




# Руководство по настройке через консольный интерфейс

PSW+UPS-Box 8x2Pro

PSW+Box 8x2Pro

PSW+Ex 8x2Pro 

PSW+UPS-Ex 8x2Pro 

Многофункциональные гигабитные управляемые коммутаторы  
для систем IP-видеонаблюдения

Версия руководства 1  
Версия встроенного ПО 1.0.0  
© Форт-Телеком, Пермь 2025

## Оглавление

1.	Введение .....	6
2.	Подключение через CLI.....	6
3.	Характеристики .....	7
4.	Общая структура команд.....	8
4.1.1	Команды управления коммутатором (см. таблица 4-1) .....	8
4.1.2	Команды управления консольным интерфейсом .....	10
4.2	Уровни доступа .....	10
4.3	Команда <i>changes</i> - просмотр, отмена, сохранение конфигурации 10	
4.4	Валидация параметров.....	11
4.5	Авто дополнение команд, подсказки и встроенная справочная информация .....	13
4.6	Информационные сообщения .....	13
4.7	Автоматизация настройки коммутатора .....	14
5.	network - настройка и просмотр сетевых параметров.....	15
5.1.	network ipif.....	15
5.1.1.	network ipif config .....	15
5.1.2.	network ipif show - Просмотр статуса .....	16
5.2.	network vlan.....	17
5.2.1.	network vlan config .....	17
5.2.2	network vlan show configuration .....	19
5.3	network port.....	20
5.3.1	network port config.....	20
5.3.2	network port mirroring .....	21
5.3.3	network port show .....	22
6.	system - настройка и просмотр системных параметров.....	22
6.1	system description.....	22

6.1.1	system description config .....	22
6.2	system log .....	23
6.2.1	system log config .....	23
6.2.2	system log show.....	27
6.3	system switch .....	27
6.3.1	system switch show .....	27
6.4	system syslog.....	28
6.4.1	system syslog config .....	28
6.4.2	system syslog show .....	29
6.5	system user.....	29
6.5.1	system user config .....	29
6.5.2	system user show .....	30
7.	services - настройка и просмотр служебных программ и сетевых протоколов	31
7.1	services igmp .....	31
7.1.1	system igmp config .....	31
7.1.2	system igmp show.....	33
7.2	services lldp.....	34
7.2.1	system lldp config.....	34
7.2.2	system lldp show.....	35
7.3	services smtp .....	36
7.3.1	system smtp config .....	36
7.3.2	system smtp show.....	37
7.4	services snmp .....	38
7.4.1	services snmp config.....	38
7.4.2	system snmp show.....	41
7.5	services sntp .....	42
7.5.1	services sntp config.....	42

7.5.2	services sntp show .....	42
7.5.3	services sntp synchronize .....	42
7.6	services stp/rstp .....	42
7.6.1	services stp/rstp config .....	43
7.6.2	services stp/rstp show .....	45
8.	special - настройка и просмотр специальных программ .....	46
8.1	special autorestart .....	46
8.1.1	special autorestart config .....	46
8.1.2	special autorestart show .....	48
8.2	special device_manager .....	48
8.2.1	special device_manager config .....	48
8.2.2	special device_manager show .....	49
8.3	special IO .....	49
8.3.1	special io config .....	49
8.3.2	special IO show .....	50
8.4	special tamper .....	50
8.4.1	special tamper show .....	50
8.5	special poe .....	51
8.5.1	special poe show .....	51
8.6	special radius .....	51
8.6.1	special radius config .....	52
8.6.2	special radius show .....	56
9.	tools - дополнительные инструменты .....	56
9.1	tools backup .....	56
9.2	tools firmware .....	57
9.2.1	tools firmware install .....	57
9.2.2	tools firmware show .....	58
9.3	tools transfer_file .....	58

9.4	tools restore.....	59
9.5	tools ping.....	60
9.6	tools traceroute.....	60
10.	Техническая поддержка .....	61

## 1. Введение

В данном руководстве дано описание процесса настройки и администрирования управляемых коммутаторов серии TFortis PSW-Pro через встроенный CLI-интерфейс. Для многих протоколов настройка приводится на конкретном примере.

## 2. Подключение через CLI

При первом включении, коммутатор имеет следующие настройки по умолчанию:

IP адрес:	192.168.0.1
Маска подсети:	255.255.255.0
Логин/Пароль:	admin/admin
Управляющий VLAN:	1
DHCP клиент:	выключен
RSTP:	включен
SSH:	включен
SNMP:	включен
IGMP:	включен

Перед подключением убедитесь, что сетевая карта компьютера находится в той же подсети, что и коммутатор (192.168.0.\*).

- Подключение к коммутатору через CLI возможно только по протоколу SSH:

```
ssh admin@192.168.0.1
```

После подключения пользователь попадает в TFortis CLI, будет указан уровень доступа пользователя и строка ввода команд **#Switch**

```
TFORTIS PSW
Fort-telecom, fort-telecom.ru
TFortis,      tfortis.ru

* WARNING: Authorised Access Only

version:          -
access level     - user
show access level - user
Switch#
```

- *Настройка ssh протокола и ssh ключей описана в руководстве по настройке коммутатора через WEB интерфейс, п.п. 6.14.1 и 6.14.2*

### 3. Характеристики

Коммутаторы **TFortis PSW-Pro** представляют собой всепогодные управляемые промышленные Ethernet-коммутаторы с PoE для систем IP-видеонаблюдения.

Коммутаторы **TFortis PSW-Pro-Ex** представляют собой взрывозащищённые управляемые промышленные Ethernet-коммутаторы с PoE.

#### Управление и мониторинг:

- Встроенный Web-интерфейс (HTTP, HTTPS)
- SSH
- SNMP (v1, v2c, v3, Traps)
- управление и мониторинг через ПО «TFortis Device Manager»
- управление пользователями
- STP
- SMTP
- Syslog
- LLDP
- системный журнал с гибкой настройкой логирования

#### Функции L2

- протоколы резервирования STP (IEEE 802.1d), RSTP (IEEE 802.1w)
- Static VLAN (IEEE 802.1q)
- Flow Control (IEEE 802.3x)
- Зеркалирование трафика
- управление мультикастом IGMP Snooping

#### Специальные

- контроль зависания видеокамер по критериям: линк, пинг, скорость
- перезагрузка камер по расписанию
- управление входами/выходами и датчиком температуры

#### Безопасность

- ограничение доступа на основе 802.1x
- возможность замены сертификатов для доступа по HTTPS
- доступ к SSH управлению на базе ключей

#### Диагностика

- Ping, Traceroute, DNS
- диагностика оптических SFP модулей
- самодиагностика аппаратных неисправностей

## 4. Общая структура команд

Консольный интерфейс (CLI) позволяет пользователю настраивать конфигурацию и просматривать статус состояние коммутатора. Для настройки и просмотра статуса используется иерархическое меню команд с соответствующими параметрами.

### Функционал Консольного интерфейса:

- авто дополнение команд;
- проверка параметров на валидность;
- фильтрацию команд по уровню доступа пользователя;
- возможность автоматизировать настройку коммутатора;
- подсказки и встроенная справочная информация;
- журнал истории команд;
- информационные сообщения;
- просмотр, отмена или сохранение изменений.

### **4.1.1 Команды управления коммутатором** (см. таблица 4-1)

В консольном интерфейсе используется иерархическое меню команд:

*switch# -> уровень 1 -> уровень 2 -> уровень 3 [config | show] ...*

Переход на следующий уровень меню, осуществляется выбором команд из списка.

После выполнения команды, не зависимо от результата или после отмены команды, меню возвращается к *приглашение командной строки*: **switch#**.

1. Меню первого уровня - категории команд;
2. Меню второго уровня - команды входящие в меню первого уровня;
3. Меню третьего уровня - две команды *config/show*;
  - Меню *config* - настройка параметров, соответствующих контексту;
  - Меню *show* - имеет 4-ый уровень меню: *status / configuration*, далее в зависимости от контекста;
    - Меню *show status* - текущая информация, статистика, состояние;
    - Меню *show configuration* - информация о настройка выбранного параметра.

**Важно:** если настройки выбранного параметра были изменены, но не сохранены, *show configuration* выводит информацию, включая изменённые параметры.

Таблица 4-1 - Общая структура команд

Уровень 1	Уровень 2	Описание
<b>system</b>		Управление системными параметрами
	description	Настройка описания системы
	log	Настройка логирования
	switch	Просмотр информации о коммутаторе
	syslog	Конфигурация syslog – отправка логов по сети
	user	Добавление/удаление пользователей
<b>network</b>		Настройка сетевых параметров
	ipif	Настройка интерфейсов управления
	port	Настройка портов, PoE, зеркалирование трафика
	vlan	VLAN 802.1Q - Создание/удаление VLAN, настройка портов в части работы с VLAN, создание интерфейсов управления
<b>services</b>		Управление сервисами
	igmp	IGMP snooping – управление мультикастом
	lldp	LLDP – управление протоколом обнаружения соседей
	smtp	SMTP – подключение к почтовому серверу, для отправки логов
	snmp	Настройка SNMP
	sntp	Настройка SNTP, синхронизация времени
	stp	Настройка STP/RSTP
<b>special</b>		Специальные функции
	autorestart	Autorestart PoE – настройка утилиты для автоматической перезагрузки PoE
	device_manager	Мониторинг устройств - настройка утилиты для взаимодействия с TFORTIS Device Manager
	io	Настройка периферии
	poe	Просмотр статуса PoE на портах
	radius	Настройка RADIUS – 802.1X

	tamper	Просмотр статуса дверцы шкафа
<b>tools</b>		Инструменты
	backup	Создание и восстановление резервной копии конфигурации
	firmware	Обновление прошивки коммутатора
	restore	Восстановление системы: сброс к настройкам по умолчанию, загрузка в режиме восстановления
	transfer file	Передача файлов
	ping	Сетевая диагностика
<b>changes</b>		Управление настройками
	show	Просмотр изменений настроек
	revert	Отмена изменений настроек
	save	Сохранение изменение настроек

#### 4.1.2 Команды управления консольным интерфейсом

К этим командам относятся:

help	Справка по CLI
history	История команд
exit	Завершение сессии

#### 4.2 Уровни доступа

Команды доступные пользователю, определяются уровнем доступа пользователя: *полный* или *только чтение*. Фильтрация команд по уровню доступа начинает работать со 2-ого уровня меню.

#### 4.3 Команда *changes* - просмотр, отмена, сохранение конфигурации

Для стабильной работы коммутатора и предотвращения потери связи с коммутатором в Консольном интерфейсе предусмотрен следующий механизм работы с конфигурацией:

- После выполнения команды с новыми настройками изменения записываются в «журнал» изменений, но не применяются;  
**Важно:** Используя команды Консольного интерфейса для просмотра конфигурации какого-либо параметра, будет выводиться

информация включая сделанные, но ещё не сохранённые изменения;

- Просмотреть текущие и не сохранённые изменения возможно с помощью команды *changes show*;
- *Отменить* текущие и не сохранённые изменения возможно с помощью команды *changes revert <config type>*. Если значение параметра *<config type>* не указано, то будут удалены все изменения.
- применение и сохранение настроек возможно с помощью команды *changes save*; после сохранения настроек, **отменить сделанные изменения не возможно**.

**Важно:** не рекомендуется изменять одни и те же параметры одновременно и через консольный интерфейс, и через Web интерфейс. Это может привести к неочевидным результатам.

#### 4.4 Валидация параметров

В консольном интерфейсе используется 2-а типа параметров:

- Перечисления: строго заданные параметры. Пользователю предлагается выбрать нужный параметр из списка;
- Пользовательские: пользователь вводит параметр. К таким параметрам относятся **строка, число, IP адрес, маска сети**.
- Все параметры команд проходят валидацию на соответствии типа.

В случае, если значение параметра не соответствует типу, выводится сообщение об ошибке, а последующие команды или параметры не доступны.

##### Перечисления

Будут описаны в разделах, соответствующих командам

##### Пользовательские типы параметров

1. IP адрес:
  - **формат**: A.B.C.D, пример: 192.168.0.1
2. Маска сети:
  - **полный формат**: A.B.C.D, пример: 255.255.255.0
  - **короткий формат**: \N, пример: \24
3. Числа:
  - **формат**: десятичные числа
  - **ограничения**: для каждого параметра определены допустимые значения
4. Диапазон:

- **полный формат:** X-Y, задаётся диапазон значение от X до Y, пример: port 2-5 - настройки будут применены к 2, 3, 4, 5 портам;
- ограничения:
  - для каждого параметра определены допустимые значения;
  - X, Y должны находится в заданном диапазоне;
  - Y должно быть больше X;
- **короткий формат:** X, пример: port 3 - настройки будут применены только к 3 порту;
- ограничения:
  - для каждого параметра определены допустимые значения.
  - X должен находится в заданном диапазоне

#### 4. Строка:

- формат:
  - Поддерживаются строки на русском и английских языках. (Кириллица и Латиница)
  - Произвольная строка, состоящая из одного слова:  
пример: stringfromoneword
    - Произвольная строка, состоящая из нескольких слов:  
пример: "string of several words".

**Важно:** строка, состоящая из нескольких слов, должна быть заключена в кавычки.

К строке, состоящей из одного слова такого требования нет.

- **ограничения:**
  - количество символов в строке. Для каждого параметра ограничение по количеству символов определено отдельно;
  - наличие запрещённых символов. Список запрещённых символов приведён в таблице 4-2.

**Важно:** символ '\ ' относится к запрещённым, но его использование не приведёт к ошибке. Этот символ будет проигнорирован, а символ, следующий за ним (кроме символов #, <, >), если он не в списке запрещённых, будет добавлен в строку, введённую пользователем.

Например: пользователь ввёл значение параметра *ifname*: ifname\nvalue. Тогда *ifname* присваивается значение: ifnamenvalue.

Таблица 4-2 - Список запрещенных символов

\$	%	^	&	=	+
[	]	{	}	;	:
	\	/	?	,	~
<	>	`	'	"	
\r	\n	\t			

#### 4.5 Авто дополнение команд, подсказки и встроенная справочная информация

- Авто дополнение команд работает по нажатию клавиши TAB;
- В консольном интерфейсе **ВЕРХНИЙ** и **НИЖНИЙ** регистр воспринимается одинаково для встроенных команд; для вводимых пользователем значений регистр имеет значение.
- Если имеется множественный выбор, будет предложен список доступных команд;
- Если доступных команд нет, значит пользователь ввёл команду целиком или в команде содержится **ошибка**;
- Подсказки и встроенная справочная информация доступны пользователю по нажатию комбинации клавиш **shift +?**
- Строка **<cr>** в конце списка команд в подсказке означает, что перечисленные в подсказке параметры являются необязательными;
- Строка **<cr>** без списка команд в подсказке означает, что пользователь ввёл команду целиком и других параметров нет;
  - \* более подробное описание обязательных и необязательных параметров будет описано разделах соответствующих команд.

#### 4.6 Информационные сообщения

Консольный интерфейс сообщает пользователю о результатах выполнения команд. Предусмотрены различные уровни сообщений:

- **info:** успешное выполнении команды;
- **warning:** изменение настроек **может** привести к некорректной работе коммутатора или потери связи. Пользователю **необходимо убедиться**, что новые настройки корректны. Проверить изменения с помощью команды *changes show*. При необходимости отменить новые настройки командой *changes revert* и установить новые корректные настройки.

- **error:** пользователь ввёл некорректные значения параметров, произошла ошибка в ходе выполнения команды.
- **critical:** выполнения команды невозможно, ошибка на системном уровне.

## 4.7 Автоматизация настройки коммутатора

Консольный интерфейс позволяет пользователю автоматизировать процесс настройки коммутатора с помощью скриптов. Пример простого скрипта на Python:

- Необходимо сформировать список команд `command_lits`
- Подключиться к коммутатору по SSH, указав логин и пароль.
- Создать функцию отправки команд и парсинг полученного ответа, используя уровни информационных сообщений.

Пример на python:

```
import pexpect
```

```
# Список команд
```

```
command_lits = [
```

```
    "system switch show status",
```

```
    "network ipif show status network",
```

```
    "network vlan show configuration all"
```

```
]
```

```
prompt = "Switch#"
```

```
user = "admin"
```

```
password = "admin"
```

```
ip = "192.168.0.1"
```

```
def send_command():
```

```
ssh_connection = user + "@" + ip + "'s [Pp]assword:"
```

```
with pexpect.spawn(f"ssh {user} @{ip}", timeout=10, encoding="utf-8") as ssh:
```

```
pass_match = ssh.expect(ssh_connection)
```

```
ssh.sendline(password)
```

```
ssh_pass = ssh.expect(prompt)
```

```
if ssh_pass == 0:
```

```
    print("connected to Tfortis switch")
```

```
    for command in command_lits:
```

```
        ssh.sendline(command)
```

```
        match = ssh.expect([prompt, pexpect.TIMEOUT, pexpect.EOF])
```

```
        output = ssh.before
```

```
        pprint(output)
```

```
    ....
```

```
# обработчик полученных сообщений
```

## 5. network - настройка и просмотр сетевых параметров

### 5.1. network ipif

#### 5.1.1. network ipif config

##### Принципы настройки:

- команда *network ipif config* позволяет настроить существующий интерфейс в системе;
- имя интерфейса является его идентификатором;
- для настройки протокола *dhcp* других параметров не требуется;
- для настройки протокола *static* доступны параметры *ip\_address / netmask, gateway* и *dns*;  
Эти параметры не зависимы, пользователь может использовать все параметры одновременно или каждый отдельно;
  - параметры *ip\_address* и *netmask* назначаются совместно;

##### **Важно:**

При настройке интерфейса управления следует иметь ввиду, что не ему не может быть назначен IP адрес из той-же подсети, которая уже используется на других интерфейсах

##### Синтаксис:

`network ipif config ifname <имя интерфейса> proto <протокол> [параметры]`

*Таблица 5-1 - Параметры команды network ipif config*

Параметр	Обязательный	Уровень доступа	Описание	Тип параметра
ifname	Да	admin	Имя интерфейса	строка
proto	да	admin	Протокол интерфейса	static / dhcp
ip_address	обязателен для netmask	admin	IP-адрес	IP адрес
netmask	обязателен для IP адреса	admin	Маска сети	Маска сети
gateway		admin	Шлюз	IP адрес
dns		admin	DNS-сервер	IP адрес

Примеры использования команд:

- network ipif config ifname eth0 proto dhcp
- network ipif config ifname eth0 proto static ip\_address 192.168.1.10 netmask /24
- network ipif config ifname eth0 proto static ip\_address 192.168.1.10 netmask 255.255.255.0 gateway 192.168.1.1 dns 8.8.8.8
- network ipif config ifname eth0 proto static gateway 192.168.1.1 dns 8.8.8.8
- network ipif config ifname eth0 proto static dns 8.8.8.8

### 5.1.2. network ipif show - Просмотр статуса

Синтаксис:

network ipif show status [тип информации] <параметры>

*Таблица 5-2 - Параметры команды network ipif show*

тип информации	описание	параметры	тип параметров
network	Статус интерфейсов		
arp	ARP-таблица		
fdb	FDB-таблица	ports	Диапазон 1-10
packet	Статистика пакетов	ports	Диапазон 1-10

Примеры использования команд:

- network ipif show status network
- network ipif show status arp
- network ipif show status fdb
- network ipif show status fdb ports 1-5
- network ipif show status packet
- network ipif show status packet ports 1-3
- network ipif show status packet ports 5

## 5.2. network vlan

### 5.2.1. network vlan config

Для команды *network vlan* доступны подкоманды:

Параметр	Описание	Тип параметра
vlanid	Команда для настройки VLAN 802.1Q. Позволяет добавлять / редактировать / удалять порты, изменять тип порта <i>not_member</i> / <i>tagged</i> / <i>untagged</i> , а также назначить имя и изменить состояние для указанного Vlan	Число 1-4094
mnngt_vlan	Команда позволяет добавлять / редактировать / удалять интерфейсы. <b>Важно:</b> для настройки интерфейса использовать команду <i>network ipif config ifname &lt;имя интерфейса&gt; [параметры]</i> из п.2.1 <i>network ipif <b>config</b> ifname &lt;имя_интерфейса&gt; proto &lt;протокол&gt;</i>	

#### 5.2.1.1. network vlan config vlanid

Принципы настройки:

- на коммутаторе “PRO” доступно 1-4095 vlan. Vlan **4095** зарезервирован системой;
- в настройках по умолчанию создан vlan 1, в который добавлены порты 1-10 *untagged*;
- *tagged* порт может быть включён в разные Vlan;
- *untagged* порт может быть включён только в один Vlan;
- если необходимо переместить *untagged* порт из одного VLAN в другой, необходимо сначала назначить *этот порт* - *not\_member*, затем назначить этот порт в нужном VLAN как *untagged* или *tagged*;

Синтаксис:

- *network vlan config vlanid <vlan\_id> action <действие> <taggedType> ports <диапазон\_портов>*
- *network vlan config vlanid <vlan\_id> name <имя vlan>*
- *network vlan config vlanid <vlan\_id> state <state value>*

Таблица 5-3 - Параметры команды `vlan config vlanid`

параметры		Обязательный	Описание	тип параметра
action				add / edit / delete
	taggedType	Да, для <i>add / edit</i> не доступен для <i>delete</i>	Тип портов	not_member / tagged / untagged not_member – доступен для действия edit
	ports на коммутаторе “PRO” доступно 1-4095 vlan	Да, для <i>add / edit</i> не доступен для <i>delete</i>	Диапазон портов	Диапазон 1-10
state			Состояние VLAN	enable / disable
name			Имя VLAN – простое текстовое описание	Строка

Примеры использования команд для настройки Vlan:

- `network vlan config vlanid 100 action add tagged ports 1-5`
- `network vlan config vlanid 200 action edit untagged ports 5`
- `network vlan config vlanid 100 state enable`
- `mngt_vlannetwork vlan config vlanid 100 name “street cameras”`

**5.2.1.2. network vlan config mngt\_vlan**

Принципы настройки Management Vlan:

- команда `network vlan config mngt_vlan` позволяет только *создать / изменить / удалить* интерфейс назначенный на определенный Vlan: *vlan\_id*;
- Чтобы назначить интерфейс на определенный Vlan, *vlan\_id* должен быть создан в системе;
  - идентификатором интерфейса является его имя: *ifname*; Имя может быть только латинскими буквами, состоять из одного слова (без пробелов), а также символы ‘-’, ‘\_’, ‘.’ и указанные в таблице 1-3 – не допускаются;
- параметры можно указывать как по одному, так и все сразу
- в системе не может быть двух и более интерфейсов с одинаковыми именами;

- количество интерфейсов в системе не ограничено;
- количество интерфейсов назначенных на определенный Vlan не ограничено;
- пользователь сам должен определять целесообразность и необходимость создания интерфейсов;
- новому интерфейсу, по умолчанию, назначается протокол **static**;
- настройка интерфейсов производится по команде `network ipif config ifname <имя интерфейса> [параметры]` в соответствии с п. 2.1.1;
- - удалённый интерфейс помечается как “удалённый интерфейс”, до сохранения или отмены новых настроек.

Синтаксис:

```
network vlan config mngt_vlan action <действие> ifname <интерфейс>
vlan_id <vlan_id>
```

*Таблица 5-4 - Параметры команды `vlan config mngt_vlan`*

Параметр	Обязательный	Описание	Тип параметра
action	да	Действие	add / edit / delete
ifname	да	Имя интерфейса	Строка
vlan_id	Да, для add / edit не доступен для action delete		Число 1-4094

Примеры использования команд:

- `network vlan config mngt_vlan action add ifname eth0 vlan_id 100`
- `network vlan config mngt_vlan action edit ifname eth0 vlan_id 200`
- `network vlan config mngt_vlan action delete ifname eth0`

### 5.2.2 network vlan show configuration

Синтаксис:

- `network vlan show configuration [vlan_id <vlan_id> | all]`

*Таблица 5-5 - Параметры команды `network vlan show configuration`*

Параметр	Обязательный	Описание	Тип параметра
vlan_id		Конкретный VLAN	Число 1-4094
all		Все VLAN	

Примеры использования команд:

- `network vlan show configuration vlan_id 100`
- `network vlan show configuration all`

## 5.3 network port

### 5.3.1 network port config

#### Принципы настройки портов:

- диапазон портов задаётся обязательным параметром *ports*, допустимый диапазон 1-10;
- порты 9-10 - SFP, имеют заводские настройки:
  - **speed: 1000 duplex full**
  - **poe:** недоступен
- изменение этих параметров будет проигнорировано, пользователь получит уведомление.
- все параметры независимы, могут выполняться как в одной команде, так и по отдельности.

#### Синтаксис:

network port config ports <диапазон портов> [параметры]

#### Параметры конфигурации:

*Таблица 5-6 -- Параметры команды network port config*

Параметр	Обязательный	Описание	Тип параметра
ports	да	Диапазон портов	Диапазон 1-10
state		Состояние порта	enable / disable
speed		Скорость порта (только порты 1-8)	auto / 1000_full / 100_full / 100_half / 10_full / 10_half
flow_control		Управление потоком	enable / disable
poe		Состояние PoE (только порты 1-8)	enable / disable

#### Примеры использования команд:

- network port config ports 1-10 state enable speed 10\_full flow\_control enable poe disable
- network port config ports 1-5 state enable speed 10\_half
- network port config ports 6 speed auto
- network port config ports 2-4 flow\_control enable
- network port config ports 1 poe enable

### 5.3.2 network port mirroring

**Зеркалирование портов** — это функция диагностики, позволяющая копировать трафик одного или нескольких портов-источников и отправлять на порт-назначения для целей мониторинга или анализа.

Это полезно для диагностики сетевых проблем, отладки и безопасности, так как позволяет подключить анализатор трафика, такой как Wireshark, к выделенному порту без прерывания нормальной работы сети.

#### Принципы настройки зеркалирования портов:

- параметр **state** - обязательный. Если выбрано значение *disable*, другие параметры не доступны;
- Порядок установки значений: *state, destination, mode*;
- *mode* устанавливается для указанных портов назначения *source*;
- при установке порта *destination*, проверяется пересечение с портами *source*;
- при установке режима *mode* для портов *source*, проверяется пересечение с портом *destination*;
- в случае пересечения портов, сначала необходимо либо изменить порт назначения *destination*, либо назначить порт источник *source* в режим *disable*. Затем назначить нужные параметры;
- вызов команды назначения портов источника *source* не отменяет предыдущие настройки портов источника; таким образом возможно настроить любую конфигурацию портов источников;
- для удаления порта, как источника *source* необходимо установить режим *disable* для нужного порта;
- рекомендуется использовать команду целиком, включая все параметры.

#### Синтаксис:

network port mirroring [параметры]

*Таблица 5-7- Параметры команды network port mirroring*

Параметр	Обязательный	Описание	Тип параметра
state	да	состояние зеркалирования порта	enable / disable
destination	доступно если state = enable	порт назначения	порт 1-10
source	доступно если state = enable	диапазон портов	Диапазон 1-10
mode	доступно если указан source	тип зеркалированного трафика	RX / TX / RX/TX

Примеры использования команд для настройки зеркалирования портов:

- network port mirroring state disable
- network port mirroring state enable
- network port mirroring state enable source 1-3 mode RX
- network port mirroring state enable destination 4
- network port mirroring state enable destination 4 source 5-7 mode RX/TX
- network port mirroring state enable source 7 mode TX destination 3

### 5.3.3 network port show

Примеры использования команд для отображения статуса портов:

- network port show status
- network port show status port 1-10
- network port show status port 1-5
- network port show status port 3

Примеры использования команд для отображения конфигурации портов:

- network port show configuration
- network port show configuration port 1-10
- network port show configuration port 1-5
- network port show configuration port 3
- 

Примеры использования команд для отображения конфигурации зеркалирования портов:

- network port show configuration mirroring

## 6. system - настройка и просмотр системных параметров

### 6.1 system description

#### 6.1.1 system description config

Принципы настройки:

- все параметры необязательные;
- для параметра **host\_name** есть дополнительные ограничения:
  - строка должна состоять из одного слова, то есть быть без пробелов;
  - допускается использовать только латинские символы;

Синтаксис:

system description config [параметры]

*Таблица 6-1 - Параметры команды system description config*

Параметр	Обязательный	Описание	Тип параметра
description	нет	краткое описание	строка
host_name	нет	имя хоста	строка
company	нет	название компании контактные данные	строка
location	нет	место размещения коммутатора	строка
notes	нет	заметки	строка

Примеры использования команд:

- system description config host\_name "test\_host\_name" description "test descr" location "тест локации" company "test company. tel: 123456789" notes test\_notes
- system description config host\_name "test\_host\_name"
- system description config description "test descr" location "тест локации" company "test company."
- system description config notes test\_notes

## 6.2 system log

### 6.2.1 system log config

Принципы настройки логов:

Общее:

- логи обрабатываются в соответствии с правилами (*rule*);
- правила (*rule*) формируются на основе фильтров (*filter*) и действий (*action*).
- если лог события проходит фильтрацию, то будет выполнено то действие (*action*), которое назначено в правиле (*rule*);
- если создано несколько правил с одним и тем же фильтром, но с разными действиями, все действия будут выполнены.
- В системе имеются базовые правила, фильтры и действия не доступные для редактирования/удаления пользователем, но доступны для просмотра и использования в создании пользовательских правил.

- для создания нового **правила** необходимо указать существующий **фильтр** и существующее **действие**;
  - для одного фильтра можно создать разные правила с разными действиями;
  - для одного действия можно создать разные правила с разными фильтрами;

команда *add/edit*

- *add* - создаёт новый *filter | action | rule*;
- *edit* - редактирует уже существующий *filter | action | rule*;
- выбор между *add* и *edit* происходит автоматически.

Если *filter | action | rule* существует: выполняется команда *edit*, если *filter | action | rule* не существует: выполняется команда *add*:

команда *delete* - удаление существующего *filter | action | rule*

- параметр *name* - является идентификатором для *filter | action | rule*
- В системе не может два одинаковых *filter | action | rule*
- Правила (*rule*):

**Важно:** если пользователь удаляет *filter* или *action*, так же *rule* сформированные на этих фильтрах или действиях автоматически удаляются

Фильтр (*filter*):

- для *фильтра* доступны 4 необязательных параметра:
  - *facility | severity | progname | content*
- типы параметров приведены в таблице 3-3;
- создание *фильтра* без параметров: будет создан фильтр, который **ничего не фильтрует! Это может быть полезно для обработки всех логов**
  - *facility*: \*
  - *severity*: \*
  - *progname*: ""
  - *content*: ""

Действия (*action*):

- типы параметров приведены в таблице 3-4;
- создание действия без параметров: будет создано действие, которое *отправляет логи в оперативную память (recent)*;

**Важно:**

- действие (*action*) *send2server* использует утилиту *syslog*. Для настройки этой утилиты используется другая команда, см. п. 3.4.
- для использования действие (*action*) *send2server* необходимо убедиться, что *syslog* в состоянии *enable*.

- *syslog* может находиться в состоянии *disable*, тогда логи не будут отправляться на удалённый сервер.

**Синтаксис:**

system log config [filter | action | rule] [add/edit | delete] [параметры]

Таблица 6-2 - Параметры rule

Параметр 1	Обязательный	Описание	Тип параметра
name	да	имя действия - его идентификатор	строка
filter	да, доступен после name	имя существующего фильтра	строка
action	да, доступен после filter	имя существующего действия	строка

Таблица 6-3 - Параметры filter

Параметры	Обязательный	Описание	тип параметра
name	да	имя фильтра - его идентификатор	строка
facility	доступен для add/edit	Выбор категории - будут логироваться все события с выбранной категорией * - все категории.	* / kernel / user / mail daemon / auth / syslog / lpr / news uucp / cron authpriv / ftp / ntp security / console local0 / local1 local2 / local3 local4 / local5 local6 / local7
severity	доступен для add/edit	Выбор уровня важности - будут логироваться все события с выбранным уровнем важности и выше. * - любой уровень важности	* / emergency / alert / critical / error warning / notice info / debug
progname	доступен для add/edit	имя программы или часть имени программы	строка
content	доступен для add/edit	фраза, которая может содержать в сообщении лога	строка

Таблица 6-4 - Параметры action

Параметр 1	Параметр 2	Параметр 3	Тип параметра
name			строка
log_action			recent / archive / send2server / email
	<b>recent</b> - отправка логов в оперативную память, после перезагрузки коммутатора логи будут удалены		
	<b>archive</b> - запись логов на flash память. После перезагрузки коммутатора логи будут сохранены		
	<b>send2server</b> - отправка логов на удалённый сервер		список IP адресов
	<b>email</b> - отправка логов на электронную почту		mail_subject / email_list
		<b>mail_subject</b> - тема сообщения	строка
		email_list	список адресов электронной почты

Примеры использования команд:

- system log config filter add/edit name "тест фильтр"
- system log config filter add/edit name "тест фильтр" facility user severity alert progname mstpd content "link down"
- system log config filter delete name "тест фильтр"
- system log config action delete name "Отправить email"
- system log config action add/edit name "Отправить email"
- system log config action add/edit name "Отправить email" log\_action email email\_list "addr1@temail.ru addr2@temail.ru" subject "switch 111 - важное событие"
- system log config rule delete name test\_rule

- `system log config rule add/edit name test_rule filter "тест фильтр" action "Отправить email"`

## 6.2.2 system log show

Синтаксис:

`system log show [Тип информации] <[Параметр]>`

*Таблица 6-5 - Параметры команды system log show configuration*

Тип информации	Параметр	Обязательный	Описание	Тип параметров
configuration		да	Конфигурация настройки логов	filter / action / rule/ all
	filter	только один из параметров	показать конфигурацию настройки <b>фильтров</b>	
	action	только один из параметров	показать конфигурацию настройки <b>действий</b>	
	rule	только один из параметров	показать конфигурацию настройки <b>правил</b>	
	all	только один из параметров	показать конфигурацию всех настроек логов	

## 6.3 system switch

### 6.3.1 system switch show

Принципы настройки:

- Команда `system switch show status` позволяет просмотреть сводную информацию
  - о системе: модель, имя хоста, версия ПО,
  - о времени: часовой пояс, текущее время на коммутаторе, время от начала работы коммутатора
  - о сети: список управляющих интерфейсов и их параметры, в том числе IP адреса, MAC адрес устройства, список VLAN;
- команда без параметров;
- полная команда `system switch show status`;

Синтаксис:

system switch show status

Примеры использования команд для настройки интерфейсов:

- system switch
- system switch show
- system switch show status

## 6.4 system syslog

### 6.4.1 system syslog config

Принципы настройки:

- Команда system syslog config позволяет настроить параметры утилиты *syslog*: состояние, протокол, порт;
- пользователь в произвольном порядке может настроить доступные параметры

Синтаксис:

system syslog config <параметры>

*Таблица 6-6- Параметры команды system syslog config*

Параметры	Обязательный	Описание	Тип параметра
state	да, хотя бы один параметр должен быть назначен	включить / выключить отправку логов на удалённый сервер	enable / disable
proto	да, хотя бы один параметр должен быть назначен	протокол, по которому отправлять логи на удалённый сервер	TCP / UDP
port	да, хотя бы один параметр должен быть назначен	номер порта	число

Примеры использования команд:

- system syslog config state disable
- system syslog config state enable proto TCP port 1231
- system syslog config proto TCP
- system syslog config proto TCP port 1231

## 6.4.2 system syslog show

### Принципы настройки:

- команда без параметров;
- полная команда `system syslog show configuration`;
- для удобства пользователя может использоваться короткая команда `system syslog show`

### Синтаксис:

`system syslog show configuration`

### Примеры использования команд:

- `system syslog show`
- `system syslog show configuration`

## 6.5 system user

### 6.5.1 system user config

#### Принципы настройки:

- команда `system user config`, позволяет только создавать и удалять пользователя. Редактировать существующего пользователя нельзя.
  - для редактирования пользователя, необходимо сначала удалить, а затем заново создать пользователя с нужными параметрами.
- параметр `password` может вводиться как в открытом, так и в скрытом виде.
  - для ввода пароля в открытом виде, следует выбрать параметр `password` после `user_name`;
  - для ввода пароля в скрытом виде, следует выбрать параметр `admin_rule` после `user_name`, нажать клавишу ENTER. Далее будет предложено ввести пароль, на экране не будет отображаться ни каких символов.

```
system user config add user_name new_user admin_rule full
Enter user password:
<ввести пароль>
```

#### **Важно:**

Ограничения при создании пользователей:

**Имя пользователя** — только цифры и английские символы, без пробела, без спецсимволов, до 32 символов

**Пароль** - цифры и английские символы, спецсимволы, до 20 символов.

- все параметры обязательны.

Синтаксис:

system user config [add | delete] <параметры>

*Таблица 6-7- Параметры команды system user config*

Параметры	Обязательный	Описание	Тип параметров
user_name	да	имя пользователя	строка
password	да, доступно для действия <i>add</i>	пароль пользователя	строка
admin_rule	да, доступно для действия <i>add</i>	права доступа	<i>full</i> - полный   <i>read_only</i> - только чтение

Примеры использования команд:

- system user config add user\_name new\_user admin\_rule full
- Enter user password:
- <ввести пароль>
- system user config add user\_name new\_user password 123 admin\_rule read\_only
- system user config delete user\_name new\_user

## 6.5.2 system user show

Принципы настройки:

- команда без параметров;
- полная команда *system user show configuration*;
- для удобства пользователя может использоваться короткая команд *system user show*;

Синтаксис:

system user show configuration

Примеры использования команд:

- system user show
- system user show configuration

## 7. services - настройка и просмотр служебных программ и сетевых протоколов

### 7.1 services igmp

#### 7.1.1 system igmp config

Принципы настройки:

- параметры настройки IGMP приведены в таблицах 4-1, 4-2, 4-3.
- Для команды *system igmp config* доступны подкоманды:

**ports | global**

*Таблица 7-1 - Параметры команды services igmp config*

Параметр	Описание	Тип параметра
ports	настройка портов	Диапазон 1-10
global	настройка глобальных параметров IGMP	state / max_snooping_table_size / multicast_querier / robustness query_interval / query_response_interval / last_member_interval /

Синтаксис:

services igmp config [*global | ports* <диапазон портов>] [параметры]

#### 7.1.1.1 system igmp config global

Синтаксис:

services igmp config global <параметры>

*Таблица 7-2 - Параметры команды system igmp config global*

Параметры	Обязательный	Описание	Тип параметров
state	нет	включить / выключить IGMP snooping	enable / disable
max_snooping_table_size	нет	максимальный размер snooping таблицы	число в диапазоне 1-1024
multicast_querier	нет	включить / выключить multicast querier	enable / disable

robustness	нет	Значение надежности. Позволяет настраиваться на ожидаемую потерю пакетов в сети	число в диапазоне 2-255 (по умолчанию 2)
query_interval	нет	Интервал в секундах между общими запросами многоадресной рассылки	число в диапазоне 30-600 (по умолчанию 125)
query_response_interval	нет	Максимальное время ответа в секундах, вводимое в периодические общие запросы	число в диапазоне 1-25 (по умолчанию 10)
last_member_interval	нет	Максимальное время ответа в секундах, указанное в запросах, относящихся к конкретной группе, отправляемых в ответ на групповые сообщения leave	число в диапазоне 1-25 (по умолчанию 1)

Примеры использования команд:

- `igmp config global state enable`
- `igmp config global state enable max_snooping_table_size 512 multicast_querier enable robustness 10`
- `igmp config global state enable max_snooping_table_size 512 multicast_querier enable robustness 10 query_interval 35 query_response_interval 4 last_member_interval 5`

**7.1.1.2 system igmp config ports**

Синтаксис:

`services igmp config ports <диапазон портов> [параметры]`

Таблица 7-3- Параметры команды `system igmp config ports <диапазон портов>`

Параметры	Обязательный	Описание	Тип параметров
state	нет	включить / выключить поддержку многоадресной рассылки	enable / disable
fast_leave	нет	включить / выключить быстрый уход	enable / disable

Примеры использования команд:

- `services igmp config ports 1-5 state disable`
- `services igmp config ports 1-5 fast_leave enable`
- `services igmp config ports 1-5 state enable fast_leave disable`

### 7.1.2 system igmp show

Синтаксис:

`system igmp show [тип информации] [port <диапазон портов>]`

Таблица 7-4 - - Параметры команды `system igmp show`

Тип информации	Параметры	Обязательный	Описание	Тип параметров
status	port	нет	показать статус igmp на порту	Диапазон 1-10
configuration				all / general / ports
	all	нет	показать все настройки IGMP	
	general	нет	показать только главные настройки IGMP	
	port	нет	показать только настройки IGMP на портах	Диапазон 1-10

Примеры использования команд:

- `services igmp show configuration all`
- `services igmp show configuration general`
- `services igmp show configuration ports 1-5`
- `services igmp show status port`

## 7.2 services lldp

### 7.2.1 system lldp config

Принципы настройки:

- параметры настройки LLDP приведены в таблицах 4-5, 4-6;
- параметр *interfaces* имеет подкоманды для добавления и удаления портов в список интерфейсов. см. таблицу 24.
- все параметры не обязательны, команду *system lldp config* с параметром *interfaces* рекомендуется использовать как отдельную команду.

Синтаксис:

services lldp config [параметры]

*Таблица 7-5 - Параметры команды system lldp config*

Параметры	Обязательный	Описание	Тип параметров
state	нет	включить / выключить LLDP	enable / disable
receive_only	нет	в режиме enable LLDP будет только прослушивать соседей	enable / disable
transmit_interval	нет	Задержка между двумя передачами LDP PDU.	число в диапазоне 5-120 (по умолчанию 30)
hold_multiplier	нет	Это значение используется для вычисления TTL передаваемых пакетов, который является произведением этого значения на задержку передачи.	число в диапазоне 2-9 (по умолчанию 4)
interfaces	нет	список портов, которые будут прослушивать и отправлять LLDP PDU пакеты. Если список пустой, то LLDP будет использовать все доступные порты	add   remove

Примеры использования команд:

- `services lldp config state enable`
- `services lldp config state enable receive_only disable transmit_interval 10 hold_multiplier 3`
- `services lldp config transmit_interval 10`

### 7.2.1.1 system lldp config interfaces

Синтаксис:

`services lldp config [interface] [параметры] ports <диапазон портов>`

*Таблица 7-6 - Параметры команды system lldp config interface*

Параметры	Обязательный	Описание	Тип параметров
add	да, на выбор	добавить порт в список LLDP интерфейсов	диапазон портов 1-10
remove	да, на выбор	удалить порт из списка LLDP интерфейсов	диапазон портов 1-10

Примеры использования команд:

- `services lldp config interfaces add ports 5-7`
- `services lldp config interfaces remove ports 5-7`

### 7.2.2 system lldp show

Синтаксис:

`system lldp show [Тип информации] [Параметры] ports <диапазон портов>`

Синтаксис system lldp show status:

`system lldp show status`

`[local | {remote | statistic | interfaces} ports <диапазон портов>]`

Таблица 7-7 - - Параметры команды *system igmp show*

Тип информации	Параметры	Обязательный	Описание	Тип параметров
status				local / remote / statistic / interfaces
	local	да, на выбор	показать статус LLDP на локальном шасси	
	remote	да, на выбор	показать обнаруженных соседей	ports диапазон портов 1-10
	statistic	да, на выбор	показать статистику	ports диапазон портов 1-10
	interfaces	да, на выбор	показать интерфейсы	ports диапазон портов 1-10
configuration				

- Если параметр *ports* для *remote / statistic / interfaces* не выбран, будет показан статус всех доступных портов

Примеры использования команд:

- `services igmp show configuration all`
- `services igmp show configuration general`
- `services igmp show configuration ports 1-5`
- `services igmp show status port`
- `services lldp show configuration`

## 7.3 services smtp

### 7.3.1 system smtp config

Принципы настройки:

- параметры *port, host, user, password, tls* - устанавливаются в соответствии с указанными у поставщика электронной почты;
- параметр получатель *to* - необходим только для отправки тестового сообщения;
- при выборе параметра *user*, становится доступным параметр *password*;
- параметр *password* может быть установлен как в открытом, так и скрытом виде.
- для ввода пароля в открытом виде, следует выбрать параметр *password* после *user*;
- для ввода пароля в скрытом виде, следует выбрать другие необходимые параметры после *user*, нажать клавишу **Enter**. Далее будет предложено ввести пароль, на экране не будет отображаться ни каких символов.

- тема тестового сообщения: “subject: TFortis test email”
- текст тестового сообщения: “Message field: TFortis test email”

Синтаксис:

services smtp config [параметры]

*Таблица 7-8 - Параметры команды system lldp config*

Параметры	Обязательный	Описание	Тип параметров
state	нет	включить / выключить SMTP	enable / disable
port	нет	порт для работы SMTP протокола	число
host	нет	IP адрес, имя хоста - почтового сервера	строка
user	нет	имя пользователя, для авторизации на почтовом сервере <b>host</b>	строка
password	да, если выбран параметр <i>user</i>	пароль, для авторизации на почтовом сервере	строка
tls	нет	включить / выключить криптографические протокол	enable / disable
to	нет	получатель тестового сообщения	email адрес

Примеры использования команд:

- services smtp config state enable port 993 host imap.yandex.ru user user@yandex.ru tls enable
- Enter user password:  
<ввести пароль>
- services smtp config state enable port 993 host imap.test\_mail.ru user my\_mail@test\_mail.ru password 123
- services smtp config to recipient\_test\_mail@test\_mail.ru

### 7.3.2 system smtp show

Синтаксис:

services smtp show configuration

services smtp config configuration password

- параметр *password* позволяет просмотреть пароль, установленный пользователем для авторизации у поставщика электронной почты;
- эта команда доступна только пользователям с полным доступом;

## 7.4 services snmp

### 7.4.1 services snmp config

Принципы настройки:

- в этой команде некоторые значения параметров, являются командой следующего уровня. То есть подменю следующего уровня зависит от значения параметра, выбранного пользователем. Подробное описание команд настройки SNMP приведено в таблицах 4-9, 4-10, 4-11;
- для параметра *state* значение *<disable>* является блокирующим, другие команды будут не доступны;
- параметр *version* имеет несколько аргументов, их содержание зависит от выбранной версии:
  - 1-ое значение: версия SNMP, которую пользователь хочет настроить
  - 2-ое значение: состояние для выбранной версии SNMP *enable / disable*. Значение *disable* блокирует следующие команды меню.
  - Значение *disable* означает, коммутатор не будет отвечать на запросы SNMP этой версии.

**Важно:**

- включение / выключение версий не зависимы. Включение одной версии не влечёт отключение другой. Одновременно могут быть активны все 3-и версии SNMP;

Следующие значения аргументов зависят от выбранной версии:

**v1 / v2c** (таблица 4-10):

- выбор группы
  - *read\_community* - сообщество для чтения
  - *write\_community* - сообщество для записи
- имя выбранного сообщества.
- доверенный источник SNMP сообщества (*source*) - для выбранный группы
  - *localhost* - запросы могут поступать только с IP адреса 127.0.0.1 - фактически это отключение чтение/записи с внешних адресов:
  - *default* - доступ из внешней сети, без ограничений
  - *custom* - пользователь определяет IP адрес и маску сети

**v3** (таблица 4-11):

- *username* - имя пользователя SNMP v3;
- *allow\_write* - разрешить или запретить запись.  
значение *enable* - разрешает запись (snmpset);
- *auth\_type* - тип аутентификации SNMPv3;
- *auth\_pass* - пароль аутентификации SNMPv3;
- *privacy\_type* - тип шифрования SNMPv3;
- *privacy\_pass* - пароль шифрования SNMPv3;
- *auth\_pass*, *privacy\_pass* - возможно вводить, как в открытом виде, так и в скрытом виде. (см. п. XXXXXX)

**Важно:**

- установка параметров *state* в состояние <disable> или *version* <v1 / v2c / v3>:<disable> не удаляет ранее настроенные параметры;
- после установки параметров *state* в состояние <enable> или
- *version* <v1 / v2c / v3>:<enable>, SNMP будет работать с ранее уже настроенными параметрами;

Синтаксис:

`services snmp config [state] [version] [параметры]`

*Таблица 7-9 - Параметры команды services snmp config*

Параметры	обязательный	Описание	Тип параметров
state	да	ВКЛЮЧИТЬ / ВЫКЛЮЧИТЬ SNMP	enable   disable
version	да	выбор версии SNMP	v1   v2c   v3
			enable   disable
		v1 / v2c	read_community   write_community
		v3	user name

### 7.4.1.1 Настройка SNMP v1 / v2c

Синтаксис:

... <v1 | v2c> <enable> <read\_community | write\_community > [параметры]

*Таблица 7-10 - Параметры команды services snmp config для версий v1 / v2c*

Параметры			Тип параметров
		имя выбранного сообщества	строка
source		доверенный источник SNMP сообщества	localhost   default custom
	custom		
		ip_addr	IP адрес
		mask	Маска сети

Примеры использования команд:

- services snmp config state disable
- services snmp config state enable version v1 enable
- services snmp config state enable version v1 enable write\_community test\_private
- services snmp config state enable version v1 enable read\_community test\_public source custom ip\_addr 192.168.0.1 mask /24

### 7.4.1.2 Настройка SNMP v3

Синтаксис:

... <v3> <enable> [параметры]

*Таблица 7-11 - Параметры команды services snmp config для версии v3*

Параметры	обязательный	Описание	Тип параметров
username	да		строка
allow_write	нет	разрешить или запретить запись	enable / disable
auth_type	нет	тип аутентификации SNMPv3	MD5   SHA1   SHA224   SHA256   SHA384   SHA512   none

auth_pass	да, если назначен auth_type	пароль аутентификации SNMPv3	строка
privacy_type	нет, доступен если назначен auth_type	тип шифрования SNMPv3	DES   AES128   none
privacy_pass	да, если назначен privacy_type	пароль шифрования SNMPv3	строка

Примеры использования команд:

- `services snmp config state enable version v3 disable`
- `services snmp config state enable version v3 enable username test_user_v3`
- `services snmp config state enable version v3 enable username test_user_v3 allow_write enable auth_type none`
- `services snmp config state enable version v3 enable username test_user_v3 allow_write enable auth_type MD5 privacy_type DES auth_pass auth_pass_phrase privacy_pass privacy_pass_phrase`

#### 7.4.2 system snmp show

Показать настройки конфигурации SNMP

Синтаксис:

`services snmp show configuration`

## 7.5 services sntp

### 7.5.1 services sntp config

Принципы настройки:

- параметры настройки SNTP приведены в таблице 4-12.

Синтаксис:

services sntp config [параметры]

*Таблица 7-12- Параметры команды services sntp config*

Параметры		обязательный	Описание	Тип параметров
state		нет	включить / выключить SNTP	enable / disable
add	host_name	нет	имя хоста или IP адрес	строка
delete				
timezone		нет	время в формате - 12..12	время

Примеры использования команд:

- services sntp config state disable
- services sntp config state enable add host\_name ntp0.ntp-servers.net timezone 6
- services sntp config timezone -2

### 7.5.2 services sntp show

### 7.5.3 services sntp synchronize

Синтаксис:

services sntp synchronize

## 7.6 services stp/rstp

Синтаксис:

services stp/rstp config [system | bridge | ports <диапазон портов>]  
[параметры]

Для команды `services stp/rstp config` доступны 3-и подкоманды `system` | `bridge` | `ports`.

### 7.6.1 services stp/rstp config

Следует учитывать, что стандарт IEEE802.w **не рекомендует превышать 7 коммутаторов в кольце** при стандартных параметрах протокола RSTP.

Принципы настройки:

- параметры настройки stp/rstp приведены в таблицах 4-13, 4-14, 4-15, 4-16

*Таблица 7-13- Параметры команды services stp/rstp config*

подкоманды	Описание	Тип параметра
system	системные настройки STP/RSTP	state   protocol   log_level
bridge	настройки STP/RSTP на уровне сетевого моста	priority   ageing   hello_time   forward_delay   tx_hold_count
ports	настройки STP/RSTP на уровне портов	treeprio   path_cost   admin_edge   auto_edge   bpdu_filter   bpdu_guard

#### 7.6.1.1 services stp/rstp config system

*Таблица 7-14 - Параметры команды services stp/rstp config system*

Параметры	Описание	Тип параметра
state	включить / выключить STP/RSTP	enable   disable
protocol	выбор версии протокола	STP   RSTP
log_level	установить уровень логирования STP/RSTP	disable   error info   debug state_machine_transition

Примеры использования команд:

- `services stp/rstp config system state enable`
- `services stp/rstp config system protocol RSTP`
- `services stp/rstp config system state enable protocol RSTP log_level error`

Таблица 7-15 - Параметры команды `services stp/rstp config bridge`

Параметры	Описание	Тип параметра
priority	Приоритет моста (0–61440). Приоритет моста по умолчанию — 32768.	0   4096   8192   12288   16384   20480   24576   28672   32768   36864   40960   45056   49152   53248   57344   614401
ageing	Максимальное время, в течение которого конфигурационные BPDU могут удерживаться мостом (6–40 секунд).	число в диапазоне 6-40
hello_time	Интервал, с которым мост отправляет hello-пакеты на соседние мосты, чтобы удостовериться, что маршруты исправны	число в диапазоне 1-10
forward_delay	Задержка перехода корневого и назначенных портов в состояние пересылки	число в диапазоне 4-30
tx_hold_count	Ограничение максимального числа посылаемых BPDU пакетов в секунду (1-10)	число в диапазоне 1-10

Примеры использования команд:

- `services stp/rstp config bridge priority 4096`
- `services stp/rstp config bridge ageing 10`
- `services stp/rstp config bridge priority 4096 ageing 10 hello_time 4 forward_delay 4 tx_hold_count 2`

### 7.6.1.2 `services stp/rstp config ports <диапазон портов>`

- допустимый диапазон портов: 1-10

Таблица 7-16 - Параметры команды `services stp/rstp config ports <диапазон портов>`

Параметры	Описание	Тип параметра
treeprio	Приоритет порта	0   4096   8192   12288   16384   20480   24576   28672   32768   36864   40960   45056   49152   53248   57344   614401
path_cost	Стоимость маршрута	число в диапазоне 1 - 200.000.000
admin_edge	Административное пограничное состояние	enable   disable
auto_edge	Автоматическое пограничное состояние	enable   disable
bpdu_filter	Фильтр BPDU	enable   disable
bpdu_guard	Защита BPDU	enable   disable

Примеры использования команд:

- `services stp/rstp config ports port_range 2-5 treeprio 8192`
- `services stp/rstp config ports port_range 6 admin_edge enable auto_edge disable`
- `services stp/rstp config ports port_range 2-5 treeprio 8192 path_cost 5 admin_edge enable auto_edge disable bpdu_filter enable bpdu_guard disable`

## 7.6.2 services stp/rstp show

Синтаксис:

`services stp/rstp show [тип информации] [параметры]`

Тип информации	Параметры	Обязательный	Описание	Тип параметров
status		да, на выбор		ports   bridge
	ports	да, на выбор		диапазон портов 1-10
	bridge	да, на выбор		
configuration				ports   bridge
	ports	да, на выбор		диапазон портов 1-10
	bridge	да, на выбор		

Примеры использования команд:

- `services stp/rstp show status ports`
- `services stp/rstp show status ports 5-10`
- `services stp/rstp show status bridge`
- `services stp/rstp show configuration ports`
- `services stp/rstp show configuration ports 6`
- `services stp/rstp show configuration bridge`

## 8. special - настройка и просмотр специальных программ

### 8.1 special autorestart

#### 8.1.1 special autorestart config

##### Принципы настройки:

- утилита *autorestart* предназначена для отслеживания работы PoE на выбранном порту;
- диапазон портов: 1-8;
- предусмотрено 3-и независимых режима работы autorestart:
  1. периодические проверки порта по выбранным пользователем параметрам;
  2. включение / выключение PoE на порту по расписанию;
  3. ручная перезагрузка PoE (доступно только в Web);

##### Периодические проверки:

- доступны следующие режимы:
  - disable: проверки на порту отключены;
  - link: проверяется состояние порта link up | link down;
  - ping: проверяется состояние link, если линк в состоянии up, проверяется ping до указанного потребителя PoE;
  - Важно:** если указать IP адрес хоста, подключенного в другой порт, но находящийся в том же VLAN, результат проверки будет положительный;
  - speed: проверяется состояние link, если линк в состоянии up, проверяется скорость передачи данных на порту;
- проверки происходят каждые 5 секунд, на всех портах одновременно.
- после 12-ти подряд (в течение 1 минуты) ошибок на одном порту, PoE на этом порту перезагружается;
- если, в течение этого времени, потребитель PoE восстановил корректную работу, счётчик ошибок уменьшается. Такой механизм позволяет предотвратить ложные перезагрузки PoE на порту, вызванные кратковременными сбоями в работе потребителя PoE;
- максимальное количество перезагрузок PoE на одном порту: 3;
- после 3-ёх перезагрузок PoE на одном порту, проверки на этом порту будут продолжаться, но в случае ошибок PoE на порту перезагружаться не будет;
- восстановить перезагрузки возможно, перезагрузив PoE в ручном режиме;
- в случае, если порт(ы) или PoE на порту находятся в состоянии *disable*, проверки на этом порту проводится не будут;

Включение / Выключение PoE на порту по расписанию:

- Пользователь может создать расписание включения / выключения PoE на порту;
- таймер срабатывает один раз в сутки.
- после срабатывания таймера, новый таймер устанавливается на следующий день;
- после *выключения* PoE по таймеру, периодические проверки отключаются;
- после *включения* PoE по таймеру, периодические проверки возобновляются;

Синтаксис:

special autorestart config port <диапазон портов 1-8> [тип конфигурации]  
[параметры]

*Таблица 8-1 - Параметры команды special autorestart config*

тип конфигурации	параметры		Описание	Тип параметров
mode				disable   link   ping   speed
	disable		на порту проверки отключены	
	link		проверка состояния линка на порту	
	ping	host	IP адрес подключенного к порту потребителя PoE	IP адрес
	speed	min_speed   max_speed	скорость передачи данных в Kbit/se	число, скорость передачи данных в Kbit/sec max_speed > min_speed
alarm				enable   disable
	enable			
		timeUp	Включить PoE на порту в указанное время	время в формате HH:mm
		timeDown	Выключить PoE на порту в указанное время	время в формате HH:mm
	disable			

Примеры использования команд:

- special autorestart config port 4 mode disable
- special autorestart config port 1-3 mode link
- special autorestart config port 5-6 mode ping host 192.168.0.101
- special autorestart config port 5-6 mode speed min\_speed 1000 max\_speed 10000

### 8.1.2 special autorestart show

Синтаксис:

```
special autorestart show [status | configuration]
```

Примеры использования команд:

- special autorestart show status
- special autorestart show configuration

## 8.2 special device\_manager

### 8.2.1 special device\_manager config

Принципы настройки:

- утилита TFortis Device Manager предназначена для обнаружения, базовой настройки, мониторинга, построения карты сети коммутаторов TFORTIS по проприетарному протоколу (см руководство по TFortis Device Manager);
- пользователь может включить | выключить взаимодействие с этой утилитой для каждого интерфейса управления, *существующего* на коммутаторе.
- если на коммутаторе существует несколько интерфейсов, прикрепленных к разным устройствам (VLAN), отвечать будет тот интерфейс, на порт которого пришёл запрос;
- если на коммутаторе существует несколько интерфейсов, прикрепленных к одному устройству (VLAN), отвечать будет произвольный интерфейс, на порт которого пришёл запрос;

**Важно:**

- все интерфейсы находятся в разных подсетях;
- отвечать будет интерфейс, у которого device\_manager в состоянии *<enable>*;

Синтаксис:

```
special device_manager config ifname <имя интерфейса> state [enable | disable]
```

Таблица 8-2 - Параметры команды `special device_manager config`

Параметры	Описание	Тип параметра
ifname	имя существующего интерфейса	строка
state	включение / выключение интерфейса для обнаружения в TFortis Device Manager	enable   disable

Примеры использования команд:

- `special device_manager config ifname test_if_name state enable`
- `special device_manager config ifname test_if_name state disable`

### 8.2.2 special device\_manager show

Синтаксис:

`special device_manager show configuration`

Примеры использования команд:

- `special device_manager show`
- `special device_manager show configuration`

## 8.3 special IO

### 8.3.1 special io config

Принципы настройки:

- в этой версии ПО, настройки IO не актуальны.

Синтаксис:

`special io config [тип конфигурации] [параметры]`

Таблица 8-3- параметры команды `special io config`

тип конфигурации	параметры	Описание	Тип параметров
input			tamper   sensor1
	state	включить / выключить отслеживание изменений для контактов input	enable   disable

	alarm_state	определяет при каком состоянии контактов, необходимо информировать пользователя	open   short   any
output			relay
	state	определяет текущее состояние контактов output	open   short

Примеры использования команд:

- `special io config input tamper state disable`
- `special io config input tamper state enable alarm_state any`
- `special io config output relay state short`

### 8.3.2 special IO show

Синтаксис:

`special io show [Тип информации] [параметры]`

*Таблица 8-4- Параметры команды `system igmp show`*

Тип информации	Параметры	Тип параметров
status	sfp   ups   input   output	только для SFP: число 1 или 2
configuration	input   output	

Примеры использования команд:

- `special io show status sfp 1`
- `special io show status ups`
- `special io show status output`
- `special io show configuration input`

## 8.4 special tamper

### 8.4.1 special tamper show

- короткая, дублирующая команда для `special io show status input`, для быстрого просмотра состояния дверцы шкафа;

Синтаксис:

`special tamper show status`

Примеры использования команды:

- special tamper
- special tamper show
- special tamper show status

## 8.5 special poe

### 8.5.1 special poe show

Синтаксис:

special poe show status [параметр]

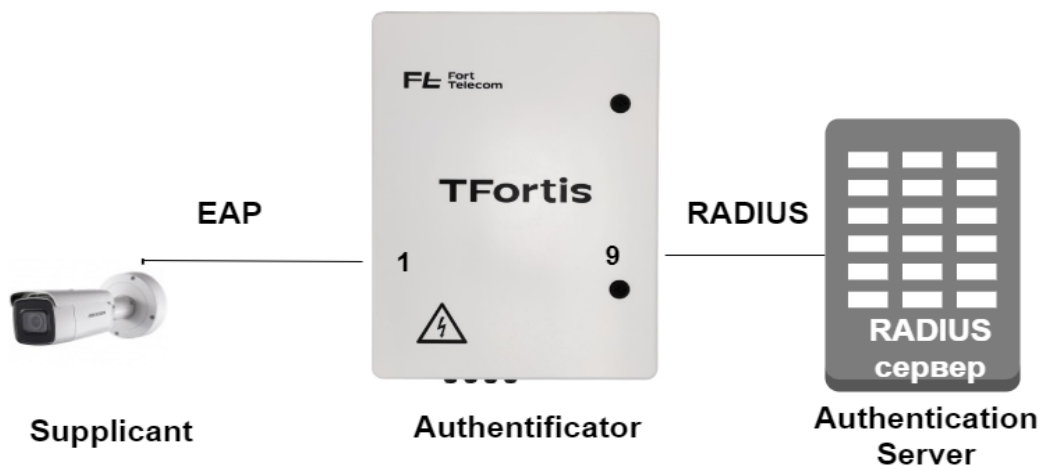
- единственный, не обязательный параметр для команды special poe show status: *extended* - показать расширенную информацию о состоянии PoE на портах.

Примеры использования команды:

- special poe
- special poe show
- special poe show status
- special poe show status extended

## 8.6 special radius

Коммутаторы TFortis поддерживают стандарт безопасности IEEE 802.1X для защиты локальной сети. Этот стандарт предотвращает несанкционированное подключение устройств к локальной сети через порты коммутатора.



Структура сети 802.1X

В стандарте 802.1X определены три типа устройств:

- Клиент (Supplicant);
- Аутентификатор (Authenticator);
- Сервер аутентификации (Authentication Server).

*Клиент* (Supplicant) — это устройство (камера), которое запрашивает доступ к локальной сети и отвечает на запросы коммутатора. Устройство должно поддерживать 802.1X аутентификацию

*Аутентификатор* (Authenticator) управляет физическим доступом к сети, основываясь на статусе аутентификации клиента. Коммутатор пересылает запросы от клиента к серверу аутентификации. На основании ответа от сервера принимает решение о разрешении/запрещении доступа для клиента.

*Сервер аутентификации* (Authentication Server) выполняет аутентификацию клиента. Он проверяет подлинность клиента и информирует коммутатор о предоставлении или отказе клиенту в доступе к локальной сети.

Эту функцию реализует сервер RADIUS

Коммутаторы поддерживают два режима аутентификации 802.1X:

- **Port based** (802.1X на основе портов);
- **MAC based** (802.1X на основе MAC-адресов).

При аутентификации на основе **портов** (Port based) защищаемый порт изначально находится в заблокированном состоянии, через него запрещена передача любого трафика, кроме EAP

После того как порт был авторизован, он переходит в состояние передачи и любой компьютер, подключенный к нему, может получить доступ к сети.

При аутентификации на основе **MAC-адресов** (MAC based) доступ разрешается индивидуально каждому конкретному MAC адресу.

### **8.6.1 special radius config**

Принципы настройки:

Синтаксис:

special radius config [тип конфигурации] [параметры]

Таблица 8-5 - Параметры команды *special radius config*

тип конфигурации	Описание	Тип параметров
general	главные настройки	state   eap_reauth_period   ca_cert   server_cert   private_key
authentication	настройки аутентификации	server_addr   server_port   server_shared_secret
accounting		
interfaces	настройки портов	state   mode
log	настройка уровня логирования	verbose   debug   info   notification   warning

### 8.6.1.1. special radius config general

Синтаксис:

special radius config [*general*] [параметры]

Таблица 8-6 - Параметры команды *special radius config general* [параметры]

параметры	описание	тип параметров
state	глобальное включение режима аутентификатора, если выключено — разрешена передаче между всеми портами	enable   disable
eap_reauth_period	Период для повторной аутентификации — период, с которым аутентификатор отправляет клиентам повторные запросы на аутентификацию (по умолчанию 3600)	число
ca_cert	PEM or DER file для EAP-TLS/PEAP/TTLS	Строка имя файла CA certificate
server_cert	Private key matching with the server certificate for EAP-TLS/PEAP/TTLS. сертификат сервера и приватный ключ — обеспечение дополнительной безопасности доступа к серверу на основе сертификатов.	Строка имя файла Server certificate
private_key	Закрытый ключ, совпадающий с сертификатом сервера для EAP-TLS/PEAP/TTLS. Это может указывать на тот же файл, что и server_cert, если и сертификат, и ключ включены в один файл	Строкам имя файла Private key

Примеры использования команд:

- special radius config general state disable
- special radius config general state disable eap\_reauth\_period 60

**8.6.1.2. special radius config [authentication | accounting]**

Синтаксис:

special radius config [*authentication | accounting*] [параметры]

*Таблица 8-7 - Параметры команды special radius config [authentication | accounting] [параметры]*

параметры	Описание	Тип параметров
addr	IP адрес сервера authentication / accounting	IP адрес
port	номер порта, на котором работает сервер authentication / accounting	число
shared_secret	пароль	строка

Примеры использования команд:

- special radius config authentication addr 192.168.0.1 port 123
- special radius config authentication addr 192.168.0.1 port 123 shared\_secret shared\_secret\_pass
- special radius config authentication shared\_secret shared\_secret\_pass
- special radius config authentication shared\_secret shared\_secret\_pass

### 8.6.1.3. special radius config interfaces

Синтаксис:

special radius config [*interfaces*] [параметры]

Таблица 8-8 - Параметры команды special radius config [*interfaces port*] [*параметры*]

параметры	Описание	Тип параметров
ports	выбор диапазона портов	диапазон портов 1-10
state	включить / выключить протокол 802.1X на порту	enable   disable
mode	<p>выбор режима</p> <p><u>Port based:</u> защищаемый порт изначально находится в заблокированном состоянии, через него запрещена передача любого трафика, кроме EAP</p> <p>После того как порт был авторизован, он переходит в состояние передачи и любой компьютер, подключенный к нему, может получить доступ к сети</p> <p><u>MAC based:</u> доступ разрешается индивидуально каждому конкретному MAC адресу</p>	port_based   mac_based

Примеры использования команд:

- special radius config interfaces ports 1-3 state enable mode mac\_based
- special radius config interfaces ports 5 state disable

### 8.6.1.4. special radius config log

Синтаксис:

special radius config [*log*] [*level*] <verbose | debug | info | notification | warning>

Примеры использования команд:

- special radius config log level debug

## 8.6.2 special radius show

Синтаксис:

special radius show [тип информации] [параметры]

*Таблица 8-9 - Параметры команды special radius show*

тип информации	параметры	Описание	Тип параметров
status			client   ports
	client	информация о клиентах на всех или выбранных портах	ports диапазон портов 1-10
	ports	информация о статусе порта	диапазон портов 1-10
configuration			all   general   ports
	all	информация обо всех настройках	
	general	информация о главных настройках	
	ports	информация о настройке портов	
certificate			

Примеры использования команд:

- special radius show status client
- special radius show status client ports 3
- special radius show status ports 5
- special radius show configuration all
- special radius show certificate

## 9. tools - дополнительные инструменты

### 9.1 tools backup

Принципы использования:

- команда *backup* позволяет создавать, применять и просматривать резервную копию настроек коммутатора;
- на коммутаторе может быть создана и хранится только одна резервная копия настроек;
- для создания другой (с другими настройками) резервной копии необходимо сохранить текущую копию на хосте, изменить настройки, создать новую резервную копию.

- предусмотрен механизм защиты резервных копий от изменения и внесения некорректных данных в конфигурационные файлы. Резервная копия, созданная командой `generate` это полная копия настроек коммутатора, сохранённая в проприетарном формате, не доступна пользователю для редактирования.
- команда `generate` создаёт резервную копию. Созданная резервная копия хранится на коммутаторе.
- команда `show` показывает сведения о резервной копии, хранящейся на коммутаторе;
- команда `apply` устанавливает резервную копию, хранящуюся на коммутаторе, затем удаляет файл резервной копии, перезагружает коммутатор.
- для сохранения резервной копии на хост или для загрузки резервной копии с хоста на коммутатор необходимо использовать команду:

```
tools transfer_file protocol tftp local_file backup action <put | get> host
```

<IP адресс>

Синтаксис:

```
tools backup [generate | show | apply ]
```

Примеры использования команд:

- `tools backup generate`
- `tools backup show`
- `tools backup apply`

## 9.2 tools firmware

### 9.2.1 tools firmware install

Принципы использования:

- команда `firmware install` позволяет обновлять ПО коммутатора;

keep setting:

- `yes`: обновить ПО коммутатора с полным сохранением настроек;
- `no`: обновить ПО коммутатора без сохранения настроек; будут применены заводские настройки;

auto:

- `yes`: автоматический режим установки, без участия пользователя; в этом режиме, будет загружен файл прошивки, проверен на валидность, установлен и система будет перезагружена;

- no: на каждом этапе обновления ПО, пользователю необходимо подтвердить дальнейшие действия.

#### remote\_file:

- если параметр не указан, обновление ПО будет происходить с заранее загруженного файла ПО;
- если параметр указан, необходимо указать имя файла обновления ПО, находящийся на удалённом TFTP сервере пользователя. Так же необходимо указать дополнительный параметр *host* <IP адрес> TFTP сервера;
- для загрузки файла прошивки на коммутатор необходимо воспользоваться командой:

*tools transfer\_file protocol tftp local\_file firmware action get host <IP адрес>*

#### Синтаксис:

*tools firmware install keep\_setting <yes | no> auto <yes | no> remote\_file <имя файла> host <IP адрес>*

#### Примеры использования команд:

- *tools firmware install keep\_setting yes auto yes remote\_file tfortis-1.0.0.bin host 192.168.0.1*

### **9.2.2 tools firmware show**

- команда *firmware show* показывает информацию о сохранённом на коммутаторе файл прошивки;
- На коммутаторе может храниться только один файл прошивки;

#### Синтаксис:

*tools firmware show*

### **9.3 tools transfer\_file**

#### Принципы использования:

- команда *transfer file* позволяет отправлять и получать файлы с удалённого сервера;
- поддерживается 2-а протокола передачи файлов:
  - tftp
  - sftp (в данной версии не поддерживается)

local\_file:

файл	описание	доступные действия
backup	файл резервной копии	put   get (для <i>action put</i> параметр <i>remote_file</i> не доступен - файл будет отправлен с именем backup)
ram_log   flash_log	логи из оперативной памяти и логи из flash памяти	<b>put</b> (параметр <i>action</i> не доступен)
firmware	Файл обновления прошивки коммутатора	<b>get</b> (параметр <i>action</i> не доступен)

Синтаксис:

```
tools transfer_file protocol <tftp | sftp> local_file <backup | ram_log | flash_log | firmware> action <put | get> remote_file <имя файла> host <IP адрес>
```

Примеры использования команд:

- tools transfer\_file protocol tftp local\_file backup action put host 192.168.0.1
- tools transfer\_file protocol tftp local\_file ram\_log remote\_file ram\_log\_010125 host 192.168.0.1

## 9.4 tools restore

Принципы использования:

- команда *restore* для восстановления системы

default:

- откат на заводские настройки (IP адрес: 192.168.0.1). Система перезагрузится с установленной версией.

recovery:

- Система перезагрузится в режим рекавери с настройками по умолчанию (IP адрес: 192.168.0.1). В режиме *recovery* система имеет минимальный функционал, достаточный для загрузки и установки прошивки.

**Важно:**

в режиме *recovery* консольный интерфейс не доступен.

auto:

- *yes*: автоматический режим, без участия пользователя;
- *no*: пользователю необходимо подтвердить дальнейшие действия.

Синтаксис:

tools restore [default | recovery] auto <yes | no>

## 9.5 tools ping

Принципы использования:

- Используется системная утилита *ping*. Проверка значений параметров, результат работы утилиты являются системными.

*Синтаксис:*

Tools ping <destination IP адрес> [параметры]

*Таблица 9-1 - Параметры команды tools ping*

параметры	Описание	Тип параметров
source	источник запроса	IP адрес / имя хоста
count	количество запросов на отправку (по умолчанию 5)	число
size	размер пакета [байт] (по умолчанию 56 байт)	число
interval	интервал в секундах между запросами	число

Примеры использования команд:

- tools ping 192.168.0.1 source 192.168.0.100 count 3 size 1024 interval 5

## 9.6 tools traceroute

Принципы использования:

- Используется системная утилита *traceroute*. Проверка значений параметров, результат работы утилиты являются системными.

Синтаксис:

tools traceroute <destination IP адрес / имя хоста>

Примеры использования команд:

- tools traceroute google.com

## 10. Техническая поддержка

Техническая поддержка по проектированию систем видеонаблюдения, вопросам эксплуатации и настройки оборудования оказывается:

- по телефону (время для звонков 8-00 — 16-00 по московскому времени)

8 800 100 112 8

+7 (342) 270 112 8

добавочный номер — 2, затем 1

- по e-mail: [support@tfortis.ru](mailto:support@tfortis.ru)
- Telegram: @tfortis\_support, [https://t.me/tfortis\\_support](https://t.me/tfortis_support)

Вся техническая документация доступна на сайте: [tfortis.ru](http://tfortis.ru)

Если у Вас есть пожелания по доработке, а может быть и идеи по созданию новых устройств, Вы можете отправить нам запрос:

<https://tfortis.ru/contacts/svyazhites-s-nami/>