ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

KRAFTWAY TELECOM OPERATING SYSTEM ВЕРСИЯ 3

Руководство администратора

643.18184162.00095-03 90

Листов 135

АННОТАЦИЯ

Настоящее руководство администратора содержит сведения об операциях, которые можно осуществлять с помощью программного обеспечения Kraftway Telecom Operating System Версия 3 (далее – ПО KTOS), обозначение 643.18184162.00095-03.

В данном руководстве описаны назначение, условия применения ПО KTOS и инструкции по базовой настройке управляемого коммутатора, а также приведены команды для его конфигурирования и управления.

Настоящее руководство предназначено для технических специалистов в области сетей передачи данных, которые занимаются установкой, настройкой и обслуживанием управляемых коммутаторов (далее - коммутатор) и знакомы с принципами построения сетей передачи данных и технологией Ethernet.

СОДЕРЖАНИЕ

1. ОБЩИЕ СВЕДЕНИЯ

1.1. Обозначение и наименование

Полное наименование программного обеспечения – Программное обеспечение Kraftway Telecom Operating System Версия 3.

Краткое наименование программного обеспечения – ПО KTOS.

Обозначение программного обеспечения – 643.18184162.00095-03.

1.2. Назначение ПО KTOS

ПО KTOS предназначена для реализации основных функций коммутатора по соединению нескольких электронных вычислительных машин (далее – ЭВМ) и других сетевых устройств в пределах одного или нескольких сегментов сети.

Также ПО KTOS может применяться для:

- определения маршрута следования информации в сети;
- назначения устройствам сетевых адресов;
- классификации данных с установкой приоритетов для их передачи;
- логирования сообщений;
- управления файлами конфигурации;
- проверки контрольной суммы программного обеспечения (далее – ПО);
- управления скоростью передачи данных.

ПО KTOS осуществляет постоянную поддержку соединений со всеми демонами протокола, хранение данных конфигурации и обширные возможности мониторинга и регистрации.

1.3. Функции и возможности ПО KTOS

ПО KTOS при функционировании и взаимодействии в составе вычислительной сети будет:

- обеспечивать возможность сегментирования локальной вычислительной сети на отдельные виртуальные локальные сети в соответствии со стандартом IEEE 802.1Q;
- обеспечивать предотвращение петель в топологии сети Ethernet по протоколу связующего дерева (Spanning Tree) в соответствии со стандартами IEEE 802.1D-2004 Edition STP, IEEE 802.1D-2004 Clause 17 Rapid Spanning Tree Protocol, IEEE 802.1Q-2005 Clause 13 Multiple Spanning Tree Protocol;
- поддерживать возможность статического и динамического по протоколу LACP агрегирования каналов передачи данных, проходящих через физические интерфейсы, согласно стандарту IEEE 802.1AX-REV-D3.1;

– обеспечивать взаимодействие с коммуникационным оборудованием на основе технологии виртуальных локальных сетей в соответствии со стандартом IEEE 802.1Q;

– поддерживать управление сетевыми пакетами, маркированными в соответствии с ГОСТ Р 58256-2018;

– поддерживать зеркалирование трафика;

– поддерживать функционал Port security;

– поддерживать функцию фильтрации сетевого трафика на 2-4 уровнях модели OSI/ISO;

– поддерживать логические туннельные интерфейсы с использованием протокола GRE;

– поддерживать статическую маршрутизацию IPv4, IPv6;

– поддерживать предоставление адресов IPv4 по технологии DHCP;

– поддерживать возможность синхронизации встроенных часов от внешних источников системы единого времени по протоколу NTP;

– поддерживать функционал тестирования кабеля на интерфейсах 10BASE-T/100BASE-TX/1000BASE-T с целью обнаружения обрывов или повреждений с использованием технологии TDR.

Для обеспечения управления и мониторинга ПО KTOS будет:

– обеспечивать возможность разграничения прав управления для пользователей с разным уровнем доступа;

– обеспечивать контроль целостности ПО и общесистемного программного обеспечения (далее – ОПО);

– обеспечивать возможность настройки параметров с помощью протоколов Telnet, SSH v2;

– обеспечивать возможность мониторинга параметров с помощью протокола SNMP v.1/2c/3;

– обеспечивать возможность настройки параметров с помощью web-интерфейса;

– обеспечивать возможность регистрации сообщений о событиях во внутреннем и/или внешнем системном журнале Syslog. Внутренний системный журнал Syslog будет храниться в энергонезависимой памяти изделия;

– обеспечивать возможность аутентификации и авторизации пользователей;

– обеспечивать возможность запроса и получения сведений о подключенных оптических приемопередатчиках SFP/SFP+;

– обеспечивать возможность поддержки протокола ICMP;

– обеспечивать возможность сброса счетчиков сетевых интерфейсов.

1.4. Работа с интерфейсами коммутатора

ПО KTOS обеспечивает работу всех сетевых интерфейсов в следующих режимах:

– «порт доступа» - режим коммутации (OSI Layer 2) без тегирования, определенного в стандарте IEEE 802.1q;

– «магистральный порт» - режим коммутации (OSI Layer 2) с тегированием IEEE 802.1q;

– «маршрутизируемый порт» - режим маршрутизации (OSI Layer 3).

Назначение интерфейсу ПО KTOS режима работы выполняется через интерфейс командной строки (далее – ИКС) или графический пользовательский интерфейс (GUI).

ПО KTOS обеспечивает создание виртуального интерфейса агрегации, объединяющего несколько физических интерфейсов, а также удаление виртуальных интерфейсов из таблиц коммутации и прочих структур данных.

В приложении 1 приведены таблицы соответствий номеров портов внешних панелей коммутаторов и идентификаторов интерфейса в интерфейсе командной строки Kraftway Telecom Operating System версия 3 (далее - KTOS) для различных моделей устройств.

1.5. Условия применения

1.5.1. Программное обеспечение, необходимое для функционирования ПО KTOS

Все составляющие ПО KTOS поставляются в предустановленном виде и являются самодостаточным ПО, не требующим для своего функционирования предустановки дополнительного ПО.

Также для взаимодействия с ПО KTOS можно рекомендовать следующее ПО, которое может быть установлено на компьютер администратора:

– программа для загрузки исполняемых и конфигурационных файлов в устройство по протоколу TFTP - tftpd32 или аналогичная программа;

– утилита для прямой записи на флеш-диск (команда dd в linux или ее аналог в других операционных системах (далее – ОС);

– ОС с поддержкой файловой системы FAT на флеш-накопителях.

В приложении 2 приведены сведения об установке самоподписанного сертификата для создания защищенного соединения между браузером на компьютере администратора и web-интерфейсом коммутатора.

1.5.2. Требования к аппаратному обеспечению

Технические характеристики коммутаторов, необходимые для работы ПО KTOS, приведены в таблице 1.

Таблица 1

Наименование параметра	Значение
Элементы передней панели, шт.: – порт Gigabit Ethernet (1 Гбит/с) – порт uplink SFP+ (10 Гбит/с) – консольный порт RJ-45 – индикатор питания (POWER) – индикатор статуса (SYS) – кнопка сброса (RESET)	 24 (48); 4; 1; 1; 1; 1
Производительность: – таблица MAC-адресов, не менее – количество Link Aggregation Groups	 16000; 64 (до восьми физических интерфейсов в одном LAG)
Размер памяти: – Nand, МБ – RAM, МБ	 512; 256
Требования к модулю защиты системного программного обеспечения (ПО)	Реализация командного интерфейса по UART. Сохранение конфигурации U-Boot в памяти SPI. Включение/выключение режима защиты записи в памяти SPI. Контроль целостности образа операционной системы KTOS
Поддержка функционала уровня L2	STP (Spanning Tree Protocol, IEEE 802.1d). RSTP (Rapid Spanning Tree Protocol, IEEE 802.1w). MSTP (Multiple Spanning Tree, IEEE 802.1s). STP Root Guard. STP BPDU Guard. BPDU Filtering. Private VLAN. STP PortFast

Наименование параметра	Значение
Основные возможности на уровне физических интерфейсов	Зеркалирование портов (SPAN)
Требования поддержки VLAN	Поддержка IEEE 802.1Q. Поддержка port based vlan. Поддержка mac based vlan
Требования к работе с MAC таблицей	Поддержка изучения MAC-адресов для каждого VLAN. Настраиваемое время хранения MAC-адресов
Требования к функции Link aggregation	Создание агрегированных интерфейсов (до восьми физических интерфейсов). Объединение физических интерфейсов с помощью протокола lacp. Алгоритмы балансировки нагрузки в агрегированном канале (source/dest mac, source mac, dest mac, source/dest ip, source ip, dest ip)
Требования к функции мониторинга	Поддержка мониторинга загрузки CPU. Мониторинг загрузки RAM. Мониторинг температуры CPU. Статистика интерфейсов
Требования к сервисной функции	Тестирование «на обрыв» кабеля типа «витая пара» по технологии TDR. Получение диагностической информации оптического трансивера по технологии DDM

1.5.3. Организационные меры

Должны быть приняты организационные (организационно-технические) меры, исключающие неконтролируемый доступ посторонних лиц к рабочему месту администратора в нерабочее время, а также в рабочее время при его отсутствии.

2. УСЛОВНЫЕ ОБОЗНАЧЕНИЯ

В таблице 2 представлены условные обозначения, использующиеся в синтаксисе команд ИКС.

Таблица 2

Условное обозначение (форматирование или символы)	Описание
`Команда оператора`	Полужирным моноширинным шрифтом обозначаются команды, вводимые оператором
`Параметр/переменная`	Курсивным моноширинным шрифтом указывается параметр или переменная, вместо которой необходимо задать соответствующее значение
Пример	Прямым моноширинным шрифтом обозначаются примеры введенных команд и результаты их выполнения
[ ]	В квадратных скобках указываются дополнительные необязательные параметры команды
{ }	В фигурных скобках указывается список обязательных параметров, разделенных знаком «|», при этом необходимо выбрать один из вариантов
<Enter> **<Ctrl+F4>**	Полужирным шрифтом в угловых скобках указана клавиша клавиатуры или сочетание клавиш, нажимаемых одновременно
`all`	Когда в команде для определения диапазона портов или параметров требуется задать определенный аргумент, и одним из его значений является «all», то оно является значением по умолчанию

3. ПРЕДВАРИТЕЛЬНАЯ НАСТРОЙКА КОММУТАТОРА

3.1. Подключение к коммутатору через последовательный интерфейс RS-232

Для управления коммутатором локально необходимо подключиться к его консольному порту. После успешной загрузки системы на экране подключенного устройства появится приглашение:

```
ktos login:
```

3.2. Использование интерфейса командной строки

ПО KTOS позволяет установить различные права доступа для различных именованных субъектов. Для разграничения набора прав доступа к командам режимов управления и конфигурирования в ПО KTOS определены три уровня доступа с назначенными для каждого уровня доступа именами и сопоставленными с ними наборами прав доступа к функциональным элементам ПО KTOS:

1) уровень доступа «Оператор»;
2) уровень доступа «Администратор»;
3) уровень доступа «СуперАдминистратор».

Помимо этого, имеется два уровня доступа для режима управления:

– «пользовательский»;
– «привилегированный».

Пользовательский режим управления вне зависимости от уровня доступа именованного объекта обладает минимальным набором прав и возможностей и предназначен для получения сведений о системе.

Для каждого уровня доступа в привилегированном режиме управления и режиме конфигурирования предусмотрен собственный набор команд. Совокупность доступных в конкретный момент команд зависит от текущего режима и уровня доступа. Ввод вопросительного знака «?» после системного приглашения позволяет вывести список доступных команд для текущего режима на текущем уровне доступа.

Именованным субъектам сопоставляются программные идентификаторы уровня доступа, характеризующие набор прав доступа именованного субъекта к функциональным элементам ПО KTOS.

3.3. Встроенные в ПО уровни доступа

3.3.1. Уровень доступа «Оператор»

Команды ИКС, доступные на уровне доступа «Оператор», являются подмножеством команд, доступных на уровнях доступа «Администратор» и «СуперАдминистратор». Команды уровня доступа «Оператор» позволяют просмотреть текущие параметры и получить сведения о системе.

Перечень возможных действий на уровне доступа «Оператор»:

– получение помощи о вводимых командах;

– отображение доступных на уровне «Оператор» текущих параметров ПО KTOS.

Переход из режима управления в режим конфигурирования для уровня доступа «Оператор» не предусмотрен.

3.3.2. Уровень доступа «Администратор»

Набор команд ИКС для уровня доступа «Администратор» включает команды для уровня доступа «Оператор». Уровень «Администратор» обеспечивает доступ к ограниченному режиму конфигурирования с помощью команды `configure terminal`.

Перечень возможных действий на уровне доступа «Администратор»:

– все приведенные права для уровня «Оператор»;

– проверка сетевой доступности узлов (методами `ping` и `traceroute`);

– создание сеанса терминального доступа к управлению коммутатора по протоколам TELNET и SSH;

– изменение параметров текущей сессии;

– работа с файловой системой;

– смена текущей директории;

– просмотр содержимого текущей директории;

– просмотр наименования текущей директории;

– просмотр файла;

– очистка доступных на уровне «Администратор» рабочих параметров ПО KTOS;

– отображение доступных на уровне «Администратор» текущих параметров ПО KTOS;

– конфигурирование доступных на уровне «Администратор» текущих параметров ПО KTOS.

3.3.3. Уровень доступа «СуперАдминистратор»

Набор команд ИКС для уровня доступа «СуперАдминистратор» включает команды для уровня доступа «Администратор». Уровень доступа «Администратор» обеспечивает доступ к полному режиму конфигурирования с помощью команды `configure` и полный доступ ко всем командам режима управления и включает команду сохранения конфигурации `write`.

Перечень возможных действий на уровне доступа «СуперАдминистратор»:

– все приведенные права для уровня «Администратор»;

– сохранение текущей конфигурации устройства в загрузочную конфигурацию;

– создание именованных субъектов;

– изменение параметров именованных субъектов (уровней доступа и паролей);

– удаление именованных субъектов;

– очистка доступных на уровне «СуперАдминистратор» рабочих параметров ПО KTOS;

– отображение доступных на уровне «СуперАдминистратор» текущих параметров ПО KTOS;

– конфигурирование доступных на уровне «СуперАдминистратор» текущих параметров ПО KTOS.

Должен присутствовать как минимум один именованный субъект с сопоставленным с ним уровнем доступа «СуперАдминистратор».

3.4. Режимы ИКС

3.4.1. Классификация режимов ИКС

Для удобства работы ИКС разделен на три режима – «пользовательский режим управления», «привилегированный режим управления» и «режим конфигурирования». Доступ к ИКС начинается с ввода имени пользователя и пароля, соответствующих одному из заданных в конфигурации ПО KTOS именованных субъектов. На диаграмме рис. 1 показана общая иерархия командных режимов.

Общая иерархия командных режимов ИКС

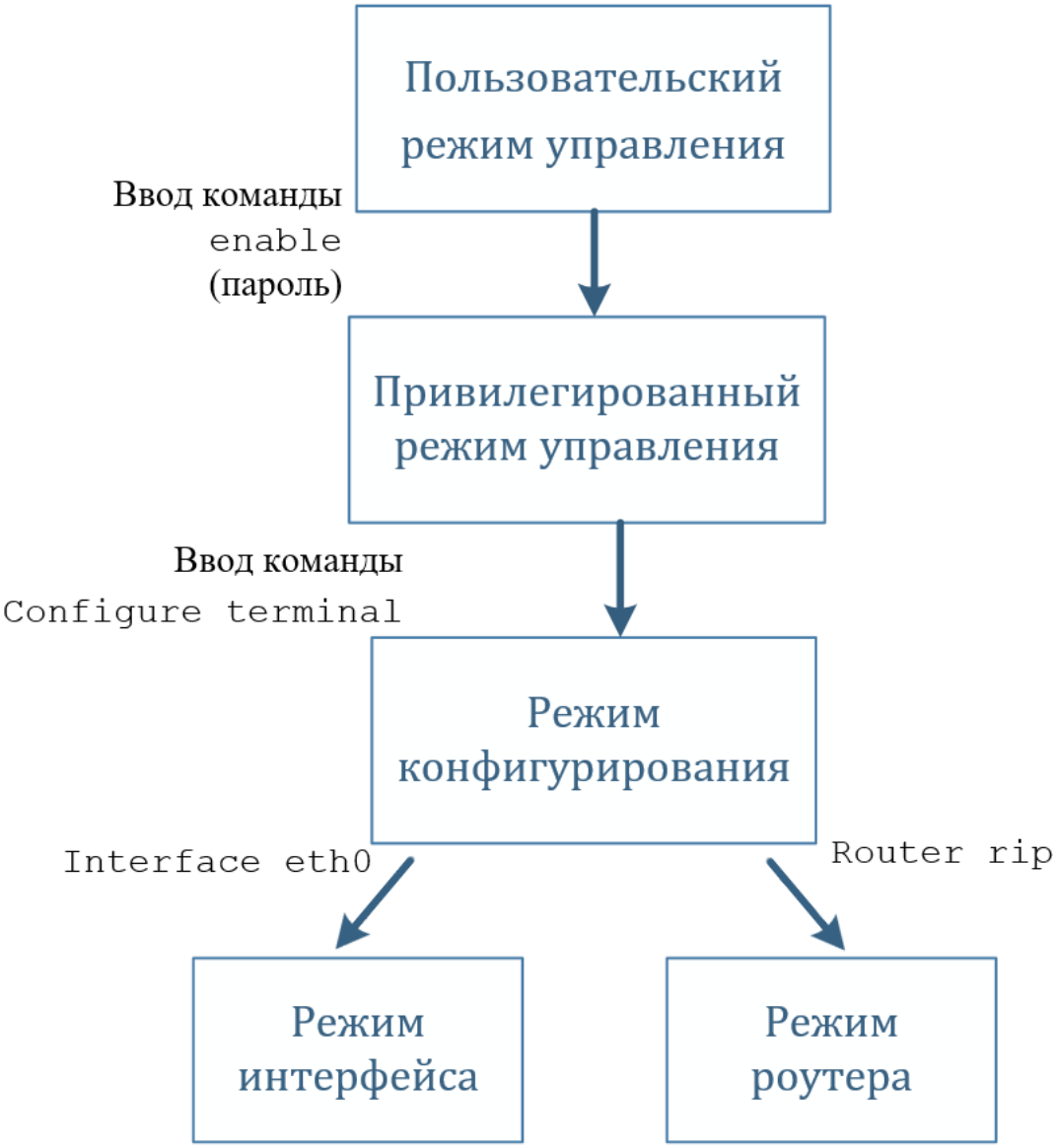


Рис. 1

Системное приглашение для пользовательского режима управления отличается от системного приглашения для привилегированного режима управления. Приглашение для пользовательского режима управления ИКС состоит из имени устройства как узла сети, за которым следует угловая скобка («>»). Приглашение привилегированного режима управления ИКС состоит из имени устройства как узла сети, за которым следует знак решетки («#»).

3.4.2. Пользовательский режим управления

Также называется режим просмотра, это первый режим, который появляется после запуска интерфейса командной строки. Этот уровень управления предназначен для задач, не изменяющих конфигурацию маршрутизатора, здесь можно выполнять основные команды, такие как `show`, `exit`, `quit`, `help` и `enable`.

3.4.3. Привилегированный режим управления

В этом режиме возможно выполнять команды `EXEC`, а также переходить в режим конфигурирования. Войти в привилегированный режим управления можно, введя `enable` в пользовательском режиме управления.

Для возврата в пользовательский режим управления необходимо использовать команду `disable.`

3.4.4. Режим глобальной конфигурации

Команды режима конфигурирования Global Configuration применяются для настройки параметров системы в целом или для перехода в специальные режимы конфигурирования, обеспечивающие настройку специфических элементов, например, интерфейсов или протоколов. Для входа в данный режим необходимо в привилегированном режиме управления ввести команду `configure terminal` и нажать клавишу <Enter>. Для возврата в привилегированный режим управления необходимо использовать команды `exit`, `end` или сочетание клавиш <Ctrl+z>.

3.5. Ввод команд

Команды ИКС представляют собой последовательность ключевых слов и аргументов. Ключевые слова определяют команды, а с помощью аргументов устанавливаются параметры настройки. Например, в команде `show interfaces status te1` слова `show`, `interfaces` и `status` являются ключевыми, `te` является аргументом, задающим тип интерфейса, а 1 является аргументом, задающим конкретный порт. Если параметры команды имеют значения по умолчанию, то они становятся активными при вводе таких команд без указания параметров.

При вводе команд с обязательными параметрами необходимые аргументы задаются после ключевых слов. Например, для того чтобы установить пароль администратора, нужно ввести:
`# username admin password 123abcdefg`.

3.5.1. Буфер команд

Каждая команда, введенная в ИКС, записывается в буфер истории команд, имеющий внутреннее управление. Команды в данном буфере хранятся по принципу «Первый зашел – первый вышел» (FIFO). При этом команды могут быть вызваны повторно, отредактированы и выполнены снова. После перезагрузки устройства содержимое буфера не сохраняется.

По умолчанию буфер истории команд включен, но его в любой момент можно отключить. Подробная информация о синтаксисе команд для включения и отключения буфера истории команд приведена в разделе описания команды `history`.

3.5.2. Отмена действия команды

Перед многими командами, использующимися при настройке устройства, можно ввести префикс «**no**» для отмены действия команды или для сброса настройки к значению по умолчанию.

3.5.3. Автоматическое заполнение команды

Интерфейс командной строки может завершить написание команды или параметра. Для завершения не полностью введенной команды необходимо нажать клавишу <tab>.

Если написание команды или параметра является неоднозначным, строка отобразит варианты, которые соответствуют сокращению.

После ввода `show i` и после нажатия клавиши <tab>, интерфейс покажет:

```
> show i
  interface  ip         ipv6
> show i
```

Строка отображает ключевые слова `interface`, `ip`, `ipv6`. Добавив `n`, чтобы выбрать `interface`, нажмите клавишу `<tab>`. Интерфейс покажет:

```
> show in
> show interface
```

3.5.4. Модификаторы команд

Можно использовать два модификатора, чтобы изменить вывод команды `show`. Модификаторы отображаются после ввода знака вопроса.

```
# show users ?
  | Output modifiers
  > Output redirection
```

Чтобы использовать выходные модификаторы, вводится «`|`» (символ вертикальной черты).

Пример:

```
> show running-config | ?
  begin     Begin with the line that matches
  exclude   Exclude lines that match
  include   Include lines that match
  redirect  Redirect output
```

3.5.4.1. Модификатор Begin

Модификатор Begin отображает выходные данные, начиная с первой строки, содержащей строку ввода (все, что вводится после ключевого слова «begin»). Пример:

```
# show run | begin eth1
...skipping
interface eth1
 ipv6 address fe80::204:75ff:fee6:5393/64
!
interface eth2
 ipv6 address fe80::20d:56ff:fe96:725a/64
!
line con 0
 login
!
End
```

После ключевого слова «begin» можно указать «регулярное выражение». В этом примере вывод начинается со строки «eth3» или «eth4»:

```
# show run | begin eth[3-4]
...skipping
interface eth3
shutdown
!
interface eth4
 shutdown
!
interface svlan0.1
 no shutdown
!
route-map myroute permit 3
!
route-map mymap1 permit 10
!
route-map rmap1 permit 3
!
line con 0
 login
line vty 0 4
 login
!
end
```

3.5.4.2. Модификатор включения Include

Модификатор include включает только те строки вывода, которые содержат строку ввода. В выводе ниже включены все строки, содержащие слово «input»:

```
# show interface eth1 | include input
    input packets 80434552, bytes 2147483647, dropped 0, multicast packets 0
    input errors 0, length 0, overrun 0, CRC 0, frame 0, fifo 1, missed 0
```

После ключевого слова include можно указать постоянное выражение. Этот пример включает в себя все строки с «input» или «output»:

```
#show int eth0 | include (in|out)put
    input packets 597058, bytes 338081476, dropped 0, multicast packets 0
    input errors 0, length 0, overrun 0, CRC 0, frame 0, fifo 0, missed 0
output packets 613147, bytes 126055987, dropped
output errors 0, aborted 0, carrier 0, fifo 0, heartbeat 0, window 0
```

3.5.4.3. Модификатор исключения Exclude

Модификатор exclude исключает все строки вывода, содержащие строку ввода. В следующем примере вывода все строки, содержащие слово «input» исключаются:

```
# show interface eth1 | exclude input
Interface eth1
  Scope: both
  Hardware is Ethernet, address is 0004.75e6.5393
  index 3 metric 1 mtu 1500 <UP,BROADCAST,RUNNING,MULTICAST>
  VRF Binding: Not bound
  Administrative Group(s): None
  DSTE Bandwidth Constraint Mode is MAM
  inet6 fe80::204:75ff:fee6:5393/64
  output packets 4438, bytes 394940, dropped 0
  output errors 0, aborted 0, carrier 0, fifo 0, heartbeat 0, window 0
    collisions 0
```

После ключевого слова exclude можно указать регулярное выражение. В этом примере исключаются строки с «output» или «input»:

```
# show interface eth0 | exclude (in|out)put
Interface eth0
  Scope: both
  Hardware is Ethernet Current HW addr: 001b.2139.6c4a
  Physical:001b.2139.6c4a  Logical:(not set)
  index 2 metric 1 mtu 1500 duplex-full arp ageing timeout 3000
  <UP,BROADCAST,RUNNING,MULTICAST>
  VRF Binding: Not bound
  Bandwidth 100m
  DHCP client is disabled.
  inet 10.1.2.173/24 broadcast 10.1.2.255
  VRRP Master of :  VRRP is not configured on this interface.
  inet6 fe80::21b:21ff:fe39:6c4a/64
    collisions 0
```

3.5.4.4. Модификатор перенаправления Redirect

Модификатор redirect записывает вывод в файл (вывод не отображается):

```
# show cli history | redirect /var/frame.txt
```

Маркер перенаправления вывода («>») делает то же самое:

```
# show cli history >/var/frame.txt
```

3.6. Справочная информация

В процессе работы администратор может получить справочную информацию по необходимым командам и их аргументам. Получить доступ к справке командной строки можно, введя пол-

ную или частичную командную строку и знак вопроса «?» (при этом знак вопроса не будет отображаться). Строка отображает ключевые слова или параметры команды вместе с кратким описанием. При вводе в командной строке ПО KTOS:

```
> show ?
```

ПО KTOS отображает этот список ключевых слов с краткими описаниями для каждого ключевого слова. При этом отображается список всех применимых команд с соответствующими справочными сообщениями.

Если ввести «?» в середине ключевого слова, командная строка отображает справку только для этого ключевого слова.

```
> show de?
debugging  Debugging functions (see also 'undebug')
```

Если неполное ключевое слово соответствует нескольким другим ключевым словам, система отобразит справку по всем соответствующим ключевым словам.

```
> show i?
interface  The layer2 interfaces
ip         Internet protocol (IP)
ipv6       Internet protocol version (IPv6)
```

3.6.1. Горячие клавиши ИКС

ИКС поддерживает ряд «горячих клавиш», облегчающих ввод команд. Указанные клавиши перечислены в таблице 3.

Таблица 3

Клавиша или сочетание клавиш	Описание
Клавиша со стрелкой вверх	Повторно вызывает команды из буфера истории, начиная с самой последней выполненной команды. Более ранние команды вызываются повторным нажатием клавиши соответствующее число раз
Клавиша со стрелкой вниз	Возвращает к последним командам из буфера после использования повторного вызова команд клавишей со стрелкой вверх. Более поздние команды вызываются повторным нажатием клавиши соответствующее число раз
Ctrl+a	Перемещение курсора в начало командной строки
Ctrl+e	Перемещение курсора в конец командной строки
Ctrl+w	Удалить последнюю введенную команду

Клавиша или сочетание клавиш	Описание
Ctrl+z/ End	Возврат в режим управления из режима конфигурирования
Клавиша возврата (Backspace)	Перемещение курсора на одну позицию назад
Esc+b	Перемещение на одно слово назад
Esc+f	Перемещение на одно слово вперед
Ctrl+u	Удалить строку
Alt+d	Удалить текущее слово
Ctrl+k	Удалить от курсора до конца строки
Ctrl+y	Вставить ранее удаленный посредством Ctrl+k, Alt+d, Ctrl+w или Ctrl+ u текст по курсору
Ctrl+t	Поменять местами текущий символ с предыдущим символом
Ctrl+c	Игнорировать введенную строку и отобразить командную строку
Ctrl+l	Очистить экран

3.6.2. Ошибки командной строки

Любая неизвестная команда приводит к отображению в интерфейсе командной строки ошибки «Unrecognized command». В ответ на «?» интерфейс снова отображает команду как последнюю введенную.

```
> show dd?
% Unrecognized command
> show dd
```

После ввода неверной команды и нажатия клавиши <Enter>, интерфейс отображает:

```
(config)#router ospf here
                        ^
% Invalid input detected at '^' marker.
```

Где «^» указывает на первый символ ошибки в команде. Если команда не завершена, интерфейс отображает следующее сообщение:

```
> show
% Incomplete command.
```

Некоторые команды слишком длинные для строки дисплея и могут переноситься на следующую строку среди ключевых слов. Это не вызывает ошибку, и команда выполняется как ожидалось.

3.7. Действия после сбоев в эксплуатации оборудования

В случае недокументированного поведения оборудования в привилегированном режиме управления ввод команды `reload` позволяет выполнить перезагрузку. В случае невозможности получения доступа к консольному и удаленному управлению необходимо осуществить перезагрузку в следующей последовательности: отключить питание от коммутатора, подождать не менее 30 с, подключить питание.

3.8. Использование графического интерфейса

ПО ПО KTOS содержит встроенный web-сервер, на основе которого реализована графическая система управления ПО KTOS. Он выполнен из набора открываемых с помощью браузера HTML-страниц, посредством которых можно осуществлять большинство настроек, доступных в ИКС, а также проводить мониторинг и сбор статистики работы ПО KTOS.

Для управления ПО KTOS через графический интерфейс пользователя (GUI), реализованного через web-интерфейс, необходимо с помощью ИКС разрешить соответствующий доступ и установить его параметры. Команды для настройки доступа к web-интерфейсу системы описаны в подразделе 4.6.

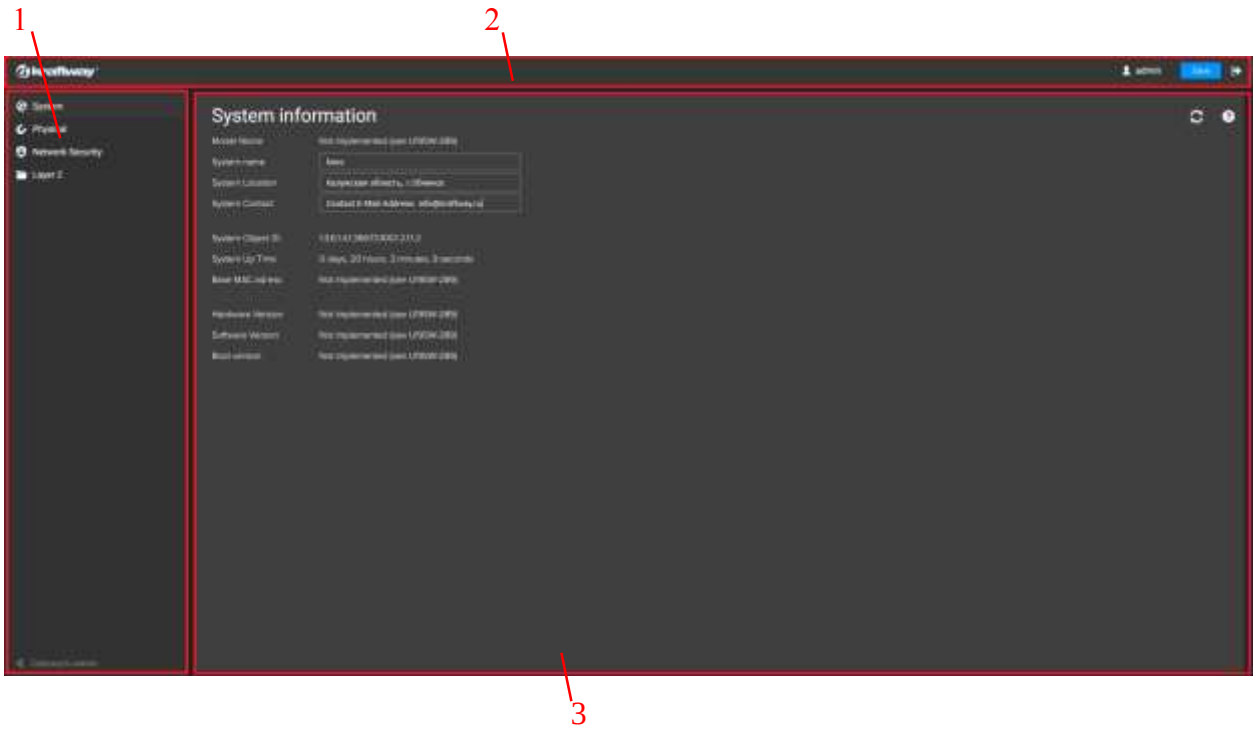
На рис. 2 показана страница авторизации пользователей в графическом интерфейсе, которая открывается, если в адресной строке браузера ввести настроенный IP-адрес порта ПО KTOS, который представлен в подразделе 4.6. Инструкции по управлению учетными записями пользователей приведены в п. 4.5.1.

Страница авторизации пользователей в графическом интерфейсе

Рис. 2

После ввода имени пользователя и пароля открывается стартовая страница web-интерфейса, которая показана на рис. 3.

Стартовая страница web-интерфейса



1 – главное меню; 2 – системное меню; 3 – область отображения информации

Рис. 3

Экранные формы графического интерфейса условно разделены на три области (см. рис. 3):

– главное меню (левая область с раскрывающимися списками всех параметров управления ПО KTOS, доступных для настройки через web-интерфейс);

– системное меню (верхняя область с элементами управления для сохранения конфигурации ПО KTOS в файл на жесткий диск и выхода из web-интерфейса);

– область отображения информации (правая область, в которой отображается подробная информация с элементами управления для пункта, выбранного из списка главного меню).

На рис. 4 показан пример настройки ПО KTOS через графический интерфейс, а именно таблиц IP Interface и ARP, и интерфейс для команды Ping.

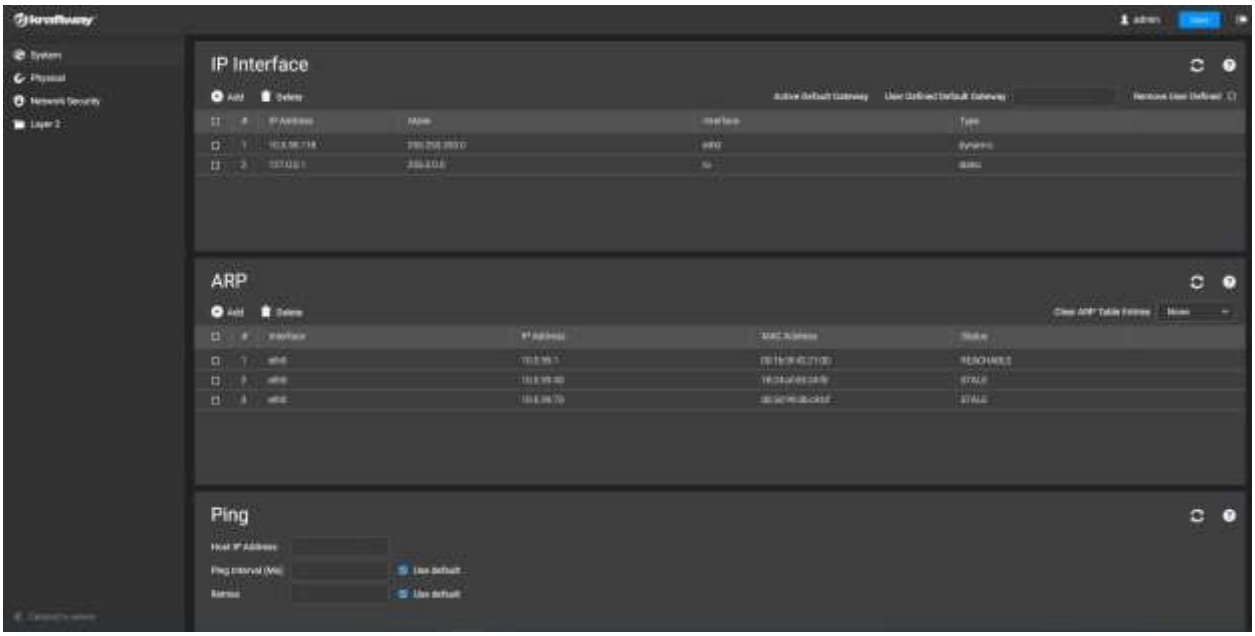


Рис. 4

3.8.1. Главное меню

Главное меню web-интерфейса ПО KTOS (см. рис. 4) содержит разделы:

– System;
– Physical;
– Network Security;
– Layer 2.

Раздел «System» в главном меню web-интерфейса ПО KTOS, изображенный на рис. 5, содержит подразделы «System settings», «Time» и «IP Addressing».

Рис. 5

Подраздел «System settings» содержит общую информацию о коммутаторе.

Подраздел «Time» содержит сведения о настройках параметров системного времени, настройках NTP и параметров для проверки подлинности NTP-сервера.

Подраздел «IP Addressing» содержит таблицы IP Interface и ARP, и интерфейс для команды Ping.

Раздел «Physical» в главном меню web-интерфейса ПО KTOS, изображенный на рис. 6, содержит подраздел «Diagnostics».

Рис. 6

Подраздел «Diagnostics» содержит таблицы Port Mirroring и Ethernet Ports.

Раздел «Network Security» в главном меню web-интерфейса ПО KTOS, изображенный на рис. 7, содержит подраздел «Traffic Control».

Рис. 7

Подраздел «Traffic Control» содержит таблицу Storm Control.

Раздел «Layer 2» в главном меню web-интерфейса ПО KTOS, изображенный на рис. 8, содержит подразделы «Interface», «Address Table», «VLAN» и «Spanning Tree».

Рис. 8

Подраздел «Interface» содержит таблицу Port configuration.

Подраздел «Address Table» содержит таблицы Static Addresses и Dynamic Addresses.

Подраздел «VLAN» содержит таблицы Properties, Membership и Interface Settings.

Подраздел «Spanning Tree» содержит интерфейс к свойствам протокола STP и таблицу Interface Settings.

При необходимости скрыть главное меню нажать в левом нижнем углу на [

]. Для обратного действия нажать [
]].

3.8.2. Системное меню

Системное меню web-интерфейса ПО KTOS изображено на рис. 9.

1 – логотип компании производителя коммутатора; 2 – пользователь; 3 – сохранение конфигурации в файл на жесткий диск; 4 – выход из web-интерфейса ПО KTOS

Рис. 9

3.8.2.1. Сохранение конфигурации коммутатора

Для сохранения конфигурации в файл на жесткий диск в системном меню нажать [Save]. Произойдет сохранение конфигурации коммутатора.

3.8.2.2. Выход из web-интерфейса ПО KTOS

Для выхода из web-интерфейса ПО KTOS в системном меню нажать []. Произойдет выход из web-интерфейса ПО KTOS.

3.8.3. Область отображения информации

Область отображения информации (см. рис. 3) предназначена для отображения сведений разделов и подразделов главного меню web-интерфейса ПО KTOS.

3.8.3.1. Раздел «System»

Раздел «System» (см. рис. 5), содержит подразделы «System settings», «Time» и «IP Addressing».

3.8.3.1.1. Подраздел «System settings»

При выборе в главном меню web-интерфейса ПО KTOS раздела «System», подраздела «System settings», в области отображения информации, изображенной на рис. 10, отобразятся общие сведения о коммутаторе.

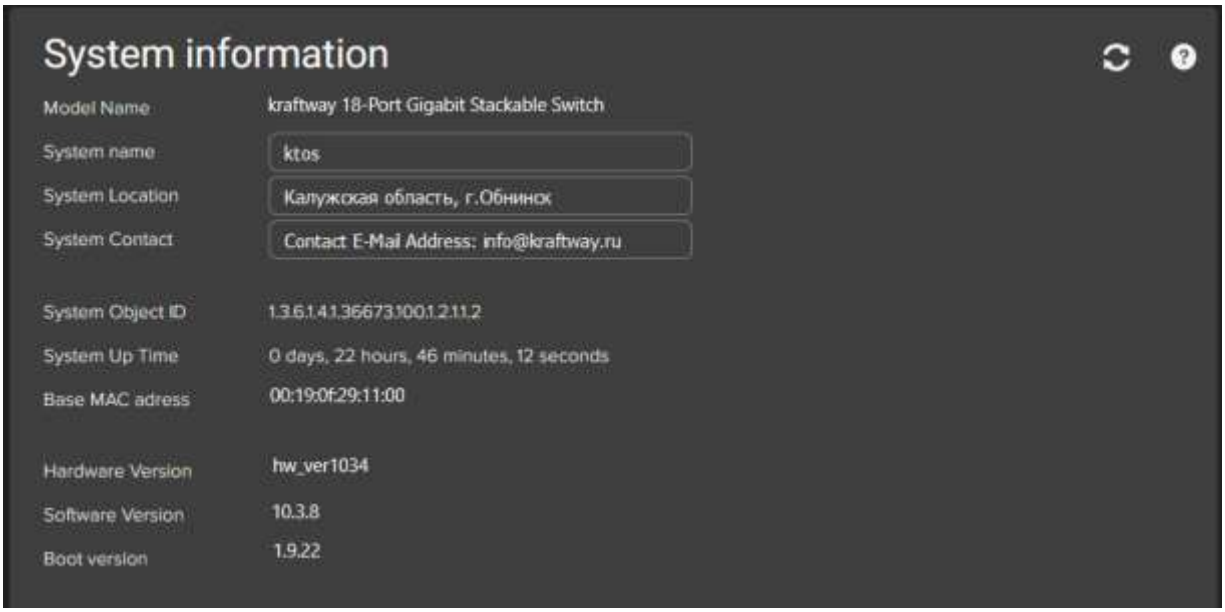


Рис. 10

Секция «System information» содержит:

1) поле «Model Name» – номер модели и название коммутатора;

2) поле «System name» – заданное пользователем имя исполняемого системного ПО, возможное число символов в имени до 160;

3) поле «System Location» – заданное пользователем наименование местоположения, в котором в текущий момент запущен коммутатор, возможное число символов в наименовании до 160;

4) поле «System Contact» – заданные пользователем сведения о контактном лице поставщике коммутатора, возможное число символов в сведениях до 160;

5) поле «System Object ID» – авторизованная идентификация поставщика подсистемы управления сетью, содержащуюся в коммутаторе;

6) поле «System Up Time» – системное время, прошедшее с момента последнего сброса коммутатора. Системное время отображается в следующем формате: Дни, Часы, Минуты, Секунды. Например: 41 день, 2 часа, 22 минуты, 15 секунд;

7) поле «Base MAC address» – MAC-адрес устройства;

8) поле «Hardware Version» – номер версии оборудования коммутатора;

9) поле «Software Version» – номер версии установленного программного обеспечения;

10) поле «Boot Version» – текущая версия загрузки, запущенная на коммутаторе.

Для обновления сведений или получения справки в текущей секции, нажать, соответственно, [] или []. Окно справки для секции «System information» изображено на рис. 11, при необходимости для выхода из окна справки, нажать [Ok] или [].

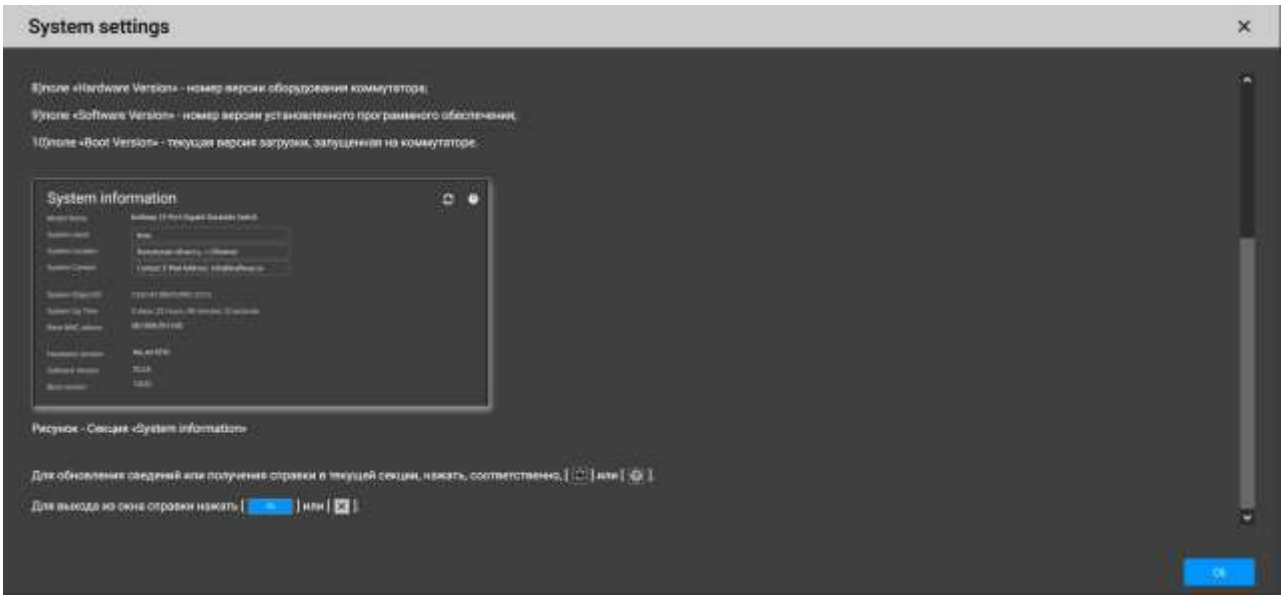


Рис. 11

3.8.3.1.2. Подразделы «Time»

При выборе в главном меню web-интерфейса ПО KTOS раздела «System», подраздела «Time», в области отображения информации, изображенной на рис. 12, отобразятся сведения о настройках параметров системного времени, настройках NTP и параметров для проверки подлинности NTP-сервера.

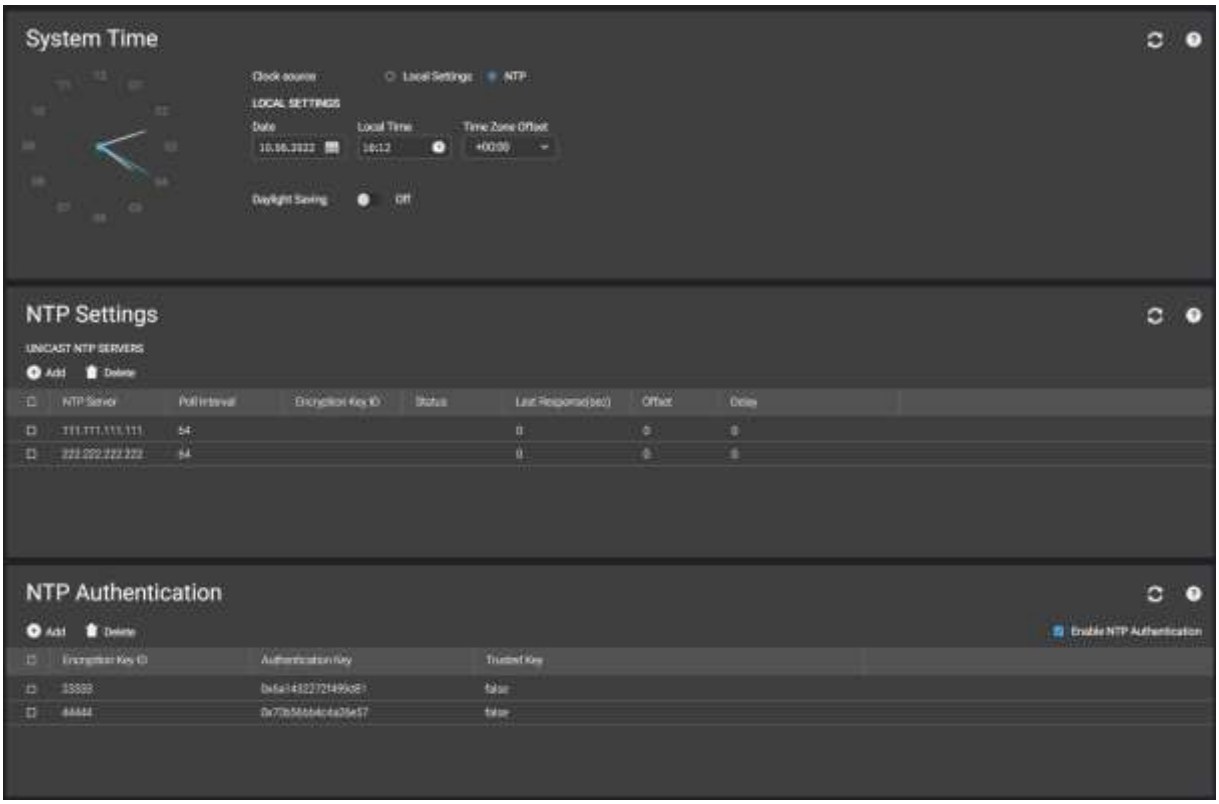


Рис. 12

Секция «System Time» показывает текущее время, которое можно установить вручную, используя флаг «Local Setting» или получить текущее время с NTP-сервера, используя флаг «NTP».

Поле «Date» задает системную дату, в формате ДД/ММ/ГГ, например: 04/May/05 (4 мая 2005 года).

Поле «Local Time» задает системное время, в формате ЧЧ:ММ:СС, например: 21:15:03.

Поле «Time Zone Offset» задает смещение часового пояса, разницу между средним временем по Гринвичу (GMT) и местным временем. Например, смещение часового пояса для города Париж равно GMT +1, в то время как смещение часового пояса для города Нью-Йорк равно GMT -5.

Переключатель «Daylight Saving» включает автоматический переход на летнее время на коммутаторе в зависимости от его местоположения.

Секция «NTP settings» содержит сведения для определения параметров NTP.

Таблица NTP Setting содержит:

1) поле [☐] – позволяет выделить одну запись или несколько записей разом и применить к ним операцию удаления, кнопка [Delete];

2) поле «NTP Server» – определенные пользователем IP-адреса NTP-сервера. Можно определить до восьми NTP-серверов;

3) поле «Poll Interval» – интервал (в секундах), с которым NTP-сервер опрашивается на предмет одноадресной информации. Интервал опроса по умолчанию составляет 1024 с;

4) поле «Encryption Key ID» – указывает, используется ли идентификатор ключа шифрования для аутентификации NTP-сервера и коммутатора. Максимальное значение поля равно 4294967295;

5) поле «Status» – указывает рабочее состояние NTP-сервера, возможные значения:

– Up – NTP-сервер в настоящее время работает нормально;

– Down – NTP-сервер в данный момент недоступен. Например, NTP-сервер в данный момент не подключен или в данный момент не работает;

– In progress – NTP-сервер в данный момент отправляет или получает информацию NTP;

– Unknown – ход отправки информации NTP в данный момент неизвестен. Например, коммутатор в данный момент ищет интерфейс;

6) поле «Last Response(sec)» – время (в секундах) последнего получения ответа от NTP-сервера;

7) поле «Offset» – указывает разницу во времени между локальными часами коммутатора и временем, полученным с NTP-сервера;

8) поле «Delay» – указывает количество времени, необходимое для того, чтобы запрос устройства достиг NTP-сервера;

9) пустое поле (последнее поле текущей таблицы) – дает возможность отредактировать запись в таблице, для этого навести на запись, нажать [], в окне (см. рис. 13) ввести новые данные и нажать [Submit].

Для добавления нового NTP-сервера нажать [Add], в окне (см. рис. 13) в поле «NTP Server» задать IP-адрес сервера, в поле «Encryption Key ID» выбрать нужное значение, нажать [Submit].

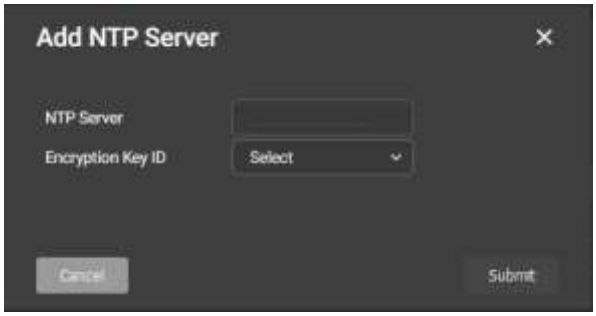


Рис. 13

Секция «NTP Authentication» предоставляет параметры по настройке проверки подлинности NTP-сервера.

Таблица NTP Authentication содержит:

1) поле [] – позволяет выделить одну запись или несколько записей разом и применить к ним операцию удаления, кнопка [Delete];

2) поле «Encryption Key ID» – указывает, используется ли идентификатор ключа шифрования для аутентификации NTP-сервера и коммутатора. Максимальное значение поля равно 4294967295;

3) поле «Authentication Key» – ключ, используемый для аутентификации;

4) поле «Trusted Key» – указывает, использовать ключ шифрования как доверенный (значение – true) или нет (значение – false);

5) пустое поле (последнее поле текущей таблицы) – дает возможность отредактировать запись в таблице, для этого навести на запись, нажать [], в окне (см. рис. 14) ввести новые данные и нажать [Submit].

Для включения проверки подлинности сеансов NTP между коммутатором и NTP-сервером, выбрать [] в «Enable NTP Authentication».

Для добавления нового ключа шифрования, нажать [Add], в окне (см. рис. 14) в поле «Encryption Key ID» задать идентификатор ключа шифрования, в поле «Authentication Key» задать ключ, для обозначения ключа как доверенного в поле «Trusted» активировать [], нажать [Submit].

Рис. 14

Для обновления сведений или получения справки в секциях «System Time», «NTP Settings» или «NTP Authentication», нажать, соответственно, [] или []. При необходимости для выхода из окна справки, нажать [Ok] или [].

3.8.3.1.3. Подраздел «IP Addressing»

При выборе в главном меню web-интерфейса ПО KTOS раздела «System», подраздела «IP Addressing», в области отображения информации, изображенной на рис. 4, отобразятся таблицы IP Interface и ARP, и интерфейс для команды Ping.

Секция «IP Interface» предоставляет поля для назначения IP-адресов.

Для задания шлюза по умолчанию использовать поле «User Defined Default Gateway» см. рис .15.

Рис. 15

Поле «Active Default Gateway» показывает активен ли шлюз заданный по умолчанию, см. рис. 16.

Рис. 16

Для удаления шлюза по умолчанию в поле «Remove User Defined», нажать [].

Таблица IP Interface содержит:

1) поле [] – позволяет выделить одну запись или несколько записей разом и применить к ним операцию удаления, кнопка [Delete];

2) поле [#] – индексирует записи в таблице;

3) поле «IP Address» – текущий настроенный IP-адрес;

4) поле «Mask» – текущую настроенную маску IP-адреса;

5) поле «Interface» – идентификатор интерфейса, возможны значения для интерфейса типа Port или VLAN;

6) поле «Type» – указывает был ли IP-адрес настроен статически или добавлен динамически, возможные значения:

– static – IP-адрес определяется пользователем;

– dynamic – IP-адрес получен от DHCP-сервера;

7) пустое поле (последнее поле текущей таблицы) – дает возможность отредактировать запись в таблице, для этого навести на запись, нажать [], в окне (см. рис. 17) ввести новые данные и нажать [Submit].

Рис. 17

Для добавления нового интерфейса, нажать [Add], в окне (см. рис. 18) в поле «Interface» выбрать «Port» или «VLAN» в выпадающем списке выбрать название интерфейса, в поле «Source IP Address» задать IP-адрес, в поле «Subnet» выбрать подсеть, нажать [Submit].

Рис. 18

Секция «ARP» предоставляет возможность настройки протокола ARP позволяющего преобразовывать IP-адреса в физические адреса и сопоставлять IP-адреса с MAC-адресоми. ARP позволяет коммутатору взаимодействовать с другими хостами только тогда, когда известен IP-адрес его соседей.

Поле «Clear ARP Table Entries» определяет типы очищаемых записей ARP, возможные значения:

– None – поддерживает записи ARP;

– All – очищает все записи ARP;

– Dynamic – удаляет только динамические записи ARP;

– Static – удаляет только статические записи ARP.

Таблица ARP содержит:

1) поле [] – позволяет выделить одну запись или несколько записей разом и применить к ним операцию удаления, кнопка [

];

2) поле [

] – индексирует записи в таблице;

3) поле «Interface» – идентификатор интерфейса, для которого отображаются параметры ARP, возможны значения для интерфейса типа Port или VLAN;

4) поле «IP Address» – указывает IP-адрес станции, связанный с MAC-адресом в таблице ARP;

5) поле «MAC Address» – MAC-адрес станции, связанной с IP-адресом;

6) поле «Status» – тип записи таблицы ARP, возможные значения:

– INCOMPLETE – первый отправленный ARP-запрос;

– REACHABLE – обычный срок действия сбрасывает счетчик использования;

– STALE – все еще пригоден для использования; требуется проверка, сброс счетчика использования; изменение состояния на задержку;

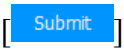
– DELAY – запланируйте ARP-запрос; требуется проверка, сбросьте счетчик использования;

– PROBE – отправка ARP-запроса для сброса счетчика использования;

– FAILED – не получен ответ на ARP-запрос;

– NOARP – нормальное истечение срока действия; никогда не проверялся сброс счетчика использования;

– PERMANENT – никогда не истекает; никогда не проверяется сброс счетчика использования;

7) пустое поле (последнее поле текущей таблицы) – дает возможность отредактировать запись в таблице, для этого навести на запись, нажать [], в окне (см. рис. 19) ввести новые данные и нажать [

].

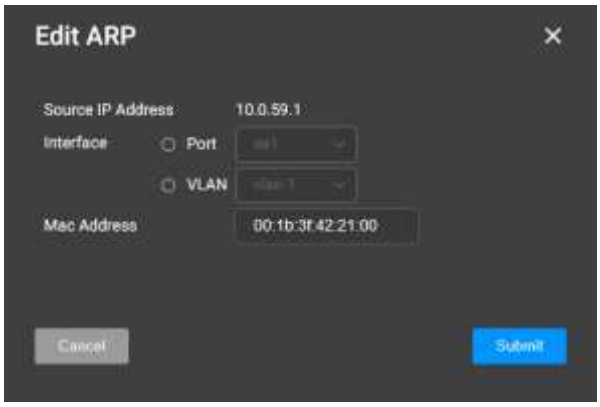


Рис. 19

Для добавления новой записи ARP в таблицу, нажать [Add], в окне (см. рис. 20) в поле «Interface» выбрать «Port» или «VLAN» в выпадающем списке выбрать название интерфейса, в поле «Source IP Address» задать IP-адрес, в поле «Mac Address» задать Mac-адрес, нажать [Submit].

Рис. 20

Секция «Ping» предоставляет возможность доступа к удаленному узлу посредством измерения времени приема-передачи эхо-пакетов, отправленных с коммутатора на целевое устройство.

Поле «Host IP Address» определяет IP-адрес хоста, который нужно проверить.

Поле «Ping Interval (ms)» определяет время в миллисекундах, в течение которого система ожидает проверки связи между пакетами. Можно задать значение по умолчанию выбирая [] в поле «Use default».

Поле «Retries» определяет число повторений отправки эхо-запросов. Можно задать значение по умолчанию выбирая [] в поле «Use default».

Для обновления сведений или получения справки в секциях «IP Interface», «ARP» или «Ping», нажать, соответственно, [] или [?]. При необходимости для выхода из окна справки, нажать [Ok] или [].

3.8.3.2. Раздел «Physical»

Раздел «Physical» (см. рис. 6), содержит подраздел «Diagnostics».

3.8.3.2.1. Подраздел «Diagnostics»

При выборе в главном меню web-интерфейса ПО KTOS раздела «Physical», подраздела «Diagnostics», в области отображения информации, изображенной на рис. 21, отобразятся таблицы Port Mirroring и Ethernet Ports.

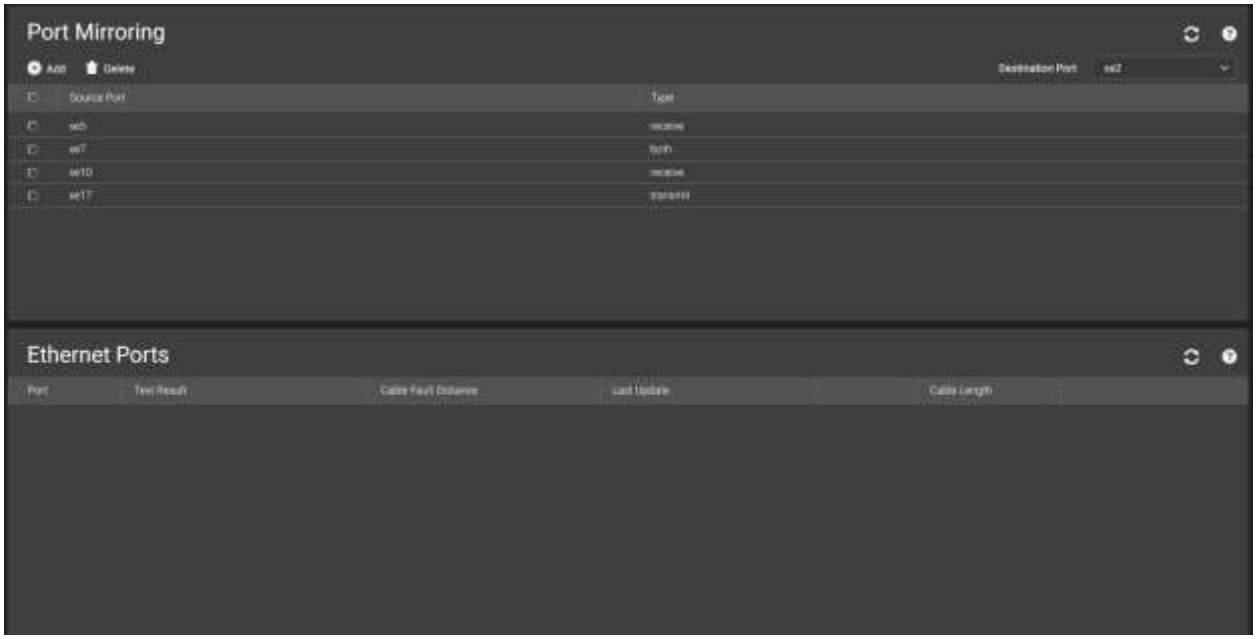


Рис. 21

Секция «Port Mirroring» позволяет отслеживать и отражать сетевой трафик, пересылая копии входящих и исходящих пакетов с одного порта на порт мониторинга.

Сетевой администратор может настроить зеркальное отображение портов, выбрав определенный порт, с которого будут копироваться все пакеты, и порт назначения, на который будут копироваться пакеты.

Поле «Destination Port» (см. рис. 22) определяет номер порта, на который копируется трафик порта источника. Обратите внимание, что этот порт должен быть отсоединен от своей сети VLAN перед настройкой зеркального отображения.

Рис. 22

Таблица Port Mirroring содержит:

1) поле [☐] – позволяет выделить одну запись или несколько записей разом и применить к ним операцию удаления, кнопка [Delete];

2) поле «Source Port» – указывает порт, с которого зеркально отражаются пакеты;

3) поле «Type» – указывает конфигурацию режима порта для зеркального отображения портов, возможные значения:

– receive – определяет зеркальное отображение портов на принимающих портах;

– transmit – определяет зеркальное отображение портов на передающих портах;

– both – определяет зеркальное отображение портов как на приемном, так и на передающем портах. Это значение по умолчанию.

Для добавления новой записи в таблицу Port Mirroring, нажать [Add], в окне (см. рис. 23) в поле «Source Port» выбрать номер порта, в поле «Type» выбрать конфигурацию режима порта, нажать [Submit].

Рис. 23

Секция «Ethernet Ports» содержит поля для выполнения тестов на медных кабелях. Тестирование кабеля предоставляет информацию о том, где в кабеле произошли ошибки, когда в последний раз проводилось тестирование, и тип возникшей ошибки. В тестах используется технология TDR для проверки качества и характеристик медного кабеля, подключенного к порту. Могут быть протестированы кабели длиной до 135 м. Кабели проверяются, когда порты находятся в выключенном состоянии, за исключением теста приблизительной длины кабеля.

Таблица Ethernet Ports содержит:

1) поле «Port» – указывает порт, к которому подключен кабель.

2) поле «Test Result» – результаты тестирования кабеля, возможные значения:

– No Cable – кабель не подключен к порту;

– Open Cable – кабель подключен только с одной стороны;

– Short Cable – в кабеле произошло короткое замыкание;

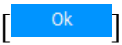
– OK – кабель прошел проверку;

3) поле «Cable Fault Distance» – расстояние от порта, где произошла ошибка кабеля;

4) поле «Last Update» – сведения когда порт был протестирован в последний раз;

5) поле «Cable Length» – приблизительная длина кабеля (с погрешностью: ± 1 м). Этот тест может быть выполнен только тогда, когда порт включен и работает со скоростью 1 Гбит/с.

Для запуска тестирования кабеля необходимо с помощью ИКС выполнить команду **`test cable-diagnostics tdr`**, описание которой приведено в п. 6.4.1 (см. «Справочное руководство по командам интерфейса командной строки KTOS»). Результат тестирования можно посмотреть в таблице Ethernet Ports.

Для обновления сведений или получения справки в секциях «Port Mirroring» или «Ethernet Ports», нажать, соответственно, [] или []. При необходимости для выхода из окна справки, нажать [

] или [].

3.8.3.3. Раздел «Network Security»

Раздел «Network Security» (см. рис. 8), содержит подраздел «Traffic Control».

3.8.3.3.1. Подраздел «Traffic Control»

При выборе в главном меню web-интерфейса ПО KTOS раздела «Network Security», подраздела «Traffic Control», в области отображения информации, изображенной на рис. 24, отобразится таблица Storm Control.

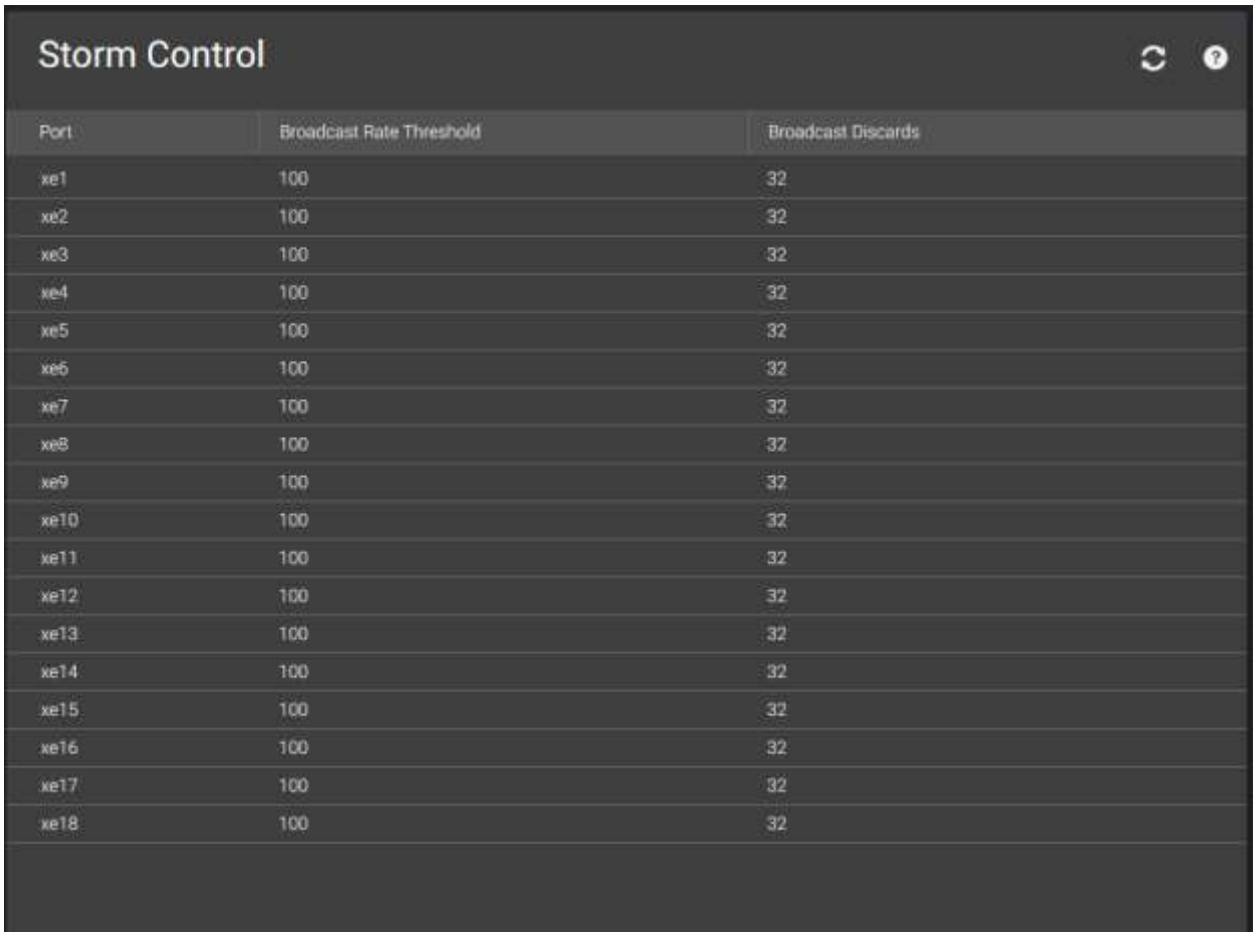


Рис. 24

Секция «Storm Control» позволяет ограничивать количество многоадресных и широковещательных кадров, принимаемых и пересылаемых коммутатором. Когда кадры уровня 2 пересылаются, широковещательные и многоадресные кадры рассылаются на все порты соответствующей сети VLAN. Это занимает полосу пропускания и загружает все узлы на всех портах.

Широковещательный шторм является результатом чрезмерного количества широковещательных сообщений, одновременно передаваемых по сети через один порт. Ответы на переадресованные сообщения накапливаются в сети, нагружая сетевые ресурсы или вызывая тайм-аут сети.

Управление штормом включается для всех гигабитных портов путем определения типа пакета и скорости, с которой передаются пакеты. Система измеряет скорость входящих широковещательных и многоадресных кадров отдельно для каждого порта и отбрасывает кадры, когда скорость превышает заданную пользователем скорость.

Таблица Storm Control содержит:

1) поле «Port» – номер порта, на котором включено управление штормом;

2) поле «Broadcast Rate Threshold» – максимальная скорость (килобит в секунду), с которой пересылаются неизвестные пакеты. Диапазон от 70 до 100000. Значение по умолчанию равно 3500;

3) поле «Broadcast Discards» – указывает, включена ли пересылка широковещательных пакетов на интерфейсе.

Для обновления сведений или получения справки в текущей секции, нажать, соответственно, [] или [?]. Для выхода из окна справки, нажать [Ok] или [×].

3.8.3.4. Раздел «Layer 2»

Раздел «Layer 2» (см. рис. 8), содержит подразделы «Interface», «Address Table», «VLAN» и «Spanning Tree».

3.8.3.4.1. Подраздел «Interface»

При выборе в главном меню web-интерфейса ПО KTOS раздела «Layer 2», подраздела «Interface», в области отображения информации, изображенной на рис. 25, отобразится таблица Port configuration.

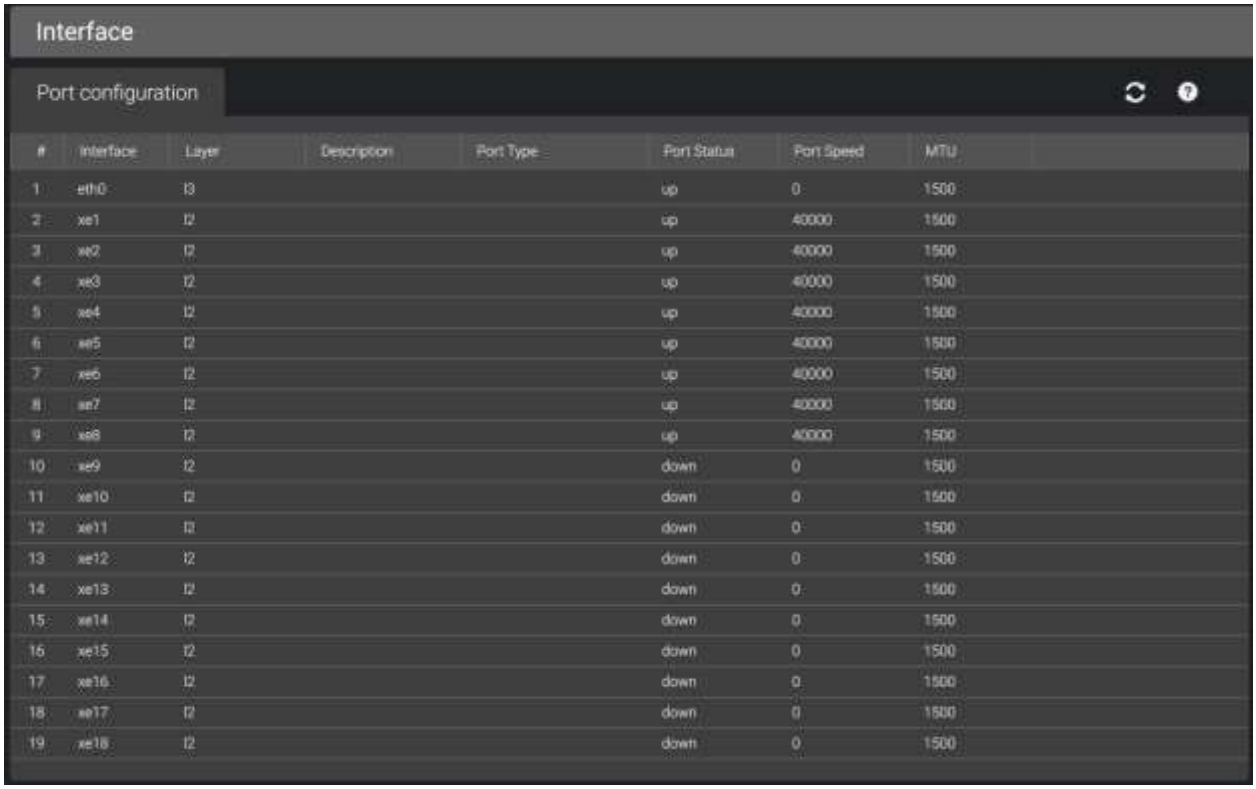


Рис. 25

Секция «Port configuration» содержит таблицу записей, которые определяют параметры портов.

Таблица Port configuration содержит:

1) поле [#] – индексирует записи в таблице;

2) поле «Interface» – идентификатор интерфейса;

3) поле «Layer» – уровень в модели OSI;

4) поле «Description» – описание порта;

5) поле «Port Type» – тип порта, возможные значения:

– Copper – указывает, что порт подключен к медному порту и работает на скорости 1000 Мбит/с;

– Fiber – указывает на то, что к порту подключен оптоволоконный порт;

6) поле «Port Status» – указывает, является ли порт в настоящее время рабочим или нерабочим, возможные значения:

– Up – порт в данный момент работает;

– Down – порт в данный момент не работает;

7) поле «Port Speed» – показывает настроенную скорость для порта. Тип порта определяет доступные параметры настройки скорости. Скорость порта можно настроить, только если автоматическое согласование отключено. Возможные значения поля:

– 10M – порт работает на скорости 10 Мбит/с;

– 100M – порт работает на скорости 100 Мбит/с;

– 1000M – порт работает на скорости 1000 Мбит/с;

– 10000M – порт работает на скорости 10000 Мбит/с.

Для настройки скорости порта необходимо с помощью ИКС выполнить команду **speed**, описание которой приведено в п. 1.1.4 (см. «Справочное руководство по командам интерфейса командной строки KTOS»).

8) поле «MTU» – максимальный объем данных в байтах, который может быть передан за одну итерацию на интерфейсе;

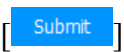
9) пустое поле (последнее поле текущей таблицы) – дает возможность отредактировать запись в таблице, для этого навести на запись, нажать []. Описание новых полей в окне (см. рис. 26):

– поле «Port» – см. описание поля «Interface»;

– поле «Current Port Status» – см. описание поля «Port Status»;

– поле «Current Port Speed» – см. описание поля «Port Speed»;

– поле «Current Layer» – см. описание поля «Layer».

Ввести новые данные и нажать [

].

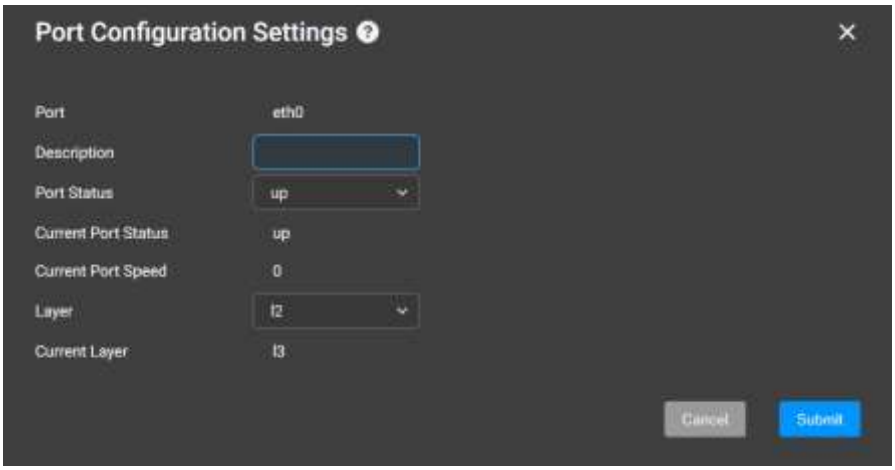


Рис. 26

Для обновления сведений или получения справки в текущей секции, нажать, соответственно, [] или []. При необходимости для выхода из окна справки, нажать [Ok] или [].

3.8.3.4.2. Подраздел «Address Table»

При выборе в главном меню web-интерфейса ПО KTOS раздела «Layer 2», подраздела «Address Table», в области отображения информации, изображенной на рис. 27, отобразятся таблицы Static Addresses и Dynamic Addresses.

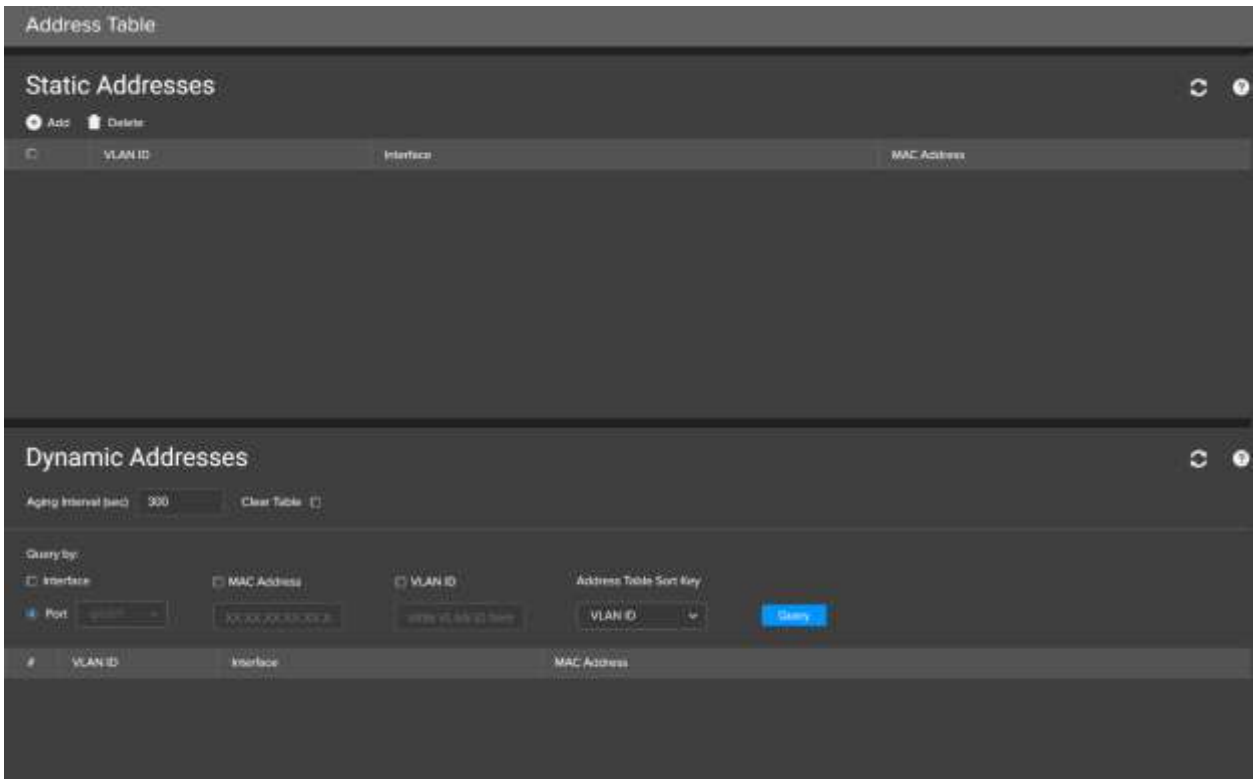


Рис. 27

Таблица Static Addresses содержит:

1) поле [] – позволяет выделить одну запись или несколько записей разом и применить к ним операцию удаления, кнопка [

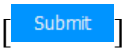
];

2) поле «VLAN ID» – идентификатор сети VLAN;

3) поле «Interface» – идентификатор интерфейса;

4) поле «MAC Address» – MAC-адрес.

Для добавления новой записи в таблицу, нажать [

], в появившемся окне ввести новые данные и нажать [

].

Секция «Dynamic Addresses» содержит:

1) поле «Aging Interval (sec)» – время в секундах, в течение которого MAC-адрес остается в таблице динамических MAC-адресов до истечения времени ожидания, если трафик от источника не обнаружен. Значение по умолчанию – 300 с;

2) флаг «Clear Table» – очищает таблицу динамических адресов, если установлен. Поддерживает записи в динамической таблице адресов в противном случае, значение по умолчанию;

3) флаг «Interface» – активизирует поле «Port»;

4) поле «Port» – номер порта, по которому происходит поиск и заполнение таблицы;

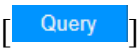
5) флаг «MAC Address» – активизирует поле «MAC Address»;

6) поле «MAC Address» – MAC-адрес, по которому происходит поиск и заполнение таблицы;

7) флаг «VLAN ID» – активизирует поле «VLAN ID»;

8) поле «VLAN ID» – идентификатор VLAN, по которому происходит поиск и заполнение таблицы;

9) поле «Address Table Sort Key» – определяет способ сортировки записей в таблице. Таблицу можно сортировать по MAC-адресу, идентификатору VLAN или идентификатору интерфейса.

Для выполнения запроса нажать [

].

Результат запроса отобразиться в таблице, содержащей:

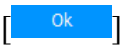
1) поле [

] – индексирует записи в таблице;

2) поле «VLAN ID» – идентификатор сети VLAN;

3) поле «Interface» – идентификатор интерфейса;

4) поле «MAC Address» – MAC-адрес.

Для обновления сведений или получения справки в текущей секции, нажать, соответственно, [] или []. При необходимости для выхода из окна справки, нажать [

] или [].

3.8.3.4.3. Подраздел «VLAN»

При выборе в главном меню web-интерфейса ПО KTOS раздела «Layer 2», подраздела «VLAN», в области отображения информации, изображенной на рис. 28, отобразятся таблицы Properties, Membership и Interface Settings.

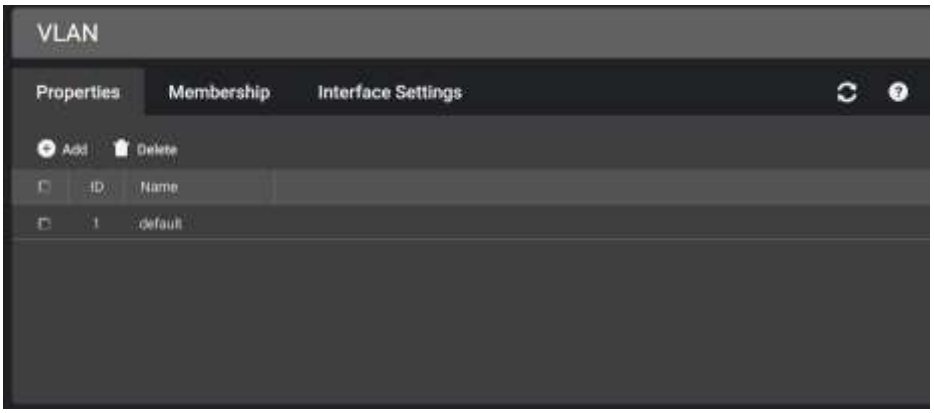


Рис. 28

Секция «Properties» содержит таблицу:

1) поле [☐] – позволяет выделить одну запись или несколько записей разом и применить к ним операцию удаления, кнопка [Delete];

2) поле «ID» – идентификатор сети VLAN;

3) поле «Name» – заданное пользователем имя VLAN;

4) пустое поле (последнее поле текущей таблицы) – дает возможность отредактировать запись в таблице, для этого навести на запись, нажать [✎]. Описание полей окна (см. рис. 29):

– поле «VLAN ID» – идентификатор сети VLAN;

– поле «VLAN Name» – заданное пользователем имя сети VLAN.

Рис. 29

Ввести новые данные и нажать [Submit].

Для добавления новой записи в таблицу, нажать [Add], в окне (см. рис. 30) ввести новые данные и нажать [Submit].

Рис. 30

Секция «Membership» (см. рис. 31) содержит таблицу, в которой параметры сети VLAN сопоставляются с идентификаторами интерфейса.

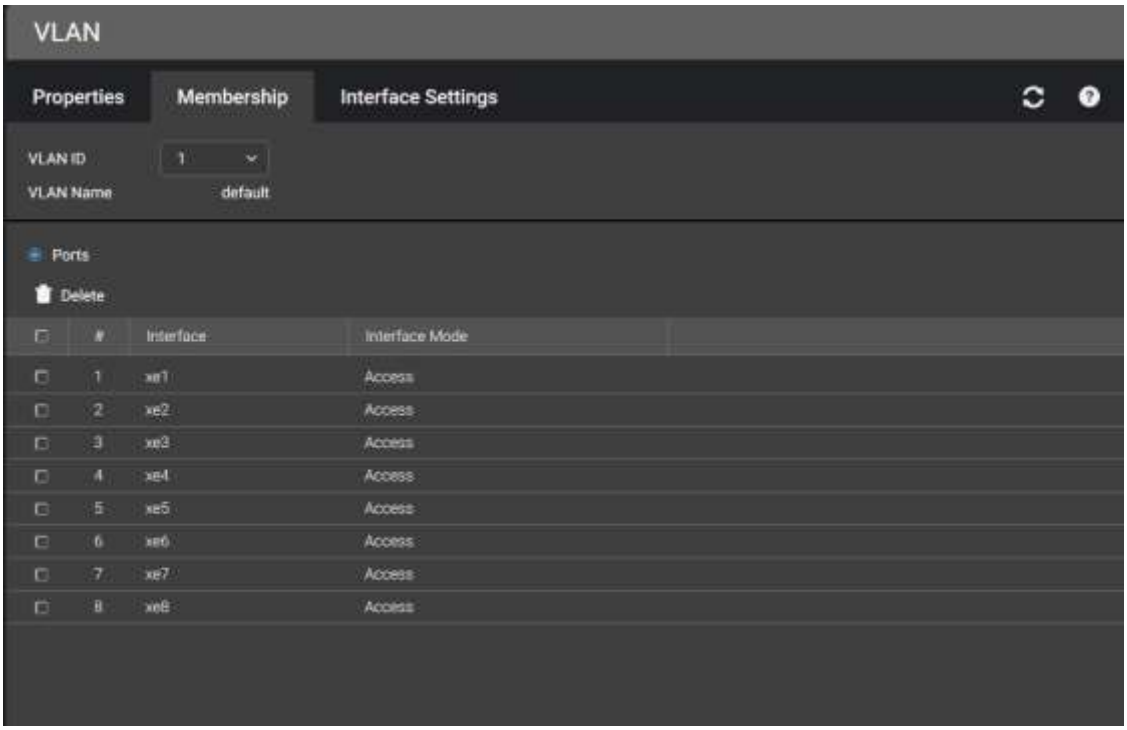


Рис. 31

Поле «VLAN ID» содержит определяемый пользователем идентификатор сети VLAN.

Поле «VLAN Name» содержит имя сети VLAN.

Поле «Ports» указывает принадлежность порта на коммутаторе.

Таблица Membership содержит:

1) поле [☐] – позволяет выделить одну запись или несколько записей разом и применить к ним операцию удаления, кнопка [Delete];

2) поле [#] – индексирует записи в таблице;

3) поле «Interface» – идентификатор интерфейса;

4) поле «Interface Mode» – режим порта, возможные значения:

– Access – порт принадлежит одной не тегированной сети VLAN. Когда порт находится в режиме Access, типы пакетов, которые принимаются портом, не могут быть назначены. Входная фильтрация не может быть включена или отключена для порта Access;

– Hybrid – порт принадлежащий к сегменту локальной сети, к которому подключены устройства, поддерживающие и не поддерживающие сеть VLAN. Следовательно, гибридный порт может передавать как кадры с тегами VLAN, так и другие кадры (без тегов или с тегами приоритета);

– Trunk – порт принадлежит к сети VLAN, в которой все порты помечены, за исключением одного порта, который может быть не помечен;

5) пустое поле (последнее поле текущей таблицы) – дает возможность отредактировать запись в таблице, для этого навести на запись, нажать [✎]. Окно (см. рис. 32) помимо известных полей содержит новое поле «Interface Status» о состоянии порта в сети VLAN, возможные значения:

– Include – включить порт в сеть VLAN;

– Exclude – исключить порт из сети VLAN;

– Forbidden – запрещает членство порта в сети VLAN;

– Untagged – указывает, что интерфейс является не тегированным членом сети VLAN. Пакеты, пересылаемые интерфейсом, не помечены;

– Tagged – указывает, что интерфейс является помеченным членом сети VLAN. Все кадры, пересылаемые интерфейсом в эту сеть VLAN, помечаются. Кадры содержат информацию о сети VLAN.

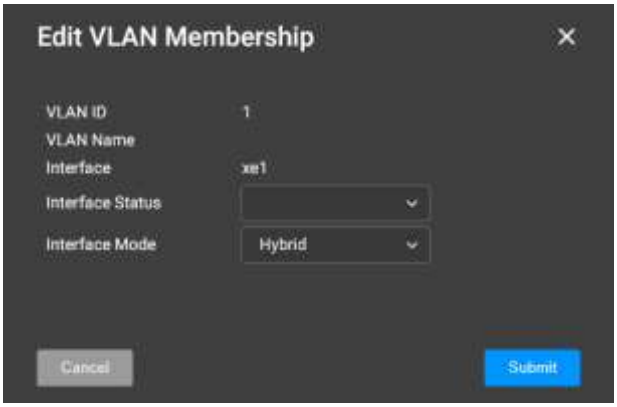


Рис. 32

Ввести новые данные и нажать [Submit].

Секция «Interface Settings» (см. рис. 33) содержит поля для управления портами являющиеся частью сети VLAN. Идентификатор сети VLAN по умолчанию для порта Port Default VLAN ID (PVID) настраивается в текущей секции. Все непомеченные пакеты, поступающие на коммутатор, помечаются PVID.

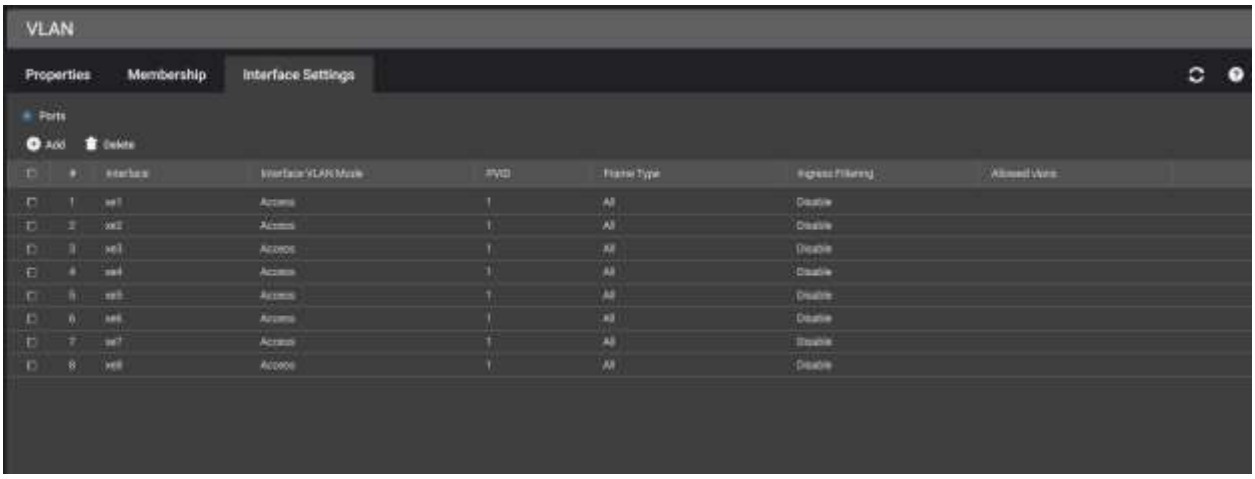


Рис. 33

Поле «Ports» указывает принадлежность к порту на коммутаторе.

Таблица содержит:

1) поле [☐] – позволяет выделить одну запись или несколько записей разом и применить к ним операцию удаления, кнопка [Delete];

2) поле [#] – индексирует записи в таблице;

3) поле «Interface» – идентификатор интерфейса;

4) поле «Interface VLAN Mode» – режим порта, возможные значения:

– General – порт принадлежит сети VLAN, и каждая сеть VLAN определяется пользователем как помеченная или не помеченная (см. IEEE802.1q);

– Access – порт принадлежит одной не тегированной сети VLAN. Когда порт находится в режиме Access, типы пакетов, которые принимаются портом, не могут быть назначены. Входная фильтрация не может быть включена или отключена для порта Access;

– Trunk – порт принадлежит к сети VLAN, в которой все порты помечены, за исключением одного порта, который может быть не помечен;

5) поле «PVID» – присваивает идентификатор VLAN ID непомеченным пакетам, возможные значения от 1 до 4093;

6) поле «Frame Type» – тип пакета, принимаемого портом. Возможные значения:

– Admit Tag Only – порт принимает только тегированные пакеты;

– Admit All – через порт принимаются как тегированные, так и не тегированные пакеты;

7) поле «Ingress Filtering» – включена ли фильтрация входящего трафика для порта, возможные значения:

– Enable – включить фильтрацию входящего трафика на коммутаторе. Входная фильтрация отбрасывает пакеты, которые определены для сетей VLAN, членом которых не является конкретный порт;

– Disable – отключить фильтрацию входящего трафика на коммутаторе;

8) поле «Allowed vlans» – разрешенные сети VLAN;

9) пустое поле (последнее поле текущей таблицы) – дает возможность отредактировать запись в таблице, для этого навести на запись, нажать [], в окне (см. рис. 34), ввести новые данные и нажать [Submit].

Рис. 34

Для обновления сведений или получения справки в текущей секции, нажать, соответственно, [] или []. При необходимости для выхода из окна справки, нажать [Ok] или [].

3.8.3.4.4. Подраздел «Spanning Tree»

При выборе в главном меню web-интерфейса ПО KTOS раздела «Layer 2», подраздела «Spanning Tree», в области отображения информации, изображенной на рис. 35, отобразится интерфейс к свойствам протокола STP и таблица Interface Settings.

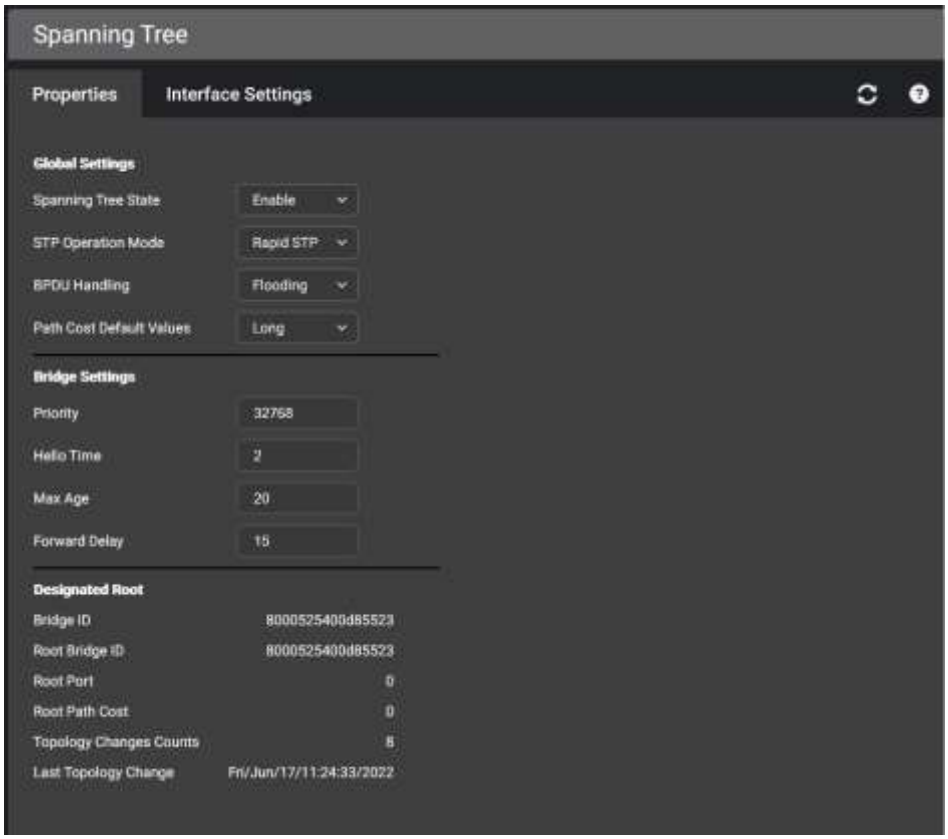


Рис. 35

Секция «Global Settings» содержит:

1) поле «Spanning Tree State» – позволяет, включить или отключить протокол STP на коммутаторе, возможные значения поля:

– Enable – включить STP;

– Disable – отключить STP;

2) поле «STP Operation Mode» – задает режим протокола STP, включенного на коммутаторе, возможные значения поля:

– Classic STP – классический протокол STP (значение по умолчанию), предполагает один экземпляр протокола остовного дерева для всей сети с мостовым соединением независимо от количества сетей VLAN;

– Rapid STP – версия протокола STP с ускоренной реконфигурацией остовного дерева;

– Multiple STP – протокол множественного остовного дерева обеспечива-ющий сопоставление нескольких сетей VLAN в пределах одного экземпляра протокола STP;

3) поле «BPDU Handling» – определяет способ управления пакетами Bridge Protocol Data Unit (BPDU), когда протокол STP отключен на порту или коммутаторе. BPDU используются для передачи информации остовного дерева. Возможные значения поля:

– Filtering – фильтрует пакеты BPDU, когда остовное дерево отключено на интерфейсе (значение по умолчанию);

– Flooding – рассылает пакеты BPDU, когда остовное дерево отключено на интерфейсе;

4) поле «Path Cost Default Values» – указывает метод, используемый для назначения стоимости пути по умолчанию для портов STP. Возможные значения поля:

– Short – указывает диапазон от 1 до 65535 (значение по умолчанию);

– Long – указывает диапазон от 1 до 200000000.

Стоимость пути по умолчанию, назначенная интерфейсу, зависит от выбранного метода, который определяется параметрами Hello Time, Max Age или Forward Delay.

Секция «Bridge Settings» содержит:

1) поле «Priority» – значение приоритета коммутатора. Если коммутаторы использует протокол STP, то каждому назначается приоритет. После обмена сообщениями BPDU коммутатор с наименьшим значением приоритета становится корневым. Диапазон от 0 до 65535. Значение приоритета порта указывается с шагом 4096. Значение по умолчанию – 32768;

2) поле «Hello Time» – интервал времени в секундах, через который корневой коммутатор отправляет конфигурационные сообщения BPDU. Диапазон от 1 до 10 с. Значение по умолчанию – 2 с;

3) поле «Max Age» – максимальное время возраста коммутатора в секундах. Максимальное время возраста – это интервал времени, которое коммутатор ожидает перед отправкой сообщений конфигурации BPDU. Диапазон от 6 до 40 с. Значение по умолчанию – 20 с;

4) поле «Forward Delay» – время задержки пересылки для коммутатора в секундах. Время задержки пересылки – это интервал времени, в течение которого коммутатор остается в состоянии прослушивания и обучения перед пересылкой пакетов. Диапазон от 4 до 30 с. Значение по умолчанию – 10 с.

Секция «Designated Root» содержит:

1) поле «Bridge ID» – приоритет и MAC-адрес коммутатора;

2) поле «Root Bridge ID» – приоритет и MAC-адрес корневого коммутатора;

3) поле «Boot Port» – номер порта, обеспечивающий путь от этого коммутатора к корневому коммутатору с наименьшей стоимостью. Это поле важно, если коммутатор не является корневым. По умолчанию – ноль;

4) поле «Root Path Cost» – стоимость пути от текущего коммутатора до корневого;

5) поле «Topology Changes Counts» – общее количество произошедших изменений состояния STP;

6) поле «Last Topology Change» – количество времени, прошедшее с момента инициализации, сброса коммутатора, или последнего топографического изменения. Время отображается в формате день /час/минута/секунда, например: 2D/5H/10M/4S.

Секция «Interface Settings» (см. рис. 36) позволяет отобразить и отредактировать параметры протокола STP.

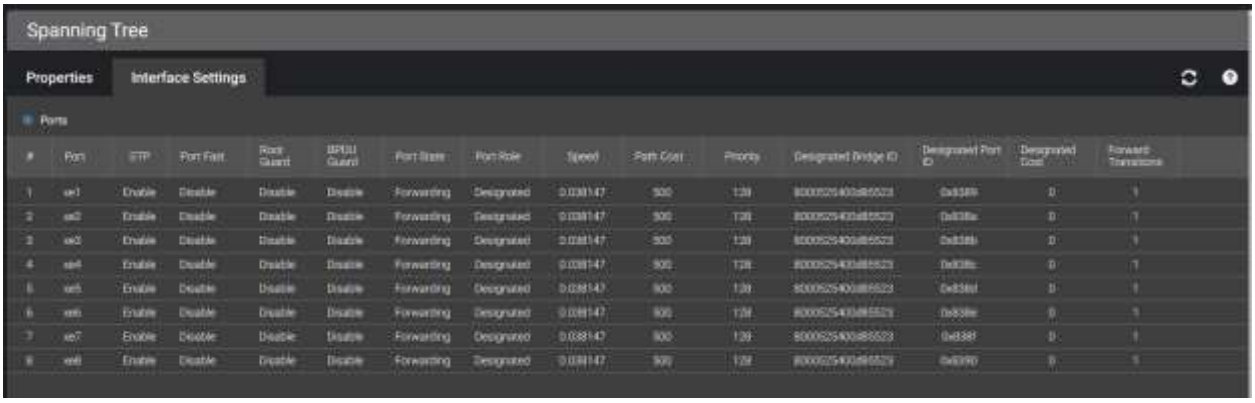


Рис. 36

Поле «Ports» обозначает интерфейс для которого отображается информация.

Таблица содержит:

1) поле [#] – индексирует записи в таблице;

2) поле «Port» – идентификатор интерфейса;

3) поле «STP» – включен ли протокол STP на порту, возможные значения поля:

- Enabled – включен;
- Disabled – отключен;

4) поле «Port Fast» – указывает, включена ли на порту функция Fast Link. Если для порта включен режим Fast Link, состояние порта автоматически переводится в состояние Forwarding, когда порт работает. Fast Link оптимизирует конвергенцию протокола STP. Конвергенция STP может занять 30-60 с в больших сетях;

5) поле «Root Guard» – предотвращает назначение устройств за пределами ядра сети в корень остовного дерева, возможные значения поля:

- Enabled – включен;
- Disabled – отключен;

6) поле «BPDU Guard» – функция поля состоит в том, чтобы не позволить порту получать BPDU. Технически при получении такого фрейма интерфейс сразу же переходит в состояние error-disabled, то есть отключается. Он будет находиться в таком состоянии до тех пор, пока сетевой администратор не устранит причину проблемы, например, не отключит коммутатор, ошибочно под-

ключенный к Port Fast. Таким образом, использование функции Port Fast делает его быстрее, а использование BPDU Guard предотвращает получение сообщений BPDU и связанное с этим образование петель трафика, возможные значения поля:

– Enabled – включен;

– Disabled – отключен;

7) поле «Port State» – текущее состояние STP порта. Если этот параметр включен, состояние порта определяет, какие действия по переадресации выполняются для трафика. Возможные состояния порта:

– Disabled – протокол STP в данный момент отключен на порту, порт перенаправляет трафик, изучая MAC-адреса;

– Blocking – порт в настоящее время заблокирован и не может пересылать трафик или узнавать MAC-адреса. Блокировка отображается, когда включен классический STP;

8) поле «Port Role» – роль порта, назначенную алгоритмом STP для предоставления путей STP. Возможные значения поля:

– Root – обеспечивает путь с наименьшей стоимостью для пересылки пакетов на корневой коммутатор;

– Designated – порт, к которому назначенный коммутатор подключен к локальной сети;

– Alternate – альтернативный путь к корневому коммутатору от корневого интерфейса;

– Backup – резервный путь к назначенному пути порта к листьям остовного дерева. Резервные порты появляются только тогда, когда два порта соединены в петлю каналом «точка-точка» или когда локальная сеть имеет два или более подключений к общему сегменту;

– Disable – порт не участвует в остовном дереве;

9) поле «Speed» – скорость, с которой работает порт;

10) поле «Path Cost» – вклад порта в стоимость корневого пути. Стоимость пути корректируется до большего или меньшего значения и используется для перенаправления трафика при перемаршрутизации;

11) поле «Priority» – приоритета порта. Он влияет на выбор порта, когда коммутатор имеет два порта, соединенных в петлю. Значение приоритета находится в диапазоне от 0 до 240. Значение приоритета определяется с шагом 16;

12) поле «Designated Bridge ID» – приоритет и MAC-адрес назначенного коммутатора;

13) поле «Designated Port ID» – приоритет выбранного порта и интерфейс;

14) поле «Designated Cost» – стоимость порта, участвующего в топологии STP. Если STP обнаружит петли, то порты с более низкой стоимостью с меньшей вероятностью будут заблокированы;

15) поле «Forward Transitions» – число раз которое порт переходил из состояния Forwarding в состояние Blocking;

16) пустое поле (последнее поле текущей таблицы) – дает возможность отредактировать запись в таблице, для этого навести на запись, нажать [], в окне (см. рис. 37), ввести новые данные и нажать [Submit].

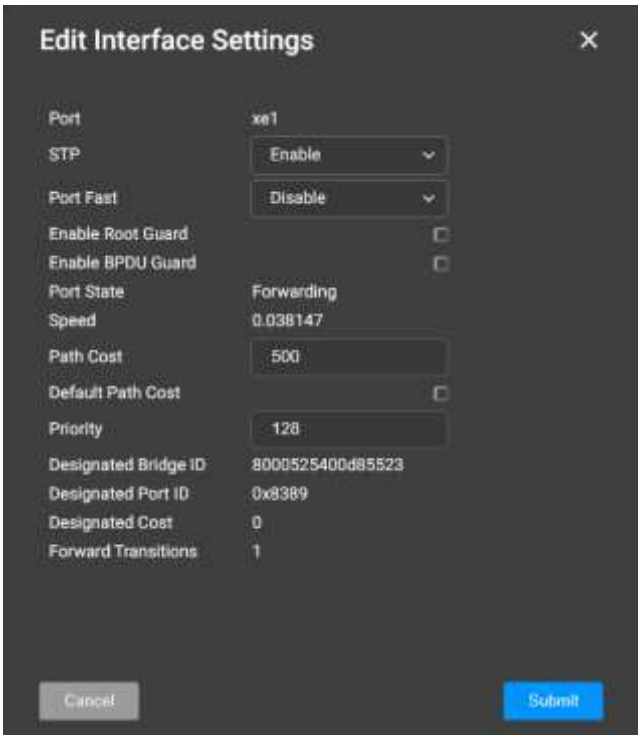


Рис. 37

Для обновления сведений или получения справки в текущей секции, нажать, соответственно, [] или []. При необходимости для выхода из окна справки, нажать [Ok] или [].

4. БАЗОВЫЕ КОМАНДЫ ДЛЯ УПРАВЛЕНИЯ КОММУТАТОРОМ

Примечание. Управление ПО KTOS детально описано с помощью ИКС, общие принципы настройки работы ПО KTOS, применимы и в web-интерфейсе.

4.1. Команды для выбора режима интерфейса командной строки

ИКС содержит два основных режима – «режим управления» и «режим конфигурирования».

Режим управления делится на «пользовательский режим управления» и «привилегированный режим управления».

В режим конфигурирования входит несколько подрежимов, каждый из которых имеет собственный характерный набор команд. Для перехода из одного режима в другой используются специальные команды.

В каждом режиме в строке ввода команд используется свое «приглашение», по которому всегда можно опознать текущий режим. В таблице 4 показано состояние «приглашения» строки ввода команд при входе в каждый режим ИКС.

Таблица 4

Режим ИКС	«Приглашение»
Режим управления	`KRAFTWAY>`
Режим общего конфигурирования (Global Configuration)	`KRAFTWAY(config)#`
Режим конфигурирования интерфейсов (Interface Configuration)	`KRAFTWAY(config-if)#`
Режим конфигурирования линии (Line Configuration)	`KRAFTWAY(config-line)#`
Режим конфигурирования VLAN (VLAN DataBASE)	`KRAFTWAY(config-vlan)#`
Режим конфигурирования протоколов динамической маршрутизации (Router Configuration)	`KRAFTWAY(config-router)#`

4.2. Базовые команды, доступные во всех режимах ИКС

Команды, которые можно использовать во всех режимах ИКС:

– **`do`** – выполнение команды режима управления из любого режима конфигурирования;

– **`help`** – вывод справочной информации по используемым командам.

4.3. Команды, доступные в режиме управления

После ввода имени пользователя и пароля ИКС запускается в пользовательском режиме управления. В данном режиме доступны следующие команды:

– **`exit`** – завершение активной терминальной сессии режима управления.

– **show** – просмотр параметров и состояние ПО KTOS;

– **enable** – переход в привилегированный режим управления.

4.4. Команды для управления режимом общего конфигурирования

Команды, использующиеся для входа в режим общего конфигурирования и выхода из него:

– **configure terminal** – переход в режим конфигурирования из привилегированного режима управления;

– **exit** – выход из любого режима конфигурирования на следующий ближайший уровень в иерархии режимов ИКС;

– **end** – выход из любого режима конфигурирования в режим управления.

4.5. Создание новых пользователей, настройка подключений к системе

4.5.1. Создание новых учетных записей пользователей системы

По умолчанию в системе присутствует одна учетная запись *admin* с паролем *admin*, которой соответствует уровень доступа «СуперАдминистратор».

Первый сеанс управления объектом управления (далее – ОО) начинается со входа под именем пользователя *admin* и паролем *admin,* после этого разрешается в режиме конфигурирования создать другие учетные записи, задав имя пользователя, пароль и уровень привилегий для каждой учетной записи.

Имя пользователя и пароль вводятся при входе в систему во время сеансов администрирования устройства. После успешной аутентификации запускается сеанс управления с минимальным уровнем доступа, для повышения уровня доступа необходимо ввести команду *enable*. Для создания нового пользователя или настройки его параметров (имя пользователя, пароль, уровень привилегий) используется команда режима конфигурирования **username**.

Синтаксис команды:

username *name* **role** *rolename* {**password** *password* | **encrypted** *enc_password*}

Параметры команды:

– *name* – имя создаваемого пользователя;

– *password* – пароль, длина пароля от 8 до 32 символов;

– *enc_password* – пароль, зашифрованный с использованием алгоритма MD5, длина пароля от 26 до 106 символов;

– *rolename* – роль пользователя в системе.

Примечания:

1. Роль «network-admin» соответствует уровню доступа «СуперАдминистратор», который является наивысшим и позволяет управлять устройством и его настройками (перезагрузка устройства или отдельных процессов, обновление прошивки, настройка подсистем и интерфейсов и т.п.).

2. Роль «network-operator» соответствует уровню доступа «Администратор». Имеет те же права, что и на уровне доступа «СуперАдминистратор», кроме сохранения конфигурации.

3. Роль «network-user» соответствует уровню доступа «Оператор» и позволяет просматривать базовую информацию об устройстве.

Пример создания пользователя «user1» с паролем «123» и уровнем доступа «network-user»:

```
KRAFTWAY#configure terminal
KRAFTWAY(config)#username user1 role network-user password 12345678
KRAFTWAY(config)#exit
KRAFTWAY#
```

4.5.2. Настройка локального и удаленного подключения к системе

Управление коммутатором производится при помощи ПО управления коммутатором.

Для управления системой предусмотрены следующие виды подключений:

– подключение к удаленной консоли по протоколу Telnet;

– подключение к удаленной защищенной консоли по протоколу SSH;

– подключение к графическому интерфейсу по протоколу HTTP;

– подключение к графическому интерфейсу по защищенному протоколу HTTPS с использованием протокола SSL.

Для настройки параметров подключения могут быть использованы различные команды.

4.5.2.1. Команда **`line`**

Используется для выбора терминала для его настройки и входа в режим его конфигурирования.

Синтаксис команды:

`line` {*`console`* | *`vty`*}

Параметры команды:

– *`console`* – локальная консоль;

– *`vty`* – удаленная консоль (Telnet, SSH).

Режим ИКС – режим общего конфигурирования.

4.5.2.2. Команда **exec-timeout**

Задает время, в течение которого система ожидает ввода символов. Если в течение данного интервала администратор ничего не вводит, то консоль отключается. Использование префикса «**no**» устанавливает значение по умолчанию.

Синтаксис команды:

exec-timeout *minutes* [*seconds*]

или

no exec-timeout

Параметры команды:

– *minutes* – количество минут (диапазон от 0 до 35791);

– *seconds* – количество секунд (диапазон от 0 до 2147483).

Состояние по умолчанию – 10 мин.

Режим ИКС – режим конфигурирования линии.

Примечание. Чтобы снять какие-либо ограничения на время ожидания ввода символов, необходимо установить значения параметров «00».

Пример настройки терминала удаленной консоли с установкой времени ожидания ввода символов 15 мин:

```
KRAFTWAY#configure
KRAFTWAY(config)#line console 0
KRAFTWAY(config-line)#exec-timeout 15
```

4.5.2.3. Команда **feature telnet**

Включает поддержку сервера Telnet и разрешает удаленное конфигурирование устройства по протоколу Telnet. Использование префикса «**no**» отключает удаленный доступ к устройству по протоколу Telnet.

Синтаксис команды:

feature telnet

или

no feature telnet

Состояние по умолчанию – удаленный доступ к устройству по протоколу Telnet выключен.

Режим ИКС – режим общего конфигурирования.

4.5.2.4. Команда **feature ssh**

Включает поддержку сервера SSH и разрешает удаленное конфигурирование устройства по защищенному протоколу SSH. Использование префикса «**no**» отключает удаленный доступ к устройству по протоколу SSH.

Синтаксис команды:

feature ssh

или

no feature ssh

Состояние по умолчанию – удаленный доступ к устройству по протоколу SSH выключен.

Режим ИКС – режим общего конфигурирования.

Примечание. Для генерации частного и публичного ключей сервера SSH необходимо использовать команды **ssh key dsa** и **ssh key rsa**. Для выполнения данных команд необходимо отключить сервис SSH с помощью команды **no feature ssh** .

4.5.2.5. Команда **ssh server port**

Используется для назначения TCP-порта, который используется сервером SSH. Использование префикса «**no**» возвращает номер порта по умолчанию.

Синтаксис команды:

ssh server port *port-number*

или

no ssh server port

Параметр команды – *port-number* – номер TCP-порта для SSH-сервера (диапазон от 1024 до 65535).

Состояние по умолчанию – номер TCP-порта по умолчанию – 22.

Режим ИКС – режим общего конфигурирования.

4.5.2.6. Команда **show ssh server**

Используется для отображения текущей конфигурации SSH-сервера.

Синтаксис команды:

show ssh server

Режим ИКС – режим управления.

4.6. Настройка доступа к GUI

4.6.1. Команды для доступа к управлению через Web-GUI

4.6.1.1. Команда **ip http server**

Включает управление ПО KTOS и просмотр его состояния через GUI. Использование префикса «**no**» отключает данную функцию.

Синтаксис команды:

ip http server

или

no ip http server

Состояние по умолчанию – Web-интерфейс выключен.

Режим ИКС – режим общего конфигурирования.

4.6.1.2. Команда **ip http port**

Используется для назначения TCP-порта для подключения через GUI. Использование префикса «**no**» возвращает номер порта по умолчанию.

Синтаксис команды:

ip http port *port-number*

или

no ip http port

Параметр команды – *port-number* – номер TCP-порта для HTTP-сервера (диапазон от 1 до 65535).

Состояние по умолчанию – номер TCP-порта по умолчанию – 80.

Режим ИКС – режим общей настройки.

4.6.1.3. Команда **ip http timeout-policy**

Устанавливает интервал ожидания при использовании web-интерфейса, после которого происходит автоматическое завершение сессии пользователя. Использование префикса «**no**» устанавливает значение интервала ожидания по умолчанию.

Синтаксис команды:

ip http timeout-policy *seconds*

или

no ip http timeout-policy

Параметр команды – *seconds* – значение интервала ожидания в секундах (диапазон от 0 до 86400).

Состояние по умолчанию – 600 с.

Режим ИКС – режим общей настройки.

Примечание. Данная команда также устанавливает интервал ожидания для защищенного подключения к web-интерфейсу по протоколу HTTPS.

4.6.1.4. Команда **ip http secure-server**

Включает управление коммутатором и просмотр его состояния через защищенное подключение к web-интерфейсу. Использование префикса «**no**» отключает данную функцию.

Синтаксис команды:

ip http secure-server

или

no ip http secure-server

Состояние по умолчанию – защищенное подключение не используется.

Режим ИКС – режим общей настройки.

4.6.1.5. Команда **ip http secure-port**

Используется для назначения TCP-порта для защищенного подключения к GUI. Использование префикса «**no**» возвращает номер порта по умолчанию.

Синтаксис команды:

ip http secure-port *port-number*

или

no ip http secure-port

Параметр команды – port-number – номер TCP-порта для HTTPS-сервера (диапазон от 1 до 65535).

Состояние по умолчанию – номер TCP-порта по умолчанию – 443.

Режим ИКС – режим общей настройки.

4.6.1.6. Команда **ip https certificate**

Используется для выбора активного сертификата для протокола HTTPS. Использование префикса «**no**» возвращает номер активного сертификата по умолчанию.

Синтаксис команды:

ip https certificate number

или

no ip https certificate

Параметр команды – number – номер сертификата (1 или 2).

Состояние по умолчанию – номер сертификата по умолчанию – 1.

Режим ИКС – режим общей настройки.

Примечание. Для генерации сертификата HTTPS необходимо использовать команду crypto certificate number generate.

4.6.1.7. Команда **show ip http**

Используется для отображения текущей конфигурации HTTP-сервера.

Синтаксис команды:

show ip http

Режим ИКС – режим управления.

4.6.1.8. Команда **show ip https**

Используется для отображения текущей конфигурации HTTPS-сервера.

Синтаксис команды:

show ip https

Режим ИКС – режим управления.

4.6.2. Контроль загрузки ресурсов и системных параметров коммутатора

4.6.2.1. Команда **show system resources**

Отображает уровень загрузки ресурсов центрального процессора.

Синтаксис команды:

show system resources

Режим ИКС – режим управления.

4.6.2.2. Команда **show users**

Отображает информацию об активных пользователях.

Синтаксис команды:

show users

Режим ИКС – режим управления.

4.6.2.3. Команда **show system uptime**

Отображает время с момента последнего запуска устройства.

Синтаксис команды:

show system uptime

Режим ИКС – режим управления.

4.6.2.4. Команда **show version**

Отображает информацию о версии исполняемого системного ПО, активном и не активном образах системного ПО.

Синтаксис команды:

show version

Пример информации, выводимой по команде:

```
Kraftway Telecom Operating System
version 3.6.0
Build # KTOS-3.6.0 on host i686-pc-linux-gnu at 08/14/23 14:04:11
Copyright (C) 2023 Kraftway Corporation PLC.  All rights reserved.
Active-image: image-ktos-3.6.0
  Version: 3.6.0
  SHA256 Digest:
 1cf59261fa0508878c0b11b59b0a44d64ff00e9e3ca5c3082ee4a8bd980a735f
  Date: 08/14/23
  Time: 14:04:11
Inactive-image: image-ktos-3.6.0
  Version: 3.6.0
  SHA256 Digest:
 1cf59261fa0508878c0b11b59b0a44d64ff00e9e3ca5c3082ee4a8bd980a735f
  Date: 08/14/23
  Time: 14:04:11
```

Режим ИКС – режим управления.

4.6.2.5. Команда **show interface**

Используется для отображения сводной информации о текущем состоянии выбранного интерфейса или группы интерфейсов устройства.

Синтаксис команды:

show interface [*interface-id*]

Параметр команды – *interface-id* – номер интерфейса, информацию о котором необходимо отобразить.

Состояние по умолчанию – без указания номера интерфейса отображается сводная информация о текущем состоянии всех интерфейсов устройства.

Режим ИКС – режим управления.

Примечание. Для отображения краткой информации о текущем состоянии выбранного интерфейса или всех интерфейсов устройства можно использовать команду **show interface brief**.

4.7. Настройка времени, даты и других системных параметров

4.7.1. Настройка системного времени и даты

Система поддерживает установку времени и даты как вручную, так и в автоматическом режиме. Во втором случае администратор может задать параметры подключения к одному или нескольким серверам времени, с которыми будет осуществляться синхронизация по протоколу NTP. В системе реализована поддержка протокола NTP v.4.

Если в системе определено несколько серверов времени, то один из них определяется в качестве «назначенного сервера». Им автоматически становится сервер с наименьшей ступенью

(stratum) в иерархии эталонов времени. В случае, когда таковых оказывается несколько, то назначенным сервером выбирается тот из них, от которого раньше всего поступит временной пакет.

Если не обнаруживается ни один из серверов времени, то система продолжает производить опрос подключенных устройств с заданным интервалом (poll interval). Коммутатор поддерживает назначение выбранных серверов времени «доверенными», при этом только они могут быть источниками синхронизации. Для подключения к таким серверам можно настроить защищенное соединение.

4.7.1.1. Команда **show clock**

Отображает системное время и дату.

Синтаксис команды:

show clock

Режим ИКС – режим управления.

4.7.1.2. Команда **clock timezone**

Устанавливает значение часового пояса. Использование префикса «**no**» устанавливает значение по умолчанию.

Синтаксис команды:

clock timezone *timezone-name*

или

no clock timezone

Параметр команды – *timezone*-name – полное название часового пояса.

Состояние по умолчанию – «*Moscow*», часовое смещение – «+3», минутное смещение – «0».

Режим ИКС – режим общего конфигурирования.

4.7.1.3. Команда **ntp enable**

Включает использование внешнего источника для установки системного времени. Использование префикса «**no**» отключает использование внешнего источника времени.

Синтаксис команды:

ntp enable

или

no ntp enable

Состояние по умолчанию – внешний источник не используется.

Режим ИКС – режим общего конфигурирования.

4.7.1.4. Команда **ntp server**

Задает адрес NTP-сервера, который будет использоваться для синхронизации системного времени. Использование префикса «**no**» удаляет выбранный сервер из списка NTP-серверов.

Синтаксис команды:

ntp server {*ipv4-address* | *ipv6-address* | *hostname*} [**maxpoll**] [**minpoll**][**key** *keyid*] **[prefer]**

или

no ntp server {*ipv4-address* | *ipv6-address hostname*}

Параметры команды:

— *ipv4-address* – IP-адрес сервера в формате IPv4;

— *ipv6-address* – IP-адрес сервера в формате IPv6;

— *hostname* – доменное имя сервера (до 158 символов);

— **maxpoll** – задает максимальный интервал опроса NTP сервера;

— **minpoll** – задает минимальный интервал опроса NTP сервера;

— **prefer** – задает предпочтительный сервер для синхронизации времени;

— **key** – включает использования ключа аутентификации;

— *keyid* – идентификатор ключа (диапазон от 1 до 65534).

Состояние по умолчанию – NTP-серверы не заданы.

Режим ИКС – режим общего конфигурирования.

Примечание. Сведения синхронизации времени, полученные от предпочтительного NTP сервера, отбрасываются, если они резко отличаются от других источников времени.

4.7.1.5. Команда **show ntp peers**

Отображает конфигурацию протокола NTP.

Синтаксис команды:

show ntp peers

Режим ИКС – режим управления.

4.7.1.6. Команда **show ntp peer-status**

Отображает текущее состояние NTP-серверов.

Синтаксис команды:

show ntp peer-status

Режим ИКС – режим управления.

4.7.1.7. Команда **ntp authentication-key**

Устанавливает ключ проверки подлинности для протокола NTP. Использование префикса «**no**» удаляет указанный ключ.

Синтаксис команды:

ntp authentication-key *key-number* **md5** *key-value*

или

no ntp authentication-key *key-number*

Параметры команды:

– *key-number* – номер ключа (диапазон от 1 до 4294967295);

– *key-value* – значение ключа(диапазон от 1 до 8 символов).

Состояние по умолчанию – проверка подлинности отключена.

Режим ИКС – режим общего конфигурирования.

4.7.1.8. Команда **ntp authenticate**

Включает проверку подлинности для NTP-трафика, полученного от серверов. Использование префикса «**no**» отключает указанную проверку.

Синтаксис команды:

ntp authenticate

или

no ntp authenticate

Состояние по умолчанию – проверка подлинности отключена.

Режим ИКС – режим общего конфигурирования.

4.7.1.9. Команда **ntp trusted-key**

Осуществляет проверку подлинности системы, от которой синхронизируется с помощью SNTP по заданному ключу. Использование префикса «**no**» отключает указанную проверку подлинности.

Синтаксис команды:

ntp trusted-key *key-number*

или

no ntp trusted-key *key-number*

Параметр команды – *key-number* – номер проверяемого ключа (диапазон от 1 до 4294967295).

Состояние по умолчанию – проверка подлинности отключена.

Режим ИКС – режим общего конфигурирования.

4.7.2. Базовые команды управления

4.7.2.1. Команда **ping**

Служит для передачи запросов (ICMP Echo-Request) протокола ICMP указанному узлу сети и для контроля поступающих ответов (ICMP Echo-Reply).

Синтаксис команды:

ping *hostname*

или

ping ip {*ipv4-address*|*hostname*}

или

ping ipv6 {*ipv6-address*|*hostname*}

Параметры команды:

- **ip** – для передачи запросов используется протокол IPv4;
- **ipv6** – для передачи запросов используется протокол IPv6;
- *ipv4-address* – IPv4-адрес узла сети;
- *ipv6-address* – IPv6-адрес узла сети;
- *hostname* – доменное имя узла сети.

Режим ИКС – режим управления.

Примечание. Для остановки передачи пакетов нажмите <**Esc**>.

4.7.2.2. Команда **traceroute**

Служит для определения маршрута трафика до узла назначения.

Синтаксис команды:

traceroute ip {*ipv4-address*|*hostname*}

или

traceroute ipv6 {*ipv4-address*|*hostname*}

или

traceroute ***hostname***

Параметры команды:

- **ip** – для определения маршрута используется протокол IPv4;
- **ipv6** – для определения маршрута используется протокол IPv6;
- *ipv4-address* – IPv4-адрес узла сети;
- *ipv6-address* – IPv6-адрес узла сети;
- *hostname* – доменное имя узла сети.

Режим ИКС – режим управления.

Команда отправляет запросы и строит маршрут путем определения времени прибытия на каждый участок маршрута до тех пор, пока не достигнет узла назначения или не истечет время жизни пакета TTL. Кроме того, процесс определения маршрута остановится при нажатии сочетания клавиш <Ctrl+c>.

В таблице 5 описаны коды ошибок, которые могут появляться при выполнении команды.

Таблица 5

Код ошибки	Описание
*	Таймаут при попытке передачи пакета
?	Неизвестный тип пакета
A	Административно недоступен. Обычно происходит при блокировании исходящего трафика по правилам в таблице доступа ACL
F	Требуется фрагментация и установка битов DF
H	Узел сети недоступен
N	Сеть недоступна
P	Протокол недоступен
Q	Источник подавлен
R	Истекло время повторной сборки фрагмента
S	Ошибка исходящего маршрута
U	Порт недоступен

4.7.2.3. Команда **`telnet`**

Используется для подключения к устройству, которое поддерживает соединение по протоколу Telnet.

Синтаксис команды:

`telnet` {*`ip-address`* | *`hostname`*} *`port`*

Параметры команды:

– *`ip-address`* – IP-адрес подключаемого устройства;

– *`hostname`* – доменное имя подключаемого устройства;

– *`port`* – TCP-порт, по которому работает служба Telnet, по умолчанию – 23;

Режим ИКС – режим управления.

4.7.2.4. Команда **hostname**

Служит для установки или редактирования сетевого имени устройства. Использование префикса «**no**» удаляет существующее имя устройства.

Синтаксис команды:

hostname *name*

или

no hostname

Параметры команды:

name – сетевое имя устройства (от 1 до 64 символов).

Состояние по умолчанию – сетевое имя устройства не определено.

Режим ИКС – режим общего конфигурирования.

4.7.2.5. Команда **reload**

Используется для перезагрузки устройства.

Синтаксис команды:

reload

Режим ИКС – привилегированный режим управления.

4.8. Использование буфера истории команд и журнала Syslog

4.8.1. Команды для работы с буфером истории команд

В интерфейсе командной строки реализован буфер истории команд, в котором хранятся до 2147483647 последних команд, ранее введенных в течение текущей терминальной сессии. Этот буфер позволяет просмотреть действия, произведенные во время данного сеанса управления устройством, и повторно вызывать ранее веденные команды, не вводя их полностью заново.

Администратор может отключить сохранение истории команд, а также установить необходимое количество сохраняемых в буфер команд.

4.8.1.1. Команда **history max**

Устанавливает размер буфера истории введенных команд. Использование префикса «**no**» возвращает значение по умолчанию.

Синтаксис команды:

history max *number-of-commands*

или

no history max

Параметр команды:

number-of-commands – количество команд, сохраняемых в буфере (диапазон от 0 до 2147483647).

Состояние по умолчанию – размер буфера истории максимальный.

Для отключения хранения истории введенных команд необходимо установить history max 0.

Режим ИКС – режим конфигурирования линии.

Примечание. Данная команда задает размер буфера истории команд для конкретного вида подключения (console, VTY).

4.8.1.2. Команда **show cli history**

Отображает историю команд, введенных в текущей сессии управления устройством.

Синтаксис команды:

show cli history

Режим ИКС – режим управления.

Примечание. Команды отображаются в хронологической последовательности, начиная от самой ранней введенной команды. Буфер продолжает работать при входе в режимы настройки и выходе из них.

4.8.2. Работа с системным журналом Syslog

В коммутаторе реализована поддержка регистрации событий с использованием протокола Syslog. Системный журнал позволяет вести историю событий, произошедших на устройстве, а также контролировать произошедшие события в реальном времени. В журнал заносятся соответствующие сообщения о событиях, при этом каждое сообщение имеет свой уровень важности. В системе выделены события 8 типов важности, представленные в таблице 6 в порядке убывания их важности.

Таблица 6

Тип событий	Условный номер	Сообщения	Описание
Emergencies	–	Чрезвычайные	Система функционирует неправильно
Alerts	1	Сигналы тревоги	Необходимо немедленное вмешательство в систему
Critical	2	Критические	В системе произошла критическая ошибка

Тип событий	Условный номер	Сообщения	Описание
`Errors`	3	Ошибки	В системе произошла ошибка
`Warnings`	4	Предупреждения	Предупреждение, неаварийное сообщение
`Notifications`	5	Уведомления	Уведомление системы, неаварийное сообщение
`Informational`	6	Информационные	Информационное сообщение системы
`Debugging`	7	Отладочные	Предоставляет пользователю информацию для корректной настройки системы

Система позволяет вести журнал регистрации событий как локально непосредственно на самом устройстве, так и использовать для этого внешний Syslog-сервер. При этом поддерживается подключение до 3 таких Syslog-серверов. В целом сообщения о событиях могут регистрироваться:

– на экране консоли (logging console);

– на экране удаленного терминала (logging monitor);

– в специальном файле, хранящемся в энергонезависимой памяти устройства (logging logfile);

– на внешнем Syslog-сервере (logging host).

4.8.2.1. Команда **`logging level`**

Изменяет уровень регистрации отладочных сообщений и сообщений об ошибках в консоли для отдельных протоколов.

Использование префикса «**`no`**» возвращает значение по умолчанию.

Синтаксис команды:

`logging level` *`protocol level`*

или

`no logging level` *`protocol`*

Параметры команды:

– *`protocol`*, возможные значения - `all` | `auth` | `dvmrp` | `hostp` | `hsl` | `lacp` | `lagd` | `ldp` | `mstp` | `ndd` | `nsm` | `oam` | `onm` | `pim` | `pservd` | `ptp` | `rib` | `rmon` | `rsvp` | `trill` | `vrrp` ;

– *`level`*, возможные значения - от 1 до 7.

Состояние по умолчанию – регистрация отладочных сообщений и сообщений об ошибках включена для вывода в консоль и удаленных сеансов.

Режим ИКС – режим общего конфигурирования.

4.8.2.2. Команда **logging console**

Включает вывод на консоль сообщений о событиях до выбранного уровня важности. Использование префикса «**no**» возвращает уровень важности по умолчанию.

Синтаксис команды:

logging console *level*

или

no logging console

Параметр команды – *level* – уровень важности регистрируемых событий - `emergencies (0)`, `alerts (1)`, `critical (2)`, `errors (3)`, `warnings (4)`, `notifications (5)`, `informational (6)`, `debugging (7)`, задается цифровым значением от 0 до 7.

Состояние по умолчанию – на консоль выводятся информационные сообщения – critical (2).

4.8.2.3. Команда **logging logfile**

Включает регистрацию сообщений о событиях до выбранного уровня важности в файл журнала. Использование префикса «**no**» отключает регистрацию сообщений в файле журнала.

Синтаксис команды:

logging logfile *file-name level size*

или

no logging logfile

Параметр команды:

- *file-name* – имя файла журнала (до 200 символов);

- *level* – уровень важности регистрируемых событий - emergencies (0), alerts (1), critical (2), errors (3), warnings (4), notifications (5), informational (6), debugging (7), задается цифровым значением от 0 до 7;

- *size* – размер файла журнала в байтах.

Состояние по умолчанию – регистрация событий отключена.

Режим ИКС – режим общего конфигурирования.

4.8.2.4. Команда **logging host**

Включает передачу сообщений о событиях до выбранного уровня важности на удаленный Syslog-сервер. Использование префикса «**no**» удаляет сетевой узел с указанными параметрами из списка Syslog-серверов.

Синтаксис команды:

logging server {*address* | *hostname*} [**severity** *level*] [**facility** *facility*] [**description** *text*]

или

no logging host {*address* | *hostname*}

Параметры команды:

– *address* – IP-адрес Syslog-сервера в формате IPv4 или IPv6;

– *hostname* – доменное имя Syslog-сервера (до 158 символов);

– *level* – уровень важности регистрируемых событий - `emergencies (0)`, `alerts (1)`, `critical (2)`, `errors (3)`, `warnings (4)`, `notifications (5)`, `informational (6)`, `debugging (7)`, задается цифровым значением от 0 до 7;

– *facility* – параметр, передаваемый внутри сообщения. Возможные значения - `local0`, `local1`, `local2`, `local3`, `local4`, `local5`, `local6`, `local7`, по умолчанию – `local7`;

– *text* – текстовое описание Syslog-сервера (до 64 символов).

Состояние по умолчанию – на внешние серверы Syslog сообщения не отправляются.

Режим ИКС – режим общего конфигурирования.

4.8.2.5. Команда **clear logging**

Удаляет все сообщения из внутреннего буфера.

Синтаксис команды:

clear logging

Режим ИКС – режим управления.

4.8.2.6. Команда **show logging logfile**

Отображает состояние файла журнала (ведется или нет), имя файла журнала и сообщения, записанные в нем.

Синтаксис команды:

show logging file

Режим ИКС – режим управления.

4.8.2.7. Команда **show logging logfile last-index**

Отображает количество записей в файле журнала.

Синтаксис команды:

show logging logfile last-index

Режим ИКС – режим управления.

4.8.2.8. Команда **show logging logfile start-seqn end-seqn**

Отображает записи из диапазона номеров указанные в файле журнала.

Синтаксис команды:

show logging logfile start-seqn *index-start-seqn* [**end-seqn** *index-end-seqn*]

Параметры команды:

– *index-start-seqn* – номер начального значения (от 0 до 2147483647) для диапазона номеров;

– *index-end-seqn* – номер конечного значения (от 0 до 2147483647) для диапазона номеров.

Режим ИКС – режим управления.

4.8.2.9. Команда **show logging logfile start-time end-time**

Отображает записи, заданные временным диапазоном из файла журнала.

Синтаксис команды:

show logging logfile start-time *year month day time* [**end-time** year *month day time*]

Параметры команды:

– *year* – начальный (конечный) год (четыре символа, в формате YYYY, пример: 2024) для задания временного диапазона;

– *month* – начальный (конечный) месяц (три символа, в формате MMM, пример: Jan, Feb, Mar, …, Oct, Nov или Dec) для задания временного диапазона;

– *day* – начальный (конечный) день (от 1 до 31, два символа, в формате DD, пример: 03) для задания временного диапазона;

– *time* – начальные (конечные) часы (от 0 до 23), минуты (от 0 до 59), секунды (от 0 до 59) для задания временного диапазона (восемь символов, в формате HH:MM:SS, пример: 06:20:49).

Режим ИКС – режим управления.

4.8.2.10. Команда **show logging server**

Отображает текущие настройки для удаленных Syslog-серверов.

Синтаксис команды:

show logging servers

Режим ИКС – режим управления.

5. БЕЗОПАСНАЯ РАБОТА С ПРОГРАММНЫМ ОБЕСПЕЧЕНИЕМ И КОНФИГУРАЦИЕЙ

5.1. Принцип хранения системного программного обеспечения

Исполняемое и загрузочное ПО, а также все настройки системы хранятся в виде файлов, расположенных во встроенной энергонезависимой памяти коммутатора. Система поддерживает загрузку и выгрузку указанных файлов, их резервное копирование, обновление, удаление и ряд других операций, необходимых для работы со встроенным ПО и настройками устройства.

Исполняемое ПО хранится в виде единого файла, представляющего собой образ ПО. При этом для обеспечения восстановления в энергонезависимой памяти устройства всегда хранятся два экземпляра, один из которых является активным и загружается при старте системы, а второй хранится в виде резервной копии. Если при старте системы образ, назначенный активным, по какой-либо причине не загружается, информация об этом будет выведена на устройство ввода-вывода с отправкой соответствующего сообщения в журнал регистрации событий Syslog.

Оба образа исполняемого ПО хранятся в энергонезависимой памяти в заархивированном виде, откуда один из них распаковывается в оперативную память при старте системы. Администратор может переназначить активный образ в процессе работы устройства, при этом настройка вступит в силу после перезапуска системы. При обновлении ПО перед загрузкой новой версии производится его автоматическая проверка на целостность и правильность формата, после чего запускается загрузка, по завершении которой обновленный образ становится неактивным. После перезагрузки коммутатора старый образ сохраняется в памяти в виде резервной копии, на которую можно вернуться в случае наличия ошибок в новой версии. Обновление системного ПО можно производить с помощью протоколов передачи файлов по сети.

5.2. Принцип хранения загрузочного программного обеспечения

В энергонезависимой памяти хранятся также загрузочные файлы. Они содержат загрузочный код, который используется для инициализации аппаратной части и запуска системы. Он выполняет распаковку исполняемого ПО из из постоянного запоминающего устройства (далее – ПЗУ) в оперативную память и управляет несколькими образами системного ПО.

5.3. Работа с конфигурационными файлами

Все произведенные в системе настройки хранятся в конфигурационных файлах, которые записываются в энергонезависимую память. При этом коммутатор содержит следующие виды конфигурационных файлов:

– Startup configuration file – конфигурационный файл, содержащий все настройки системы и значения соответствующих параметров, которые активизируются при старте системы;

– Running configuration file – конфигурационный файл, в котором хранятся все настройки системы и значения соответствующих параметров, которые администратор изменил в процессе работы устройства. Указанные настройки продолжают действовать до тех пор, пока система не будет перезапущена или администратор не внесет новые изменения в настройки;

– Empty configuration file – пустой конфигурационный файл, применяющийся для загрузки устройства с настройками по умолчанию.

Примечание. Для сохранения изменений, внесенных в конфигурацию систему в процессе ее работы, рекомендуется файл Running configuration скопировать в файл Startup configuration. В противном случае после перезагрузки устройства все новые настройки будут утеряны.

Администратор может производить следующие операции с конфигурационными файлами:

- загрузка стартовой или текущей конфигурации из внешнего источника;
- копирование текущей конфигурации в стартовую;
- копирование пустой конфигурации в стартовую.

Вносить изменения в настройки администратор может как непосредственно на самом устройстве через ИКС, так и путем создания соответствующего файла на внешнем ПК и его последующей загрузки в коммутатор.

6. КОМАНДЫ ДЛЯ РАБОТЫ С ПО И КОНФИГУРАЦИОННЫМИ ФАЙЛАМИ

При выполнении операций над файлами в аргументах соответствующих команд указываются URL-адреса местонахождения файлов, а также используются ключевые слова. В таблице 7 описаны ключевые слова и префиксы адресов, которые используются в операциях над файлами.

Таблица 7

Ключевое слово, префикс	Описание
`running-config`	Файл текущей конфигурации
`startup-config`	Файл стартовой конфигурации
`empty-config`	Пустой файл конфигурации
`active-image`	Файл активного образа системного ПО
`inactive-image`	Файл неактивного образа системного ПО
`ftp`	Использование протокола ftp для доступа к файлу
`tftp`	Использование протокола tftp для доступа к файлу
`sftp`	Использование протокола sftp для доступа к файлу
`scp`	Использование протокола scp для доступа к файлу
`log`	Использование директории системых журналов

6.1. Операции над файлами системного ПО

6.1.1. Действия с конфигурацией

6.1.1.1. Команда **`copy`**

Используется для копирования файла из местоположения источника в местоположение назначения. Данная команда может использоваться как для локального копирования файлов, так и для копирования между локальным устройством и удаленной системой.

Синтаксис команды:

`copy` *`source destination`*

Параметры команды:

– `source` – местонахождения копируемого файла;

– `destination` – назначения файла, в который данные будет скопирован файл источник.

Режим ИКС – привилегированный режим управления.

Примечание. При указании адресов используются префиксы и ключевые слова, описанные в таблице 7. Процесс копирования может длиться до нескольких минут и зависит от используемого протокола и структуры сети между источником и назначением.

В качестве источника или назначения может выступать файл удаленного устройства в таком случаи используются протоколы удаленного доступа: ftp, tftp,sftp, scp.

Синтаксис команд при работе с протоколами удаленного доступа:

copy {ftp | tftp | sftp | scp} {*url* | **active-image | inactive-image | running-config | startup-config**}

или

copy {**log** *file-name* | ***active-image*** / ***inactive-image*** / ***running-config*** / ***startup-config***} {**ftp | tftp | sftp | scp**} [*url*]

Параметры команды – *url* – адрес файла на удаленном устройстве.

Примечание. Параметр *url* является опциональном, в случаи его отсутствия, команда будет выполнена в интерактивном режиме. В интерактивном режиме предлагается последовательно ввести необходимые данные для доступа к файлу через протокол удаленного доступа.

Наиболее часто используемые схемы копирования файлов:

– сохранение активного образа системного ПО на сервере:

copy active-image destination

– сохранение log файла на сервере:

copy log *file-name* destination

– копирование файла конфигурации с сервера в текущую конфигурацию:

copy *source* **running-config**

Команды из загруженной конфигурации добавляются к уже существующей текущей конфигурации так, что итоговая текущая конфигурация является комбинацией, существующей и вновь загруженной экземпляров. В случаи возникновение ошибки при выполнении добавляемой команды, данная команда будет пропущена, при этом процесс добавления других команд будет продолжен.

– сохранение текущей или стартовой конфигурации на сервере:

copy running-config destination
copy startup-config destination

– сохранение текущей конфигурации в стартовую конфигурацию:

copy running-config startup-config

– сохранение пустой конфигурации в стартовую конфигурацию:

copy empty-config startup-config

Существуют недопустимые комбинации адресов источника и назначения, которые описываются следующими условиями:

– исходный файл и файл назначения не могут совпадать;

– TFTP-сервер не может быть одновременно указан в адресе исходного местонахождения и адресе назначения;

– копирование файлов конфигурации с сервера в стартовую конфигурацию запрещено;

– копирование файлов образа системного ПО с сервера в файл активного или неактивного образа системного ПО запрещено, системное ПО может быть загружено командой **boot system**.

Процесс копирования сопровождается отображением количества успешно скопированных данных.

В следующем примере производится копирование файла конфигурации `start-conf` с TFTP-сервера с адресом `192.168.122.1` в энергонезависимую память коммутатора:

– с указанием параметра *url* :

```
KRAFTWAY#copy tftp tftp://192.168.122.1/start-conf startup-config
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  9298  100  9298    0     0  2013k      0 --:--:-- --:--:-- --:--:-- 2013k
100  9298  100  9298    0     0   776k      0 --:--:-- --:--:-- --:--:--  776k
Copy Success
```

– без указания параметра *url*, в интерактивном режиме:

```
KRAFTWAY#copy tftp startup-config
Enter IP:192.168.122.1
Enter port [69]:
Enter filename:start-conf
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  9298  100  9298    0     0  1509k      0 --:--:-- --:--:-- --:--:-- 1509k
100  9298  100  9298    0     0   662k      0 --:--:-- --:--:-- --:--:--  662k
Copy Success
```

6.1.1.2. Команда **write**

Сохраняет текущую конфигурацию в файл стартовой конфигурации.

Синтаксис команды:

write [**memory | terminal**]

Параметры команды:

– **memory** – сохранение текущую конфигурацию в файл стартовой конфигурации;

– **terminal** –вывод текущей конфигурации на экран.

Режим ИКС – привилегированный режим управления.

6.1.1.3. Команда **boot system**

Используется для назначения активного файла системного ПО, который будет загружаться при старте системы.

Синтаксис команды:

boot system {**inactive-image** | *url*}

Параметры команды:

– **inactive-image** – при следующем старте системы загрузится образ, который в текущий момент является неактивным;

– *url* – адрес URL копируемого образа, который загрузится при следующем старте системы.

Режим ИКС – привилегированный режим управления.

Примечание. Для определения, какой файл в текущий момент является активным, используется команда **show version**.

6.1.2. Просмотр конфигурации

6.1.2.1. Команда **show running-config**

Отображает содержимое файла текущей конфигурации.

Синтаксис команды:

show running-config

Режим ИКС – режим управления.

6.1.2.2. Команда **show startup-config**

Отображает содержимое файла стартовой конфигурации.

Синтаксис команды:

show startup-config

Режим ИКС – режим управления.

6.1.2.3. Команда **show version**

Показывает активный файл системного ПО, который загружается при старте системы.

Синтаксис команды:

show version

Режим ИКС – режим управления.

Пример использования команды:

```
KRAFTWAY#show version
Kraftway Telecom Operating System
version 3.6.0
Build # KTOS-3.6.0 on host i686-pc-linux-gnu at 08/14/23 14:04:11
Copyright (C) 2023 Kraftway Corporation PLC.  All rights reserved.
Active-image: image-ktos-3.6.0
  Version: 3.6.0
  SHA256 Digest:
 1cf59261fa0508878c0b11b59b0a44d64ff00e9e3ca5c3082ee4a8bd980a735f
  Date: 08/14/20
  Time: 14:04:11
Inactive-image: image-ktos-3.6.0
  Version: 3.6.0
  SHA256 Digest:
 1cf59261fa0508878c0b11b59b0a44d64ff00e9e3ca5c3082ee4a8bd980a735f
  Date: 08/14/23
```

7. НАСТРОЙКА ЗЕРКАЛИРОВАНИЯ ТРАФИКА

7.1. Поддержка функции зеркалирования трафика

Для анализа трафика и мониторинга устройств предполагается возможность определить порт, в который будет перенаправлена копия всего трафика, проходящего через заданные порты. Администратор может включить зеркалирование трафика на порту назначения. По умолчанию зеркалирование трафика не включено. Предусматривается только один порт назначения. Администратор может зеркалировать один или несколько портов в порт назначения одновременно.

В случае если в качестве источника используется несколько портов, трафик, направляемый в порт назначения, помещается в его очередь и обслуживается по принципу «первый пришел, первым обслужен», а любой избыточный трафик будет отброшен без предупреждений. Это может означать, что на порт анализатора, подключенный к порту назначения, будет направлено произвольно выбранное подмножество фактического трафика, проходящего через порты источников.

При создании сессии зеркалирования следует учитывать следующие ограничения:

- сессия зеркалирования вмещает до 16 портов источников и одного порта назначения;
- один порт не может быть одновременно и портом источника, и портом назначения;
- oob-порт не может быть ни портом источника, ни портом назначения;
- протокол 802.1x не может быть включен на порту назначения.

7.2. Команды для настройки зеркалирования трафика

7.2.1. Создание сессии зеркалирования трафика

7.2.1.1. Команда **mirror interface**

Используется для создания сессии назначения зеркалирования трафика. Данная команда выполняется из режима настройки интерфейса, на который будет осуществляться зеркалирование. Порт коммутатора на который осуществляется зеркалирование трафика не должен принадлежать к тому же bridge-domain, что и порт-источник.

Для удаления порта назначения из bridge-domain необходимо использовать команду «**no**» **bridge-group 1** из режима конфигурации интерфейса.

Синтаксис команды:

mirror interface *interface-id* **direction** [both | receive | transmit]

или

no mirror interface *interface-id*

Параметры команды:

- *interface-id* – идентификатор интерфейса, которым должен быть физический порт;
- **direction** - направление потока трафика относительно интерфейса;

– **both** – захват всего трафика проходящего через интерфейс;

– **receive** – захват входящего трафика на коммутатор;

– **transmit** – захват исходящего трафика от коммутатора.

Состояние по умолчанию – зеркалирование отключено.

Режим ИКС – режим конфигурирования интерфейса.

7.2.2. Отображение текущего состояния зеркалирования трафика

7.2.2.1. Команда **show mirror**

Отображает текущее состояние всех сессий зеркалирования трафика. При использовании дополнительного параметра **interface**, отображает информацию по конкретному интерфейсу.

Синтаксис команды:

show mirror interface *interface-id*

Параметр команды – *interface-id* – идентификатор интерфейса, которым должен быть физический порт.

Режим ИКС – режим управления.

8. РАБОТА С ТАБЛИЦЕЙ MAC-АДРЕСОВ

8.1. Принцип формирования таблицы MAC-адресов

Коммутация пакетов на втором уровне сетевой модели OSI системой производится с использованием базы данных пересылки (Forwarding Data BASE, FDB). Она хранится в троичной ассоциативной памяти, реализованной непосредственно в структуре пакетного процессора. В состав базы данных пересылки входит таблица MAC-адресов, в которой хранятся MAC-адреса сетевых устройств, которые пересылали пакеты через интерфейсы коммутатора. Аппаратная реализация таблицы MAC-адресов позволяет осуществлять коммутацию пакетов без участия центрального процессорного устройства (далее – ЦПУ), т.е. без потери скорости передачи данных.

В системе поддерживается привязка отдельной таблицы MAC-адресов к каждому интерфейсу. Заполнение таблицы MAC-адресов происходит как в динамическом, так и статическом режимах. В первом случае происходит «обучение» указанной таблицы, при котором в нее вносятся новые записи по мере прохождения через интерфейс пакета с не зафиксированным до этого MAC-адресом отправителя. После перезагрузки системы такие записи не сохраняются, и процесс «обучения» запускается по новому циклу. Кроме того, такие записи имеют заданное время действия (aging time), по истечении которого автоматически удаляются из таблицы.

Во втором случае отдельные записи в таблицу MAC-адресов можно внести вручную статически. Такие записи сохраняются после перезагрузки системы и не подвергаются устареванию, т.е. не имеют времени действия (aging time). Они сохраняются в конфигурационном файле и могут быть удалены или отредактированы только в статическом режиме вручную.

8.2. Команды для работы с таблицей MAC-адресов

8.2.1. Добавление/удаление MAC-адресов

8.2.1.1. Команда **bridge 1 address**

Необходима для добавления заданного MAC-адреса отправителя в таблицу адресов. Использование префикса «**no**» удаляет заданный MAC-адрес отправителя из таблицы адресов.

Синтаксис команды:

bridge 1 address *mac-address* **forward** *interface-id* **vlan** *vlan-id*

или

no bridge 1 address *mac-address* **forward** *interface-id* **vlan** *vlan-id*

Параметры команды:

– *mac-address* – добавляемый MAC-адрес отправителя;

– *vlan-id* – номер сети VLAN (диапазон от 2 до 4094);

– *interface-id* – номер интерфейса, к которому прикрепляется таблица MAC-адресов.

Состояние по умолчанию – статические записи отсутствуют.

Режим ИКС – режим общего конфигурирования.

8.2.1.2. Команда **clear mac address-table**

Удаляет статические или динамические записи из таблицы MAC-адресов.

Синтаксис команды:

clear mac address-table [**dynamic** | **static**] [**interface** *interface-id* | **vlan** *vlan-id* | **cvlan** c*vlan-id* | **address** *mac-address* | **bridge** *bridge-id*]

Параметры команды:

– **dynamic** – удаление динамических записей;

– **static** – удаление статических записей;

– *interface-id* – удаление всех записей привязанных к заданному интерфейсу - порту Ethernet или группе агрегированных портов;

– *vlan-id* удаление всех записей привязанных к заданному vlan;

– *cvlan-id* удаление всех записей привязанных к заданному cvlan;

– *mac-address* удаление записи с указанным MAC-адресом;

– *bridge-id* удаление всех записей привязанных к заданному bridge.

При манипуляциях с таблицой MAC-адресов указание bridge-id 1 является обязательным.

Пример выполнения команды:

clear mac address-table dynamic *interface eth1 bridge 1*

Режим ИКС – режим управления.

8.2.2. Задание времени хранения адреса

8.2.2.1. Команда **bridge 1 ageing-time**

Устанавливает время хранения адреса в таблице MAC-адресов. Использование префикса «**no**» возвращает указанному времени значение по умолчанию.

Синтаксис команды:

bridge 1 ageing-time *seconds*

или

no bridge 1 ageing-time

Параметр команды – *seconds* – время хранения MAC-адреса в таблице в секундах (от 10 до 1000000 с).

Состояние по умолчанию – 300 с.

Режим ИКС – режим общего конфигурирования.

8.2.3. Просмотр таблицы MAC-адресов

8.2.3.1. Команда **show mac address-table**

Отображает таблицу MAC-адресов для указанного интерфейса или всех интерфейсов.

Синтаксис команды:

show mac address-table bridge 1 **[dynamic** | **static** | **address** *mac-address* | **interface** *inetface-id* | **vlan** *vlan-id*]

Параметры команды:

– **dynamic** – отображаются только динамические адреса;

– **static** – отображаются только статические адреса;

– *vlan-id* – номер сети VLAN (1-4094);

– *interface-id* – номер интерфейса - порт Ethernet или группа агрегированных портов;

– *mac-address* – MAC-адрес.

Режим ИКС – режим управления.

8.2.3.2. Команда **show mac address-table count bridge 1**

Отображает количество записей в таблице MAC-адресов для указанного интерфейса или для всех интерфейсов.

Синтаксис команды:

show mac address-table count bridge 1 [**vlan** *vlan-id* | **interface** *interface-id* | **address** *mac-address* | **static** | **dynamic**]

Параметры команды:

– *vlan-id* – номер сети VLAN (1-4094);

– *interface-id* – номер интерфейса - порт Ethernet или группа агрегированных портов;

– *mac-address* – MAC-адрес.

Режим ИКС – режим управления.

9. НАСТРОЙКА АГРЕГАЦИИ КАНАЛОВ

9.1. Поддержка функции агрегации каналов

Система поддерживает механизм агрегации каналов, при котором можно несколько физических портов объединить в один логический интерфейс. Это увеличивает пропускную способность всего агрегированного соединения в тех случаях, когда возможности отдельных физических портов этого сделать не позволяет, а также повышает отказоустойчивость канала.

Коммутатор обеспечивает объединение до восьми интерфейсов Ethernet в одной группе агрегированных каналов (Link Aggregation Group, LAG) и до восьми групп LAG на устройстве. Каждая группа портов должна состоять из интерфейсов Ethernet с одинаковой скоростью, работающих в одинаковом дуплексном режиме.

Устройство поддерживает два режима создания группы портов – статическая группа и группа, работающая по протоколу LACP (Link Aggregation Control Protocol). При этом если для интерфейса произведены настройки, то для добавления его в группу следует вернуть настройки по умолчанию.

9.2. Команды для настройки агрегированных каналов

9.2.1. Выбор/добавление каналов

9.2.1.1. Команда `interface`

Может использоваться для выбора интерфейса, к которым будет применяться последующая команда.

Синтаксис команды:

`interface` *`interface-id`*

Параметр команды:

– *`interface-id`* – идентификатор интерфейса;

Режим ИКС – режим общего конфигурирования.

9.2.1.2. Команда `static-channel-group`

Используется для добавления выбранного интерфейса Ethernet в группу статических агрегированных каналов. Использование префикса «**`no`**» удаляет интерфейс Ethernet из группы статических агрегированных каналов.

Синтаксис команды:

static-channel-group *port-channel*

или

no static-channel-group

Параметр команды – *port-channel* – номер группы агрегированных портов в диапазоне от 1 до 12, в который добавляется интерфейс.

Состояние по умолчанию – порт не принадлежит к группе агрегированных каналов.

Режим ИКС – режимы конфигурирования интерфейса (Ethernet).

9.2.1.3. Команда **channel-group**

Используется для добавления выбранного интерфейса Ethernet в группу агрегированных каналов LACP. Использование префикса «**no**» удаляет интерфейс Ethernet из группы статических агрегированных каналов.

Синтаксис команды:

channel-group *port-channel* **mode** {***active*** | ***passive***}

Параметры команды:

- *port-channel* – номер группы агрегированных портов, принадлежащий диапазону от 1 до 65535, в который добавляется интерфейс;

– **mode active** – добавление интерфейса с использованием протокола LACP в активном режиме;

– **mode passive** – добавление интерфейса с использованием протокола LACP.

Состояние по умолчанию – порт не принадлежит к группе агрегированных каналов.

Режим ИКС – режимы конфигурирования интерфейса (Ethernet).

9.2.2. Просмотр каналов

9.2.2.1. Команда **show static-channel-group**

Отображает информацию обо всех статических агрегированных каналах.

Синтаксис команды:

show static-channel-group

Режим ИКС – режим управления.

9.2.3. Балансировка нагрузки

9.2.3.1. Команда **load-balance**

Предназначена для задания механизма балансировки нагрузки для группы агрегированных каналов. Использование префикса «**no**» удаляет параметры конфигурации механизма балансировки нагрузки для группы агрегированных каналов.

Синтаксис команды:

load-balance *{dst-ip | dst-mac | ip-port | ip-port-proto | src-dst-ip | src-dst-mac | src-dst-port | src-ip | src-mac}*

или

no load-balance

Параметры команды:

– **dst-ip** – механизм балансировки основывается на IP-адресе получателя;

– **dst-mac** – механизм балансировки основывается на MAC-адресе получателя;

– **ip-port** – механизм балансировки основывается на IP-адресе и номере TCP/UDP порта отправителя и получателя;

– **ip-port-proto** – механизм балансировки основывается на IP-адресе, номере TCP/UDP порта, протоколе отправителя и получателя;

– **src-dst-ip** – механизм балансировки основывается на IP-адресе отправителя и получателя;

– **src-dst-mac** – механизм балансировки основывается на MAC-адресе отправителя и получателя;

– **src-dst-port** – механизм балансировки основывается на номере TCP/UDP порта отправителя и получателя;

– **src-ip** – механизм балансировки основывается на IP-адресе отправителя;

– **src-mac** – механизм балансировки основывается на MAC-адресе отправителя.

Режим ИКС – режим конфигурации интерфейса.

10. НАСТРОЙКА ВИРТУАЛЬНЫХ ЛОКАЛЬНЫХ СЕТЕЙ VLAN

10.1. Поддержка виртуальных локальных сетей VLAN

Система поддерживает создание и обслуживание до 4094 виртуальных локальных сетей VLAN. Они широко используются для разделения пользователей на логические группы. Для коммутаторов, работающих на нескольких уровнях сетевой модели OSI, использование виртуальных локальных сетей VLAN обычно означает, что пользователи из разных сетей VLAN по-прежнему могут связываться, но должны для этого использовать IP-маршрутизацию.

Сеть VLAN может быть задана для отдельного коммутатора или она может занимать несколько коммутаторов путем определения сети VLAN на каждом из них, но при условии использования одного и того же тэга VLAN и соединения коммутаторов через порты, которые являются членами этой сети VLAN. При этом коммутация пакета системой производится в контексте отдельной сети VLAN. Каждый пакет классифицируется на входе в VLAN, причем такая классификация определяется на основе тэга VLAN в пакете (т.е. когда тэг задан внешне) или производится по некоторым установленным пользователем правилам на основе входного порта или каких-либо значений из заголовка пакета. Классификация VLAN является частью входной обработки пакета.

На рис. 38 показана последовательность обработки данных при прохождении кадра (frame) от входного порта коммутатора к выходному.

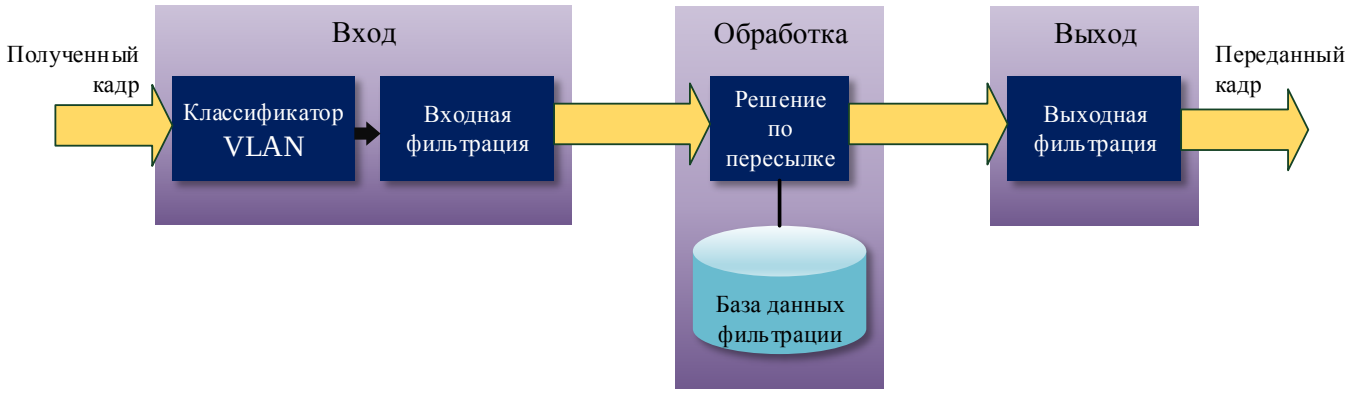


Рис. 38

Полученный кадр вначале классифицируется на принадлежность к той или иной сети VLAN следующим образом: если полученный кадр содержит тэг VLAN, то он используется для классификации; в противном случае кадр классифицируется на основе параметра PVID порта. После классификации кадр может пройти через входную фильтрацию (если она включена), где кадр будет отброшен, если его VLAN ID не найден в списке сетей VLAN, к которым принадлежит входной порт. Далее принимается решение по пересылке (forwarding decision) на основе VLAN ID и MAC-адреса назначения. Наконец, выходные правила определяют, должен ли кадр быть отправлен с тэгом или без него.

Администратор может создавать/удалять в системе сети VLAN (кроме «Сети по умолчанию» Default VLAN, которая существует всегда). Каждый порт в VLAN может быть настроен как имеющий тэг (Tagged) и не имеющий его (Untagged), запрещенный и исключенный (не член VLAN). За исключением default VLAN, администратор может настроить установку и снятие тэга (Tagged/Untagged) на выходном порту.

10.2. Команды для работы с сетями VLAN

Перед началом создания виртуальных частных сетей необходимо задать **bridge 1**, а также указать протокол предотвращения петель для данного коммутатора.

Синтаксис:

bridge 1 protocol [**ieee vlan-bridge** | **rstp vlan-bridge** | **mstp**]

Параметры:

– **ieee vlan-bridge** – работа коммутатора в режиме STP;

– **rstp vlan-bridge** – работа коммутатора в режиме RSTP;

– **mstp** – работа коммутатора в режиме MSTP.

Режим ИКС – режим общего конфигурирования.

Подробное описание **bridge** см. в разделе 11.

10.2.1. Создание VLAN

10.2.1.1. Команда **vlan**

Используется для создания новой сети VLAN. Использование префикса «**no**» удаляет выбранную или все существующие сети VLAN.

Примечание. Для входа в режим конфигурирования VLAN необходимо ввести команду **vlan database** .

Синтаксис команды:

vlan *vlan-range* **bridge 1**

или

no vlan *vlan-range* **bridge 1**

Параметр команды – *vlan-range* – список номеров создаваемых сетей VLAN (в диапазоне от 2 до 4094). Номера могут быть перечислены через запятую; если используются несколько номеров подряд, то их можно задать в виде диапазона через дефис.

Режим ИКС – режим конфигурации VLAN.

10.2.2. Конфигурирование VLAN

10.2.2.1. Команда **interface vlan.***vlan-id*

Используется для вхождения в режим конфигурирования выбранной сети VLAN и настройки ее параметров.

Синтаксис команды:

interface vlan 1.*vlan-id*

Параметр команды – *vlan-id* – номер конфигурируемой сети VLAN.

Режим ИКС – режим общего конфигурирования.

10.2.2.2. Команда **show vlan**

Отображает информацию о выбранной сети или обо всех сетях VLAN.

Синтаксис команды:

show vlan [*vlan-id* | **brief**]

Параметры команды:

– *vlan-id* – номер сети VLAN;

– `brief` – отображение всех VLAN созданных в системе.

Режим ИКС – режим управления.

10.3. Настройка параметров физических интерфейсов

10.3.1. Изменение режимов физических интерфейсов

10.3.1.1. Команда **switchport**

Предназначена для перевода интерфейса в режим Layer 2, модели OSI, и обратно в режим Layer 3.

Синтаксис команды:

switchport

или

no switchport

Состояние по умолчанию – режим работы портов не задан.

Режим ИКС – режим конфигурации интерфейса (Ethernet, Port Channel).

Примечания:

1. Для перевода интерфейса в режим Layer 3 применяется команда **no switchport**.
2. После выполнения команды **switchport** необходимо указать принадлежность интерфейса к заранее созданному bridge, для этого используется команда **bridge-group 1**.

10.3.1.2. Команда **switchport mode**

Предназначена для перевода порта в режим членства в VLAN (access, trunk) Использование префикса «**no**» устанавливает значения по умолчанию.

Синтаксис команды:

switchport mode { access | trunk**}**

Параметры команды:

– access – не тегированный порт 2 уровня;

– trunk – магистральный порт 2 уровня.

10.3.2. Назначение/удаление портов

10.3.2.1. Команда **switchport access vlan**

Предназначена для назначения порта к указанному VLAN. Интерфейс в режиме *access* может принадлежать только одному VLAN. Использование префикса «**no**» устанавливает значения по умолчанию.

Синтаксис команды:

switchport access vlan v*lan-id*

или

no switchport access vlan

Параметр команды – *vlan-id* - идентификатор VLAN, значение которого принадлежит диапазону от 2 до 4094.

Режим ИКС – режим конфигурации интерфейса (Ethernet, Port Channel).

10.3.2.2. Команда **switchport trunk allowed vlan**

Предназначена для добавления/удаления VLAN к магистральному порту. Магистральный порт может быть членом не тегированного VLAN, и одновременно членом одной или нескольких тегированных VLAN.

Синтаксис команды:

switchport trunk allowed vlan { **all** | **add** *vlan-list* | **remove** *vlan-list* | **except** *vlan-list* | **none** }

Параметры команды:

– *vlan-list* – список идентификаторов VLAN. Одиночные идентификаторы разделяются запятой без пробела. Граничные значения диапазона идентификаторов отделяются дефисом;

– **all** – задает все VLAN. В любой момент порт принадлежит всем VLAN, существующим на данный момент (в диапазоне от 1 до 4094);

– **add** – добавляет список VLAN к порту;

– **remove** – удаляет список VLAN из порта;

– **except** – указывает, что порт принадлежит всем VLAN, за исключением тех, что указаны в списке;

– **none** – запрещает все VLAN, порт не принадлежит ни одному из VLAN.

Состояние по умолчанию – магистральный порт принадлежит ко всем созданным VLAN.

Режим ИКС – Режим конфигурации интерфейса (Ethernet, Port Channel).

11. НАСТРОЙКА ПРОТОКОЛА SPANNING TREE

11.1. Поддержка протокола Spanning Tree

Протокол Spanning Tree (STP, протокол остовного дерева) защищает широковещательный домен от петель и штормов пакетов, которые могут образоваться в результате выборочного включения интерфейсов в режим ожидания, в котором они не передают пользовательские данные, но автоматически повторно активируются при изменении топологии. Коммутаторы периодически обмениваются конфигурационными сообщениями, используя специально отформатированные кадры, называемые BPDU, и выборочно включают и отключают передачу трафика на портах.

Система поддерживает три типа STP протоколов:

- Spanning Tree protocol (IEEE802.1D – классический SPT);
- Rapid Spanning Tree Protocol (IEEE802.1w – RSTP);
- Multiple Spanning Tree Protocol (IEEE802.1s – MSTP).

По умолчанию протокол не задан. Поддерживается возможность фильтрации BPDU или отключения STP на указанных портах.

11.2. Команды для настройки протокола STP

Перед началом настройки коммутации необходимо задать в системе **bridge 1**, а также указать тип протокола остовного дерева.

Синтаксис:

bridge 1 protocol [**ieee vlan-bridge** | **rstp vlan-bridge** | **mstp**]

Для изменения типа протокола необходимо повторно ввести команду с указанием нового типа.

Параметры:

- **ieee vlan-bridge** – работа коммутатора в режиме STP;
- **rstp vlan-bridge** – работа коммутатора в режиме RSTP;
- **mstp** – работа коммутатора в режиме MSTP.

Состояние по умолчанию – протокол STP не задан.

Режим ИКС – режим общего конфигурирования.

11.2.1. Приоритеты/«стоимость» устройств

11.2.1.1. Команда **bridge 1 priority**

Определяет приоритет устройства, используемый для выбора корневого коммутатора. Использование префикса «**no**» восстановит установки по умолчанию.

Синтаксис команды:

bridge 1 priority *priority*

или

no bridge 1 priority

Параметр команды – *priority* – значение приоритета коммутатора (диапазон от 0 до 61440 с шагом в 4096).

Состояние по умолчанию – 32768.

Режим ИКС – режим общего конфигурирования.

Примечание. Коммутатор с наименьшим значением приоритета становится корневым. Если больше чем один коммутатор имеет наименьшее значение приоритета – коммутатор с наименьшим MAC адресом становится корневым.

11.2.1.2. Команда **bridge-group 1 path-cost**

Определяет «стоимость» STP пути на интерфейсе. Использование префикса «**no**» восстановит установки по умолчанию.

Синтаксис команды:

bridge-group 1 path-cost *cost*

или

no bridge-group 1 path-cost *cost*

Параметр команды – *cost* – значение стоимости пути интерфейса (диапазон от 1 до 200000000).

Состояние по умолчанию – значение «стоимости» пути по умолчанию зависит от скорости интерфейса и метода определения стоимости (быстрый или медленный) см. таблицу 8.

Таблица 8

Интерфейс	RSTP	STP
Port-channel (10 Gbps)	1000	1
TenGigabit Ethernet (10 Gbps)	2000	2
Gigibit Ethernet (1 Gbps)	20000	4
Ethernet (10 Mbps)	2000000	19

Режим ИКС – режимы настройки интерфейса.

11.2.1.3. Команда **bridge-group 1 priority**

Определяет стоимость STP пути на интерфейсе. Использование префикса «**no**» восстановит установки по умолчанию.

Синтаксис команды:

bridge-group 1 priority *priority*

или

no bridge-group 1 priority

Параметр команды – *priority* – значение приоритета интерфейса (диапазон от 1 до 240 с шагом в 16).

Состояние по умолчанию – 128.

Режим ИКС – режимы настройки интерфейса.

11.2.2. Изменение режимов устройств

11.2.2.1. Команда **spanning-tree portfast**

Включает режим portfast на интерфейсе. В режиме portfast интерфейс немедленно переходит в состояние передачи, используется на портах уровня доступа. Использование префикса «**no**» выключает режим portfast на интерфейсе.

Синтаксис команды:

spanning-tree portfast

или

no spanning-tree portfast

Состояние по умолчанию – режим portfast выключен.

Режим ИКС – режимы настройки интерфейса.

11.2.2.2. Команда **spanning-tree bpdu-guard**

Переводит порт в состояние errdisable в случае получения BPDU сообщения. Использование префикса «**no**» восстановит установки по умолчанию.

Синтаксис команды:

spanning-tree bpdu-guard {**enable** | **disable** | **default**}

или

no spanning-tree bpdu-guard

Параметры команды:

– *enable* – включить функцию BPDU-guard;

– *disable* – выключить функцию BPDU-guard;

– *default* – использовать значение по умолчанию.

Состояние по умолчанию – режим bpdu-guard выключен.

Режим ИКС – режимы настройки интерфейса.

11.2.2.3. Команда **spanning-tree bpdu-filter**

Включает режим, при котором на порту не принимаются и не отправляются BPDU сообщения. Использование префикса «**no**» восстановит установки по умолчанию.

Синтаксис команды:

spanning-tree bpdu-filter {**enable** | **disable** | **default**}

или

no spanning-tree bpdu-filter

Параметры команды:

– *enable* – включить функцию BPDU-filter;

– *disable* – выключить функцию BPDU-filter;

– default – использовать значение по умолчанию

Состояние по умолчанию – режим bpdu-filter выключен.

Режим ИКС – режимы настройки интерфейса.

11.2.2.4. Команда **spanning-tree guard root**

Включает режим, при котором на порту запрещено получение superior BPDU сообщения, в случае получения такого сообщения порт переводится в состояние err-disabled. Использование префикса «**no**» восстановит установки по умолчанию.

Синтаксис команды:

spanning-tree guard root

или

no spanning-tree guard root

Состояние по умолчанию – режим guar root выключен.

Режим ИКС – режимы настройки интерфейса.

Примечание. В случае, если интерфейс находится в состоянии errdisable, необходимо устранить причину вызвавшую данное состояние, после чего провести деактивацию и повторную активацию данного интерфейса командами **shutdown/no shutdown** из режима настройки интерфейса.

11.2.2.5. Команда **bridge spanning-tree portfast**

Включает режим portfast с функцией BPDU-guard или BPDU-filter на коммутаторе. Использование префикса «**no**» отключает функцию BPDU-filter (или BPDU-guard).

Синтаксис команды:

```
bridge 1 spanning-tree portfast { bpdu-filter | bpdu-guard }
```

или

```
no bridge 1 spanning-tree portfast { bpdu-filter | bpdu-guard }
```

Параметры команды:

– **bpdu-filter** – задает функцию BPDU-filter на портах с поддержкой portfast;

– **bpdu-guard** – указать, чтобы защитить порты portfast от приема BPDU.

Состояние по умолчанию – режим portfast для STP отключен.

Режим ИКС – режим общего конфигурирования.

Примечание. На порту в режиме portfast с включенной функцией BPDU-filter при приеме сообщений BPDU интерфейс теряет свой текущий режим и повторно включает протокол остовного дерева. Следовательно, STP удаляется из интерфейса, что является ожидаемым поведением.

12. НАСТРОЙКА IP-АДРЕСАЦИИ И МАРШРУТИЗАЦИИ

IP-маршрутизация, то есть обработка и передача данных на втором уровне сетевой модели OSI, является одним из базовых сетевых сервисов системы. Для этого в ней реализована поддержка протоколов ARP, DNS, DHCP для сетей IP VLAN. Имеется возможность ввода статических маршрутов и внесение записей в таблицу соответствий ARP.

Коммутатор может функционировать в следующих двух режимах обработки и передачи данных:

– режим моста (Bridging Mode). При этом для пересылки пакетов используется адресная информация второго уровня сетевой модели OSI (L2 Forwarding);

– режим маршрутизации (Routing Mode). При этом для пересылки пакетов используется адресная информация третьего уровня сетевой модели OSI (L3 Forwarding).

Примечание. Описание всех настроек и команд приведено для случая использования IP-адресов формата IPv4.

12.1. Использование статической и динамической IP-адресации

Примечания:

1. Если IP-адрес настраивается для интерфейса физического порта или группы агрегированных портов, то этот интерфейс удаляется из сети VLAN, которой ранее принадлежал.

2. Команда назначает IP-адрес интерфейсу, которым может быть физический порт, агрегированный канал или VLAN. Использование префикса «**no**» удаляет назначенный ранее интерфейсу IP-адрес.

3. Перед назначением IP-адресов физическому или логическому интерфейсу необходимо использовать команду **no switchport** в режиме конфигурации интерфейса.

12.2. Команды работы со статической и динамической IP-адресацией

12.2.1. Команды работы со статической IP-адресацией

12.2.1.1. Команда **ip address**

Синтаксис команды:

ip address *ip-address mask*

Параметр команды – *ip-address mask* – IP-адрес назначения и маска подсети в формате *A.B.C.D A.B.C.D* или *A.B.C.D*/*M*.

Состояние по умолчанию – интерфейсам IP-адреса не назначены.

Режим ИКС – режимы конфигурирования интерфейса (Ethernet, Port-channel, VLAN).

Команда не может быть применена к группе интерфейсов.

Примечания:

1. Назначение интерфейсу статического IP-адреса автоматически отключает на нем DHCP-клиент.

2. Назначаемые отдельным интерфейсам IP-адреса должны принадлежать различным подсетям. Если коммутатор работает в режиме моста, то назначаемый ему единый IP-адрес привязывается к порту, через который в текущий момент разрешено управление системой.

12.2.1.2. Команда **ip address dhcp**

Используется для получения IP-адреса для настраиваемого интерфейса от DHCP-сервера. Использование префикса «**no**» отключает динамическое присваивание интерфейсу IP-адреса и освобождает этот адрес. Интерфейсом может быть физический порт, агрегированный канал или VLAN.

Синтаксис команды:

ip address dhcp

или

no ip address dhcp

Режим ИКС – режимы конфигурирования интерфейса (Ethernet, Port-channel, VLAN).

Команда не может быть применена к группе интерфейсов.

Примечание. Включение на интерфейсе DHCP-клиента автоматически удаляет назначенный ему статический IP-адрес.

12.2.1.3. Команда **ip route 0.0.0.0/0**

Устанавливает для коммутатора шлюз по умолчанию. Использование префикса «**no**» удаляет шлюз по умолчанию.

Синтаксис команды:

ip route 0.0.0.0/0 *ip-address*

или

no ip route 0.0.0.0/0

Параметр команды – *ip-address* – IP-адрес шлюза по умолчанию.

Режим ИКС – режим общего конфигурирования.

Состояние по умолчанию – шлюз по умолчанию не установлен.

12.2.2. Просмотр состояния IP-адресации

12.2.2.1. Команда **show ip interface**

Отображает текущую конфигурацию IP-адресации для всех интерфейсов или для указанного интерфейса.

Синтаксис команды:

show ip interface [*interface-id*] **brief** [**secondary**]

Параметры команды:

– **brief** - краткое описание статуса и конфигурации IP;

– *interface-id* – номер интерфейса (порт, агрегированный канал, VLAN);

– **secondary** – информация о вторичных IP-адресах.

Режим ИКС – режим управления.

12.2.3. Использование протокола DNS для трансляции адресов, команды, использующиеся для настройки работы с использованием протокола DNS

В системе реализована поддержка протокола DNS, использующегося для определения IP-адреса сетевого устройства по его доменному имени и обратно. Коммутатор является полнофункциональным DNS-клиентом, поддерживающим до восьми DNS-серверов с базами данных соответствий доменных имен узлов сети и их IP-адресов. При этом один из таких серверов назначается «первичным» (primary), и к нему система обращается в первую очередь. Кроме того, администратор может статически прописать до 64 записей таких соответствий непосредственно на самом устройстве.

12.2.3.1. Команда **ip domain-lookup**

Включает трансляцию доменных имен сетевых устройств в их IP-адреса с использованием протокола DNS. Использование префикса «**no**» отключает трансляцию адресов.

Синтаксис команды:

ip domain-lookup

или

no ip domain-lookup

Состояние по умолчанию – поддержка DNS в системе включена.

Режим ИКС – режим общего конфигурирования.

12.2.3.2. Команда **ip domain-name**

Определяет доменное имя по умолчанию, которое будет использоваться программой для дополнения неполных доменных имен (доменных имен без точки). Для доменных имен без точки в конец имени будет добавляться точка и указанное в команде выражение. Использование префикса «**no**» удаляет доменное имя по умолчанию.

Синтаксис команды:

ip domain-name *name*

или

no ip domain-name

Параметр команды – *name* – доменное имя по умолчанию (диапазон от 1 до 158 символов).

Состояние по умолчанию – доменное имя по умолчанию не задано.

Режим ИКС – режим общего конфигурирования.

Примечание. При вводе доменного имени по умолчанию необходимо использовать только символы ASCII - буквы A-Z (заглавные), цифры 0-9, символ подчеркивания («_») и дефис («-»). Точка используется для разделения слов.

12.2.3.3. Команда **ip name-server**

Определяет IPv4/IPv6-адреса для доступных DNS-серверов. Использование префикса «**no**» удаляет IP-адрес DNS-сервера из списка доступных.

Синтаксис команды:

ip name-server {*server1-address*} [*server2-address*] [*server3-address*]

или

no ip name-server {*server1-address*} [*server2-address*] [*server3-address*]

Параметр команды – *server-address* – IPv4/IPv6-адрес DNS-сервера, можно задать до трех серверов.

Состояние по умолчанию – DNS-сервера не заданы.

Режим ИКС – режим общего конфигурирования.

Примечание. Приоритет использования DNS-серверов определяется порядком их следования в команде. Сервера могут быть также заданы несколькими отдельными командами.

12.2.3.4. Команда **ip host**

Определяет статические соответствия имен узлов сети IP-адресам и добавляет установленное соответствие в кэш-память коммутатора. Использование префикса «**no**» удаляет статическое соответствие.

Синтаксис команды:

ip host *name address* [*address2*]

или

no ip host *name*

Параметры команды:

– *name* – доменное имя (от 1 до 158 символов);

– *address* – ассоциированный с доменным именем IP-адрес. К одному доменному имени можно привязать до двух IP-адресов.

Состояние по умолчанию – статические соответствия не заданы.

Режим ИКС – режим общего конфигурирования.

Примечание. При вводе доменного имени по умолчанию необходимо использовать только символы ASCII - буквы A-Z (заглавные), цифры 0-9, символ подчеркивания («_») и дефис («-»). Точка используется для разделения слов.

12.2.3.5. Команда **show hosts**

Показывает список DNS-серверов и статические соответствия имен узлов сети и IP-адресов, доменное имя по умолчанию.

Режим ИКС – режим управления.

12.3. Настройка IP-маршрутизации

Коммутатор поддерживает работу системы в режиме маршрутизации проходящего трафика. При этом IP-маршруты можно прописать в таблице маршрутизации статически.

12.3.1. Команды для настройки IP-маршрутизации проходящего трафика

12.3.1.1. Команда **ip route**

Создает статическое правило маршрутизации. Использование префикса «**no**» удаляет статическое правило из таблицы маршрутизации.

Синтаксис команды:

ip route *prefix mask gateway* [*distance* | **tag** *tag_value* | **description** *description*]

или

no ip route *prefix* ***mask*** *gateway* [*distance* | **tag** *tag_value* | **description** *description*]

Параметры команды:

– *prefix mask*– IP-адрес и маска сети назначения в формате *A.B.C.D A.B.C.D или A.B.C.D/M*;

– *gateway* – IP-адрес шлюза для доступа к сети назначения;

– *distance* – «вес» маршрута (диапазон от 1 до 255);

– **tag** - тег, используемый как значение «соответствия» для управления перераспределением через карты маршрутов;

– **description** - описание маршрута (максимум 80 знаков).

Состояние по умолчанию – «вес» маршрута по умолчанию равен 1.

Режим ИКС – режим общего конфигурирования.

12.3.1.2. Команда **show ip route**

Отображает текущее состояние таблицы маршрутизации или отдельных записей из нее.

Синтаксис команды:

show ip route [**all** | **database**| **interface** *ifname*| **next-hop** *nh_address*| **summary** | **connected** | **static** | *ip-address* | *ip-prefix*]

Параметры команды:

– **connected** – отображает только подключенные к интерфейсам и функционирующие маршруты;

– **all** – отображает все маршруты;

– **database** – отображает все маршруты, в том числе и неактивные;

– **interface** – отображает только маршруты доступные через определенный интерфейс;

– **next-hop** – отображает только маршруты доступные через заданный IP;

– **summary** – отображает суммарное количество маршрутов;

– **static** – отображает только статически прописанные маршруты;

– *ip-address* – отображает маршрут только до указанного IP-адреса;

– *ip-prefix* – отображает маршрут только до указанного IP-адреса с указанием маски подсети в двоичном представлении (диапазон от 0 до 32).

Режим ИКС – режим управления.

13. НАСТРОЙКА СПИСКОВ КОНТРОЛЯ ДОСТУПА

Правила контроля доступа, проходящего через коммутатор, реализованы на основе применения списков контроля доступа (Access Control List - ACL) к интерфейсам устройства. Данные списки позволяют фильтровать проходящие пакеты по IP-адресу или MAC-адресу отправителя и получателя, типу протокола, параметрам портов и других характеристикам.

Списки контроля доступа ACL применяются к отдельным интерфейсам и обрабатывают входящий трафик. Система в целом поддерживает до 2048 списков ACL. При этом каждый список ACL может состоять из одного или несколько правил доступа (Access Control Element - ACE). Если список ACL состоит из нескольких правил доступа ACE, то проверка пакета начинается последовательно по этим правилам до первого совпадения, после чего проверка на соответствие остальным правилам не производится. Поэтому порядок следования правил в списке ACL имеет большое значение.

В случае соответствия пакета какому-либо правилу производится указанное в этом правиле действие над пакетом – пересылка по адресу назначения, отбрасывание и т.д. Один и тот же список ACL можно применить к нескольким интерфейсам. Списки ACL можно применять к физическим портам, логическим интерфейсам либо агрегированным каналам.

При создании списков ACL следует учитывать следующие ограничения:

– списки ACL на базе IPv6, IPv4 и MAC-адресов не должны иметь одинаковые названия;

– списки ACL на базе IPv4 и IPv6 и MAC могут работать вместе на одном физическом интерфейсе;

– два списка одинакового типа не могут быть применены к одному и тому же интерфейсу.

13.1. Настройка простых списков доступа ACL

13.1.1. Создание простых списков доступа ACL

13.1.1.1. Команда **access-list**

Используется для создания нового списка контроля доступа или для редактирования существующего списка с указанным названием. Использование префикса «**no**» удаляет существующий список контроля доступа с указанным названием.

Синтаксис команды:

access-list {*acl-number* | *access-list-name*} {***permit*** | ***deny***} { *network wildcard* | ***any*** | ***host*** *address*}

или

no access-list {*acl-number* | *access-list-name*}

Параметры команды:

- *acl-number* - номер списка доступа. Для создания простого списка доступа используются значения в диапазонах от 1 до 99 и от 1300 до 1999;
- *access-list-name* именное название простого списка доступа;
- *permit* – создание разрешающего правила;
- *deny* – создание запрещающего правила;
- *network* – адрес сети;
- *wildcard* - обратная маска IP-сети;
- *address* – IP адрес конкретного устройства в сети;
- *any* – использование IP адреса `0.0.0.0 255.255.255.255`.

Состояние по умолчанию – списков на основе IP не существует.

Режим ИКС – режим общего конфигурирования.

13.2. Настройка расширенных списков ACL на базе IP

В подразделе описаны команды для создания, удаления и редактирования расширенных списков контроля доступа ACL на базе IP-адресов отправителя и получателя фильтруемого трафика. Для создания расширенного списка доступа используются значения номера списка доступа в диапазонах от 100 до 199 и от 2000 до 2699.

Примечания:

1. Описание всех настроек и команд приведено для случая использования IP-адресов формата IPv4. Вместе с тем в системе реализована полнофункциональная поддержка списков ACL на базе IPv6.При этом в синтаксисе или параметрах соответствующих команд, как правило, достаточно заменить **ip** на **ipv6**.

2. Для создания списка ACL на базе IPv6 необходимо использовать команду **ipv6 access-list** режима общей настройки.

13.2.1. Создание расширенных списков доступа ACL

13.2.1.1. Команда **access-list**

Используется для создания нового списка контроля доступа или для редактирования существующего списка с указанным названием. Использование префикса «**no**» удаляет существующий список контроля доступа с указанным названием.

Синтаксис команды:

access-list *acl-number* {**permit | deny**} *protocol* {**any** | *source source-wildcard* | ***host*** *src-host* } {**any** | *destination destination-wildcard* | ***host*** *dst-host*} [**dscp** *number* | **fragments** fragments *number* | **precedence** *number*]

Для протоколов ICMP, IGMP, а также групп протоколов TCP и UDP данная команда имеет специальный синтаксис:

access-list *acl-number* {**permit | deny**} **icmp** {**any** | *source source-wildcard* | ***host*** *src-host* } {**any** | *destination destination-wildcard* | ***host*** *dst-host* } [*icmp-type*] [*icmp-code* | **dscp** *number* | **precedence** *number* | **fragments**]

или

access-list *acl-number* {**permit deny**} **igmp** {**any** | *source source-wildcard* | ***host*** *src-host* } {**any** | *destination destination-wildcard* | ***host*** *dst-host* } [**dscp** *number* | **precedence** *number* | **fragments**]

или

access-list *acl-number* {**permit | deny**} **tcp** {**any** | *source source-wildcard* | ***host*** *src-host*} {**any** | ***eq*** *src-port* | ***gt*** *src-port* | ***lt*** *src-port* | ***neq*** *src-port* | **range** port-range} {**any** | *destination destination-wildcard* | ***host*** *dst-host* } [**eq** *dst-port* | **gt** *dst-port* | **lt** *dst-port* | **neq** *dst-port* | **range** port-range] [**dscp** *number* | **precedence** *number*] [*list-of-flags*]

или

access-list *acl-number* {**permit|deny**} **udp** {**any** | *source source-wildcard* | ***host*** *src-host* } {**any** | ***eq*** *src-port* | ***gt*** *src-port* | ***lt*** *src-port* | ***neq*** *src-port* | **range** port-range} {**any** | *destination destination-wildcard* | ***host*** *dst-host* } [***eq*** *dst-port* | ***gt*** *dst-port* | ***lt*** *dst-port* | ***neq*** *dst-port* | **range** port-range] [**dscp** *number* | **precedence** *number*]

Параметры команды:

– *protocol* – название или номер IP-протокола. Доступные названия протоколов – ***ahp***, ***any***, ***eigrp***, ***esp***, ***ethertype***, ***gre***, ***icmp***, ***igmp***, ***ip***, ***ipcomp***, ***mac***, ***nos***, ***pim***, ***rsvp***, ***tcp***, ***udp***, ***vrrp***;

– *source* – IP-адрес отправителя пакета;

– *source-wildcard* – битовая маска, применяемая к IP-адресу отправителя пакета. Маска определяет биты IP-адреса, которые необходимо игнорировать. В значения игнорируемых битов должны быть записаны единицы;

– *destination* – IP-адрес получателя пакета;

– *destination-wildcard* – битовая маска, применяемая к IP-адресу получателя пакета;

– *dscp number* – значение DSCP-поля diffserv в заголовке пакета. Возможные коды сообщений поля dscp (диапазон от 0 до 63);

– *precedence number* – значение приоритета IP-трафика (диапазон от 0 до 7);

– *eq* – используется для указания конкретного TCP/UDP порта;

– gt - используется для указания всех портов больше заданного значения;

– lt - используется для указания всех портов меньше заданного значения;

– neq - используется для указания исключения заданного значения;

– *icmp-type* – тип сообщений протокола ICMP, используемый для фильтрации ICMP-пакетов. Необходимо ввести номер типа (диапазон от 0 до 255) или одно из следующих значений:

1) icmp-type;
2) administratively-prohibited;
3) prohibited;
4) alternate-address;
5) conversion-error;
6) dod-host-prohibited;
7) dod-net-prohibited;
8) dscp;
9) echo;
10) echo-reply;
11) fragments;
12) general-parameter-problem;
13) host-isolated;
14) host-precedence-unreachable;
15) host-redirect;
16) host-tos-redirect;
17) host-tos-unreachable;
18) host-unknown;
19) host-unreachable;
20) information-reply;
21) information-request;
22) mask-reply;
23) mask-request;
24) mobile-redirect;
25) net-redirect;
26) net-tos-redirect;
27) net-tos-unreachable;
28) net-unreachable;
29) network-unknown;
30) no-room-for-option;
31) option-missing;
32) packet-too-big;
33) parameter-problem;

34) port-unreachable;

35) precedence;

36) precedence-unreachable;

37) protocol-unreachable;

38) reassembly-timeout;

39) redirect router-advertisement;

40) advertisements;

41) router-solicitation;

42) solicitations;

43) source-quench;

44) source-route-failed;

45) time-exceeded;

46) timestamp-reply;

47) timestamp-request;

48) traceroute;

49) ttl-exceeded;

50) unreachable;

– *icmp-code* – код сообщений протокола ICMP, используемый для фильтрации ICMP-пакетов (диапазон от 0 до 255);

– *igmp-type* – тип сообщений протокола IGMP, используемый для фильтрации IGMP-пакетов (диапазон от 0 до 255). Необходимо ввести номер типа (диапазон от 0 до 255) или одно из следующих значений:

1) host-query;

2) host-report;

3) dvmrp;

4) pim;

5) cisco-trace;

6) host-report-v2;

7) host-leave-v2;

8) host-report-v3;

– *src-port* – UDP/TCP-порт отправителя. Необходимо указать номер порта (диапазон от 0 до 65535) или одно из следующих значений (текстовых или числовых):

1) для TCP - *chargen* (*19*), *daytime* (*13*), *discard* (*9*), *domain* (*53*), *echo* (*7*), *finger* (*79*), *ftp* (*21*), *ftp-data* (*20*), *gopher* (*70*), *hostname* (*42*), *irc* (*194*), *klogin* (*543*), *kshell* (*544*), *lpd* (*515*), *nntp* (*119*), *pop2* (*109*), *pop3* (*110*), *smtp* (*25*), *sunrpc* (*1110*), *syslog* (*514*), *tacacs-ds* (*49*), *talk* (*517*), *telnet* (*23*), *time* (*37*), *uucp* (*117*), *whois* (*43*), *www* (*80*);

2) для UDP - *biff* (*512*), *bootpc* (*68*), *bootps* (*67*), *discard* (9), *dnsix* (*90*), *domain* (*53*), *echo* (*7*), *mobile-ip* (*434*), *nameserver* (*42*), *netbios-dgm* (*138*), *netbios-ns* (*137*), *on500-isakmp* (*4500*), *ntp* (*123*), *snmp* (*161*), *snmptrap* (*162*), *sunrpc* (*111*), *syslog* (*514*), *tacacs-ds* (*49*), *talk* (*517*), *tftp* (*69*), *time* (*37*), *who* (*513*), *xdmcp* (*177*). Можно указать диапазон портов через дефис;

– *dst-port* – UDP/TCP-порт назначения. Параметры аналогичны *src-port*;

– *list-of-flags* – список флагов протокола TCP. Если для условия фильтрации флаг должен быть установлен, то перед ним ставится знак «**+**», если не должен быть установлен, то «**-**». Возможные варианты флагов - *urg*, *ack*, *psh*, *rst*, *syn*, *fin*, *urg*, *ack*, *psh*, *rst*, *syn* и *fin*. При использовании нескольких флагов в условии фильтрации, флаги объединяются в одну строку и записываются через пробел;

– `fragments` – проверка не исходных фрагментов;

– `port-range` – диапазон номеров портов от 0 до 65535.

Состояние по умолчанию – весь трафик разрешен.

Режим ИКС – общий режим конфигурирования.

После включения первого правила доступа ACE в список контроля доступа ACL в его конец в неявном виде автоматически добавляется запрещающее правило на весь остальной трафик, не соответствующий данному правилу **`permit`**. Это означает, что, если в списке не окажется ни одного правила, которому пакет будет соответствовать, то такой пакет будет запрещен к дальнейшей пересылке. До тех пор, пока в список не включено ни одного запрещающего или разрешающего правила, все пакеты считаются разрешенными.

13.3. Настройка списков ACL на базе MAC

13.3.1. Команды для работы со списками ACL на базе MAC-адресов

13.3.1.1. Команда **access-list**

Используется для создания нового списка контроля доступа на основе MAC-адресов или для редактирования существующего списка с указанным названием. Использование префикса «**no**» удаляет существующий список контроля доступа с указанным названием.

Синтаксис команды:

access-list *acl-number* **{permit | deny} mac**

или

no access-list *acl-number*

Параметр команды – *acl-number* – номер расширенного списка доступа, возможные значения в диапазонах от 100 до 199 и от 2000 до2699.

Состояние по умолчанию – списков на основе MAC не существует.

Режим ИКС – режим общего конфигурирования.

13.3.2. Создания правил фильтрации

13.3.2.1. Команда **permit(MAC)**

Используется для создания разрешающего правила фильтрации в списке контроля доступа ACL на базе MAC.

13.3.2.2. Команда **deny(MAC)**

Используется для создания разрешающего/запрещающего правила фильтрации в списке контроля доступа ACL на базе MAC.

Синтаксис команды:

access-list *acl-number* {**permit | deny**} **mac** {**any** | **host** *source* | source *source-wildcard*} {**any** | **host** *destination* | *destination destination-wildcard*} [*eth-type* | *IPv4 Ethertype* | *IPv6 Ethertype*]

Параметры команды:

– *source* – MAC-адрес отправителя пакета. Возможно указание адреса в следующих форматах:

1) XX-XX-XX-XX-XX-XX;
2) XX:XX:XX:XX:XX:XX;
3) XXXX.XXXX.XXXX;

– *source-wildcard* – маска, применяемая к MAC-адресу отправителя пакета для определения битов адреса, которые необходимо игнорировать. В значения игнорируемых битов должны быть записаны единицы. Например, для адресов 00:00:02:AA.xx.xx необходимо задать значение маски 00:00:00:00:FF:FF, формат маски аналогичен формату адреса источника;

– *destination* – MAC-адрес получателя пакета;

– *destination-wildcard* – маска, применяемая к MAC-адресу получателя пакета;

– *eth-type* – Ethernet-тип фильтруемых пакетов в шестнадцатеричной записи (диапазон от 0 до 0xFFFF);

– *IPv4 Ethertype* 0x0800;

– *IPv6 Ethertype* 0MIPSdd;

Состояние по умолчанию – весь трафик разрешен.

Режим ИКС – режим общего конфигурирования.

После включения первого правила доступа ACE в список контроля доступа ACL в его конец в неявном виде автоматически добавляется запрещающее правило на весь остальной трафик, не соответствующий данному правилу **permit**. Это означает, что, если в списке не окажется ни одного правила, которому пакет будет соответствовать, то такой пакет будет запрещен к дальнейшей пересылке. До тех пор, пока в список не включено ни одного запрещающего или разрешающего правила, все пакеты считаются разрешенными.

13.4. Применение списков ACL и установка временных параметров

13.4.1. Команды для работы со списками контроля доступа ACL на базе IP-адресов

13.4.1.1. Команда **ip access-group**

Применяет указанный список контроля доступа на основе IPv4 и IPv6 к физическому интерфейсу. Использование префикса «**no**» удаляет список контроля доступа с физического интерфейса.

Синтаксис команды:

ip access-group {*acl-number* | *access-list-name*} [in | out]

или

no ip access-group {*acl-number* | *access-list-name*} [in | out]

Параметры команды:

– *access-list-name* – название применяемого списка контроля доступа ACL;

– *acl-number* - номер списка доступа;

– in – применение списка доступа для входящих пакетов;

– out - применение списка доступа для исходящих пакетов.

Состояние по умолчанию – к интерфейсам списки ACL не применены.

Режим ИКС – режимы конфигурирования интерфейса (Ethernet, VLAN, Port-channel).

13.4.1.2. Команда **mac access-group**

Применяет указанный список контроля доступа на основе MAC-адресов к физическому интерфейсу. Использование префикса «**no**» удаляет список контроля доступа с физического интерфейса.

Синтаксис команды:

mac access-group {*acl-number* | *access-list-name*} in

или

no mac access-group {*acl-number* | *access-list-name*}

Параметры команды:

– *access-list-name* – название применяемого списка контроля доступа ACL;

– *acl-number* - номер списка доступа;

– in – применение списка доступа для входящих пакетов.

Состояние по умолчанию – к интерфейсам списки ACL не применены.

Режим ИКС – режимы конфигурирования интерфейса (Ethernet, VLAN, Port-channel).

Примечания:

1. Списки ACL на базе IPv4 и IPv6 и MAC могут работать вместе на одном физическом интерфейсе.

2. Два списка одинакового типа не могут быть применены к одному и тому же интерфейсу.

3. К интерфейсу, к которому уже применен список ACL, нельзя добавить другой список ACL. В случае применения нового списка ACL старый будет автоматически удален.

13.4.2. Просмотр списков контроля доступа

13.4.2.1. Команда **show access-lists**

Отображает все списки контроля доступа, существующие в системе.

Синтаксис:

show access-lists

Режим ИКС – режим управления.

Команда **clear access-lists counters** обнуляет все счетчики списков ACL.

Синтаксис команды:

clear access-lists counters [*acl-name*]

Параметр команды – *acl-name* – идентификатор списка ACL.

Режим ИКС – режим управления.

14. НАСТРОЙКА ПРОТОКОЛА SNMP

Система управляется с помощью комбинации базы данных MIB (Management Information Base) переменных, чьи комбинации значений представляют все аспекты состояния системы, и протокола SNMP, предназначенного для изучения и изменения этих значений.

SNMP является базовым объектом системы. Все функции и также опции ее конфигурации отражаются в переменной MIB или во многих переменных. Существуют обширные стандарты, охватывающие различные аспекты, касающиеся организации базы MIB, ее функционирования и взаимодействия с протоколом SNMP.

В системе реализована поддержка протокола SNMP версий 1, 2c и 3.

14.1. Настройка протокола SNMP

14.1.1. Команды настройки протокола SNMP

14.1.1.1. Команда **snmp-server enable**

Включает протокол SNMP на устройстве. Использование префикса «**no**» отключает поддержку протокола snmp.

Синтаксис команды:

snmp-server enable snmp

или

no snmp-server enable snmp

Состояние по умолчанию – протокол SNMP включен.

Режим ИКС – режим общего конфигурирования.

14.1.1.2. Команда **snmp-servercommunity**

Определяет пароль, разрешающий доступ к устройству по протоколу SNMP версий 1 и 2c. Использование префикса «**no**» восстановит установки по умолчанию.

Синтаксис команды:

snmp-server community *community-string* [*ro* | *rw* | ***view*** *view-name* | **group** *group-id* | **use-acl** *name-acl*]

или

no snmp-server server community *community-string*

Параметры команды:

– *community-string* – строка пароля, разрешающего доступ к устройству (диапазон от 1 до 20 символов);

– *ro* – доступ только для чтения, используется по умолчанию;

– *rw* – доступ для чтения и записи;

– *group-id* – доступ SNMP с ограничениями аналогичными группам заданным в системе. Возможные значения - network-user, network-operator, network-admin;

– *name-acl* – список доступа;

– *view-name* – список MIB объектов доступных для указанного пароля.

Состояние по умолчанию – пароль не определен, получение данных по SNMP v1 и v2 недоступно.

Режим ИКС – режим общего конфигурирования.

14.1.1.3. Команда **snmp-server user**

Определяет пользователей протокола SNMPv3. Использование префикса «**no**» удалит пользователя протокола SNMPv3.

Синтаксис команды:

snmp-server user *username groupname* [**auth** {**md5** | **sha**} auth-password] [**priv {des | aes}** *priv-password*]

или

no snmp-server user *username*

Параметры команды:

– *username* – имя пользователя (до 20 символов);

– *groupname* – имя группы, к которой принадлежит пользователя (network-admin или network-operator);

– *md5* – уровень аутентификации HMAC-MD5-96;

– *sha* – уровень аутентификации HMAC-SHA-96;

– *des* – алгоритм шифрования Data Encryption Standard (DES);

– *aes* – алгоритм шифрования Advanced Encryption Standard (AES);

– *auth-password* – строка пароля аутентификации (до 32 символов);

– *priv-password* – строка пароля шифрования (до 64 символов).

Состояние по умолчанию – пользователи не определены.

Режим ИКС – режим общего конфигурирования.

14.1.2. Просмотр состояния протокола SNMP

14.1.2.1. Команда **show snmp**

Отображает информацию о состоянии протокола SNMP.

Синтаксис команды:

show snmp

Режим ИКС – режим управления.

15. РЕАЛИЗАЦИЯ ФУНКЦИЙ БЕЗОПАСНОСТИ СРЕДЫ ФУНКЦИОНИРОВАНИЯ

При реализации функций безопасности, связанных со средой функционирования ПО KTOS, необходимо придерживаться политик безопасности организации. В данные политики безопасности должны быть включены меры по организационной и физической защите доступа к ПО KTOS и коммутатору.

ПРИЛОЖЕНИЕ 1

СООТВЕТСТВИЕ НОМЕРОВ ПОРТОВ И ИДЕНТИФИКАТОРОВ ИНТЕРФЕЙСА

Соответствие номеров портов на внешней панели коммутатора KS-1024T-4X (КРПЕ.465615.002) и идентификаторов интерфейса в интерфейсе командной строки KTOS приведено в таблице 1.1.

Таблица 1.1

Номер порта на внешней панели коммутатора	Идентификатор интерфейса в интерфейсе командной строки KTOS
1	ge1
2	ge2
3	ge3
…	…
…	…
…	…
24	ge24
25	xe1
26	xe2
27	xe3
28	xe4

Соответствие номеров портов на внешней панели коммутатора KS-1048T-4X (КРПЕ.465615.004) и идентификаторов интерфейса в интерфейсе командной строки KTOS приведено в таблице 1.2.

Таблица 1.2

Номер порта на внешней панели коммутатора	Идентификатор интерфейса в интерфейсе командной строки KTOS
1	ge1
2	ge2
3	ge3
…	…
…	…
…	…

Номер порта на внешней панели коммутатора	Идентификатор интерфейса в интерфейсе командной строки KTOS
48	ge48
49	xe1
50	xe2
51	xe3
52	xe4

Соответствие номеров портов на внешней панели коммутатора KS-1024T-4X (КРПЕ.465615.002) и идентификаторов интерфейса в интерфейсе командной строки KTOS приведено в таблице 1.3.

Таблица 1.3

Номер порта на внешней панели коммутатора	Идентификатор интерфейса в интерфейсе командной строки KTOS
1	ge1
2	ge2
3	ge3
…	…
…	…
…	…
24	ge24
25	xe1
26	xe2
27	xe3
28	xe4

ПРИЛОЖЕНИЕ 2

УСТАНОВКА САМОПОДПИСАННОГО СЕРТИФИКАТА

Получить самоподписанный сертификат у производителя коммутатора.

На рабочем столе запустить приложение «Google Chrome». В окне (см. рис. 2.1) ввести IP адрес коммутатора, например, 10.0.59.118.

Окно Google Chrome

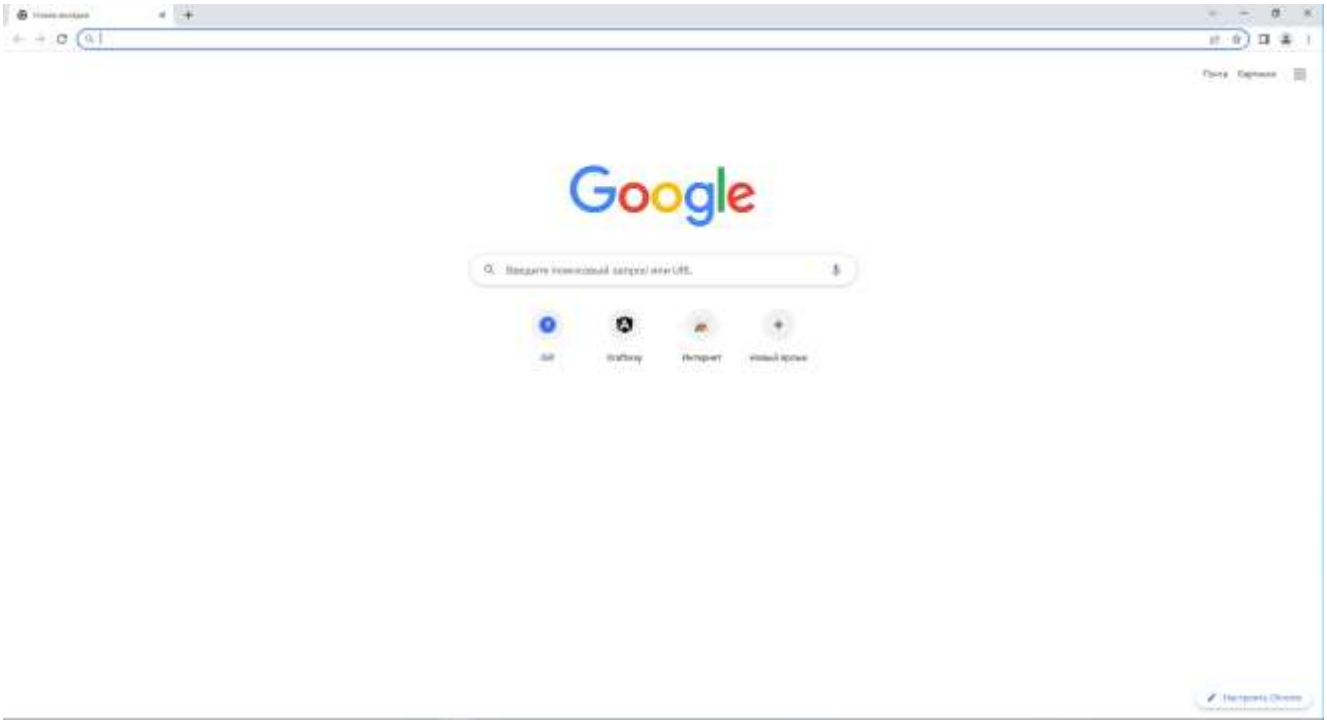


Рис. 2.1

Окно примет вид, показанный на рис. 2.2.

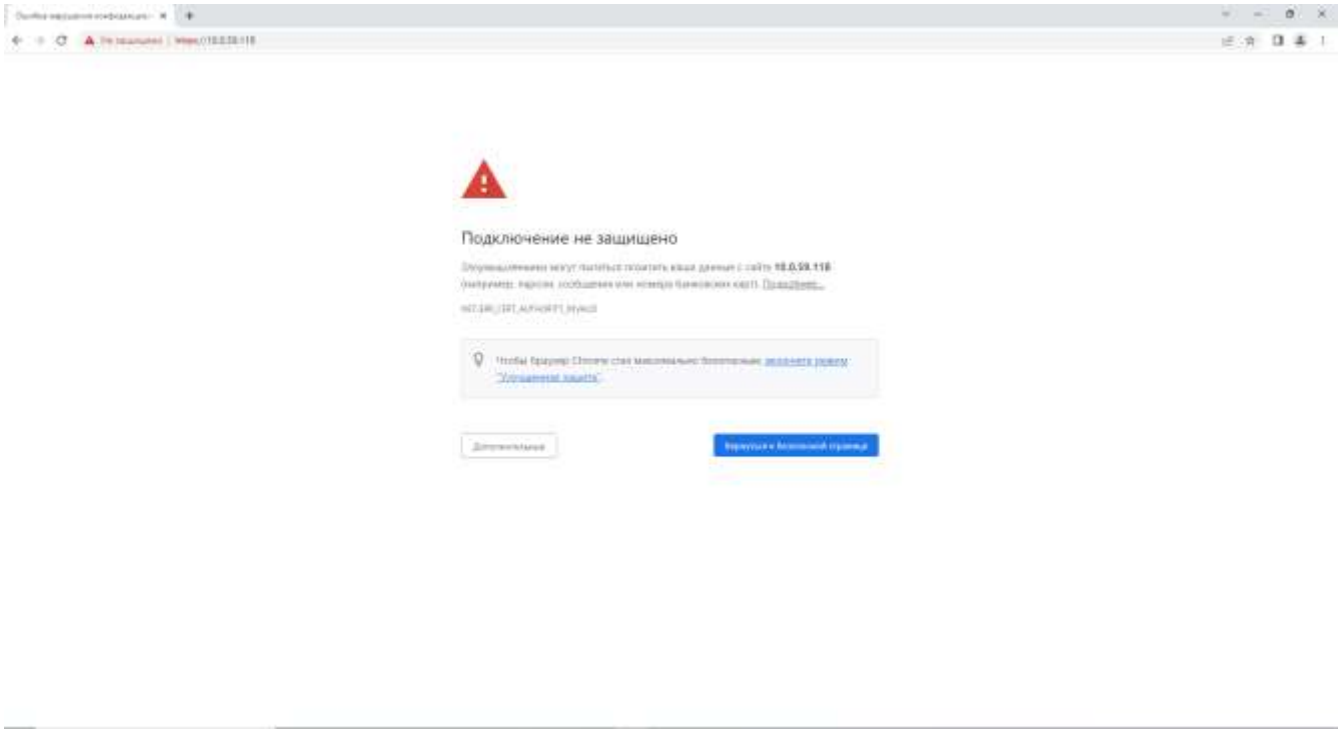


Рис. 2.2

Нажать на [Не защищено]. В сплывающем окне (см. рис. 2.3) нажать [Настройки сайтов].

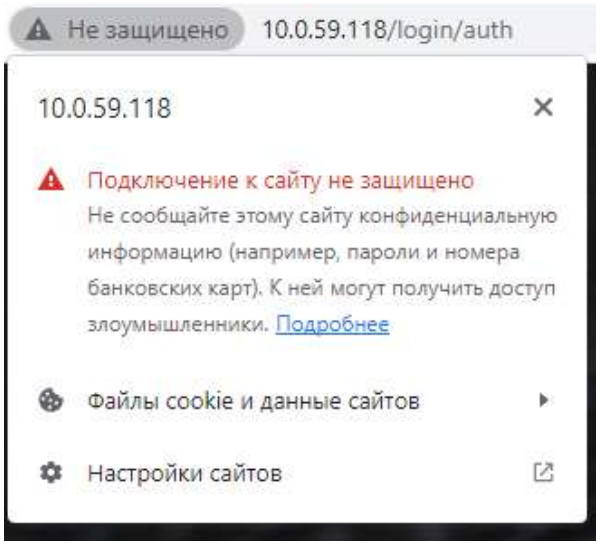


Рис. 2.3

В окне (см. рис. 2.4) нажать [Конфиденциальность и безопасность].

Конфиденциальность и безопасность

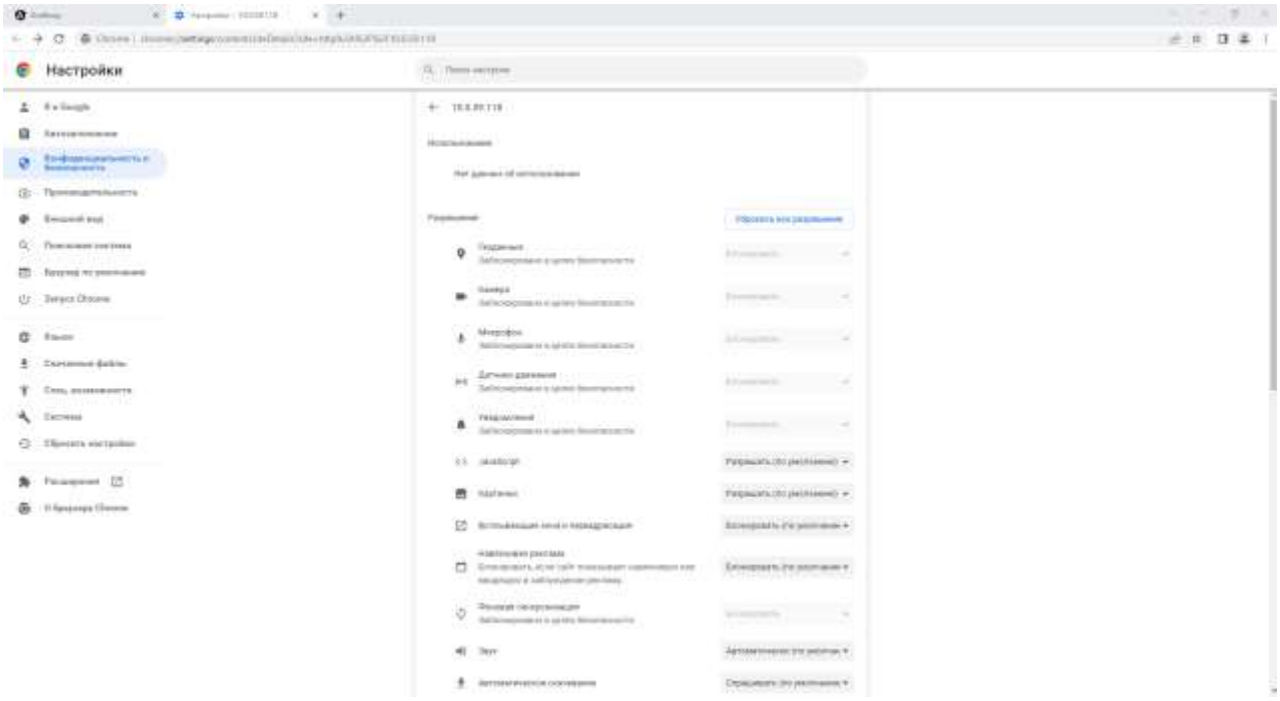


Рис. 2.4

В окно (см. рис. 2.5) нажать [Безопасность].

Безопасность

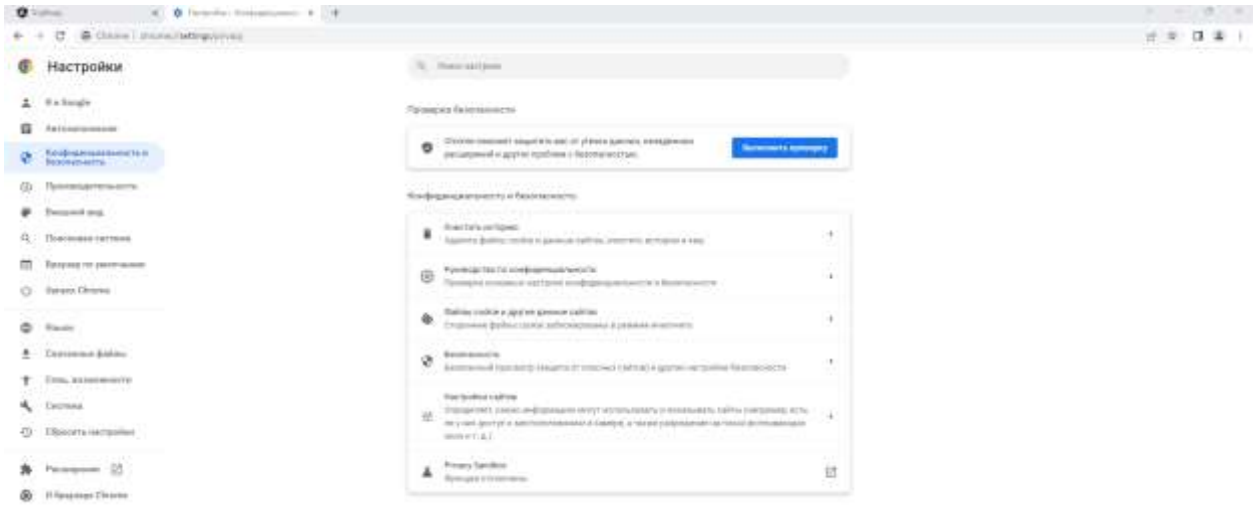


Рис. 2.5

В окне (см. рис. 2.6) нажать [Управление сертификатами устройства].

Управление сертификатами устройства

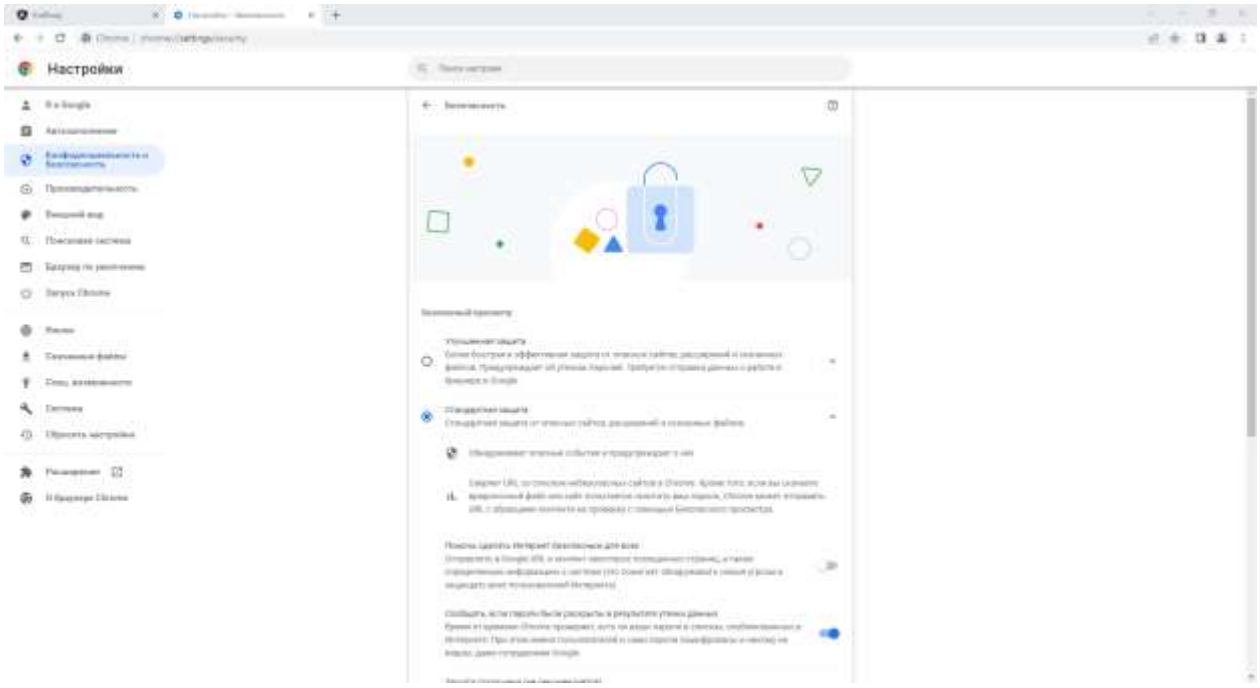


Рис. 2.6

В окне (см. рис. 2.7) нажать - «Импорт…».

Импорт

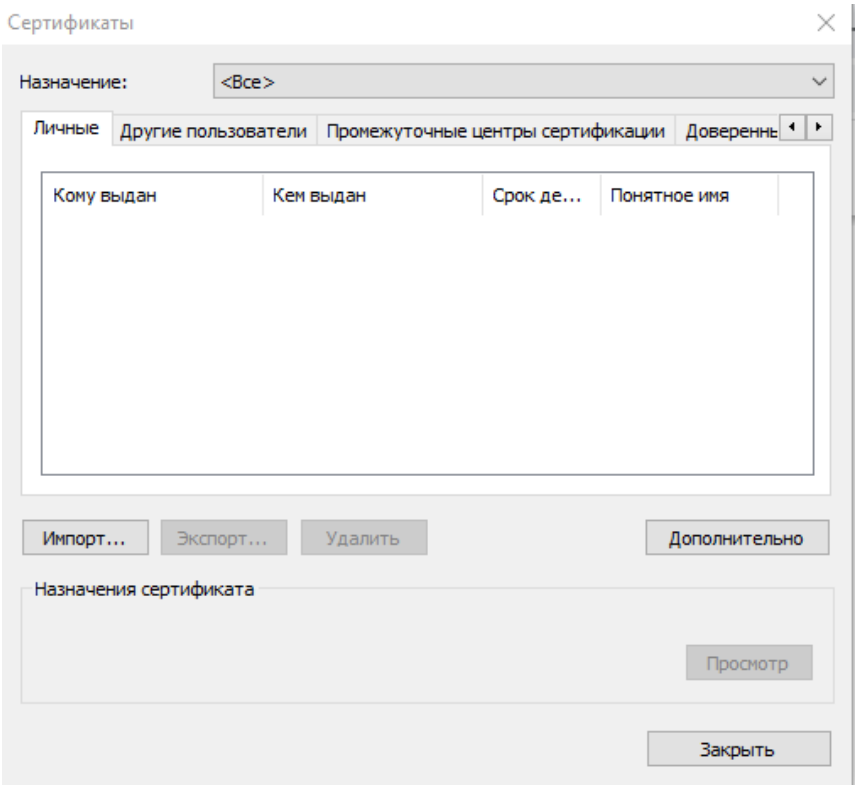


Рис. 2.7

В окне (см. рис. 2.8) нажать - «Далее».

Мастер импорта сертификатов

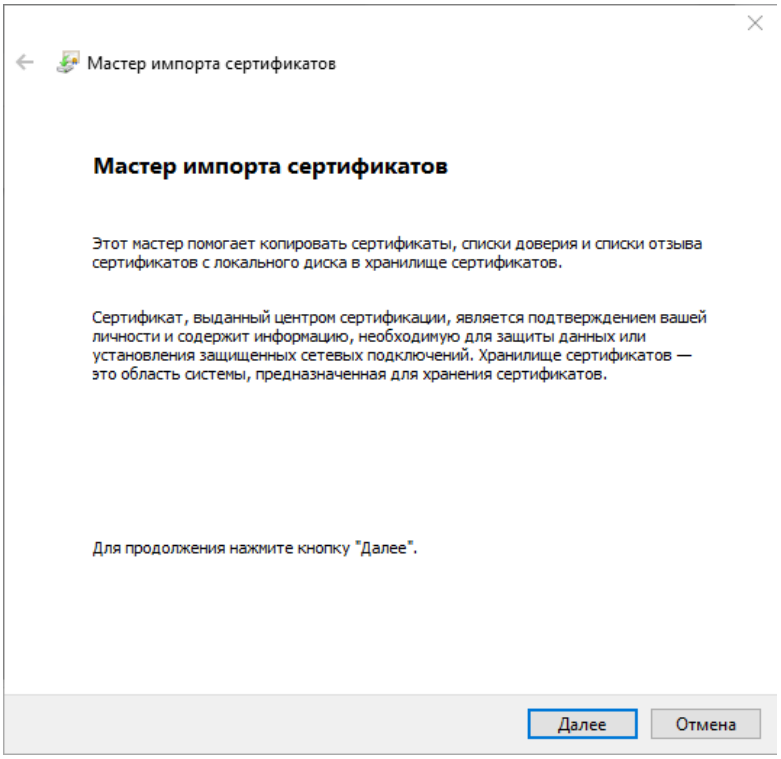


Рис. 2.8

В окне (см. рис. 2.9) нажать [Обзор].

Импорт файлов

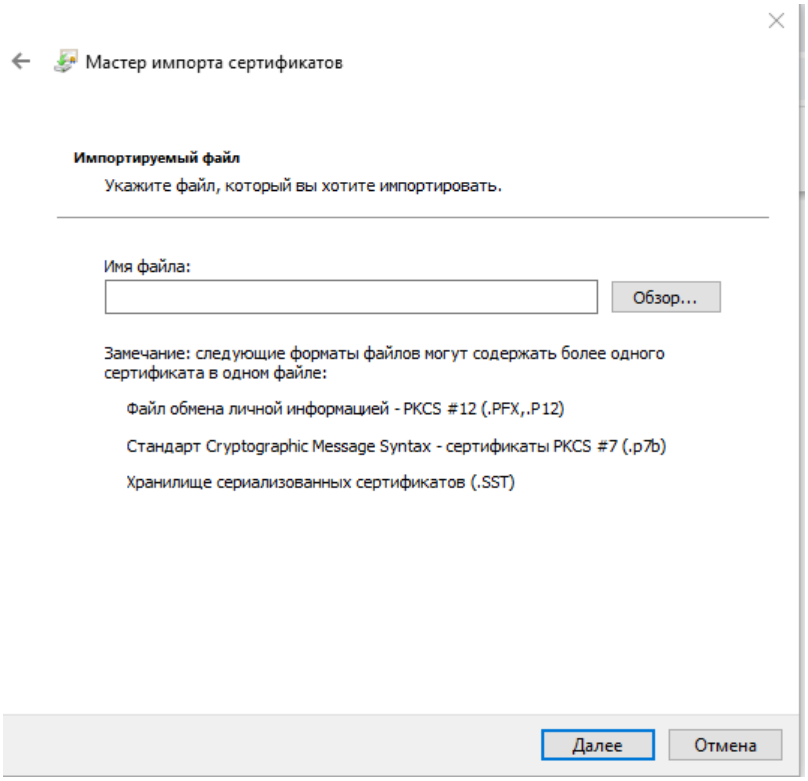


Рис. 2.9

В окне (см. рис. 2.10) указать путь к сертификату и нажать [Открыть].

Путь к сертификату

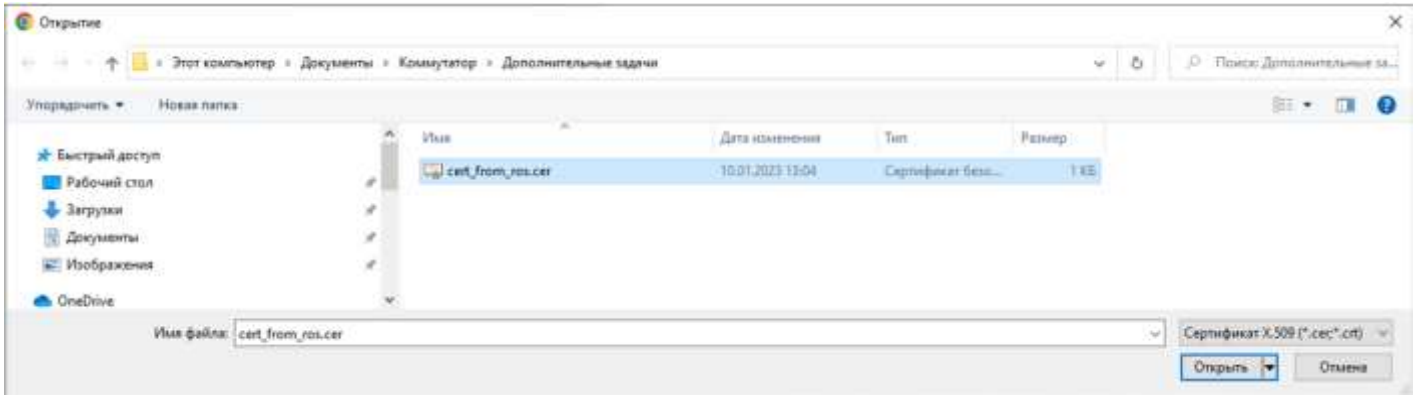


Рис. 2.10

В окне (см. рис. 2.11) нажать [Далее].

Хранилище сертификатов

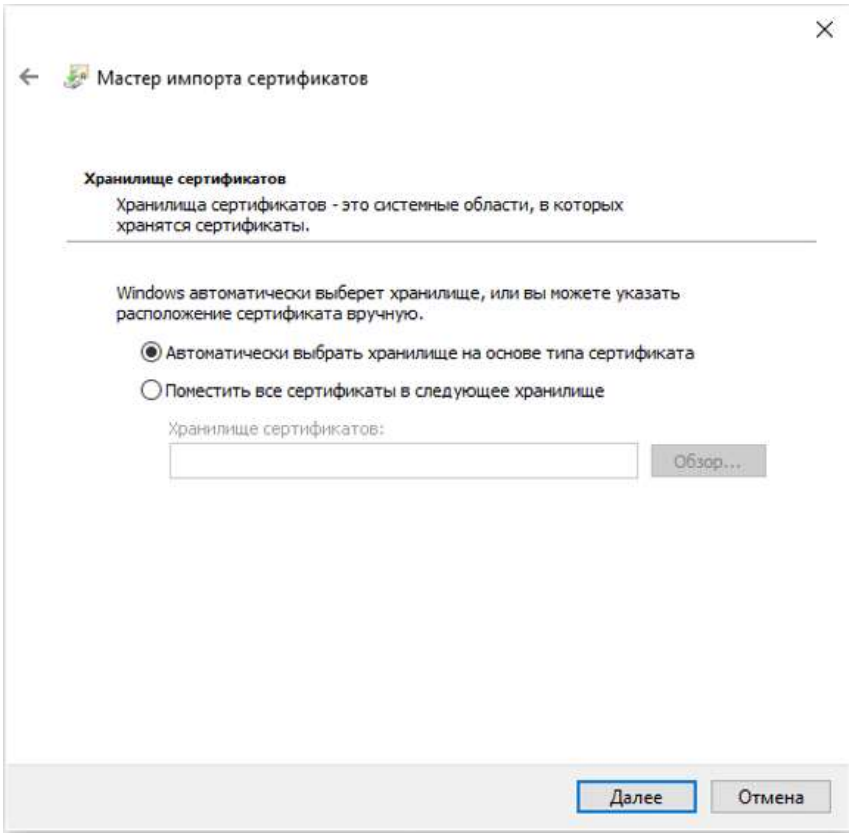


Рис. 2.11

В окне (см. рис. 2.12) нажать [Далее].

Поместить все сертификаты в следующее хранилище

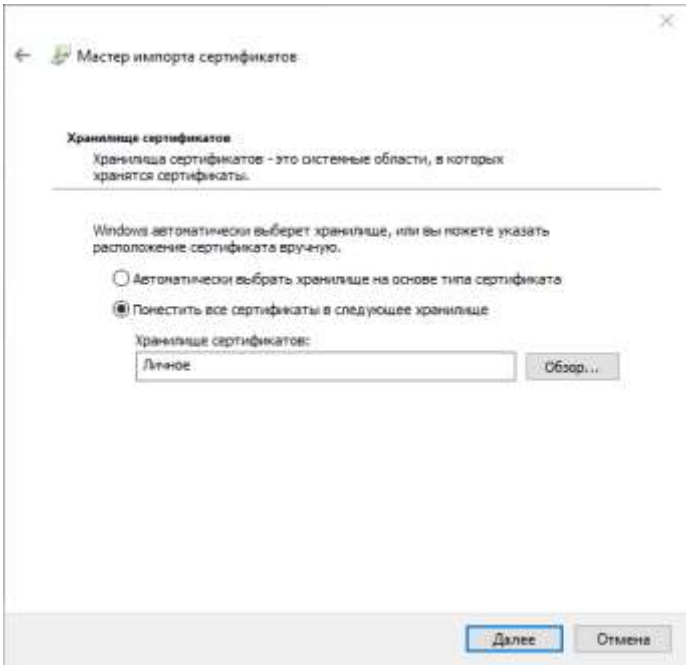


Рис. 2.12

В окне (см. рис. 2.13) нажать [Готово].

Завершение мастера импорта сертификатов

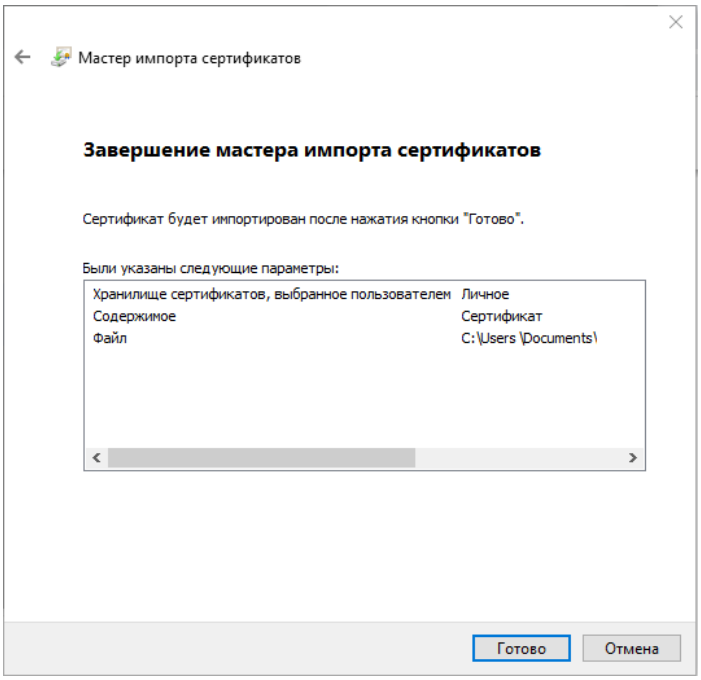


Рис. 2.13

Окно примет вид показанный на рис. 2.14, в следующем окне (см. рис. 2.14) появится сообщение: «Импорт успешно выполнен».

Сертификаты

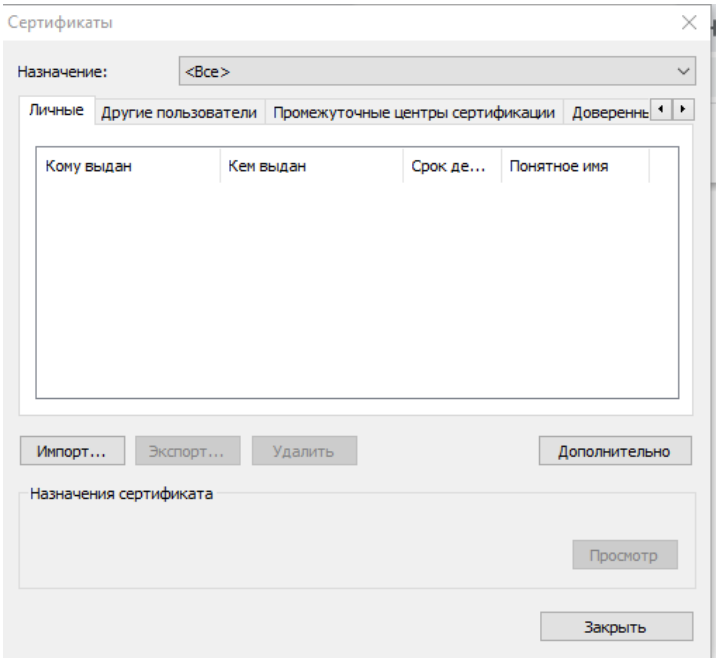


Рис. 2.14

Импорт успешно выполнен

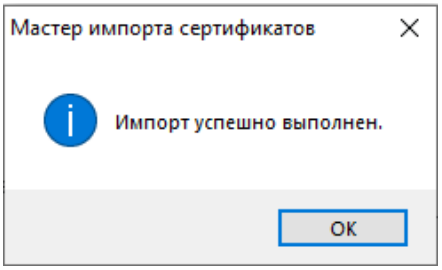


Рис. 2.15

Далее в окне «Мастер импорта сертификатов», показанном на рис. 2.14, нажать [Ok]. И в окне «Сертификаты» (см. рис. 2.15) нажать [Закрыть].

Перейти во вкладку «Kraftway» и выбрать [ ]. Окно примет вид показанный на рис. 2.16.

Соединение защищено

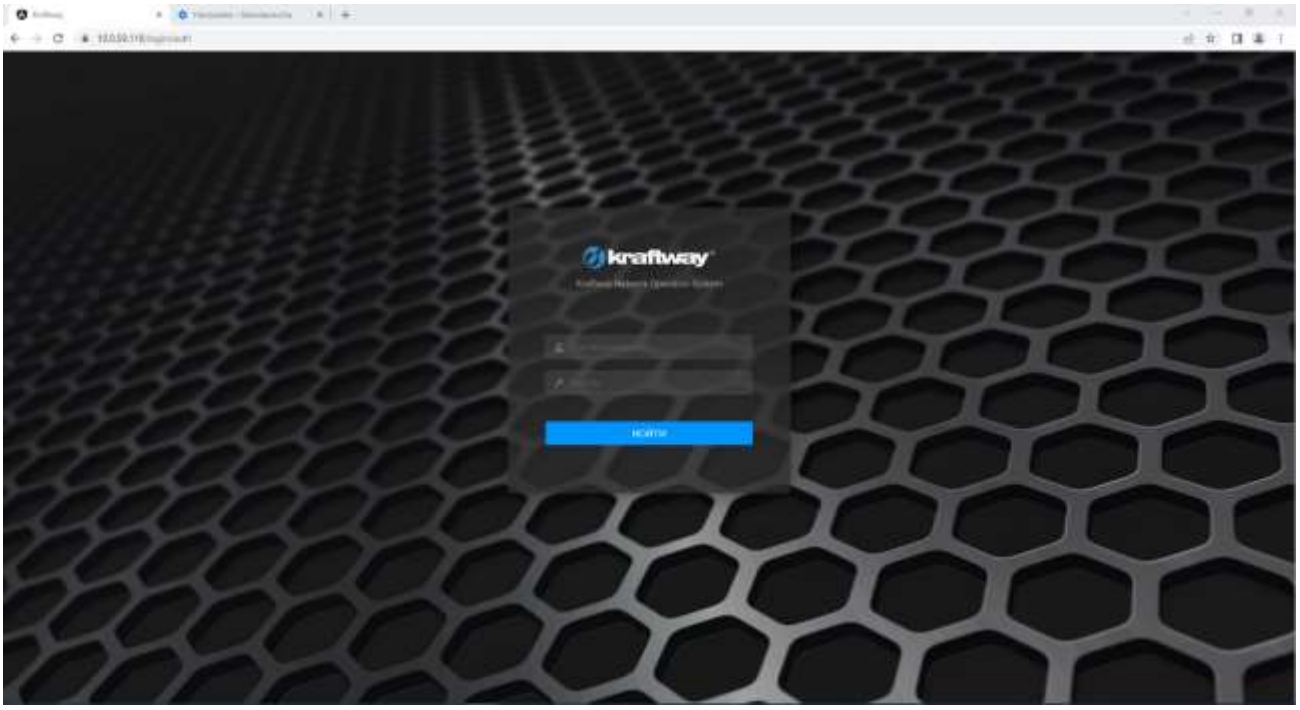


Рис. 2.16

Самоподписанный сертификат успешно импортирован и защищенное соединение установлено.

Приведенная инструкция построена на основе сведений, полученных с сайта support.google.com: https://support.google.com/chrome/#topic=7439538.

ПЕРЕЧЕНЬ ПРИНЯТЫХ ТЕРМИНОВ И СОКРАЩЕНИЙ

Термин, сокращение	Наименование и определение
ИКС	Интерфейс командной строки
ОО	Объект управления
ОПО	Общесистемное программное обеспечение
ОС	Операционная система
ПЗУ	Постоянное запоминающее устройство
ПК	Персональный компьютер
ПО	Программное обеспечение
ПО KTOS	Программное обеспечение Kraftway Telecom Operating System Версия 3
ЦПУ	Центральное процессорное устройство
ЭВМ	Электронная вычислительная машина
ACE	англ. Access Control Element – правило доступа в ACL
ACL	англ. англ. Access Control List – список управления доступом
AES	англ. Advanced Encryption Standard – симметричный алгоритм блочного шифрования
ARM	англ. Advanced RISC Machine – система команд 32-битных и 64-битных микропроцессорных ядер, разрабатываемых компанией ARM Limited
ARP	англ. Address Resolution Protocol – протокол определения адреса, предназначенный для определения MAC-адреса по IP-адресу другого компьютера
ASCII	англ. American Standard Code for Information Interchange – название таблицы (кодировки, набора), в которой некоторым распространенным печатным и непечатным символам сопоставлены числовые коды
BPDU	англ. Bridge Protocol Data Unit – блок данных протокола мостового перенаправления; фрейм (единица данных) протокола управления сетевыми мостами
DES	англ. Data Encryption Standard – алгоритм для симметричного шифрования
DHCP	англ. Dynamic Host Configuration Protocol – сетевой протокол, позволяющий сетевым устройствам автоматически получать IP-адрес и другие параметры, необходимые для работы в сети TCP/IP
DNS	англ. Domain Name System – компьютерная распределенная система для получения информации о доменах

Термин, сокращение	Наименование и определение
DSCP	англ. Differentiated Services Code Point – элемент архитектуры компьютерных сетей, описывающий простой масштабируемый механизм классификации, управления трафиком и обеспечения качества обслуживания
ECMP	англ. Equal-Cost Multi-Path routing – технология балансировки маршрутизации по маршрутам с равной метрикой
Ethernet	англ. Ethernet – семейство технологий пакетной передачи данных между устройствами для компьютерных и промышленных сетей, локальная компьютерная сеть
FAT	англ. File Allocation Table – классическая архитектура файловой системы ОС Windows
FDB	англ. Forwarding DataBase – таблица коммутации. В FDB-таблице коммутатора содержатся записи о том какой MAC-адрес на каком интерфейсе коммутатора находится
FIFO	англ. First In, First Out – способ организации и манипулирования данными относительно времени и приоритетов, принцип технической обработки очереди или обслуживания конфликтных требований путем упорядочения процесса по принципу «первым пришел – первым обслужен»
GRE	англ. Generic Routing Encapsulation – протокол туннелирования сетевых пакетов
GUI	англ. Graphical User Interface – система средств для взаимодействия пользователя с компьютером, графический пользовательский интерфейс
HMAC	англ. Hash-based Message Authentication Code – код аутентификации (проверки подлинности) сообщений, использующий хеш-функции
HTML	англ. HyperText Markup Language – стандартизированный язык разметки документов в сети Интернет
HTTP	англ. HyperText Transfer Protocol – протокол прикладного уровня передачи данных
HTTPS	англ. HyperText Transfer Protocol Secure – расширение протокола HTTP для поддержки шифрования в целях повышения безопасности
ICMP	англ. Internet Control Message Protocol – сетевой протокол, входящий в стек протоколов TCP/IP. В основном ICMP используется для передачи сообщений об ошибках и других исключительных ситуациях
IEEE	англ. Institute of Electrical and Electronics Engineers – международная некоммерческая ассоциация специалистов в области техники, мировой лидер в области разработки

Термин, сокращение	Наименование и определение
	стандартов по радиоэлектронике, электротехнике и аппаратному обеспечению вычислительных систем и сетей
IGMP	англ. Internet Group Management Protocol – протокол управления групповой (multicast) передачей данных в сетях, основанных на протоколе IP
IP	англ. Internet Protocol – маршрутизируемый протокол сетевого уровня стека TCP/IP
ISO	англ. International Organization for Standardization – международная организация, занимающаяся выпуском стандартов
LACP	англ. Link Aggregation Control Protocol – протокол, предназначенный для объединения нескольких физических каналов в один логический в сетях Ethernet
LAG	англ. Link Aggregation Group – группа агрегированных каналов
LSDB	англ. Link State DataBase – список всех записей о состоянии каналов. База данных состояния каналов
MAC	англ. Media Access Control – подуровень канального (второго) уровня модели OSI, согласно стандартам IEEE 802
MAC-адрес	англ. Media Access Control – уникальный идентификатор, присваиваемый каждой единице активного оборудования или некоторым их интерфейсам в компьютерных сетях Ethernet
MD5	англ. Message Digest 5 – алгоритм хеширования. Предназначен для создания «отпечатков» или дайджестов сообщения произвольной длины и последующей проверки их подлинности
MIB	англ. Management Information Base – виртуальная база данных, используемая для управления объектами в сети связи
MIPS	англ. Microprocessor without Interlocked Pipeline Stages – система команд и микропроцессорных архитектур, разработанных компанией MIPS Computer Systems
MSTP	англ. Multiple Spanning Tree Protocol – канальный протокол. В один экземпляр MSTP могут входить несколько виртуальных сетей при условии, что их топология одинакова
NAND	англ. Not AND – тип флеш-памяти по принципу изменения информации в ее ячейках
NTP	англ. Network Time Protocol – сетевой протокол для синхронизации внутренних часов компьютера с использованием сетей с переменной латентностью

Термин, сокращение	Наименование и определение
OSI	англ. Open Systems Interconnection basic reference model – сетевая модель стека сетевых протоколов OSI/ISO
Port Mirroring	англ. Port Mirroring – отслеживает и отражает сетевой трафик, пересылая копии входящих и исходящих пакетов с одного порта на порт мониторинга
RS-232	англ. Recommended Standard 232 – стандарт асинхронного последовательного интерфейса
RSTP	англ. Rapid STP – версия протокола STP с ускоренной реконфигурацией дерева, использующегося для исключения петель (исключения дублирующих маршрутов) в соединениях коммутаторов Ethernet с дублирующими линиями
SFP/SFP+	англ. Small Form-factor Pluggable/Enhanced Small Form-factor Pluggable – промышленный стандарт модульных компактных приемопередатчиков (трансиверов), используемых для передачи и приема данных в телекоммуникациях
SNMP	англ. Simple Network Management Protocol – стандартный интернет-протокол для управления устройствами в IP-сетях на основе архитектур TCP/UDP
SSH	англ. Secure SHell – сетевой протокол прикладного уровня, позволяющий производить удаленное управление операционной системой и туннелирование TCP-соединений
SSL	англ. Secure Sockets Layer – криптографический протокол, который подразумевает безопасную связь
STP	англ. Spanning Tree Protocol (протокол остовного дерева) – канальный протокол
Storm Control	англ. Storm Control – ограничивает количество многоадресных и широковещательных кадров, принимаемых и пересылаемых коммутатором
Syslog	англ. System log – системный журнал. Стандарт отправки и регистрации сообщений о происходящих в системе событиях (то есть создания логов), использующийся в компьютерных сетях, работающих по протоколу IP
TCP	англ. Transmission Control Protocol – протокол управления передачей
TDF	англ. Time Domain Reflectometry – технология позволяющая определить характеристик электрических линий путем наблюдения отраженных сигналов
TELNET	англ. TELetype NETwork – сетевой протокол для реализации текстового терминального интерфейса по сети (в современной форме – при помощи транспорта TCP)
TFTP	англ. Trivial File Transfer Protocol – простой протокол передачи файлов

Термин, сокращение	Наименование и определение
TTL	англ. Time To Live – время жизни пакета данных в протоколе IP (предельно допустимое время его пребывания в системе), время актуальности записей DNS
UDP	англ. User Datagram Protocol – протокол пользовательских датаграмм – один из ключевых элементов TCP/IP, набора сетевых протоколов для Интернета
URL	англ. Uniform Resource Locator – система унифицированных адресов электронных ресурсов, или единообразный определитель местонахождения ресурса
VLAN	англ. Virtual Local Area Network – логическая («виртуальная») локальная компьютерная сеть
VRRP	Virtual Router Redundancy Protocol – сетевой протокол, предназначенный для увеличения доступности маршрутизаторов, выполняющих роль шлюза по умолчанию
VTY	англ. Virtual Teletype – виртуальное устройство, терминал, соединенный со стандартным вводом/выводом
USB	англ. Universal Serial Bus – универсальная последовательная шина