




Руководство по настройке через WEB интерфейс

PSW+UPS-Box 8x2Pro

PSW+Box 8x2Pro

PSW+Ex 8x2Pro 

PSW+UPS-Ex 8x2Pro 


Многофункциональные гигабитные управляемые коммутаторы
для систем IP-видеонаблюдения

Условные обозначения.....	4
1 Введение	5
2 Характеристики коммутаторов.....	6
3 Световая индикация.....	8
4 Кнопки сброса настроек и перезагрузки.....	9
5 Управление коммутатором.....	10
5.1 Интерфейсы управления.....	10
5.2 Что нужно знать перед подключением.....	10
5.3 Подключение через WEB-интерфейс.....	10
5.4 Стратегия настройки.....	12
5.5 Сохранение и применение настроек.....	13
6 Настройка.....	14
6.1 Сетевые настройки.....	14
6.1.1 Редактирование Интерфейса.....	14
6.1.2 Создание нового Интерфейса.....	16
6.2 Настройка учётных записей пользователей	17
6.3 Описание устройства.....	18
6.4 Настройка времени.....	19
6.5 Настройка языка	20
6.6 Обновление ПО.....	20
6.7 Сохранение и восстановление резервной копии настроек	21
6.8 Сброс настроек.....	22
6.9 Загрузка в режим рекавери.....	23
6.10 Перезагрузка.....	23
6.11 Порты.....	24
6.11.1 Настройка портов.....	24
6.11.2 Состояние портов.....	24
6.11.3 Информация об SFP.....	25
6.11.4 Зеркалирование портов	28
6.12 VLAN 802.1Q	29
6.12.1 Пример настройки VLAN.....	30
6.13 Настройка STP и RSTP	33
6.14 Безопасность	37
6.14.1 Управление через SSH	37
6.14.2 SSH ключи	38
6.14.3 Настройка HTTP/ HTTPS.....	39
6.15 Настройка IGMP	43
6.16 Настройка SMTP.....	46
6.17 LLDP.....	48
6.17.1 Настройка LLDP.....	48
6.17.2 Статистика LLDP.....	50
6.18 SNMP.....	50
6.18.1 Настройка SNMP v1 / v2c.....	51

6.18.2	Настройка SNMP v3.....	52
6.18.3	Настройка SNMP Трапов.....	53
6.19	Настройка входов/выходов.....	53
6.19.1	Настройка входов.....	54
6.19.2	Релейный выход.....	54
6.19.3	Датчик температуры/влажности (опция).....	55
6.20	ИБП.....	55
6.21	Настройка контроля зависания видеокамер	56
6.22	Средства диагностики.....	57
6.22.1	Дистанционный пинг.....	57
6.23	Статистика	58
6.23.1	Статистика портов.....	58
6.23.2	Графики загрузки интерфейсов.....	59
6.23.3	Графики загрузки системы.....	59
6.23.4	Таблица MAC адресов.....	60
6.23.5	ARP Таблица	60
6.24	Журналирование.....	61
6.24.1	Журналы.....	61
6.24.2	Syslog.....	62
6.24.3	Настройка логирования	64
6	Техническая поддержка.....	68
	Приложение А. Коды аппаратных ошибок и их расшифровка.....	69

Условные обозначения

В данном руководстве приняты следующие обозначения:

Обозначение	Что означает
	Знак «Обратите внимание».
<i>Сеть → Интерфейсы</i>	При описании настройки через Web-интерфейс, курсивом указывается путь к web-странице
DEFAULT	Полужирным шрифтом выделяется какой-либо значащий параметр, значение, название кнопки и т.д.

1 Введение

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

2 Характеристики коммутаторов

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
- SNMP
- 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

3 Световая индикация

Коммутаторы TFortis PSW-Pro имеют 4 светодиодных индикатора, показывающих режим работы процессора коммутатора. Это индикаторы **DEFAULT, CPU, ALARM, READY**

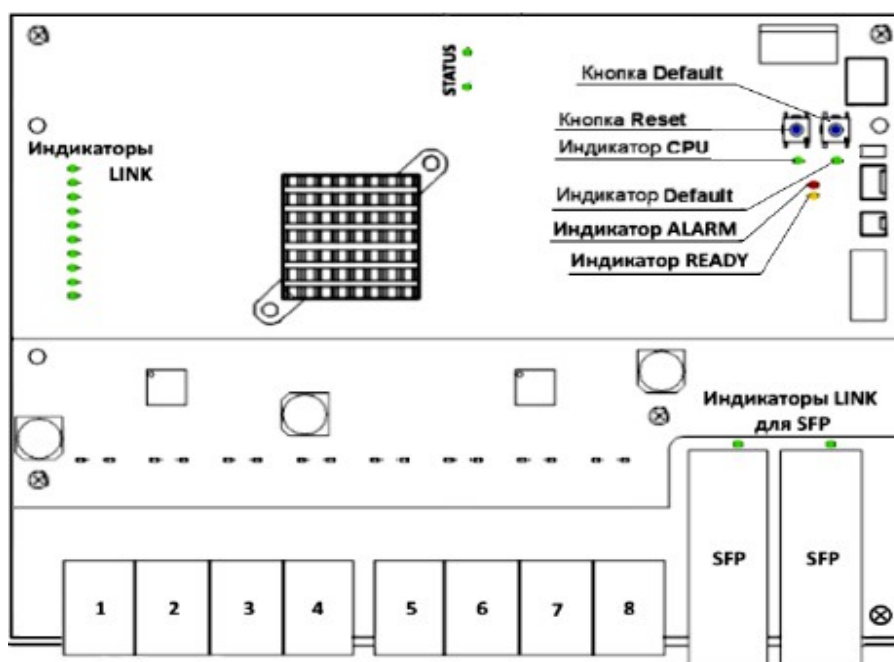


рис. 3.1 — расположение индикаторов и кнопок

Таблица 1.1 Назначение индикаторов

Индикатор	Состояние устройства
CPU	Индикация работы системы: <ul style="list-style-type: none"> быстрое мигание — идёт загрузка системы редкое мигание — система запущена
DEFAULT	Индикация заводских настроек Устройство в неконфигурированном состоянии, состояния с заводскими установками (IP адрес 192.168.0.1)
READY	Индикатор начинает светиться, когда устройство загрузилось и готово для выполнения своих функций.
ALARM	Диагностирована неисправность на аппаратном или программном уровне. Обратитесь в службу технической поддержки. Число миганий данного индикатора определяет код ошибки. Описание кодов представлено в Приложении А.

4 Кнопки сброса настроек и перезагрузки

Коммутаторы TFortis PSW-Pro имеют 2 аппаратные кнопки для сброса настроек на заводские установки и для перезагрузки. Расположение кнопок представлено на рис. 3.1.

- Для перезагрузки коммутатора кратковременно нажмите на кнопку **CPU**.
- Для сброса настроек на заводские установки нажмите и удерживайте кнопку **DEFAULT** около 15 секунд.
При этом индикатор **DEFAULT** **начнёт мигать**, как только индикатор **загорится постоянно**, кнопку можно отпустить.

5 Управление коммутатором

5.1 Интерфейсы управления

Коммутаторы PSW-Pro имеют несколько вариантов удалённого управления: WEB-интерфейс и консольный интерфейс. В данном документе рассматривается настройка через WEB-интерфейс.

5.2 Что нужно знать перед подключением

Обратите внимание!



Элементы блоков питания находятся под высоким напряжением. Категорически запрещается касаться токопроводящих элементов блоков питания под напряжением.

5.3 Подключение через WEB-интерфейс

При первом включении, коммутатор имеет следующие настройки по умолчанию:

IP адрес:	http://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.*).

Запустите Web-браузер и в адресной строке введите IP адрес коммутатора.(рис 5.3.1.1)

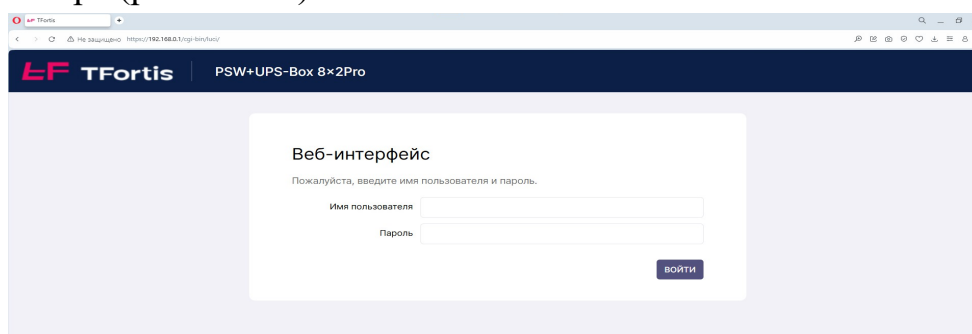


Рис. 5.3.1.1. Подключение к коммутатору

После подключения, мы должны попасть на главную страницу web-интерфейса.(рис 5.3.1.2)

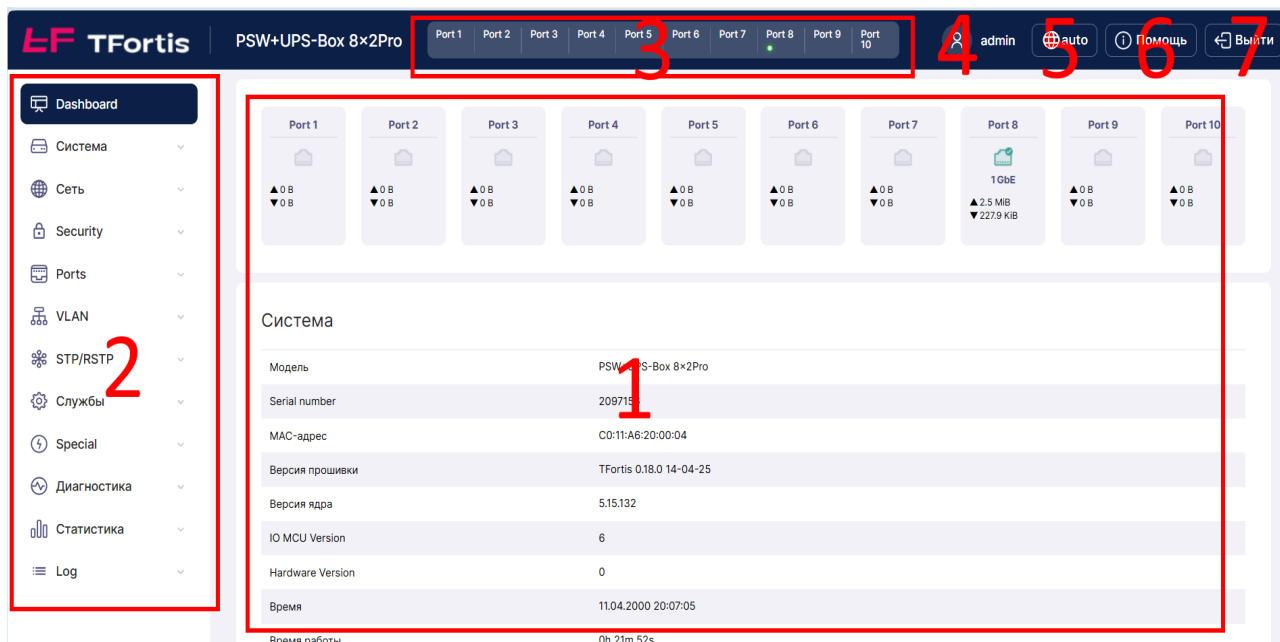


Рис. 5.3.1.2. Обзор элементов Web-интерфейса

В Web-интерфейсе можно выделить несколько зон, как показано на рисунке 5.3.1.2:

- 1 — основное окно, содержащее страницу настройки или статистики
- 2 — боковое меню, через него осуществляется доступ к различным группам настройки
- 3 — шапка интерфейса с состоянием линка и PoE на портах
- 4 — имя пользователя, осуществившего вход в систему
- 5 — кнопка выбора языка интерфейса
- 6 — кнопка вызова встроенной справки
- 7 — кнопка выхода, завершения сессии

5.4 Стратегия настройки

Можно выделить две основные стратегии настройки:

- сначала выполняется полная настройка коммутатора, а потом осуществляется его монтаж, в соответствии с проектом
- сначала выполняется монтаж в соответствии с проектом, но без настройки. При этом фиксируются серийный номер или MAC-адрес каждого коммутатора (с этикетки на корпусе). После монтажа сеть сканируется программой TFortis Device Manager и через неё назначаются сетевые настройки каждому коммутатору

Процесс настройки можно разбить на несколько ключевых этапов:

1. **Установка сетевых настроек** (задание уникального IP адреса в пределах подсети, установка маски и шлюза).
2. **Изменение логина и пароля** для ограничения доступа к настройкам.
3. **Заполнение информации** о названии устройства, его местоположении и портах. Эта информация в дальнейшем поможет при обслуживании сети.
4. **Настройка RSTP**, если используется отказоустойчивая топологию кольцо
5. **Настройка VLAN** для разграничения трафика на подсети. Всегда рекомендуется разграничивать подсеть для управления коммутаторами и подсеть для видеокамер настройкой отдельных VLAN.
6. **Настройка мониторинга**. Для удобства администрирования можно настроить систему логирования событий. Настроить протоколы Syslog, SMTP, SNMP для внешнего мониторинга. Для автоматизированного построения карты сети используется протокол LLDP.
Также можно настроить мониторинг при помощи программы TFortis Device Manager.
7. Для повышения стабильности работы видеокамер можно настроить **функцию контроля за зависанием камер**.
8. Для повышения уровня **сетевой безопасности** рекомендуется отключить HTTP, оставить только HTTPS. Настроить RADIUS

5.5 Сохранение и применение настроек

В интерфейсе коммутатора предусмотрено применение настроек в 2 этапа: сначала сохранение настроек, а потом их применение. Это позволяет сначала произвести все настройки, а потом применить всё одновременно.

Также поддерживается безопасное (failsafe) применение настроек: после применения настроек проверяется доступность коммутатора, если он перестал быть доступным, настройки откатываются на предыдущие.

Если требуется применить настройки, после которых коммутатор станет недоступным (Например при настройке VLAN, когда требуется настройка промежуточных узлов), то можно применить настройки без проверки доступности. (Рис. 5.5.1)

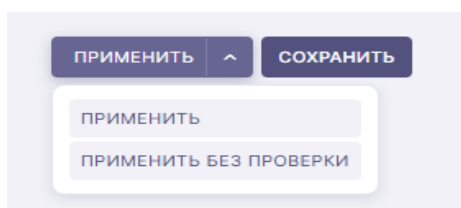


Рис. 5.5.1. Кнопки применения и сохранения настроек

Все не применённые настройки отображаются в верхней части интерфейса:

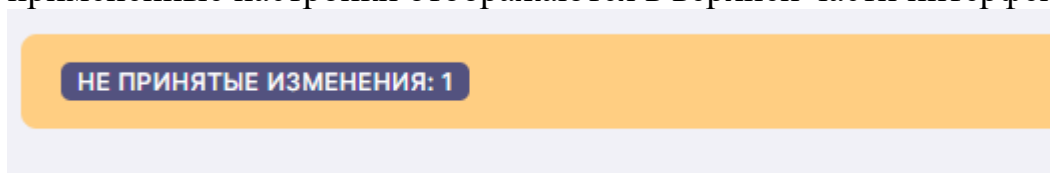


Рис. 5.5.2. Уведомление о не принятых изменениях

После нажатия Применить появляется всплывающее окно:



Рис. 5.5.3.

Уведомление о процессе применения настроек

Если для применения настроек был выбран способ с проверкой доступности (безопасный) и при этом доступ до коммутатора не восстановился в течении 90 секунд, то применённая конфигурация будет отменена. Будет выведено предупреждающее сообщение:

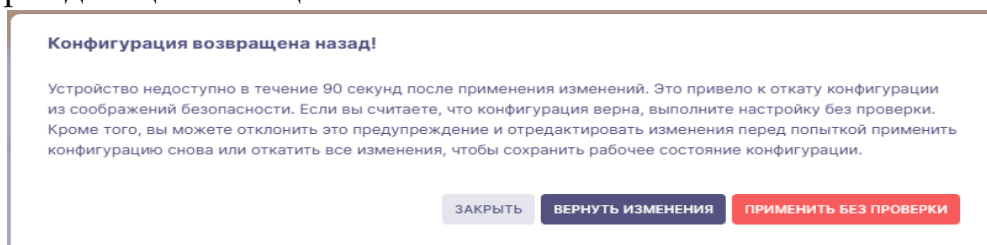


Рис. 5.5.4. Предупреждение об откате конфигурации

Можно отменить все изменения, либо принудительно применить настройки без проверки.

6 Настройка

6.1 Сетевые настройки

Сеть → Интерфейсы

В данном разделе меняются сетевые настройки для интерфейсов управления. Изначально создан один интерфейс управления. При необходимости можно создать несколько интерфейсов, привязка интерфейсов возможна к разным VLAN

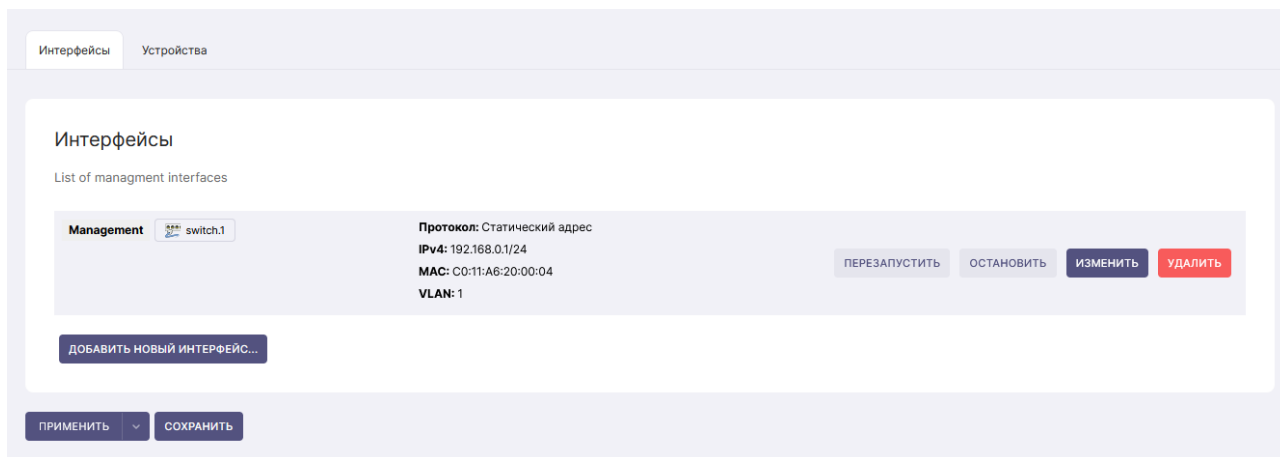


Рис. 6.1 - список созданных интерфейсов

6.1.1 Редактирование Интерфейса

Для редактирования нажмите **Изменить**

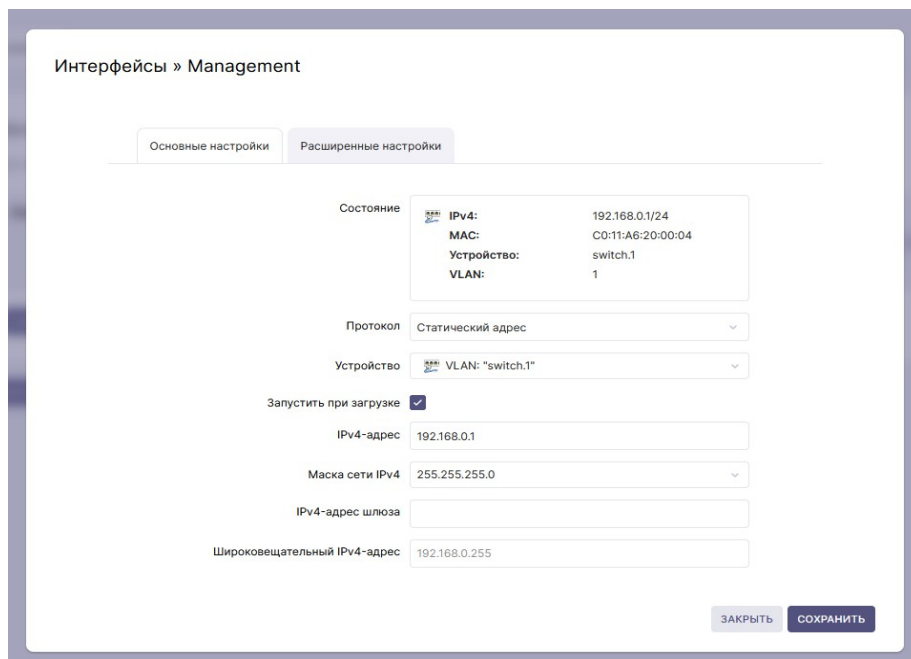


Рис. 6.1.1 Редактирование настроек интерфейса

Протокол — режим работы настройки интерфейса. Сейчас поддерживаются следующие режимы:

- Статический адрес
- DHCP-клиент

Устройство — логическое название устройства, к которому применится этот интерфейс. Интерфейс управления можно присоединить только к определенному VLAN.

Запустить при загрузке – запускать интерфейс при старте системы. Если галочку убрать, то после перезагрузки интерфейс будет выключен и доступ к нему будет отсутствовать.

IP адрес- Сетевой адрес устройства. При работе в пределах одной подсети необходимо обеспечить уникальность сетевого адреса.

Маска сети - битовая маска, позволяющая разделить IP-адрес на адрес подсети и адрес узла внутри этой подсети.

IP адрес шлюза - адрес маршрутизатора, который используется для доступа во внешнюю сеть, если не используется, оставьте поле пустым

TFortis Device Manager agent – включение поддержки широковещательного поиска и настройки через ПО TFortis Device Manager.

Если производится изменение настроек существующего интерфейса, при которых может пропасть доступ (Например, смена IP адреса), система выдаст предупреждение:

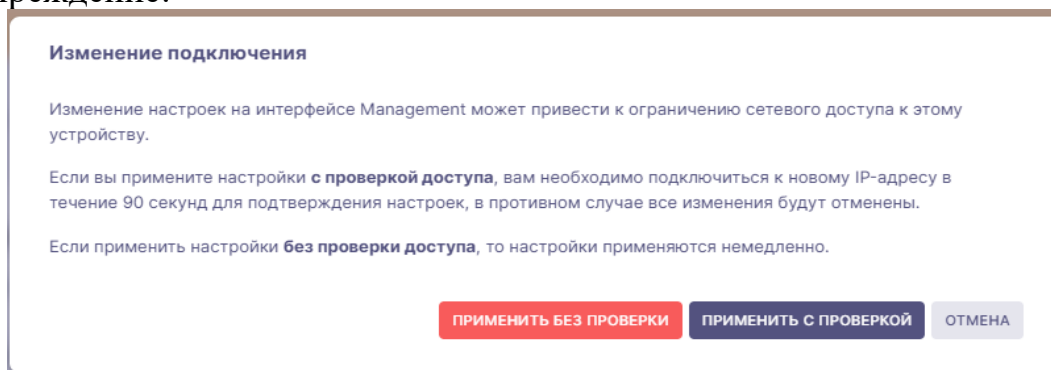
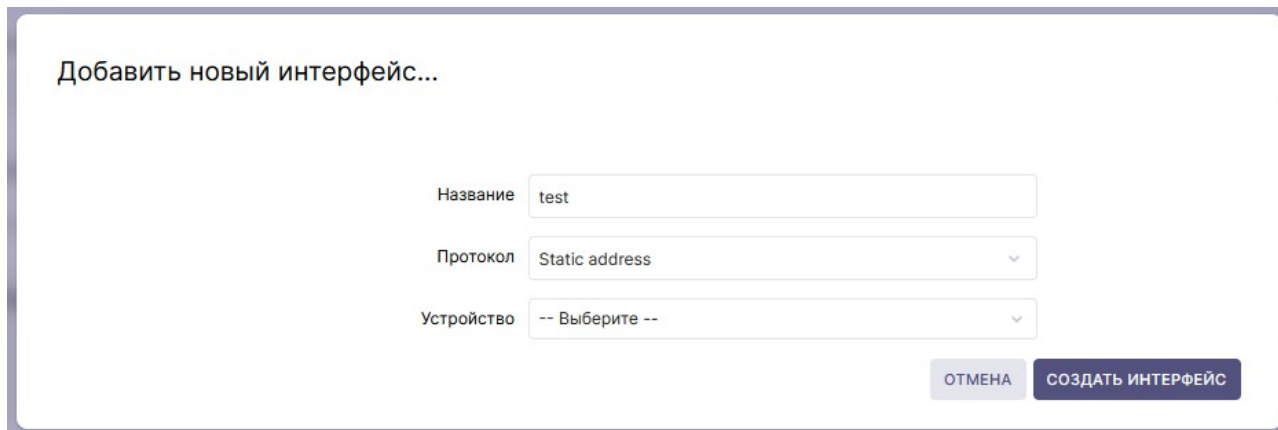


Рис. 6.1.2 Предупреждение при изменении сетевых настроек

Если нажать **Применить с проверкой**, то в течение 90 секунд нужно успеть переподключиться по новому адресу, иначе настройки будут отменены. Если Вы уверены в корректности настроек, можно нажимать **Применить без проверки**.

6.1.2 Создание нового Интерфейса

Для создания нового интерфейса нажмите **ДОБАВИТЬ НОВЫЙ ИНТЕРФЕЙС**. В открывшемся окне укажите название, тип адреса и устройство (VLAN), к которому привязывается интерфейс.



Добавить новый интерфейс...

Название

Протокол

Устройство

Рис. 6.1.2.1 Создание нового интерфейса

После нажатия Создать интерфейс откроется окно редактирования настроек, как на рис. 5.3.2.2. Необходимо будет указать название и тип интерфейса, а также указать, к какому устройству будет привязан новый интерфейс.

6.2 Настройка учётных записей пользователей

Система → Управление пользователями

В данном разделе содержатся настройки учетных записей пользователей. Данные учётные записи используются для доступа как к WEB интерфейсу, так и к консольному интерфейсу (SSH)

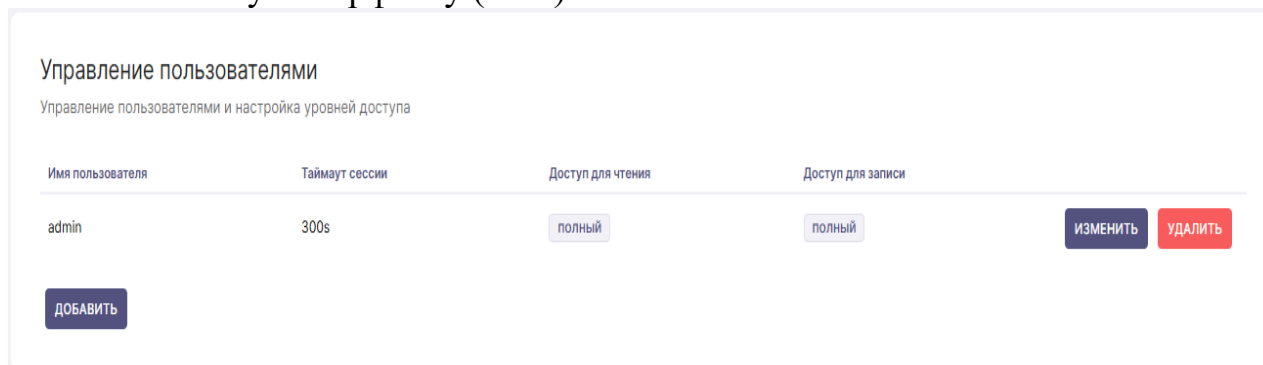


Рис. 6.2.1 Список пользователей

По умолчанию единственной учетной записью является учетная запись администратора **admin**.

Для ограничения доступа обязательно следует создать новую учётную запись, либо отредактировать существующую.

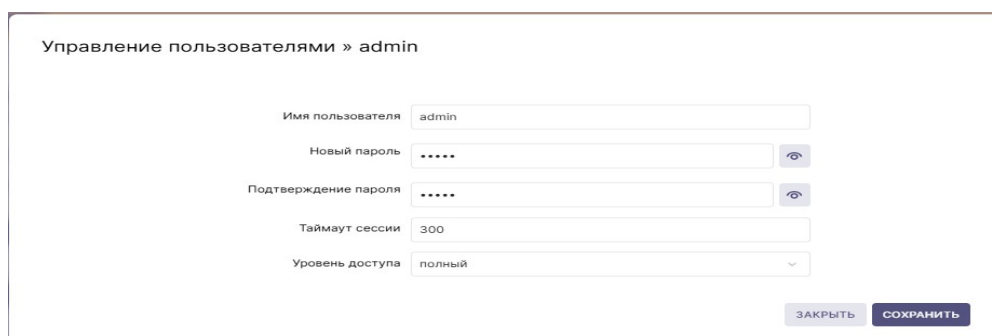


Рис. 6.2.2 Редактирование пользователя

Имя пользователя - имя пользователя для доступа к WEB-интерфейсу и SSH

Пароль – пароль для доступа к WEB-интерфейсу и SSH

Таймаут сессии — таймаут на сессию в WEB-интерфейсе

Уровень доступа — возможны следующие уровни доступа:

- **полный** — пользователю доступно чтение и запись всех параметров
- **только чтение** - пользователю доступно только чтение параметров

Существуют ограничения при создании пользователей:

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

Пароль - цифры и английские символы, пробелы, спецсимволы, до 20 символов

6.3 Описание устройства

Система → Система → Описание

Имя хоста	<input type="text" value="TFortis"/>
	<small>Used to identify the device in network</small>
Описание	<input type="text" value="Коммутатор №23"/>
	<small>Необязательное, краткое описание для этого устройства</small>
Расположение	<input type="text" value="КПП №2"/>
	<small>Необязательное, местоположение устройства</small>
Контактная информация	<input type="text" value="8(800)100-112-8 support@tfortis.ru"/>
	<small>Необязательное, обслуживающая организация</small>
Примечания	<div style="border: 1px solid #ccc; height: 150px; width: 100%;"></div>
	<small>Необязательные, произвольные заметки об этом устройстве</small>

Рис. 6.3.1 Описание устройства

Имя хоста — сетевое имя, hostname

Описание - Название устройства

Расположение — описание месторасположения устройства

Контакты - Контактная информация обслуживающей компании или ответственного лица

Примечания — дополнительное текстовое поле

Данные поля являются необязательными для заполнения и служат лишь для упрощения идентификации коммутатора.

6.4 Настройка времени

Система → Система → Дата/Время

Рис. 6.4.1 Настройка времени

Коммутатор имеет встроенные часы реального времени, которые зарезервированы отдельным источником питания. Поэтому при отключении питания, установленное время сохраняется.

Рекомендуется однократно синхронизировать время при первичной настройке.

Скопировать из браузера — ручная синхронизация времени через системное время браузера (совпадает со временем на ПК)

Синхронизировать по NTP - ручная синхронизация времени через NTP сервер. Если используются внешние NTP сервера, то необходимо обеспечить доступ в интернет.

Часовой пояс — часовой пояс используется для вычисления локального времени из UTC.

Включить NTP-клиент — включить поддержку NTP (необходимо для синхронизации времени через NTP)

6.5 Настройка языка

Система → Система → Язык

Свойства системы

Настройка основных параметров вашего устройства, таких как имя или часовой пояс.

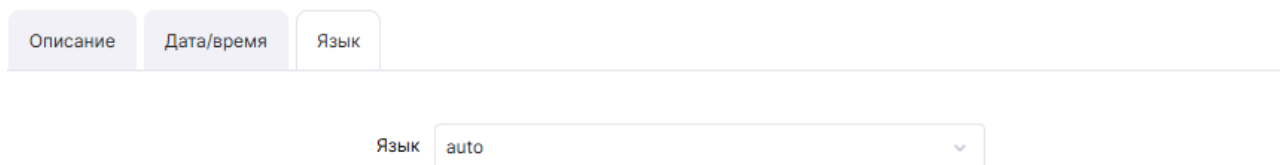


Рис. 6.5.1 Настройка языка

Для WEB интерфейса доступны 2 варианта перевода интерфейса: русский и английский.

По умолчанию используется автоматическое определение языка на основании свойства браузера

6.6 Обновление ПО

Система → Обновление/Восстановление

Обновление встроенной прошивки возможно через WEB-интерфейс и через TFTP сервер через консольный интерфейс.

В данном случае рассмотрим обновление через WEB.

Для загрузки файла новой прошивки нажмите «установка образа» и выберите файл.

Установить новый образ прошивки

Загрузите образ для замены работающей прошивки.

Образ

УСТАНОВКА ОБРАЗА...

Рис. 6.6.1 Окно установки новой прошивки

После чего нажмите «загрузить» (рис. 5.3.7.2). Файл будет загружен в оперативную память и проверен на целостность. Если файл загрузился успешно, будет предложено начать обновление (рис. 5.3.7.2).

При этом есть возможность сохранить текущую конфигурацию, установив галочку «Сохранить настройки и оставить текущую конфигурацию».

Если галочку снять, то после обновления коммутатор запустится с настройками по умолчанию.

После нажатия на **«продолжить»** запустится процесс обновления. Не отключайте питание и не перезагружайте коммутатор при этом

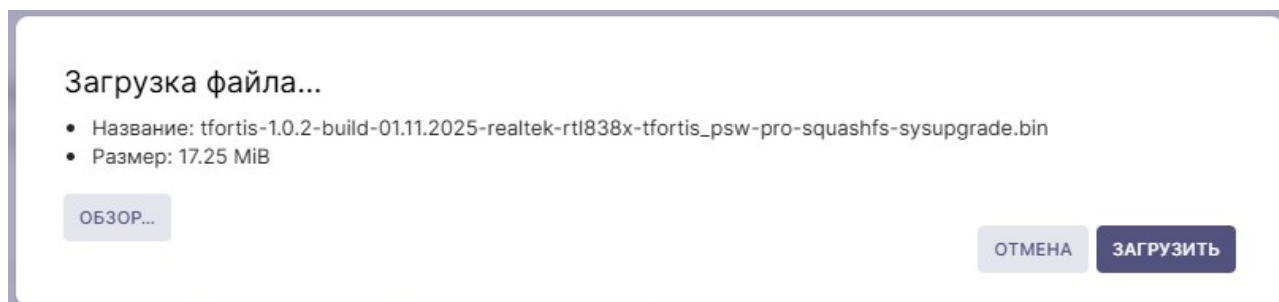


Рис. 6.6.2 Окно загрузки файла

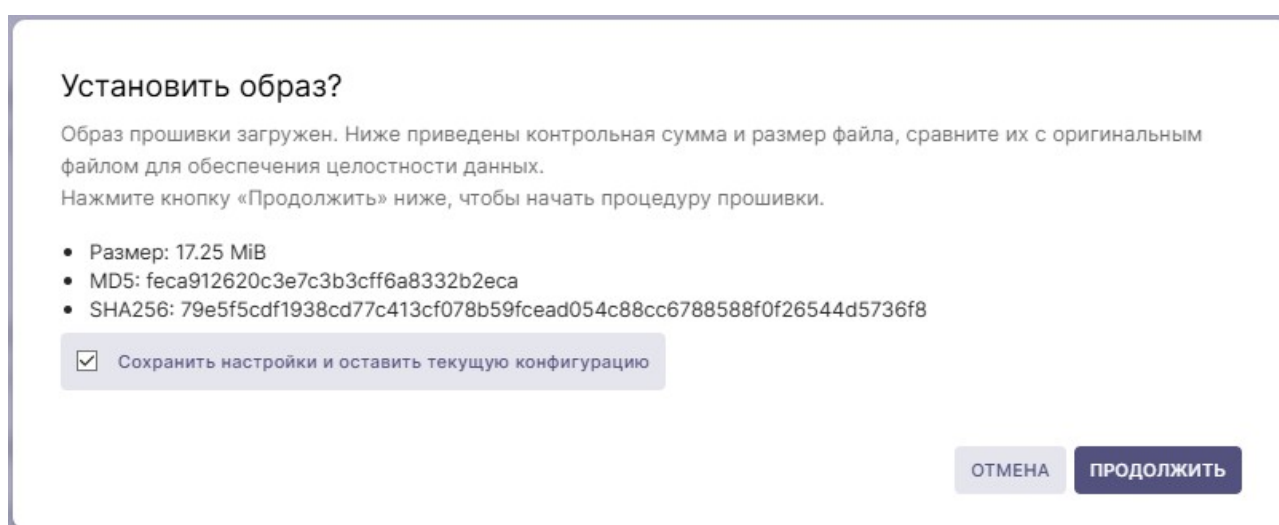


Рис. 6.6.3 Подтверждение обновления

Обновление занимает несколько минут.

6.7 Сохранение и восстановление резервной копии настроек

Система → Обновление/Восстановление

1. Для сохранения резервной копии настроек, нажмите сначала **«Создать архив»**, а затем **«Скачать архив»** (рис. 6.7.1)

2. Для восстановления настроек из резервной копии нажмите **«Загрузить архив»** (рис. 6.7.1)

Резервная копия настроек привязывается к конкретному устройству, восстановить резервную копию с другого коммутатора невозможно

Создание резервной копии настроек

Нажмите 'Создать архив', чтобы создать резервную копию текущих настроек системы.

Создание резервной копии настроек

СОЗДАТЬ АРХИВ

Скачивание резервной копии настроек

DOWNLOAD ARCHIVE

Восстановление настроек из резервной копии

Чтобы восстановить настройки из ранее созданной резервной копии, нажмите "Загрузить архив".

Восстановить резервную копию

ЗАГРУЗИТЬ АРХИВ...

Пользовательские файлы (сертификаты, скрипты) могут остаться в системе. Чтобы этого не произошло, выполните сначала сброс к заводским настройкам.

Рис. 6.7.1 Сохранение и Восстановление настроек

6.8 Сброс настроек

Система → Обновление/Восстановление

Сброс настроек

Для сброса настроек нажмите "Выполнить сброс".

Сброс настроек на заводские

СБРОСИТЬ НАСТРОЙКИ

Система перезагрузится с настройками по умолчанию (IP адрес: 192.168.0.1)

Перезагрузиться в режим Рекавери

ПЕРЕЗАГРУЗИТЬСЯ В РЕКАВЕРИ

Система перезагрузится в режим рекавери с настройками по умолчанию (IP адрес: 192.168.0.1).

Рис. 6.8.1 Сброс настроек

Для сброса всех настроек на заводские нажмите кнопку «Сбросить настройки». (Рис. 6.8.1)

Рекомендуется сделать перед этим резервную копию настроек.

6.9 Загрузка в режим рекавери

Система → Обновление/Восстановление

В коммутаторе предусмотрен режим восстановления прошивки (режим рекавери). Это минималистичная прошивка, расположенная на разделе диска «только для чтения» (Read Only).

Рекавери поддерживает только одну функцию — обновление основной прошивки.

Рекавери всегда стартует с настройками по умолчанию:

IP: 192.168.0.1 (только WEB интерфейс)
 Логин/Пароль: admin/admin
 VLAN: 1 (Все порты Untagged)

Этот режим необходим в следующих случаях:

- в процессе обновления произошёл сбой и прошивка не запускается. В этом случае коммутатор автоматически перезапустится в режиме рекавери.
- Если в основной прошивке произошёл сбой и не работает обновление ПО, то в режиме рекавери можно принудительно перепрошить коммутатор. Для этого нажмите кнопку «Перезагрузиться в рекавери» (Рис. 6.8.1)

6.10 Перезагрузка

Система → Обновление/Восстановление

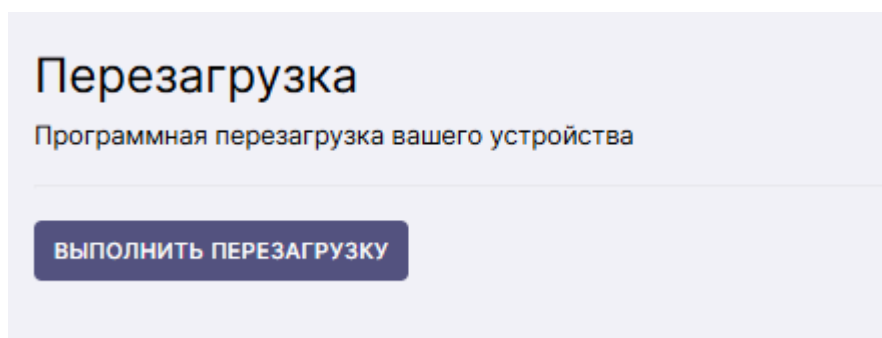


Рис. 6.10.1 Кнопка перезагрузки

Для перезагрузки коммутатора нажмите кнопку «Выполнить перезагрузку»

6.11 Порты

6.11.1 Настройка портов

Порты → Настройка портов

Интерфейс	Состояние	Скорость/Дуплекс	Контроль потока	PoE
Port 1	Включено	Автоматически	Включено	Включено
Port 2	Включено	Автоматически	Включено	Включено
Port 3	Включено	Автоматически	Включено	Включено
Port 4	Включено	Автоматически	Включено	Включено

Рис. 6.11.1 Настройка портов

На данной странице производятся основные настройки портов:

Состояние — включение/выключение порта

Скорость/Дуплекс — доступно либо автоматическое определение скорости на основе автосогласования, либо ручная установка.

Контроль потока — Flow Control - механизм, который управляет передачей данных, чтобы предотвратить перегрузку приемника и потерю данных

PoE - Power-over-Ethernet – возможность управлять подачей питания на выбранном порту

6.11.2 Состояние портов

Порты → Состояние портов

Интерфейс	Состояние	Линк	Скорость/Дуплекс	Контроль потока	PoE
Port 1	Up	Up	100M Full Duplex	RX/TX	Питание подаётся: 2.9W
Port 2	Up	Down	–	RX/TX	Поиск
Port 3	Up	Down	–	RX/TX	Поиск
Port 4	Up	Down	–	RX/TX	Поиск

Рис. 6.11.2 Состояние портов

На данной странице отображается текущий статус работы портов:

Состояние — административное состояние порта (включен ли он в настройках)

Линк — оперативное состояние порта (состояние физического соединения)

Скорость/Дуплекс — фактическое состояние скорости и дуплекса

Контроль потока - фактическое состояние контроля потока

PoE – статус подачи питания через порт.

Может принимать следующие состояния

- **Выключено** — подача питания выключена в настройках
- **Поиск** — подача питания включена в настройках, но фактически не подаётся, т. к. потребитель не подключен
- **Питание подаётся** — PoE потребитель подключен, питание подаётся

6.11.3 Информация об SFP

Порты → Информация об SFP

Информация об SFP

Детальная информация о подключенном SFP модуле (DDM, производитель, тип и т.д.)

Название	Значение
Модуль установлен	Да
Потеря сигнала	Да
Производитель (Vendor)	optronic
Идентификатор производителя	
Номер партии	TBSF15312GSC3C3I
Ревизия	538976321

Рис. 6.11.3 Информация об SFP

Коммутатор поддерживает чтение параметров из SFP модуля.

Следует отметить: информация в модуль записывается производителем модуля, данная информация может использоваться только как ориентировочная.

Многие SFP модули поддерживают функцию DDM (Digital Diagnostics Monitoring) – функция диагностики и мониторинга параметров модуля (температура модуля, оптическая мощность приёмника и передатчика, напряжение питания модуля).

Информацию о значении оптической мощности можно использовать для косвенной диагностики оптической линии.

Рассмотрим примеры для различных ситуаций:

- Рисунок 6.11.3 — всё в норме, выходная мощность передатчика соответствует заявленной в документации на модуль, оптическая мощность сигнала на приёме не меньше чем порог чувствительности, температура не выше температуры эксплуатации.

Температура	38
Напряжение (мВ)	3291
Ток (мкА)	700
Ток смещения передатчика	32991
Мощность передатчика (Дб)	-6.9
Мощность передатчика (мкВт)	2033
Мощность приёмника (Дб)	-8.0
Мощность приёмника (мкВт)	1758

Рис. 6.11.3 Информация об SFP — нормальный уровень затухания

- Рисунок 6.11.4 — температура и выходная мощность в норме, а мощность сигнала на приёмнике низкая, хотя и ещё укладывается в порог чувствительности (-20dBm для данного модуля). В этом случае наблюдаются или могут наблюдаться проблемы в канале связи. Необходимо искать причину высокого затухания сигнала.

Температура	38
Напряжение (мВ)	3291
Ток (мкА)	700
Ток смещения передатчика	32991
Мощность передатчика (Дб)	-6.9
Мощность передатчика (мкВт)	2033
Мощность приёмника (Дб)	-19.2
Мощность приёмника (мкВт)	987

Рис. 6.11.4 Информация об SFP — пониженный уровень сигнала

- Рисунок 6.11.5 — очень низкий уровень входного сигнала, при этом нет связи с удалённой стороной, линк отсутствует. Необходим ремонт оптической линии

Температура	38
Напряжение (мВ)	3291
Ток (мкА)	700
Ток смещения передатчика	32991
Мощность передатчика (Дб)	-6.9
Мощность передатчика (мкВт)	2033
Мощность приёмника (Дб)	-26.7
Мощность приёмника (мкВт)	397

Рис. 6.11.5 Информация об SFP — очень низкий уровень сигнала

6.11.4 Зеркалирование портов

Порты → Зеркалирование портов

Порт назначения

Состояние зеркалирования

Порт назначения

Порт источника

Интерфейс	Режим
Port 1	-
Port 2	RX/TX
Port 3	RX/TX
Port 4	-
Port 5	-

Рис. 6.11.6 Настройка зеркалирования портов

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.

Состояние зеркалирования — глобальное включение/выключение зеркалирования

Порт-назначения — порт, на который будет пересылаться сетевой трафик

Порт-источника — порт с которого пересылается трафик на порт-назначения.

Режим — режим работы зеркалирования на порту (Выключен, Только RX, Только TX, RX/TX)

6.12 VLAN 802.1Q

VLAN → 802.1Q

VLAN (Virtual Local Area Network) — группа устройств, имеющих возможность взаимодействовать между собой напрямую на канальном уровне, хотя физически при этом они могут быть подключены к разным сетевым коммутаторам. И наоборот, устройства, находящиеся в разных VLAN'ах, невидимы друг для друга на канальном уровне, даже если они подключены к одному коммутатору, и связь между этими устройствами возможна только на сетевом и более высоких уровнях.

Management VLAN ID - номер VLAN для сети управления. Доступ к WEB интерфейсу возможен только из данной сети. При необходимости

VID (VLAN ID) – номер виртуальной сети, поддерживается VID в диапазоне от 1 до 4094.

VTU (VLAN Table Unit)- таблица, содержащая список виртуальных сетей, сконфигурированных на данном коммутаторе.

Описание — простое текстовое описание записи VLAN.

Состояние порта в данном VLAN. Порт может быть в 3-х состояниях:

- **N** (Не является членом) - порт не является членом данного VLAN.
- **U** (Нетегированный порт) — при прохождении кадра через данный порт метка тега VLAN не добавляется, либо снимается.
Нетегированным порт может быть только в одном VLAN
- **T** (Тегированный порт) - при прохождении кадра через данный порт метка тега VLAN добавляется, либо, если она уже присутствует в кадре, то проверяется.
Для тегированного порта можно установить в соответствие несколько VID.

6.12.1 Пример настройки VLAN

Пусть есть необходимость настроить сеть так, как показано на схеме (5.3.13.1). У нас есть часть сети с видеонаблюдением, часть сети с контролем периметра, их необходимо разделить. Также необходимо ограничить доступ к интерфейсам управления коммутаторов.

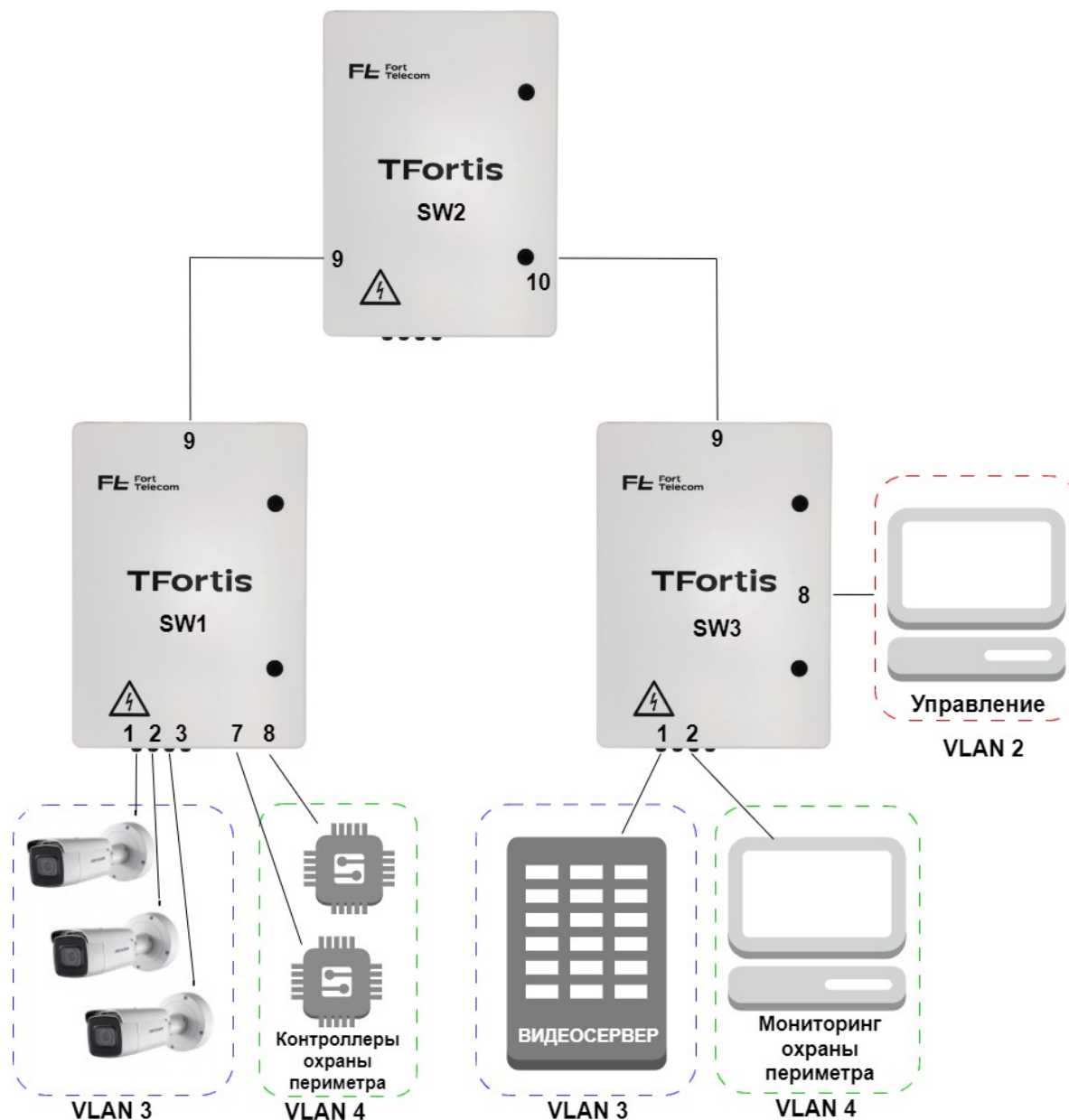


Рис. 6.12.1 Топология сети

Разобьем сеть на несколько VLAN:

VLAN 2 – подсеть управления, с ее помощью управляем коммутаторами SW1, SW2, SW3.

VLAN 3 — подсеть для видеонаблюдения, в него добавлены камеры и видеосервер

VLAN 4 – подсеть для периметральной охраны (периметральные контролеры и сервер охраны)

Настраивать мы будем с ПК Управления.

Начнем конфигурацию с самого удаленного коммутатора **SW1**.

Порты **1-3** принадлежат только **VLAN3** и подключены к конечным устройствам, следовательно эти порты — untagged порты.

Аналогично порты **7, 8** нетегированы в **VLAN4**

Через порт **9** проходят сразу 3 VLAN: **VLAN2, VLAN3, VLAN4**, поэтому установим его в тегированное состояние.

Исходя из этого установим следующие значения:

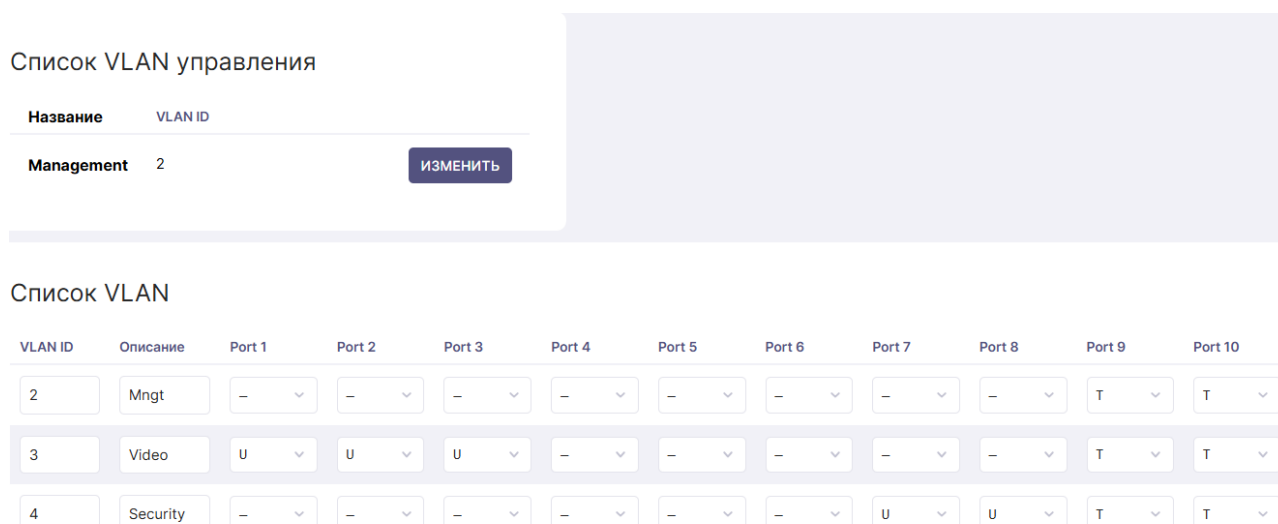


Рис. 6.12.2 Настройка в SW1

Нажмем кнопку **Применить без проверки**. Связь с устройством пропадет.

Конфигурируем коммутатор **SW2**.

Коммутатор пропускает сквозь себя транзитом **VLAN2, VLAN3, VLAN4**, поэтому установим порты **9 и 10** в тегированный режим.

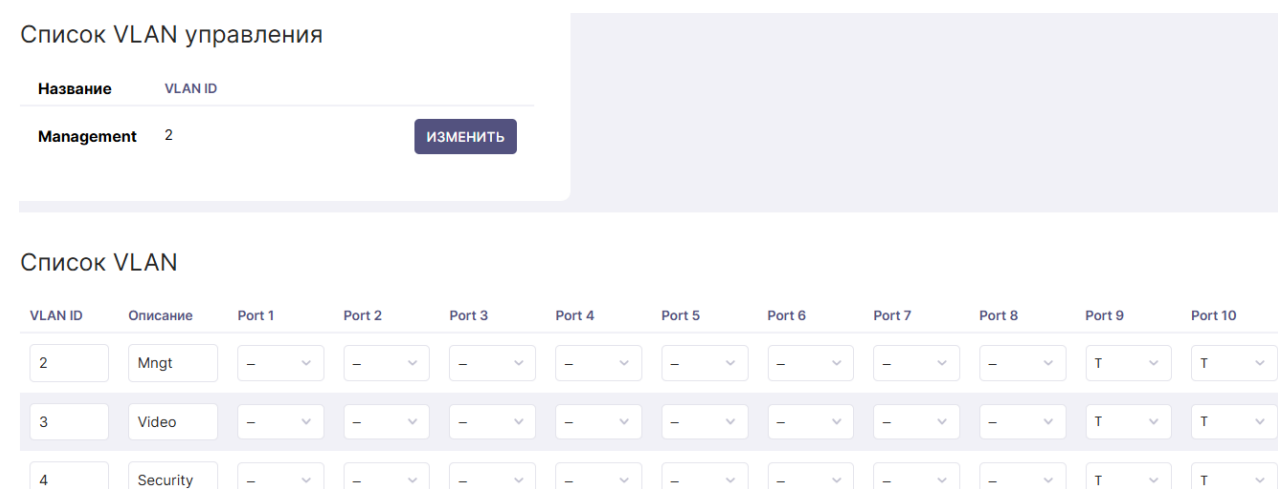


Рис. 6.12.3 Настройка в SW2

Нажмем кнопку **Применить без проверки**. Связь с устройством пропадет. Конфигурируем коммутатор **SW3**.

Установим следующие значения:

Список VLAN управления

Название	VLAN ID
Management	2

ИЗМЕНИТЬ

Список VLAN

VLAN ID	Описание	Port 1	Port 2	Port 3	Port 4	Port 5	Port 6	Port 7	Port 8	Port 9	Port 10
2	Mngt	-	-	-	-	-	-	-	U	T	T
3	Video	U	-	-	-	-	-	-	-	T	T
4	Security	-	U	-	-	-	-	-	-	T	T

Рис. 6.12.4 Настройка в SW3

Нажмем кнопку **Применить**. При этом после применения настроек коммутатор **SW3** останется доступным. Также появится доступ до коммутаторов **SW2** и **SW1** через порт 8 коммутатора **SW3**.

6.13 Настройка STP и RSTP

STP/RSTP → Настройки

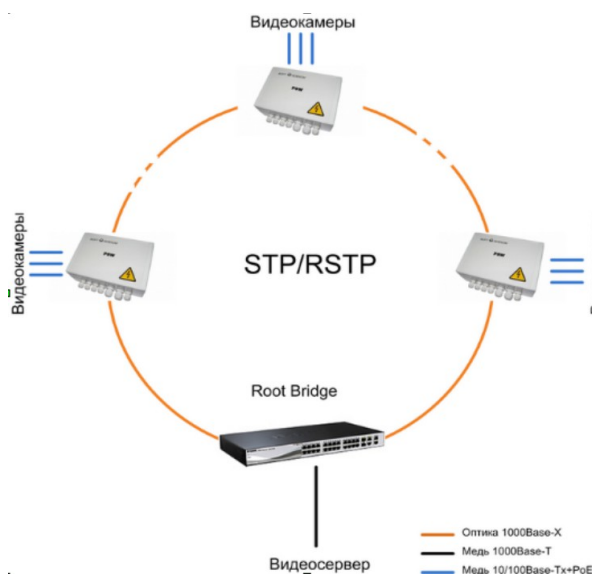


Рис. 6.13.1 Топология типа «кольцо»

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

В коммутаторах PSW реализована поддержка протокола Spanning Tree Protocol (STP, IEEE 802.1d), который позволяет создавать кольцевые маршруты в сетях Ethernet. Постоянно анализируя конфигурацию сети, STP автоматически выстраивает древовидную топологию, переводя избыточные коммуникационные линии в резерв. В случае нарушения целостности построенной таким образом сети (например, обрыв оптики), STP в считанные секунды включает в работу необходимые резервные линии, восстанавливая древовидную структуру сети.

Кроме того, в коммутаторах PSW реализована более мощная разновидность данного протокола - Rapid Spanning Tree Protocol (RSTP, IEEE 802.1w), позволяющая снизить время перестройки сети до нескольких миллисекунд. При использовании RSTP обрыв оптики приводит к кратковременному замиранию картинки от видеокамеры (меньше 1 сек.) с последующим восстановлением нормальной работы.

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

Настройка RSTP

Для большинства случаев достаточно конфигурации по умолчанию, но при необходимости её можно изменить.

Включить	Enable	▼
Глобальное включение STP/RSTP		
Протокол	RSTP	▼
STP — Каждый порт моста посылает STP BPDU; RSTP — Каждый порт моста отправляет RSTP BPDU и автоматически переходит в STP-совместимый режим при обнаружении соединения с мостом, работающим по протоколу STP.		
Приоритет	32768	▼
Приоритет моста (0–61440). Приоритет моста по умолчанию — 32768.		
Время «hello time»	2	
Интервал, с которым мост отправляет hello-пакеты на соседние мосты, чтобы удостовериться, что маршруты исправны (1–10 секунд).		
Время «forward delay»	15	
Задержка перехода корневого и назначенных портов в состояние пересылки (4–30 секунд).		
Время «max age»	20	
Максимальное время, в течение которого конфигурационные BPDU могут удерживаться мостом (6–40 секунд).		
Параметр «transmit hold count»	6	
(1–10)		
Уровень журналирования	Информационные сообщения (2)	▼
Вы можете настроить уровень журналирования		

Рис. 6.13.2 Базовая настройка RSTP

Включение - глобальное включение протокола STP и RSTP, если отключить, коммутатор не будет обеспечивать защиту от петель.

Протокол — выбор протокола: STP или RSTP. Всегда рекомендуется выбирать более быстрый протокол RSTP.

Приоритет — приоритет моста (коммутатора), устанавливается с шагом 4096

(1-32768). Необходим для определения Root Bridge (корневого коммутатора). Корневым коммутатором становится тот, у которого значение Bridge Priority меньше.

Время «Hello Time» - период рассылки BPDU пакетов в секундах (1-2 секунд).

Время «Forward delay» - задержка перехода состояний портов из состояния прослушивания (Listening) и обучения (Learning) в состояние передачи (Forwarding) (в секундах) (6-60).

Время «Max Age» - время ожидания моста в секундах, по истечению которого он сам высылает сообщение о перестроении сети (6-40 секунд).

Transmit Hold Count - ограничение максимального числа посылаемых BPDU пакетов в секунду (1-10).

Уровень журналирования — при возникновении проблем в работе протокола, можно временно повысить уровень логирования для более подробного анализа поведения и диагностики проблем.

Настройка портов

Приоритет - приоритет порта (0-240) меняется с шагом 16.

Стоимость маршрута - стоимость пути порта (1-200000000). При наличии нескольких альтернативных путей всегда выбирается тот, у которого сумма стоимостей пути минимальна. Стоимость порта зависит от его пропускной способности, для порта FastEthernet – 200000, для порта GigabitEthernet – 20000. 0 – автоматическое определение стоимости маршрута.

Автоматическое пограничное состояние - ручное или автоматическое определение пограничного порта. Edge port – это такой порт, который напрямую соединяется с сегментом сети, где создание петли является невозможным. Примером пограничного порта может служить порт, напрямую соединяемый с рабочей станцией. Порты, которые сконфигурированы как пограничные, переходят в состояние продвижения пакетов немедленно, минуя состояния прослушивания и изучения. Пограничный порт теряет свой статус сразу же, как только он принял BPDU-пакет, становясь при этом обычным портом spanning tree.

Административное пограничное состояние — если галочка **Автоматическое пограничное состояние** отключена, то эта настройка задаёт состояние пограничного порта в ручном режиме. Если галочка установлена, то порт перейдёт в режим EDGE

Фильтр BPDU – установленная галочка отключает обработку BPDU на порту, равносильно отключению протокола на порту

Защита BPDU – BPDU Guard - это функция безопасности, которая блокирует

(переводит в состояние err-disabled) порт коммутатора, если он получает BPDU-пакеты.

Интерфейс	Приоритет	Стоимость маршрута	Административное пограничное состояние	Автоматическое пограничное состояние	Фильтр BPDU	Защита BPDU
Port 1	128	0	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Port 2	128	0	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Port 3	128	0	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Port 4	128	0	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Port 5	128	0	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Рис. 6.13.3 Настройка портов RSTP

При настройке параметров **Forward Delay Time**, **Bridge Hello Time**, **Bridge Max Age** необходимо выполнение следующего условия:

$$2 * (\text{Forward Delay Time} - 1) \geq \text{Bridge Max Age} \geq 2 * (\text{Bridge Hello Time} + 1).$$

После настройки RSTP проконтролируйте результат формирования топологии во вкладке **RSTP Status**.

Подробнее про настройку: **Руководство по настройке RSTP** (<https://tfortis.ru/assets/files/manual/tfortis.-nastrojka-rstp.pdf>)

6.14 Безопасность

6.14.1 Управление через SSH

Безопасность → SSH/HTTPS → Доступ через SSH

Интерфейсы SSH

УДАЛИТЬ

Интерфейс *не определено*

Принимать подключения только на указанном интерфейсе или, если интерфейс не задан, на всех интерфейсах

Порт 22

С помощью пароля

Разрешить SSH аутентификацию с помощью пароля

Порты шлюза

Разрешить удалённое подключение к локальным перенаправленным портам SSH

ДОБАВИТЬ ЭКЗЕМПЛЯР

Рис. 6.14.1 Настройка SSH интерфейсов

Для управления по SSH по умолчанию создан один SSH интерфейс.

Для отключения доступа по SSH просто удалите этот интерфейс. При необходимости можно создать интерфейс заново, либо добавить интерфейсы на разные порты.

Интерфейс — только на выбранных интерфейсах управления будет возможно управление через SSH. Если ничего не выбрано, доступ будет через любые интерфейсы управления.

Порт — номер сетевого порта для SSH (По умолчанию 22)

С помощью пароля — разрешить аутентификацию с помощью пароля, если отключить галочку, доступ будет возможен только по ключам.

Порты шлюза — разрешить удалённое управление через шлюз (из внешней подсети)

6.14.2 SSH ключи

Безопасность → SSH/HTTPS → SSH ключи

Для повышения безопасности можно организовать доступ к SSH управлению через SSH-ключи.

Для этого необходимо:

1. снять галочку «С помощью пароля» в настройке SSH интерфейса (рис 5.3.15.1)
2. Добавить свой публичный ключ в текстовое поле (рис 5.3.15.2) и нажмите «Добавить ключ»

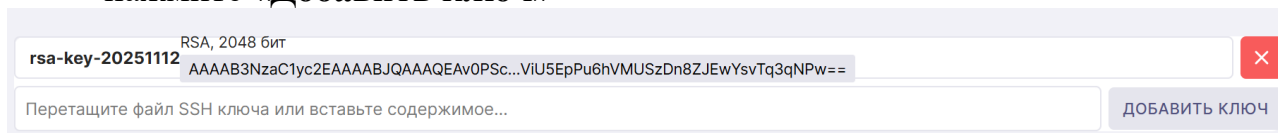


Рис. 6.14.2 Добавление SSH ключа

Создание SSH-ключей и добавление в PuTTY

Ниже краткая инструкция по настройке PuTTY

1. Запустите утилиту PuTTYgen, нажмите Generate, после чего утилита сгенерирует публичный и приватный ключ.

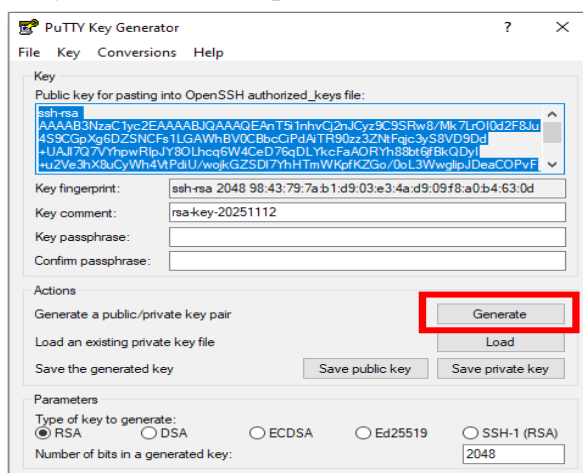


Рис. 6.14.3 Генерация ключей

2. Публичный ключ скопируйте и вставьте в настройки SSH ключей (рис 6.14.2)
3. Сохраните приватный ключ на ПК (Save private key)
4. Запустите утилиту PuTTY, укажите IP адрес и порт

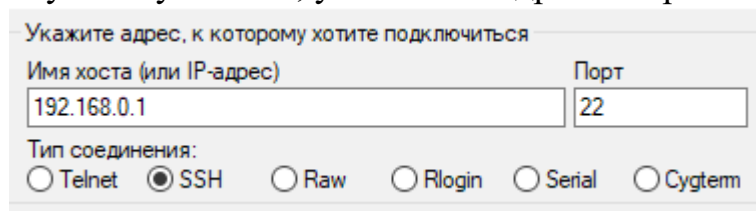


Рис. 6.14.4 Настройка подключения

5. Во вкладке **Соединение** → **SSH** → **Аутентификация** укажите путь до сохранённого файла приватного ключа
6. После чего нажмите **Соединение** для подключения к коммутатору

6.14.3 Настройка HTTP/ HTTPS

Безопасность → *SSH/HTTPS* → *Доступ по HTTP(S)*

HTTPS
Настройка WEB-сервера

Включить HTTP

HTTP порт

Включить HTTPS

HTTPS порт

Только локальное управление
Разрешить доступ только с локальных адресов

SSL сертификат
Вы можете загрузить собственные SSL-сертификаты. По умолчанию используются автоматически сгенерированные самоподписанные сертификаты.

Ключ для SSL сертификата

Опция кэширования SSL сессии

Таймаут SSL сессии

Рис. 6.14.5 Настройка HTTP сервера

Коммутатор поддерживает управление как через HTTP, так и через HTTPS

Включить HTTP – разрешить управление по протоколу HTTP

HTTP порт — сетевой порт для HTTP управления (По умолчанию — 80)

Включить HTTPS - разрешить управление по протоколу HTTPS

HTTPS порт — сетевой порт для HTTPS управления (По умолчанию — 443)

Перенаправлять на HTTPS – принудительно перенаправлять запросы на зашифрованную версию (HTTPS) для повышения безопасности.

Только локальное управление — управление доступно только из локальной сети. Если требуется доступ из внешней сети, снимите эту галочку.

SSL сертификат и ключ для сертификата — для работы HTTPS коммутатор генерирует самоподписанный сертификат. Если есть необходимость заменить его на свой, загрузите через поля ввода свои сертификаты.

6.14.4 Настройка 802.1x для авторизации через RADIUS-сервер

Безопасность → *802.1X*

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

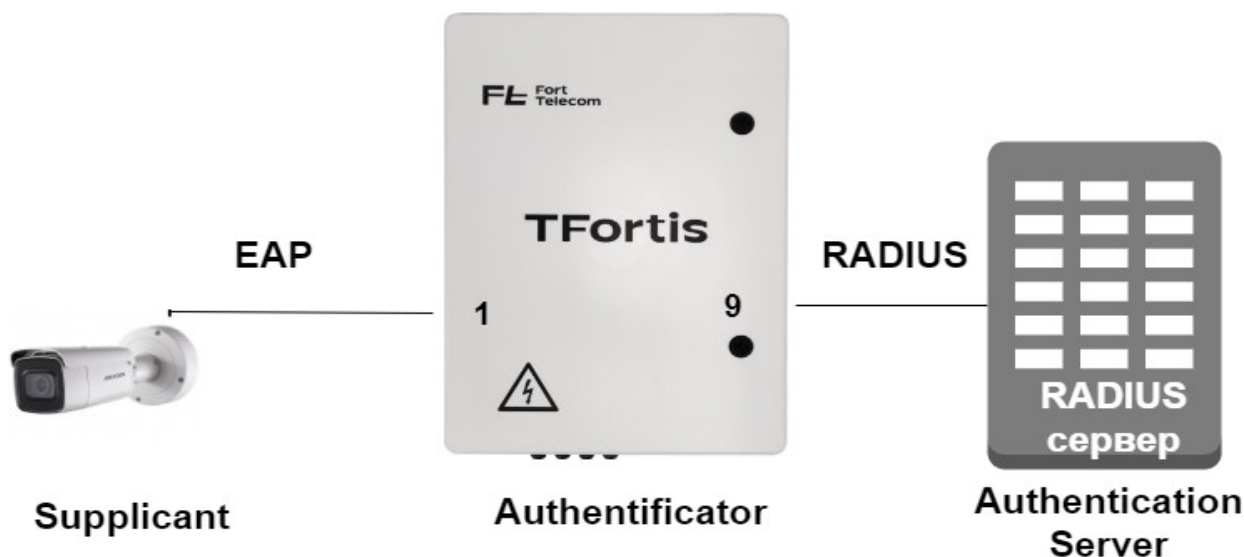


Рис. 6.14.6 802.1X – структура сети

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.

Включить

Сервер аутентификации
Сервер аутентификации RADIUS

Порт для сервера аутентификации

Пароль для сервера аутентификации

Сервер учёта
Сервер учёта RADIUS, если не используется, оставьте пустым

Порт для сервера учёта

Пароль для сервера учёта

Период повторной аутентификации EAP

Корневой сертификат
(PEM или DER файл) для EAP-TLS/PEAP/TTLS

Сертификат сервера
(PEM или DER файл) для EAP-TLS/PEAP/TTLS

Приватный ключ
Приватный ключ, соответствующий сертификату сервера для EAP-TLS/PEAP/TTLS. Он может указывать на тот же файл, что и сертификат сервера, если и сертификат, и ключ находятся в одном файле.

Рис. 6.14.7 802.1X – основные настройки

На вкладке (Рис. 6.14.7) представлены основные настройки аутентификатора **Включить** - глобальное включение режима аутентификатора, если выключено — разрешена передача между всеми портами.

Сервер аутентификации — IP адрес RADIUS сервера, который выполняет аутентификацию клиентов.

Порт для сервера аутентификации — номер порта, на котором работает сервер аутентификации.

Пароль для сервера аутентификации — пароль, который позволяет

удостовериться серверу в том, что запрос прошёл с верного аутентификатора
Сервер учёта — адрес сервера учёта, после успешной аутентификации на сервер учёта отправляется информация о начале сессии.

Порт для сервера учёта — номер порта, на котором работает сервер учёта.

Пароль для сервера учёта — пароль, который позволяет удостоверить серверу учёта в том, что запрос прошёл с верного аутентификатора

Период для повторной аутентификации — период с которым аутентификатор отправляет клиентам повторные запросы на аутентификацию

Корневой сертификат, сертификат сервера и приватный ключ — обеспечение дополнительной безопасности доступа к серверу на основе сертификатов.

Настройки интерфейсов

Состояние 802.1X – включение 802.1X на интерфейсе

Режим — выбор режима: MAC based или Port based

Состояние - текущее состояние порта. Отображается запущена ли служба на порту (Running), а также фактическое состояние интерфейса:

- Blocked – линк на порту отсутствует, либо порт заблокирован в режиме Port based
- Forwarding – линк присутствует и порт работает в MAC based, либо порт работает в режиме Port based и доступ через порт разрешён.

Список клиентов — отображается список подключенных клиентов, с отображением статуса аутентификации

Интерфейсы

Interface	Состояние 802.1X	Режим	Статус	Список клиентов
Port 1	<input type="checkbox"/>	MAC based		
Port 2	<input checked="" type="checkbox"/>	MAC based	Running Forwarding	
Port 3	<input type="checkbox"/>	MAC based		

Рис. 6.14.8 802.1X – настройка интерфейсов

Настройка журналирования

Журналирование



Рис. 5.3.15.9 802.1X – настройка логирования

На вкладке «Журналирование» можно изменить уровень логирования для получения более подробных сообщений в журналах, если это требуется.

6.15 Настройка IGMP

Службы → IGMP

IGMP snooping разработан для предотвращения широковещательной (broadcast) ретрансляции multicast трафика компьютерам-потребителям, которые явно не заявили о своей заинтересованности в нём. Это позволяет коммутаторам исключать такой трафик из потоков, направляемых через порты, к которым не подключено его потребителей, тем самым существенно снижая нагрузку на сеть.

В примере на рис. 6.15.1 камеры подключены к портам 1 - 3. Эти порты являются портами-источниками мультикаста. Потребитель мультикаста (видеосервер) находится за портом 9. На камерах настроено вещание мультикаст трафика, все клиенты мультикаста находятся за портом 9.

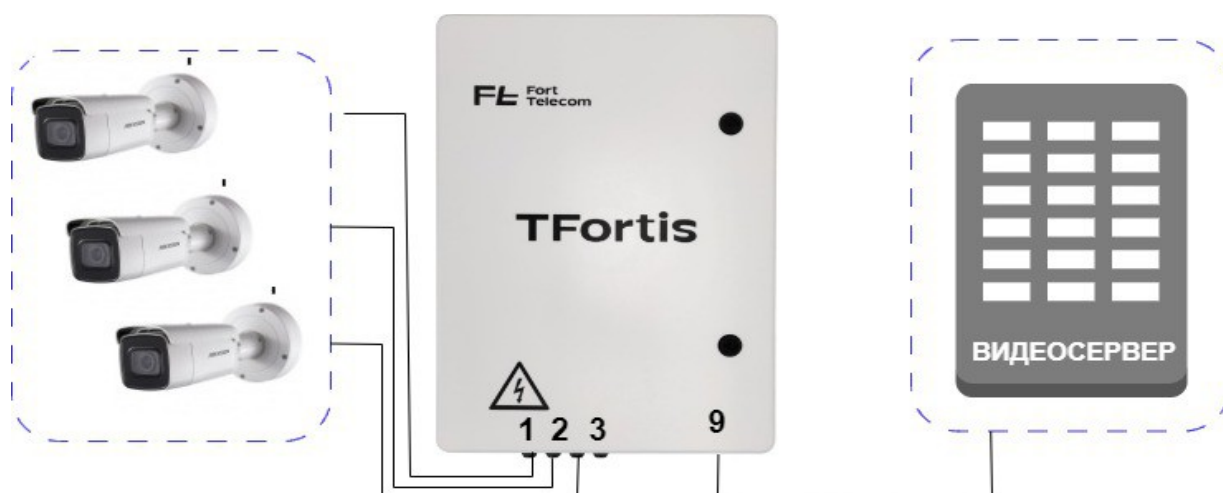


Рис. 6.15.1 Пример сети

При настройках по умолчанию IGMP snooping глобально включен и активен на всех портах. При необходимости можно изменить заводские настройки:

Основные настройки

Включить поддержку IGMP

Включает IGMP snooping на данном мосту

Максимальный размер таблицы слежения

Включить мультикаст querier

Надёжность

Значение надёжности позволяет настроить ожидаемую потерю пакетов в сети. Если в сети ожидаются потери, значение надёжности может быть увеличено. IGMP устойчив к (надёжность - 1) потерям пакетов

Интервал запроса

Интервал в секундах между запросами General. Изменяя значение, администратор может регулировать количество IGMP-сообщений в подсети; чем больше значение, тем реже отправляются IGMP-запросы.

Интервал ответа на запрос

Максимальное время ответа в секундах, добавляемое в периодические общие запросы. Изменяя это значение, администратор может настроить интенсивность IGMP-сообщений в подсети; чем больше значение, тем менее интенсивным становится трафик, поскольку ответы хостов распределяются по большему интервалу.

Интервал последнего членства

Максимальное время ответа (в секундах), интервал времени между сообщениями о выходе из группы. Это значение можно настроить для изменения задержки выхода из группы. Уменьшение значения приводит к сокращению времени обнаружения потери последнего участника группы.

Применяемая версия IGMP

Применяемая версия MLD

Рис. 6.15.2 настройка IGMP Snooping

- **Включить поддержку IGMP** - состояние протокола IGMP, можно включить или отключить.
По умолчанию - включено
- **Максимальный размер таблицы слежения** – максимальное число IGMP клиентов на устройстве, можно установить значение меньше, ограничив максимальное число клиентов.
По умолчанию - 512
- **Включить мультикаст Querier** – коммутатор может становиться Querier

и посылать General Query. Если в сети есть другой Querier, то необходимо **отключить** эту галочку.

По умолчанию - отключено

- **Надёжность** - количество IGMP Query без ответа, после отправки которых коммутатор удалит запись IGMP snooping. Если в сети возможны потери, рекомендуется увеличить это значение.
По умолчанию — 2
- **Интервал запроса** - интервал времени между отправкой сообщений Query (1-255 секунд).
По умолчанию **125 секунд**.
- **Интервал ответа на запрос** - максимальное время ожидания ответа от хоста на отправку периодических общих Query. (1-25 секунд). По умолчанию **10 секунд**.
- **Интервал последнего членства** - максимальное время ответа (в секундах), интервал времени между сообщениями о выходе из группы. Это значение можно настроить для изменения задержки выхода из группы. Уменьшение значения приводит к сокращению времени обнаружения потери последнего участника группы.
По умолчанию — 1 секунда
- **Применяемая версия IGMP** – можно выбрать определённую поддерживаемую версию IGMP
По умолчанию поддерживаются все версии
- **Применяемая версия MLD** – можно выбрать определённую поддерживаемую версию MLD
По умолчанию поддерживаются все версии

Настройки интерфейсов:

- **Включить поддержку мультикаста** - активность IGMP Snooping на выбранном порту. Если галочка снята, мультикаст будет обрабатываться по правилам бродкаста
- **Включить мультикаст fast leave** - сразу же исключать порт из таблицы передачи многоадресного трафика при получении им сообщения о выходе из группы. Это позволяет прекратить передачу по сети ненужных потоков данных и более эффективно использовать полосу пропускания.

Статистика IGMP

На данной странице отображается список мультикаст клиентов с привязкой к портам и номеру VLAN

Статистика IGMP

Информация о IGMP группах

	Группа	Порт	VLAN
27	224.168.100.1	Port 8	2
3	239.192.152.143	Port 8	2
4	239.255.102.18	Port 8	2
5	239.255.255.250	Port 8	2

Рис. 6.15.3 Статистика мультикаст клиентов

6.16 Настройка SMTP

Службы → SMTP


SMTP – (Simple Mail Transfer Protocol) протокол передачи e-mail сообщений по сети. SMTP используется для передачи сообщений на почтовый сервер. SMTP используется для отправки информационных сообщений

Настройки SMTP

Включить

SMTP сервер

Пользователь

Пароль 

Порт

Использовать TLS

Получатель для тестового Email

Отправить тестовый Email

Результат теста

Рис. 6.16.1 Настройка SMTP

Параметры настройки:

- **Включить** — состояние SMTP
- **SMTP сервер** - IP адрес или доменное имя почтового сервера
- **Пользователь** - почтовый адрес отправителя/имя учётной записи на почтовом сервере
- **Пароль** — пароль от учётной записи
- **Порт** - номер TCP порта, через который происходит отправка писем (0 - 65534).
По умолчанию 25.
- **Использовать TLS** – включить шифрование для передачи писем
- **Получатель для тестового Email** – почтовый адрес, который используется только для тестирования настроек. Имя получателя для отправки информационных сообщений указывается в настройках Логирования (Логирование → Настройки).

Для проверки корректности настроек есть возможность отправки тестового письма. Нажмите **ТЕСТ** для отправки тестового письма. В поле **Результат теста** отобразится статус отправки.

Существует несколько вариантов организации работы электронной почты:

- В локальной сети находится специально выделенный почтовый сервер.
- Используется внешний почтовый сервер.

У каждого варианта есть свои достоинства и недостатки. Вариант с выделенным почтовым сервером можно порекомендовать в том случае, если сеть видеонаблюдения физически отделена от сети Интернет и невозможно использовать внешние почтовые сервисы, либо в сети уже существует почтовый сервер и не требуется дополнительных усилий по созданию и поддержанию работы сервера. Использование внешних почтовых сервисов делает настройку проще и быстрее, избавляет от необходимости содержать почтовый сервер, однако в таком случае требуется постоянное подключение к сети Интернет, что не всегда может быть возможным из-за политик безопасности предприятия.

6.17 LLDP

Службы → LLDP

Link Layer Discovery Protocol (LLDP) — протокол канального уровня, позволяющий сетевому оборудованию оповещать оборудование, работающее в локальной сети, о своём существовании и передавать ему свои характеристики, а также получать от него аналогичные сведения.

Информация, собранная посредством LLDP, накапливается в устройствах и может быть с них запрошена посредством SNMP. Таким образом, топология сети, в которой используется LLDP, может быть получена с управляющего компьютера последовательным обходом и опросом каждого устройства. При этом получаемая информация содержит:

- имя устройства и его описание
- имя порта и его описание
- IP-адрес устройства, по которому оно доступно для управления (запросов) по протоколу SNMP;
- функции устройства — коммутация (switching), маршрутизация (routing)

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

6.17.1 Настройка LLDP

Службы → LLDP → Настройка

Основные настройки Сетевые интерфейсы **Расширенные настройки**

Включить LLDP

Адреса управления данной системы

Адреса управления данной системой. Если не указано, используется первый IPv4 и первый IPv6 адреса. Если указан конкретный IP-адрес, он будет использован как адрес управления без какой-либо проверки.

Задержка отправки

Задержка между двумя передачами LLDP PDU. Значение по умолчанию составляет 30 секунд.

Значение «transmit hold»

Это значение используется для вычисления TTL переданных пакетов, которое является произведением этого значения и задержки передачи. Значение по умолчанию равно 4. Соответственно, значение TTL по умолчанию составляет 120 секунд.

Включить режим «только приём»

С этой опцией LLDPd не будет отправлять какие-либо пакеты. LLDPd будет только прослушивать сеть для обнаружения соседей.

Рис. 6.17.1 Настройка LLDP

- **Включить LLDP** - состояние протокола LLDP.
По умолчанию включен.
- **Адрес управления системы** — используется для информирования о адресе управления, если не указано, то адрес управления определяется автоматически
- **Задержка отправки** — интервал отправки информационных сообщений LLDP. (5-120 секунд)
По умолчанию: 30 секунд
- **Значение Tx Hold**- множитель хранения (2 - 10), используется для расчёта TTL(время хранения записи об устройстве)
($TTL = \text{Message Transmit Interval} * \text{Tx Hold Multiplier}$)
- **Включить режим «только приём»** - LLDP будет только прослушивать сеть, но отправлять пакеты не будет.
- **Сетевые интерфейсы** – состояние протокола LLDP на порту. При включении, порт принимает и отправляет LLDP сообщения. Если ничего не указано, LLDP будет использовать все доступные порты.
- **Сетевые интерфейсы, используемые для вычисления ID шасси** -
Указывается какие интерфейсы будут использоваться для вычисления идентификатора шасси (chassis ID). Если интерфейсы не указаны, будут использованы все интерфейсы. LLDP получит первый MAC-адрес из всех доступных интерфейсов для вычисления ID шасси.
По умолчанию: не указаны

Расширенные настройки

В разделе расширенных настроек можно изменить класс устройства, настроить ограничение на рассылку определённых параметров, изменить поведение при обнаружении нескольких соседей

6.17.2 Статистика LLDP

Службы → LLDP → Состояние

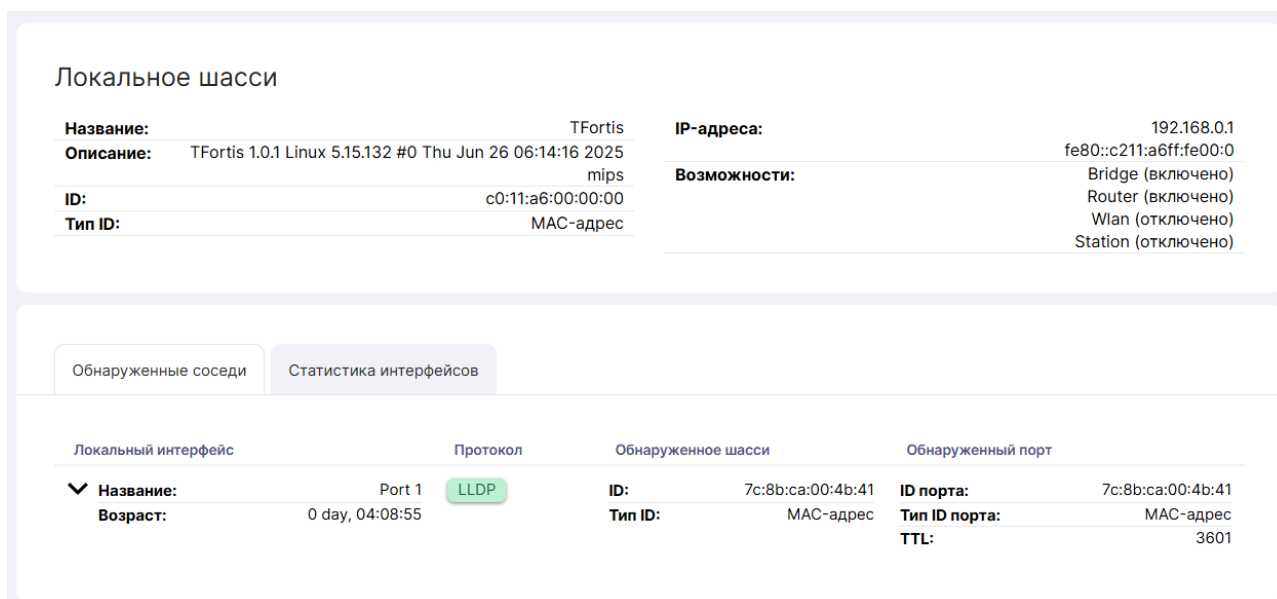


Рис. 6.17.2 Страница статистики LLDP

Локальное шасси — информация о настройке самого коммутатора, его идентификаторах и возможностях.

Обнаруженные соседи — информация об обнаруженных соседях на портах.

Статистика интерфейсов - статистика о режиме работы интерфейса и статистике принятых/отправленных пакетов LLDP.

6.18 SNMP

Службы → SNMP

SNMP (Simple Network Management Protocol) — протокол, который используется для управления и мониторинга за сетевыми устройствами. С помощью протокола SNMP, программное обеспечение может получать доступ к информации, которая хранится на управляемых устройствах (например, на коммутаторе). На управляемых устройствах SNMP хранит информацию об устройстве, на котором он работает, в базе данных, которая называется MIB.

Глобальная настройка

Включить SNMP – глобальное включение/выключение SNMP

Порт — номер порта, на котором работает SNMP

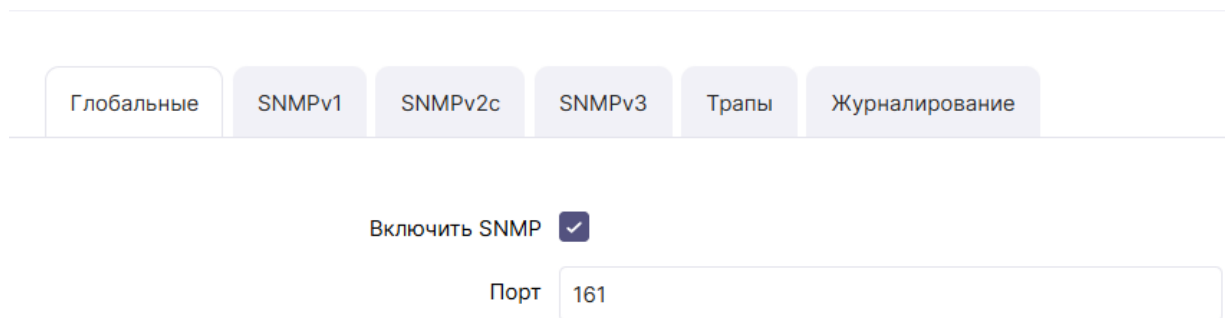


Рис. 6.18.1 Глобальная настройка SNMP

6.18.1 Настройка SNMP v1 / v2c

Настройки SNMP v1 и v2c схожи, рассмотрим на примере SNMP v1

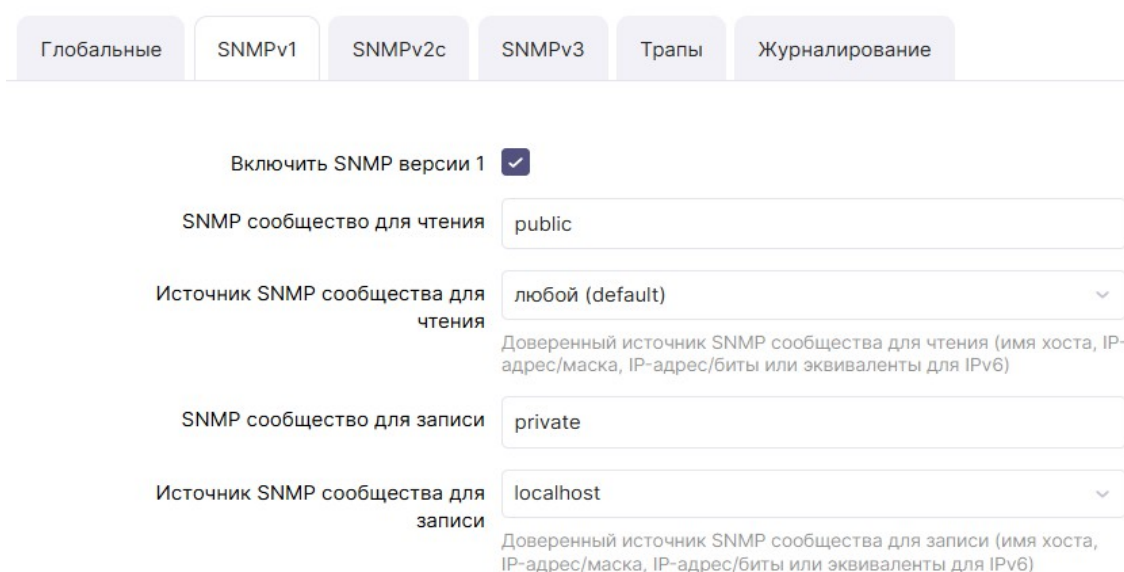


Рис. 6.18.2 Настройка SNMP v1 / v2c

- **Включить SNMP версии 1** — включение поддержки конкретной версии.
- **SNMP сообщество для чтения** — имя сообщества только для чтения параметров, строка используемая для аутентификации в SNMP v1/v2c.
- **Источник SNMP сообщества для чтения** — это то имя хоста или IP адрес, которому разрешено чтение данных с этого устройства.
Может принимать следующие значения:
 1. localhost – фактически запрещено чтение
 2. любой(default) - чтение разрешено с любого узла
 3. пользовательский — чтение разрешено с указанного узла
- **SNMP сообщество для записи** — имя сообщества, используемое для записи параметров, строка используемая для аутентификации в SNMP v1/v2c.
- **Источник SNMP сообщества для записи** — это то имя хоста или IP

адрес, которому разрешено записывать данные на этого устройство.
 Может принимать следующие значения:

1. localhost – фактически запрещена запись
2. любой(default) - запись разрешена с любого узла
3. пользовательский — запись разрешена с указанного узла

6.18.2 Настройка SNMP v3

SNMP v3 обеспечивает более высокий уровень безопасности по сравнению с SNMP v1 и v2c

The screenshot shows the configuration page for SNMPv3. At the top, there are tabs for 'Глобальные', 'SNMPv1', 'SNMPv2c', 'SNMPv3', 'Трапы', and 'Журналирование'. The 'SNMPv3' tab is active. The settings are as follows:

- Включить SNMP версии 3:**
- Имя пользователя SNMPv3:** test
- Тип аутентификации SNMPv3:** ничего
- Пароль аутентификации SNMPv3:** masked
- Тип шифрования SNMPv3:** ничего
- Пароль шифрования SNMPv3:** masked
- Разрешить запись:**

Рис. 6.18.3 Настройка SNMP v3

- **Включить SNMP версии 3** — включение поддержки конкретной версии.
- **Имя пользователя SNMPv3** – имя пользователя используемое для чтения и записи в SNMPv3
- **Тип аутентификации SNMPv3** — выбор способа аутентификации
 - *ничего* — аутентификация не используется
 - *SHA* – используется аутентификация по паролю, алгоритм SHA
 - *MD5*– используется аутентификация по паролю, алгоритм MD5
- **Пароль аутентификации SNMPv3** — пароль, используемый для аутентификации по методам SHA и MD5
- **Тип шифрования SNMPv3** — выбор алгоритма шифрования:
 - *ничего* — шифрование не используется
 - *AES* – используется шифрование AES
 - *DES* – используется шифрование DES
- **Пароль шифрования SNMPv3** — пароль, используемый для

- шифрования по алгоритмам AES и DES
- **Разрешить запись** — включить возможность записи параметров

6.18.3 Настройка SNMP Трапов

SNMP Трапы — это асинхронные сообщения, испускаемые коммутатором

Рис. 6.18.4 Настройка SNMP Трапов

Включение SNMP трапов — разрешить отправку трапов

Версия SNMP трапов — версия SNMP: 1 или 2c

Порт — номер UDP порта. По умолчанию - 162

SNMP сообщество — строка сообщества для трапов.

6.19 Настройка входов/выходов

Специальные → Входы/Выходы

Коммутаторы TFortis оснащены разъемами для подключения контактных датчиков (сухих контактов) и встроенным датчиком вскрытия. Они могут использоваться для целей безопасности, например, для контроля вскрытия шкафа.

Варианты передачи тревожного события:

1. Через протоколы Syslog, SMTP, SNMP Trap. При срабатывании сухого контакта формируется сообщение, которое отправляется на сервер, где организуется приём, логирование и информирование оператора о возникшем событии.

2. С использованием блоков интеграции **Teleport-1**, который имеет цифровые выходы, можно настроить трансляцию срабатывания сухого контакта в коммутаторе PSW на выход в БИ Teleport. Другими словами, если произошло замыкание входа на коммутаторе, который значительно удалён от сервера, то на блоке интеграции Teleport, который может устанавливаться в серверной одновременно замыкается выход. И уже выход можно просто подключить к любой охранной системе. Данный функционал пока не реализован

6.19.1 Настройка входов

Специальные → Входы/Выходы

Входы

Название	Активно	Аварийное состояние	Текущее состояние
sensor1	<input checked="" type="checkbox"/>	Замкнуто	Разомкнуто
sensor2	<input checked="" type="checkbox"/>	Замкнуто	Разомкнуто

Рис. 6.19.1 Настройка входов

Коммутатор имеет 2 входа типа «сухой контакт»:

- **Sensor 1** – пользовательский вход, предназначен для подключения различных датчиков с релейным выходом (СМК, датчик движения, и др.)
- **Sensor 2** – вход для подключения штатного датчика вскрытия (СМК)

Входы имеют следующие настройки:

- **Активно** - разрешение работы входа. Аварийное сообщение будет отправлено, если произошло совпадение **Аварийное состояние** и **Текущее состояние**
- **Аварийное состояние** - состояние входа, которое считается аварийным.
- **Текущее состояние** - текущее состояние входа.

6.19.2 Релейный выход

Специальные → Входы/Выходы

Коммутатор имеют встроенное оптореле, которое можно использовать для управления различными исполнительными устройствами.

Управление реле возможно в двух режимах:

- 1) Ручное управление. (через web-интерфейс, snmp, ssh)
- 2) Трансляция состояние входа с удалённых устройств (Например блоков интеграции Teleport-1). **Пока в разработке**

ВЫХОДЫ

Название	Состояние	Текущее состояние
relay	Разомкнуто	Разомкнуто

Рис. 6.19.2 Настройка выхода

6.19.3 Датчик температуры/влажности (опция)

Специальные → Входы/Выходы

Датчик температуры

Название	Состояние	Температура	Влажность
SHT01	Подключен	29.3	30

Рис. 6.19.3 Датчик температуры/влажности

Коммутаторы TFortis поддерживают подключение дополнительных датчиков температуры и влажности.

На данный момент поддерживаются датчики SHT-01.

6.20 ИБП

Специальные → ИБП

Название	Значение
Модуль ИБП	Ок
Источник питания	Внешнее питание
Напряжение АКБ	26.125 V
Ток через АКБ	164 mA
Ток зарядки	26.175 V
Аппаратная версия	0
Версия ПО	9
Температура	32 °C

Рис. 6.20.1 Статистика по работе ИБП

Коммутаторы TFortis серии UPS имеют встроенный источник бесперебойного питания. На данной странице приводится статистика по работе узлов ИБП.

6.21 Настройка контроля зависания видеокamer

Специальные → *Авторестарт камер*

Данная функция предназначена для автоматического перезапуска видеокamеры при ее зависании. Перезапуск осуществляется только в том случае, когда камера питается по PoE.

Автоматическая перезагрузка невозможна, если питание осуществляется через внешний блок питания, либо от стороннего PoE инжектора.

Интерфейсы

Интерфейс	Критерий	IP-адрес	Мин. скорость, Кб/с	Макс. скорость, Кб/с	Запланировать перезагрузку	Время вкл.	Время выкл.	Статус	Ручная перезагрузка
Port 1	Ping	192.168.1.1			<input type="checkbox"/>				ПЕРЕЗАГРУЗКА
Port 2	Speed		100	3000	<input type="checkbox"/>				ПЕРЕЗАГРУЗКА
Port 3	Disable				<input checked="" type="checkbox"/>	23:59	23:58		ПЕРЕЗАГРУЗКА
Port 4	Link				<input type="checkbox"/>				ПЕРЕЗАГРУЗКА
Port 5	Disable				<input type="checkbox"/>				ПЕРЕЗАГРУЗКА

Рис. 6.21.1 Настройка контроля зависания камер

Коммутатор поддерживает несколько критериев оценки работы камер:

- **Link** - пропадание сигнала **Link** от видеокamеры. Если при активном статусе подачи PoE, на порту будет отсутствовать линк более 1 минуты, то камера будет перезагружена
- **PING** - отсутствие ответов на служебные запросы **Ping**. Если отсутствуют ответы на запросы ICMP в течении 1 минуты, то камера будет перезагружена
- **Speed** — интенсивность трафика на порту отличается от заданных границ. В общем случае укажите только нижнюю границу скорости (Мин. скорость), если скорость опустится ниже заданной границы, то камера перезагрузится.

Если указать минимальную и максимальную скорость, то камера будет перезагружена, если скорость на порту будет выходить за заданный диапазон.

Скорость указывается в **Кбит/сек.**

- **Запланировать перезагрузку** – перезагрузка по расписанию. Можно включить перезагрузку камеры по расписанию. Указывается время включения и выключения порта.
- **Состояние** — статус работы камеры, ошибки. Если камера работает без сбоев, то отображается строка **Ок**. Если зафиксировано зависание камеры и она не проходит проверку по критериям, то отобразится ошибка. Если камера перезагружалась, то будет отображаться время последней перезагрузки и общее число перезагрузок.
- **Перезагрузка** — ручная перезагрузка камеры. При нажатии на эту кнопку на порту будет отключено PoE на 20 секунд

Если включен контроль зависания по критериям Ping и Speed, то дополнительно запускается проверяется статус Link.

6.22 Средства диагностики

6.22.1 Дистанционный пинг

Диагностика → Пинг-запрос

Пинг-запрос — Утилита для проверки доступности указанного адреса, отправляет 4 пакета по 32 байта на указанный адрес и контролирует их возвращение.

Трассировка - позволяет проследить маршрут следования данных до указанного адреса.

DNS запрос - запрос, отправляемый на DNS-сервер для преобразования доменного имени в IP-адрес

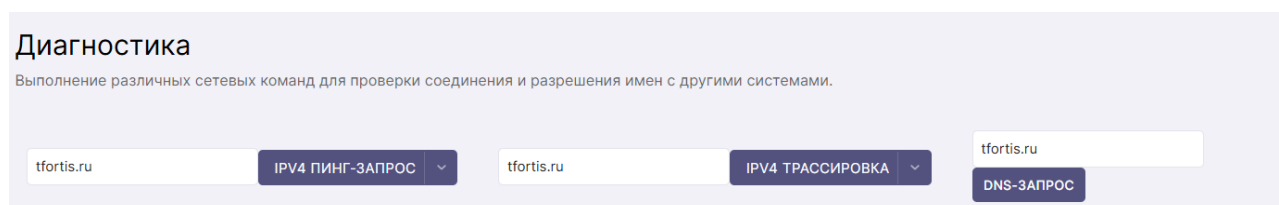


Рис. 6.22.1 Инструменты сетевой диагностики

6.23 Статистика

6.23.1 Статистика портов

Статистика → Статистика портов

Статистика портов

Детальная статистика о счётчиках пакетов на портах

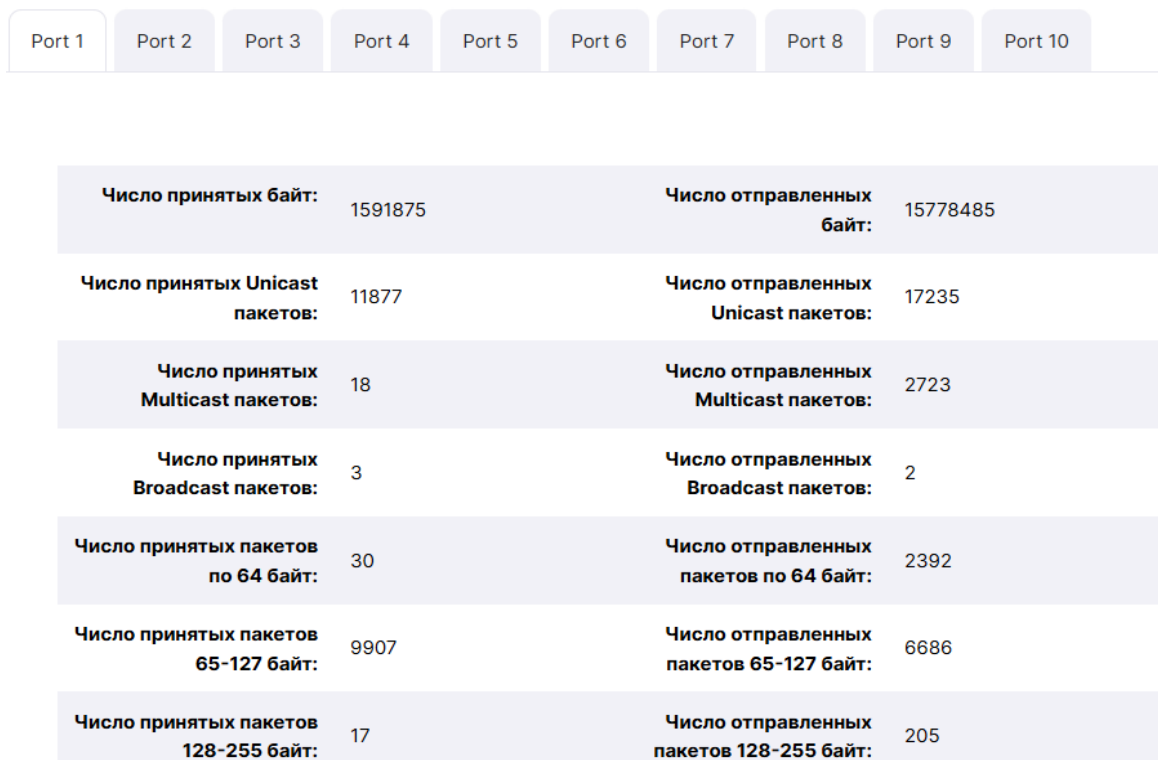


Рис. 6.23.1 Статистика по порту 1

Данная страница отображает расширенную статистику по принятым и отправленным данным по каждому порту коммутатора.

Отображается:

- Число принятых и отправленных данных с разбивкой по размеру пакета, доступны следующие диапазоны: 64, 65-127, 128-255, 256-511, 512-1023, 1024-1518, более 1518 байт
- Число принятых и отправленных данных с разбивкой по типу пакета: unicast, multicast, broadcast
- Pause пакеты
- Число пакетов, меньше минимального размера, пакетов, больше максимального размера
- Число пакетов с следующими типами ошибок: Rx MacDiscards, SingleCollisionFrames, MultipleCollisionFrames, LateCollisions, ExcessiveCollisions, SymbolErrors, ControlInUnknownOpCodes, DeferredTransmissions, dot1dTpPortInDiscards

6.23.2 Графики загрузки интерфейсов

Статистика → Графики → Интерфейсы

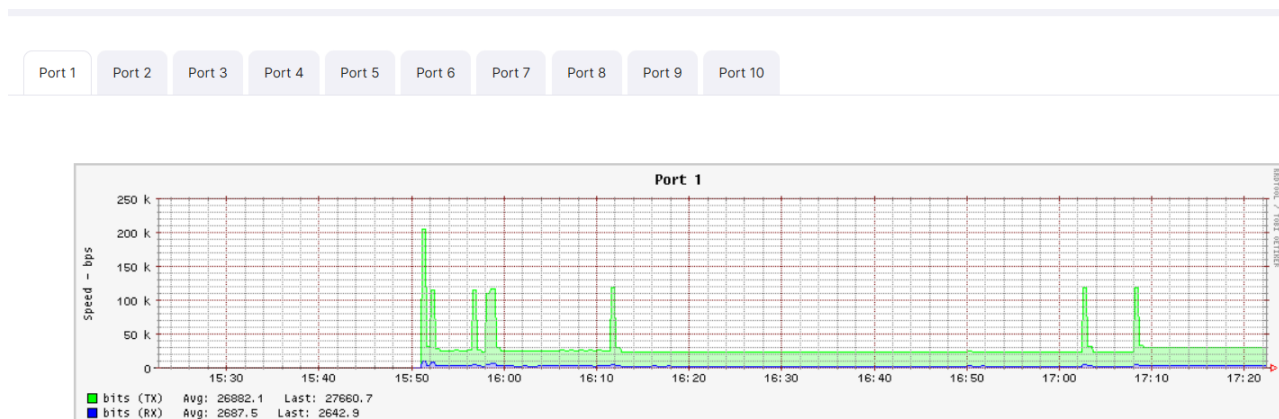


Рис. 6.23.2 График загрузки интерфейса

Данная страница отображает статистику загрузки интерфейсов в виде графика. Отображаются принятые и отправленные данные в бит/с.

Можно выбрать диапазон отображения графика:

- последние 2 часа
- последний день
- последняя неделя
- последний месяц
- последний год

Но следует отметить, что все данные хранятся в оперативной памяти, поэтому сбрасываются при перезагрузках.

6.23.3 Графики загрузки системы

Статистика → Графики → Оперативная память и Загрузка системы

На данной странице отображаются графики расхода оперативной памяти и загрузки CPU. Эти инструменты помогают при диагностике системы.

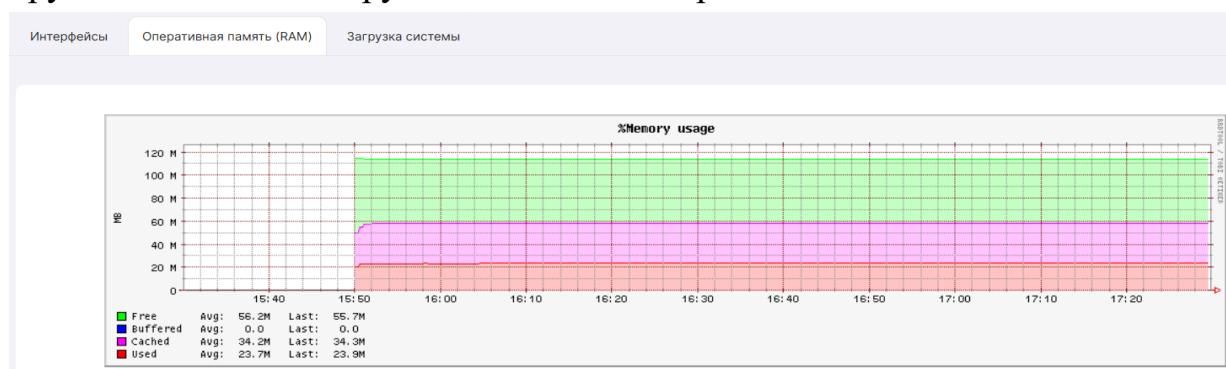


Рис. 6.23.3 График расхода оперативной памяти

6.23.4 Таблица MAC адресов

Статистика → ARP/MAC таблицы → MAC таблица

Показать VLAN:

Фильтр записей:

№	MAC	VLAN	Интерфейс
1	7c:8b:ca:50:00:d4	VLAN1	Port 1
2	7c:8b:ca:77:02:d7	VLAN1	Port 1
3	7c:8b:ca:75:e6:d9	VLAN1	Port 1
4	7c:8b:ca:84:4f:4a	VLAN1	Port 1
5	7c:8b:ca:69:15:f8	VLAN1	Port 1
6	7c:8b:ca:48:d3:8f	VLAN1	Port 1
7	7c:8b:ca:f6:22:91	VLAN1	Port 1
8	7c:8b:ca:d0:6b:c4	VLAN1	Port 1
9	7c:8b:ca:45:d3:d8	VLAN1	Port 1
10	7c:8b:ca:61:8d:be	VLAN1	Port 1
11	7c:8b:ca:e6:1d:f0	VLAN1	Port 1
12	7c:8b:ca:f4:cc:cf	VLAN1	Port 1
13	7c:8b:ca:eb:b3:a6	VLAN1	Port 1
14	7c:8b:ca:49:2c:80	VLAN1	Port 1
15	7c:8b:ca:77:02:d7	VLAN1	Port 1

Рис. 6.23.4 Таблица MAC адресов

На данной странице отображается таблица MAC адресов (FDB Table) – привязка MAC адреса к порту и VLAN.

В верхней части есть Фильтр по VLAN, а также текстовая строка поиска (Для фильтрации по MAC адресам или портам)

6.23.5 ARP Таблица

Статистика → ARP/MAC таблицы → ARP таблица

Страница содержит ARP кэш процессора коммутатора, представленный в виде таблицы.

Фильтр записей:

№	IP	MAC	Интерфейс
1	192.168.0.102	7c:8b:ca:00:4b:41	switch.1

Рис. 6.23.5 ARP Таблица

6.24 Журналирование

6.24.1 Журналы

Логирование → Журналы

Журнал в оперативной памяти | Журнал во флеш-памяти | Журнал ядра

Отображать по убыванию времени (последнее сверху)

Отображать приоритеты: Notice (122) | Info (666) | Error (15) | Warning (27) | Critical (2)

Отображать столбцы: № | Временная метка | Тег | Приоритет | Категория | Сообщение

Фильтр записей:

№	Временная метка	Тег	Приоритет	Категория	Сообщение
832	19.11.2025 18:18:16	netifd	Notice	daemon	Network device 'lan8' link is down
831	19.11.2025 18:18:16	mstpd[2087]	Info	daemon	set_if_up: Port lan8 : down
830	19.11.2025 18:18:16	kernel	Info	kern	switch: port 9(lan8) entered disabled state
829	19.11.2025 18:18:16	kernel	Info	kern	rt183xx-switch switch@1b000000 lan8: Link is Down
828	19.11.2025 18:18:15	kernel	Info	kern	switch: port 9(lan8) entered blocking state
827	19.11.2025 18:18:15	kernel	Info	kern	rt183xx-switch switch@1b000000 lan8: Link is Up - 1Gbps/Full - flow control off
826	19.11.2025 18:18:15	netifd	Notice	daemon	Network device 'lan8' link is up
825	19.11.2025 18:18:15	mstpd[2087]	Info	daemon	set_if_up: Port lan8 : up
824	19.11.2025 18:18:15	mstpd[2087]	Info	daemon	set_if_up: Port lan8 : down
823	19.11.2025 18:18:15	mstpd[2087]	Info	daemon	MSTP_OUT_flush_all_fids: switch:lan8:0 Flushing forwarding database

Рис. 6.24.1 Страница отображения логов

Коммутатор поддерживает запись в следующие журналы:

- **Журнал в оперативной памяти** — записанные данные хранятся в оперативной памяти. Этот тип журнала позволяет записывать большие объемы подробных логов. Данные в журнале хранятся только до момента перезагрузки. По умолчанию используется для записи всех событий от всех компонентов системы.
- **Журнал во флеш-памяти** — записанные данные хранятся на встроенном флеш-накопителе, поэтому сохраняются после перезагрузки. Данный журнал ограничен по объему и по ресурсу накопителя, поэтому предназначен для записи редких и важных событий. По умолчанию на него настроена запись событий об изменении статусов Link и PoE
- **Журнал ядра** — журнал сообщений ядра Linux, хранится также в оперативной памяти.

Страница отображения журналов позволяет:

- фильтровать события по приоритету и ключевым словам
- Скачивать файлы журнала для дальнейшего анализа
- Очищать файлы журналов

6.24.2 Syslog

Логирование → Syslog

Syslog — стандарт отправки сообщений о происходящих в системе событиях (логов), использующийся в IP сетях. Протокол syslog прост: при наступлении определенных событий, коммутатор PSW посылает короткое текстовое сообщение получателю сообщения. Сообщения отправляются по UDP (порт 514). Syslog используется для удобства администрирования и обеспечения информационной безопасности.

Настройки Syslog

Настройки отправки Syslog сообщений

Включить

Порт

Протокол внешнего сервера системного журнала

Рис.6.24.2. Настройка Syslog

Включить — глобальное включение поддержки syslog

Порт — UDP порт сервера приёма syslog сообщений

Протокол внешнего сервера — протокол, через который будут отправляться логи

Адрес сервера настраивается отдельно на странице настройки логирования.

Получение Syslog сообщений

После настройки коммутатора, переходим к настройке сервера.

Рассмотрим пример для ОС Windows. Существует большое число программ для работы с syslog-сообщениями. Вот некоторые из них:

- Kiwi Syslog
- Syslog Watcher
- Datagram SyslogServer Suite
- syslogbroadband
- LogZilla
- Syslog Server Free Tool

Остановим свой выбор на программе Kiwi Log Viewer - это бесплатная упрощенная версия программы Kiwi Syslog Server. Но тем не менее она

удовлетворяет поставленным задачам.

Адрес для загрузки - <http://www.kiwisyslog.com/downloads.aspx>

Установка программы не отличается особой сложностью, единственное, в окне Choose Operating Mode установите Install as Service (В этом случае Kiwi Syslog установится как служба: будет запускаться при старте ОС и резидентно сидеть в трее)



Рис. 6.24.3. Установка программы Kiwi Syslog

После установки, запускайте программу. По умолчанию в главном окне будут отображаться все принятые сообщения. Эти сообщения пишутся в текстовый файл. Также есть возможность настроить пересылку на email.

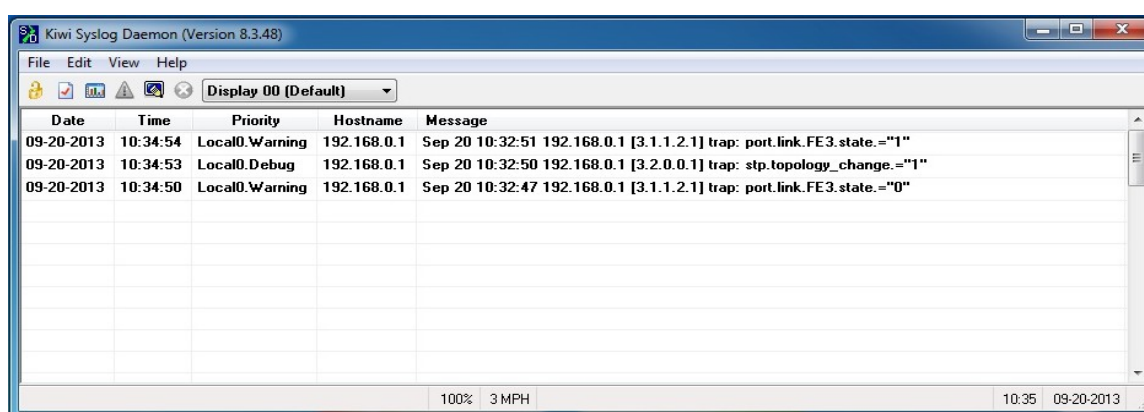


Рис. 6.24.4. Интерфейс программы Kiwi Syslog

6.24.3 Настройка логирования

Логирование → Настройки

Настройка правил обработки всех событий происходит на этой странице (Рис. 6.24.5).

Общий подход к обработке событий такой:

1. Возникает какое-то событие (Например: изменился линк на порту 1)
2. Для этого события находится соответствующее правило фильтрации события. Если правило не нашлось, то событие дальше никак не обрабатывается.
3. Если для события нашёлся соответствующий **фильтр**, то запускается соответствующее **действие**.

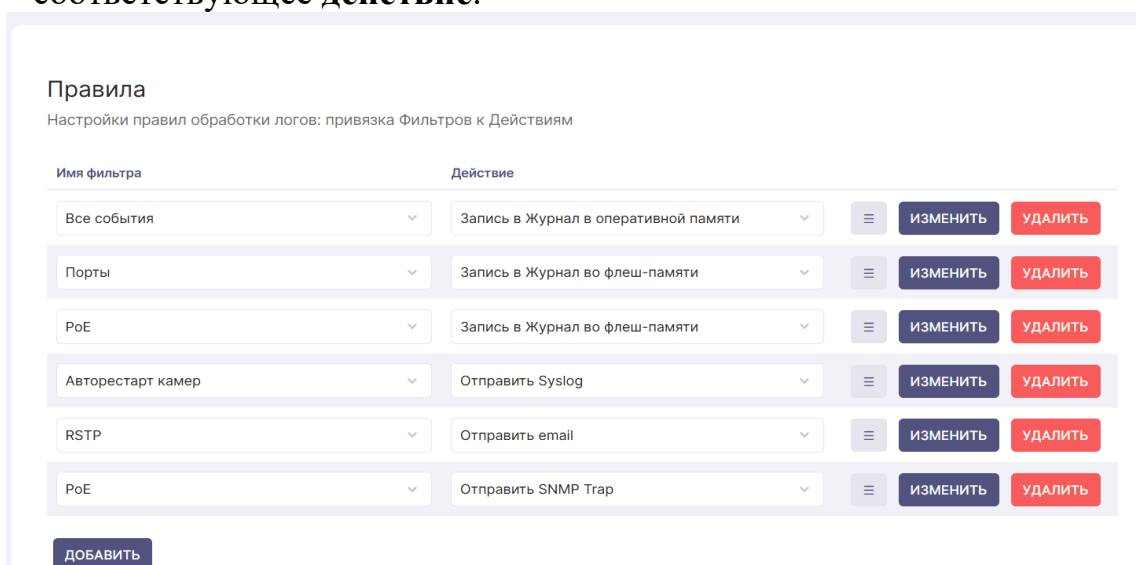


Рис. 6.24.5. Интерфейс настройки правил обработки событий

Фильтры

По умолчанию созданы базовые фильтры событий:

- События ядра – события ядра
- Все события
- Порты
- PoE
- RSTP
- 802.1X
- Авторестарт камер
- TFDM
- SNMP
- LLDP

Дополнительно можно создавать пользовательские фильтры.

Для создания фильтра, нажмите Добавить, после чего заполните следующие

ПОЛЯ:

The screenshot shows a web interface for configuring a filter. It contains five main input fields, each with a label and a dropdown or text input:

- Название**: A text input field.
- Категория**: A dropdown menu with an asterisk (*) selected. Below it is a note: "Выберите необходимую Категорию, * - все категории. Будут логироваться все события с выбранной категорией".
- Уровень важности**: A dropdown menu with an asterisk (*) selected. Below it is a note: "Выберите необходимый уровень важности, * - любая важность. Будут логироваться все события с выбранным уровнем важности и выше".
- Имя Тега**: A text input field. Below it is a note: "Фильтр по Тегу, пустая строка - отсутствие фильтра".
- Содержит**: A text input field. Below it is a note: "Фильтр по тексту сообщения, пустая строка - отсутствие фильтра".

Рис. 6.24.6. Интерфейс настройки фильтра

Название - простое текстовое описание фильтра.

Категория — выбор необходимой категории, указан стандартный список категорий (Facility). Если нет подходящей категории, оставьте «*» (любая категория)

Уровень важности — выбор необходимого уровня важности. Будут логироваться все события с выбранным уровнем важности и выше.

Например, если выбран уровень важности Warning, то будут логироваться события с уровнем Warning, Error, Critical и т. д.

Если уровень важности не важен, то установите - «*»

Имя Тега — имя тега, часто — это имя программы, которая была источником события. Пустая строка — отсутствие фильтра.

Содержит — фильтр по содержимому сообщения. Будет фильтроваться событие, которое включает текст из фильтра.

Действия

При срабатывании фильтра запускается выполнение определённых действий.

Поддерживаются следующие действия:

- Запись в журнал в оперативной памяти
- Запись в журнал во флеш-памяти
- Отправка Syslog
- Отправка Email
- Отправка SNMP трапа

Запись в журнал в оперативной памяти

Записанные данные хранятся в оперативной памяти. Этот тип журнала позволяет записывать большие объёмы подробных логов. Данные в журнале хранятся только до момента перезагрузки.

По умолчанию используется для записи всех событий от всех компонентов

системы.

При достижении размера в 40 000 строк, файл журнала ротится: удаляются 30 % самых старых сообщений.

Запись в журнал во флеш-памяти

Записанные данные хранятся на встроенном флеш-накопителе, поэтому сохраняются после перезагрузки. Данный журнал ограничен по объему и по ресурсу накопителя, поэтому предназначен для записи редких и важных событий.

При достижении размера в 30 000 строк, файл журнала ротится: удаляются 30 % самых старых сообщений.

Отправка Syslog

Сообщение отправляется на внешний Syslog сервер. Предварительно нужно настроить Syslog на странице Логирование → Syslog. На вкладке «Действия» указывается один или несколько серверов, на которые будет отправляться.

Рис. 6.24.7. Настройка действия на отправку syslog

Отправка Email

Сообщение отправляется на почтовый сервер. Предварительно нужно настроить SMTP (*Службы* → *SMTP*)

При настройке Действия указываются: тема письма и один или несколько получателей (рис 6.24.8)

Рис. 6.24.8 Настройка действия на отправку email

Отправка SNMP трапа

Сообщение отправляется в виде SNMP трапа на указанный адрес сервера. Предварительно нужно настроить SNMP и активировать в нём поддержку Трапов (*Службы* → *SNMP*)

Название	<input type="text" value="Отправить SNMP Трап"/>
Действие	<input style="border-bottom: 1px solid #ccc;" type="text" value="Отправить SNMP Трап"/> ▾
Сервер	<input type="text" value="192.168.0.100"/> <input style="background-color: #333; color: white; border: none; padding: 2px 5px;" type="button" value="+"/>

Рис. 6.24.9 Настройка действия на отправку SNMP трапа

6 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
- Telegram: @tfortis_support
https://t.me/tfortis_support

Вся техническая документация доступна на сайте:

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/>

Приложение А. Коды аппаратных ошибок и их расшифровка

Коммутаторы TFortis серии Pro имеют встроенные средства самодиагностики. При возникновении неполадок, индикатор Alarm начинает мигать. Число миганий индикатора до задержки в 3 секунды соответствует коду ошибки.

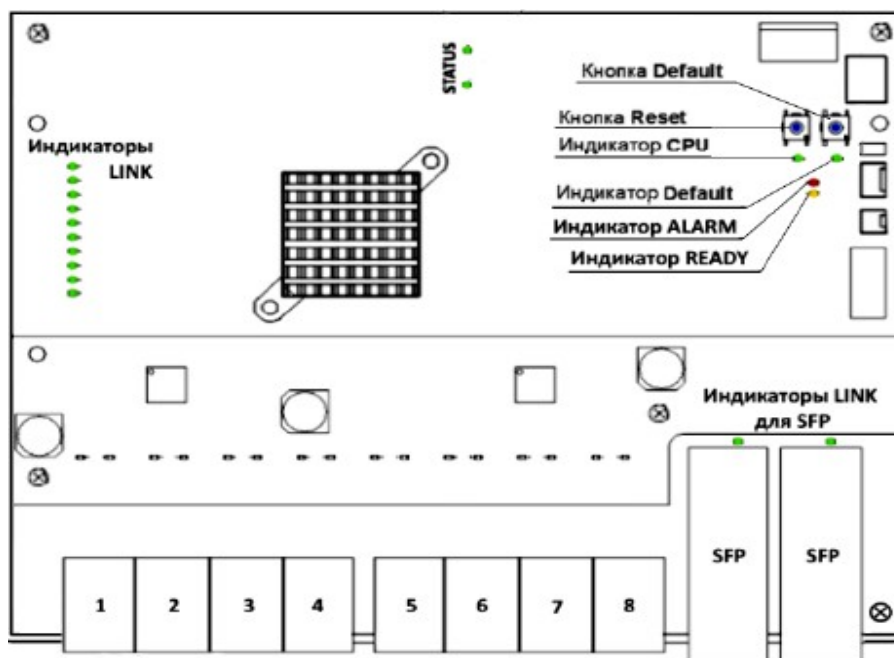


Рис.А.1. Расположение индикатора Alarm на плате

Код ошибки	Описание
1, 2, 3	Внутренние опорные напряжения находятся не в диапазоне. Коммутатор может работать нестабильно.
4	Ошибка в коммуникации с периферийным микроконтроллером. Основные функции коммутатора работают, может не работать периферия (входы/выходы, датчики температуры, SFP DDM)
5,6,7	Ошибки PoE контроллера. В этом случае может не подаваться питание по PoE, либо отсутствует индикация PoE в интерфейсе.