КОД безопасности

Аппаратно-программный комплекс шифрования

Континент

Версия 3.9 (исполнение 3.М3)

Руководство администратора

Сетевые функции

RU.88338853.501430.022 0390 10

© Компания "Код Безопасности", 2023. Все права защищены.

Все авторские права на эксплуатационную документацию защищены.

Этот документ входит в комплект поставки изделия. На него распространяются все условия лицензионного соглашения. Без специального письменного разрешения компании "Код Безопасности" этот документ или его часть в печатном или электронном виде не могут быть подвергнуты копированию и передаче третьим лицам с коммерческой целью.

Информация, содержащаяся в этом документе, может быть изменена разработчиком без специального уведомления, что не является нарушением обязательств по отношению к пользователю со стороны компании "Код Безопасности".

Почтовый адрес:	**115127, Россия, Москва, а/я 66** **ООО "Код Безопасности"**
Телефон:	**8 495 982-30-20**
E-mail:	**info@securitycode.ru**
Web:	**https://www.securitycode.ru**

Оглавление

Список сокращений ... **5**

Введение ... **6**

Настройка интерфейсов ... **7**

Сетевые интерфейсы ... 7

Параметры сетевых интерфейсов ... 8

VLAN-интерфейсы ... 10

Вызов списка VLAN-интерфейсов ... 10

Регистрация нового VLAN-интерфейса ... 10

Редактирование параметров VLAN-интерфейса ... 11

Удаление VLAN-интерфейса ... 11

VLAN-интерфейсы на криптокоммутаторе ... 11

Альтернативные адреса КШ и КК ... 12

Замена IP-адреса внешнего интерфейса ЦУС ... 12

Настройка объединения интерфейсов ... 12

Особенности агрегации интерфейсов в кластере ... 15

Модемное подключение и поддержка PPPoE ... 16

Подключение модема Huawei E3372 ... 16

Подключение и настройка 3G-модема ... 18

Локальная настройка модемного подключения КШ ... 19

Изменение адреса подключения к ЦУС ... 20

Управление режимами работы сетевого устройства ... **21**

Настройка Multi-WAN ... 21

Настройка режима Multi-WAN ... 21

Обеспечение отказоустойчивости канала связи ... 24

Балансировка трафика между внешними интерфейсами сетевого устройства ... 25

Настройки сервиса DHCP ... 27

Включение и настройка режима сервера ... 27

Включение и настройка ретранслятора ... 33

Отключение сервиса DHCP ... 34

Просмотр статистики сервера DHCP ... 35

Настройка параметров маршрутизации ... 35

Переход к настройке параметров ... 35

Переключение режима маршрутизации ... 35

Статическая маршрутизация ... 36

Динамическая маршрутизация ... 38

Настройка фрагментации пакетов ... 40

Особенность работы КШ как транзитного устройства ... 42

Управление списком связанных сетевых устройств ... 42

Установка времени на КШ с ЦУС ... 45

Настройка DNS ... 47

Настройка дистанционного доступа по протоколу SSH ... 48

Диагностика сетевого устройства ... 49

Обращение в техподдержку ... 50

Управление трафиком ... **52**

Определение классов трафика ... 52

Управление приоритизацией трафика ... 53

Окно управления QoS ... 53

Настройка общих параметров очереди на интерфейсе ... 54

Настройка параметров очереди ... 54

Резервирование полосы пропускания для управляющего трафика ... 55

Экспорт/импорт конфигурации очередей ... 56

Режим изолированной сети ... 57

Приложение ... **59**

Переход к меню локальной настройки параметров сетевого устройства ... 59

Команды дополнительного меню 59
Формат и примеры конфигурационных файлов 61
Формат конфигурационного файла OSPF 62
Формат конфигурационного файла BGP 63
Примеры конфигурационного файла RIP 65
Управление очередью заданий 67

Документация **68**

Список сокращений

АПКШ	Аппаратно-программный комплекс шифрования
БД	База данных
ДА	Детектор (компьютерных) атак
ДСЧ	Датчик случайных чисел
КК	Криптографический коммутатор
КШ	Криптографический шлюз
ЛВС	Локальная вычислительная сеть
НСД	Несанкционированный доступ
ОС	Операционная система
ПАК	Программно-аппаратный комплекс
ПО	Программное обеспечение
ПУ	Программа управления
СД	Сервер доступа
СКЗИ	Средство криптографической защиты информации
СОВ	Система обнаружения вторжений (компьютерных атак)
СУ	Сетевое устройство (КШ, КК, ДА)
СУБД	Система управления базами данных
ЦУС	Центр управления сетью
DHCP	Dynamic Host Configuration Protocol
ICMP	Internet Control Message Protocol
IP	Internet Protocol
LACP	Link Aggregation Control Protocol
LAG	Link Aggregation Group
MTU	Maximum Transmission Unit
NAT	Network Address Translation
PPPoE	Point to Point Protocol over Ethernet
RAS	Remote Access Service
RPC	Remote Procedure Call
SMB	Server Message Block
SNMP	Simple Network Management Protocol
SPAN	Switched Port Analyzer
SSH	Secure Shell
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
USB	Universal Serial Bus
VID	VLAN Identifier
VLAN	Virtual Local Area Network
VoIP	Voice over IP
VPN	Virtual Private Network

Введение

Документ предназначен для администраторов изделия " Аппаратно- программный комплекс шифрования "Континент". Версия 3.9 (исполнение 3.М3)" (далее — комплекс, АПКШ "Континент"). В нем содержатся сведения, необходимые администраторам для настройки сетевых параметров компонентов комплекса.

Дополнительные сведения, необходимые администратору комплекса, содержатся в [**1**]–[**5**].

Сайт в интернете. Информация о продуктах компании "Код Безопасности" представлена на сайте https://www.securitycode.ru.

Служба технической поддержки. Связаться со службой технической поддержки можно по телефону 8 800 505- 30- 20 или по электронной почте support@securitycode.ru.

Учебные курсы. Освоить аппаратные и программные продукты компании "Код Безопасности" можно в авторизованных учебных центрах. Список учебных центров и условия обучения представлены на сайте компании https://www.securitycode.ru. Связаться с представителем компании по вопросам организации обучения можно по электронной почте education@securitycode.ru.

Глава 1
Настройка интерфейсов

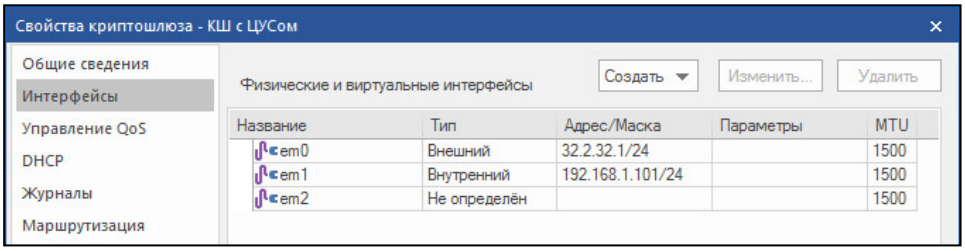
Сетевые интерфейсы

Любой интерфейс сетевого устройства может иметь несколько IP-адресов.

Интерфейс, определенный как SPAN-порт, должен использоваться только для целей анализа сетевого трафика. Подключать его к любым сетям запрещается, так как это может привести к лавинообразному росту трафика и выходу сети из строя. Также для SPAN- порта запрещено указывать автоматический выбор режима (скорости) работы.

Для настройки интерфейсов сетевого устройства:

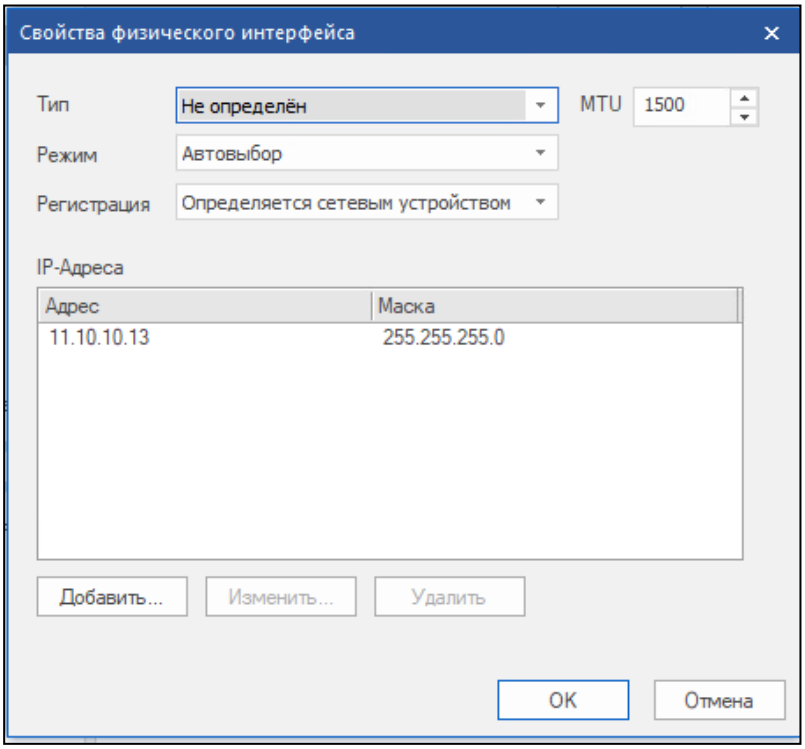
1. Вызовите окно свойств сетевого устройства и перейдите на вкладку "Интерфейсы".



Примечание. Имена интерфейсов, отображаемые в таблице, соответствуют именам, указанным на корпусе сетевого устройства рядом с каждым разъемом.

2. Для изменения параметров интерфейса выберите его в таблице, нажмите кнопку "Изменить...".

   Появится окно "Свойства физического интерфейса".



3. Внесите необходимые изменения (описание параметров приведено в таблицах ниже) и нажмите кнопку "ОК".

Примечание. Для смены или удаления интерфейса резервирования необходимо предварительно задать дополнительный интерфейс резервирования либо выключить режим резервирования (см. [**2**], "Управление кластером").

4. Для добавления нового модемного или виртуального интерфейса нажмите кнопку "Создать", выберите тип интерфейса, заполните поля его параметров (см. ниже) в появившемся окне и нажмите кнопку "ОК".
5. Для удаления модемного или виртуального интерфейса выберите его в таблице, нажмите кнопку "Удалить" и подтвердите удаление, нажав кнопку "Да" в появившемся окне.

Параметры сетевых интерфейсов

Табл.1 Параметры интерфейса Ethernet

Параметр	Описание
Тип	Тип интерфейса: • Внешний — интерфейс, подключаемый к сетям общего пользования. • Внутренний — интерфейс, подключаемый к защищаемой сети (только для КШ). • Резервирование <сетевого устройства>— интерфейс для обмена служебной информацией между основным и резервным устройством в кластере (интерфейс резервирования). • SPAN — интерфейс для подключения компьютера с установленной на нем системой обнаружения сетевых атак. • Управление (только для ДА) — интерфейс для связи с ЦУС или другими сетевыми устройствами. • Мониторинг (только для ДА) — интерфейс , подключаемый к span-порту для анализа зеркального трафика. • Порт криптокоммутатора (только для КК) — интерфейс, используемый в составе виртуального коммутатора для создания криптографической коммутируемой сети. • Не определен — интерфейс при работе сетевого устройства не используется
Режим	Режим работы сетевой карты. Доступные режимы: • Автовыбор. • 10base-T / half duplex. • 10base-T / full duplex. • 100base-TX / half duplex. • 100base-TX / full duplex. • 1000base-T / half duplex. • 1000base-T / full duplex. Отображаемый список режимов зависит от установленных трансиверов и сетевых адаптеров. При смене трансивера выбранный ранее режим может не поддерживаться. В этом случае следует установить значение "Автовыбор". **Внимание!** Вместо режима "* / full duplex" необходимо установить режим "Автовыбор"
Регистрация	Задание правила регистрации событий в журналах. Значения: • определяется сетевым устройством (правило наследуется из свойств сетевого устройства); • первые 64 байта; • тело пакета
MTU	Максимальная единица передачи данных (в байтах). Допустимые значения: • для КШ (внутренние и внешние интерфейсы) 576–9000; • для КК (внешний интерфейс) 576–9100. Если типом интерфейса является "порт криптокоммутатора", по умолчанию устанавливается значение 1500, которое изменять не рекомендуется

Параметр	Описание
IP-адреса	Список IP-адресов интерфейса. Для добавления нового адреса нажмите кнопку "Добавить", укажите IP-протокол (IPv4 или IPv6; IPv6 используется только для внешних интерфейсов) и далее введите адрес и маску (префикс для IPv6). Для удаления выбранного IP-адреса используйте кнопку "Удалить"

Табл.2 Параметры VLAN-интерфейса

Параметр	Описание
Название	Наименование VLAN-интерфейса. Присваивается автоматически (vlan0, vlan1 и т.д.)
Тип	Тип интерфейса: • Не определен — интерфейс предназначен для каких-либо специальных задач. • Внешний — интерфейс, подключаемый к сетям общего пользования. • Внутренний — интерфейс, подключаемый к защищаемой сети (для КШ). • Порт криптокоммутатора (для КК)
MTU	Максимальная единица передачи данных (в байтах)
VLAN-идентификатор	Идентификатор виртуальной локальной сети (VID). Значение параметра должно быть в пределах от 1 до 4094
Родительский интерфейс	Выберите в раскрывающемся списке родительский интерфейс
IP-адреса	Список IP-адресов интерфейса (до 16). Для добавления нового адреса нажмите кнопку "Добавить", укажите IP-протокол (IPv4 или IPv6; IPv6 используется только для внешних интерфейсов) и далее введите адрес и маску (префикс для IPv6). Для удаления выбранного IP-адреса используйте кнопку "Удалить"
Регистрация	Задание правила регистрации событий в журналах. Значения: • определяется сетевым устройством (правило наследуется из свойств сетевого устройства); • первые 64 байта; • тело пакета

Табл.3 Параметры PPP-интерфейса

Параметр	Описание
Название	Наименование PPP-интерфейса. Присваивается автоматически (tun0, tun1 и т. д.)
Тип	Тип интерфейса: Внешний — интерфейс, подключаемый к сетям общего пользования
MTU	Максимальная единица передачи данных (в байтах)
Режим работы	PPPoE (Исходящий) или CDCE. Поле доступно, если сетевое устройство выведено из эксплуатации
IP-адрес	IP-адрес RAS-клиента для подключения к серверу удаленного доступа
Имя пользователя, пароль	Имя пользователя, зарегистрированного у провайдера, и его пароль (только для режима PPPoE (Исходящий))

Параметр	Описание
Регистрация	Задание правила регистрации событий в журналах. Значения: • определяется сетевым устройством (правило наследуется из свойств сетевого устройства); • первые 64 байта; • тело пакета
Имя сервиса	Имя сервиса (только для режима PPPoE (Исходящий))
Интерфейс	Название интерфейса, через который осуществляется подключение (только для режима PPPoE (Исходящий))

VLAN-интерфейсы

Комплекс поддерживает работу с виртуальными локальными сетями.

Вызов списка VLAN-интерфейсов

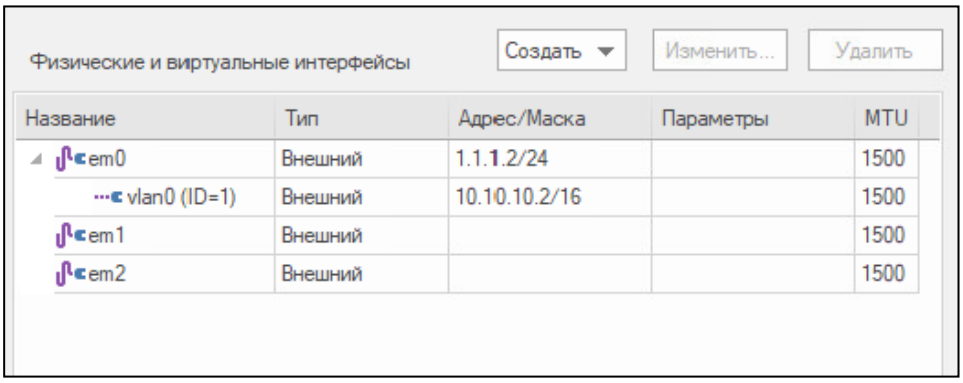
VLAN-интерфейсы отображаются в общем списке интерфейсов сетевого устройства.

Для вызова списка VLAN-интерфейсов:

1. Вызовите контекстное меню объекта с именем сетевого устройства, параметры которого требуется изменить, и активируйте команду "Свойства…".

   На экране появится окно "Свойства <сетевого устройства>".
2. Перейдите на вкладку "Интерфейсы".

   В правой части окна отобразится список интерфейсов.



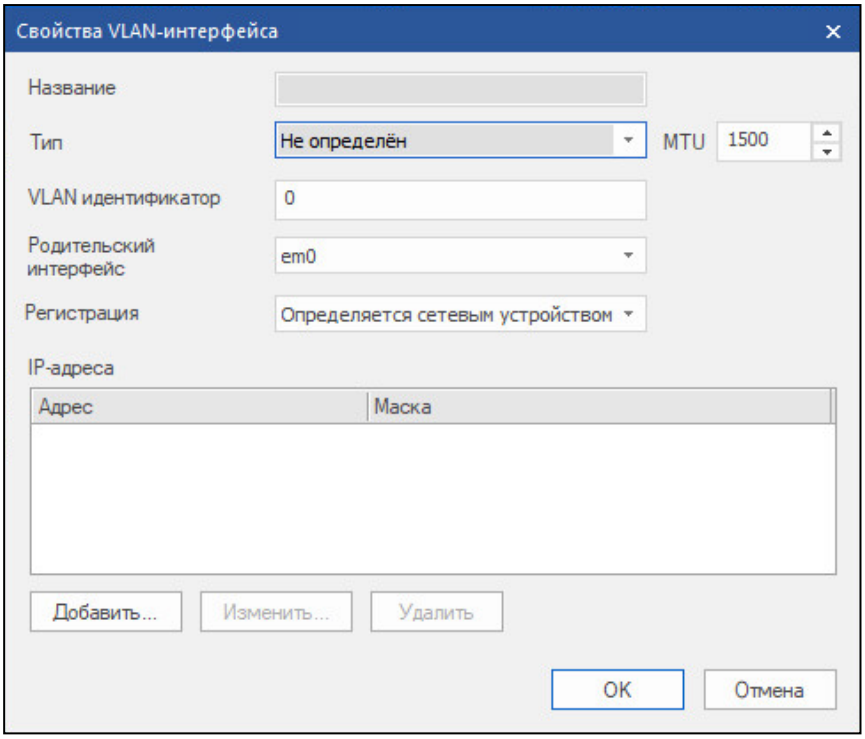
Зарегистрированные VLAN-интерфейсы отображаются с названием vlanN, где N — номер, присваиваемый при регистрации.

Регистрация нового VLAN-интерфейса

Для регистрации нового VLAN-интерфейса:

1. В списке интерфейсов нажмите кнопку "Создать" и выберите "VLAN".

   На экране появится окно "Свойства VLAN-интерфейса".



Описание параметров VLAN-интерфейса приведено на стр. **9**.

2. Укажите значения параметров VLAN-интерфейса и нажмите кнопку "OK".

   VLAN-интерфейс появится в общем списке интерфейсов сетевого устройства.

Редактирование параметров VLAN-интерфейса

Для редактирования параметров:

1. Выберите нужную запись в списке интерфейсов и нажмите кнопку "Изменить".

   На экране появится окно "Свойства VLAN-интерфейса".

2. Внесите необходимые изменения и нажмите кнопку "OK". Описание параметров приведено на стр. **9**.

Удаление VLAN-интерфейса

Для удаления VLAN-интерфейса:

- Выберите удаляемую запись в списке интерфейсов и нажмите кнопку "Удалить".

VLAN-интерфейсы на криптокоммутаторе

VLAN-интерфейсы на КК используются для обмена тегированным трафиком с устройствами, работающими по L2 и расположенными между КК и конечными устройствами (коммутаторами с транковыми портами, обращенными в сторону криптокоммутатора). При этом используется функция перенаправления трафика из одной VLAN в другую (vlan mapping).

Если транковый порт от коммутатора подключен к физическому интерфейсу криптокоммутатора с типом "Порт криптокоммутатора", поступивший кадр сразу "оборачивается" в UDP. Исходный тег в кадре в данном случае никак не модифицируется.

Если транковый порт от коммутатора подключен к физическому родительскому интерфейсу с типом "Не определен" и на данном физическом интерфейсе создан VLAN-интерфейс с типом привязки "Порт криптокоммутатора", с поступившего кадра снимается метка vlan. Далее кадр передается по туннелю.

Затем на аналогичном выходном интерфейсе в кадр добавляется метка той VLAN, которая указана на виртуальном интерфейсе парного устройства.

Внимание! Если на криптокоммутаторе локально включен режим Jumbo frame на портах коммутации, а в качестве порта КК используется VLAN-интерфейс, необходимо вручную выставлять значение MTU на родительском интерфейсе.

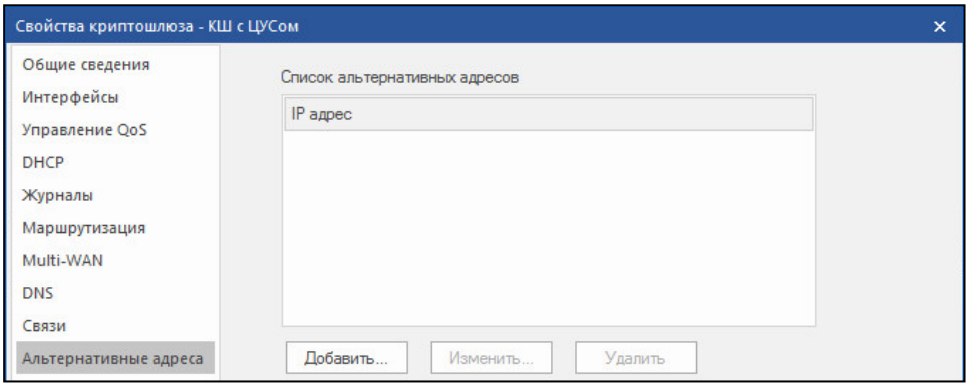
Альтернативные адреса КШ и КК

При недоступности КШ или КК сетевые устройства комплекса могут переключиться на резервный канал связи. Для этого необходимо заранее задать альтернативный IP-адрес этого КШ или КК.

Также этот параметр необходим для корректной процедуры замены IP-адреса внешнего интерфейса ЦУС.

Для назначения альтернативного адреса:

1. Вызовите меню свойств КШ или КК и перейдите на вкладку "Альтернативные адреса".



2. Сформируйте список альтернативных адресов. Для этого используйте кнопки "Добавить…", "Изменить..." и "Удалить". Затем нажмите кнопку "Применить".

   При вводе альтернативного адреса укажите протокол (IPv4 или IPv6).

   Система приступит к скрытой рассылке альтернативных адресов на сетевые устройства комплекса.
3. Нажмите кнопку "Закрыть".

Замена IP-адреса внешнего интерфейса ЦУС

Для замены IP-адреса ЦУС:

1. Назначьте альтернативный адрес ЦУС (см. выше).
2. Вызовите на экран меню свойств КШ с ЦУС и перейдите на вкладку "Интерфейсы".
3. Выберите интерфейс, IP-адрес которого требуется заменить, и нажмите кнопку "Изменить…".

   На экране появится окно "Свойства физического интерфейса".
4. Приведите список IP-адресов в требуемое состояние, используя кнопки "Добавить…", "Изменить..." и "Удалить", и нажмите кнопку "ОК".

   Изменения в адресации на выбранном интерфейсе сразу вступят в силу.
5. Для завершения настройки нажмите кнопку "ОК".

Настройка объединения интерфейсов

Для повышения надежности и пропускной способности канала целесообразно объединить несколько физических интерфейсов в один логический (LAG - Link Aggregation Group).

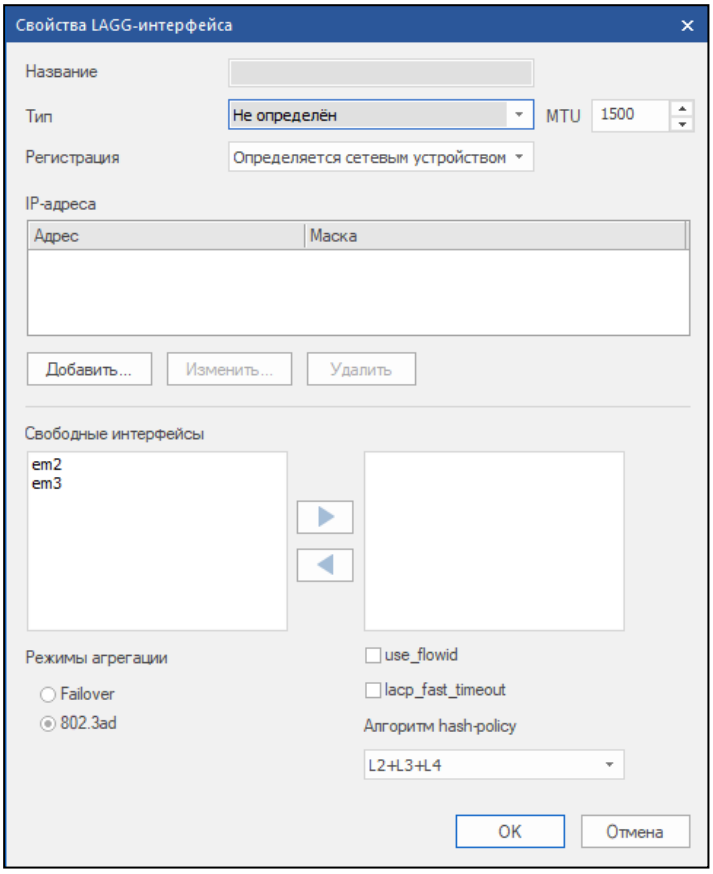
Текущая реализация поддерживает следующие режимы объединения интерфейсов (агрегации):

- Failover;
- 802.3ad.

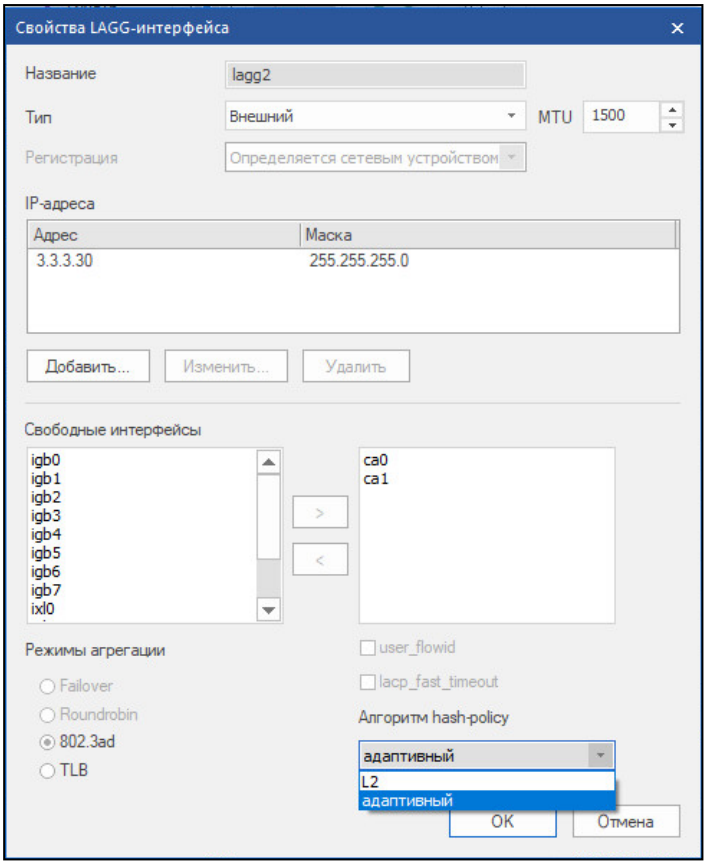
Для настройки агрегации интерфейсов:

1. На вкладке "Интерфейсы" (см. стр. 7) нажмите кнопку "Создать" и выберите тип интерфейса "LAGG".

   Появится окно настройки агрегации интерфейсов.



Внимание! Окно настройки для криптокоммутатора с криптоускорителем имеет следующий вид:



2. Задайте значения параметров.

Параметр	Описание
Название	Наименование LAGG-интерфейса. Присваивается автоматически (lagg0, lagg1 и т.д.)
Тип	Тип интерфейса: • Внешний — интерфейс, подключаемый к сетям общего пользования. • Внутренний — интерфейс, подключаемый к защищаемой сети (только для КШ). • Управление (только для ДА) – интерфейс для связи с ЦУС. • Мониторинг (только для ДА) – интерфейс , подключаемый к span-порту для анализа зеркального трафика. • Порт криптокоммутатора (только для КК) – интерфейс, используемый в составе виртуального коммутатора для создания криптографической коммутируемой сети. • Не определен — интерфейс при работе сетевого устройства не используется
MTU	Максимальная единица передачи данных (в байтах). Допустимые значения: • для КШ (внутренние и внешние интерфейсы) 576–9000; • для КК (внешний интерфейс) 576–9100. Если типом интерфейса является "порт криптокоммутатора", по умолчанию устанавливается значение 1500, которое изменять не рекомендуется
Регистрация	Задание правила регистрации событий в журналах. Значения: • определяется сетевым устройством (правило наследуется из свойств сетевого устройства); • первые 64 байта; • тело пакета

Параметр	Описание
IP-адреса	Список IP-адресов интерфейса. Для добавления нового адреса нажмите кнопку "Добавить", укажите версию IP-протокола (IPv6 используется только для внешних интерфейсов) и далее введите адрес и маску (префикс для IPv6). Для удаления выбранного IP-адреса используйте кнопку "Удалить"

3. Сформируйте список агрегируемых интерфейсов из списка свободных физических интерфейсов (с типом "не определен"), используя кнопки добавления [>] и удаления [<] интерфейса.

Примечание.
- Физические интерфейсы, на основе которых сформированы логические интерфейсы VLAN, недоступны для всех режимов агрегации.
- Настройки физических интерфейсов, добавляемых в LAGG-интерфейс, будут сброшены.
- Приоритет агрегируемых интерфейсов определяется порядком их добавления в состав LAGG-интерфейса.

4. Выберите режим агрегации. В случае выбора 802.3ad выберите режим хэширования и при необходимости дополнительные опции.

Режим	Описание
Failover	Передача трафика осуществляется через интерфейс с наивысшим приоритетом (активный), остальные интерфейсы играют роль резервных. При выходе активного интерфейса из строя трафик автоматически станет передаваться через работоспособный резервный интерфейс с наивысшим приоритетом. При восстановлении работоспособности интерфейса с наивысшим приоритетом трафик автоматически станет передаваться через него
По протоколу LACP (802.3ad)	Агрегация по протоколу LACP. Выбор интерфейса происходит по специальной формуле, в зависимости от выбранного режима хэширования: • L2 — учет MAC-адресов источника и назначения трафика; • L3 — учет IP-адресов источника и назначения трафика (обычно используется вместе с L2); • L4 — учет номеров портов источника и назначения трафика (обычно используется вместе с L3). Для криптокоммутатора с криптоускорителем доступны только два варианта: L2 и адаптивный
TLB	Только для криптокоммутатора с криптоускорителем. Режим адаптивной балансировки нагрузки передачи. Доступны два варианта: L2 и адаптивный
Опция use_flowid	Включение локального вычисления хэш-функции для RSS-хэша на интерфейсе
Опция lacp_fast_timeout	Автоматическая перенастройка значения параметра timeout на 1 секунду (быстрый тайм-аут) для передачи пакетов BPDU

Примечание. В случае агрегации по протоколу LACP необходима соответствующая настройка оборудования на другом конце агрегированного канала связи.

5. Нажмите "ОК".

   Созданный логический интерфейс появится в списке интерфейсов.

Особенности агрегации интерфейсов в кластере

В функционирующем кластере после добавления (или изменения состава существующего) агрегированного интерфейса, а также после удаления агрегированного интерфейса (или уменьшения количества интерфейсов, входящих в состав агрегированного интерфейса) необходимо выполнить следующее:

1. Выключить резервный узел.

2. Перезагрузить основной узел.
3. Включить резервный узел.

Модемное подключение и поддержка PPPoE

Подключение сетевого устройства с помощью модема возможно только к внешней сети. В качестве протокола аутентификации используется протокол CHAP. Протоколы MS-PAP и MS-CHAP не поддерживаются.

Поддерживается работа с модемами Huawei E3372 (версия прошивки — 22.323.01.00.143) и ZTE MF823D (версия прошивки — APP_IN_VERSION=PCW_COMRUSMF823DV1.0.0B01).

Добавление или удаление PPP-интерфейса, а также изменение параметра "Режим работы" возможно только в том случае, если сетевое устройство выведено из эксплуатации. После изменения режима работы необходимо выполнить инициализацию сетевого устройства.

При локальной настройке модемного подключения результаты в программе управления не отображаются.

При регистрации 3G-модема укажите для параметра "Режим работы" значение "Dialup (Исходящий)". Остальные параметры настройки модема необходимо получить у провайдера.

Внимание! При подключении КШ с ЦУС к внешней сети через PPP-интерфейс необходимо прописать выданный RAS-сервером IP-адрес в альтернативные адреса КШ с ЦУС (см. стр. **12**).

Примечание. Для установки парной связи сетевых устройств с динамическими внешними IP-адресами необходимо прописать IP-адреса, получаемые при выходе в сеть, в альтернативные адреса сетевых устройств (см. стр. **12**).

Подключение модема Huawei E3372

В данном подразделе приводится описание настроек, которые должны быть выполнены при использовании модема Huawei E3372.

Внимание!

- Модем Huawei E3372 работает только с криптошлюзами версии 3.7.6 и выше.
- Подключение модема к КШ с ЦУС не предусмотрено.
- Подключение и отключение модема выполняют только при выключенном КШ.

Ниже приведен общий порядок подключения модема и настройки сетевого устройства. Предполагается, что сетевое устройство, к которому должен быть подключен модем, не инициализировано. Порядок подключения и настройки для проинициализированного сетевого устройства приведен в конце подраздела.

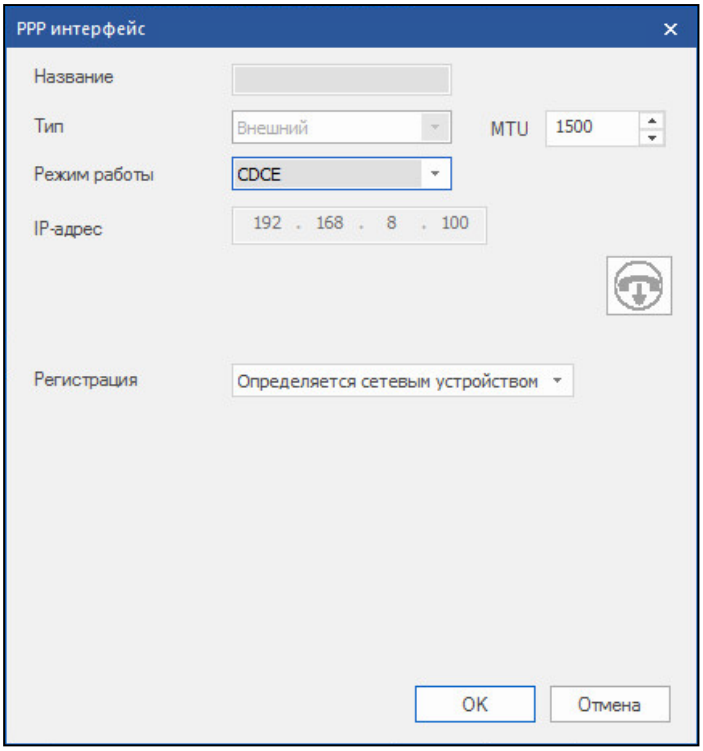
Для подключения модема и настройки сетевого устройства:

1. Зарегистрируйте сетевое устройства в ПУ ЦУС, если до этого оно не было зарегистрировано (см. [**3**]).
2. Выключите сетевое устройство и подсоедините к USB-разъему модем.
3. В ПУ ЦУС выберите в списке сетевое устройство с подключенным модемом, вызовите контекстное меню и выберите пункт "Свойства...".

   На экране появится окно свойств сетевого устройства.
4. Перейдите на вкладку "Интерфейсы" и нажмите кнопку "Создать | PPP".

   На экране появится окно "Свойства PPP-интерфейса".
5. В поле "Режим работы" укажите CDCE, выбрав его из раскрывающегося списка.

   Поле "IP-адрес" автоматически заполнится значением 192.168.8.100.



6. Нажмите кнопку "OK".

   Окно "PPP-интерфейс" закроется.

7. Задайте для сетевого устройства с модемом маршрут по умолчанию. Для этого в окне свойств сетевого устройства перейдите на вкладку "Маршрутизация" и нажмите кнопку "Добавить".

   На экране появится окно "Ввод адреса".

8. Укажите значения параметров.

Параметр	Значение
Адрес	0.0.0.0
Маска	0
Следующий узел	192.168.8.1

   Примечание. Если маршрут с таким IP-адресом уже существовал, предварительно удалите его.

   Нажмите кнопку "OK".

   Окно "Ввод адреса" закроется, и в списке появится добавленный маршрут по умолчанию.

9. Запишите конфигурацию и комплект ключей сетевого устройства на USB-флеш-накопитель (см. [**3**]).

10. Включите сетевое устройство с модемом и средствами локального управления выполните его инициализацию (см. [**3**]). При выполнении инициализации сетевого устройства загрузите конфигурацию и комплект ключей, сохраненные на USB-флеш-накопителе.

11. На вкладке "Общие сведения" окна свойств сетевого устройства установите отметку в поле "Введен в эксплуатацию". Нажмите кнопку "Применить".

Для подключения модема к ранее проинициализированному сетевому устройству:

1. На вкладке "Общие сведения" свойств сетевого устройства удалите отметку из поля "Введен в эксплуатацию", если она была установлена. Нажмите кнопку "Применить". При этом осуществится разрыв управляющего соединения ЦУС с сетевым устройством.

2. Перейдите на вкладку "Интерфейсы" и добавьте PPP- интерфейс с режимом работы CDCE (см. выше).
3. Вернитесь на вкладку "Общие сведения" и установите отметку в поле "Введен в эксплуатацию". Нажмите кнопку "Применить".
4. Сохраните конфигурацию сетевого устройства на USB-флеш-накопителе (см. [**3**]).
5. Выключите сетевое устройство и подсоедините к USB-разъему модем.
6. Включите сетевое устройство, перейдите к режиму настройки сетевого устройства и в меню "Управление" выполните загрузку конфигурации, сохраненной на USB-флеш-накопителе (см. [**3**]).

Подключение и настройка 3G-модема

Подключение 3G-модема предполагает использование КШ для парной связи с КШ, установленным в головном или центральном офисе и имеющим белый статический адрес. При этом скорость передачи данных и качество связи в значительной степени зависят от таких факторов, как мощность радиосигнала, удаленность от базовой станции, помехи, создаваемые промышленным оборудованием, и пр.

Внимание! В ПУ ЦУС КШ с 3G-модемом могут отображаться как "КШ за symmetric-NAT". Создать парные связи между такими КШ нельзя.

Далее приведены примеры подключения к КШ 3G-модема в зависимости от состояния криптошлюза и условий его работы.

Рассматриваются два варианта:

Вариант 1. КШ введен в эксплуатацию и в ПУ ЦУС в списке отображается со статусом "Включен".

Вариант 2. КШ зарегистрирован в ПУ ЦУС, но не проинициализирован и не введен в эксплуатацию. В ПУ ЦУС КШ отображается со статусом "Выключен".

Для подключения и настройки 3G-модема (вариант 1):

1. Вызовите окно свойств КШ, снимите отметку в поле "Введен в эксплуатацию" и нажмите кнопку "Применить".
2. Перейдите на вкладку "Интерфейсы", создайте новый PPP-интерфейс (см. стр. **7**).

   На экране появится окно настроек PPP-интерфейса.
3. В поле "Режим работы" выберите из раскрывающегося списка значение "PPPoE (Исходящий)".
4. В полях "Имя пользователя" и "Пароль" укажите значения, предоставленные провайдером.
5. Заполните остальные параметры PPP-интерфейса (см. стр. **9**) и нажмите кнопку "ОК".
6. Перейдите на вкладку "Общие сведения", установите отметку в поле "Введен в эксплуатацию" и нажмите кнопку "Применить".
7. Подключите 3G-модем к USB-порту КШ.
8. Перезагрузите КШ средствами ПУ ЦУС или средствами локального управления (см. [**2**]).

Для подключения и настройки 3G-модема (вариант 2):

1. Выполните пп. **1**–**5** процедуры варианта 1 (см. выше).
2. Запишите конфигурацию КШ на внешний носитель.
3. Выполните локально инициализацию КШ (см. [**3**]). При выполнении процедуры инициализации используйте внешний носитель с конфигурацией, записанной при выполнении п. **2**.
4. После завершения процедуры инициализации отключите внешний носитель и подключите 3G-модем к USB-порту КШ.

5. В ПУ ЦУС вызовите окно свойств КШ, установите отметку в поле "Введен в эксплуатацию" и нажмите кнопку "ОК".

Локальная настройка модемного подключения КШ

Данную процедуру выполняют для ликвидации нештатной ситуации, когда после настройки модемного подключения средствами централизованного управления связь между ЦУС и КШ установить не удалось.

Предварительно следует настроить модемное подключение централизованно в ПУ ЦУС (см. стр. **18**).

Модемное подключение не предусмотрено для ЦУС и КШ с установленным сервером доступа.

Для настройки режима PPPoE:

1. Перейдите к меню локальной настройки параметров сетевого устройства (см. стр. **59**).

```
1: Сохранение конфигурации
2: Загрузка конфигурации
3: Изменение адреса активного ЦУС
4: Настройка PPPoE-соединений
5: Настройка шифрования
6: Настройка фрагментации
7: Настройка коммутации
8: Настройка отладочного журнала
9: Настройка доступа удаленного терминала
10: Настройка режима ретранслятора DHCP (replace)
11: Выключение Agent relay information (опции 82) на DHCP-ретрансляторе
12: Установить ПО криптоускорителя
0: Выход
Выберите пункт меню (0 - 12):
```

2. Введите в строке ввода номер команды "Настройка PPPoE-соединений" и нажмите клавишу <Enter>.

   На экране появится сообщение:

```
Задан режим PPPoE
Доступные интерфейсы: <перечень интерфейсов>
Название интерфейса, через который осуществляется подключение:
```

3. Введите название интерфейса и нажмите клавишу <Enter>.

   На экране появится сообщение:

```
Имя сервиса (пустое - любой):
```

4. При необходимости введите имя сервиса и нажмите клавишу <Enter>.

   На экране появится сообщение:

```
Имя пользователя:
```

5. Введите имя пользователя и нажмите клавишу <Enter>.

   На экране появится сообщение:

```
Пароль:
```

6. Введите пароль и нажмите клавишу <Enter>.

   На экране появится меню управления.

7. Перейдите к настройке следующего параметра или выйдите из меню.

Изменение адреса подключения к ЦУС

Данная процедура выполняется средствами локального управления для ликвидации нештатной ситуации, когда по каким-либо причинам связь между сетевым устройством и ЦУС установить не удалось.

Предварительно необходимо задать адрес сетевого устройства централизованно в программе управления ЦУС (см. стр. **12**).

Изменение внешнего адреса возможно только при отключенном режиме динамической маршрутизации.

Для изменения адреса подключения к ЦУС:

1. Перейдите к меню локальной настройки параметров сетевого устройства (см. стр. **59**).
2. Введите в строке ввода номер команды "Изменение адреса активного ЦУС" и нажмите клавишу <Enter>.

   На экране появится запрос на ввод нового IP-адреса ЦУС.
3. Введите IP-адрес ЦУС и нажмите клавишу <Enter>.

   На экране появится меню управления.
4. Введите в строке ввода номер команды "Выход" и нажмите клавишу <Enter>, чтобы завершить процедуру.

Глава 2
Управление режимами работы сетевого устройства

Настройка Multi-WAN

Данные настройки предоставляют возможность сконфигурировать сеть при одновременном подключении КШ или КК к нескольким внешним сетям. Имеются следующие режимы Multi-WAN:

- передача трафика в соответствии с таблицей маршрутизации;
- обеспечение отказоустойчивости канала связи;
- балансировка трафика между внешними интерфейсами КШ или КК.

Настройку режимов и каналов выполняют на вкладке "Multi-WAN" окна свойств сетевого устройства.

Примечание. Для сетевого устройства с включенным режимом динамической маршрутизации данная функция не поддерживается.

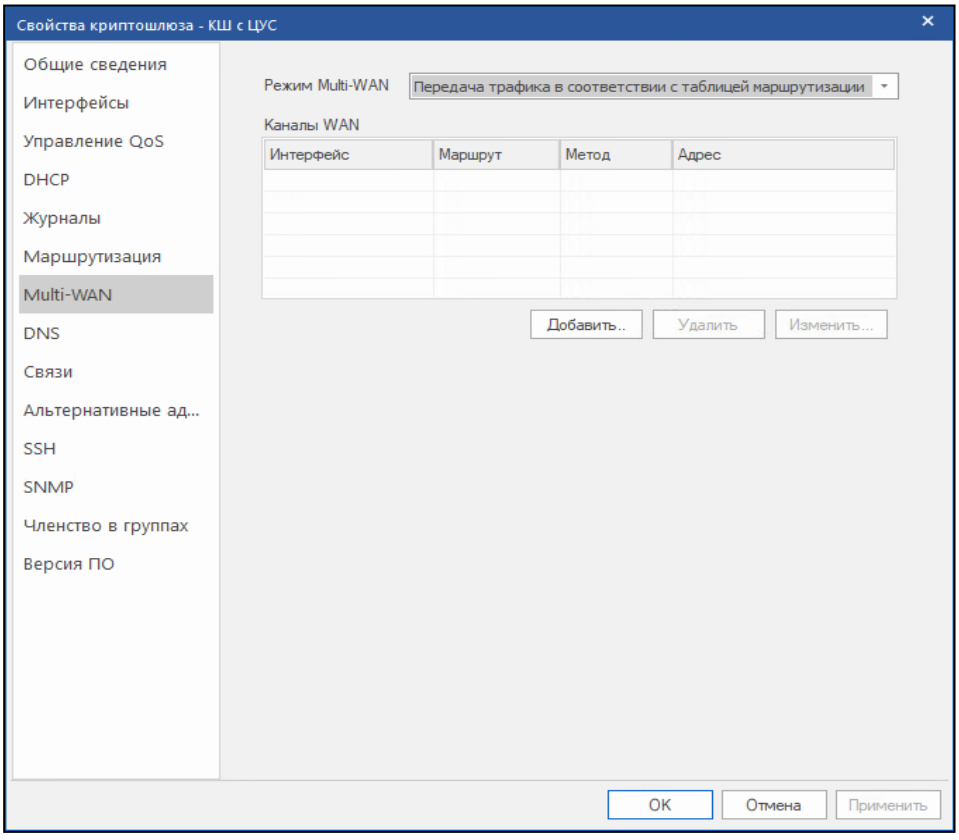
Настройка режима Multi-WAN

Перечень внешних каналов связи формируют на вкладке "Multi-WAN" окна свойств сетевого устройства. На этой вкладке выбирают нужный режим Multi-WAN, от этого зависят прочие поля настроек. Режим по умолчанию — "Передача трафика в соответствии с таблицей маршрутизации".

Для формирования перечня каналов связи и выбора режима:

1. В окне свойств сетевого устройства выберите вкладку "Multi-WAN".

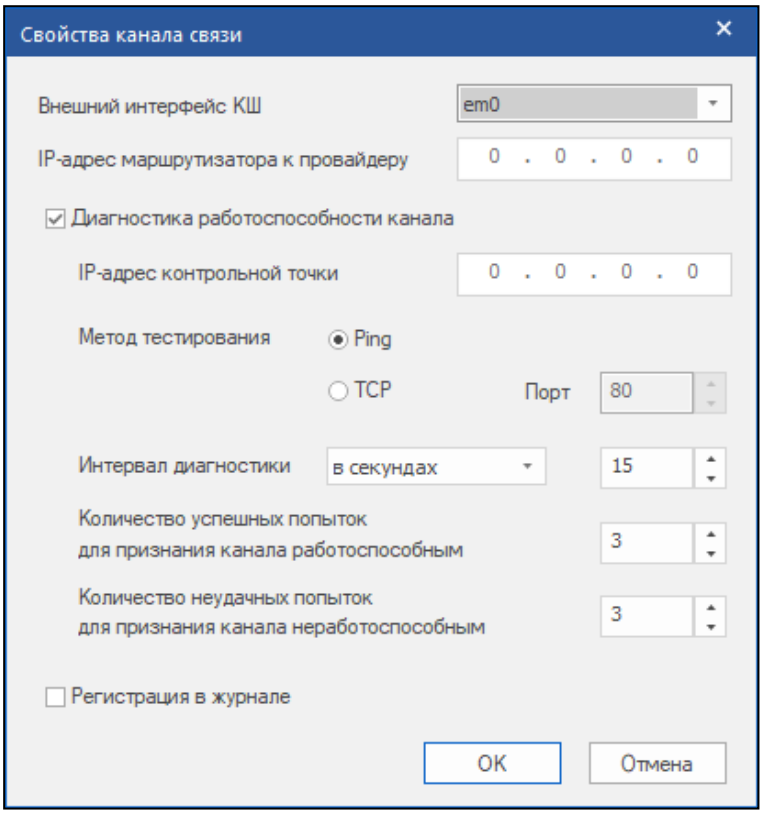
   В правой части окна отобразятся настройки Multi-WAN: наименование режима и список каналов WAN (если он был сформирован).



2. Сформируйте перечень используемых внешних каналов. Для формирования списка используйте кнопки:

Добавить...	Вызывает на экран окно "Свойства канала связи" для создания в списке новой записи
Удалить	Удаляет из списка выбранную запись
Изменить...	Вызывает на экран окно "Свойства канала связи" для редактирования выбранной записи

При добавлении или изменении записи открывается окно "Свойства канала связи".



3. Укажите параметры и нажмите кнопку "OK".

Параметр	**Описание**
Внешний интерфейс сетевого устройства	Наименование настраиваемого интерфейса сетевого устройства
IP-адрес маршрутизатора к провайдеру	IP-адрес маршрутизатора, обеспечивающий связь с внешней сетью. Маршрутизатор должен находиться в той же сети, к которой подключен настраиваемый интерфейс
Диагностика работоспособности канала	Включает режим диагностики работоспособности канала. При отключенной диагностике канал будет считаться безусловно доступным
IP-адрес контрольной точки	IP-адрес хоста во внешней сети, наличие соединения с которым будет проверяться
Метод тестирования	• Ping — проверка доступности контрольной точки с помощью команды ping. • TCP — проверка доступности контрольной точки по протоколу TCP. Необходимо указать порт, через который будет устанавливаться соединение
Интервал диагностики	Промежуток времени в секундах или миллисекундах между попытками установления соединения с контрольной точкой

Параметр	Описание
Количество успешных попыток для признания канала работоспособным	Количество последовательных успешных попыток установления соединения с контрольной точкой после восстановления работоспособности канала для присвоения каналу статуса "работоспособный"
Количество неудачных попыток для признания канала неработоспособным	Количество неудачных попыток установления соединения с контрольной точкой для присвоения каналу статуса "неработоспособный"
Регистрация в журнале	При наличии отметки в системном журнале регистрируются события, связанные с изменением статуса канала

4. В поле "Режим Multi-WAN" выберите в раскрывающемся списке нужный режим.

Передача трафика в соответствии с таблицей маршрутизации	Не требует дополнительной настройки
Обеспечение отказоустойчивости канала связи	См. стр. 24
Балансировка трафика между внешними интерфейсами КШ	См. стр. 25

5. Нажмите кнопку "OK".

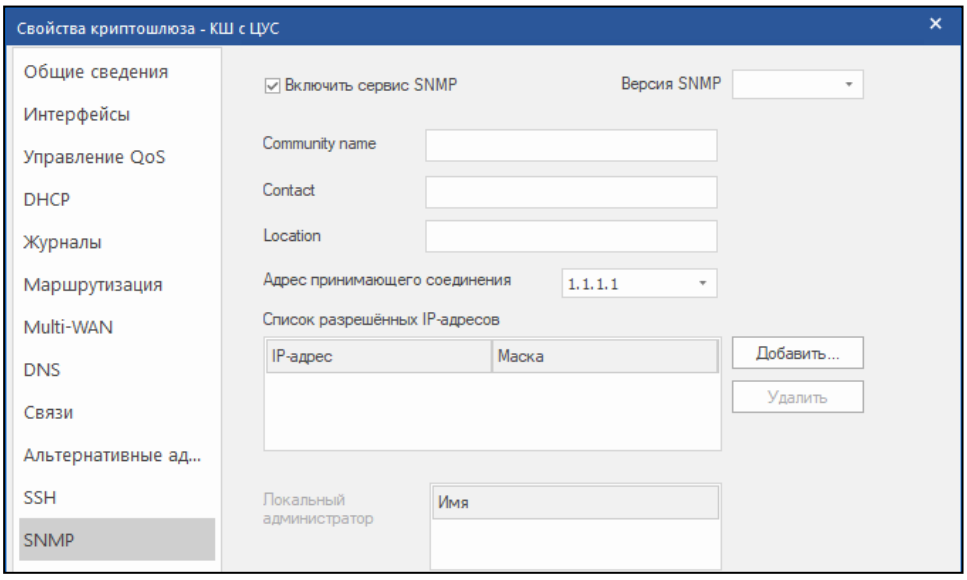
Для выключения режима:

- В окне свойств сетевого устройства выберите вкладку "Multi-WAN", удалите все каналы из списка, выберите режим "Передача трафика в соответствии с таблицей маршрутизации" и нажмите кнопку "OK".

Внимание! После изменения состава интерфейсов, используемых в качестве внешних каналов (каналы WAN), для получения корректных данных о них по SNMP необходимо перезапустить сервис SNMP.

Для перезапуска сервиса SNMP:

1. В окне свойств сетевого устройства перейдите на вкладку "SNMP" и удалите отметку в поле "Включить сервис SNMP".

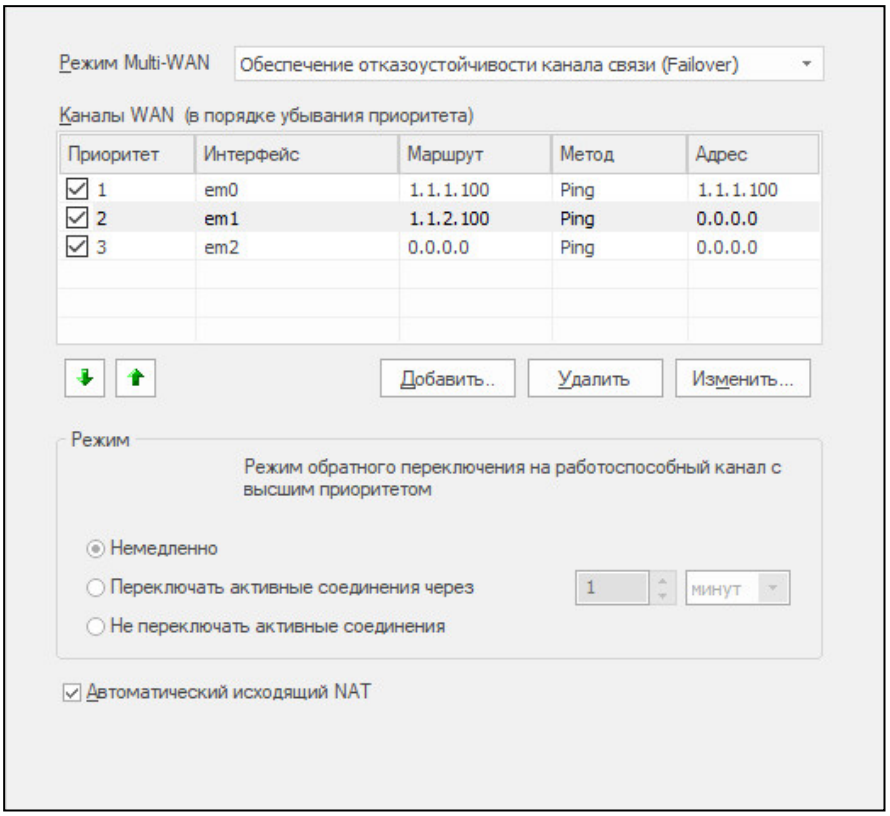


2. Сохраните изменения и затем повторно установите отметку.

Обеспечение отказоустойчивости канала связи

Для настройки режима обеспечения отказоустойчивости:

1. Сформируйте перечень каналов (см. стр. 21) и выберите режим "Обеспечение отказоустойчивости канала связи".



2. Укажите приоритет каналов. Для этого используйте кнопки со стрелками слева под списком каналов.

Примечание. Кнопки со стрелками перемещают выбранную запись в списке на одну позицию в выбранном направлении.

Последовательность записей в списке соответствует приоритету данного канала.

Удаление отметки в левой части записи отключает использование данного канала без удаления записи из списка.

3. Выберите режим обратного переключения на работоспособный канал:

Немедленно	Обратное переключение на канал с более высоким приоритетом будет выполнено немедленно после восстановления его работоспособности независимо от наличия активных соединений
Переключать активные соединения через	Обратное переключение на канал с более высоким приоритетом будет выполнено через указанное время после восстановления работоспособности канала
Не переключать активные соединения	Обратное переключение на канал с более высоким приоритетом будет выполнено после закрытия всех активных соединений

Внимание! Данная настройка распространяется только на открытый трафик с контролем состояния соединения.

4. Для автоматического создания правил трансляции, которые для всего исходящего трафика подменяют адрес отправителя на адрес активного в

данный момент внешнего интерфейса, установите отметку в поле "Автоматический исходящий NAT".

5. Нажмите кнопку "OK" или "Применить".

Примечание. При переключении между WAN-каналами в качестве шлюза по умолчанию автоматически устанавливается маршрутизатор, заданный в настройках свойств канала. Для просмотра текущего значения IP-адреса маршрутизатора используется команда "Вывести таблицы маршрутизации" дополнительного меню локального управления сетевым устройством. В таблице IP-адрес маршрутизатора отображается как шлюз по умолчанию.

Рекомендуется отключать тестирование на наименее приоритетном канале.

Балансировка трафика между внешними интерфейсами сетевого устройства

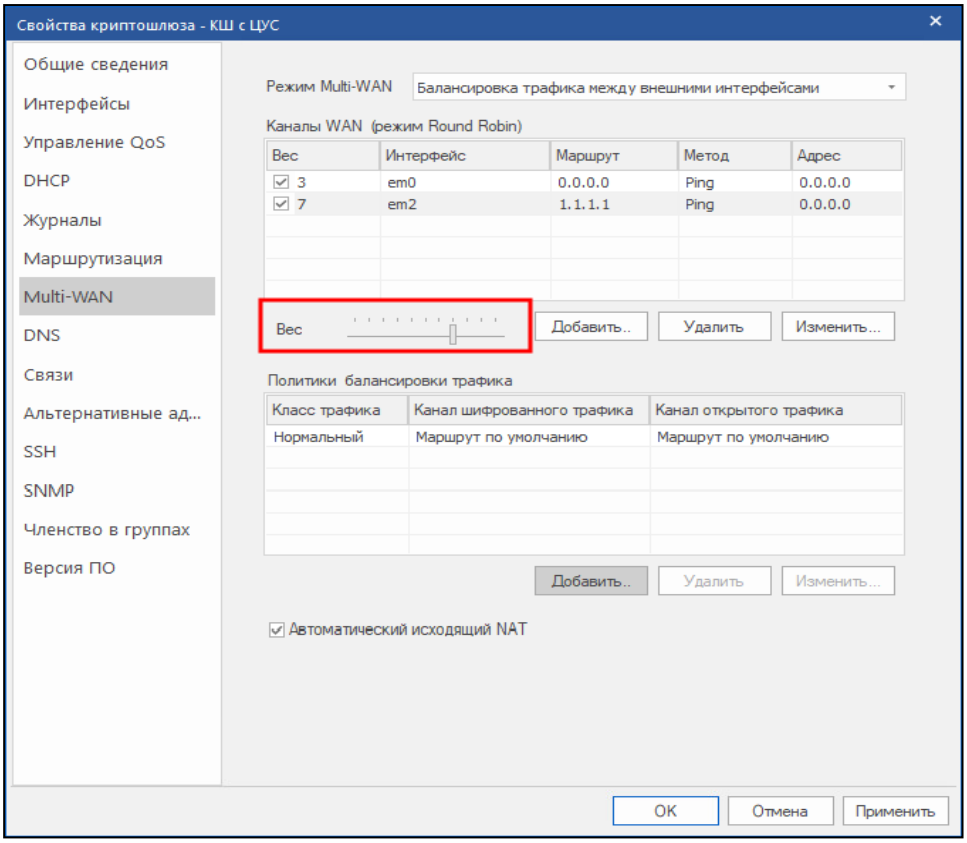
В режиме балансировки трафика распределение нагрузки на внешние интерфейсы осуществляется в соответствии с назначенными для внешних каналов весами.

Вес канала — количество последовательных соединений для данного класса исходящего трафика. По достижении заданного количества соединений исходящий трафик перенаправляется на другой внешний канал. Вес канала может составлять от 0 до 10.

Примечание. При установке веса канала равным 0 и при наличии каналов с весом больше 0 открытый трафик будет перенаправляться в эти каналы (режим round robin), минуя канал с весом 0, и будет распределяться согласно их весам. Если активен только канал с весом 0, трафик будет направлен в этот канал. При активности нескольких каналов с весом 0 трафик будет последовательно распределяться между этими каналами.

Для настройки режима балансировки нагрузки:

1. Сформируйте перечень каналов и выберите режим "Балансировка трафика между внешними интерфейсами <сетевого устройства>" (см. стр. **21**).
2. В поле "Каналы WAN" укажите вес канала. Вес выбранного канала устанавливают с помощью ползунка, расположенного слева под списком каналов.



Удаление отметки в левой части записи отключает использование данного канала без удаления записи из списка.

3. В области "Политики балансировки трафика" сформируйте перечень правил распределения трафика. Для формирования списка используйте кнопки:

Добавить...	Вызывает на экран окно "Параметры политики балансировки трафика" для создания в списке новой записи
Удалить	Удаляет из списка выбранную запись
Изменить...	Вызывает на экран окно "Параметры политики балансировки трафика" для редактирования выбранной записи

Параметры политики:

Класс трафика	Зарегистрированный в справочнике класс трафика (см. стр. **52**)
Канал WAN для передачи шифрованного трафика	Внешний канал для передачи зашифрованного трафика
Канал WAN для передачи открытого трафика	• Внешний канал для передачи открытого трафика. • Режим Round Robin (распределение трафика между каналами в соответствии с их весами)

4. При необходимости установите отметку в поле "Автоматический исходящий NAT". При наличии отметки автоматически создаются правила трансляции, которые для всего исходящего трафика подменяют адрес отправителя на адрес указанного в настройках балансировки внешнего интерфейса. Правила трансляции, заданные администратором, отменяются.
5. Нажмите кнопку "Применить" и перейдите на вкладку "Маршрутизация".
6. Укажите маршрут к ЦУС и нажмите кнопку "ОК".

Внимание! Если политики балансировки трафика не заданы, трафик на внешних интерфейсах будет распределяться в соответствии с настройками маршрутизации.

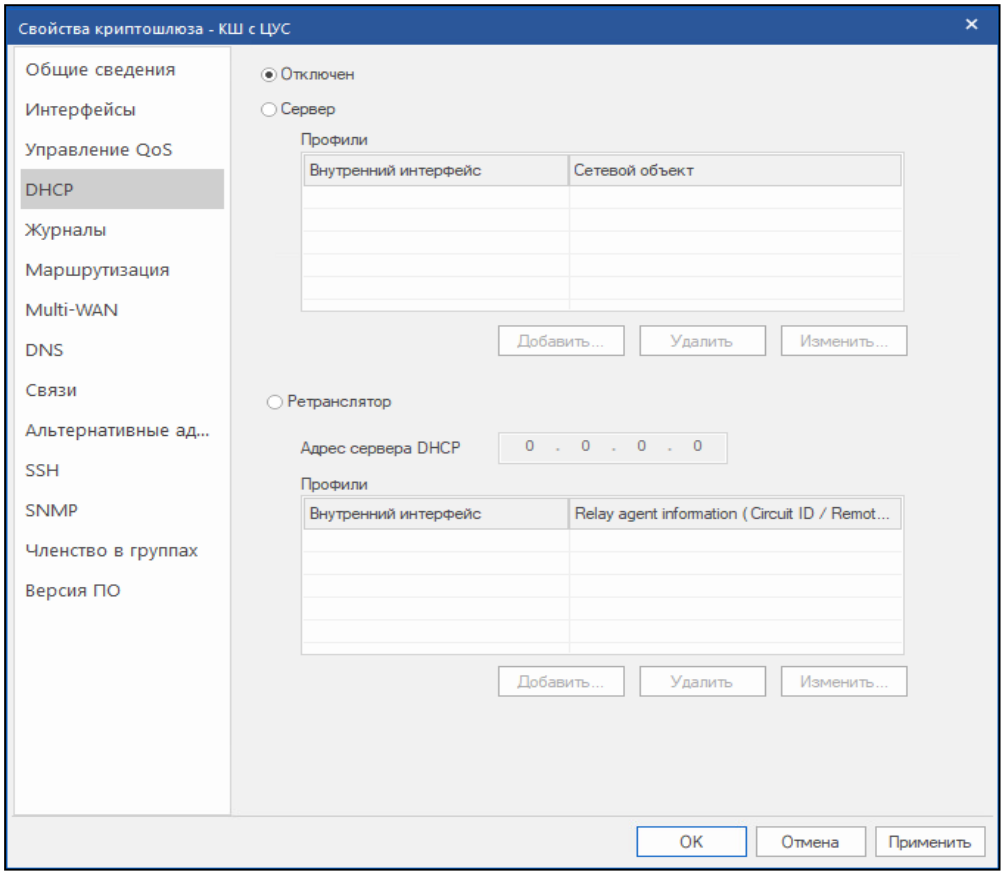
Настройки сервиса DHCP

По умолчанию после установки и инициализации КШ сервис DHCP отключен.

Настройки сервиса DHCP на КШ выполняют в окне "Свойства криптошлюза" на вкладке "DHCP".

На вкладке отображается установленный для данного устройства один из трех возможных режимов работы сервиса DHCP:

- Отключен;
- Сервер;
- Ретранслятор.



При установленном режиме "Сервер" доступна настройка списка профилей DHCP (см. ниже). Профиль сервера — это пара "внутренний интерфейс – сетевой объект", для которой администратором заданы параметры сервиса DHCP. При задании параметров можно использовать DHCP-опции (как стандартные, так и пользовательские).

При установленном режиме "Ретранслятор" доступна настройка IP-адреса сервера DHCP и профилей ретранслятора DHCP (см. стр. **33**). Профиль ретранслятора — это внутренний интерфейс сетевого устройства, на котором должен работать сервис, и соответствующий данному интерфейсу параметр Relay agent information, включающий в себя два компонента: RemoteID и Circuit ID.

Включение и настройка режима сервера

Настройка DHCP-сервера заключается в задании списка профилей (см. выше). В профиле указываются значения его основных параметров. Кроме этого могут быть дополнительно заданы DHCP-опции.

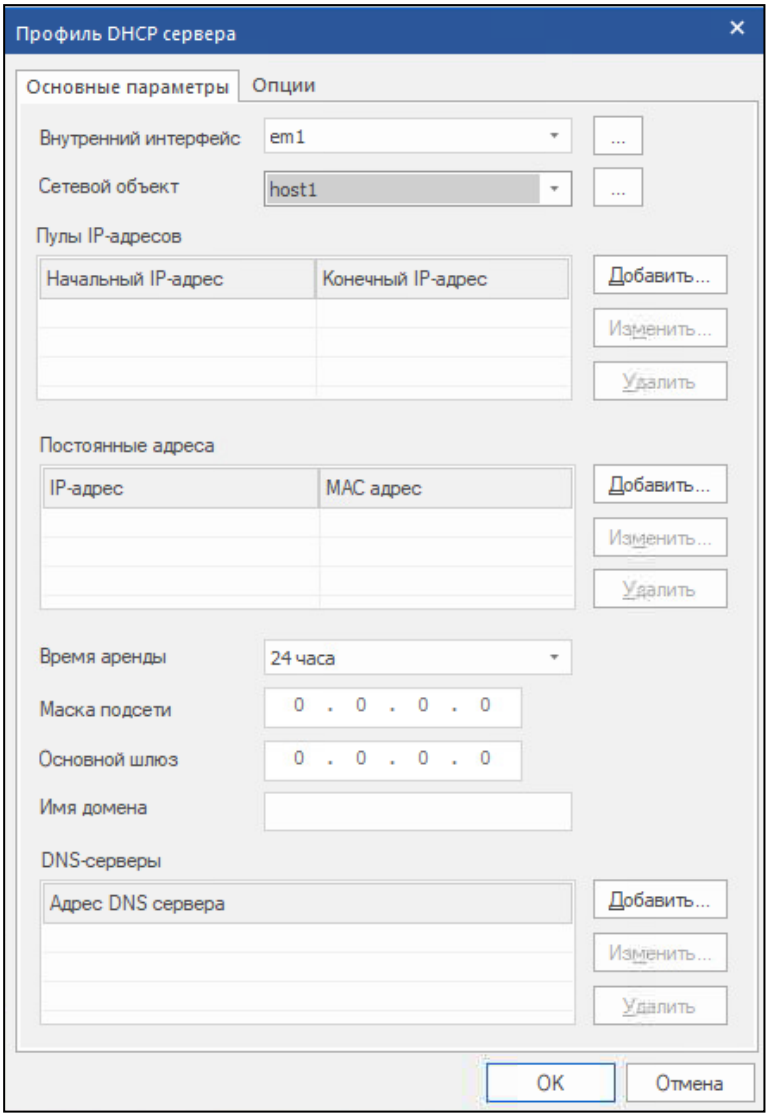
Для включения и настройки:

1. На вкладке "DHCP" окна свойств КШ установите отметку в поле "Сервер".

Станут доступны кнопки управления списком профилей.

2. Для добавления нового профиля нажмите кнопку "Добавить".

   На экране появится окно "Профиль DHCP-сервера", состоящее из двух вкладок: "Основные параметры" и "Опции".



3. Заполните поля параметров на вкладке "Основные параметры".

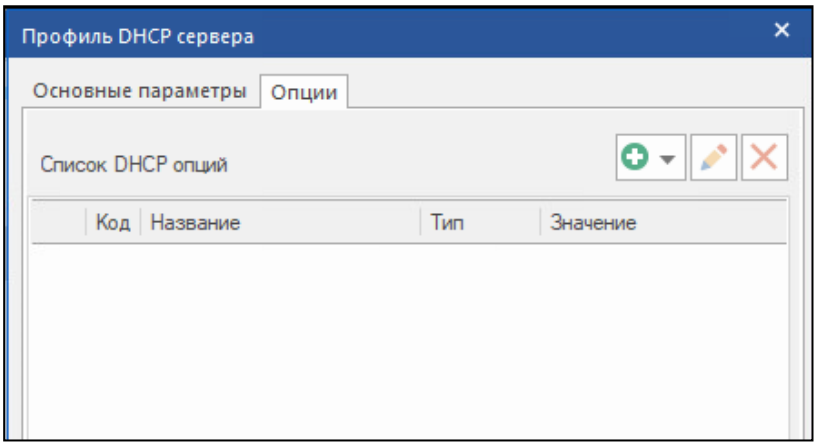
Основные параметры	
Внутренний интерфейс	Внутренний интерфейс сетевого устройства, на котором должен работать DHCP-сервер. Для выбора внутреннего интерфейса из детализированного списка используйте кнопку, расположенную справа
Сетевой объект	Сетевой объект, привязанный к указанному внутреннему интерфейсу, который должен ограничивать область раздачи адресов. Для выбора объекта из детализированного списка используйте кнопку, расположенную справа. При выборе из детализированного списка можно выбрать объект и просмотреть его свойства, нажав соответствующую кнопку
Пулы IP-адресов	Один или несколько диапазонов адресов, ограниченные начальным и конечным IP-адресом
Постоянные адреса	Назначаемые вручную постоянные IP-адреса, не входящие в указанные пулы адресов и привязанные к MAC-адресам
Время аренды	По умолчанию 24 часа

Основные параметры	
Маска подсети	В маску должны попадать пулы адресов и маршрутизатор
Основной шлюз	IP-адрес шлюза не должен попадать в пулы адресов
Имя домена	Необязательный параметр
DNS-серверы	Адреса DNS-серверов

- Если использование опций DHCP не требуется, перейдите к п. **16**.
- Если требуется использование опций DHCP, перейдите на вкладку "Опции".

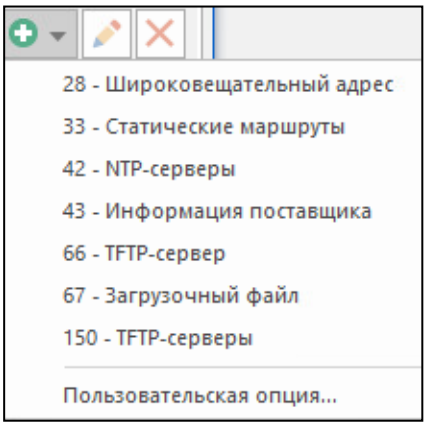
  Внимание! Если заданы DHCP-опции, параметры, указанные в них, имеют более высокий приоритет по сравнению с основными параметрами.

  На вкладке представлен список опций, используемых в данном профиле. Если опции в профиль не добавлялись, список будет пустым.



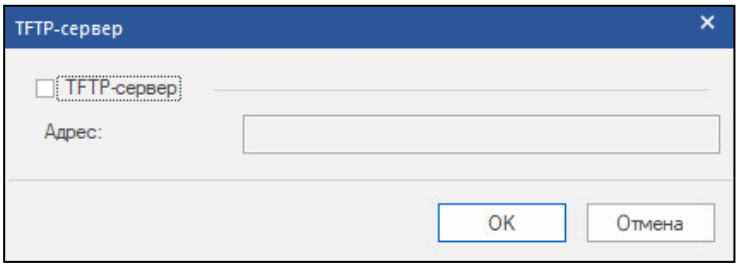
4. Для добавления опции нажмите кнопку "Создать новую опцию".

Откроется список стандартных опций (не полный) и ссылка "Пользовательская опция".

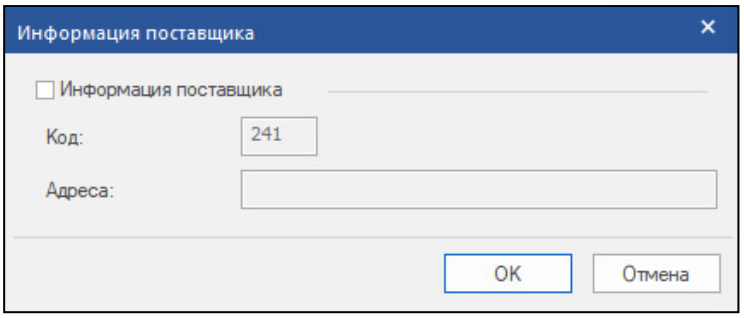


5. Выберите опцию из списка.

Откроется окно задания значения параметра опции. Вид и содержание окна зависит от выбранной опции, например



или



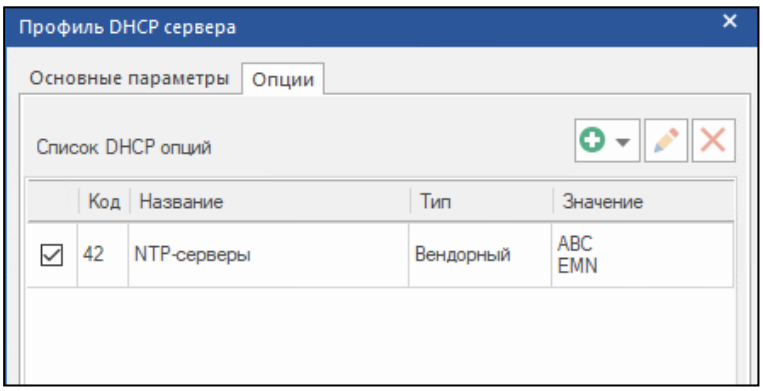
Если требуется добавить стандартную опцию, отсутствующую в списке, или создать пользовательскую опцию, перейдите к п. **9**.

6. Установите отметку у названия опции.

   Станут доступными поля для ввода значений параметров опции.

7. Введите значение и нажмите кнопку "OK".

   Опция добавится в список DHCP-опций профиля.



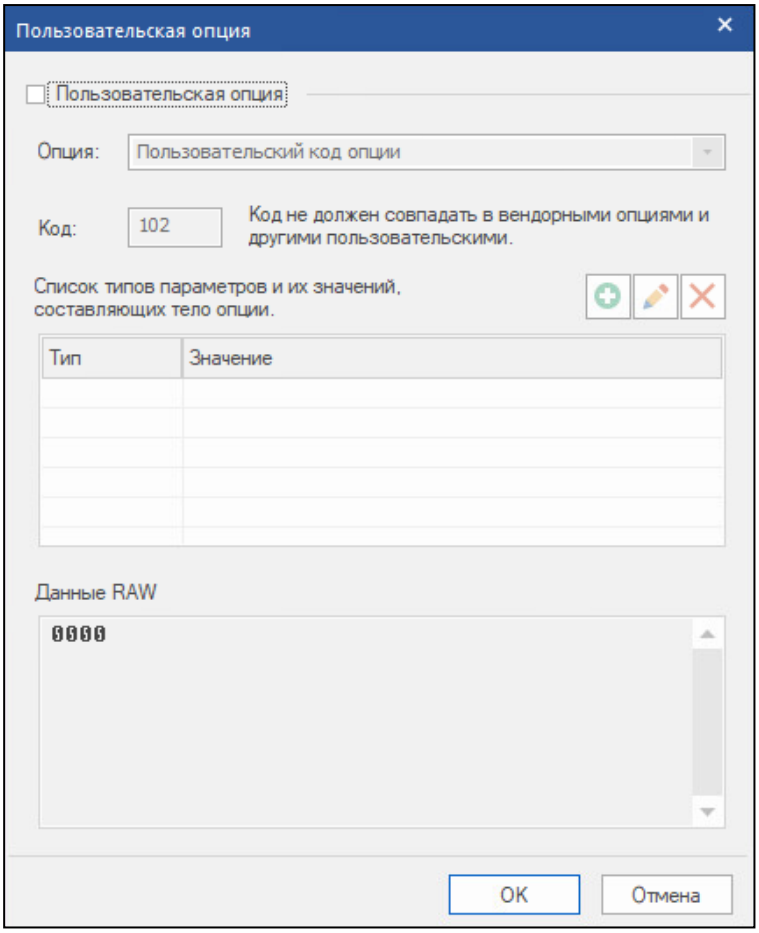
Для каждой опции в списке приводится следующая информация:

- код;
- название;
- тип (вендорный или пользовательский);
- значение.

По умолчанию у добавленной опции установлена отметка, означающая, что опция активна.

8. Для добавления в профиль других опций повторите пп. **4**–**7**.
9. Для добавления стандартной опции, отсутствующей в списке, или создания пользовательской опции нажмите ссылку "Пользовательская опция...".

   На экране появится окно "Пользовательская опция".



10. Установите отметку "Пользовательская опция".

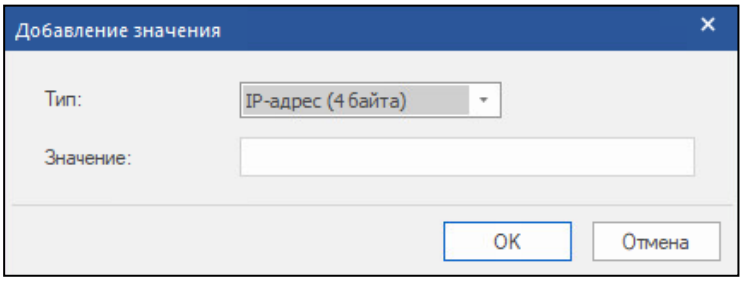
Станут доступны настройки параметров опции.

11. В поле "Опция" введите название опции или выберите опцию из раскрывающегося списка.

Если опция выбирается из списка, поле "Код" будет заполнено автоматически. Если название опции вводится вручную, введите код. Код не должен совпадать с вендорными опциями и другими пользовательскими.

12. Добавьте параметр. Для этого нажмите кнопку "Добавить новый параметр опции".

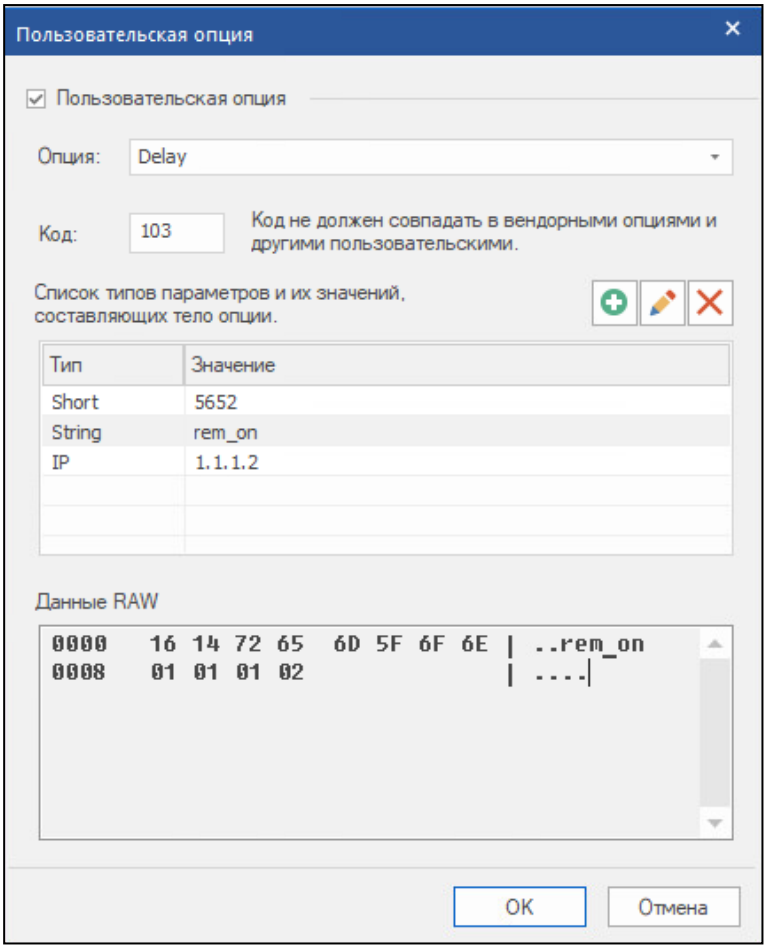
Появится окно задания типа параметра и его значения.



13. Выберите тип параметра, укажите значение и нажмите кнопку "OK".

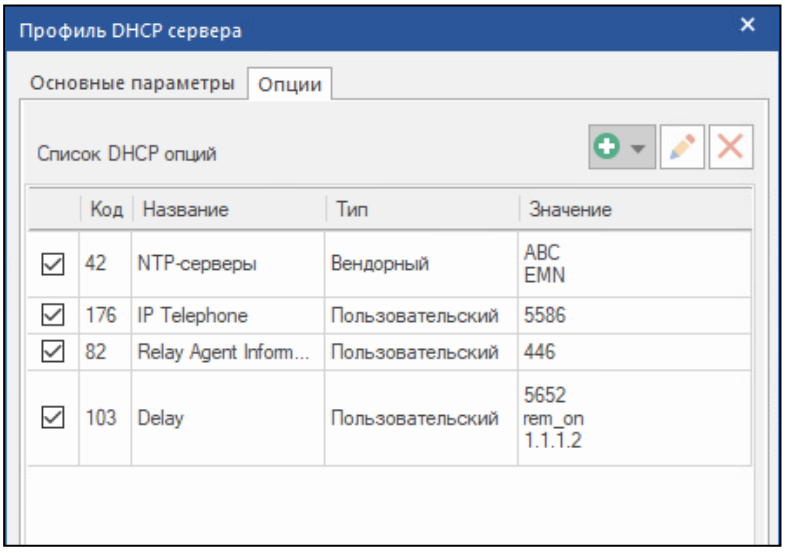
Параметр добавится в опцию.

При необходимости добавьте другие параметры.

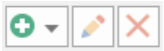


14. Нажмите кнопку "OK".

Пользовательская опция добавится в общий список опций профиля.



15. Добавьте в список все необходимые опции. Для редактирования списка опций используйте кнопки:



16. Нажмите кнопку "OK" в нижней части окна "Профиль DHCP-сервера".

Профиль будет добавлен в настройки DHCP-сервера.

17. Для редактирования списка профилей используйте кнопки "Добавить...", "Удалить" и "Изменить...".
18. Для сохранения изменений и завершения настройки нажмите кнопку "OK".

Включение и настройка ретранслятора

Настройка ретранслятора включает в себя:

- Задание профилей.

  Профиль задается для каждого внутреннего интерфейса КШ, на котором должен действовать DHCP-сервис. Настройка выполняется в ПУ ЦУС.
- Задание режима работы ретранслятора при передаче DHCP-серверу запросов, поступающих от клиента.

  Предусмотрены следующие режимы:
  - replace;
  - append;
  - forward;
  - discard.

  Настройка выполняется средствами локального управления КШ.
- Включение/выключение на ретрансляторе опции 82 при передаче ответа клиенту от DHCP-сервера.

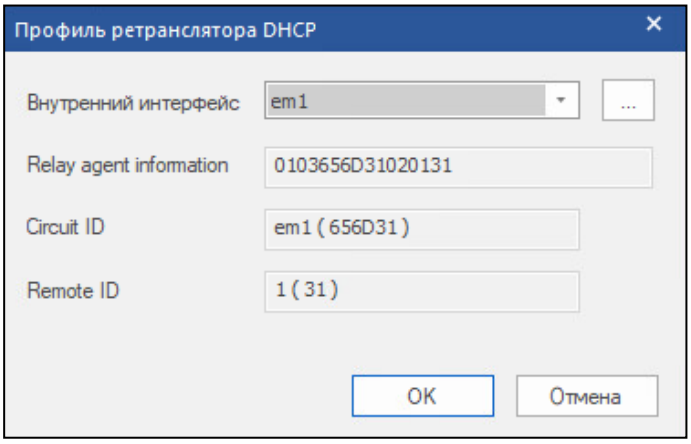
  Настройка выполняется средствами локального управления КШ.

Для включения и задания профилей:

1. На вкладке "DHCP" окна свойств КШ установите отметку в поле "Ретранслятор".

   Станут доступны поле "Адрес сервера DHCP" и кнопки управления списком профилей ретранслятора.
2. В поле "Адрес сервера DHCP" введите IP-адрес сервера, на который сетевое устройство будет перенаправлять запросы клиентов.
3. Для добавления нового профиля нажмите кнопку "Добавить".

   На экране появится окно "Профиль ретранслятора DHCP".



4. Заполните поля параметров. Для выбора внутреннего интерфейса из детализированного списка используйте кнопку, расположенную справа.

   Внимание! Для корректной работы DHCP-ретранслятора выбираемый внутренний интерфейс должен иметь не более одного IP-адреса (см. стр. 7).

   После выбора внутреннего интерфейса остальные поля профиля заполняются автоматически.
5. Нажмите кнопку "OK".

   Окно "Профиль ретранслятора DHCP" закроется, и на вкладке "DHCP" в списке появится новый профиль ретранслятора.

6. При необходимости добавления профиля для другого внутреннего интерфейса выполните пп. **3**–**5**.
   - Для изменения адреса сервера DHCP введите в соответствующем поле его IP-адрес.
   - Для редактирования списка профилей используйте кнопки "Добавить", "Удалить" и "Изменить".
7. Для сохранения изменений и завершения настройки нажмите кнопку "OK".

Внимание! После включения режима ретранслятора настройки для режима сервера DHCP будут сброшены.

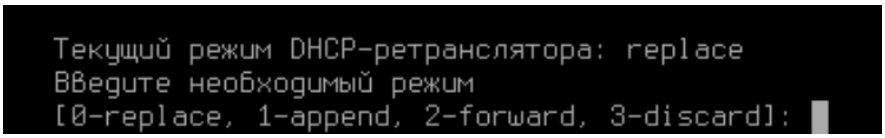
Для задания режима работы ретранслятора:

1. Перейдите к меню локальной настройки параметров КШ (см. стр. **59**).

```
1: Сохранение конфигурации
2: Загрузка конфигурации
3: Изменение адреса активного ЦУС
4: Настройка PPPoE-соединений
5: Настройка шифрования
6: Настройка фрагментации
7: Настройка коммутации
8: Настройка отладочного журнала
9: Настройка доступа удаленного терминала
10: Настройка режима ретранслятора DHCP (replace)
11: Выключение Agent relay information (опции 82) на DHCP-ретрансляторе
12: Установить ПО криптоускорителя
0: Выход
Выберите пункт меню (0 - 12):
```

2. Введите номер команды "Настройка режима ретранслятора DHCP" и нажмите клавишу <Enter>.

   На экране отобразится текущий режим DHCP-ретранслятора.



3. Для изменения режима введите соответствующий ему номер (0-3) и нажмите клавишу <Enter>.

   В меню локальной настройки параметров КШ у команды "Настройка режима ретранслятора DHCP" отобразится новый режим.

Для включения/выключения опции 82:

- В меню локальной настройки введите номер команды "Включение/выключение Agent relay information (опции 82) на DHCP- ретрансляторе" и нажмите клавишу <Enter>.

  Название команды изменится на обратное.

Отключение сервиса DHCP

Для отключения сервиса:

1. На вкладке "DHCP" окна свойств КШ установите отметку в поле "Отключен".

   Кнопки управления списками профилей для режимов "Сервер" и "Ретранслятор" станут недоступны.
2. Для сохранения изменений и завершения настройки нажмите кнопку "OK".

Внимание! После отключения сервиса DHCP все настройки, выполненные ранее для сервиса, будут сброшены.

Просмотр статистики сервера DHCP

При включенном на сетевом устройстве режиме сервера DHCP в ПУ ЦУС можно просмотреть статистику сервера и таблицу арендованных адресов. Статистика и арендованные адреса отображаются на вкладке "DHCP" дополнительного окна.

Статистика включает в себя следующие сведения:

- имя внутреннего интерфейса сетевого устройства;
- общее количество адресов пула;
- количество используемых адресов пула;
- количество доступных адресов пула.

В таблице арендованных адресов приводятся следующие сведения:

- IP-адрес, выданный клиенту из пула адресов;
- MAC-адрес клиента;
- сетевое имя клиента;
- дата и время начала аренды;
- дата и время окончания аренды.

Для просмотра статистики:

- В главном окне ПУ ЦУС выберите в списке сетевое устройство, работающее в режиме сервера DHCP.

  На вкладке "DHCP" дополнительного окна отобразятся статистика сервера и таблица арендованных адресов.

Настройка параметров маршрутизации

Переход к настройке параметров

Режимы работы сетевого устройства:

- динамическая маршрутизация;
- статическая маршрутизация.

Просмотр и настройка параметров режима работы осуществляются в окне свойств сетевого устройства на вкладке "Маршрутизация". Вид вкладки и ее содержание зависят от режима, в котором работает в данный момент сетевое устройство.

Если настройка режимов не производилась, вкладка "Маршрутизация" отображает настройки статической маршрутизации. На вкладке представлены таблица маршрутов для данного сетевого устройства и кнопки, с помощью которых выполняется формирование этой таблицы.

Переключение режима маршрутизации

Для переключения со статической на динамическую маршрутизацию:

1. На вкладке "Маршрутизация" окна свойств сетевого устройства в поле "Тип" измените значение на "Динамическая (поддержка протоколов OSPF, RIP, BGP)".

   Вид вкладки изменится и станет соответствовать режиму динамической маршрутизации. На вкладке будут отображаться раздел с информацией о маршрутах и разделы с конфигурациями для данного сетевого устройства.

   Справа от каждого раздела расположены кнопки.

Прервать обновление	Прерывает процесс обновления отображаемых сведений о маршрутах, поступающих от ЦУС. После открытия вкладки "Маршрутизация" кнопка недоступна в течение примерно 50 секунд. После завершения загрузки информации о маршрутах кнопка заменяется кнопкой "Обновить список маршрутов" (см. ниже)
Обновить список маршрутов	Запускает процесс обновления отображаемых сведений о маршрутах. Если сетевое устройство в данный момент выключено, кнопка недоступна
Загрузить конфигурацию из файла	Запускает стандартную процедуру загрузки файла. Используется для загрузки конфигурационного файла zebra и конфигураций для поддерживаемых протоколов
Сохранить маршруты/конфигурацию в файл	Запускает стандартную процедуру сохранения содержимого соответствующего раздела в текстовый файл

2. Выполните процедуру настройки динамической маршрутизации (см. стр. **38**).

Для переключения с динамической маршрутизации на статическую:

1. На вкладке "Маршрутизация" окна свойств сетевого устройства в поле "Тип" измените значение на "Статическая".

   Вид вкладки изменится и станет соответствовать режиму статической маршрутизации.

2. Нажмите кнопку "Применить".

   В поле "Информация о маршрутах" появятся правила, сформированные автоматически, и станут доступными кнопки <Добавить>, <Изменить> и <Удалить>.

3. При необходимости измените список правил (см. стр. **37**).

Статическая маршрутизация

Правила маршрутизации подразделяются на два типа:

- правила, сформированные комплексом автоматически;
- правила, заданные администратором.

Правила, сформированные автоматически, предусматривают взаимодействие только между сегментами сети, подключенными непосредственно к интерфейсам сетевого устройства. Формирование таких правил происходит при добавлении очередного адреса сетевого интерфейса. Правила этого типа действуют постоянно и не могут быть удалены или изменены администратором. Начальное заполнение поля "Правила маршрутизации" осуществляется на этапе подключения сетевого устройства.

На основе правил маршрутизации постоянного действия комплекс автоматически формирует временные правила. Временное правило формируется при поступлении на сетевое устройство IP-пакета, адресованного одному из абонентов защищаемой сети. Такое правило имеет ограниченное время действия, и если за это время на данный адрес не поступает новый пакет, правило уничтожается. Если пакет поступает, отсчет времени действия правила начинается заново. Кроме приведенного примера временные правила создаются также при наличии на пути прохождения IP-пакета сетей, характеризующихся значением MTU меньшим, чем у интерфейса сетевого устройства. Правила этого типа не могут быть удалены или изменены администратором. Они не отображаются на экране.

Если защищаемая сеть подсоединена к сетевому устройству через маршрутизатор, правила маршрутизации для абонентов этой сети задаются администратором. Эти правила действуют постоянно.

Внимание! Не изменяйте настройки в окне "Маршрутизация" без крайней необходимости. При некорректном вводе правил маршрутизации сетевое устройство работать не будет.

Список правил маршрутизации отображается в виде таблицы, каждая строка которой соответствует одному правилу. Перечень полей таблицы правил маршрутизации и их описание представлены в таблице ниже.

Табл.4 Поля таблицы правил маршрутизации

Поле	Описание
Адрес	IP-адрес подсети абонента-получателя
Маска	Маска подсети абонента-получателя
Следующий узел	IP-адрес следующего узла, через который должны проходить IP-пакеты для абонента-получателя

Правило маршрутизации с нулевыми маской и адресом назначения отображает маршрут по умолчанию.

Внимание! Если маршрут по умолчанию связывает сетевое устройство с ЦУС, то после его изменения соединение устройства с ЦУС становится невозможным. В этом случае требуется запись новой конфигурации на носитель и повторная инициализация сетевого устройства.

Нулевой адрес в столбце "Следующий узел" указывает, что данная подсеть доступна напрямую через интерфейс, без промежуточных маршрутизаторов.

Для настройки правил маршрутизации:

1. Перейдите к настройке параметров маршрутизации (см. стр. **35**).

   При необходимости переключите вкладку на соответствие режиму статической маршрутизации (см. стр. **35**).

2. Определите параметры правил.
   - Чтобы добавить запись в список правил маршрутизации, нажмите кнопку "Добавить", укажите протокол (IPv4 или IPv6) и введите адрес и маску (префикс) для данной сети. Если защищаемая сеть подсоединена к сетевому устройству через маршрутизатор, в поле "Следующий узел" укажите адрес этого маршрутизатора. Затем нажмите кнопку "OK".

     Введенные данные появятся в списке правил маршрутизации.
   - Для изменения записи в списке правил маршрутизации выберите нужную строку. Параметры выбранного правила будут отображены в полях, расположенных под списком. Нажмите кнопку "Изменить" и внесите необходимые изменения.
   - Чтобы удалить запись из списка правил маршрутизации, выберите нужную строку и нажмите кнопку "Удалить". Выбранная запись будет удалена немедленно.

   Изменения в настройках таблицы маршрутизации применяются немедленно.

Примечание. С помощью групповых операций правила маршрутизации можно назначить одновременно нескольким сетевым устройствам. Описание групповых операций с параметрами статической маршрутизации приведено в [**5**].

Динамическая маршрутизация

Динамическая маршрутизация не поддерживается в следующих случаях:

- включен режим привязки маршрутизаторов к MAC-адресам (см. [**2**], "Привязка аппаратных адресов маршрутизаторов");
- включен один из режимов Multi-WAN (см. стр. **21**).

Для поддержки протоколов динамической маршрутизации необходимо сформировать конфигурационный файл zebra.conf, а также конфигурационные файлы используемых протоколов (ospfd.conf, bgpd.conf, ripd.conf).

Внимание! Поддерживаются следующие версии протоколов:

- OSPF — версия 2;
- BGP — версия 4;
- RIP — версия 1, версия 2.

Настройку динамической маршрутизации выполняют в следующем порядке:

- создание конфигурационного файла (см. стр. **61**);

  Внимание! В конфигурационном файле zebra.conf необходимо прописать статические маршруты, так как настроенные ранее статические маршруты после переключения из режима статической маршрутизации в режим динамической маршрутизации будут действовать только до первой перезагрузки сетевого устройства.

  При переключении со статической на динамическую маршрутизацию в кластере ранее настроенные статические маршруты на резервном сетевом устройстве будут удалены, а на основном устройстве они будут действовать до первой перезагрузки;
- настройка параметров динамической маршрутизации (см. ниже).

Для настройки параметров:

1. Перейдите к настройке параметров маршрутизации (см. стр. **35**) и при необходимости переключите вкладку на соответствие режиму динамической маршрутизации.
2. Определите параметры правил маршрутизации:
   - Загрузите конфигурационный файл zebra.conf. Для этого используйте кнопку справа от поля "Конфигурация zebra" или введите в поле текст конфигурационного файла вручную.

   Внимание! В конфигурационном файле zebra.conf не допускается задание IP- адресов интерфейсов, так как это может привести к неработоспособности комплекса. Для задания IP-адресов сетевого устройства используйте процедуру, приведенную на стр. **7**.
   - Откройте вкладку нужного протокола и загрузите для него конфигурационный файл. Для этого используйте кнопку , расположенную справа, или введите текст конфигурационного файла вручную.
   - При необходимости установите отметку в поле "Анонсирование ЗС, доступных через узел".

     Примечание. Для корректной работы анонсирования ЗС через протоколы BGP и OSPF необходимо добавить в конфигурационный файл протокола BGP строку "!bgp router-id 127.0.0.1".
3. Нажмите кнопку "Применить".

   Сетевому устройству будет отправлена команда на загрузку в ЦУС списка маршрутов, и в ЦУС начнется обновление информации о сетевом устройстве.

   Примечание. Подтверждение о ходе выполнения команды отображается в очереди заданий (см. стр. **67**).

После завершения обновления из ЦУС в ПУ поступит список маршрутов данного сетевого устройства, который отобразится в разделе "Информация о маршрутах". Кнопка прерывания обновления заменится на кнопку обновления списка маршрутов.

Внимание! При достаточно большом количестве маршрутов обновление информации на ЦУС может потребовать дополнительного времени и отобразится часть таблицы маршрутизации. При этом кнопка прерывания обновления в течение примерно 50 секунд будет недоступна. Если в просмотре информации о маршрутах нет необходимости, откажитесь от обновления. Для этого нажмите кнопку прерывания обновления. Полная таблица маршрутизации доступна в технологическом отчете.

4. Если необходимо сохранить в виде текстового файла информацию о маршрутах или конфигурациях, используйте кнопку , расположенную справа от соответствующего раздела.

Внимание! После закрытия окна свойств сетевого устройства информация о маршрутах, отображаемая на вкладке "Маршрутизация", не сохраняется. При следующем открытии окна на вкладке "Маршрутизация" раздел "Информация о маршрутах" будет пустым.

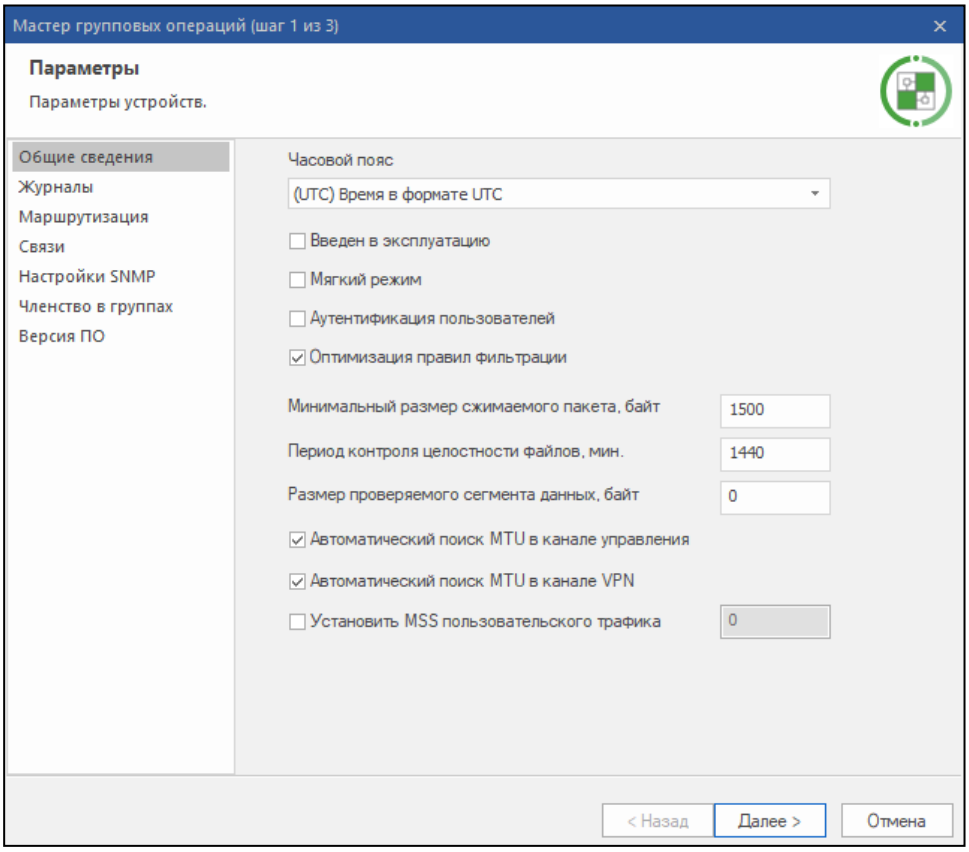
Групповая настройка динамической маршрутизации

Одинаковые настройки динамической маршрутизации можно выполнить одновременно для нескольких сетевых устройств. При этом используется один и тот же заранее подготовленный конфигурационный файл zebra.conf и конфигурационный файл протокола.

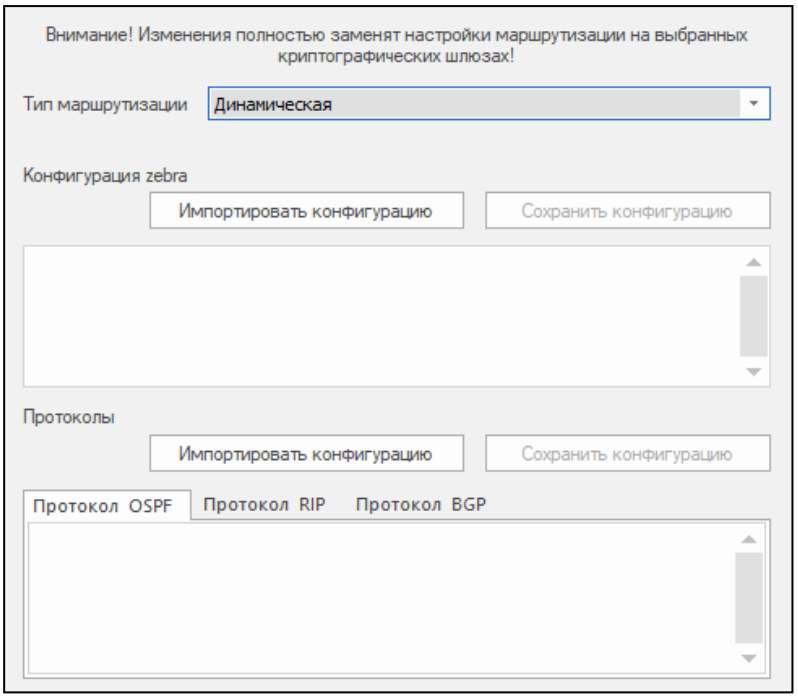
Для групповой настройки:

1. Перейдите к списку сетевых устройств и выделите с помощью клавиши <Ctrl> группу устройств, для которых необходимо настроить динамическую маршрутизацию.
2. Нажмите на панели инструментов кнопку "Групповые операции".

   На экране появится окно мастера групповых операций.



3. Перейдите в раздел "Маршрутизация" и выберите тип маршрутизации — "Динамическая".



4. Загрузите конфигурационный файл zebra. Для этого нажмите кнопку "Импортировать конфигурацию" и укажите путь к файлу.
5. Перейдите на вкладку требуемого протокола и загрузите соответствующий конфигурационный файл.
6. Нажмите кнопку "Далее".

   На экране появится следующее окно мастера с предупреждением о выполняемой операции.
7. Нажмите кнопку "Применить".

   Операция будет выполнена, и на экране появится следующее окно мастера, отображающее результаты выполненной операции. В нижней части окна расположена ссылка "Посмотреть отчет", по которой можно вызвать детализированные результаты операции в виде текстового файла.
8. Нажмите кнопку "Готово" для завершения операции.

Настройка фрагментации пакетов

В рамках механизмов фрагментации передаваемых пакетов на сетевом устройстве предусмотрены следующие настройки:

- принудительная установка флага DF (Don't fragment);
- задание значения MSS.

Принудительная установка флага DF выполняется раздельно на канале управления и каналах VPN. По умолчанию после установки ПО и инициализации сетевого устройства принудительная установка флага DF для канала управления и VPN-каналов включена.

Внимание! Настройку фрагментации пакетов выполняют централизованно средствами ПУ ЦУС. Приведенные ниже процедуры настройки рекомендуется применять в тех случаях, когда по каким-либо причинам настройку нельзя выполнить централизованно.

Для настройки фрагментации пакетов:

1. Перейдите к меню локальной настройки параметров сетевого устройства (см. стр. **59**).

2. Введите в строке ввода номер команды "Настройка фрагментации" и нажмите клавишу <Enter>.

   На экране появится меню настроек фрагментации.

```
1: Текущие настройки фрагментации
2: Блокировать фрагментированный трафик
3: Отключение автоматического поиска PMTU для канала
управления
4: Отключение автоматического поиска PMTU для канала VPN
5: Настройка MSS
0: Выход
Выберите пункт меню (0 – 5):
```

3. Для настройки фрагментации или выхода из меню введите номер нужной команды и нажмите клавишу <Enter>.

Для просмотра текущего состояния настроек фрагментации:

1. В меню настроек фрагментации введите номер команды "Текущие настройки фрагментации" и нажмите клавишу <Enter>.

   На экране будут отображены значения текущих настроек фрагментации:

```
Поиск MTU для канала управления включен
Поиск MTU для VPN каналов включен
MSS пользовательского трафика не изменяется
```

Примечание. "Поиск MTU для <название канала> включен"— флаг DF на IP-пакеты ставится; "Поиск MTU для <название канала> выключен" — флаг DF на IP-пакеты не ставится.

2. Для настройки фрагментации или выхода из меню введите номер нужной команды и нажмите клавишу <Enter>.

Для блокировки/разблокировки фрагментированного трафика:

1. В меню настроек фрагментации введите номер команды "Блокировать/разблокировать фрагментированный трафик" и нажмите клавишу <Enter>.

   Выполнится блокировка/разблокировка фрагментированного трафика и на экране появится меню настроек фрагментации.

2. В меню настроек фрагментации введите номер команды "Выход" и нажмите клавишу <Enter> для возврата в меню настроек.

Для включения/отключения принудительной установки флага DF:

1. В меню настроек фрагментации введите номер команды "Отключение/включение автоматического поиска PMTU..." для канала управления или VPN-каналов и нажмите клавишу <Enter>.

   Выполнится включение/отключение режима принудительной установки флага DF и на экране появится меню настроек фрагментации.

Примечание. Для проверки результата выполнения команды используйте команду "Показать текущие настройки фрагментации".

2. В меню настроек фрагментации введите номер команды "Выход" и нажмите клавишу <Enter> для возврата в меню настроек.

Для настройки MSS:

1. В меню настроек фрагментации введите номер команды "Настройка MSS" и нажмите клавишу <Enter>.

   На экране появится меню настройки MSS.

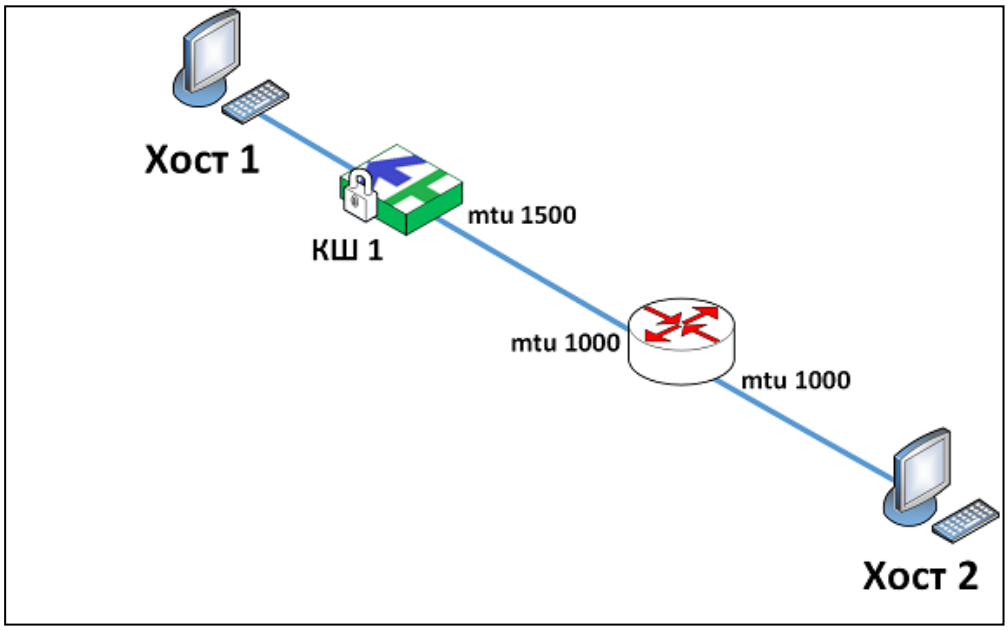
```
1: Просмотр значения MSS
2: Установка значения MSS
3: Текущее значение MSS
0: Выход
Выберите пункт меню (0 – 3):
```

Команда	Описание
Просмотр значения MSS	Вывод на экран текущего значения MSS. **Внимание!** После установки ПО и инициализации сетевого устройства по умолчанию установлено значение "MSS пользовательского трафика не изменяется"
Установка значения MSS	Ввод вручную значения из диапазона 536–1408
Текущее значение MSS	Значение MSS устанавливается автоматически
Выход	Возврат в меню настроек фрагментации

2. Введите номер нужной команды и нажмите клавишу <Enter>.

Особенность работы КШ как транзитного устройства

Ниже на рисунке показаны Хост 1, защищаемый криптошлюзом КШ 1, и Хост 2. Криптошлюз КШ 1 выполняет функции межсетевого экрана.



На интерфейсах роутера задан mtu 1000. На интерфейсах КШ 1 mtu по умолчанию — 1500.

Хост 1 посылает пакеты хосту 2 с mtu 1300. Так как на роутере задано значение mtu 1000, он не пропускает пакеты от хоста 1 и посылает хосту 1 icmp-сообщение о необходимости уменьшить размер отправляемых пакетов.

По умолчанию КШ 1 не пропускает icmp-сообщение от роутера к хосту 1. Поэтому для того чтобы хост 1 получил icmp-сообщение о необходимости уменьшить размер отправляемых пакетов, на КШ 1 необходимо задать правило фильтрации, разрешающее прохождение icmp-пакетов от роутера к хосту 1.

Управление списком связанных сетевых устройств

Перечень сетевых устройств, с которыми данное устройство должно устанавливать защищенные соединения, определяется списком связанных сетевых устройств. В этом случае трафик между сетевыми устройствами зашифровывается, в противном случае нет.

Если КШ с ЦУС в пассивном режиме имеет парные связи с другими устройствами, то в ходе синхронизации БД ЦУС при получении актуальной БД произойдет удаление ключей этих связей. Ключи автоматически

восстановятся, но в это время возможны перерывы в прохождении шифрованного трафика. В связи с этим не рекомендуется создавать парные связи на устройствах в пассивном режиме.

Внимание! При резервировании ЦУС не рекомендуется создавать парные связи на КШ с ЦУС во избежание потери части шифрованного трафика на этих устройствах.

Количество защищенных соединений (VPN-каналов) для каждой пары связанных сетевых устройств соответствует количеству зарегистрированных в системе классов трафика (см. стр. **52**). Состояние VPN-каналов отображается в разделе "Центр управления сетью" области объектов управления.

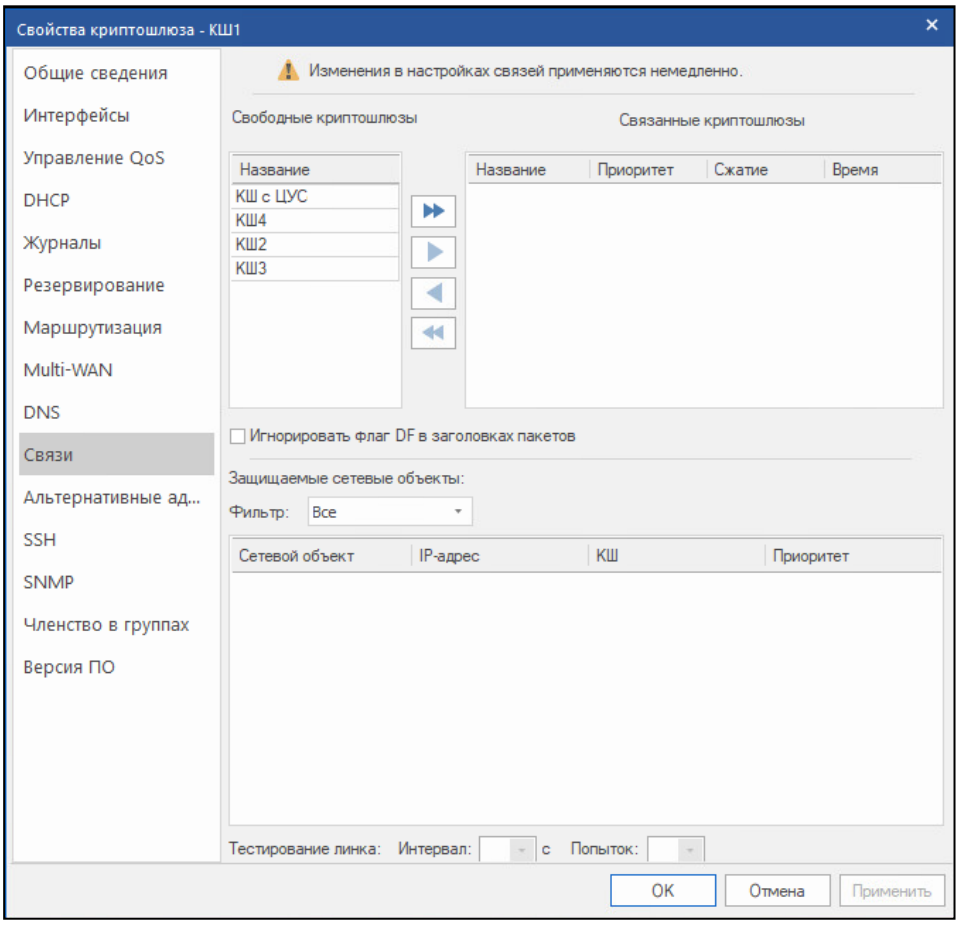
Для формирования списка связанных сетевых устройств:

1. Вызовите контекстное меню криптошлюза, для которого необходимо сформировать парные связи, и активируйте команду "Свойства…".

   На экране появится окно настройки свойств данного криптошлюза.

2. Перейдите на вкладку "Связи".

   На вкладке отображаются два списка: "Свободные криптошлюзы" и "Связанные криптошлюзы".



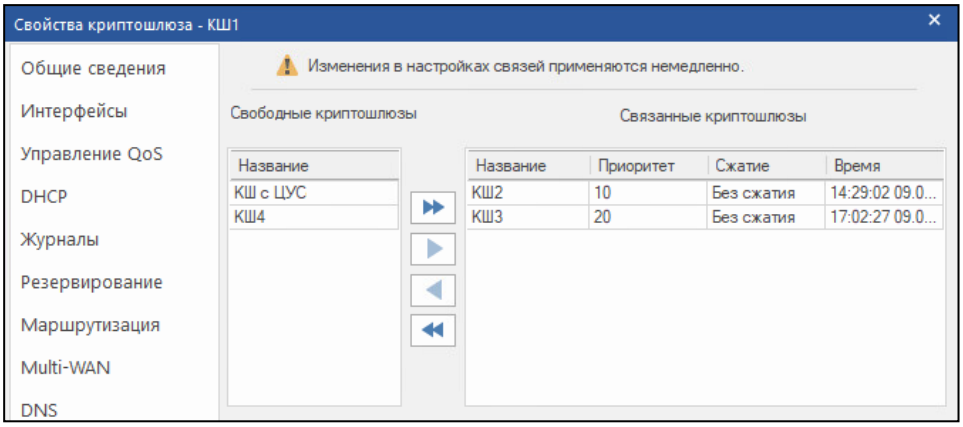
   Если парные связи между криптошлюзами не создавались, список связанных криптошлюзов будет пустым.

3. Сформируйте список связанных сетевых устройств. Для этого переместите криптошлюзы, с которыми должна быть установлена парная связь данного криптошлюза, в список "Связанные криптошлюзы".

   Перемещайте выбранные элементы из списка в список с помощью кнопок "<", "<<" и ">", ">>".

4. Если данный КШ (на рисунке ниже КШ 1) имеет парные связи с двумя другими КШ (КШ 2 и КШ 3), к которым имеет привязку один и тот же защищаемый сетевой объект, необходимо для каждой связи (КШ 1—КШ 2 и

КШ 1—КШ 3) указать приоритеты, в соответствии с которыми КШ 1 будет отправлять зашифрованные пакеты защищаемому сетевому объекту. Для этого выделите поле "Приоритет", раскройте список и выберите в нем нужное значение. Допустимые значения: 1–255.



5. При необходимости для каждого КШ из списка "Связанные криптошлюзы" укажите нужный режим сжатия передаваемых IP-пакетов. Для этого выделите поле "Сжатие", раскройте список и выберите в нем нужное значение.

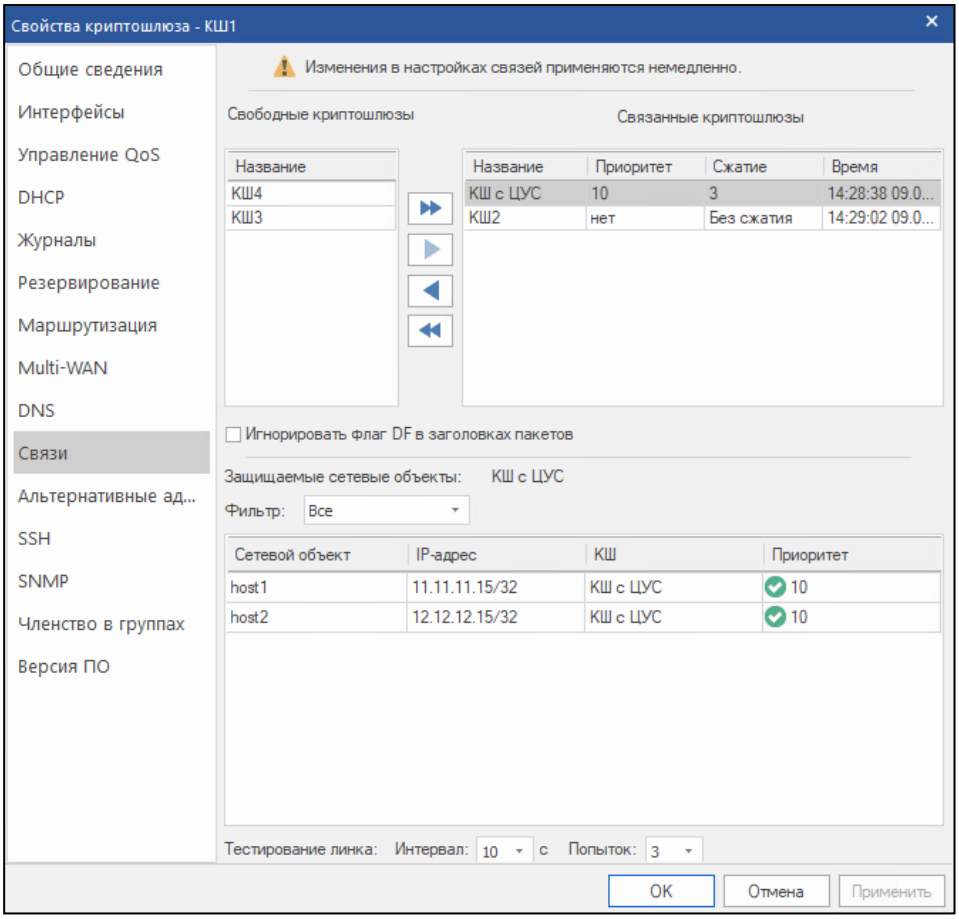
   Список содержит значения от "1" до "9" и "Без сжатия". При переходе от режима "1" к режиму "9" степень сжатия IP-пакетов увеличивается и, соответственно, увеличивается время сжатия. При выборе значения "Без сжатия" сжатие IP-пакетов не осуществляется.

6. Если при обработке IP-пакетов необходимо игнорировать флаг DF в заголовках, установите соответствующую отметку.

7. Для каждой парной связи данного КШ (на рисунке выше — КШ 1) задайте параметры проверки работоспособности канала. Для этого выделите в списке "Связанные криптошлюзы" строку парной связи.

   В нижней части окна отобразится список защищаемых сетевых объектов.

   На рисунке ниже выбрана парная связь КШ 1 — КШ с ЦУС. При этом в списке защищаемых сетевых объектов отобразятся привязанные к КШ с ЦУС сетевые объекты host 1 и host 2.



Внимание! Для просмотра списка защищаемых сетевых объектов можно использовать фильтр. Варианты использования фильтра:

- Все — в списке отображаются все сетевые объекты, привязанные в рамках выбранной парной связи;
- Много связей — отображаются сетевые объекты, привязанные к более чем одному КШ;
- Одна связь — отображаются сетевые объекты, привязанные только к одному КШ.

8. В поле "Интервал" выберите интервал времени между проверками работоспособности канала. Доступные значения: 1–60 секунд.

   В поле "Попыток" выберите количество проверок, на основании которых принимается решение о неработоспособности канала. Доступные значения: 1–10.

Примечание. Введенные значения будут применены к каждому КШ парной связи.

9. Нажмите кнопку "OK" для сохранения изменений.

   Изменения в данном диалоге вступают в силу сразу после их внесения.

   С этого момента данные сетевые устройства могут устанавливать между собой защищенное соединение.

Внимание! Параметры сжатия IP-пакетов каждого из двух криптошлюзов, составляющих пару взаимодействующих КШ, настраиваются отдельно и могут не совпадать.

Установка времени на КШ с ЦУС

Правильную текущую дату и время на КШ с ЦУС можно установить вручную или использовать режим синхронизации с NTP-серверами точного времени.

Для задания режима синхронизации с NTP-сервером необходимо указать его DNS или IP-адрес. Синхронизация с NTP-сервером осуществляется каждый час.

Предусмотрена возможность задать список серверов точного времени. В этом случае для синхронизации автоматически выбирается наиболее точный из них.

Для NTP-сервера, работающего под управлением ОС Windows, должны быть установлены следующие значения параметров реестра:

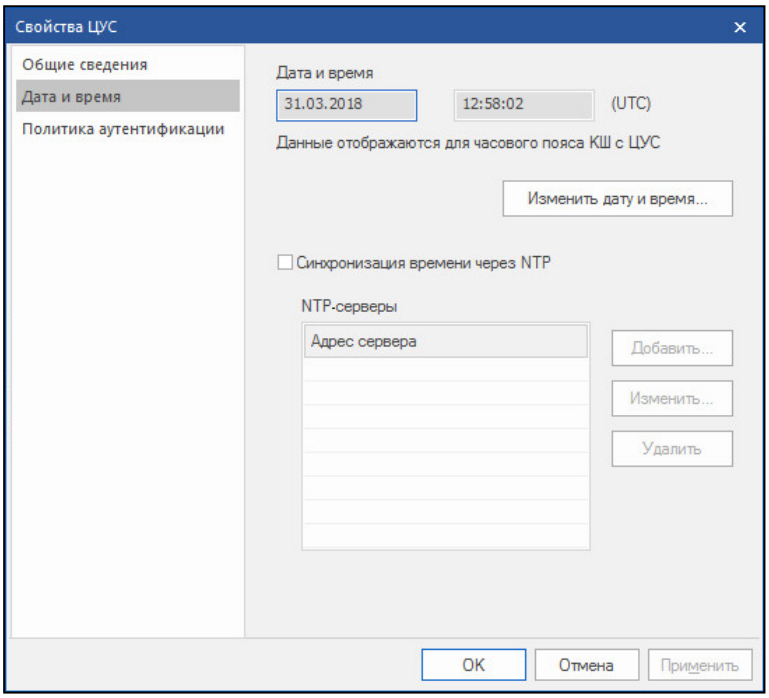
- regedit SYSTEM\CurrentControlSet\Services\W32Time\Config\ LocalClockDispersion = 0
- regedit SYSTEM\CurrentControlSet\Services\W32Time\Config\AnnounceFlags = 5

Для установки времени на КШ с ЦУС:

1. Вызовите контекстное меню раздела "ЦУС" области объектов управления и выберите команду "Свойства".

   Появится окно "Свойства ЦУС".

2. Перейдите на вкладку "Дата и время".



   На вкладке отображаются:

   - текущая дата и время для часового пояса КШ с ЦУС;
   - поле включения или отключения режима синхронизации с NTP-серверами;
   - список NTP-серверов (если режим включен).

3. Для установки даты и времени вручную удалите отметку в поле "Синхронизация времени через NTP" (если она установлена) и нажмите кнопку "Изменить дату и время...".

   Появится окно настройки даты и времени.

4. Введите дату и время и перейдите к п. **8**.

5. Для задания режима синхронизации установите отметку в поле "Синхронизация времени через NTP".

   Станет доступной кнопка "Добавить".

6. Нажмите кнопку "Добавить".

   На экране появится окно для ввода адреса NTP-сервера.

   Введите адрес NTP-сервера и нажмите кнопку "OK".

   Примечание. Допускается ввод как IP-адреса NTP-сервера, так и его сетевого имени. Если вводится сетевое имя, в свойствах КШ с ЦУС необходимо указать DNS-сервер (см. ниже).

   Окно ввода адреса закроется, и NTP-сервер будет добавлен в список.

7. При необходимости добавьте в список другие серверы.

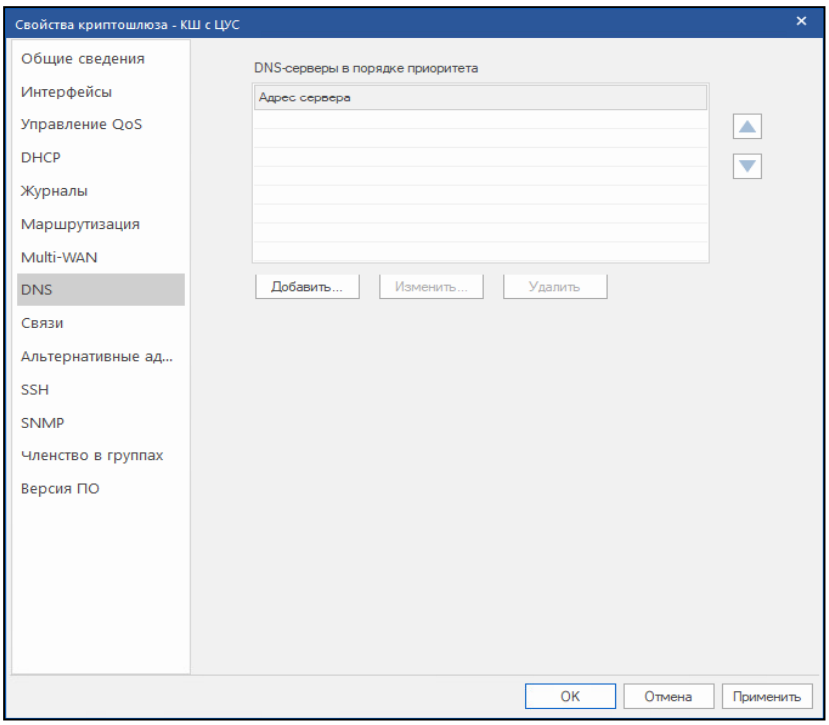
   Для работы со списком используйте кнопки, расположенные справа.

8. Для сохранения выполненных изменений нажмите кнопку "OK".

Настройка DNS

Для настройки списка DNS-серверов:

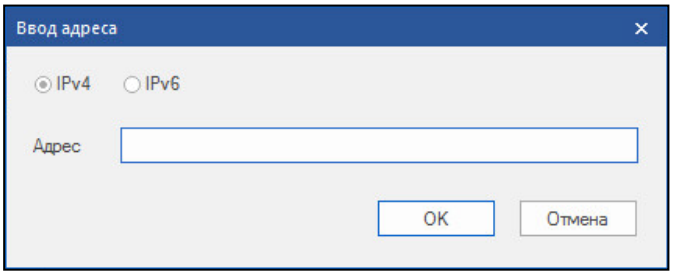
1. Вызовите окно свойств КШ с ЦУС и выберите вкладку "DNS".



   На вкладке отображается список DNS-серверов, упорядоченный по убыванию приоритета.

2. Для добавления нового сервера в список нажмите кнопку "Добавить".

   На экране появится окно ввода IP-адреса.



3. Выберите протокол (IPv4 или IPv6), введите IP-адрес и нажмите кнопку "OK".

   Указанный адрес появится в списке DNS-серверов.

4. При необходимости добавьте другие DNS-серверы и упорядочьте список в соответствии с приоритетами серверов с помощью кнопок, расположенных справа.

   Для удаления или изменения адреса выбранного в списке сервера используйте кнопки "Удалить" и "Изменить..." соответственно.

5. Для сохранения выполненных изменений нажмите кнопку "OK".

Настройка дистанционного доступа по протоколу SSH

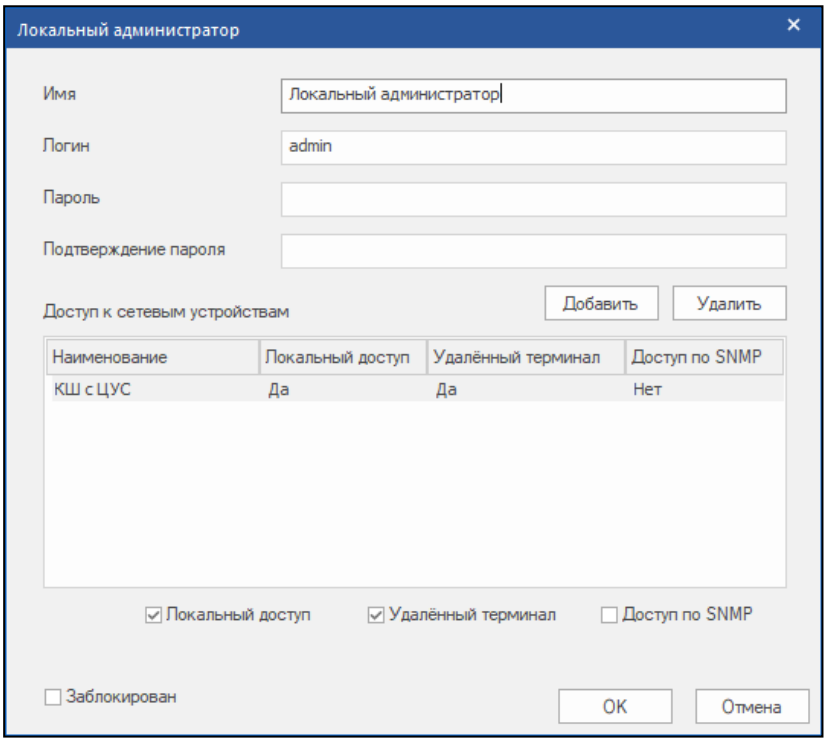
Настройку доступа к сетевому устройству по протоколу SSH можно выполнить средствами локального управления (см. [**2**]) или в ПУ ЦУС. Ниже приведено описание настройки в ПУ ЦУС.

Для доступа по протоколу SSH необходимо настроить учетную запись администратора и добавить его удаленный IP-адрес в список разрешенных IP-адресов соответствующего сетевого устройства.

Примечание. События, связанные с доступом к сетевому устройству по протоколу SSH, регистрируются в его сетевом журнале.

Для предоставления администратору права дистанционного доступа:

1. В ПУ ЦУС создайте новую учетную запись локального администратора КШ (см. [**2**]) или перейдите к уже созданной записи.

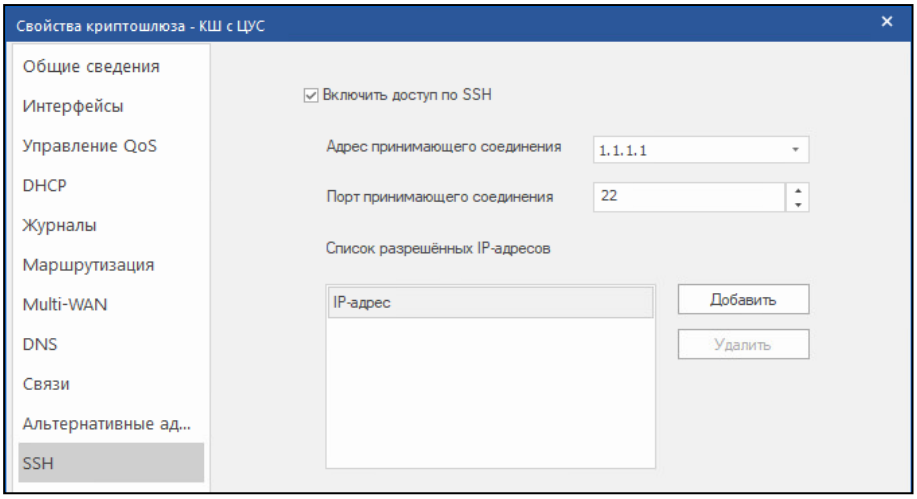


2. В свойствах учетной записи администратора выберите требуемые сетевые устройства и установите отметку в поле "Удаленный терминал", затем нажмите кнопку "ОК".

Совет. Для выбора нескольких устройств допустимо использовать клавиши <Ctrl>, <Shift> и/или мышь.

Для формирования списка разрешенных IP-адресов:

1. Вызовите окно свойств сетевого устройства, перейдите к вкладке "SSH" и установите отметку в поле "Включить доступ по SSH".



2. Выберите в поле адреса принимающего соединения IP-адрес требуемого интерфейса управления, затем укажите порт принимающего соединения.
3. Сформируйте список IP-адресов, имеющих административный доступ к этому сетевому устройству по протоколу SSH, используя кнопки "Добавить" и "Удалить".
4. Нажмите кнопку "ОК".

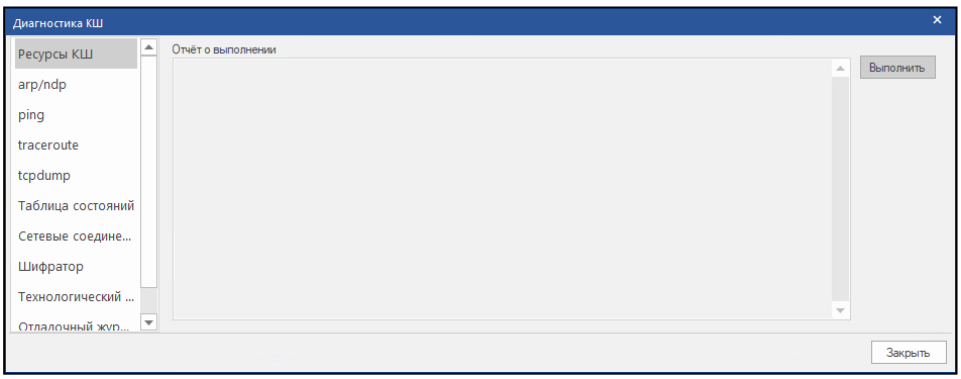
Диагностика сетевого устройства

Для диагностики работы сетевого устройства в ПУ ЦУС:

Внимание! В текущей версии ПО диагностика ДА не поддерживается.

1. Выберите в области объектов управления тип устройства, затем вызовите контекстное меню требуемого устройства и выберите команду диагностики сетевого устройства.

   На экране появится окно диагностики сетевого устройства.



2. Выберите требуемую вкладку, при необходимости укажите необходимые данные и нажмите кнопку "Выполнить" или "Получить".

Вкладка	Описание
Ресурсы <сетевого устройства>	Информация о ресурсах сетевого устройства: • загруженность каждого процессора; • общий, используемый и свободный объем оперативной памяти; • отчет по использованию дискового пространства; • сведения о заполненности журналов
Arp/ndp	Содержимое ARP- и NDP-кеша сетевого устройства
Ping* (только для КШ)	Результаты выполнения команды ping на сетевом устройстве. Необходимо предварительно указать IP-адрес, соединение с которым необходимо проверить, и количество тест-пакетов

Вкладка	Описание
Traceroute* (только для КШ)	Результаты выполнения команды traceroute на сетевом устройстве. Необходимо предварительно указать IP-адрес назначения и максимальное количество "прыжков"
Tcpdump	Информация о сетевом трафике на определенном интерфейсе. Необходимо предварительно выбрать интерфейс, фильтр в формате команды tcpdump и количество пакетов трафика для просмотра. Для сетевого устройства, выведенного из эксплуатации, также доступно выполнение команды tcpdump в двоичном коде для последующего сохранения и просмотра в специализированном приложении
Таблица состояний (только для КШ)	Сведения о максимальном количестве возможных сетевых соединений на сетевом устройстве и таблица состояний (см. [**4**]). Необходимо предварительно выбрать версию протокола IP
Сетевые соединения	Сведения об открытых сетевых соединениях
Шифратор (только для КШ)	Статистическая информация о работе шифратора
Пропущенные пакеты (только для ДА)	Статистическая информация по пакетам, обработанным ДА
Технологический отчет	Технологический отчет для отправки в службу поддержки. При нажатии кнопки "Выполнить" — формирование отчета. При нажатии кнопки "Сохранить" откроется стандартное окно ОС Windows для сохранения файла отчета
Отладочный журнал**	Отладочный журнал для отправки в службу поддержки. При нажатии кнопки "Получить" — формирование журнала. При нажатии кнопки "Сохранить" откроется стандартное окно ОС Windows для сохранения файла журнала

* Для выполнения команд ping и traceroute на сетевом устройстве автоматически создаются временные правила фильтрации, разрешающие прохождение соответствующих пакетов.

** Для получения отладочного журнала необходимо предварительно определить, какой уровень детализации служебных сообщений он будет содержать (см. ниже).

Обращение в техподдержку

При неполадках в работе сетевого устройства, требующих вмешательства со стороны разработчика, может потребоваться передача соответствующих технологических отчетов и отладочных журналов. Перед формированием отладочного журнала необходимо определить, какой уровень детализации служебных сообщений он будет содержать.

Для определения состава отладочного журнала:

1. В окне свойств требуемого сетевого устройства перейдите к вкладке "Журналы".
2. Установите отметку в поле "Уровень детализации" и выберите требуемый уровень в выпадающем списке. Уровень отладочных сообщений содержит полный перечень всех произошедших событий, уровень ошибок — только сообщения об ошибках.
3. Нажмите кнопку "ОК".

Для формирования отладочного журнала:

1. Выберите требуемый тип устройства в области объектов управления, затем вызовите контекстное меню проблемного сетевого устройства и выберите команду его диагностики.

На экране появится окно диагностики сетевого устройства.

2. Выберите вкладку "Отладочный журнал", нажмите кнопку "Получить" и дождитесь окончания процедуры формирования отладочного журнала.
3. Нажмите кнопку "Сохранить".

   На экране появится стандартное окно ОС Windows для сохранения файла журнала. Файл журнала по умолчанию получает имя systemLog_DDMMYYYY_HHMMSS.txt, где DDMMYYYY_HHMMSS — дата и время его создания.
4. Сохраните файл и отправьте его разработчику по доверенному каналу.

Для формирования технологического отчета:

1. Выберите требуемый тип устройства в области объектов управления, затем вызовите контекстное меню проблемного сетевого устройства и выберите команду его диагностики.

   На экране появится окно диагностики сетевого устройства.
2. Выберите вкладку "Технологический отчет", нажмите кнопку "Выполнить" и дождитесь окончания процедуры формирования отладочного журнала.
3. Нажмите кнопку "Сохранить".

   На экране появится стандартное окно ОС Windows для сохранения файла отчета. Файл отчета по умолчанию получает имя debug_report_DDMMYYYY_HHMMSS.dump, где DDMMYYYY_HHMMSS — дата и время его создания.
4. Сохраните файл и отправьте его разработчику по доверенному каналу.

Глава 3
Управление трафиком

Определение классов трафика

Для определения класса трафика:

1. В левой части окна программы управления выберите папку "Центр управления сетью> Классы трафика".

   В правой части окна отобразится перечень классов трафика.

   Примечание. Класс трафика "Нормальный" создается автоматически при инициализации ЦУС.

2. В списке классов трафика вызовите контекстное меню и активируйте нужную команду:

Создать	Вызывает окно для регистрации нового класса трафика
Свойства	Вызывает окно свойств класса для редактирования выбранной записи

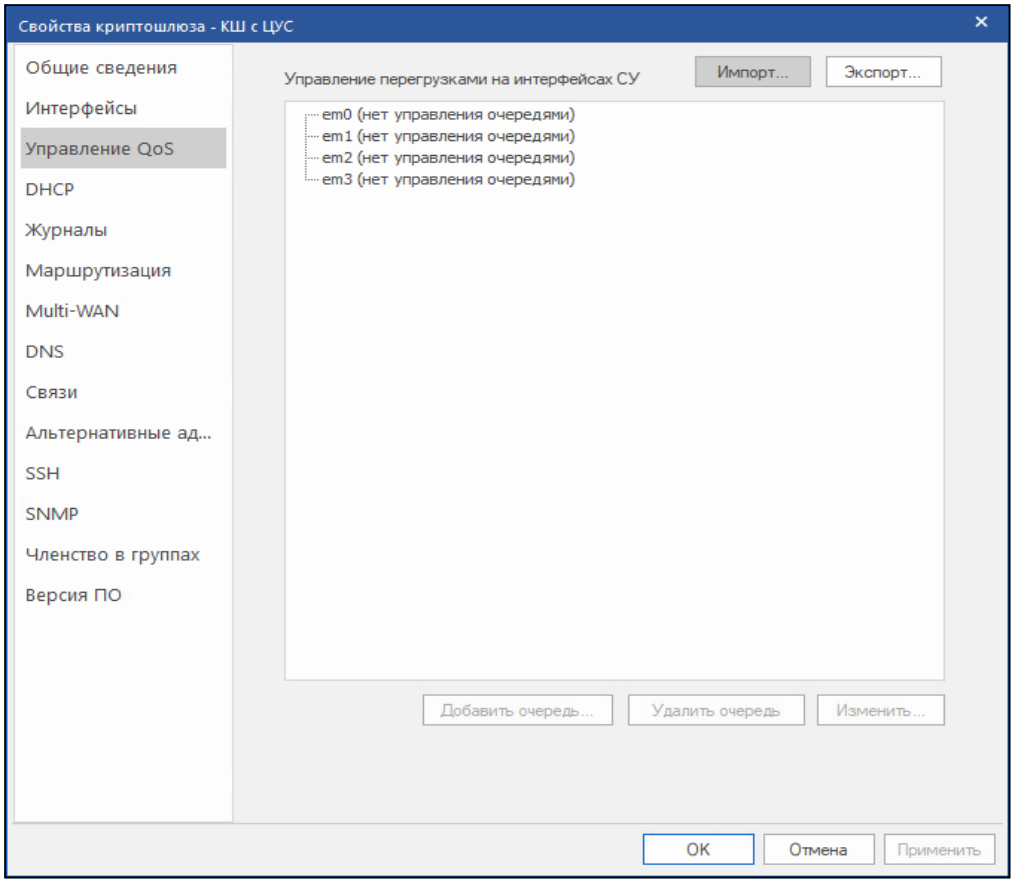
3. Заполните поля параметров и нажмите кнопку "OK".

Параметр	Описание
Название	Наименование класса трафика
Описание	Произвольный текстовый комментарий (необязательный параметр)
Приоритет шифрования	Очередность обработки IP-пакета, отнесенного к данному классу, блоком криптографической защиты. Возможные значения 0–31. Большему значению соответствует более высокий приоритет
Порт внешнего интерфейса для зашифрованного трафика	Порт внешнего интерфейса, с которого отправляются IP-пакеты данного класса
Не менять	Сохраняет значение поля ToS у исходящего IP-пакета таким же, как у входящего
Установить значение	Только для криптошлюзов. Назначает исходящему IP-пакету значение поля ToS, указанное ниже
Bin/Hex	Отображает назначаемое значение поля ToS в двоичном или шестнадцатеричном виде
Код DSCP (биты 1 – 6)	Определяет значение поля ToS по шестибитному классификатору DSCP. Возможные значения 0–63
Приоритет (биты 1 – 3)	Определяет первые три бита значения поля ToS по классификатору IPP. Возможные значения 0–7
Низкая задержка	Определяет четвертый бит значения поля ToS. Наличие отметки указывает режим низкой задержки
Высокая пропускная способность	Определяет пятый бит значения поля ToS. Наличие отметки указывает режим высокой пропускной способности
Высокая надежность	Определяет шестой бит значения поля ToS. Наличие отметки указывает режим высокой надежности

Управление приоритизацией трафика

Окно управления QoS

Настройку очереди на отправку для КШ и КК выполняют в окне свойств сетевого устройства на вкладке "Управление QoS".



На вкладке отображается иерархический список сетевых интерфейсов данного устройства и действующих на них очередей. Для формирования очередей используйте кнопки:

Кнопка	Описание
Импорт…	Запускает процедуру импорта конфигурации очередей из XML-файла
Экспорт…	Формирует XML-файл для переноса конфигурации очередей на другое устройство
Добавить очередь…	Вызывает на экран окно для настройки параметров новой очереди
Удалить очередь	Удаляет выбранную очередь
Изменить…	Вызывает на экран окно для настройки параметров выбранного интерфейса или очереди

Внимание! На физических интерфейсах, входящих в агрегированный канал, приоритизация трафика, в том числе управляющего, не поддерживается. Также не поддерживается приоритизация трафика на интерфейсах ix и ixl.

Настройка общих параметров очереди на интерфейсе

Для настройки общих параметров очереди:

1. На вкладке "Управление QoS" окна свойств сетевого устройства выберите нужный сетевой интерфейс и нажмите кнопку "Изменить…".

   На экране появится окно параметров интерфейса.

2. Заполните поля параметров и нажмите кнопку "OK":

Тип приоритизации	Метод обработки очереди (нет/PRIQ/CBQ/HFSC)
Полоса пропускания, Кбит/с	Общая пропускная способность данного интерфейса

Настройка параметров очереди

Для настройки очереди:

1. На вкладке "Управление QoS" окна свойств сетевого устройства выберите нужный интерфейс и нажмите кнопку "Добавить очередь…".

   Примечание. Добавление очереди возможно лишь на интерфейсе с установленным управлением очередями (см. выше "Настройка общих параметров очереди на интерфейсе").

   На экране появится окно для настройки свойств очереди. Вид окна зависит от выбранного типа приоритизации (см. выше).

2. Заполните поля параметров и нажмите кнопку "OK".

Параметр	Описание
КШ/КК	Наименование сетевого устройства (недоступно для изменений)
Интерфейс	Наименование интерфейса (недоступно для изменений)
Общая полоса пропускания, Кбит/с	Общая пропускная способность данного интерфейса (недоступно для изменений)
Тип приоритизации	Метод обработки очереди (недоступно для изменений)
Название очереди	Наименование очереди
Очередь по умолчанию	При наличии отметки данная очередь назначается очередью по умолчанию. В эту очередь будут попадать IP-пакеты, для которых очереди не определены. Для интерфейса может быть настроена только одна очередь по умолчанию. Если настраиваемая очередь не является очередью по умолчанию, удалите отметку
Управляющий трафик	Очередь будет использоваться для управляющего трафика. Для интерфейса может быть настроена только одна очередь для управляющего трафика. Для настройки очереди предварительно должна быть настроена очередь по умолчанию. Если настраиваемая очередь не является очередью для управляющего трафика, удалите отметку
Классы трафика	Перечень классов трафика, включаемых в данную очередь. Для формирования списка используйте кнопки "Добавить…" и "Удалить"
Полоса пропускания, %	Доля общей полосы пропускания, выделенная для данной очереди, в процентах (только для CBQ). Значение "0" недопустимо
Увеличить по возможности (borrow)	Установка отметки включает механизм заимствования общей полосы пропускания в случае неиспользования ее другими очередями (только для CBQ)
realtime, %	Доля общей полосы пропускания, выделенная для режима realtime, в процентах (только для HFSC)
upperlimit, %	Максимальная доля общей полосы пропускания, в процентах (только для HFSC)

Параметр	Описание
linkshare, %	Доля общей полосы пропускания, выделенная для режима linkshare, в процентах (только для HFSC)
Приоритет	Последовательность обработки очередей. Возможные значения 0–7 для CBQ и HFSC, 0–15 для PRIQ. Большему значению соответствует более высокий приоритет
Количество слотов	Количество пакетов, которые КШ сможет поместить в очередь. Минимальное значение — 0, максимальное значение — 65535
Защита от перегрузок	Установка отметки включает указанный механизм защиты от перегрузок (RED, RIO, ECN)

Резервирование полосы пропускания для управляющего трафика

На сетевом устройстве можно зарезервировать полосу пропускания для управляющего трафика. Для этого настраивается отдельная очередь с наивысшим приоритетом, в которую попадают только пакеты следующих трафиков:

- ПУ ЦУС — ЦУС;
- ПУ СД — СД;
- ЦУС — КШ, КК, ДА (передача обновлений ПО, БРП, системные правила, логи);
- DNS;
- SSH;
- DHCP;
- тестирование Multi-WAN;
- DHCP-relay;
- Syslog;
- SNMP;
- SNMP-trap;
- синхронизация между ЦУС;
- авторизация хоста.

Внимание! Если на внутреннем интерфейсе КШ с установленным DHCP-сервером настроены очереди, ответные пакеты от DHCP-сервера в очередь для управляющего трафика не попадают.

Для создания очереди для управляющего трафика:

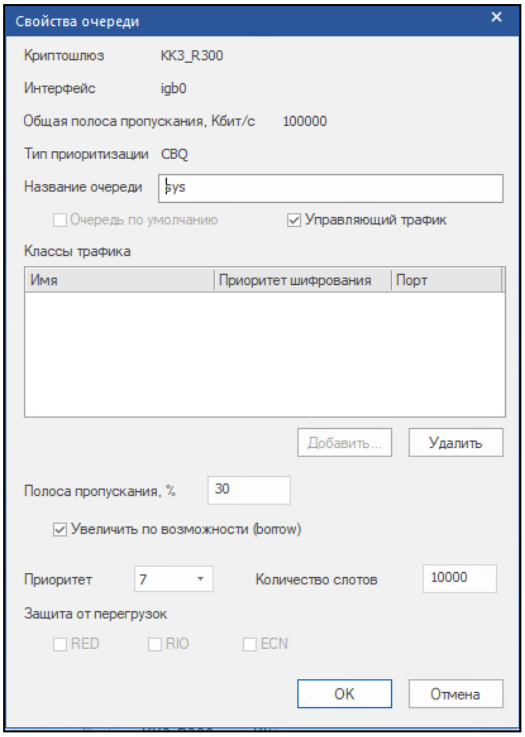
1. На вкладке "Управление QoS" окна свойств сетевого устройства выберите интерфейс, на котором необходимо настроить очередь для управляющего трафик, и проверьте в списке очередей данного интерфейса наличие очереди по умолчанию.

   Если очередь по умолчанию отсутствует, создайте ее (см. стр. **54**). При настройке очереди установите отметку в поле "Очередь по умолчанию".

2. Добавьте новую очередь. При настройке параметров очереди задайте максимальный приоритет.

   Станет доступным поле "Управляющий трафик".

3. Установите отметку в поле "Управляющий трафик".



4. После настройки всех параметров очереди нажмите кнопку "OK".

   Очередь для управляющего трафика добавится в список очередей с пометкой "system".

Экспорт/импорт конфигурации очередей

Для переноса настроек на другие сетевые устройства имеется возможность экспорта/импорта конфигурации очередей на сетевых интерфейсах с помощью файла XML.

Для экспорта конфигурации:

1. Перейдите к вкладке "Управление QoS" и нажмите кнопку "Экспорт…".

   На экране появится стандартное окно ОС Windows для сохранения файла.
2. Выберите папку, укажите название файла и нажмите кнопку "Сохранить".

Для импорта конфигурации:

1. Перейдите к вкладке "Управление QoS" и нажмите кнопку "Импорт…".

   На экране появится стандартное окно ОС Windows для открытия файла.
2. Выберите нужные папку и файл и нажмите кнопку "Открыть".

   На экране появится окно "Импорт настроек QoS".

   В левой части окна представлен перечень интерфейсов сетевого устройства, в правой части отображается импортируемая конфигурация очередей.
3. Сопоставьте интерфейсам сетевого устройства названия интерфейсов импортируемой конфигурации. С этой целью для каждого значения в поле "Интерфейс на <сетевом устройстве>" выберите нужное значение из раскрывающегося списка в поле "Интерфейс из XML".
4. Нажмите кнопку "OK".

   На вкладке "Управление QoS" отобразится импортированная конфигурация очередей.

Режим изолированной сети

Предусмотрен режим изоляции криптошлюзов от внешней среды, при котором ни одно из сетевых устройств, входящих в криптографическую сеть ЦУС, не будет пропускать через свои внешние интерфейсы открытый трафик. По умолчанию режим изолированной сети выключен.

Внимание! Режим изолированной сети не может быть включен, если в сети:

- зарегистрированы сетевые устройства с установленным АПКШ "Континент" версии ниже 3.7;
- установлены связи со сторонними криптографическими сетями.

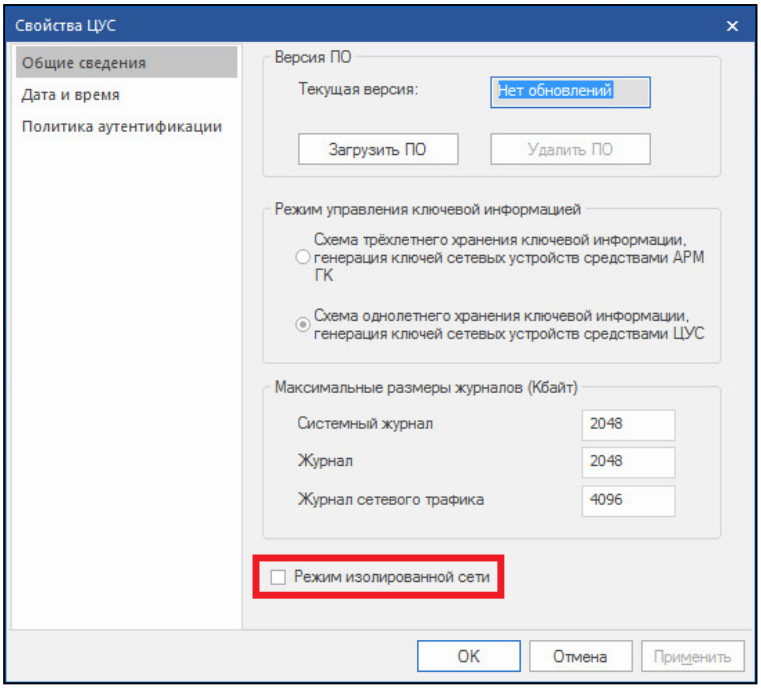
При включенном режиме изолированной сети действуют следующие ограничения:

- На внешних интерфейсах сетевого устройства разрешены только управляющий трафик и трафик, передаваемый между связанными сетевыми устройствами (см. стр. **42**).
- В режиме Multi-WAN функция тестирования каналов недоступна.
- Запрещена отправка во внешнюю сеть DNS- и NTP-запросов.
- В дополнительном меню локального управления сетевым устройством (см. стр. **59**) команды "Выполнить ping" и "Выполнить traceroute" с адресами, принадлежащими внешним сетям, выполняться не будут.
- Динамическая адресация на внешних интерфейсах сетевого устройства не используется.
- Пакеты от DHCP-ретранслятора с внешнего интерфейса КШ не отправляются.
- Синхронизация БД ЦУС через внешние интерфейсы не выполняется. Для синхронизации БД ЦУС необходимо обеспечить доступность между ЦУС через внутренние интерфейсы. IP-адреса этих интерфейсов должны быть в списках альтернативных адресов соответствующих ЦУС.

Для включения/выключения режима изолированной сети:

1. Вызовите контекстное меню раздела "ЦУС" области объектов управления и выберите команду "Свойства".

   Появится окно "Свойства ЦУС".
2. Установите или удалите отметку в поле "Режим изолированной сети" и нажмите кнопку "ОК".



В результате выполнения процедуры на всех сетевых устройствах будет установлен режим, соответствующий выполненному действию, и автоматически будут обновлены правила фильтрации.

Приложение

Переход к меню локальной настройки параметров сетевого устройства

Для перехода к меню:

1. Откройте главное окно локального управления сетевым устройством. Для этого необходимо нажать клавишу <Enter> в короткий промежуток времени после перезагрузки узла.

```
1: Завершение работы
2: Перезагрузка
3: Управление конфигурацией
4: Настройка безопасности
5: Настройка СД <функция недоступна>
6: Тестирование
0: Выход
Выберите пункт меню (0-6):
```

2. Введите номер команды "Управление конфигурацией" и нажмите клавишу <Enter>.

   На экране появится меню локальной настройки параметров сетевого устройства.

```
1: Сохранение конфигурации
2: Загрузка конфигурации
3: Изменение адреса активного ЦУС
4: Настройка PPPoE-соединений
5: Настройка шифрования
6: Настройка фрагментации
7: Настройка коммутации
8: Настройка отладочного журнала
9: Настройка доступа удаленного терминала
10: Настройка режима ретранслятора DHCP (replace)
11: Выключение Agent relay information (опции 82) на DHCP-ретрансляторе
12: Установить ПО криптоускорителя
0: Выход
Выберите пункт меню (0 - 12):
```

Команды дополнительного меню

Для использования дополнительного меню к системному блоку сетевого устройства заранее должны быть подключены клавиатура и монитор.

Для перехода к дополнительному меню:

1. У сетевого устройства в рабочем режиме нажмите комбинацию клавиш <ALT>+<F2>.

   На экране появится запрос на предъявление персонального идентификатора администратора.

2. Предъявите персональный идентификатор, при необходимости введите пароль.

   Количество неудачных попыток предъявления персонального идентификатора и время блокировки задаются политикой аутентификации администраторов (см. [**2**]).

   На экране появится дополнительное меню (см. Табл.5).

3. Введите номер команды и нажмите клавишу <Enter>.

Выполняйте указания, отображаемые на экране.

4. Для выхода из дополнительного меню нажмите комбинацию клавиш <ALT>+<F1>.

Табл.5 Команды дополнительного меню

Команда	Описание
Сведения об устройстве	Отображает на экране следующие сведения: • тип аппаратной платформы; • версия, контрольная сумма и конфигурация ПО; • идентификатор СУ; • статус мягкого режима (вкл/выкл); • ввод в эксплуатацию (да/нет). Если устройство входит в состав кластера, отображается статус – основной/резервный. Дополнительные сведения для ЦУС: • режим работы ЦУС в кластере (активный/пассивный); • дата и время последнего изменения БД ЦУС
Ключи и носители	Отображает на экране следующий список команд: • подготовить ключ, присланный с ЦУС; • информация о загруженных ключах; • выход
Вывести список авторизованных пользователей	Отображает на экране список авторизованных пользователей. Список содержит IP-адреса авторизованных пользователей и время их подключения
Список правил фильтрации	Отображает на экране список всех правил фильтрации с возможностью сохранения информации в файл и экспорта его на внешний носитель информации
Список правил NAT	Отображает на экране список всех правил NAT с возможностью сохранения информации в файл и экспорта его на внешний носитель информации
Вывести полный список интерфейсов	Отображает на экране список всех интерфейсов с возможностью сохранения информации в файл и экспорта его на внешний носитель информации
Вывести таблицы маршрутизации	Отображает на экране таблицы маршрутизации для протоколов IPv4 и IPv6 с возможностью сохранения информации в файл и экспорта его на внешний носитель информации
Просмотр таблицы состояний (keep-state)	Отображает на экране количество установленных соединений с возможностью раздельного просмотра сессий IPv4 и IPv6. При просмотре сессий могут быть использованы фильтр и функция поиска
Диагностика	Выводит на экран меню команд диагностики (см. Табл.6)
Перезагрузка	Запускает перезагрузку сетевого устройства
Завершение работы	Выключает электропитание сетевого устройства
Выход	Закрывает дополнительное меню

Табл.6 Команды меню "Диагностика"

Команда	Описание
Загруженность ЦП	Отображает на экране информацию о загруженности каждого процессора
Использование памяти	Отображает на экране общий, используемый и свободный объем оперативной памяти
Использование жесткого диска	Отображает на экране общий объем жесткого диска, а также объем используемого и свободного пространства

Команда	Описание
Выполнить ping*	Запускает на компьютере команду ping и отображает на экране результаты выполнения этой команды. Укажите IP-адрес, соединение с которым необходимо проверить
Выполнить traceroute*	Запускает на компьютере команду traceroute и отображает на экране результаты выполнения этой команды. Укажите IP-адрес, маршрут к которому требуется определить
Выполнить arp/ndp	Отображает на экране содержимое ARP- и NDP-кеша с возможностью сохранения результатов в файл и экспорта его на внешний носитель информации
Сведения о сетевых соединениях	Отображает на экране сведения об открытых сетевых соединениях с возможностью сохранения информации в файл и экспорта его на внешний носитель информации
Количество пропущенных пакетов	Отображает на экране ДА сведения о количестве пропущенных пакетов
Сведения о работе шифратора	Статистическая информация о работе шифратора с возможностью ее сохранения в файл и экспорта его на внешний носитель информации
Просмотр дампа сетевого трафика	Отображает на экране информацию о сетевом трафике. Для запуска команды задайте имя тестируемого интерфейса, фильтр в формате команды tcpdump и количество пакетов для просмотра. Есть возможность сохранения результатов в файл и экспорта его на внешний носитель информации. Для сетевого устройства, выведенного из эксплуатации, предусмотрено сохранение информации в двоичном коде для последующего просмотра в специализированном приложении
Сведения о состоянии журналов	Отображает на экране максимальные и текущие объемы журналов
Сохранить конфигурацию и журналы событий динамической маршрутизации**	Записывает конфигурационные файлы на отчуждаемый носитель
Сохранить технологическую информацию	Выгружает на отчуждаемый носитель технологический отчет для отправки в службу поддержки. Файл отчета получит имя debug_report_DDMMYYYY_HHMMSS.dump, где DDMMYYYY_HHMMSS - дата и время его создания
Сохранить отладочные журналы	Выгрузка информации системных журналов на USB-флеш-накопитель в файл syslog
Командная строка	Переход в режим командной строки (Continent Shell). Выход по команде exit
Идентифицировать интерфейсы	Запускает идентификацию выбранного порта на корпусе сетевого устройста
Выход	Закрывает меню "Диагностика"

* Для выполнения команд ping и traceroute на КШ автоматически создаются временные правила фильтрации, разрешающие прохождение соответствующих пакетов.

** Для сохранения журналов событий в конфигурационном файле для используемых протоколов маршрутизации должна быть включена функция логирования (Log stdout) и указан путь к файлу журнала. Например, для протокола BGP: log file /var/bgpd.log.

Формат и примеры конфигурационных файлов

Для создания конфигурационных файлов можно использовать любой текстовый редактор, например "Блокнот".

В конфигурационных файлах должны быть определены:

- маршруты по умолчанию;
- статические маршруты, которые должны быть загружены в таблицу маршрутизации.

В конце конфигурационных файлов должна быть пустая строка.

Формат конфигурационного файла OSPF

В таблицах ниже представлены основные параметры конфигурационных файлов, используемые для настройки динамической маршрутизации.

Табл.7 Формат файла zebra.conf

Параметр	Описание
hostname <имя хоста>	Установка имени хоста
log stdout	Установка режима протоколирования на консоль
log file/var/zebra.log	Экспорт журналов событий динамической маршрутизации из КШ на USB-флеш-накопитель (локально)
ip route <адрес/маска> <шлюз>	Определение статического маршрута и маршрута по умолчанию

Табл.8 Формат файла ospfd.conf

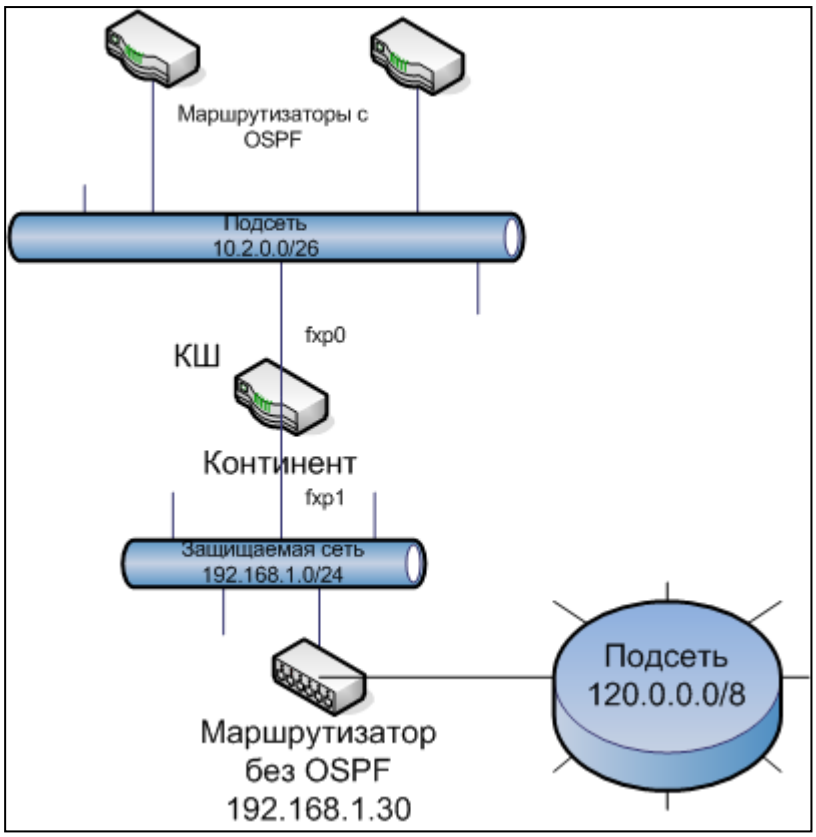
Параметр	Описание
router ospf	Включение OSPF-процесса
network <адрес/маска> <шаблон> area <номер>	Определение диапазона адресов интерфейсов, которые используются для обмена служебной информацией в процессе OSPF-маршрутизации
interface <имя>	Определение имени интерфейса, используемого для обмена служебной информацией в процессе OSPF-маршрутизации
ip ospf authentication message-digest	Установка режима аутентификации OSPF-маршрутизатора
ip ospf message-digest-key 1 <алгоритм> <ключ>	Установка аутентификационного ключа OSPF-маршрутизатора. Использовать указанный алгоритм и ключ (ключ может достигать длины 16 символов)

Примеры конфигурационных файлов

Данный пример иллюстрирует создание конфигурационных файлов для КШ в типовой схеме включения, показанной на рисунке ниже.

Защищаемая сеть 192.168.1.0/24 (например, территориальный филиал какой-либо организации) для связи с другим удаленным филиалом (на рисунке не показан) использует подсеть 10.2.0.0/26 с маршрутизаторами, поддерживающими OSPF.

В состав защищаемой сети входит подсеть 120.0.0.0/8. Для связи с подсетью используется маршрутизатор без OSPF (192.168.1.30).



Для того чтобы обеспечить динамическую маршрутизацию при прохождении трафика между подсетью 120.0.0.0/8 и другим удаленным филиалом, на КШ должна быть выполнена настройка динамической маршрутизации.

Для приведенной выше схемы конфигурационные файлы имеют следующий вид:

zebra.conf

```
hostname continent
log stdout
# статический маршрут в подсеть
ip route 120.0.0.0/8 192.168.1.30
```

ospfd.conf

```
log stdout
router ospf
network 10.2.0.0/26 area 0.0.0.1
area 0.0.0.1 authentication message-digest
# разрешается анонсирование статических маршрутов
redistribute static
interface fxp0
ip ospf authentication message-digest
ip ospf message-digest-key 1 md5 1234567890
```

Формат конфигурационного файла BGP

В таблицах ниже представлены основные параметры конфигурационных файлов, используемые для настройки динамической маршрутизации по протоколу BGP.

Табл.9 Формат файла zebra.conf

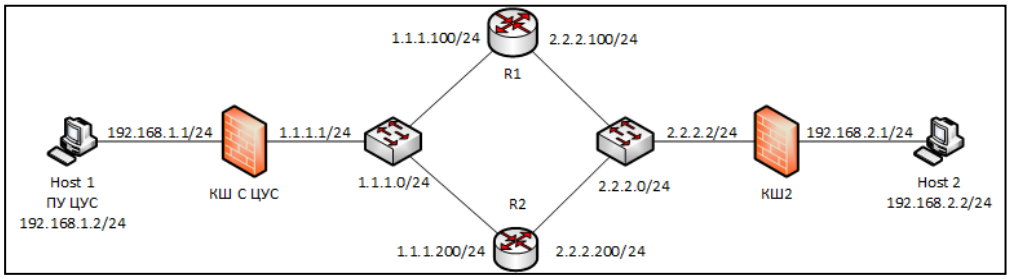
Параметр	Описание
hostname <имя хоста>	Установка имени хоста
interface <имя>	Установка интерфейса
ip forwarding	Включение пересылки IP-пакетов
line vty	Включение режима конфигурирования интерфейса VTY
exec-timeout <минуты секунды>	Установка времени ожидания подключения по VTY
log stdout	Установка режима протоколирования на консоль
log file /var/zebra.log	Экспорт журналов событий динамической маршрутизации из КШ на USB-флеш-накопитель (локально)

Табл.10 Формат файла bgpd.conf

Параметр	Описание
hostname <имя хоста>	Установка имени хоста
router bgp <имя АС>	Включение BGP-процесса для АС
bgp router-id <идентификатор>	Установка ИД роутера
bgp log-neighbor-changes	Включение регистрации изменений состояния BGP-соседей
no synchronization	Отключение синхронизации маршрутов
network <IP-диапазон>	Объявление сети для всех соседей
neighbor <IP-адрес> remote-as <имя АС>	Создание соседа
neighbor <IP-адрес> weight <величина>	Указание веса соседа (больший приоритет имеет сосед с большим весом)
log stdout	Установка режима протоколирования на консоль
log file /var/bgp.log	Экспорт журналов событий динамической маршрутизации из КШ на USB-флеш-накопитель (локально)

Примеры конфигурационных файлов

Данный пример иллюстрирует создание конфигурационных файлов для КШ в типовой схеме включения, показанной на рисунке ниже.



Для приведенной выше схемы конфигурационные файлы имеют следующий вид:

zebra.conf для Host 1

```
hostname CUS
interface em0
ip forwarding
line vty
exec-timeout 0 0
log stdout
log file /var/bgp.log
```

bgpd.conf для Host 1

```
hostname CUS
router bgp 10
bgp router-id 1.1.1.1
bgp log-neighbor-changes
no synchronization
network 1.1.1.0/24
neighbor 1.1.1.100 remote-as 100
neighbor 1.1.1.100 weight 2000
neighbor 1.1.1.200 remote-as 200
neighbor 1.1.1.200 weight 1000
log stdout
log file /var/bgp.log
```

zebra.conf для Host 2

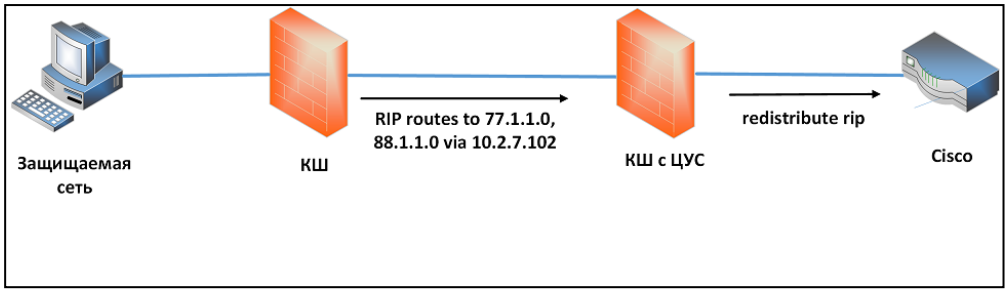
```
hostname CGW2
interface em0
ip forwarding
line vty
exec-timeout 0 0
log stdout
log file /var/bgp.log
```

bgpd.conf для Host 2

```
hostname CGW2
router bgp 20
bgp router-id 2.2.2.2
bgp log-neighbor-changes
no synchronization
network 2.2.2.0/24
neighbor 2.2.2.100 remote-as 100
neighbor 2.2.2.100 weight 2000
neighbor 2.2.2.200 remote-as 200
neighbor 2.2.2.200 weight 1000
log stdout
log file /var/bgp.log
```

Примеры конфигурационного файла RIP

Ниже приведены примеры конфигурационных файлов RIP с фильтрацией маршрутов между двумя узлами — КШ и КШ с ЦУС.



Для КШ конфигурационные файлы имеют следующий вид:

```
zebra.conf
hostname cgw2-zebra
password 123
log stdout
ip route 0.0.0.0 0.0.0.0 10.2.0.1
ip route 155.1.1.0/24 10.2.7.102
ip route 166.1.1.0/24 10.2.7.102
ip route 77.1.1.0/24 10.2.7.102
ip route 88.1.1.0/24 10.2.7.102


ripd.conf
hostname cgw2-rip
password 123
router rip
network em0
neighbor 10.2.7.100
!redistribute connected
no redistribute static
redistribute connected route-map TO-RIP
redistribute kernel route-map TO-RIP
redistribute static route-map TO-RIP
interface em0

ip prefix-list rip-new seq 10 permit 77.1.1.0/24 le 32
ip prefix-list rip-new seq 20 permit 88.1.1.0/24 le 32
ip prefix-list rip-new seq 30 deny any

route-map TO-RIP permit 10
 match ip address prefix-list rip-new
log stdout
```

Для КШ с ЦУС конфигурационные файлы имеют следующий вид:

```
zebra.conf
hostname ncc-zebra
password 123
log stdout
ip route 0.0.0.0 0.0.0.0 10.2.0.1
ip route 100.1.1.0/24 10.2.7.100
ip route 101.1.1.0/24 10.2.7.100
ip route 102.1.1.0/24 10.2.7.100
ip route 103.1.1.0/24 10.2.7.100
ip route 104.1.1.0/24 10.2.7.100
```

```
ripd.conf
hostname ncc-rip
password 123
router rip
network em0
neighbor 10.2.7.102
!redistribute connected
redistribute static
!redistribute kernel
distribute-list private in em0
distribute-list private out em0
access-list private permit any
```

Управление очередью заданий

С помощью ПУ ЦУС можно просмотреть и изменить очередь заданий любого сетевого устройства комплекса. Очередь заданий сетевого устройства содержит список текущих заданий, которые сформированы для устройства, но еще не выполнены.

Для просмотра очереди заданий:

- Выберите в области объектов управления нужное устройство и перейдите к вкладке "Очередь заданий" дополнительного окна.

На этой вкладке отображается список текущих заданий данного сетевого устройства. Этот список будет пуст, если все текущие задания выполнены.

Список заданий, составляющих очередь, отображается в форме таблицы, каждая строка которой соответствует одному заданию.

Табл.11 Перечень полей списка заданий

Поле	Описание
Описание	Наименование задания
Время ожидания	Интервал времени, прошедший с момента формирования задания

В случае необходимости очередь заданий может быть полностью удалена.

Для управления очередью заданий:

1. Для удаления задания выберите его в списке и нажмите на панели инструментов кнопку "Удалить".
2. Для полной очистки очереди заданий нажмите на панели инструментов кнопку "Очистить".

   На экране появится окно подтверждения выполнения операции.
3. Нажмите кнопку "Да" в окне запроса.

   Очередь заданий будет полностью удалена.

Документация

1. Аппаратно-программный комплекс шифрования "Континент". Версия 3.9 (исполнение 3.М3). Руководство администратора. Принципы функционирования комплекса.
2. Аппаратно-программный комплекс шифрования "Континент". Версия 3.9 (исполнение 3.М3). Руководство администратора. Управление комплексом.
3. Аппаратно-программный комплекс шифрования "Континент". Версия 3.9 (исполнение 3.М3). Руководство администратора. Ввод в эксплуатацию.
4. Аппаратно-программный комплекс шифрования "Континент". Версия 3.9 (исполнение 3.М3). Руководство администратора. Межсетевое экранирование.
5. Аппаратно-программный комплекс шифрования "Континент". Версия 3.9 (исполнение 3.М3). Руководство администратора. Настройка VPN.