той же VLAN.
- Порт 3 соединен с другим коммутатором. Он должен быть настроен как «транк-порт». Они будут использовать протокол GVRP.
- Порт 4 соединен с одним нетегированным устройством, принадлежащим VLAN 2; он должен быть настроен как «порт доступа» с PVID 2.
- Порт 5 соединен с одним нетегированным устройством, принадлежащим VLAN 3; он должен быть настроен как «порт доступа» с PVID 3.
- Порт 6 соединен с одним нетегированным устройством, принадлежащим VLAN 5; он должен быть настроен как «порт доступа» с PVID 5.
- Порт 7 соединен с одним нетегированным устройством, принадлежащим VLAN 4; он должен быть настроен как «порт доступа» с PVID 4.

При такой настройке:

- Пакеты от устройства А будут проходить через «транк-порт 3» с тегированным VID 5. Коммутатор В распознает их VLAN, направит пакеты на порт 6, и затем, удалив теги, передаст на устройство G.
- Пакеты от устройства В и С будут проходить через «транк-порт 3» с тегированным VID 2. Коммутатор В распознает их VLAN, направит пакеты на порт 4, и затем, удалив теги, передаст на устройство F.
- Пакеты от устройства D будут проходить через «транк-порт 3» с тегированным VID 3. Коммутатор В распознает их VLAN, направит пакеты на порт 5, и затем, удалив теги, передаст на устройство H. Пакеты от устройства H будут проходить через «транк-порт 3» с

PVID 3. Коммутатор А распознает их VLAN, направит пакеты на порт 2, но, не удаляя теги, передаст на устройство D.

- Пакеты от устройства E будут проходить через «транк-порт 3» с тегированным VID 4. Коммутатор В распознает их VLAN, направит пакеты на порт 7, и затем, удалив теги, передаст на устройство I. Пакеты от устройства I будут проходить через «транк-порт 3» с тегированным VID 4. Коммутатор А распознает их VLAN, направит пакеты на порт 2, но не удаляя теги, передаст на устройство E.

Настройка виртуальной сети и VLAN

Настройки VLAN

Для настройки 802.1Q VLAN и Port-Based VLAN коммутатора используйте страницу **VLAN Settings**.

Режимы VLAN

Параметр	Описание	Значение по умолчанию
802.1Q VLAN	Включает режим 802.1Q VLAN.	802.1Q VLAN
Port-based VLAN	Включает режим Port-based VLAN.	
Unaware VLAN	Включает режим Unaware VLAN.	

Примечание:

Режим Unaware VLAN поддерживают следующие модели коммутаторов:

- EDS-728
- IKS-6726/6728
- PT-508/510, PT-7710, PT-G7509, PT-7728, PT-7528

802.1Q VLAN Settings (Настройки режима 802.1Q VLAN)

Port	Type	PVID	Fixed VLAN (Tagged)	Fixed VLAN (Untagged)	Forbidden VLAN
1	Access	1			
2	Trunk	1			
3	Hybrid	1			
4	Access	1			
5	Access	1			
6	Access	1			
7	Access	1			
8	Access	1			

Management VLAN ID (VLAN ID для управления коммутатором)

Параметр	Описание	Значение по умолчанию
VLAN ID from 1 to 4094 VLAN ID от 1 до 4094	VLAN ID системы управления данным коммутатором.	1

Port Type (Тип порта)

Параметр	Описание	Значение по умолчанию
Access Порт доступа	Порт, используемый для подключения единственного нетегированного устройства.	Access Порт доступа
Trunk	Порт, используемый для соединения с другой сетью	

<i>Транк-порт</i>	802.1Q VLAN.	
Hybrid <i>Гибридный порт</i>	Порт, используемый для соединения с другим коммутатором Access 802.1Q VLAN или с другой сетью LAN, содержащей в себе тегированные и/или нетегированные устройства и/или другие коммутаторы/концентраторы	



Внимание!

При построении отказоустойчивой сети назначьте порты **Redundant Port, Coupling Port** и **Coupling Control Port** транк-портами, поскольку эти порты работают как магистраль для передачи пакетов различных VLAN различным коммутаторам Moxa.

Port PVID (Порт PVID)

Параметр	Описание	Значение по умолчанию
VID ranges from 1 to 4094 <i>Диапазоны VID от 1 до 4094</i>	VLAN ID по умолчанию для нетегированных устройств, подключенных к порту.	1

Fixed VLAN List (Tagged) – Список фиксированных VLAN (Тегированных)

Параметр	Описание	Значение по умолчанию
VID ranges from 1 to 4094 <i>Диапазоны VID от 1 до 4094</i>	Данное поле будет активным только при выборе транк- или гибридного типа порта. Пропишите VLAN ID тегированных устройств, подключенных к порту. Используйте запятые для разделения различных VID.	Нет

Fixed VLAN List (Untagged) – Список фиксированных VLAN (Нетегированных)

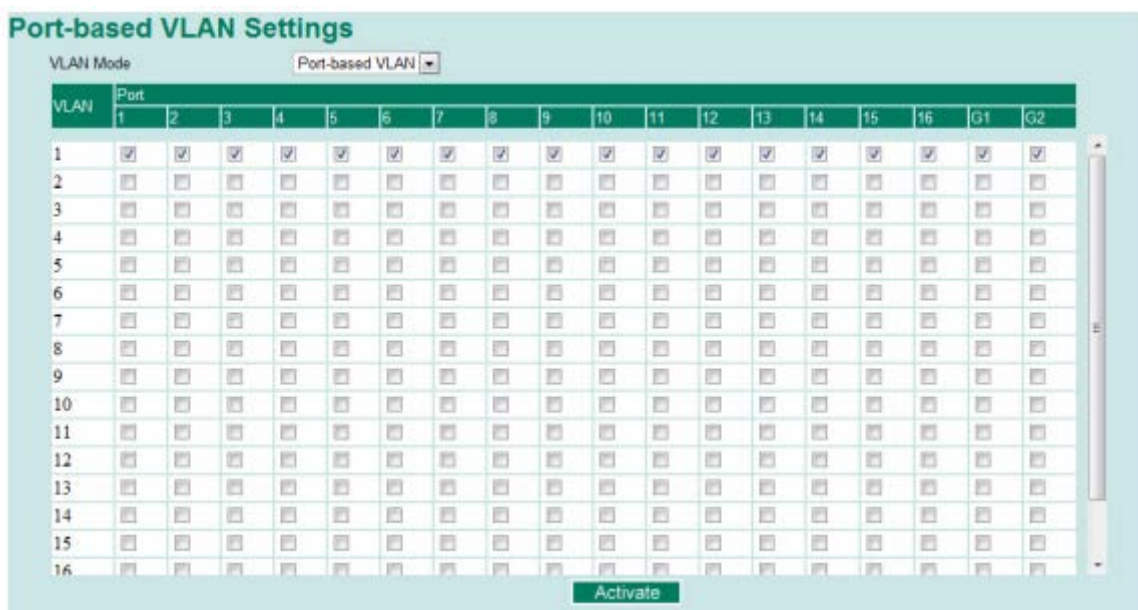
Параметр	Описание	Значение по умолчанию
VID ranges from 1 to 4094 <i>Диапазоны VID от 1 до 4094</i>	Данное поле будет активным только при выборе гибридного типа порта. Пропишите VLAN ID для тегированных устройств, подключенных к порту, теги которых должны быть удалены в исходящих из порта пакетах. Используйте запятые для разделения диапазонов VID.	Нет

Forbidden VLAN List (Запрещенный список VLAN)

Параметр	Описание	Значение по умолчанию
VID ranges from 1 to 4094 <i>Диапазоны VID от 1 до 4094</i>	Данное поле будет активным только при выборе транк- или гибридного типа порта. Установите VLAN ID, которые не будут поддерживаться этим портом. Используйте запятые для разделения различных диапазонов VID.	Нет

Port-Based VLAN Settings (Настройка режима Port-Based VLAN)

Назначьте каждому порту его VLAN ID, как указано в таблице. Количество возможных VLAN ID совпадает с количеством портов коммутатора.



Примечание:

Функция Port-Based VLAN поддерживается следующими моделями коммутаторов:

- Серия EDS (исключая EDS-728/828)
- IKS-6726A/6728A

Функция Port-Based VLAN не поддерживается следующими моделями коммутаторов:

- EDS-728/828
- IKS-G6524A/G6824A
- Серия ICS

Примечание:

Когда включена функция Port-Based VLAN, функция IGMP Snooping будет отключена.

Unaware VLAN Settings (Настройка режима Unaware VLAN)

Режим **Unaware VLAN** предоставляет пользователям возможность более гибкой настройки сети VLAN. Когда включен режим **Unaware VLAN**, коммутатор не проверяет теги VLAN во входящих Ethernet-кадрах. Все теги VLAN могут входить и выходить в коммутатор с режимом **Unaware VLAN**, а коммутатор не будет влиять на теги VLAN Ethernet-кадров.



Примечание:

Когда включена функция **Unaware VLAN**, все порты переходят в режим Unaware.

QinQ Setting (Настройка функции QinQ)

Примечание:

Коммутаторы Моха 3 уровня поддерживают функцию IEEE 802.1ad. Данная функция позволяет пользователям объединять двойные заголовки VLAN в один Ethernet-кадр.

Q in Q Setting

Port	Q in Q Enable	TPID (8100-FFFF, hexadecimal value)
1	<input type="checkbox"/>	8100
2	<input type="checkbox"/>	8100
3	<input type="checkbox"/>	8100
4	<input type="checkbox"/>	8100
5	<input type="checkbox"/>	8100
6	<input type="checkbox"/>	8100
7	<input type="checkbox"/>	8100
8	<input type="checkbox"/>	8100
9	<input type="checkbox"/>	8100
10	<input type="checkbox"/>	8100
11	<input type="checkbox"/>	8100
12	<input type="checkbox"/>	8100
13	<input type="checkbox"/>	8100
14	<input type="checkbox"/>	8100
15	<input type="checkbox"/>	8100
16	<input type="checkbox"/>	8100
17	<input type="checkbox"/>	8100
18	<input type="checkbox"/>	8100
21	<input type="checkbox"/>	8100
22	<input type="checkbox"/>	8100
23	<input type="checkbox"/>	8100
24	<input type="checkbox"/>	8100

Activate

QinQ Enable (Включение функции QinQ)

Параметр	Описание	Значение по умолчанию
Включена/выключена	Включение функции VLAN QinQ	Выключена

TPID

Параметр	Описание	Значение по умолчанию
8100...FFFF	Назначение TPID второму тегу VLAN	8100

VLAN Table (Таблица VLAN)

VLAN Table

VLAN Mode
VLAN Mode: 802.1Q VLAN

Management VLAN
Management VLAN: 1

Current 802.1Q VLAN List

Index	VID	Joined Access Port	Joined Trunk Port	Joined Hybrid Port
1	1	1, 4, 5, 6, 7, 8,	2,	3,

VLAN Table

VLAN Mode
VLAN Mode: Port-based VLAN

Current Port-based VLAN List

Index	VLAN	Joined Port
1	1	1, 4, 5, 6, 7, 8,
2	2	2,
3	3	3,

Используйте таблицу **802.1Q VLAN** для просмотра созданных групп VLAN, добавленных портов доступа (Joined Access Ports), транк-портов (Trunk Ports) и гибридных портов (Hybrid Ports), а также используйте таблицу **Port-based VLAN** для обзора групп VLAN и добавленных портов (Joined Ports).

Примечание:

Большинство управляемых коммутаторов Moxa поддерживают до 64 VLAN. А коммутаторы серий IKS-G6524/G6824 и ICS-G7000 – до 256.

Фильтр рация многоадресного трафика

Фильтрация многоадресного трафика (Multicast Filtering) улучшает производительность сетей, передающих многоадресные пакеты. В данном разделе рассмотрено, как фильтрация многоадресного трафика может быть применена на Вашем коммутаторе Moxa.

Концепция фильтрации многоадресного трафика

Что такое многоадресный IP-пакет?

Многоадресный пакет – это пакет, посылаемый одним хостом нескольким устройствам. Его получают только те устройства, которые принадлежат к соответствующей сетевой группе. Если сеть настроена корректно, многоадресный пакет может быть послан только на конечную станцию или подмножество конечных станций сети LAN или VLAN, принадлежащих к группе получения многоадресного трафика. Члены этой группы могут быть распределены между несколькими подсетями, поэтому многоадресная передача может происходить как внутри LAN, так и через WAN. Кроме того, сети, которые поддерживают многоадресную передачу через IP, могут отсылать только одну копию данных, пока пути доставки данных к целевым группам не разойдутся. Чтобы не занимать пропускную полосу сети, только в точках разветвления многоадресные пакеты дублируются и пересылаются дальше. Многоадресный пакет имеет адрес группы получения многоадресного трафика в поле адреса назначения в IP-заголовке пакета.

Преимущества многоадресного трафика:

- Использование наиболее эффективного и гибкого метода доставки одной и той же информации нескольким получателям за одну передачу.
- Понижение нагрузки на источник передачи данных (например, сервер), поскольку ему не придется делать несколько копий передаваемых данных.
- Эффективное использование пропускной способности сети и отсутствие проблем при расширении групп получения многоадресного трафика.
- Работает совместно с другими IP-протоколами и сервисами, такими как Quality of Service.

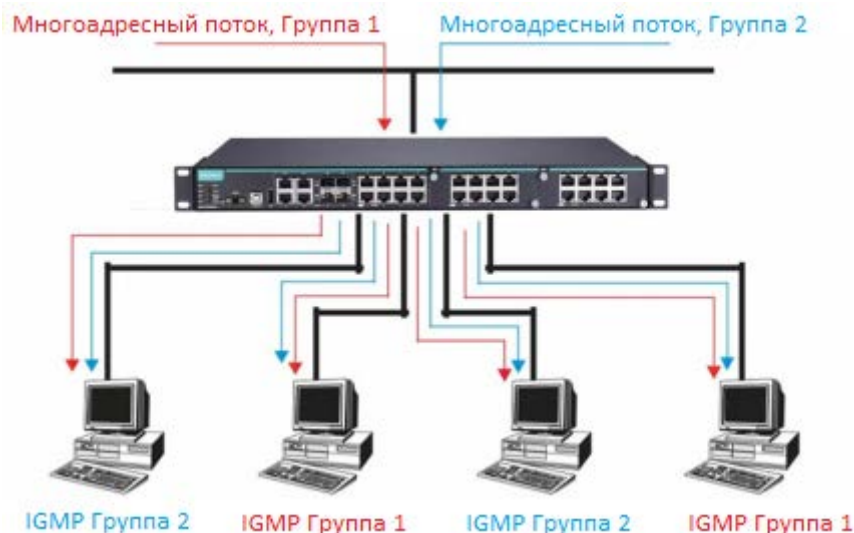
Для некоторых приложений многоадресная передача гораздо более эффективна и разумна, чем индивидуальная рассылка. К примеру, многоадресная передача часто используется для видеоконференций, поскольку большие объемы трафика должны отсылаться на несколько конечных станций одновременно, а это может вызвать значительное снижение производительности сети. Кроме того, многие промышленные протоколы, такие как Allen-Bradley, EtherNet/IP, Siemens Profibus, Foundation Fieldbus HSE, используют многоадресную передачу. Эти промышленные Ethernet-протоколы – это коммуникационные модели publisher/subscriber (издатель/подписчик), осуществляющие многоадресную передачу пакетов, которые могли бы «затопить» сеть трафиком. Функция IGMP Snooping позволяет доставлять многоадресный трафик только тем устройствам, которые реально его используют, снижая общий трафик в сетях Ethernet LAN.

Фильтрация многоадресного трафика

Функция фильтрации многоадресного трафика позволяет гарантировать, что этот трафик получат только соответствующие группы конечных станций. При активации данной функции сетевые устройства могут передавать многоадресные пакеты только на порты, соединенные с зарегистрированными конечными станциями. Две схемы, представленные ниже, иллюстрируют, как ведет себя сеть при использовании и без использования фильтрации многоадресного трафика.

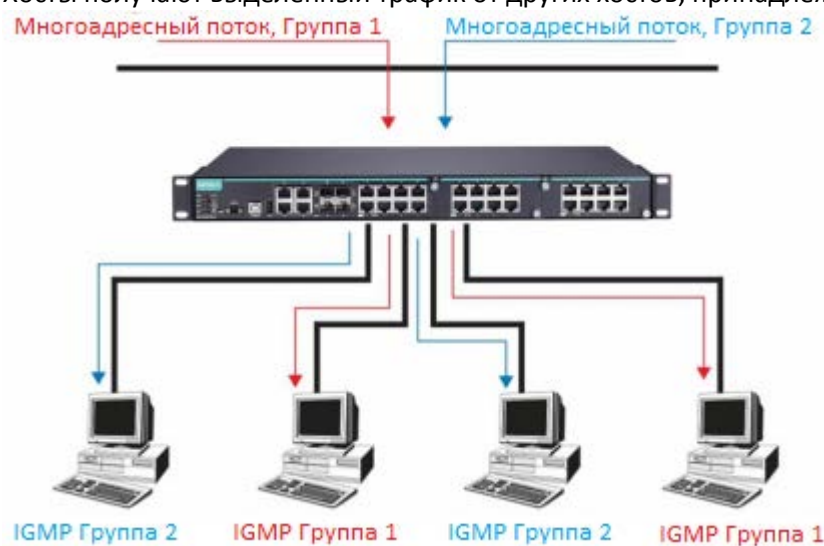
Сеть без фильтрации многоадресной передачи

Все хосты получают многоадресный трафик, даже если он им не нужен.



Сеть с фильтрацией многоадресной передачи

Хосты получают выделенный трафик от других хостов, принадлежащих только к той же группе.



Фильтрация многоадресного трафика и промышленные коммутаторы MOXA

Коммутатор Moxa использует функцию IGMP (Интернет-протокол управления группами) Snooping, GMRP (Многоадресный протокол регистрации GARP) и функцию добавления статического многоадресного MAC-адреса вручную для автоматической фильтрации многоадресного трафика.

Snooping Mode (Режим слежения)

Режим Snooping Mode (Режим слежения) позволяет Вашему коммутатору передавать многоадресные пакеты только на соответствующие порты. Коммутатор отслеживает обмен данными между хостами и IGMP устройствами, такими как маршрутизаторы, и определяет порты,

которые нуждаются в получении этих пакетов, и далее соответствующим образом устанавливает свои фильтры.

IGMP Snooping Enhanced Mode (Расширенный режим слежения IGMP)

Режим Snooping Enhanced позволяет вашему коммутатору пересылать многоадресные пакеты на порт другого коммутатора Moxa. Если отключить данный режим, пакеты данных будут отправляться на порт Querier, также как на порт элемента многоадресной передачи.

Query Mode (Режим запросов)

Режим запросов позволяет коммутатору работать как Querier, если у него самый низкий IP-адрес в подсети, к которой он принадлежит.

Примечание:

Режим IGMP Snooping Enhanced поддерживается только коммутаторами 2 уровня.

Режим IGMP-запросов (IGMP querying) активирован на коммутаторах Moxa по умолчанию, чтобы избежать ситуаций, когда маршрутизаторы многоадресного трафика не следуют правилу выбора самого низкого IP-адреса. Активируйте режим запросов для запуска многоадресных сессий в сетях, где нет IGMP-маршрутизаторов (или querier-устройств). Режим запросов позволяет пользователям включить IGMP Snooping с помощью VLAN ID. Коммутаторы Moxa поддерживают IGMP Snooping версии 1, версии 2 и версии 3. Версия 2 совместим с версией 1. Версией по умолчанию является IGMP V1/V2.

Примечание:

Коммутаторы 3 уровня совместимы с любым устройством с протоколом IGMP v2 и IGMP v3. Коммутаторы 2 уровня поддерживают только протокол IGMP v1/v2.

IGMP Multicast Filtering (фильтрация многоадресного трафика IGMP)

Функция IGMP используется сетевыми устройствами с поддержкой IP для регистрации хостов многоадресных групп. Он может использоваться во всех сетях LAN и VLAN, состоящих из IP-маршрутизаторов, способных передавать многоадресный трафик, и других сетевых устройств, поддерживающих многоадресную фильтрацию. Коммутаторы Moxa поддерживают функцию IGMP версий 1, 2 и 3.

IGMP версии 1 и 2 работает следующим образом:

- IP-маршрутизатор (или querier) периодически отправляет пакеты запросов на все конечные станции LAN или VLAN, подсоединенные к нему. Для сетей с несколькими IP-маршрутизаторами, устройством querier будет маршрутизатор с самым низким IP-адресом. Коммутатор с IP-адресом ниже, чем у других IGMP queriers сети, может стать IGMP querier.
- Когда IP-хост получает пакет с запросом, он отправляет назад отчетный пакет, который указывает, что данная конечная станция хотела бы присоединиться к многоадресной группе.
- Когда отчетные пакеты доставляются на порт коммутатора с активированной функцией IGMP Snooping, коммутатор понимает, что порт должен передать трафик многоадресной группе, и далее передает отчетный пакет маршрутизатору.
- Когда маршрутизатор получает отчетный пакет, он фиксирует, что в LAN или VLAN требуется отправлять трафик для многоадресных групп.
- Когда маршрутизатор направляет трафик многоадресной группе LAN или VLAN, коммутаторы только пересылают трафик на порты, которые получили отчетный пакет.

IGMP версии 3:

IGMP версии 3 поддерживает "фильтрацию источника", который позволяет системе определить, как отфильтровать пакеты от указанных источников адресов. Система может вести либо белый, либо черный список источников.

Сравнение версий функции IGMP

Версия IGMP	Особенности	Образец
V1 <i>Версия 1</i>	а. Периодический запрос	RFC-1112
V2 <i>Версия 2</i>	Совместим с версией 1 и дополнениями: а. Запросы для конкретной группы б. Сообщения выхода из группы с. Передача особых запросов для того, чтобы убедиться, что сообщение выхода было последним в группе д. Выбор Querier	RFC-2236
V3 <i>Версия 3</i>	Совместим с версиями 1, 2 и дополнениями: а. Фильтрация источников - принимать многоадресный трафик от конкретного источника - принимать многоадресный трафик от любого источника, кроме указанного	RFC-3376

GMRP (Многоадресный протокол регистрации GARP)

Коммутаторы Moxa поддерживают протокол IEEE 802.1D-1998 GMRP (Многоадресный протокол регистрации GARP), который отличается от протокола IGMP (Интернет-протокол управления группами). GMRP – это многоадресный протокол на основе MAC-адреса, а IGMP – на основе IP. GMRP обеспечивает механизм, позволяющий промежуточным и конечным устройствам динамически регистрироваться и отменять регистрацию в группе. Функции GMRP аналогичны GVRP, за исключением того, что GVRP регистрирует многоадресные адреса на портах. Когда порт получает сообщение **GMRP-join**, он регистрирует в своей базе данных многоадресные адреса, если такой адрес не зарегистрирован, а все многоадресные пакеты с этого адреса будут перенаправлены в этот порт. Когда порт получает сообщение **GMRP-leave**, он отменит регистрацию многоадресного адреса в своей базе данных, а все многоадресные пакеты с этого адреса не смогут быть перенаправлены в этот порт.

Статический многоадресный MAC-адрес

Некоторые устройства могут поддерживать только многоадресные пакеты, но не поддерживают ни IGMP Snooping, ни GMRP. Коммутаторы Moxa поддерживают добавление многоадресных групп вручную для групповой фильтрации.

Включение фильтрации многоадресного трафика

Используйте Web- или последовательную консоль для включения/отключения функций IGMP Snooping и IGMP querying. Если функция IGMP Snooping недоступна, тогда многоадресный IP-трафик всегда перенаправляется на все порты, нагружая сеть.

Настройка IGMP Snooping

Примечание:

Когда включена функция Port-Based VLAN, функция IGMP Snooping будет отключена.

Функция IGMP Snooping анализирует все пакеты многоадресного трафика и передаёт пакеты только на те порты, которым этот трафик предназначен, уменьшая тем самым объем трафика в сети.

Layer 2 switch setting page (Страница настроек коммутатора второго уровня)

Layer 3 switch setting page (Страница настроек коммутатора третьего уровня)

IGMP Snooping Enable (Включение функции IGMP Snooping)

Параметр	Описание	Значение по умолчанию
Включена/выключена	Активируйте галочку IGMP Snooping Enable в верхней части страницы для включения функции на коммутаторе.	Выключена

Примечание: Необходимо включить функцию IGMP Snooping, если в сети используются также коммутаторы 3 уровня стороннего производителя.

Query Interval (Период времени между запросами)

Параметр	Описание	Значение по умолчанию
Численное значение, задаваемое пользователем	Задайте интервал между запросами от 20 до 600 секунд.	125 секунд

Enable Multicast Fast Forwarding Mode (Включение режима Multicast Fast Forwarding)

Параметр	Описание	Значение по умолчанию
<i>Включен/выключен</i>	Активируйте галочку Enable Multicast Fast Forwarding Mode для активации быстрого перестроения маршрутов многоадресной передачи данных в случае срабатывания резервирования по технологии «кольцо». Необходимое условие: Протокол Turbo Ring или Turbo Chain должен быть включен.	<i>Выключен</i>

IGMP Snooping Enhanced Mode (Расширенный режим IGMP Snooping)

Параметр	Описание	Значение по умолчанию
<i>Включен</i>	Многоадресные пакеты IGMP будут направлены в: <ul style="list-style-type: none"> • Порты Auto-Learned Multicast Querier • Порты – члены группы (member ports) 	<i>Выключен</i>
<i>Выключен</i>	Многоадресные пакеты IGMP будут направлены: <ul style="list-style-type: none"> • Порты Auto-Learned Multicast Router • Порты Static Multicast Querier • Подключенные порты Querier • Порты – члены группы (member ports) 	

Примечание: Расширенный режим IGMP Snooping работает в сетях, полностью состоящих из коммутаторов Moxa.

IGMP Snooping

Параметр	Описание	Значение по умолчанию
<i>Включена/выключена</i>	Включает или выключает функцию IGMP Snooping для конкретного порта VLAN.	Включена, если IGMP Snooping активирована на коммутаторе.

Querier (Опрашивающее устройство)

Параметр	Описание	Значение по умолчанию
<i>Включена/выключена</i>	Включает или выключает функцию Querier.	Включена, если IGMP Snooping активирована на коммутаторе.
<i>Флажки V1/V2 и V3</i>	V1/V2: Включает функцию отправки запросов IGMP snooping Querier версии 1 и 2. V3: Включает функцию отправки запросов IGMP snooping Querier версии 3.	V1/V2

Static Multicast Querier Port (Статический порт Multicast Querier)

Параметр	Описание	Значение по умолчанию
<i>Выбрать/отменить</i>	Выберите порты, которые будут подключены к	<i>Выключен</i>

выбор	маршрутизатору. Эти порты будут получать все многоадресные пакеты от источника. Данная функция будет активна только тогда, когда включена функция IGMP Snooping.	
-------	--	--

Примечание:

Если маршрутизатор или коммутатор 3 уровня подключен к сети, он будет выступать в качестве опрашивающего устройства Querier, а на коммутаторах 2 уровня данная функция будет отключена.

Если все коммутаторы Moxa в сети – коммутаторы 2 уровня, тогда только один коммутатор будет выступать в роли опрашивающего устройства Querier.

Таблица IGMP

Коммутатор Moxa показывает текущие активные группы IGMP. Ниже показаны настройки группы IGMP по VLAN ID.

Страница на коммутаторе второго уровня

VID	Auto Learned Multicast Querier Port	Static Multicast Querier Port	Querier Connected Port	Act as Querier	Active IGMP Groups		
					IP	MAC	Members Port

Страница на коммутаторе третьего уровня

VID: 4

Auto Learned Multicast Router Port	Static Multicast Router Port	Querier Connected Port	Act as Querier
	13,14,15,16,17,18,19,20		Yes

Index	Group	Port	Version	Filter Mode	Sources
-------	-------	------	---------	-------------	---------

Refresh

Информация о данных настройках:

- Auto-learned Multicast Router Port: Данный параметр указывает на то, что маршрутизатор подключается к/посылает пакеты из этого порта (-ов).
- Static Multicast Router Port: Отображает статические порты multicast querier.
- Querier Connected Port: Отображает порт, подключенный к опрашивающему устройству querier.
- Act as a Querier: Отображает, является ли этот порт VLAN опрашивающим портом querier (выигравшем процедуру выбора), или нет.

Current Active IGMP Streams (Активные потоки IGMP)

На рисунке ниже отображено состояние передачи многоадресного потока по VLAN ID:

Current Active IGMP Streams

VID:

Index	Stream Group	Stream Source	Port	Member Ports
1	239.255.255.250	192.168.127.131	22	1,2

Stream Group: IP-адрес группы.

Stream Source: IP-адрес источника многоадресного потока данных.

Port: Порт, который принимает многоадресный поток данных.

Member ports: Порты, который переадресовывают многоадресный поток данных.

Примечание:

Таблица многоадресного потока IGMP доступна к просмотру только на коммутаторах 3 уровня.

Static Multicast MAC Addresses (Статические многоадресные MAC-адреса)

Страница на коммутаторе второго уровня

Static Multicast MAC Address

Current Static Multicast MAC Address List

<input type="checkbox"/> All	Index	MAC Address	Join Port
<input type="button" value="Remove Select"/>			

Add New Static Multicast MAC Address to the List

MAC Address - - - - -

Join Port 1-1 1-2 1-3 1-4 1-5 1-6 1-7 1-8 2-1 2-2 2-3 2-4 2-5
 2-6 2-7 2-8 3-1 3-2 3-3 3-4 3-5 3-6 3-7 3-8 4-1 4-2

Страница на коммутаторе третьего уровня

Примечание: 01:00:5E:XX:XX:XX – это MAC-адреса IP Multicast. Активируйте функцию IGMP Snooping для автоматической классификации.

Add New Static Multicast Address to the List (Добавление в список нового статического многоадресного MAC-адреса)

Параметр	Описание	Значение по умолчанию
MAC Address <i>MAC-адрес</i>	Введите нужный MAC-адрес.	Нет

MAC Address (MAC-адрес)

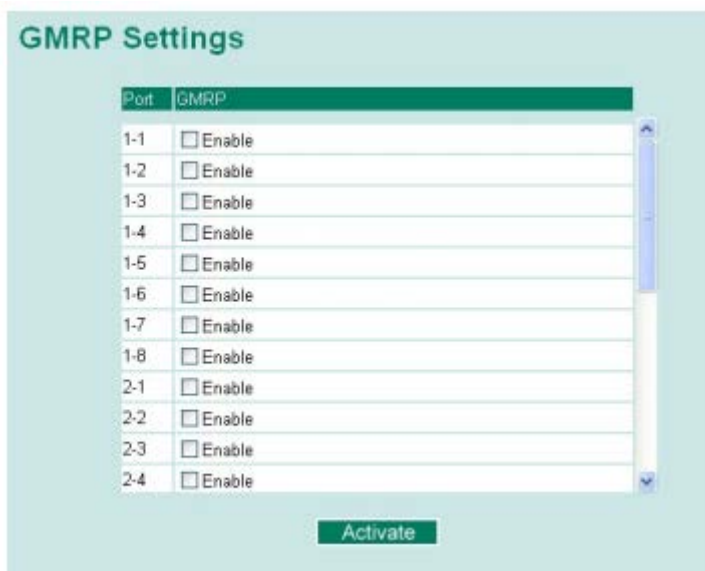
Параметр	Описание	Значение по умолчанию
Integer	Введите номер VLAN, которой принадлежит данный MAC-адрес.	Нет

Join Port

Параметр	Описание	Значение по умолчанию
<i>Выбрать/отменить выбор</i>	Проставьте флажки около портов, которые хотите добавить в multicast-группу.	Нет

Наст ройка прот окола GMRP

GMRP – это протокол управления многоадресными рассылками по MAC-адресам, в отличие от протокола IGMP, основывающегося на IP-адресах. GMRP обеспечивает механизм, позволяющий промежуточным и конечным устройствам динамически регистрироваться и отменять регистрацию в группе.

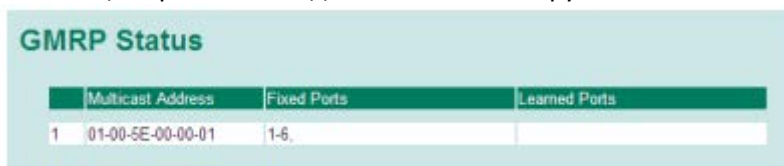


GMRP enable (Включение функции GMRP)

Параметр	Описание	Значение по умолчанию
Включен/выключен	Включает или выключает функцию GMRP для порта, выбранного в колонке Port (на картинке выше).	Выключен

Таблица GMRP

В таблице отражены найденные активные группы GMRP:



Параметр	Описание
Fixed Ports	Адрес многоадресной рассылки, заданный в виде статического адреса.
Learned Ports	Адрес многоадресной рассылки, определенный с помощью GMRP.

Multicast Filtering Behavior (Алгоритм м фильтр рации многоадресных рассылок)



Параметр	Описание	Значение по умолчанию
Multicast Filtering Behavior <i>Алгоритм фильтрации многоадресных рассылок</i>	Алгоритм фильтрации бывает трех типов: Forward All (Отправлять все): отправлять все многоадресные пакеты на порты VLAN. Forward Unknown (Отправлять неизвестные): отправлять неизвестные многоадресные пакеты на порты VLAN, в то время как известные пакеты отправляются указанным группам. Filter Unknown (Фильтровать неизвестные): блокировать неизвестные многоадресные пакеты и отправлять только известные пакеты указанным группам.	Forward Unknown <i>(Отправлять неизвестные)</i>

Конт роль пропускной способност и по порт ам

Как правило, одно устройство не должно занимать собой всю полосу пропускания сети, особенно когда оно работает неисправно. Из-за неправильной топологии сети или наличия неисправных устройств могут возникать так называемые ширококвещательные штормы. Промышленные Ethernet-коммутаторы Moxa не только предотвращает ширококвещательные штормы, но и позволяют настраивать пропускную способность всех пакетов по входу, предоставляя администраторам полный контроль над ограниченной пропускной способностью сети и предотвращая сбои.

Наст ройка управления пропускной способност ью

Тип настройки управления пропускной способностью зависит от модели коммутатора:

Тип	Поддерживаемые модели
Тип 1	Серия EDS-400A, EDS-505A/508A/510A/G509, EDS-P506A-4PoE/P510/P510A-8PoE, серия EDS-600, IKS-G6524/G6824, серия ICS-G7000
Тип 2	EDS-516A/518A, EDS-728/828, IKS-6726/6726-8PoE/6728

Тип 1

Traffic Rate Limiting Settings (Настройка ограничения скорости передачи трафика)

Traffic Rate Limiting Settings						
Control Mode: Normal						
Port	Policy	Ingress Priority Queue Rate				
		Low	Normal	Medium	High	
1	Limit Broadcast	8M	8M	8M	8M	
2	Limit Broadcast	8M	8M	8M	8M	
3	Limit Broadcast	8M	8M	8M	8M	
4	Limit Broadcast	8M	8M	8M	8M	
5	Limit Broadcast	8M	8M	8M	8M	
6	Limit Broadcast	8M	8M	8M	8M	
7	Limit Broadcast	8M	8M	8M	8M	
G1	Limit Broadcast	8M	8M	8M	8M	
G2	Limit Broadcast	8M	8M	8M	8M	

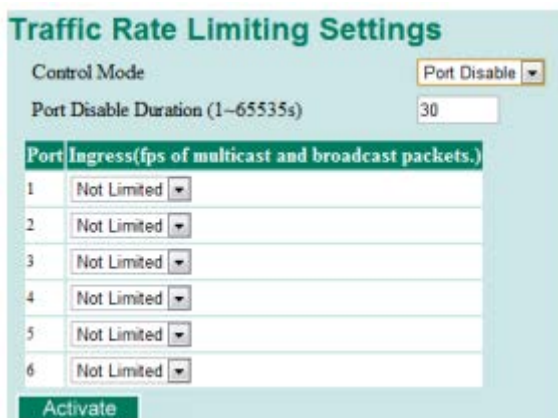
Control Mode (Режим управления)

Параметр	Описание	Значение по умолчанию
Normal	Ограничение максимальной скорости передачи	Normal

<i>Нормальная</i>	для различных типов входящих пакетов.	
Port Disable <i>Порт выключен</i>	Когда поток входящих multicast- и broadcast-пакетов превышает установленный предел, порт будет выключен на определенный период времени. В течение этого периода все пакеты на данном порту будут игнорированы.	

Ingress Rate Limit – Normal (Предел скорости входящих пакетов – Нормальный режим)

Параметр	Описание	Значение по умолчанию
Limit All <i>Предел для всех пакетов</i>	Установите предел входящего трафика для различных типов пакетов: Not Limited (безлимитный), 128K (128 Кб), 256K (256 Кб), 512K (512 Кб), 1M (1 Мб), 2M (2 Мб), 4M (4 Мб), 8M (8 Мб)	Limit Broadcast 8M
Limit Broadcast, Multicast, Flooded Unicast <i>Предел для пакетов Broadcast, Multicast, Flooded Unicast</i>		
Limit Broadcast, Multicast <i>Предел для пакетов Broadcast, Multicast</i>		
Limit Broadcast <i>Предел для пакетов Broadcast</i>		



Ingress Rate Limit – Port Disable (Предел скорости входящих пакетов – Порт выключен)

Параметр	Описание	Значение по умолчанию
Port disable duration (1~65535 seconds) <i>Время, на которое будет выключен порт (1~65535 секунд)</i>	Когда входящие multicast- и broadcast-пакеты превышают предел установленного трафика, порт будет выключен на определенный период времени. В течение этого периода все пакеты на данном порту будут игнорированы.	30 секунд
Ingress (fps) <i>Лимит входящих пакетов (кадр/с)</i>	Выберите предел входного потока (кадр/с) для всех пакетов из следующих вариантов: Not Limited (безлимитный), 4464, 7441, 14881, 22322, 37203, 52084, 74405	Безлимитный

Egress Rate Limit (Предел скорости исходящего потока)

Параметр	Описание	Значение по умолчанию

Egress rate Скорость исходящего потока	Выберите предел скорости исходящего потока (% от максимальной пропускной способности) для всех пакетов из следующих вариантов: Not Limited (безлимитный), 3%, 5%, 10%, 15%, 25%, 35%, 50%, 65%, 85%	Безлимитный
---	---	-------------

Тип 2

Broadcast Storm Protection (Защита от широковещательного шторма)



Параметр	Описание	Значение по умолчанию
<i>Включен/выключен</i>	Включает или выключает функцию Broadcast Storm Protection на всём коммутаторе.	<i>Включен</i>

Include Multicast Packet (Включая многоадресные пакеты)

Параметр	Описание	Значение по умолчанию
<i>Включен/выключен</i>	Включает или выключает функцию Broadcast Storm Protection для Multicast-пакетов.	<i>Выключен</i>

Include Unknown Multicast and Unknown Unicast Packet (Включая неизвестные многоадресные и неизвестные одноадресные пакеты)

Параметр	Описание	Значение по умолчанию
<i>Включен/выключен</i>	Включает или выключает функцию Broadcast Storm Protection для неизвестных Multicast-пакетов и неизвестных Unicast-пакетов.	<i>Включен</i>

Traffic Rate Limiting Settings (Настройка ограничения скорости передачи трафика)

Traffic Rate Limiting Settings

Control Mode:

Port	Ingress	Egress
1	Not Limited	Not Limited
2	Not Limited	Not Limited
3	Not Limited	Not Limited
4	Not Limited	Not Limited
5	Not Limited	Not Limited
6	Not Limited	Not Limited
7	Not Limited	Not Limited
8	Not Limited	Not Limited
9	Not Limited	Not Limited
10	Not Limited	Not Limited
11	Not Limited	Not Limited
12	Not Limited	Not Limited
13	Not Limited	Not Limited
14	Not Limited	Not Limited
15	Not Limited	Not Limited
16	Not Limited	Not Limited

Ingress and Egress Rate Limit – Normal (Предел скорости входящих и исходящих пакетов – Нормальный режим)

Параметр	Описание	Значение по умолчанию
Ingress rate Скорость входящих пакетов	Выберите предел потока входящих/исходящих пакетов (% от максимальной пропускной способности) для всех пакетов из следующих вариантов: Not Limited (безлимитный), 3%, 5%, 10%, 15%, 25%, 35%, 50%, 65%, 85%	Безлимитный
Egress rate Скорость исходящих пакетов		

Traffic Rate Limiting Settings

Control Mode:

Period (1-65535s):

Port	Ingress
1	Not Limited
2	Not Limited
3	Not Limited
4	Not Limited
5	Not Limited
6	Not Limited
7	Not Limited
8	Not Limited
9	Not Limited
10	Not Limited
11	Not Limited
12	Not Limited
15	Not Limited
16	Not Limited

Ingress Rate Limit – Port Disable (Предел скорости входящих пакетов – Порт выключен)

Параметр	Описание	Значение по умолчанию
Port disable duration	Когда входящие multicast- и broadcast-пакеты	30 секунд

(1~65535 seconds) Время, на которое выключен порт (1~65535 секунд)	превышают установленный предел скорости потока, порт будет выключен на определенный период времени. В течение этого периода все пакеты на данном порту будут игнорированы.	
Ingress (fps) Лимит входящих пакетов (кадр/с)	Выберите предел скорости входящего потока (кадр/с) для всех пакетов из следующих вариантов: Not Limited (безлимитный), 4464, 7441, 14881, 22322, 37203, 52084, 74405	Безлимитный

Unicast Filter Behavior (Функция фильтрации Unicast-пакетов)

Примечание: Данная функция поддерживается коммутаторами EDS-728/828 и стоечными коммутаторами.

Когда коммутатор получает неизвестный unicast-пакет, он пересылает его на все порты в локальной сети. Функция Unicast Filter Behavior предотвращает переполнение сети такими пакетами. Поставьте галочку для активации данной функции.



Параметр	Описание	Значение по умолчанию
Enable Filter unknown Unicast <i>Включение функции фильтрации Unicast-пакетов</i>	Включите данную функцию для предотвращения переполнения локальной сети неизвестными unicast-пакетами.	Disable <i>Выключена</i>

Безопасность

Примечание: Функции безопасности не поддерживаются коммутаторами серии EDS-400A.

Функцию безопасности можно разделить на два уровня: имя пользователя/пароль для управления коммутатором и доступ к портам. Для уровня безопасности «имя пользователя/пароль» коммутаторы Moxa предлагают два варианта входа в систему: Terminal Access Controller Access-Control System Plus (TACACS+) и Remote Authentication Dial In User Service (RADIUS). Оба варианта, TACACS+ и RADIUS, представляют собой централизованную систему "AAA" (Authentication, Authorization and Accounting - Аутентификация, Авторизация и Учет) для подключения к сетевым службам. Основная цель TACACS + и RADIUS – обеспечение эффективного и безопасного механизма для управления учетными данными пользователей.

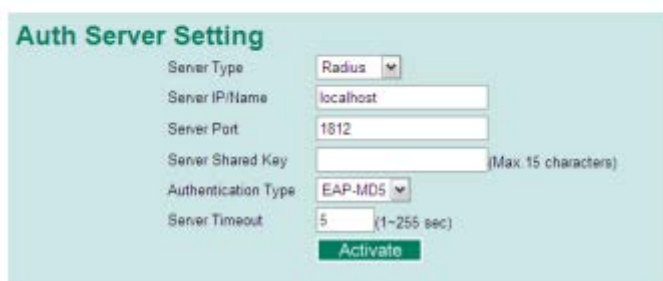
User Login Authentication – User Login Settings (Вход в систему с помощью имени пользователя – Настройка входа в систему)

Страница выбора опции TACAS+ или RADIUS представлен ниже



User Login Authentication – Auth Server Setting (Вход в сист ему с помощью имени пользует еля – Наст ройка сервера аут ент ификации)

Настройки серверов TACAS+ и RADIUS показаны ниже:



Параметр	Описание	Значение по умолчанию
Server Type <i>Тип сервера</i>	Выбор типа сервера аутентификации.	TACACS+
Server IP/Name <i>IP-адрес/имя сервера</i>	Установка IP-адреса внешнего сервера TACACS+/RADIUS как базы данных для аутентификации.	Localhost
Server Port <i>Порт сервера</i>	Установка коммуникационного порта внешнего сервера TACACS+/RADIUS как базы данных для аутентификации.	TACACS+: 49 RADIUS: 1812
Server Shared Key <i>Ключ доступа к серверу</i>	Задайте конкретные символы для проверки подлинности сервера.	Нет
Authentication Type <i>Тип аутентификации</i>	Тип аутентификации для сервера RADIUS – isEAP-MD5.	ASCII для TACACS+
Server Timeout <i>Время ожидания ответа сервера</i>	Время ожидания ответа сервера.	TACACS+: 30 RADIUS: 5

Серт ификат проверки подлинност и сервера

Коммутаторы Моха обладают двумя методами шифрования связи: сертификат SSL Certificate и SSH Key. Невозможно одновременное использование двух методов шифрования. Метод SSL (Secure Socket Layer) предназначен для обеспечения безопасности веб-коммуникаций. Он обеспечивает защиту данных между двумя устройствами сети. Метод SSH (Secure Shell) – это протокол безопасности уровня приложения и транспортного уровня. Он шифрует данные для обеспечения безопасности.

Примечание:

Коммутатор поддерживает одновременное использование только одного типа шифрования



Выберите тип сертификата и нажмите Activate для завершения.

Управление доступом к порту

У коммутаторов Moxa есть два вида управления доступом к порту: Static Port Lock (Статическая блокировка порта) и стандарт IEEE 802.1X.

Static Port Lock (Статическая блокировка порта)

Коммутатор Moxa может быть настроен так, чтобы фиксировать статические MAC-адреса для конкретного порта. С помощью функции блокировки порты не будут пополнять таблицу дополнительными MAC-адресами и будут получать данные только от заданных статических MAC-адресов, защищаясь таким образом от подключения постороннего оборудования и от атак хакеров.

Стандарт IEEE 802.1X

Стандарт IEEE 802.1X определяет протокол для контроля доступа и аутентификации по схеме клиент/сервер. Протокол ограничивает несанкционированный доступ клиентов к локальной сети через порты, которые подключены к интернету и были бы легко доступны. Целью сервера аутентификации является проверка каждого клиента, который запрашивает доступ к порту. Клиенту будет разрешен доступ к порту только в случае успешного прохождения проверки подлинности.

Стандарт IEEE 802.1X основан на трех составляющих: Client/Supplicant (Клиент/запрашивающий), Authentication Server (Авторизационный сервер) и Authenticator (Аутентификатор).

Client/Supplicant (Клиент/запрашивающий): Конечное устройство, которое запрашивает доступ к локальной сети и коммутатору, а также отвечает на запросы коммутатора.

Authentication Server (Авторизационный сервер): Сервер, который выполняет фактическую авторизацию запрашивающего устройства.

Authenticator (Аутентификатор): Пограничный коммутатор или беспроводная точка доступа, которые действуют как прокси-сервер между запрашивающим устройством и сервером аутентификации и запрашивают информацию об идентификации от запрашивающего устройства, сверяют информацию с авторизационным сервером и передают ответ запрашивающему устройству.

В стандарте IEEE 802.1X коммутатор Moxa выполняет роль аутентификатора. Запрашивающий и аутентификатор обмениваются друг с другом кадрами EAPOL (Extensible Authentication Protocol

over LAN). Пользователь может использовать внешний RADIUS-сервер в качестве авторизационного сервера или реализовать авторизационный сервер на базе коммутатора Моха, используя локальную базу данных пользователей в качестве справочной таблицы для авторизации. При использовании сервера RADIUS в качестве авторизационного сервера, аутентификатор и аутентификационный сервер обмениваются друг с другом кадрами EAP (Extensible Authentication Protocol).

Авторизация может быть инициирована запрашивающим устройством или аутентификатором. Когда запрашивающее устройство инициирует процесс авторизации, оно посылает аутентификатору кадр **EAPOL-Start**. Когда аутентификатор инициирует процесс авторизации или получает кадр **EAPOL-Start**, он посылает запрашивающему устройству кадр **EAP Request/Identity** с запросом имени пользователя.

Configuring Static Port Lock (Настройка статической блокировки порта)

Коммутатор Моха поддерживает добавление unicast-групп вручную, если это требуется.

Статический MAC-адрес unicast

Параметр	Описание	Значение по умолчанию
MAC Address <i>MAC-адрес</i>	Добавьте статический MAC-адрес unicast в таблицу адресов.	Нет
Port <i>Порт</i>	Связывает статический адрес с конкретным портом.	1 или 1-1

Настройка стандарта IEEE 802.1X

Database Option (Выбор базы данных)

Параметр	Описание	Значение по умолчанию
Local (Max. of 32 users) <i>Локальная (макс.32 пользователя)</i>	Выберите этот параметр для авторизации через локальную базу данных пользователей.	Local
Radius	Выберите этот параметр для установки внешнего RADIUS сервера в качестве базы данных для авторизации. Механизм авторизации – EAP-MD5.	
Radius, Local	Выберите этот параметр для установки внешнего RADIUS сервера в качестве базы данных для авторизации, он будет приоритетным. Механизм авторизации – EAP-MD5. Второй по приоритету будет локальная пользовательская база данных.	

Radius Server (Сервер Radius)

Параметр	Описание	Значение по умолчанию
IP address or domain name <i>IP-адрес или имя домена</i>	IP-адрес или имя домена сервера RADIUS.	localhost

Server Port (Порт сервера)

Параметр	Описание	Значение по умолчанию
Numerical <i>Числовое значение</i>	UDP-порт сервера RADIUS.	1812

Shared Key (Ключ доступа)

Параметр	Описание	Значение по умолчанию
alphanumeric (Max. of 40 characters) <i>Буквенно-числовое значение (до 40 знаков)</i>	Общий ключ для использования внешнего сервера RADIUS и коммутатора Moxa. Оба должны использовать один и тот же ключ.	Нет

Re-Auth (Повторная авторизация)

Параметр	Описание	Значение по умолчанию
Enable/Disable <i>Включена/выключена</i>	Функция требует повторной авторизации клиента при отсутствии активности в течение заданного периода времени.	Disable <i>Выключена</i>

Re-Auth Period (Повторная авторизация после заданного периода времени)

Параметр	Описание	Значение по умолчанию
Numerical (60 to 65535 sec.) <i>Числовое значение (60...65535 секунд)</i>	Функция определяет, как часто конечные устройства должны повторно вводить имя пользователя/пароль, чтобы оставаться на связи.	3600

802.1X (Стандарт 802.1X)

Параметр	Описание	Значение по умолчанию
Enable/Disable <i>Включен/выключен</i>	Поставьте флажок в колонке 802.1X, чтобы включить стандарт IEEE 802.1X для одного или нескольких портов. Все конечные устройства должны ввести имя пользователя/пароль до предоставления доступа к портам.	Disable <i>Выключен</i>

802.1X Re-Authentication (Повторная авторизация 802.1X)

Коммутаторы Моха могут запросить подключенные устройства пройти повторную авторизацию вручную.



802.1X Re-Authentication (Повторная авторизация 802.1X)

Параметр	Описание	Значение по умолчанию
<i>Включен/выключен</i>	Включает/выключает повторную авторизацию 802.1X.	Disable <i>Выключен</i>

Настройка локальной базы данных пользователей

При настройке локальной базы пользователей в качестве базы данных для авторизации, вначале настройте базу данных.



Local User Database Setup (Настройка локальной пользовательской базы данных)

Параметр	Описание	Значение по умолчанию
User Name (Max. of 30 characters)	Имя пользователя для локальной пользовательской базы данных.	Нет

Имя пользователя (макс.30 символов)		
Password (Max. of 16 characters) Пароль (макс.16 символов)	Пароль для локальной пользовательской базы данных.	Нет
Description (Max. of 30 characters) Описание (макс.30 символов)	Описание для локальной пользовательской базы данных.	Нет

Примечание:

Имя пользователя для локальной пользовательской базы данных хранится без учета регистра.

Dot1X Radius Server Setting (Настройки сервера Dot1X Radius)

Same as Auth Server Setting (Настройки идентичны настройкам сервера авторизации)

Параметр	Описание	Значение по умолчанию
Включен/выключен	Включает настройки, идентичные настройкам сервера авторизации.	Выключен

Server Setting (Настройки сервера)

Параметр	Описание	Значение по умолчанию
Server IP/Name IP-адрес/имя сервера	Определение IP-адреса/имени сервера.	localhost
Server Port Порт сервера	Определение порта сервера.	1812
Server Shared Key Ключ доступа к серверу	Определение ключа доступа к серверу.	Нет

Port Access Control Table (Таблица контроля доступа к порту)



Состояние порта будет отображаться как авторизованный или неавторизованный.

Авт ома т ические предупреждения

Так как промышленные Ethernet-сети часто территориально распределены, абоненты сети не всегда знают, что происходит в других концах сети. Это значит, что промышленный Ethernet-коммутатор, к которому подключены абоненты, должны оповещать администраторов сети о возможных авариях в режиме реального времени. Даже когда инженеры центра управления находятся вне диспетчерской в течение длительного периода времени, они все равно могут оставаться информированными о состоянии устройств почти постоянно. Коммутаторы Moxa обеспечивают различные методы автоматического предупреждения операторов о сбоях, в частности, e-mail сообщения и релейный выход. Также отправлять оповещения по Email или управлять состоянием реле можно по факту изменения состояния датчиков, подключенных к цифровым входам коммутатора.

Наст ройка предупреждений по e-mail

Функция автоматического предупреждения по e-mail призвана информировать пользователя об определенных событиях сети, заданных пользователем.

Для запуска автоматического предупреждения по e-mail следуйте этой последовательности:

Настройка типов событий: Выберите необходимые типы событий на странице событий **Event Types** консоли или web-интерфейса (описание каждого типа событий представлено ниже, в разделе *Email Alarm Events setting*).

Настройка Email: Для настройки передачи Email-сообщений с последовательной, Telnet-консоли или через web-обозреватель введите IP-адрес/имя почтового сервера, имя аккаунта, пароль аккаунта, повтор пароля и адреса email, на которые будут приходить сообщения о сбоях.

Активация настроек и проверка e-mail, если это необходимо: После настройки и активации Event Types и Email Setup, Вы можете использовать функцию тестирования email **Test Email**, чтобы проверить правильность настроек.

Настройка типов событий

Типы событий могут быть разделены на две базовые группы: **System Events** (Системные события) и **Port Events** (События портов). Системные события относятся к работе всего коммутатора, а события портов – к работе отдельных портов.

Системное событие	Предупреждающий Email отправляется, когда...
Switch Cold Start <i>Холодный старт</i>	Питания полностью выключено и затем включено.
Switch Warm Start <i>Горячий старт</i>	Коммутатор перезагружается, например, при изменении сетевых параметров (IP-адрес, маска сети и т.д.).
Power Transition (On→Off) <i>Перемена питания On→Off</i>	Коммутатор выключен.
Power Transition (Off→On) <i>Перемена питания Off → On</i>	Коммутатор выключен.
DI1/DI2 (On→Off)	Цифровой вход 1/2 выключен.
DI1/DI2 (Off→On)	Цифровой вход 1/2 включен.
Configuration Change Activated <i>Активация изменения настроек</i>	Изменена какая-либо из настроек.
Authentication Failure <i>Сбой авторизации</i>	Введен неверный пароль.
Comm. Redundancy Topology Changed <i>Изменение топологии резервирования связи</i>	<ul style="list-style-type: none"> Какой-либо из коммутаторов Spanning Tree Protocol изменил свое состояние (относится только к «корню» дерева). Изменился Master сети Turbo Ring, или активирован резервный маршрут

Событие порта	Предупреждающий Email отправляется, когда...
Link-on	Порт подсоединен к устройству.
Link-off	Порт отсоединен (например, выдернут кабель, или выключилось устройство, к которому подсоединен порт).
Traffic-Overload <i>Превышение трафика</i>	Превышен порог трафика на данном порту (когда данная функция включена).
Traffic-Threshold (%)	Введите число, не равное нулю, если активирована функция

<i>Порог трафика (%)</i>	Traffic Overload.
<i>Traffic-Duration (sec.) Продолжительность трафика (секунды)</i>	Сообщения о превышении трафика посылаются через интервал, равный значению Traffic Duration, если в этот период превышен порог трафика.

Примечание:

Функции Traffic Overload, Traffic Threshold (%) и Traffic Duration (c) взаимосвязаны. При активации Traffic Overload введите значение Traffic Threshold (не равное нулю) и Traffic Duration (1-300 секунд).

Примечание:

Предупреждающие сообщения по e-mail будут приходить от отправителя:

Managed-Redundant-Switch-00000@Switch_Location

где Managed-Redundant-Switch – это имя коммутатора по умолчанию, 00000 – серийный номер коммутатора, а Switch_Location – месторасположение сервера по умолчанию. Обратитесь к разделу Basic Settings (Базовые настройки), чтобы поменять имя и месторасположение коммутатора.

Настройки Email

Mail Server IP/Name (IP-адрес/имя почтового сервера)

Параметр	Описание	Значение по умолчанию
IP address <i>IP-адрес</i>	IP-адрес почтового сервера.	Нет

SMTP Port (Порт SMTP)

Параметр	Описание	Значение по умолчанию
SMTP port <i>Порт SMTP</i>	Номер порта SMTP.	25

Account Name (Имя аккаунта)

Параметр	Описание	Значение по умолчанию
Макс. 45 символов	Ваш email-аккаунт.	Нет

Password Setting (Настройка пароля)

Параметр	Описание	Значение по умолчанию
Change account password <i>Изменить пароль аккаунта (включите для изменения)</i>	Для изменения пароля через web-интерфейс активируйте смену пароля и введите старый пароль, затем новый пароль, еще раз новый пароль и нажмите Activate.	<i>Выключен</i>
Old password <i>Старый пароль</i>	Введите текущий пароль.	Нет
New password <i>Новый пароль</i>	Введите новый пароль; макс. 45 символов	Нет
Retype password <i>Повтор нового пароля</i>	Подтвердите новый пароль.	Нет

Email Address (Email-адрес)

Параметр	Описание	Значение по умолчанию
Макс. 30 символов	Вы можете настроить 4 email-адреса для получения сигнальных сообщений от коммутатора Moxa.	Нет

Send Test Email (Отправить тестовый Email)

После завершения настройки email-оповещений для их активации нажмите **Activate**, затем **Send Test Email**, чтобы убедиться, что настройка произведена правильно.

Примечание:

Автоматические предупреждения по e-mail будут отсылаться SMTP-сервером с поддержкой механизмов аутентификации CRAM-MD5, LOGIN, PAIN методов SASL (Simple Autentification and Security Level).

Мы настоятельно рекомендуем не вводить имя и пароль, если e-mail сообщения могут доставляться без использования механизмов аутентификации.

Настройка предупреждений через релейный выход

Функция автоматического предупреждения через релейный выход призвана информировать пользователя об определенных событиях сети, заданных пользователем. Для запуска автоматического предупреждения через релейный выход необходимо выполнить следующие действия:

Настройка типов событий: Выберите необходимые типы событий на странице событий **Event Types** консоли или web-интерфейса (описание каждого типа событий представлено ниже, в разделе *Relay Alarm Events setting*).

Активация настроек: активируйте типы событий.

Настройка типов событий

Relay Warning Events Settings

System Events

Override Relay 1 Warning Settings

Power Input 1 failure(On→Off) Disable

DI 1 (Off) Disable DI 1 (On) Disable

Turbo Ring Break Disable

Override Relay 2 Warning Settings

Power Input 2 failure(On→Off) Disable

DI 2 (Off) Disable DI 2 (On) Disable

Port Events

Port	Link	Traffic-Overload	Rs-Threshold(%)	Traffic-Duration(s)
1	Ignore	Disable		
2	Ignore	Disable		
3	Ignore	Disable		
4	Ignore	Disable		
5	Ignore	Disable		
6	Ignore	Disable		
7	Ignore	Disable		
8	Ignore	Disable		
9	Ignore	Disable		
10	Ignore	Disable		
11	Ignore	Disable		
12	Ignore	Disable		
13	Ignore	Disable		
14	Ignore	Disable		
15	Ignore	Disable		
16	Ignore	Disable		
G1	Ignore	Disable		
G2	Ignore	Disable		

Activate

Типы событий могут быть разделены на две базовые группы: **System Events** (Системные события) и **Port Events** (События портов). Системные события относятся к работе всего коммутатора, а события портов – к работе отдельных портов.

Коммутатор Моха поддерживает 2 релейных выходов. Вы можете задать соответствующий выход соответствующему событию. Это помогает администраторам обозначить важность различных событий.

Системное событие	Выход реле сработает, когда...
Power Transition (On → Off) <i>Перемена питания On→Off</i>	Коммутатор выключен.
Power Transition (Off → On) <i>Перемена питания Off → On</i>	Коммутатор выключен.
DI1/DI2 (On→Off)	Цифровой вход 1/2 выключен.
DI1/DI2 (Off→On)	Цифровой вход 1/2 включен.
Обрыв Turbo Ring	Кольцо Turbo Ring разорвано. Только коммутатор MASTER пошлет предупреждение через релейный выход.

Событие порта	Выход реле сработает, когда...
Link-on	Порт подсоединен к устройству.
Link-off	Порт отсоединен (например, выдернут кабель, или выключилось устройство, к которому подсоединен порт).
Traffic-Overload <i>Превышение трафика</i>	Превышен порог трафика на данном порту (когда данная функция включена).
Traffic-Threshold <i>Порог трафика (%)</i>	Введите число, не равное нулю, если активирована функция Traffic Overload.
Traffic-Duration Продолжительность трафика (секунды)	Выход реле сообщит о превышении трафика через интервал, равный значению Traffic Duration, если в этот период превышен порог трафика.

Функция Override relay alarm settings (Временное аннулирование настроек релейного выхода)

Активируйте функцию Override relay alarm settings для временного аннулирования настроек. Данная функция позволяет администратору произвести необходимо работы по устранению проблем.

Примечание:

Функции Traffic Overload, Traffic Threshold (%) и Traffic Duration (с) взаимосвязаны. При активации Traffic Overload введите значение Traffic Threshold (не равное нулю) и Traffic Duration (1-300 секунд).

Список аварийных сигнализаций реле

Используйте данную таблицу для просмотра событий сигнализации реле.



Использование функции Line-Swap-Fast-Recovery

Функция Line-Swap Fast Recovery, активированная по умолчанию, позволяет коммутатору MOXA быстро вернуться к работе после отключения абонентских устройств и подключения их к другим портам. Время восстановления соединения составляет миллисекунды, что дает огромное преимущество по сравнению с офисными коммутаторами, у которых это время может растянуться до нескольких минут. Для отключения функции Line-Swap Fast Recovery или повторной ее активации используйте страницу **Line-Swap Fast Recovery** консоли или web-интерфейса, как показано ниже.

Настройка функции Line-Swap Fast Recovery



Enable Line-Swap-Fast-Recovery (Включение функции Line-Swap-Fast-Recovery)

Параметр	Описание	Значение по умолчанию
<i>Включена/выключена</i>	Установите флажок для активации функции Line-Swap-Fast-Recovery.	Enable <i>Включена</i>

Уст ановка IP-адреса уст роист ва

Чтобы сократить усилия, требуемые для настройки IP-адресов подключенных устройств, коммутатор Мохы оснащен DHCP/BootP-сервером, и поддерживает RARP-протокол для автоматической настройки IP-адресов Ethernet-устройств.

При активации функция **Set Device IP** позволяет коммутатору Моха автоматически присваивать IP-адреса подключенным устройствам с настроенным *DHCP-клиентом* или *RARP-протоколом*. В результате, коммутатор работает как DHCP-сервер, назначая подключенным устройствам уникальные IP-адреса, хранящиеся в памяти коммутатора. Каждый раз при включении или перезагрузке подключенного устройства, коммутатор отправляет ему соответствующий IP-адрес.

Для использования функции **Set Device IP** (Назначение IP-адреса устройств) проделайте следующее:

Шаг 1 – Настройка подключенных устройств

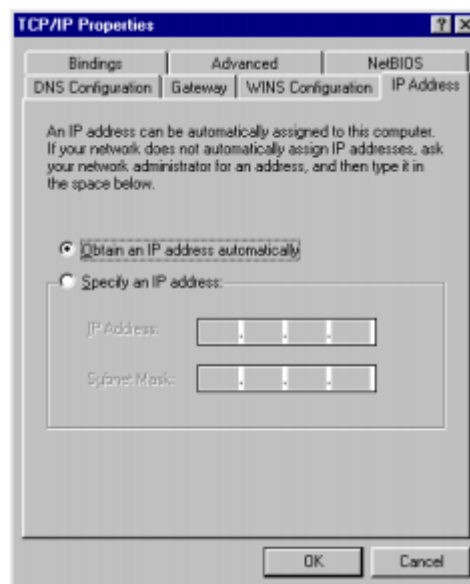
Задайте соответствующие настройки тем Ethernet-устройствам, для которых Вы бы хотели, чтобы их IP-адрес настраивался автоматически. Устройства должны быть настроены так, чтобы иметь возможность получить IP-адрес автоматически.

Утилита настройки устройств должна иметь опцию типа *Obtain an IP address automatically*.

Пример – окно Windows TCP/IP Properties. Хотя утилита настройки Ваших устройств может выглядеть несколько иначе, этот пример должен подсказать Вам, в каком направлении искать.

Вам также необходимо решить, к каким портам коммутатора Моха будут подключены Ваши устройства.

Вам потребуется настроить каждый из этих портов отдельно, как описано в следующем шаге.



Шаг 2

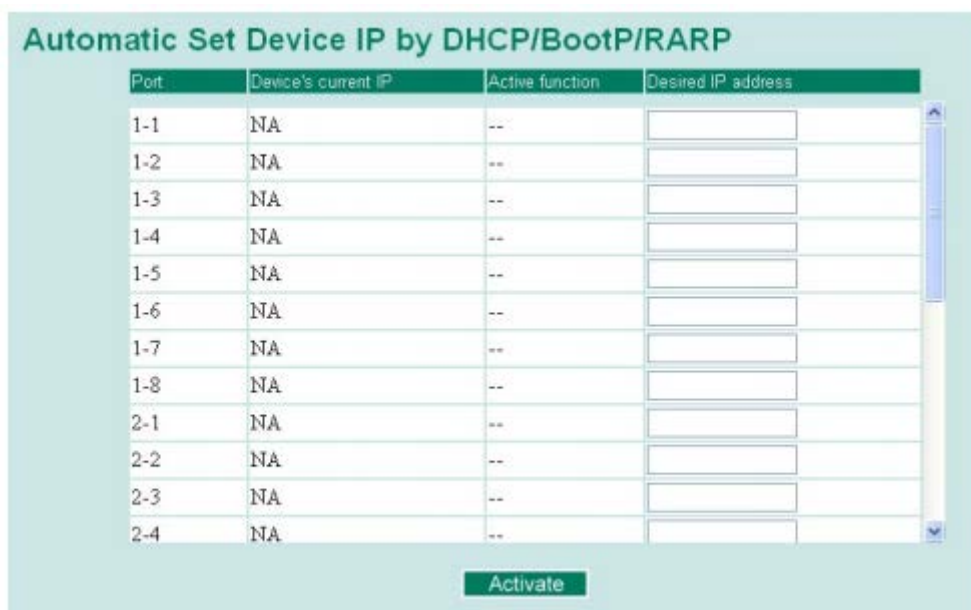
Настройте функцию **Set Device IP** либо с консоли, либо через web-обозреватель. В любом из этих случаев, Вам просто необходимо ввести желаемый IP-адрес (**Desired IP**) для каждого порта.

Шаг 3

Не забудьте активировать настройки

- При использовании web-обозревателя активируйте настройки нажатием на кнопку **Activate**.
- При использовании консоли выделите **Activate** и нажмите **Enter**. Вы получите сообщение **Set device IP settings are now active! (Press any key to continue)**.

Automatic "Set Device IP" by DHCP/BootP/RARP (Авт ома т ическая наст ройка функции «Set Device IP» с помощью DHCP/BootP/RARP-сервера)



Desired IP Address (Желаемый IP-адрес)

Параметр	Описание	Значение по умолчанию
IP Address <i>IP-адрес</i>	Установите желаемый IP-адрес для подключенных устройств.	Нет

Наст ройка функции DHCP Relay Agent

Функция DHCP Relay Agent позволяет отправлять широковещательные DHCP-сообщения через маршрутизаторы. Данная функция позволяет клиентам получать IP-адреса с DHCP-сервера, находящегося в удаленной подсети, или не находящегося в локальной подсети.

DHCP Relay Agent (Option 82)

Опция 82 используется агентом ретрансляции, чтобы вставлять дополнительную информацию в DHCP-запрос клиента. Информация Relay Agent Information вставляется агентом ретрансляции DHCP при пересылке клиентских DHCP-пакетов на DHCP-сервер. Серверы могут распознавать опции Relay Agent Information и использовать информацию для присвоения IP-адресов клиентам.

Когда на коммутаторе включена опция 82, абонентское устройство идентифицируется с помощью порта коммутатора, через который он подключается к сети (в дополнение к его MAC-адресу). В локальной сети абонентского устройства к одному порту коммутатора могут быть подключены и определены несколько хостов доступа.

Опция 82 состоит из двух частей, Circuit ID (ID канала) и Remote ID (удаленный ID), которые определяют отношения между IP-адресом конечного устройства и DHCP-сервером Option 82.

Circuit ID представляет собой 4-байтовое число, сгенерированное Ethernet-коммутатором – комбинация физического номера порта и VLAN ID. Формат Circuit ID показан ниже:

FF-VV-VV-PP

Где первый байт "FF" – это "01", второй и третий байт "VV-VV" – идентификатор VLAN-порта в шестнадцатеричном формате и последний байт "PP" – это номер порта в шестнадцатеричном формате. Например:

01-00-0F-03 – “Circuit ID” порта 3 с VLAN ID 15.

Remote ID идентифицирует агента ретрансляции и может быть:

1. IP-адресом агента ретрансляции;
2. MAC-адресом агента ретрансляции;
3. Комбинацией IP-адреса и MAC-адреса агента ретрансляции;
4. Определенной пользователем строкой.

DHCP Relay Agent

Server IP Address

1st Server:

2nd Server:

3rd Server:

4th Server:

DHCP Option 82

Enable Option 82

Type: IP

Value: 192.168.127.253

Display: 00A87FFD

DHCP Function Table

Port	Circuit-ID	Option 82
1-1	01000101	<input type="checkbox"/> Enable
1-2	01000102	<input type="checkbox"/> Enable
1-3	01000103	<input type="checkbox"/> Enable
1-4	01000104	<input type="checkbox"/> Enable
1-5	01000105	<input type="checkbox"/> Enable
1-6	01000106	<input type="checkbox"/> Enable
1-7	01000107	<input type="checkbox"/> Enable

Activate

Server IP Address (IP-адрес сервера)

1st Server (Первый сервер)

Параметр	Описание	Значение по умолчанию
IP Address for the 1st DHCP server <i>IP-адрес первого DHCP-сервера</i>	IP-адрес первого DHCP-сервера, к которому коммутатор пытается получить доступ.	Нет

2nd Server (Второй сервер)

Параметр	Описание	Значение по умолчанию
IP Address for the 2nd DHCP server <i>IP-адрес второго DHCP-сервера</i>	IP-адрес второго DHCP-сервера, к которому коммутатор пытается получить доступ.	Нет

3rd Server (Третий сервер)

Параметр	Описание	Значение по умолчанию
IP Address for the 3rd DHCP server <i>IP-адрес третьего DHCP-сервера</i>	IP-адрес третьего DHCP-сервера, к которому коммутатор пытается получить доступ.	Нет

4th Server (Четвёртый сервер)

Параметр	Описание	Значение по умолчанию
IP Address for the 4th DHCP server <i>IP-адрес четвертого DHCP-сервера</i>	IP-адрес четвертого DHCP-сервера, к которому коммутатор пытается получить доступ.	Нет

DHCP Option 82**Enable Option 82 (Включение опции 82)**

Параметр	Описание	Значение по умолчанию
<i>Включена</i> или <i>выключена</i>	Включает или выключает функцию DHCP Option 82	<i>Выключена</i>

Type (Тип)

Параметр	Описание	Значение по умолчанию
IP	В качестве удаленного ID использует IP-адрес коммутатора.	IP
MAC	В качестве удаленного ID использует MAC-адрес коммутатора.	
Client-ID	В качестве удаленного ID использует комбинация IP-адреса и MAC-адреса коммутатора	
Other <i>Другое</i>	Используется назначенный пользователем ID.	

Value (Значение)

Параметр	Описание	Значение по умолчанию
Макс.12 символов	Отображает значение, которое было установлено. Заполните это поле, если тип был установлен в значение Other.	Switch IP address <i>IP-адрес коммутатора</i>

Display (Отображение)

Параметр	Описание	Значение по умолчанию
<i>только чтение</i>	Шестнадцатеричное значение на DHCP-сервере для Remote-ID. Это значение генерируется автоматически, в соответствии с полем Value. Пользователи не могут изменить его.	COA87FFD

DHCP Function Table (Таблица функций DHCP)**Enable**

Параметр	Описание	Значение по умолчанию
<i>Включена</i> или <i>выключена</i>	Включает или выключает функцию DHCP Option 82 для этого порта.	<i>Выключена</i>

Диагнос

Т ика

Коммутатор Моха обеспечивает три важных для администратора инструмента для диагностики сети.

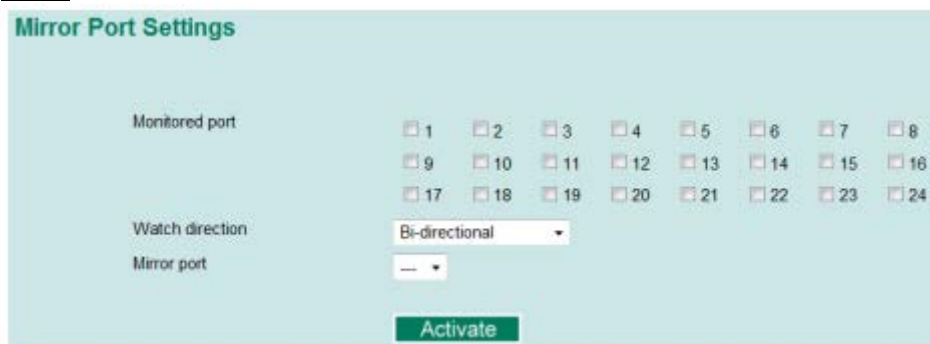
Зеркалирование порт а (Mirror Port)

Функция зеркалирования порта (**Mirror Port**) может быть использована для мониторинга данных, транслируемых через определенный порт. Это осуществляется путем настройки другого порта (порт зеркалирования) на получение данных, исходящих или поступающих и исходящих с порта, мониторинг которого производится. Это позволяет администратору следить за сетевой активностью порта.

Обратите внимание, что существует два типа настроек зеркалирования порта, тип настроек зависит от конкретной модели коммутатора. В настройках коммутаторов Типа 1 поддерживаются функции зеркалирования multi-to-one и one-to-one. В настройках коммутаторов Типа 2 поддерживается только функция зеркалирования one-to-one.

Тип	Поддерживаемые модели
Типе 1 Тип 1	EDS-728/828, IKS-6726/6726-8PoE/6728/G6524/G6824, серия ICS-G7000
Типе 2 Тип 2	Серия EDS 400A/500A/600, EDS-P506A-4PoE/P510/P510A-8PoE/G509

Тип 1

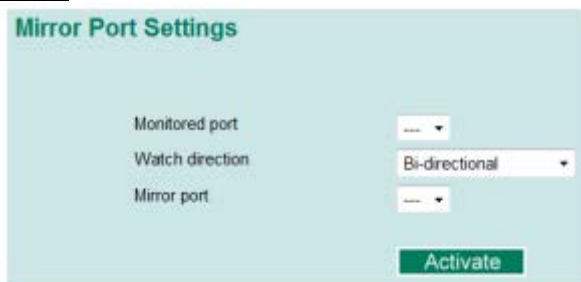


Mirror Port Settings (Настройки функции Mirror Port)

Параметр	Описание
Monitored Port <i>Отслеживаемый порт</i>	Выберите номера портов, чья сетевая активность будет отслеживаться.
Watch Direction <i>Вариант отслеживания</i>	Выберите один из следующих вариантов отслеживания: <ul style="list-style-type: none">• Input data stream: Выберите этот вариант для отслеживания только входящих пакетов данных.• Output data stream: Выберите этот вариант для отслеживания только исходящих пакетов данных.• Bi-directional: Выберите этот вариант для отслеживания и входящих, и исходящих пакетов данных.
Mirror Port <i>Зеркалирование на порт</i>	Выберите номер порта, который будет осуществлять отслеживание сетевой активности порта Monitored Port.

Примечание: В настройках коммутаторов Типа 1 пользователи могут выбрать для функции Mirror Port несколько отслеживаемых портов.

Тип 2



Параметр	Описание
Monitored Port <i>Отслеживаемый порт</i>	Выберите номер порта, чья сетевая активность будет отслеживаться.
Watch Direction <i>Вариант отслеживания</i>	Выберите один из следующих вариантов отслеживания: <ul style="list-style-type: none">• Input data stream: Выберите этот вариант для отслеживания только входящих пакетов данных.• Output data stream: Выберите этот вариант для отслеживания только исходящих пакетов данных.• Bi-directional: Выберите этот вариант для отслеживания и входящих, и исходящих пакетов данных.
Mirror Port <i>Зеркалирование на порт</i>	Выберите номер порта, который будет осуществлять отслеживание сетевой активности порта Monitored Port.

Примечание: В настройках коммутаторов Типа 2 пользователи могут выбрать для функции Mirror Port только один отслеживаемый порт.

Ping



Функция **Ping** использует команды *ping* для обеспечения пользователей простым, но мощным инструментом устранения неполадок сети. Уникальная особенность этой функции в том, что даже если команда *ping* введена пользователем с клавиатуры компьютера, настоящая команда *ping* будет передана от самого коммутатора Моха. Таким образом, пользователь может отправлять команды *ping* через порты коммутатора.

Для использования этой функции введите желаемый IP-адрес и нажмите **Enter** при управлении через последовательную консоль, или кликните **Ping** при использовании web-обозревателя.

Функция LLDP

Введение

LLDP (Link Layer Discovery Protocol) – протокол коммутаторов 2 уровня модели OSI, описанный в стандарте IEEE 802.11AB. Функция LLDP позволяет каждому сетевому устройству, такому как управляемый коммутатор Моха, периодически отправлять информацию о себе и своей конфигурации своим соседям.



Благодаря этому, все устройства с функцией LLDP постоянно получают информацию о состоянии и конфигурации друг друга, а с функцией SNMP эта информация также может быть передана программному обеспечению Моха для автоматического отображения топологии и настройки сети, **MXview**.

С помощью web-обозревателя пользователь может включить/отключить функцию LLDP и установить интервал передачи информации. Кроме того, можно просматривать список соседей каждого коммутатора. Самое главное, включенная функция LLDP позволяет программному обеспечению Моха MXview автоматически отображать топологию сети и детали настройки системы, такие как VLAN и Trunking.

LLDP Settings (Настройка функции LLDP)



General Settings (Общие настройки)

LLDP

Параметр	Описание	Значение по умолчанию
Enable or Disable <i>Включена или выключена</i>	Включает или выключает функцию LLDP.	Enable <i>Включена</i>

Message Transmit Interval (Интервал отправки сообщений)

Параметр	Описание	Значение по умолчанию
5...32768 секунд	Установите интервал отправки LLDP-сообщений (в секундах).	30 (секунд)

LLDP Table (Таблица LLDP)

Таблица LLDP отображает следующую информацию:

Port: Номер порта, подключенного к соседнему устройству.

Neighbor ID: Уникальное свойство (Обычно – MAC-адрес), определяющее соседнее устройство.

Neighbor Port: Номер порта соседнего устройства.

Neighbor Port Description: Текстовое описание интерфейса соседнего устройства.

Neighbor System: Имя хоста соседнего устройства.

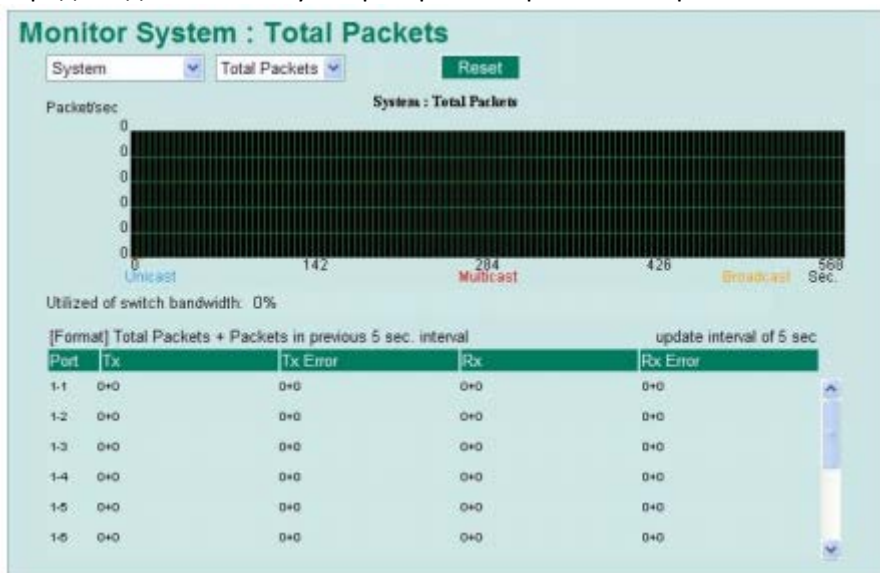
Использование функции мониторинга

Вы можете осуществлять мониторинг статистики в режиме реального времени с помощью web-обозревателя или последовательной консоли.

Мониторинг коммутатора

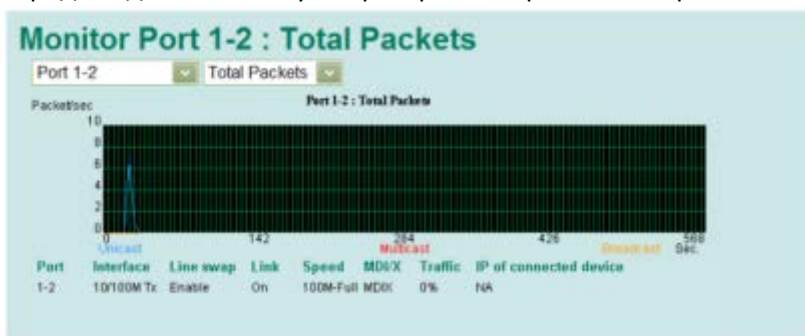
Получите доступ к мониторингу, выбрав раздел **System** в левом вертикальном меню. Monitor by System позволяет пользователю увидеть график, показывающий общую активность передачи данных всех портов коммутатора Моха. Выберите одну из 4 опций – **Total Packets, TX Packets, RX**

Packets, Error Packets для просмотра активности пакетов определенного типа. Не забудьте, что TX пакеты – это пакеты, отсылаемые коммутатором, RX пакеты – это пакеты, полученные от подключенных устройств, Error Packets – это пакеты, не прошедшие алгоритм проверки на ошибки TCP/IP. Опция Total Packets показывает график активности всех типов пакетов, TX, RX и TX Error, RX Error Packets. Активность передачи данных отражена на осях графика **Packets/s** (т.е. число пакетов в секунду или pps) и **sec.** (секунды). Фактически, на одном и том же графике показаны три кривые: пакеты **Uni-cast** (красным), пакеты **Multi-cast** (зеленым) и пакеты **Broad-cast** (синим). График обновляется каждые несколько секунд, позволяя пользователю анализировать активность передачи данных коммутатора в режиме реального времени.



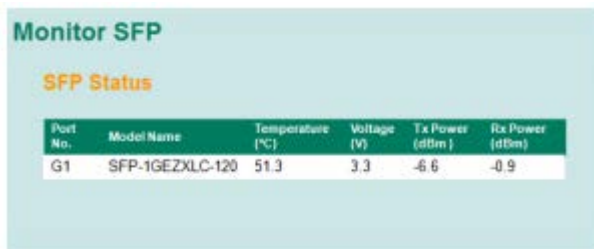
Мониторинг порта

Получите доступ к функции Monitor by Ports, выбрав из левого списка раздел **ALL 10/100M or 1G Ports** или **Port i**, в котором i=1, 2, ..., G2. Опция **Port i** идентична функции Monitor by System, о которой шла речь выше и которая используется для мониторинга All Packets, TX Packets, RX Packets или Error Packets, а в данном случае для мониторинга конкретного порта. Опция **All Ports** показывает активность конкретного порта, которую Вы можете увидеть с помощью функции Console Monitor, описанной выше. Опция **All Ports** отражена с помощью трех вертикальных столбцов для каждого порта. Высота столбца соответствует **Packets/s** для данного типа пакетов в момент времени просмотра. Столбец увеличивается и уменьшается, благодаря чему пользователь может судить об изменении скорости передачи данных по порту. Синий столбец показывает статистику по **Uni-cast** пакетам, красный – по **Multi-cast**, оранжевый – по **Broad-cast**. График обновляется каждые несколько секунд, позволяя пользователю анализировать активность передачи данных коммутатора в режиме реального времени.



Мониторинг SFP-модулей

Оптоволокно обычно используется для передачи данных на большие расстояния. Но устранение проблем при авариях на волоконно-оптическом кабеле на удаленных объектах является очень дорогостоящим. Для решения этой проблемы промышленные Ethernet-коммутаторы Moxa обладают функциями цифровой диагностики и мониторинга SFP-модулей Moxa с оптоволокном и позволяют пользователям измерять параметры оптики и ее производительность из центра управления. Данная функция может значительно облегчить процесс поиска неисправностей на оптоволоконных линиях и сократить расходы на отладку.



The screenshot shows a web interface titled "Monitor SFP" with a sub-section "SFP Status". It contains a table with the following data:

Port No.	Model Name	Temperature (°C)	Voltage (V)	Tx Power (dBm)	Rx Power (dBm)
G1	SFP-1GEZXLC-120	51.3	3.3	-6.6	-0.9

Параметр	Описание
Port No. <i>Номер порта</i>	Номер порта коммутатора, к которому подключен SFP-модуль.
Model Name <i>Модель</i>	Модель SFP-модуля.
Temperature (°C) <i>Температура (°C)</i>	Рабочая температура SFP-модуля.
Voltage (V) <i>Напряжение питания (В)</i>	Напряжение питания SFP-модуля.
Tx power (dBm) <i>Мощность Tx (дБм)</i>	Мощность сигнала, передаваемого по оптоволоконному кабелю.
Rx power (dBm) <i>Мощность Rx (дБм)</i>	Мощность сигнала, получаемого по оптоволоконному кабелю.

Примечание:

Возможны погрешности между реальными данными и данными измерений.

Параметр	Погрешность
Temperature (°C) <i>Температура (°C)</i>	± 3°C
Voltage (V) <i>Напряжение питания (В)</i>	± 0.1 В
Tx power (dBm) <i>Мощность Tx (дБм)</i>	± 3 дБ
Rx power (dBm) <i>Мощность Rx (дБм)</i>	± 3 дБ

Использование таблицы MAC-адресов

В данном разделе речь пойдет о таблице MAC-адресов коммутатора Moxa.

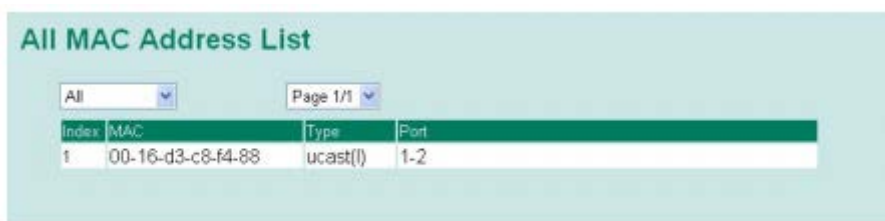


Таблица может быть настроена на показ следующих групп MAC-адресов (группы адресов доступны в выпадающем списке):

ALL	Выберите данный параметр для показа всех MAC-адресов коммутатора Мохы.
ALL Learned	Выберите данный параметр для показа MAC-адресов, изученных коммутатором в процессе работы.
ALL Static Lock	Выберите данный параметр для показа статически заблокированных MAC-адресов на коммутаторе Мохы.
ALL Static	Выберите данный параметр для показа статических, статически заблокированных и статических широковещательных MAC-адресов коммутатора Мохы.
ALL Static Multicast	Выберите данный параметр для показа статических широковещательных MAC-адресов коммутатора Мохы.
Port x	Выберите данный параметр для показа всех MAC-адресов определенных портов.

Таблица будет включать следующие данные:

MAC	MAC-адрес
Type	Тип MAC-адреса
Port	Порт, которому принадлежит MAC-адрес

Использование списка управления доступом (ACL)

Примечание:

Список управления доступом доступен в коммутаторах 3 уровня.

Использование списка управления доступом (ACL) увеличивает удобство и безопасность управления сетью.

ACL предоставляет возможность фильтрации трафика для входящих или исходящих пакетов. Список управления доступом коммутаторов Мохы позволяет управлять критериями фильтрации для различных протоколов и предоставляет пользователям возможность индивидуальной настройки критериев фильтрации. Например, пользователи могут запретить доступ к конкретному источнику или получателю IP/MAC-адресов.

Интерфейс управления списком управления доступом очень прост в использовании. Пользователи могут быстро устанавливать правила фильтрации, управлять приоритетами правил, а также просматривать общие настройки на странице интерфейса.

Концепция функции ACL

Что такое ACL?

Список управления доступом является основным способом для фильтрации трафика входящих и исходящих пакетов. Данная функция может изучать информацию о каждом Ethernet-пакете и принимать необходимые меры. Коммутаторы Мохы 3 уровня обеспечивают возможность полноценной фильтрации. Критерии списка управления доступом могут включать в себя IP-адрес

пакетов, MAC-адрес пакетов источника или приемника, IP-протоколы или любую другую информацию. Функция ACL может проверить эти критерии, чтобы решить, следует разрешить или запретить доступ пакету.

Преимущества функции ACL

Функция ACL осуществляется в зависимости от типа интерфейса, от направления пакета и от возможности фильтрации протокола. Данные возможности могут обеспечить базовую защиту сети путем фильтрации определенных пакетов. Основные преимущества ACL заключаются в следующем:

- **Управление полномочием хостов:** Функция ACL может ограничивать доступ определенным устройствам с помощью фильтрации MAC-адресов. Пользователь может запретить все или только некоторые пакеты, поступающие от конкретных устройств.
- **Управление полномочием подсети:** Настройка правил фильтрации для определенных IP-адресов подсети. Функция ACL может ограничить пакеты, отправляемые или получаемые от определенных подсетей.
- **Безопасность сети:** Вопрос об обеспечении безопасности сети очень актуален. Функция ACL может обеспечить базовую защиту, которая работает аналогично Ethernet-шлюзу безопасности (firewall).
- **Управление потоком трафика с помощью фильтрации определенных протоколов:** Функция ACL может фильтровать определенные IP-протоколы (TCP- или UDP-пакеты).

Как работает функция ACL?

Структура ACL основана на списках доступа. Каждый список доступа представляет собой фильтр. Когда пакет входит или выходит из коммутатора, ACL будет сравнивать пакет с правилами в списках доступа, начиная с первого правила. Если пакет запрещен или разрешен первым правилом, коммутатор будет пропускать или передавать этот пакет напрямую без проверки остальной части с более низким приоритетом правил. Другими словами, список управления доступом обладает свойством «Индекс приоритета» (“Priority Index”) для определения приоритета правила.

Есть два типа настроек для ACL: настройка *списка (list)* и настройка *правила (rule)*. Для создания списка управления доступом необходимы следующие параметры *списка*: имя, индекс приоритета, тип фильтра и порты, к которым нужно применить данные настройки. После создания каждый список управления доступом имеет свои собственные настройки правил. Индекс приоритета представляет собой приоритет имен в списке доступа. Имена в индексе приоритета 1 (Priority Index 1) имеют первый приоритет в фильтрации пакетов. Индекс приоритета настраивается каждый раз, когда пользователю необходимо изменить приоритет. В функции доступны два типа фильтрации пакетов:

- По IP-адресу
- По MAC-адресу

Тип фильтрации указывает на то, как следует проверять пакеты – по MAC-адресу или по IP-адресу. Дальнейшие настройки фильтра будут зависеть от его типа. После настройки фильтрации выберите номера портов, к которым вы хотите применить фильтр. Также можно выбрать, к какому трафику (входящему или исходящему) применять фильтр.

Вы можете также создавать правила уже после добавления нового списка управления доступом. Каждая группа ACL поддерживает 10 правил. Правила могут фильтровать пакеты по IP/MAC-адресу источника или получателя, IP-протоколу, порту TCP или UDP, типу Ethernet-кадра или по VLAN ID. После того как установлены все правила, список ACL будет фильтровать пакеты по правилу с наивысшим индексом приоритета (меньше номер означает выше приоритет). Если правило запрещает или разрешает доступ пакету, пакет будет соответственно отброшен или передан.

Access Control List Settings (Настройки списка управления доступом)

Создание списка управления доступом начинается на странице Access Control List Setting.

The screenshot shows the 'Access Control List Setting' interface. It includes a table with columns 'Priority Index', 'Name', and 'Filter'. Below the table, there are input fields for 'Priority Index' (set to 5), 'Name', and 'Filter' (set to 'MAC Base'). Below these fields are two port mapping tables: 'Ingress Port Map' and 'Egress Port Map', each with a grid of checkboxes for ports 1 through 20. At the bottom, there are 'Add' and 'Activate' buttons.

На этой странице вы можете настроить два параметра:

Добавить/изменить список управления доступом

Эта функция позволяет добавить новый список управления доступом или изменить существующий. Настройка функции зависит от индекса приоритета (Priority Index), который выбирает пользователь. Если индекс приоритета по-прежнему пуст, вы можете начать с создания нового списка управления доступом.

Параметры для редактирования:

- **Priority Index** (Индекс приоритета): ACL проверяет последовательность правил на основе этого показателя. Меньший индекс обладает более высоким приоритетом для фильтрации пакетов. Если пакет отфильтрован списком доступа с более высоким приоритетом, то списки доступа с более низким приоритетом не будут реализованы.

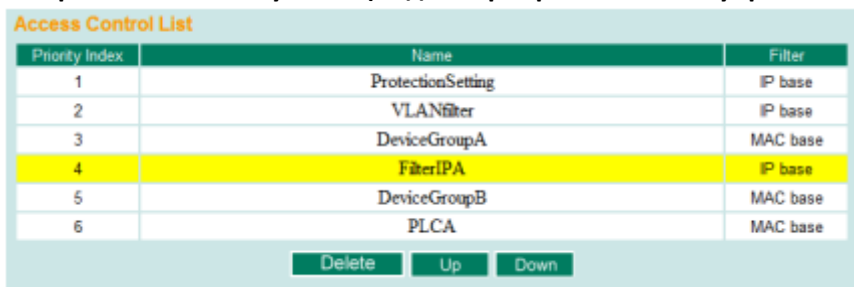
Примечание: Индекс приоритета не является одинаковым для каждого списка. Он меняется при изменении приоритета различных списков управления доступом.

Максимальный индекс приоритета – 16.

- **Name** (Имя): Вы можете назвать список управления доступом в этом разделе. Все списки доступа должны иметь уникальное имя.
- **Filter** (Фильтр): Выберите тип фильтрации: по IP- или MAC-адресу. Детальную настройку можно произвести на странице **Access Control Rule Settings**.
- **Ingress Port Map/Egress Port Map** (Отображение входных/выходных портов): Вы можете выбрать, к каким портам будут применены правила. Состояние входных/выходных портов использует логику **OR**. Это означает, что для проверки пакет должен соответствовать хотя бы одному параметру (входной или выходной порта).

Если выбранный индекс приоритета уже есть в списке управления доступом, Вы можете изменять параметры, описанные выше. После настройки нажмите **Activate** для подтверждения. После этого новый список появится в таблице **Access Control List**.

Настройка ACL Priority Index (индекс приоритета списка управления доступом)



Priority Index	Name	Filter
1	ProtectionSetting	IP base
2	VLANfilter	IP base
3	DeviceGroupA	MAC base
4	FilterIPA	IP base
5	DeviceGroupB	MAC base
6	PLCA	MAC base

Buttons: Delete, Up, Down

Изменять установленные приоритеты списков управления доступом очень легко. Компания Моха создала простой интерфейс, который позволит вам быстро установить приоритет. Для этого выполните три шага, описанные ниже:

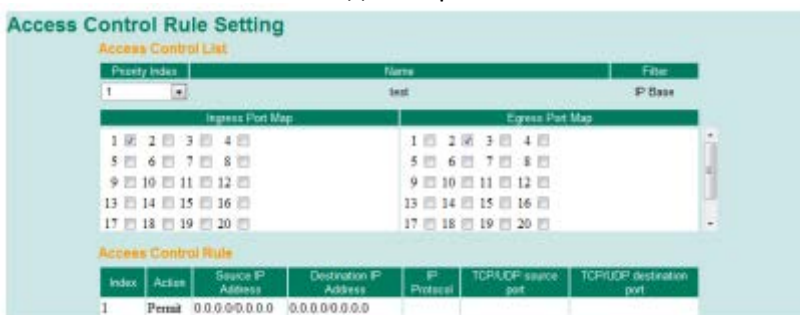
Шаг 1: Выберите список.

Шаг 2: Нажмите кнопку **Up/Down** (Вверх/Вниз) для установки последовательности. Параметр Priority Index (Индекс приоритета) будет меняться в зависимости от позиции в списке.

Шаг 3: Нажмите **Activate** для подтверждения настроек.

Access Control Rule Settings (Настройка правил управления доступом)

На этой странице Вы можете настраивать правила списка управления доступом. Каждый список ACL может включать в себя до 10 правил.



Priority Index	Name	Filter
1	test	IP Base

Ingress Port Map				Egress Port Map			
1	2	3	4	1	2	3	4
5	6	7	8	5	6	7	8
9	10	11	12	9	10	11	12
13	14	15	16	13	14	15	16
17	18	19	20	17	18	19	20

Index	Action	Source IP Address	Destination IP Address	IP Protocol	TCP/UDP source port	TCP/UDP destination port
1	Permit	0.0.0.0/0.0.0.0	0.0.0.0/0.0.0.0			

Во-первых, выберите список, в котором Вы хотели бы изменить параметр Priority Index (Индекс приоритета). Ingress/Egress Port map (Отображение входных/выходных портов) будет отображать настройки портов.

Примечание:

На этой странице также доступна настройка карты портов. Любые изменения будут менять настройки списка управления доступом.

Правила управления доступом отображают настройки параметров в зависимости от используемого типа фильтрации.

IP-Based (По IP-адресу)

После настройки нажмите **Add**, чтобы добавить правило в список. Затем нажмите **Activate**, чтобы активировать настройки.

Access Control Rule

Index	Action	Source IP Address	Destination IP Address	IP Protocol	TCP/UDP source port	TCP/UDP destination port
1	Permit	0.0.0.0/0.0.0.0	0.0.0.0/0.0.0.0			

Action:

Source IP Address:

Source IP Address Mask:

Destination IP Address:

Destination IP Address Mask:

IP Protocol: (0x00 ~ 0xFF)

TCP/UDP Source Port: (1~65535)

TCP/UDP Destination Port: (1~65535)

- **Action (Действие):** Запрещать или разрешать доступ, если критерий правила выполняется.
- **Source IP Address/Source IP Address Mask (IP-адрес источника/Маска IP-адреса источника):** Определяет правило IP-адреса. Используя маску, Вы можете назначить определенные диапазоны подсети для фильтрации. Вы можете указать как устройство-источник, так и устройство-получатель пакета. Выберите **Any**, если не хотите использовать данный критерий.
- **IP Protocol (IP-протокол):** Выберите тип протоколов для фильтрации: **ICMP, IGMP, IP over IP, TCP** и **UDP**.
- **TCP/UDP Source Port, TCP/UDP Destination Port (Порт источника TCP/UDP, порт принимающего устройства TCP/UDP):** Если TCP или UDP выбраны в качестве протокола фильтрации, данный параметр позволяет выбрать номера портов для фильтрации.

После того, как настройка завершена, нажмите **Add**, чтобы добавить правило в список. Затем нажмите **Activate**, чтобы активировать настройки.

MAC-Based (На основе MAC-адреса)

Access Control Rule

Index	Action	Source MAC Address	Destination MAC Address	Ether Type	VLAN ID

Action:

Source MAC Address: (00:XX:XX:XX:XX:XX)

Source MAC Address Mask: (00:XX:XX:XX:XX:XX)

Destination MAC Address: (00:XX:XX:XX:XX:XX)

Destination MAC Address Mask: (00:XX:XX:XX:XX:XX)

Ether Type: (0x0000 ~ 0xFFFF)

VLAN ID: (1 - 4094)

- **Action (Действие):** Запрещать или разрешать доступ, если критерий правила выполняется.
- **Source MAC Address/Source MAC Address Mask (MAC-адрес источника/Маска MAC-адреса источника):** Определяет правило MAC-адреса. Используя маску, Вы можете назначить определенные диапазоны подсети для фильтрации. Это позволяет проверить источник пакета или принимающее пакет устройство. Выберите **Any**, если не хотите использовать данный критерий.
- **Ethernet Type (Тип Ethernet-протокола):** Выберите тип Ethernet-протокола для фильтрации: **IPv4, ARP, RARP, IEEE802.1Q, IPv6, IEE802.3, PROFIENT, LLDP** или **IEEE1588**.
- **VLAN ID:** Введите VLAN ID, по которому осуществлять фильтрацию.

После того, как настройка завершена, нажмите **Add**, чтобы добавить правило в список. Затем нажмите **Activate**, чтобы активировать настройки.

Port Configuration Display (Отображение настроек порта)

На странице Port Configuration Display отражены все настройки всех списков ACL. Здесь Вы можете увидеть правила **Ingress** (входного) порта, **Egress** (выходного) порта или **Priority Index** (Индекс приоритета). Нажмите на выпадающее меню для выбора порта (Port) или индекса приоритета (Priority Index), все правила будут отображены в таблице.

Port Configuration Display

Select Port

Port	Direction
1	Ingress

Access Control List

Priority Index	Name	Filter
1	test	IP Base

Access Control Rule

Index	Action	Source IP Address	Destination IP Address	IP Protocol	TCP/UDP source port	TCP/UDP destination port
1	Permit	0.0.0.0/0.0.0.0	0.0.0.0/0.0.0.0			

Примечание:

Для серий EDS-828 и PT-7828 существуют два ограничения для настроек списков ACL. На основании типа входного порта правил списка ACL, существует два типа ограничения количества настроек.

Ingress Port Map				Egress Port Map			
1-1	<input type="checkbox"/>	1-2	<input type="checkbox"/>	1-3	<input type="checkbox"/>	1-4	<input type="checkbox"/>
3-1	<input type="checkbox"/>	3-2	<input type="checkbox"/>	3-3	<input type="checkbox"/>	3-4	<input type="checkbox"/>
4-1	<input type="checkbox"/>	4-2	<input type="checkbox"/>	4-3	<input type="checkbox"/>	4-4	<input type="checkbox"/>
5-1	<input type="checkbox"/>	5-2	<input type="checkbox"/>	5-3	<input type="checkbox"/>	5-4	<input type="checkbox"/>
6-1	<input type="checkbox"/>	6-2	<input type="checkbox"/>	6-3	<input type="checkbox"/>	6-4	<input type="checkbox"/>

Ограничение 1 типа:

Когда правила содержат входные порты Fast Ethernet (FE), **общее количество настроек в правилах не должно превышать 160.**

Ограничение 2 типа:

Когда правила содержат входные порты Gigabit Ethernet (GE) или не содержат входных портов вообще, **общее количество настроек не должно превышать 40.**

Пример 1 для 1 типа

Правило А включает 3 входных порта FE и 4 выходных порта FE, следовательно, количество настроек будет $3 \times 4 = 12$.

Правило В включает 5 входных портов FE и 6 выходных портов FE, следовательно, количество настроек будет $5 \times 6 = 30$.

Правило С включает из 7 входных портов FE и 0 выходных портов, следовательно, количество настроек будет равно 7.

Убедитесь, что сумма чисел "12+30+7" не больше, чем 160.

Пример 2 для 2 типа

Правило D включает 1 входной порт GE и 2 выходных порта FE, следовательно, количество настроек будет $1 \times 2 = 2$.

Правило E включает 3 входных порта GE и 4 выходных порта GE, следовательно, количество настроек будет $3 \times 4 = 12$.

Правило F включает 5 входных портов GE и 0 выходных портов, следовательно, количество настроек будет равно 5.

Правило G включает 0 входных портов и 6 выходных портов FE, следовательно, количество настроек будет равно 6.

Правило H включает 0 входных портов и 7 выходных портов GE, следовательно, количество настроек будет равно 7.

Убедитесь, что сумма чисел “2+12+5+6+7” не больше, чем 40.

Пример 3 для 1 и 2 типа

Правило Z включает 3 входных порта FE, 2 входных порта GE и 5 выходных портов GE.

Следовательно, количество настроек для 1 типа будет 3 x 5 = 15, для 2 типа – 2 x 5 = 10.

Убедитесь, что сумма “15” не больше, чем 160.

Убедитесь, что сумма “10” не больше, чем 40.

Примечание:

Коммутаторы серий EDS-828 и PT-7828 предлагают только 6 типов правил ACL.

Примечание:

В коммутаторах серий EDS-828 и PT-7828 фильтры Broadcast и Multicast трафика не поддерживаются на выходных портах в настройках ACL. А Broadcast и Multicast адреса не могут быть установлены, как адрес источника/принимающего устройства.

Использование журнала событий

Index	Bootup	Date	Time	System Startup Time	Event
991	419	--	--	0d0h42m37s	Port 1-2 link off
992	420	--	--	0d0h0m1s	Cold start
993	420	--	--	0d0h0m3s	Port 3-8 link on
994	420	--	--	0d0h1m14s	192.168.127.1 admin Auth. ok
995	420	--	--	0d0h1m54s	Port 3-8 link off
996	421	--	--	0d0h0m1s	Cold start
997	421	--	--	0d0h0m4s	Port 1-2 link on
998	421	--	--	0d0h0m12s	192.168.127.1 admin Auth. ok
999	421	--	--	0d0h53m26s	Configuration change activated
1000	421	--	--	0d0h53m33s	192.168.127.1 admin Auth. ok

Event Log Table (журнал событий) отражает следующую информацию:

Bootup <i>Перезагрузка</i>	Показывает, сколько раз коммутатор был перезагружен или запущен с холодного старта.
Date <i>Дата</i>	Дата обновляется в соответствии с настройками в разделе Basic Setting (Базовые настройки).
Time <i>Время</i>	Время обновляется в соответствии с настройками в разделе Basic Setting (Базовые настройки).
System Startup Time <i>Время запуска системы</i>	Время запуска системы, связанное с событием.
Events <i>События</i>	Возникшие события.

Примечание:

Следующие события будут записаны в Event Log Table Моха (в журнале событий):

- Холодный старт
 - Горячий старт
 - Активированы изменения настроек
 - Перемена питания 1/2 (On→Off, Off→On)
 - Ошибка авторизации
 - Изменение топологии сети
 - Настройки устройства Master некорректные
 - Перегрузка трафика порта
 - Ошибка авторизации dot1x
 - Связь по порту есть/нет
-

Использование функции Syslog

Функция Syslog передаёт журналы событий на syslog-сервер. Функция поддерживает 3 настраиваемых syslog-сервера с возможностью указания их UDP-портов. Когда происходит событие, оно будет отправлено в виде syslog UDP-пакета на указанные серверы системного журнала.

The screenshot shows a configuration interface titled 'Syslog Settings'. It contains three rows, each representing a syslog server. Each row has a text input field for the server IP address and a port selection dropdown menu. The first dropdown menu has '514' selected and '(1-65535)' as the range. Below the port selection, there is a green 'Activate' button.

Syslog Server 1/2/3 (Сервер системных журналов 1/2/3)

Параметр	Описание	Значение по умолчанию
Syslog server <i>Сервер Syslog</i>	Введите IP-адрес syslog-сервера 1/2/3, используемого Вашей сетью.	Нет
Port Destination (1 ... 65535) <i>Порт сервера</i>	Введите номер UDP-порта syslog-сервера 1/2/3.	514

Примечание:

Следующие события будут записаны в Event Log (в журнале событий) коммутатора Моха и отправлены на специальный syslog-сервер:

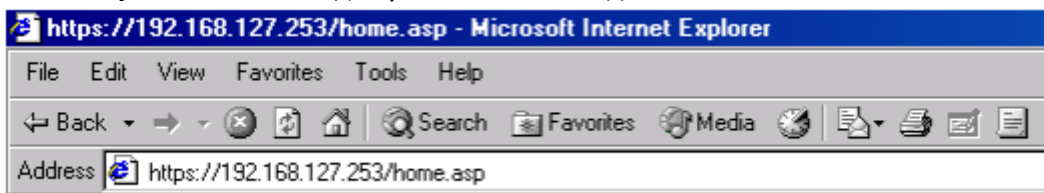
- Холодный старт
 - Горячий старт
 - Активированы изменения настроек
 - Перемена питания 1/2 (On→Off, Off→On)
 - Ошибка авторизации
 - Изменение топологии сети
 - Настройки устройства Master некорректные
 - Перегрузка трафика порта
-

- Ошибка авторизации dot1x
 - Связь по порту есть/нет
-

Использование прот оков HTTPS/SSL

Для обеспечения безопасности доступа по HTTP, коммутаторы Moxa поддерживают протоколы HTTPS/SSL для шифрования всего трафика HTTP. Для получения доступа к web-обозревателю коммутатора Moxa через HTTPS/SSL следуйте инструкции ниже.

1. Откройте Internet Explorer и введите в адресную строку **https://{IP-адрес коммутатора Moxa}**. Нажмите Enter для установления соединения.



2. Появится предупреждающее сообщение о том, что сертификат безопасности выдан компанией, не выбранной в качестве доверенных.



3. Нажмите **Yes** для входа в web-обозреватель коммутатора Moxa и получения доступа к интерфейсу, защищенному с помощью HTTPS/SSL.

Примечание:

Компания Moxa обеспечивает сертификат Root CA. После установки этого сертификата на ваш компьютер или ноутбук, Вы сможете получить доступ к интерфейсу web-обозревателю напрямую, и больше не будете видеть никаких предупреждений. Вы можете загрузить этот сертификат с CD-диска, входящего в комплект поставки коммутатора Moxa.

Утилита настроек коммутатора EDS

Утилита EDS Configurator (Конфигуратор EDS) – это Windows-утилита, используемая для настройки и работы с несколькими коммутаторами Моха. Набор полезных функций поможет Вам обнаружить коммутаторы Моха в той же сети LAN, что и Ваш компьютер (независимо от того, знаете ли Вы их IP-адрес), подсоединиться к коммутатору Моха, чей адрес Вы знаете, изменить настройки одного или нескольких коммутаторов, обновить микропрограммное обеспечение (firmware) коммутаторов. Конфигуратор EDS разработан для обеспечения постоянного и полного контроля над всеми коммутаторами Моха Вашей сети, независимо от их местоположения. Вы можете бесплатно скачать конфигуратор с сайта производителя.

В этой главе рассмотрено:

- Начало работы с конфигуратором EDS
- Широковещательный поиск
- Поиск по IP-адресу
- Обновление микропрограммного обеспечения
- Изменение IP-адреса
- Экспорт настроек
- Импорт настроек
- Разблокировка сервера

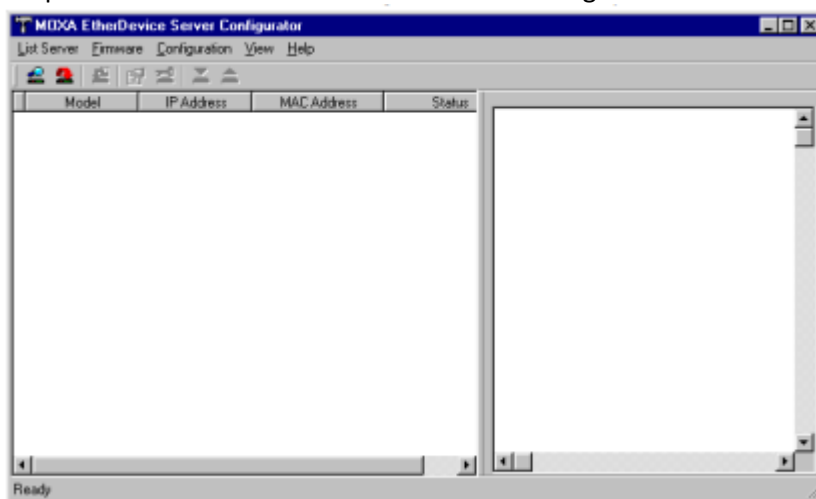
Начало работ ы с Конфигурат ором EDS

Для начала работы с Конфигуратором найдите и запустите файл edscfgui.exe:

- Если Вы разместили файл на рабочем столе Windows, он будет выглядеть, как показано ниже. Для его запуска потребуется дважды кликнуть мышью по иконке.



- Откроется окно MOXA EtherDevice Server Configurator.




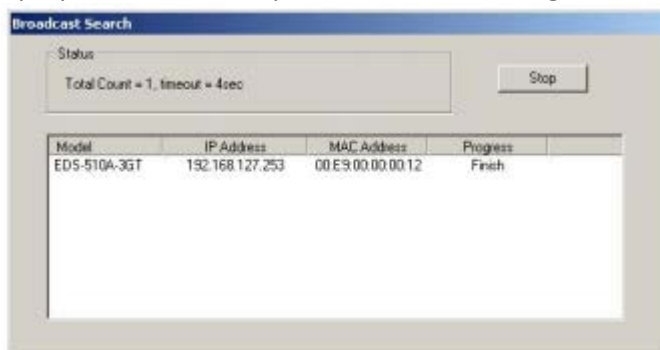
Примечание:

Вы можете скачать конфигуратор с официального сайта производителя – www.moxa.com.

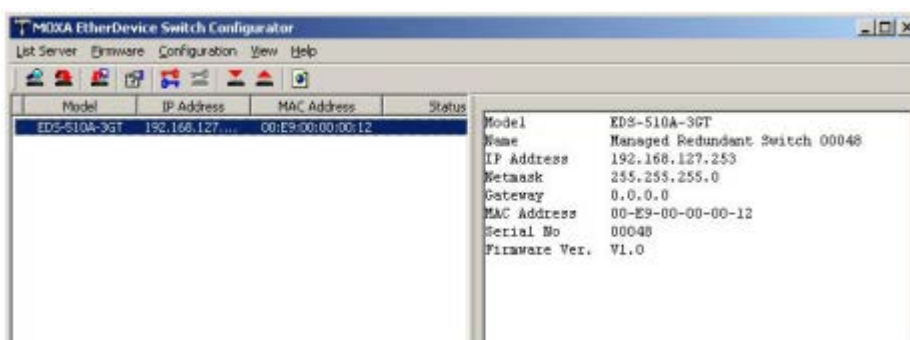
Широковещат ельный поиск

Используйте утилиту **Broadcast Search** для обнаружения всех коммутаторов Мохы в сети LAN. Поскольку поиск производится по MAC-адресу, широковещательный поиск не сможет обнаружить коммутаторы, которые находятся за пределами ПК-хоста сети LAN.

1. Начните с нажатия на иконку  или выберите **Broadcast Search** в меню **List Server**. Откроется окно Broadcast Search, осуществляющее поиск всех коммутаторов сети, а прогресс поиска отобразится в колонке **Progress**.




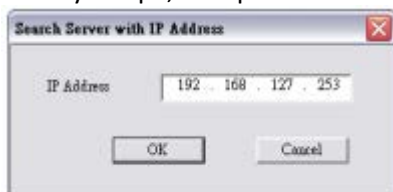
2. После завершения поиска в окне будет представлен полный список обнаруженных коммутаторов.



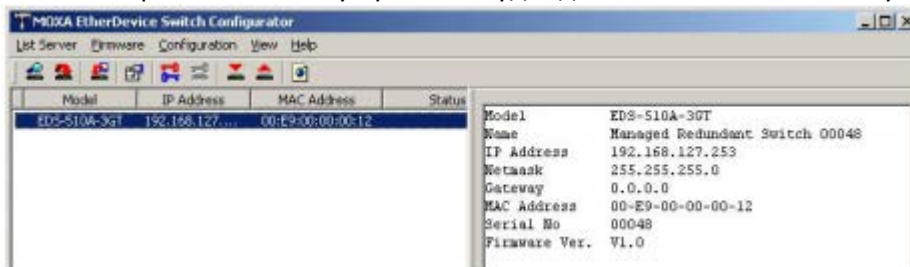
Поиск по IP-адресу

Используйте команду **Search by IP Address** для поиска одного коммутатора. Поиск осуществляется по IP-адресу, поэтому убедитесь, что искомое устройство корректно настроено в своей сети LAN, WAN или Internet.

1. Начните с нажатия на иконку **Specify by IP address**  или выберите **Specify IP address** в меню **List Server**. Откроется окно **Search Server with IP Address**. Введите IP-адрес коммутатора, который Вы хотите найти, и нажмите **OK**.



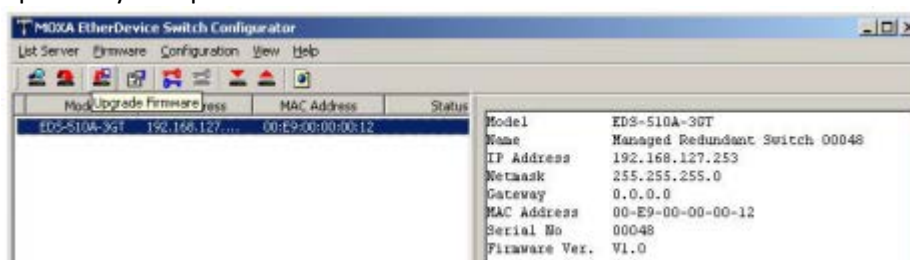
2. После завершения поиска устройство будет добавлено в список коммутаторов сети.




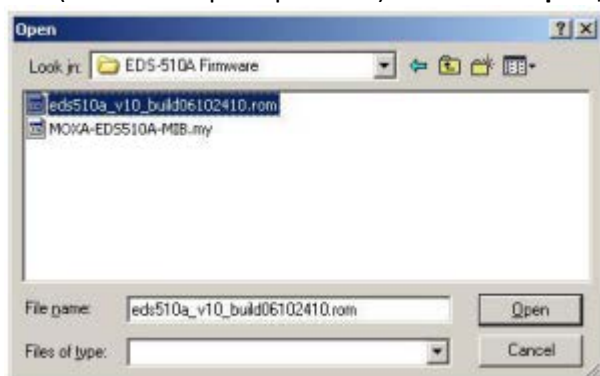
Обновление микропрограммного обеспечения

Обновляйте микропрограммное обеспечение коммутатора Мохы в соответствии с последней версией прошивки. Для обновления встроенного микропрограммного обеспечения (Upgrade Firmware) Вам необходимо:

1. Скачайте *.rom файл обновленной прошивки с сайта www.moxa.com.
2. Кликните на коммутатор (в окне конфигуратора **Moxa EtherDevice Server Configurator**), прошивку которого Вы хотите обновить.




3. Кликните на иконку **Upgrade Firmware**  или выберите **Upgrade** в меню **Firmware**. Если доступ к коммутатору заблокирован, Вам будет предложено ввести имя пользователя и пароль.
4. Используйте окно **Open** для доступа к файлу прошивки, затем выберите нужный *.rom файл (**eds.rom** в примере ниже). Кликните **Open** для запуска процесса обновления.



Изменение IP-адреса


Вы можете использовать функцию **Modify IP Address** для изменения сетевых настроек коммутатора Мохэ.

1. Нажмите на иконку **Modify IP address**  или выберите **Modify IP address** в меню **Configuration**.
2. Откроется окно **Setup Configuration**. Активируйте или деактивируйте DHCP, введите IP-адрес, маску подсети, шлюз, DNS IP. Нажмите **OK** для сохранения изменений.

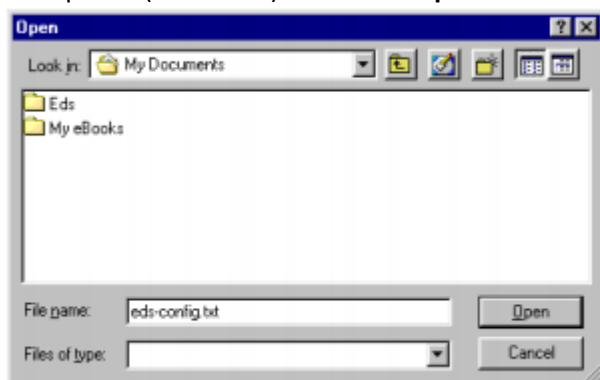


Экспорт настроек

Функция **Export Configuration** используется для сохранения настроек какого-либо коммутатора в текстовом файле.

1. Выберите коммутатор (из списка в левой части окна Конфигуратора), нажмите на иконку **Export**  или выберите **Export Configuration** в меню **Configuration**. Используйте окно

Open для доступа к папке, в которой Вы хотите сохранить файл настроек, а затем введите имя файла (**File name**). Нажмите **Open**.



2. Нажмите на **OK** в появившемся окне **Export configuration to file OK**.




3. Вы можете использовать стандартные текстовые редакторы типа Notepad (Блокнот) для просмотра и внесения изменений в файл настроек.

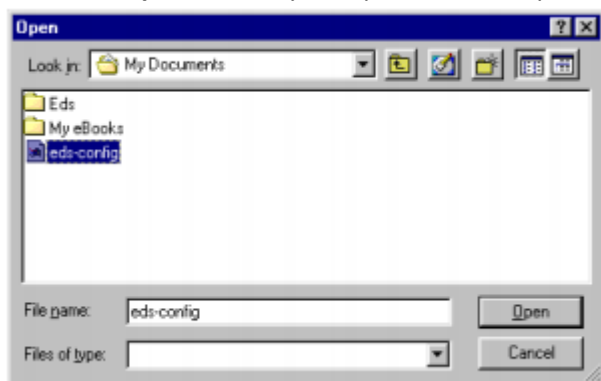


Импорт настроек

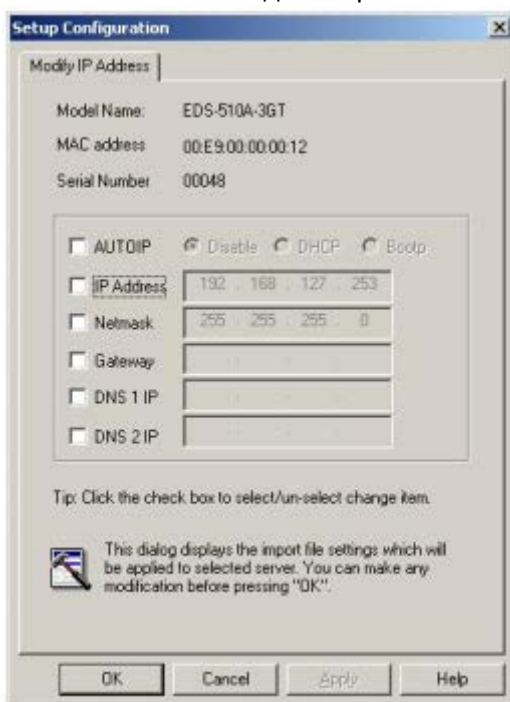
Функция **Import Configuration** используется для импорта настроек из текстового файла. Она используется для присвоения настроек одного коммутатора другому. Необходимо сначала экспортировать настройки нужного коммутатора (как было описано в предыдущем разделе), а затем выполнить импорт настроек.

1. Выберите коммутатор (из списка в левой части окна конфигуратора), нажмите на иконку **Import**  или выберите **Import Configuration** в меню **Configuration**.

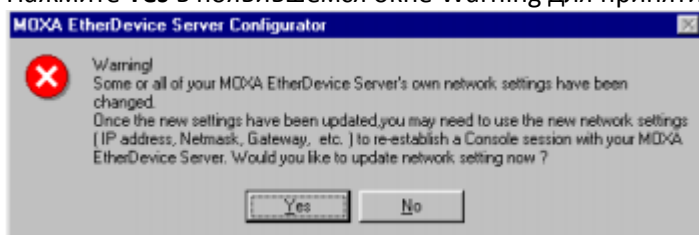
- Используйте окно **Open** для доступа к папке, в которой Вы храните файл настроек, и нажмите **Open** для запуска процесса импорта.



- Появится окно **Setup Configuration** с примечанием в нижней части окна. В окне Вы увидите измененные параметры. Вы можете снова отредактировать параметры, если необходимо, а затем нажмите **OK** для сохранения изменений.



- Нажмите **Yes** в появившемся окне Warning для принятия новых настроек.



Разблокировка сервера

Функция **Unlock Server** (разблокировки сервера) используется для доступа к защищенному паролем коммутатору. В колонке **Status** есть шесть параметров. **Status** показывает, как коммутатор был обнаружен и какой тип защиты имеет.

Шесть возможных статусов представлены ниже (термин **Fixed** был заимствован из терминологии *fixed IP address*):

Locked


Коммутатор защищен паролем, был найден через **Broadcast Search**, в текущей сессии пароль еще не введен.

Unlocked

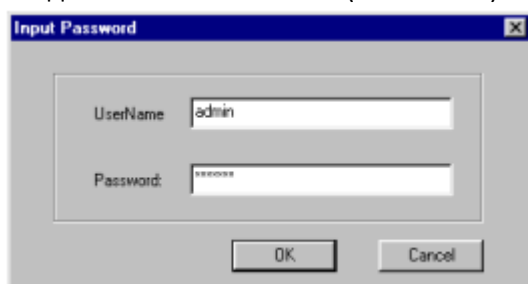
Коммутатор защищен паролем, был найден через **Broadcast Search**, в текущей сессии пароль уже был введен. Значит, в этой сессии для активации различных утилит не потребуется повторное введение пароля.

Blank

Коммутатор не защищен паролем, был найден через **Broadcast Search**.

Следуйте шагам, приведенным ниже, для разблокировки заблокированного коммутатора (т.е. коммутатора со статусом «Locked» или «Fixed Locked»). Выберите коммутатор (из списка в левой части окна конфигуратора), нажмите на иконку **Unlock** , или выберите **Unlock** в меню **Configuration**.

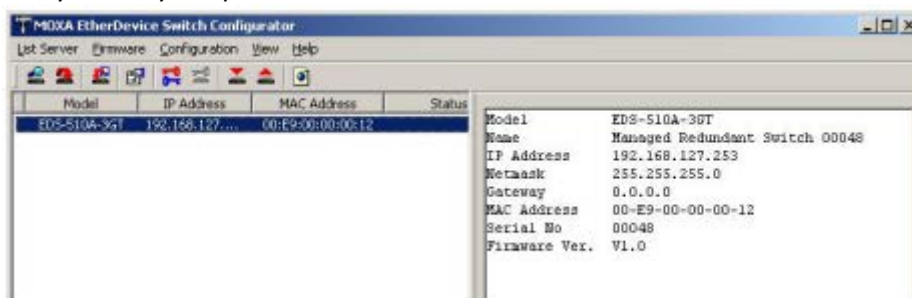
1. Введите имя пользователя (**User Name**) и пароль (**Password**) и нажмите ОК.



2. Когда в окне **Unlock status** состояние в графе Progress сменится на **OK**, нажмите кнопку **Close** в правом верхнем углу окна.



3. Статус коммутатора станет **Unlocked**.



MIB-группы

Коммутатор Moxa поставляется со встроенным SNMP-агентом (Simple Network Management Protocol), который поддерживает trap-сообщения о холодном/горячем запуске, подключении/отключении линии связи, а также RFC 1213 MIB-II.

Стандартные поддерживаемые MIB-группы:

MIB II.1—System Group

sysORTable

MIB II.2—Interfaces Group

ifTable

MIB II.4 – IP Group

ipAddrTable

ipNetToMediaTable

IpGroup IpBasicStatsGroup

IpStatsGroup

MIB II.5—ICMP Group

IcmpGroup

IcmpInputStatus

IcmpOutputStats

MIB II.6—TCP Group

tcpConnTable

TcpGroup

TcpStats

MIB II.7—UDP Group

udpTable

UdpStats

MIB II.10—Transmission Group

dot3

dot3StatsTable

MIB II.11—SNMP Group

SnmpBasicGroup

SnmpInputStats

SnmpOutputStats

MIB II.17—dot1dBridge Group

dot1dBase

dot1dBasePortTable

dot1dStp

dot1dStpPortTable

dot1dTp

dot1dTpFdbTable

dot1dTpPortTable

dot1dTpHCPortTable

dot1dTpPortOverflowTable

pBridgeMIB

dot1dExtBase

dot1dPriority

dot1dGarp

qBridgeMIB

```
dot1qBase
dot1qTp
    dot1qFdbTable
    dot1qTpPortTable
    dot1qTpGroupTable
    dot1qForwardUnregisteredTable
dot1qStatic
    dot1qStaticUnicastTable
    dot1qStaticMulticastTable
dot1qVlan
    dot1qVlanCurrentTable
    dot1qVlanStaticTable
    dot1qPortVlanTable
```

Коммутатор Мохы также имеет приватный MIB-файл (**Moxa-[switch's model name]-MIB.my**), расположенный на CD-диске, входящем в комплект поставки коммутатора.

Сообщения Public Trap

Cold Start
Link Up
Link Down
Authentication Failure
dot1dBridge New Root
dot1dBridge Topology Changed

Сообщения Private Trap

Configuration Changed
Power On
Power Off
Traffic Overloaded
Turbo Ring Topology Changed
Turbo Ring Coupling Port Changed
Turbo Ring Master Mismatch

Поддержка МОХА в Интернет

Наша первоочередная задача - удовлетворение пожеланий заказчика. С этой целью была создана служба MOXA Internet Services для организации технической поддержки, распространения информации о новых продуктах, предоставления обновленных драйверов и редакций руководств пользователя.

Для получения технической поддержки пишите на наш адрес электронной почты:
support@moxa.ru

Для получения информации об изделиях обращайтесь на сайт:
<http://www.moxa.ru>