КОД БЕЗОПАСНОСТИ

Администрирование АПКШ "Континент" версии 3.9. Дополнительные настройки

Учебно-методическое пособие

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

Оглавление

Список сокращений

FPGA	Field-Programmable Gate Array — программируемая логическая интегральная схема (ПЛИС)
ICMP	Internet Control Message Protocol
IP	Internet Protocol
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
USB	Universal Serial Bus
VPN	Virtual Private Network
АПКШ	Аппаратно-программный комплекс шифрования
КК	Криптографический коммутатор
КШ	Криптографический шлюз
ЛВС	Локальная вычислительная сеть
МСЭ	Межсетевой экран
НСД	Несанкционированный доступ
ОС	Операционная система
ПАК	Программно-аппаратный комплекс
ППЖ	Программа просмотра журналов
ПУ	Программа управления
ПУ ЦУС	Программа управления Центром управления сетью
СУ	Сетевое устройство
УЗ	Учетная запись
ЦОД	Центр обработки данных
ЦУС	Центр управления сетью КШ

Введение

Учебно-методическое пособие "Администрирование АПКШ «Континент» версии 3.9. Дополнительные настройки" является продолжением учебно-методического пособия "Администрирование АПКШ «Континент» версии 3.9" и разработано для изучения дополнительных настроек межсетевого экранирования и шифрования в сертифицированном изделии "Аппаратно-программный комплекс шифрования «Континент». Версия 3.9" (далее – комплекс, АПКШ "Континент").

Во время прохождения обучения слушатели на практике будут изучать настройку и работу механизма QoS и параметры шифратора для повышения производительности VPN-соединений.

Учебно-методическое пособие ориентировано на специалистов в сфере информационной безопасности, системных администраторов, руководителей ИТ-служб, архитекторов систем информационной безопасности, которые отвечают за защиту каналов связи при передаче информации ограниченного доступа между сегментами сложных распределенных сетей по публичным или выделенным каналам связи, на всех, кто занимается внедрением, обслуживанием и администрированием систем безопасности, основанных на АПКШ "Континент".

Учебно-методическое пособие предполагает наличие у слушателей опыта администрирования операционных систем Windows и UNIX, понимание принципов работы сетей передачи данных, знание стека протоколов TCP/IP, а также наличие опыта настройки оборудования локальной сети. Также предполагается, что слушатели прошли учебный курс "Администрирование АПКШ «Континент» версии 3.9".

Данное учебно-методическое пособие рассчитано на 1-дневное обучение (8 академических часов) в учебном центре под руководством сертифицированного ООО "Код Безопасности" преподавателя – специалиста по АПКШ "Континент".

Условные обозначения

В учебно-методическом пособии для выделения некоторых элементов текста (примечаний и ссылок) используется ряд условных обозначений.

Внутренние ссылки обычно содержат указание на номер страницы с нужными сведениями. Ссылки на другие документы или источники информации размещаются в тексте примечаний или на полях.

Важная и дополнительная информация оформлена в виде примечаний. Степень важности содержащихся в них сведений отображают пиктограммы на полях:

- так обозначается дополнительная информация, которая может содержать примеры, ссылки на другие документы или другие части методического пособия;

- такой пиктограммой выделяется важная информация, которую необходимо принять во внимание;

- эта пиктограмма сопровождает информацию предостерегающего характера.

Исключения. Некоторые примечания могут и не сопровождаться пиктограммами. А на полях, помимо пиктограмм примечаний, могут быть приведены и другие графические элементы, например, изображения кнопок, действия с которыми упомянуты в тексте расположенного рядом абзаца.

Другие источники информации

Сайт в интернете. Если у вас есть доступ в интернет, вы можете посетить сайт компании "Код Безопасности" (https://www.securitycode.ru/) или связаться по вопросам технического характера с представителями компании по электронной почте (info@securitycode.ru).

Учебные курсы. Перечень курсов и условия обучения представлены на сайте https://www.securitycode.ru.

Глава 1
Управление QoS

Определение классов трафика

Классы трафика описываются администратором в ПУ ЦУС и используются при проведении следующих настроек:

- определение правил балансировки трафика (Multi-WAN);
- описание очередей на отправку IP-пакетов на сетевом интерфейсе (механизм QoS);
- определение очередности обработки IP-пакетов блоком криптографической защиты (механизм QoS) посредством указания приоритета шифрования. Возможные значения: 0–31, большему значению соответствует более высокий приоритет.

При инициализации ЦУС автоматически создается класс трафика "Нормальный" с установленным приоритетом уровня 5 и портом 10000 внешнего интерфейса.

Настройка приоритизации трафика

Комплекс поддерживает механизм управления QoS, который позволяет приоритизировать IP-трафик, обеспечивая тем самым высокое качество передачи данных. Это имеет большое значение, например, при использовании приложений видеоконференций, где устойчивость и скорость сетевого трафика влияют на качество передачи изображения и звука. Кроме того, механизм QoS позволяет регулировать пропускную способность передаваемого трафика (traffic shaping) путем резервирования либо ограничения полосы пропускания для определенного протокола передачи данных.

В сети по умолчанию (без использования очередей) стек TCP/IP и его подсистема фильтрации обрабатывают пакеты в порядке их поступления на интерфейс (FIFO – первым вошел – первым вышел).

Приоритизация трафика основана на распределении пакетов по очередям с целью управления пропускной способностью. Очереди являются одной из форм буферов для сетевых пакетов. Пакеты будут находиться в очереди до тех пор, пока они не будут либо удалены, либо отправлены по пути их следования, в зависимости от критериев и с учетом доступной пропускной способности данной очереди.

Очереди прикрепляются к конкретным интерфейсам, и управление пропускной способностью осуществляется на базе интерфейса, с разделением доступной пропускной способности.

Очереди выделяют определенную часть из полосы пропускания, а иногда и иерархический приоритет. В данном контексте приоритет является показателем предпочтений того, какую очередь необходимо обслуживать в кратчайшие сроки. Некоторые очереди могут настраиваться в сочетании выделения полосы пропускания и приоритета.

После определения очередей распределение по ним трафика будет осуществляться через набор правил, которые следует переписать с указанием конкретной очереди для каждого вида трафика. При этом любой трафик, который явно не назначен в определенную очередь, ставится в очередь по умолчанию. Алгоритм распределения определяет, какие пакеты будут задержаны, какие отброшены, а какие сразу переданы. В комплексе поддерживаются три планировщика очередей:

- PRIQ (Priority Queueing). Очереди основаны на приоритетах в общей полосе пропускания. У них не может быть дочерних очередей. Каждой очереди присваивается уникальный приоритет в диапазоне от 0 до 15. Пакеты с высшим номером приоритета обслуживаются быстрее;
- CBQ (Class Based Queueing). Очереди основаны на классах и определяют постоянную аренду пропускной способности от общедоступной либо в процентах, либо в единицах килобит, мегабит или гигабит в секунду. Присоединенные к интерфейсу очереди могут иметь дочерние очереди, создавая дерево. Для каждой очереди назначается пропускная способность и приоритет в диапазоне от 0 до 7 (более высокий приоритет обслуживается в первую очередь). Пакеты

находятся в очереди, пока доступна полоса пропускания. Для очередей, которые подразделяются на очереди с приоритетом и ассигнованием пропускной способности, пакеты, соответствующие критериям более высокого приоритета, обслуживаются быстрее. За счет этого регулируется пропускная способность;

- HFSC (Hierarchical Fair Service Curve). В родительской очереди определяется суммарная пропускная способность для всех очередей интерфейса (общая пропускная способность, предоставляемая провайдером и не зависящая от скорости сетевого интерфейса). В дочерней очереди эта директива определяет максимальную скорость передачи информации в битах, которая будет обработана очередью в любой момент. Таким образом, режим HFSC позволяет создавать очереди с гарантированным минимальным выделением полосы и жесткими верхними лимитами.

Примечание. Приоритизировать можно только исходящий (upload) трафик, так как входящий (download) уже пришел и ограничить его нельзя.

Настройки шифрования для оптимизации работы комплекса при организации L2 и L3VPN

Сетевое взаимодействие между абонентами VPN-соединения обеспечивается криптошлюзами (L3VPN) и криптокоммутаторами (L2VPN) "Континент" по–разному. КШ отслеживает соединения (сессии) на уровне L3/L4 и использует для этого в настройках шифратора структуру L3-хэша – совокупность IP-адреса, протокола и порта источника и IP-адреса, протокола и порта получателя. КК работает на уровне L2 и для идентификации сессий использует L2-хэш, в котором указаны MAC-адреса взаимодействующих хостов, подключенных к портам парных (связанных) криптокоммутаторов.

В "Континент" 3.9 шифрование трафика при VPN-соединении построено на так называемых потоках шифрования, которые могут распределяться по ядрам процессора. Шифрование одной сессии между абонентами сетевого обмена более качественно производится в одном потоке на одном физическом/логическом ядре процессора. Поэтому:

- на одной сессии (один поток шифрования на одном ядре процессора) невозможно добиться максимальной производительности узла "Континент";
- общая пропускная способность будет максимальной только при одновременном запуске нескольких соединений передачи данных (несколько потоков шифрования, распределенных по ядрам процессора).

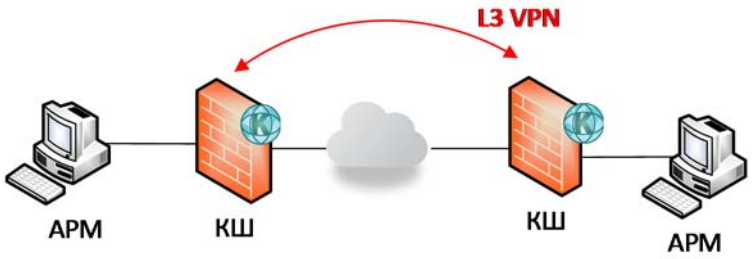
Для оптимизации работы шифратора и управления распределением шифрования сессий по ядрам процессора при организации VPN в локальном меню сетевых узлов "Континент" предусмотрены следующие настройки:

- "Разрешение / Запрет распределения пакетов с учетом соединений" – опция позволяет включить/отключить распределение потоков шифрования по ядрам процессора. По умолчанию на КШ данный параметр включен (разрешено распределение потоков по ядрам), а на КК – выключен (см. ниже);
- "Задать число потоков шифрования" – опция позволяет явно указать при необходимости количество потоков шифрования. По умолчанию данный параметр определен системой. На младших платформах количество потоков автоматически установлено как 75% от текущего количества доступных ядер. При этом в настройках BIOS рекомендуется включить параметр "Hyper-threading" (HT). Для некоторых младших платформ (новых моделей) количество потоков по умолчанию определено отдельно. На средних и старших платформах количество потоков шифрования определено аналогично.

Как уже отмечалось, КШ отслеживает сессии на уровне L3/L4 по совокупности IP-адреса, протокола и порта источника и IP-адреса, протокола и порта получателя. Если в VPN-канале между двумя хостами из защищаемых сетей запущено несколько сетевых соединений, например, по SMB-, RDP- и HTTP-протоколам, то каждое из них будет отдельной сессией и будет шифроваться в отдельном потоке. В этом случае включенное по умолчанию распределение потоков шифрования по ядрам процессора является оптимальной настройкой шифратора, поскольку каждая сессия будет шифроваться одним ядром и таким образом будет обеспечена максимальная производительность узла и наиболее полная утилизация сетевого канала.

Если же в VPN-канале между двумя хостами из защищаемых сетей запущено только одно сетевое соединение (например, по SMB-протоколу), производительность КШ при включенном распределении потоков шифрования по ядрам процессора будет ограничена производительностью одного ядра и утилизации канала в этом случае добиться не удастся.

Сессия: "Source_ip:proto:port – Destination_ip:proto:port"

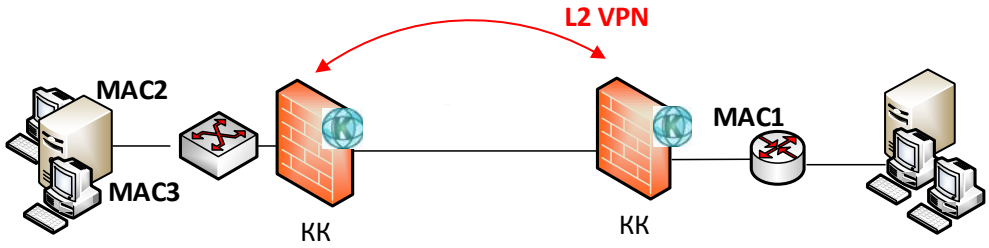


У КК сессия – это обмен между хостами по MAC-адресам. Если за портами криптокоммутаторов располагаются маршрутизаторы, то для КК все сетевое взаимодействие между хостами через VPN-канал будет считаться одной сессией. В этом случае оптимальным для производительности будет установленный по умолчанию запрет распределения шифрования соединений по ядрам процессора. Тогда общая пропускная способность канала будет максимальной только в случае наличия одновременно десятков соединений на L3-уровне. Утилизация канала будет близка к максимальной, но в то же время каждое из соединений будет работать на минимальной скорости передачи.

Если же при такой конфигурации включить распределение, то для шифрования будет задействовано только одно ядро процессора, а остальные будут простаивать. Утилизации канала в этом случае добиться не удастся, но в то же время при наличии только одного соединения на уровне L3+L4 (например, копирование файла по SMB-протоколу) для него будет достигнута максимальная скорость передачи.

В случае подключения защищаемых хостов к портам криптокоммутатора без промежуточного L3-оборудования (т.е. КК "видит" всю защищаемую сеть, много сессий по MAC-адресам) оптимальным будет разрешить распределение пакетов с учетом соединений (изменить настройку по умолчанию). Тогда будет достигнуто оптимально максимальное использование ресурсов КК и канала передачи данных.

Сессия: "MACx – MACy"



В комплексе "Континент" версии 3.9.1 будут сделаны следующие доработки:

- распознавание сессий в КК по уровню L3 (IP-адрес + протокол). То есть если между двумя хостами будут запущены, например, SMB-, RDP- и HTTP-соединения – это будет считаться одной сессией и будет шифроваться на одном ядре;
- достижение производительности работы сетевых устройств на одной сессии до 70% от заявленной.

Лабораторный модуль №1 "Управление QoS"

Краткое описание учебного стенда

Поскольку данный курс является продолжением основного учебного курса "Администрирование АПКШ «Континент» версии 3.9", для выполнения лабораторных работ рекомендуется использовать виртуальные машины учебного стенда из основного курса (см. рис. 1).

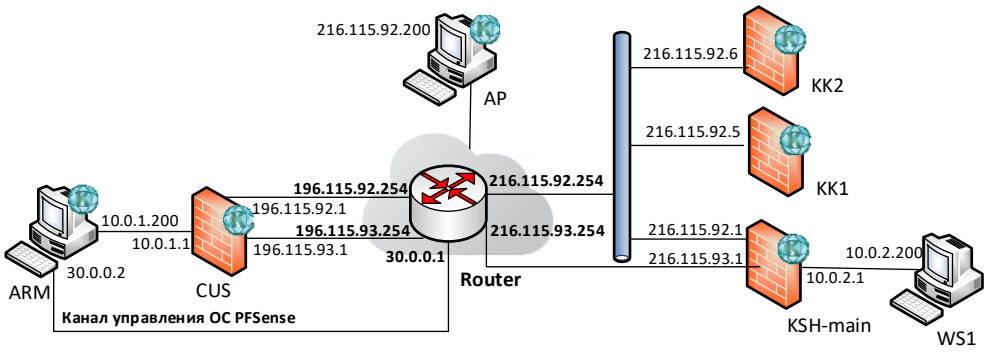


Рис. 1. Схема стенда "Континент" 3.9

Стенд содержит следующие виртуальные локальные подсети:

- 10.0.1.X/24 – имитирует внутреннюю/защищаемую сеть организации;
- 196.115.92.X/24 и 196.115.93.X/24 – имитируют внешние сети организации;
- 216.115.92.X/24 и 216.115.93.X/24 – имитируют внешние сети филиала;
- 10.0.2.X/24 – имитирует внутреннюю/защищаемую сеть филиала;
- 30.0.0.X/30 – подсеть управления маршрутизатором.

Далее приводится краткое описание всех ВМ стенда. Детальные характеристики виртуальных машин и подробная инструкция по развертыванию и подготовке к работе стенда содержатся в документе "Описание стенда" (файл "cont39_add_stand.docx").

ВМ **Router** выполняет функции роутера с установленной гостевой ОС pfSense 2.4.4-p3 (64-bit) с пакетом OpenBGPD и следующими настройками:

- прописаны адреса сетевых интерфейсов без указания шлюза по умолчанию (см. рис. 1):
  - WAN (le0) – 196.115.92.254/24;
  - OPT1 (le1) – 196.115.93.254/24;
  - OPT2 (le2) – 216.115.92.254/24;
  - OPT3 (le3) – 216.115.93.254/24;
  - LAN (le4) – 30.0.0.1/30;
- для управления маршрутизатором используйте следующие параметры подключения через веб-интерфейс: адрес – **https://30.0.0.1**, логин – **admin**, пароль – **pfsense**;
- добавлены статические маршруты согласно таблице ниже;

IP-адрес сети (хоста) назначения и маска	IP-адрес шлюза по умолчанию
10.0.1.200 mask 255.255.255.255	196.115.92.1
10.0.2.200 mask 255.255.255.255	216.115.92.1

- для сетевых интерфейсов WAN, OPT1, OPT2 и OPT3 установлены правила контроля трафика согласно таблице ниже.

Действие	Версия TCP/IP	Протокол	Источник, порт	Получатель, порт
pass	IPv4	TCP/UDP	any	any
pass	IPv4	ICMP	any	any
pass	IPv6	any	any	any

ВМ **CUS** выполняет функции криптографического шлюза с установленной ОС "Континент" в конфигурации "центр управления сетью, сервер доступа". Параметры ЦУС:

- идентификатор криптошлюза – **1010**;
- строка конфигурации КШ:

000003F24em0*02BDem1*02BDem2*02BDem3*02BDffff;

- номер модели аппаратной платформы **4** – IPC-25 (92D9);
- выполнены инициализация сетевого устройства, описание сетевых интерфейсов и параметров маршрутизации согласно схеме учебного стенда. Реквизиты главного администратора – **admin / 11111111**.

ВМ **ARM** выполняет функции рабочего места администратора АПКШ "Континент" с подсистемой управления. Данная ВМ имеет следующие характеристики:

- установлена роль веб-сервера (IIS) вместе со службами ftp-сервера;
- установлен Internet Explorer 11;
- встроенная УЗ локального администратора: логин – **Администратор**, пароль – **P@ssw0rd**;
- выключены UAC и брандмауэр Windows;
- установлена СУБД MS SQL 2008 Express x64;
- установлены агент ЦУС и СД, ПУ ЦУС и настроено подключение к ЦУС с реквизитами главного администратора – **admin / 11111111**;
- на локальном диске "C:\" в папке "Дистрибутивы" размещено необходимое ПО.

ВМ **KSH-main** выполняет функции криптографического шлюза "Континент". Выполнены инициализация сетевого устройства, описание сетевых интерфейсов и параметров маршрутизации согласно схеме учебного стенда. Реквизиты локального администратора – **kshadmin / P@ssw0rd**.

ВМ **KK1** и **KK2** выполняют функции криптографических коммутаторов "Континент". Выполнены инициализация сетевых устройств, описание сетевых интерфейсов и параметров маршрутизации согласно схеме учебного стенда. Реквизиты локального администратора – **kk1admin / P@ssw0rd** и **kk2admin / P@ssw0rd** соответственно. Установлена связь между криптокоммутаторами.

ВМ **AP** выполняет роль рабочей станции. Данная ВМ имеет следующие характеристики:

- установлена гостевая ОС Microsoft Windows 7 SP1 (64-bit);
- прописаны параметры сетевых интерфейсов согласно рис. 1, выключен протокол IPv6 и заданы параметры маршрутизации согласно таблице ниже;

IP-адрес сети (хоста) назначения и маска	IP-адрес шлюза по умолчанию
0.0.0.0 mask 0.0.0.0	216.115.92.254

- на локальном диске "C:\" размещена папка "Дистрибутивы" с необходимым ПО;
- в папке "C:\test" созданы папки "up" и "down", к которым настроен общий доступ. В папке "up" размещен файл для скачивания размером 1,6 Гбайт;
- УЗ локального администратора: логин – **admin**, пароль – **P@ssw0rd**;
- выключен брандмауэр Windows.

ВМ **WS1** выполняет роль компьютера в защищаемой сети и имеет следующие характеристики:

- установлена гостевая ОС Microsoft Windows Server 2008 R2 SP1 (64-bit);
- прописаны параметры сетевых интерфейсов согласно рис. 1, выключен протокол IPv6 и заданы параметры маршрутизации согласно таблице ниже;

IP-адрес сети (хоста) назначения и маска	IP-адрес шлюза по умолчанию
0.0.0.0 mask 0.0.0.0	10.0.2.1

- установлен компонент "Клиент Telnet";
- на локальном диске "C:\" в папке "Дистрибутивы" размещено необходимое ПО;
- в папке "C:\test" созданы папки "up" и "down", к которым настроен общий доступ. В папке "up" размещен файл для скачивания размером 1,6 Гбайт;

- УЗ локального администратора: логин – **admin**, пароль – **P@ssw0rd**;
- разрешено подключение по RDP и выключен переход в спящий режим;
- выключен брандмауэр Windows.

Перед началом работы стенд следует развернуть с использованием VMware vSphere Client. Файл-образы пула находятся в комплекте с методическими материалами по данному курсу.

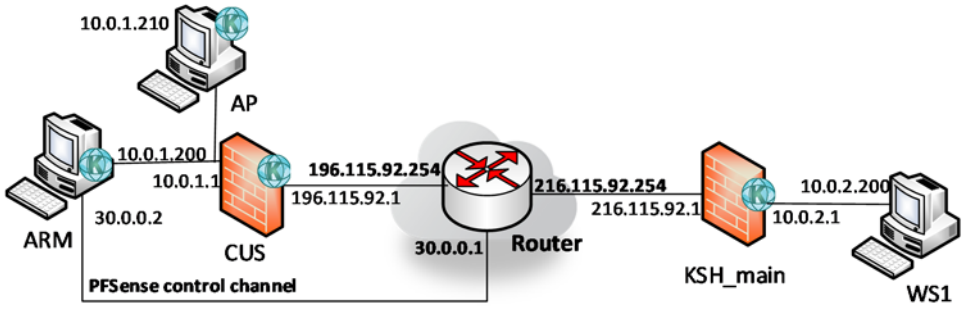
Здесь и далее в лабораторных работах предполагается, что:

- стенд развернут и вы подключились к нему с помощью клиента VMware vSphere Client;
- включена ВМ Router. Остальные виртуальные машины включаются/выключаются по ходу выполнения лабораторных работ;
- по ходу выполнения лабораторных работ все необходимые изменения на стенде проводятся слушателями самостоятельно.

Лабораторная работа №1 "Настройка QoS на сетевых интерфейсах узлов "Континент"

Сценарий. Для приоритизации отдельных видов IP-трафика с целью повышения качества передачи данных между защищаемыми сетями, которые располагаются за разными криптошлюзами "Континент", администратор настраивает на КШ механизм управления QoS и описывает параметры очередей для передаваемого трафика (traffic shaping) путем ограничения полосы пропускания для определенных протоколов передачи данных.

В данной лабораторной работе задействованы ВМ, которые показаны на рисунке ниже.



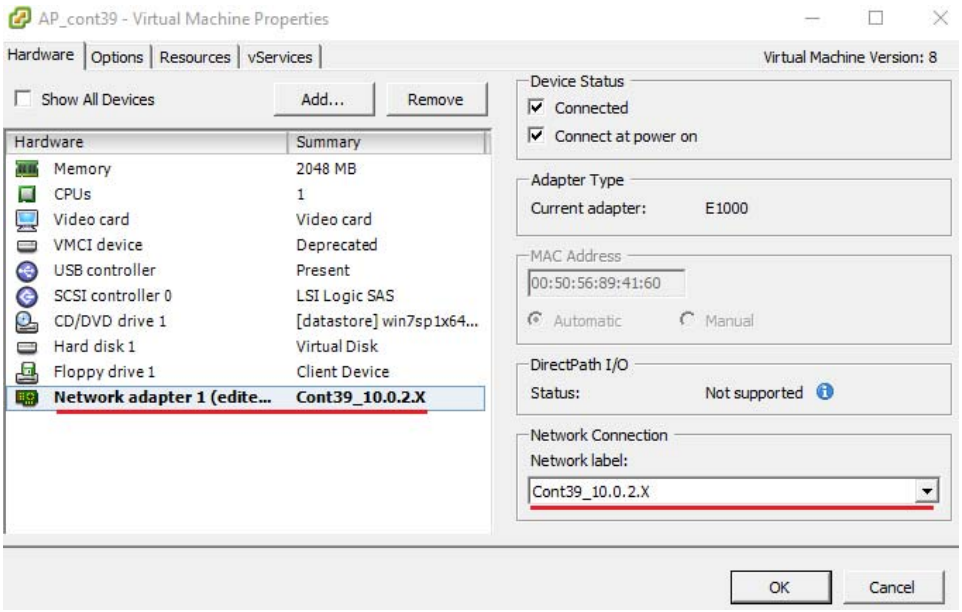
Настройка на криптошлюзах "Континент" механизма управления QoS и проверка его работы будет проводиться в следующем порядке:

1. Для последующего сравнения оценивается средняя скорость передачи трафика (SMB-протокол) при прямом сетевом взаимодействии (без промежуточных сетевых узлов) в разных направлениях.
2. Оценивается средняя скорость передачи трафика по отдельным сетевым протоколам (SMB- и FTP-протоколы) в разных направлениях при взаимодействии между защищаемыми подсетями, которые расположены за разными криптошлюзами "Континент". Полученные результаты сравниваются с показателями из п. 1.
3. На сетевых интерфейсах узлов "Континент" через ПУ ЦУС проводится настройка очередей для передаваемого трафика путем ограничения полосы пропускания для SMB- и FTP-протоколов передачи данных.
4. Оценивается средняя скорость передачи трафика между защищаемыми подсетями по SMB- и FTP-протоколам в разных направлениях с учетом сделанных настроек механизма QoS. Полученные результаты сравниваются с показателями из п. 2.

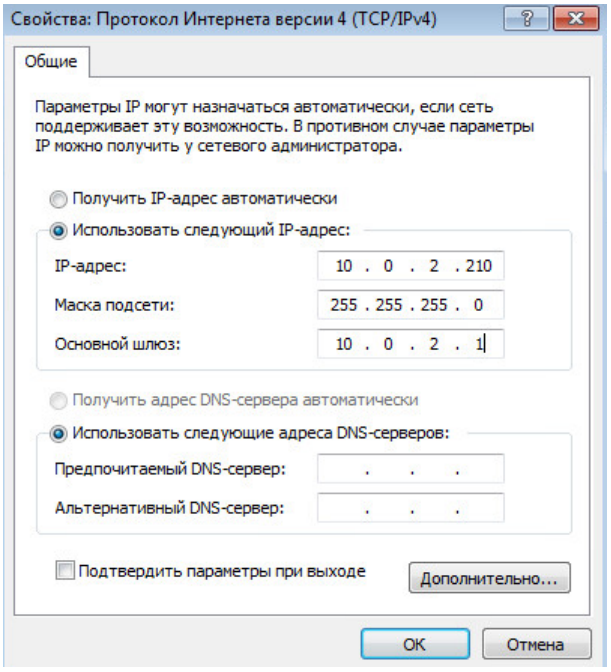
Внимание! Перед началом выполнения лабораторной работы убедитесь, что к ВМ ARM подключен съемный USB-флеш–накопитель с файлом "contkey.str", содержащим ключ администратора ЦУС.

1. Измените настройки учебного стенда так, чтобы между виртуальными машинами AP и WS1 было прямое сетевое взаимодействие. Для этого на ВМ AP сделайте следующее:

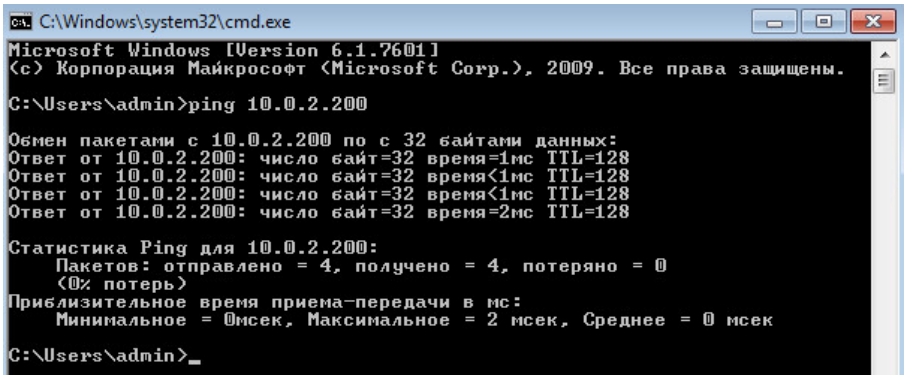
- в настройках ВМ переподключите сетевой интерфейс на тот, к которому подключена ВМ WS1;



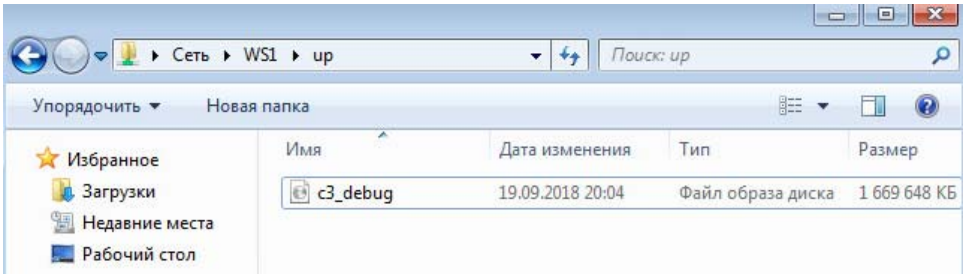
- в свойствах сетевого подключения в ОС Windows установите: IP-адрес / маска – **10.0.2.210/255.255.255.0**, основной шлюз – **10.0.2.1**;

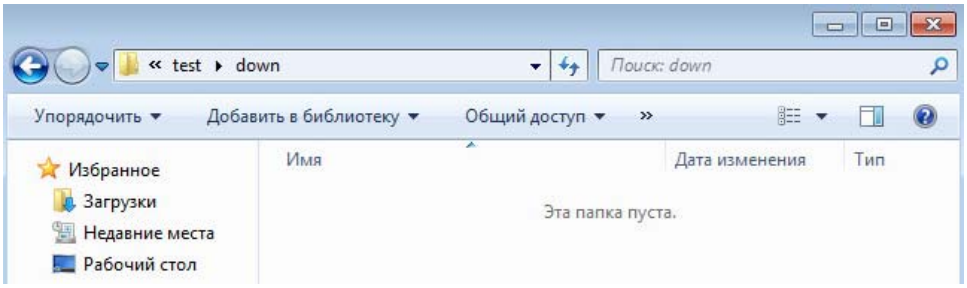


- перезагрузите ВМ, авторизуйтесь с УЗ **admin / P@ssw0rd** и убедитесь в сетевой доступности ВМ WS1.

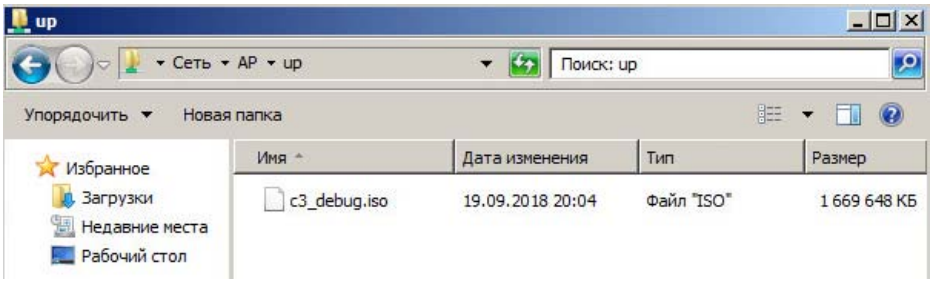


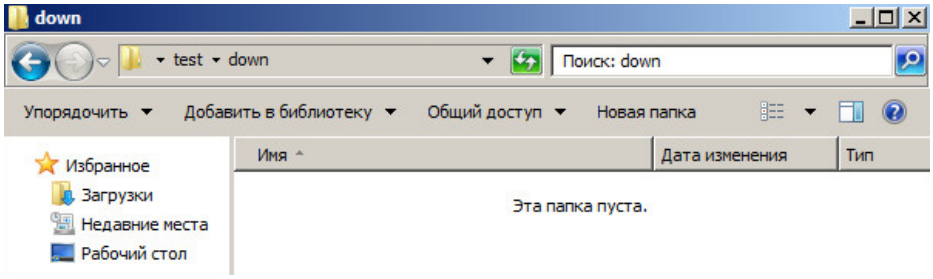
2. Убедитесь, что на виртуальных машинах AP и WS1:
   - сетевые интерфейсы работают со скоростью 1 Гбит/с;
   - значение MTU – 1500 байт **(netsh interface ipv4 show subinterfaces)**.
3. Проведите оценку средней скорости передачи трафика в разных направлениях между виртуальными машинами AP и WS1 в процессе копирования файла с использованием папок общего доступа ОС Windows (протокол SMB). Для этого сделайте следующее:
   - в окне консоли ВМ AP откройте расположенную на ВМ WS1 общедоступную папку "up" (локальный путь – "C:\test\up"), содержащую файл размером 1,6 Гбайт, а также локальную пустую папку "C:\test\down";



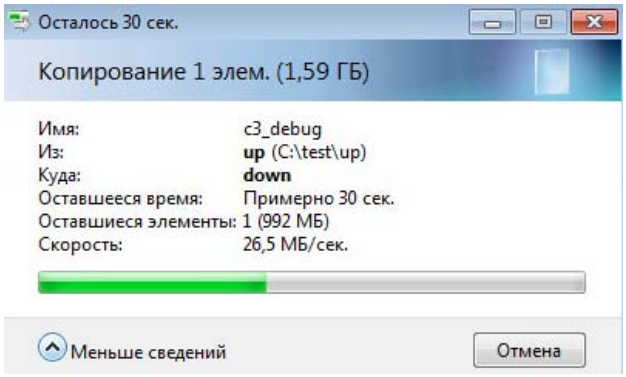


   - в окне консоли ВМ WS1 откройте расположенную на ВМ AP общедоступную папку "up" (локальный путь – "C:\test\up"), содержащую файл размером 1,6 Гбайт, а также локальную пустую папку "C:\test\down";

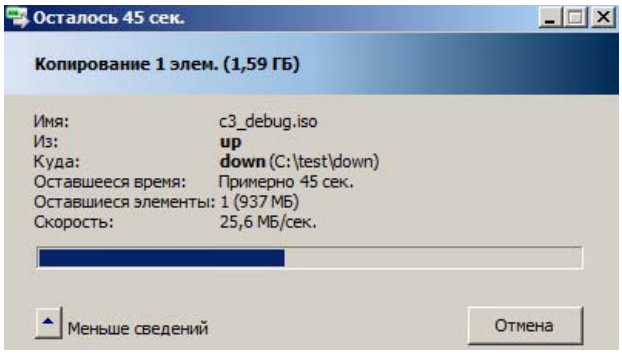




- в окне консоли ВМ АР (ОС Windows 7 SP1 x64) запустите процесс копирования файла с ВМ WS1 (ОС Windows Server 2008 R2 SP1 x64) из общедоступной папки "up" в локальную папку "C:\test\down" и оцените среднюю скорость передачи (поскольку учебный стенд построен в виртуальной среде, показатели скорости копирования будут зависеть от степени загруженности ESXi-сервера);



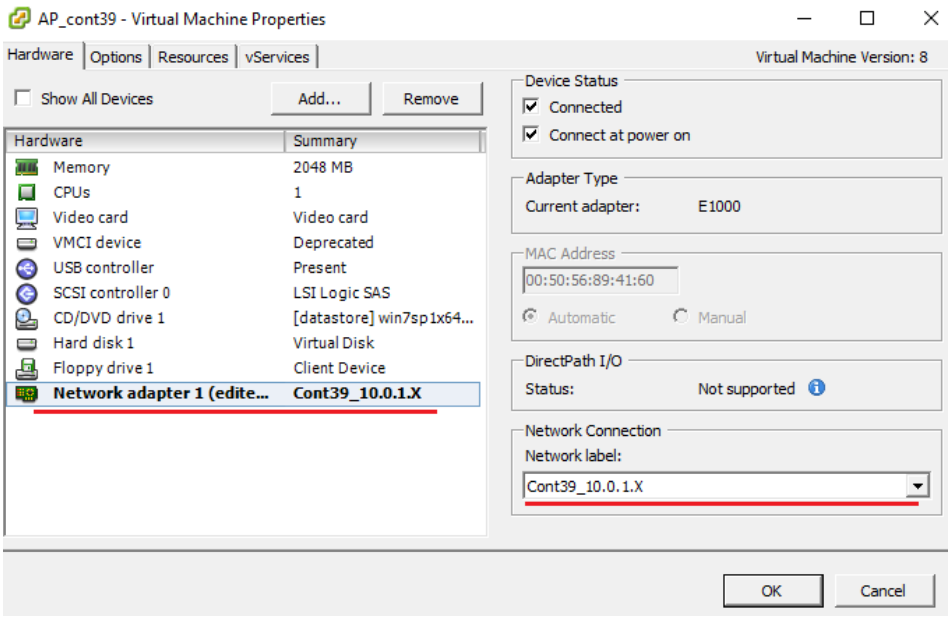
- в окне консоли ВМ WS1 (ОС Windows Server 2008 R2 SP1 x64) запустите процесс копирования файла с ВМ АР (ОС Windows 7 SP1 x64) из общедоступной папки "up" в локальную папку "C:\test\down" и оцените среднюю скорость передачи (поскольку учебный стенд построен в виртуальной среде, показатели скорости копирования будут зависеть от степени загруженности ESXi-сервера);



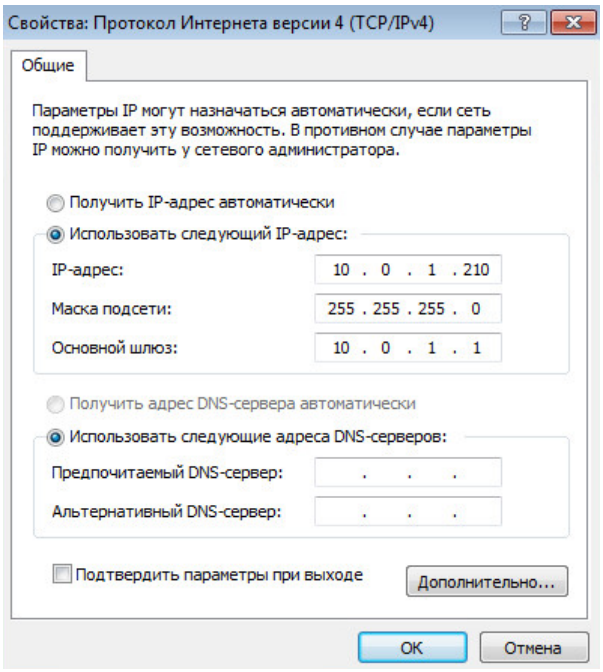
- на ВМ WS1 и АР удалите скопированный файл (<Shift>+<Del>) из локальной папки "C:\test\down".

4. Измените настройки виртуальной машины АР так, чтобы виртуальные машины АР и WS1 располагались за разными криптошлюзами. Для этого на ВМ АР сделайте следующее:

   - в настройках ВМ переподключите сетевой интерфейс на тот, к которому подключен внутренний сетевой интерфейс КШ с ЦУСом;



- в свойствах сетевого подключения в ОС Windows установите: IP-адрес / маска – **10.0.1.210/255.255.255.0**, основной шлюз – **10.0.1.1**;



- перезагрузите ВМ и авторизуйтесь с УЗ **admin / P@ssw0rd**.

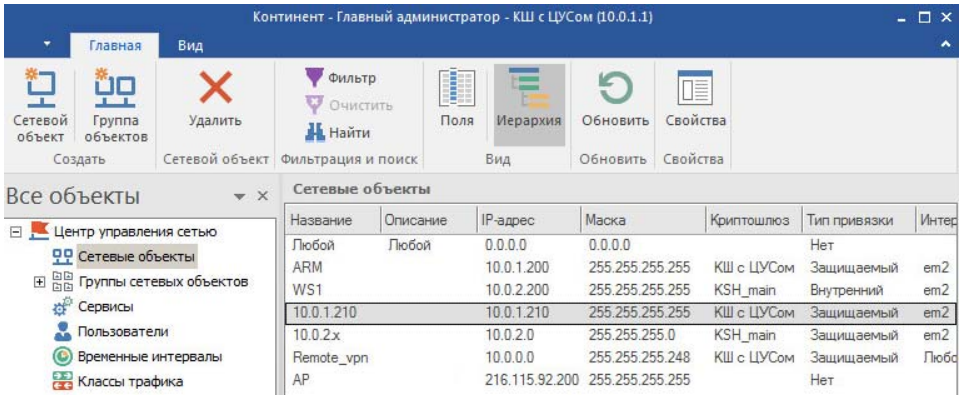
5. Для того чтобы обеспечить сетевое взаимодействие между виртуальными машинами, которые располагаются за разными сетевыми узлами "Континент", и описать трафик, который будет приоритизироваться посредством очередей, переключитесь в окно ВМ ARM и в ПУ ЦУС сделайте следующее:

- создайте новые сетевые объекты или внесите изменения в уже существующие с реквизитами согласно представленным ниже таблицам;

Наименование поля	**Значение**	**Значение**
Название	10.0.1.210	10.0.2.x
IP-адрес/маска	10.0.1.210/255.255.255.255	10.0.2.0/255.255.255.0
Тип привязки	Защищаемый	Защищаемый
Криптошлюз	КШ с ЦУСом	KSH_main
Интерфейс	em2	em2

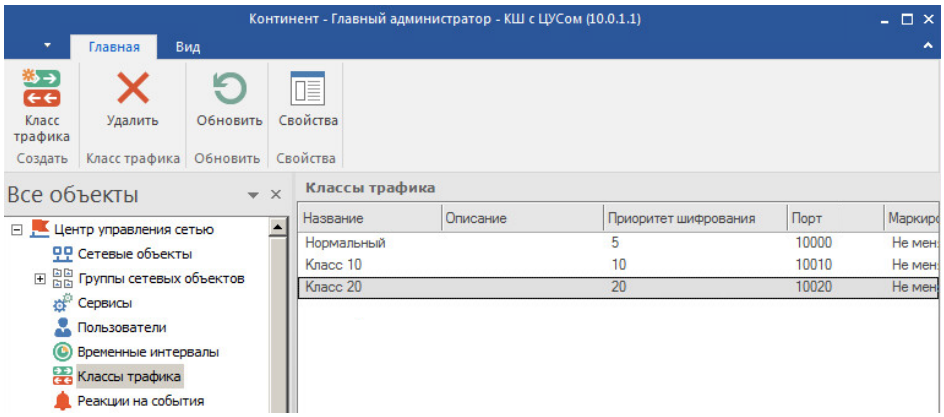
Наименование поля	**Значение**	**Значение**
Название	ARM	WS1

Наименование поля	Значение	Значение
IP-адрес/маска	10.0.1.200/255.255.255.255	10.0.2.200/255.255.255.255
Тип привязки	Защищаемый	Внутренний
Криптошлюз	КШ с ЦУСом	KSH_main
Интерфейс	em2	em2



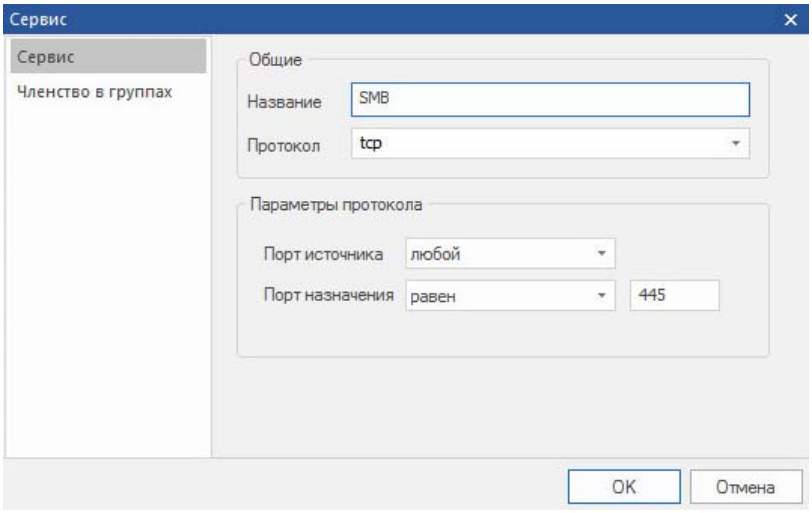
- в области объектов управления выберите "Центр управления сетью / Классы трафика" и убедитесь, что помимо записи по умолчанию "Нормальный" в списке присутствуют два класса трафика с параметрами согласно представленной ниже таблице;

Класс трафика	**Класс 10**	**Класс 20**
Приоритет шифрования	10	20
Порт внешнего интерфейса для зашифрованного трафика	10010	10020



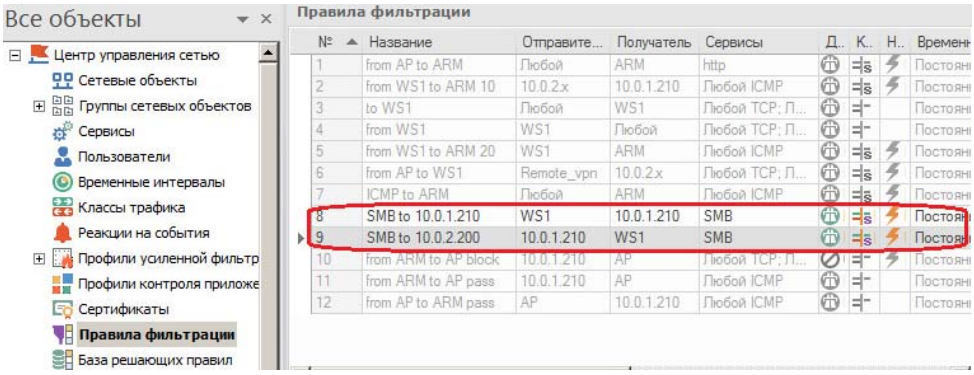
- в области объектов управления выберите "Центр управления сетью / Сервисы" и с помощью кнопки "Создать сервис" (

) создайте сетевой сервис (элемент правила фильтрации IP-пакетов, определяющий их характеристики, для которых это правило будет действовать) с реквизитами согласно представленному ниже рисунку;



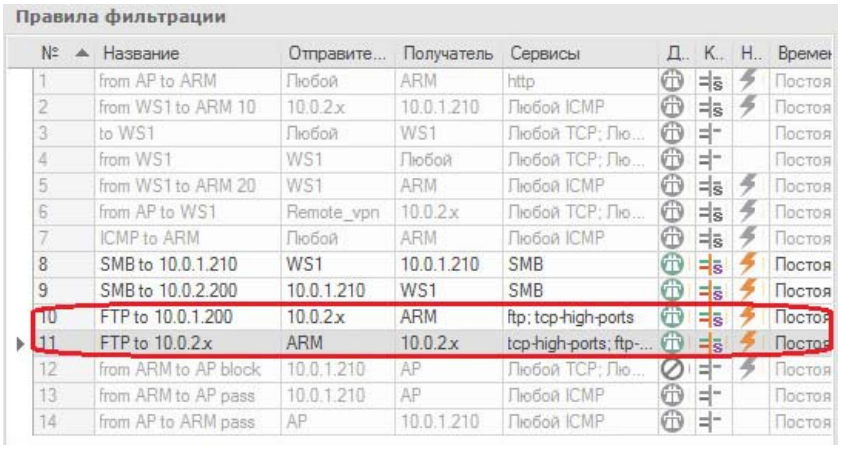
- создайте правила фильтрации или внесите изменения в уже существующие с реквизитами согласно представленной ниже таблице;

Наименование поля	Значение	Значение
Название	SMB to 10.0.1.210	SMB to 10.0.2.200
Отправитель	WS1	10.0.1.210
Получатель	10.0.1.210	WS1
Сервисы	SMB	SMB
Действие	Пропустить	Пропустить
Класс трафика	"Класс 10"	"Класс 10"
Контролировать состояние соединений	Включить	Включить
Применить и завершить обработку	Включить	Включить



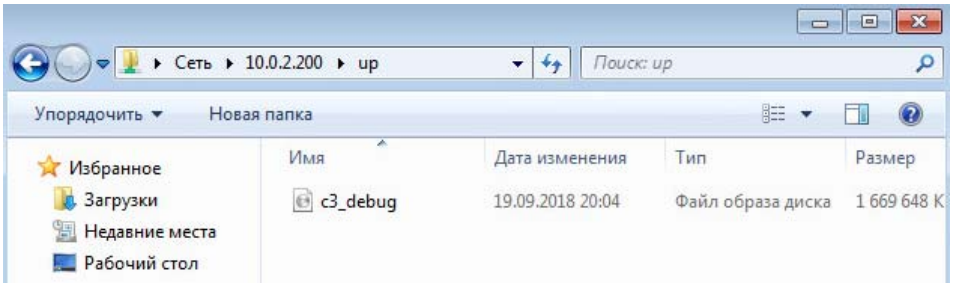
- создайте правила фильтрации с реквизитами согласно представленной ниже таблице, а затем – сохраните сделанные изменения.

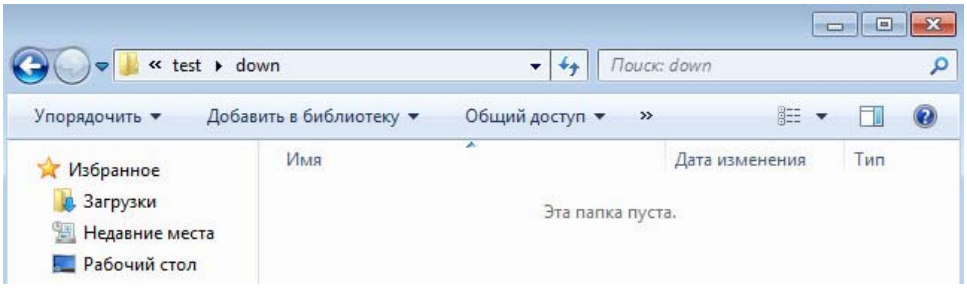
Наименование поля	Значение	Значение
Название	FTP to 10.0.2.x	FTP to 10.0.1.200
Отправитель	ARM	10.0.2.x
Получатель	10.0.2.x	ARM
Сервисы	ftp-data, tcp-high-ports	ftp, tcp-high-ports
Действие	Пропустить	Пропустить
Класс трафика	"Класс 20"	"Класс 20"
Контролировать состояние соединений	Включить	Включить
Применить и завершить обработку	Включить	Включить



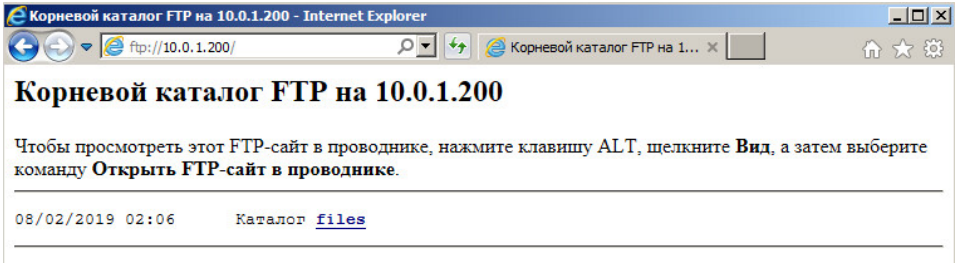
6. Проведите оценку скорости передачи SMB- и FTP-трафика между сетевыми узлами "Континент" и сравните результаты с показателями, которые были получены в процессе копирования файлов с использованием папок общего доступа (протокол SMB) при выполнении п. 3 данной лабораторной работы. Для этого сделайте следующее:

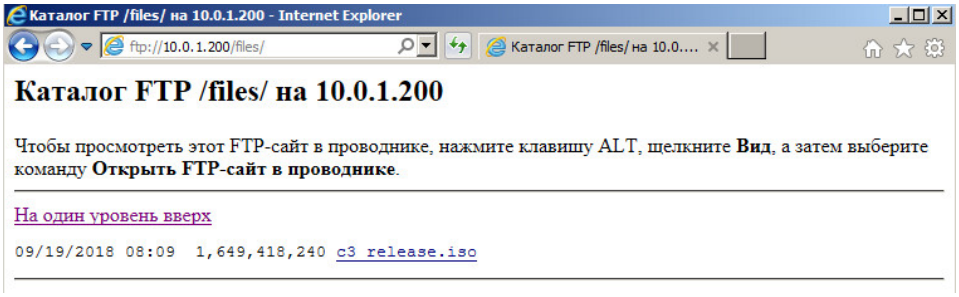
- в окне консоли ВМ AP откройте расположенную на ВМ WS1 (10.0.2.200) общедоступную папку "up" (локальный путь – "C:\test\up"), содержащую файл размером 1,6 Гбайт, а также локальную папку "C:\test\down";



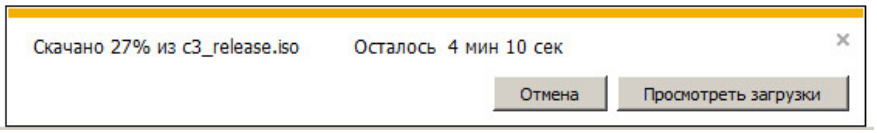


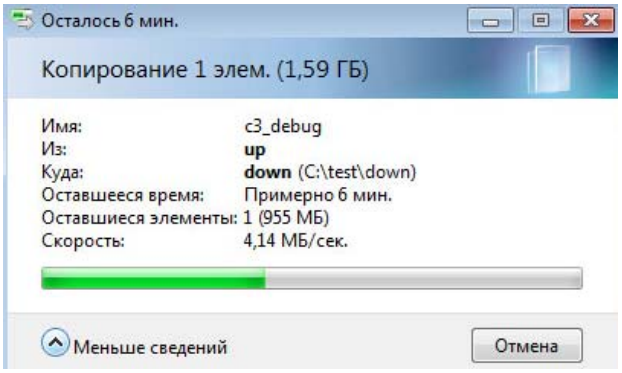
- в окне консоли ВМ WS1 откройте браузер IE и в адресной строке введите ftp://10.0.1.200 – откроется страница корневого каталога FTP–сайта (ВМ ARM, 10.0.1.200). Выберите папку "files", содержащую файл для скачивания;





- запустите одновременно два параллельных процесса:
  - в окне консоли ВМ WS1 в браузере IE сохранение файла с FTP-сервера (ВМ ARM, 10.0.1.200) в локальную папку "C:\test\down";
  - в окне консоли ВМ AP копирование файла из общедоступной папки "up" на ВМ WS1 в локальную папку "C:\test\down";
- по ходу выполнения запущенных процессов скачивания файлов обратите внимание на следующие моменты:
  - передача трафика по FTP- и SMB-протоколам проходит с примерно одинаковой скоростью;

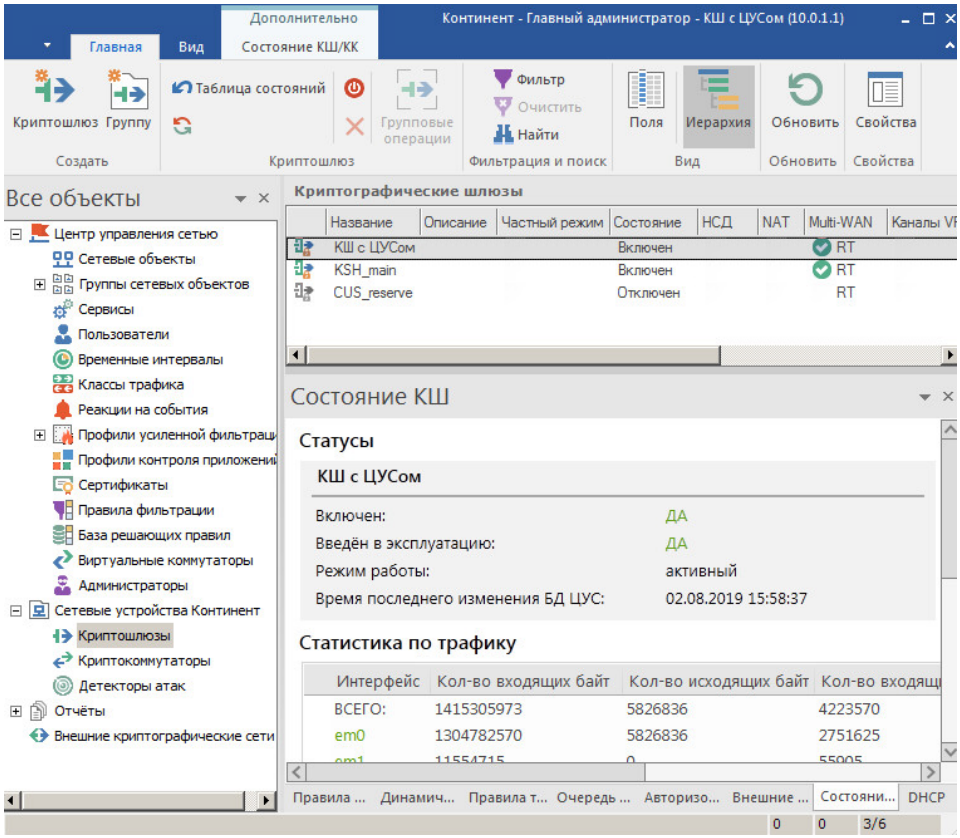




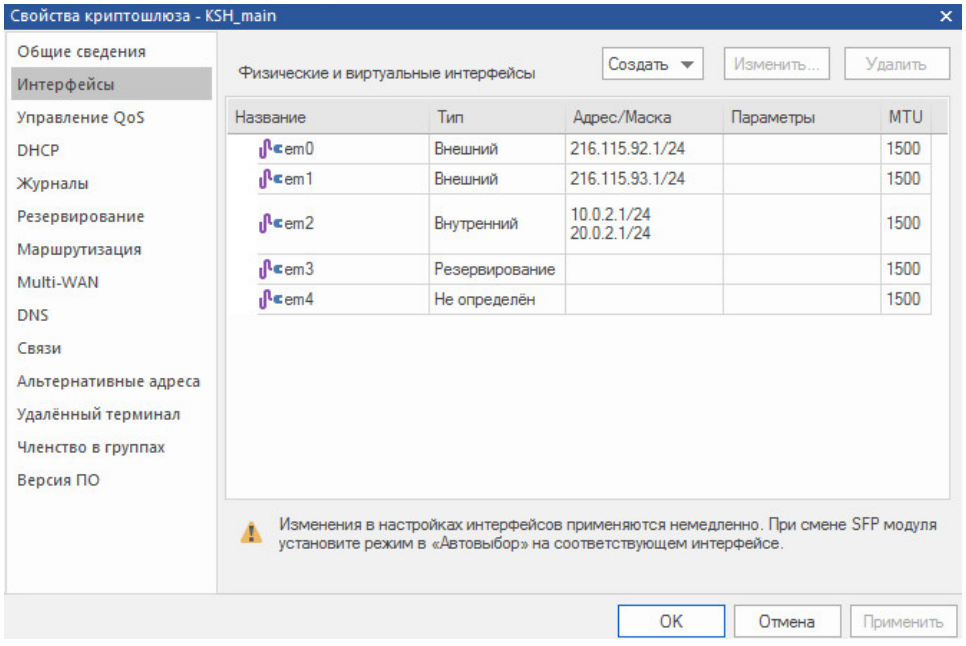
  - поскольку трафик между виртуальными машинами AP и WS1 проходит через три промежуточных сетевых устройства с функциями маршрутизации и фильтрации пакетов, скорость передачи в разы ниже, чем при прямом сетевом взаимодействии (см. п. 3). Кроме того, поскольку учебный стенд построен в виртуальной среде, показатели скорости зависят также от степени загруженности ESXi-сервера;
- на ВМ WS1 и AP удалите скопированный файл (<Shift>+<Del>) из локальной папки "C:\test\down".

7. Для того чтобы описать параметры очередей для приоритизации сетевого трафика, в ПУ ЦУС сделайте следующее:

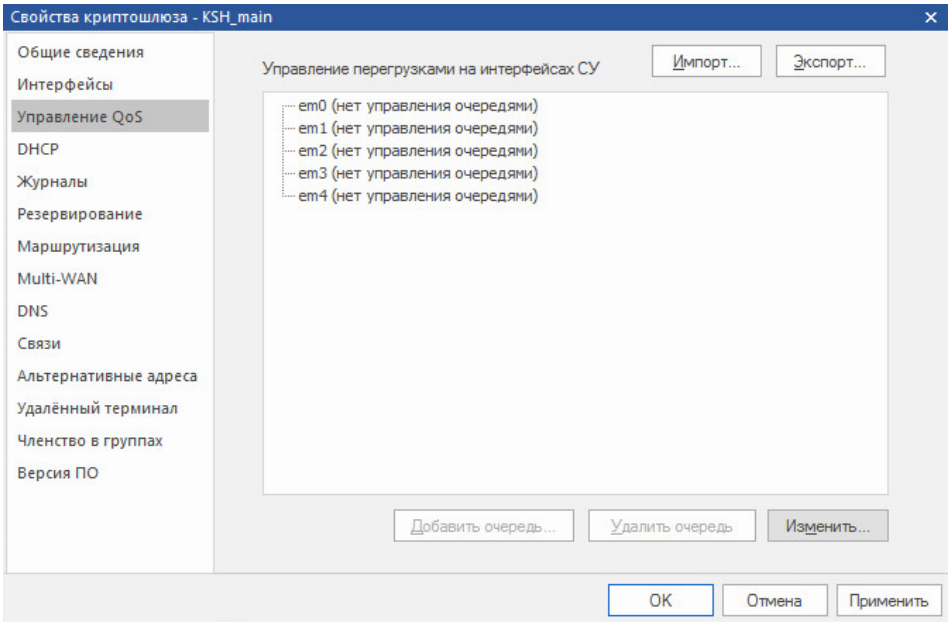
- в области объектов управления выберите "Сетевые устройства Континент / Криптошлюзы";

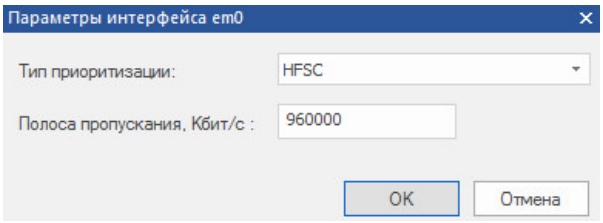


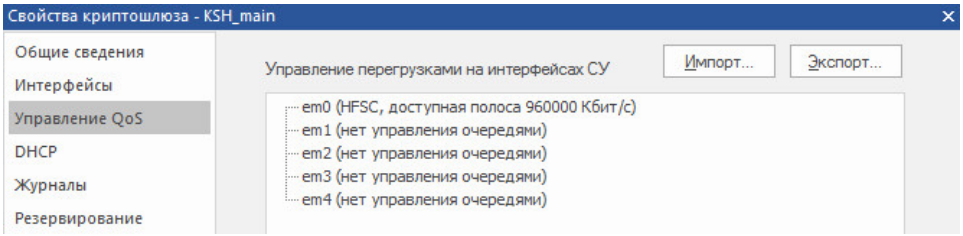
- через контекстное меню криптошлюза KSH_main откройте окно его свойств и выберите категорию "Интерфейсы". Убедитесь, что для внешних и внутренних интерфейсов параметр MTU имеет значение 1500 (по умолчанию) – такое же, как и на компьютерах в защищаемых сетях (см. выше, п. 2);



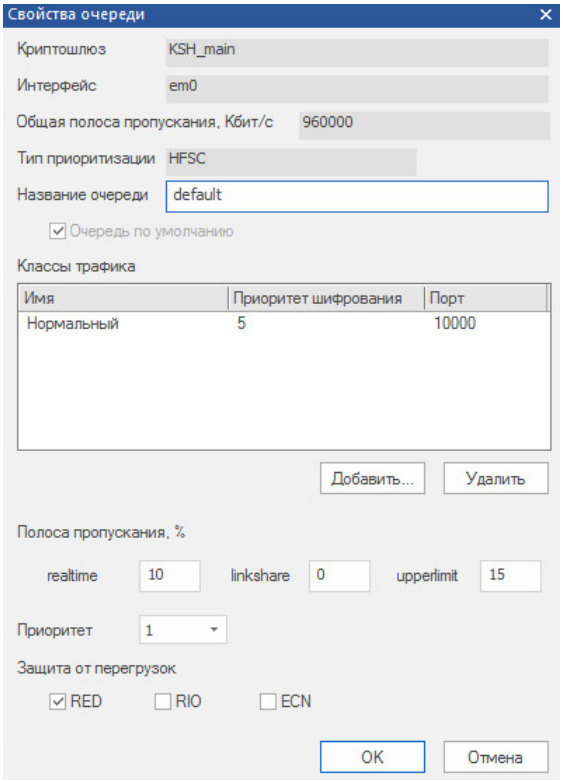
- выберите категорию параметров "Управление QoS" и для внешнего интерфейса "em0" установите: "Тип приоритизации" – "HFSC", "Полоса пропускания, Кбит/с" – **960000** – определяет суммарную пропускную способность родительской очереди для всех очередей интерфейса. Важно указать этот параметр чуть меньшим, чем максимальная пропускная способность канала, поскольку планировщик может ставить данные в очередь и не передавать на вышестоящий роутер. В данном примере – это 96% от 1000000 Кбит/с (1 Гбит/с) – скорости работы интерфейса;



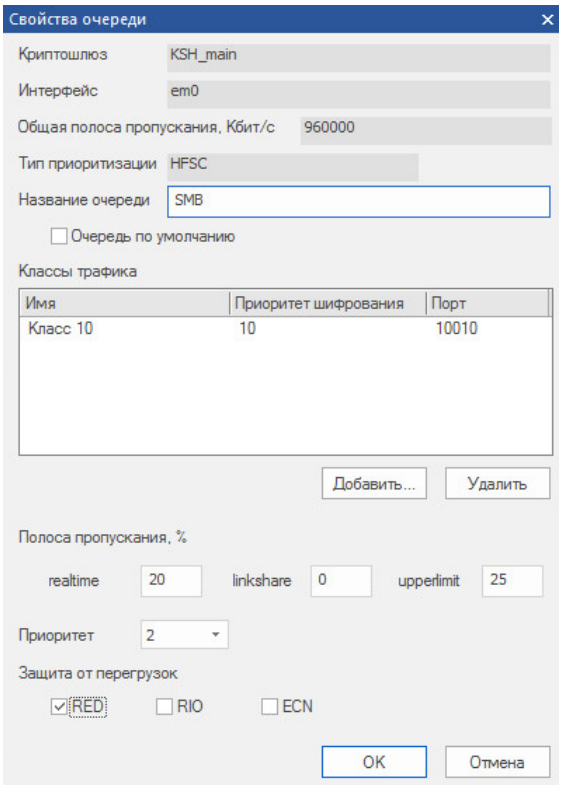




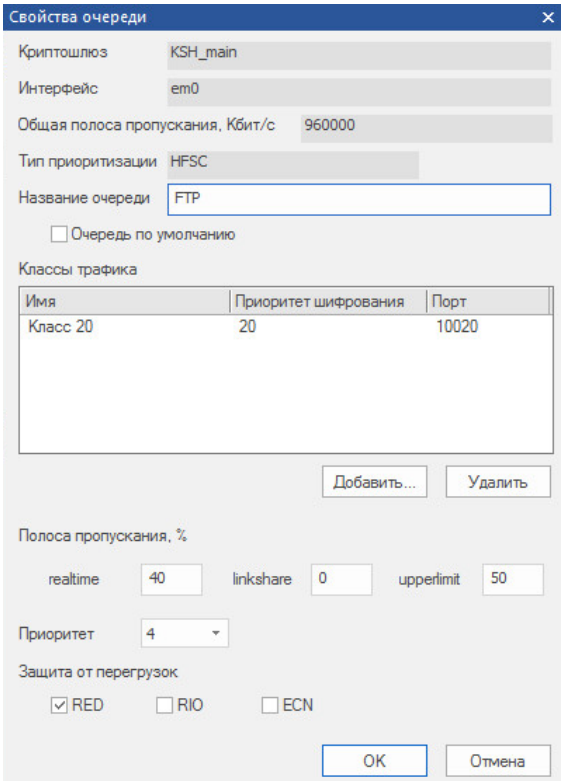
- для постановки трафика, который не будет явно приоритизирован (например, системный трафик между узлами "Континент"), создайте очередь по умолчанию. Для этого нажмите кнопку "Добавить очередь" и в открывшемся окне укажите следующие параметры:
  - "Название очереди" – **default** (произвольно);
  - "Классы трафика" – используя кнопку "Добавить", выберите класс "Нормальный" (см. выше п. 5);
  - в группе "Полоса пропускания, %": "realtime" – **10** (доля общей полосы пропускания, которая гарантируется очереди независимо от того, в какой полосе нуждается любая другая очередь. Допустимый диапазон – от 0 до 80%), "upperlimit" – **15** (количество полосы пропускания, которую очередь не может превысить, даже если канал свободен), linkshare – **0** (доля общей полосы пропускания, выделенная для режима linkshare, который настраивается при необходимости использования нелинейной кривой сервиса – NLSC или просто SC. Здесь данная настройка использоваться не будет);
  - "Приоритет" – 1 – уровень, определяющий порядок, в котором сервис будет обслуживаться относительно других очередей. Чем выше значение, тем выше приоритет. Этот параметр указывает, какие пакеты будут отправлены первыми, по сравнению с другими. Приоритет не задает полосу пропускания, но определяет порядок, в котором пакеты буферизуются перед отправкой;
  - в группе "Защита от перегрузок" выберите параметр "RED"– Random Early Detection – оптимизированный алгоритм отбрасывания пакетов, которые могут предположительно перегрузить очередь. Работает быстрее, чем алгоритм ECN (Explicit Congestion Notification);



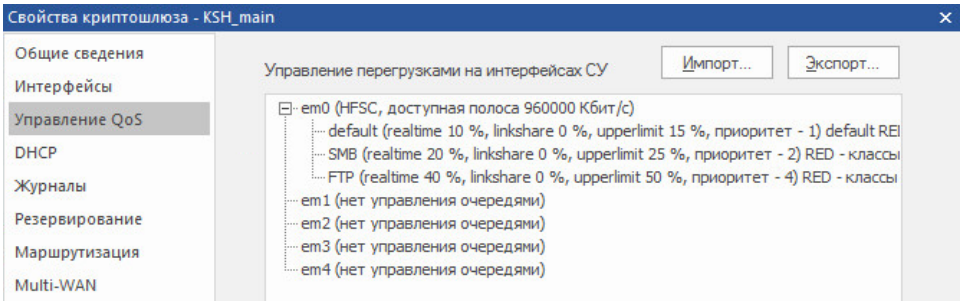
- нажмите кнопку "ОК". В структуре интерфейса "em0" появится запись очереди по умолчанию. Аналогично создайте очередь для приоритизации SMB-трафика, указав следующие параметры:
  - "Название очереди" – **SMB** (произвольно);
  - "Классы трафика" – выберите класс "Класс 10" (см. описание соответствующих правил фильтрации в п. 5);
  - в группе "Полоса пропускания, %": "realtime" – **20**, "upperlimit" – **25**;
  - "Приоритет" – 2 (выше, чем у очереди по умолчанию);
  - в группе "Защита от перегрузок" выберите параметр "RED";



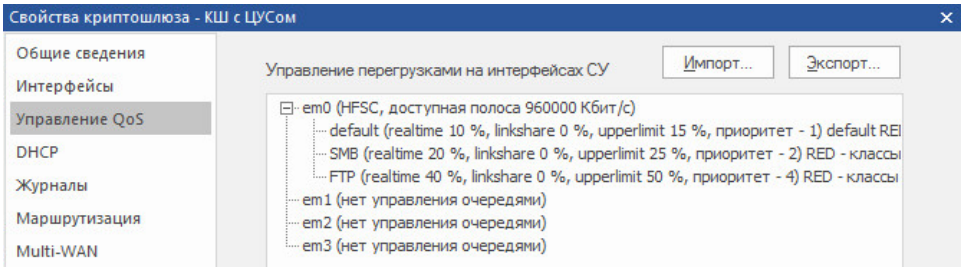
- нажмите кнопку "ОК". В структуре интерфейса "em0" появится запись очереди "SMB". Аналогично создайте очередь для приоритизации FTP–трафика, указав следующие параметры:
  - "Название очереди" – **FTP** (произвольно);
  - "Классы трафика" – выберите класс "Класс 20" (см. описание соответствующих правил фильтрации в п. 5);
  - в группе "Полоса пропускания, %": "realtime" – **40**, "upperlimit" – **50**;
  - "Приоритет" – 4 (выше, чем у других очередей);
  - в группе "Защита от перегрузок" выберите параметр "RED";



- нажмите кнопку "ОК". В структуре интерфейса "em0" появится запись очереди "FTP";

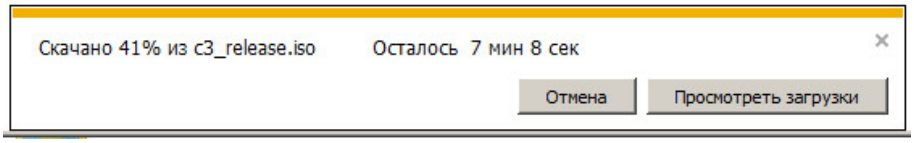


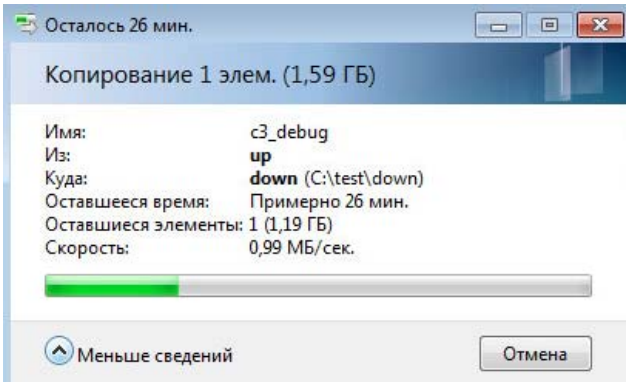
- в окне свойств криптошлюза KSH_main нажмите кнопку "ОК". Параметры очередей для приоритизации сетевого трафика на узле KSH_main заданы;
- проведите аналогичную настройку очередей с такими же параметрами для приоритизации сетевого трафика на внешнем интерфейсе "em0" узла КШ с ЦУСом и дождитесь завершения применения конфигурации.



8. Проведите оценку скорости передачи SMB- и FTP-трафика между сетевыми узлами "Континент" и сравните результаты с показателями, которые были получены при выполнении п. 6 данной лабораторной работы. Для этого сделайте следующее:

- используя описание п. 6 данной лабораторной работы, запустите одновременно два параллельных процесса:
  - в окне консоли ВМ WS1 в браузере IE сохранение файла с FTP-сервера (ВМ ARM, 10.0.1.200) в локальную папку "C:\test\down";
  - в окне консоли ВМ AP копирование файла из общедоступной папки "up" на ВМ WS1 в локальную папку "C:\test\down";
- по ходу выполнения запущенных процессов скачивания файлов обратите внимание на следующие моменты:
  - поскольку на сетевых узлах "Континент" очередь FTP-трафика имеет более высокий приоритет и более широкую полосу пропускания по сравнению с очередью SMB-трафика (см. п. 7), загрузка файла с FTP-сервера проходит существенно быстрее;
  - передача трафика по SMB-протоколу (копирование на ВМ AP файла из общедоступной папки с ВМ WS1) имеет более низкий приоритет и ограничена выделенной квотой – 20-25% от общей полосы пропускания канала;

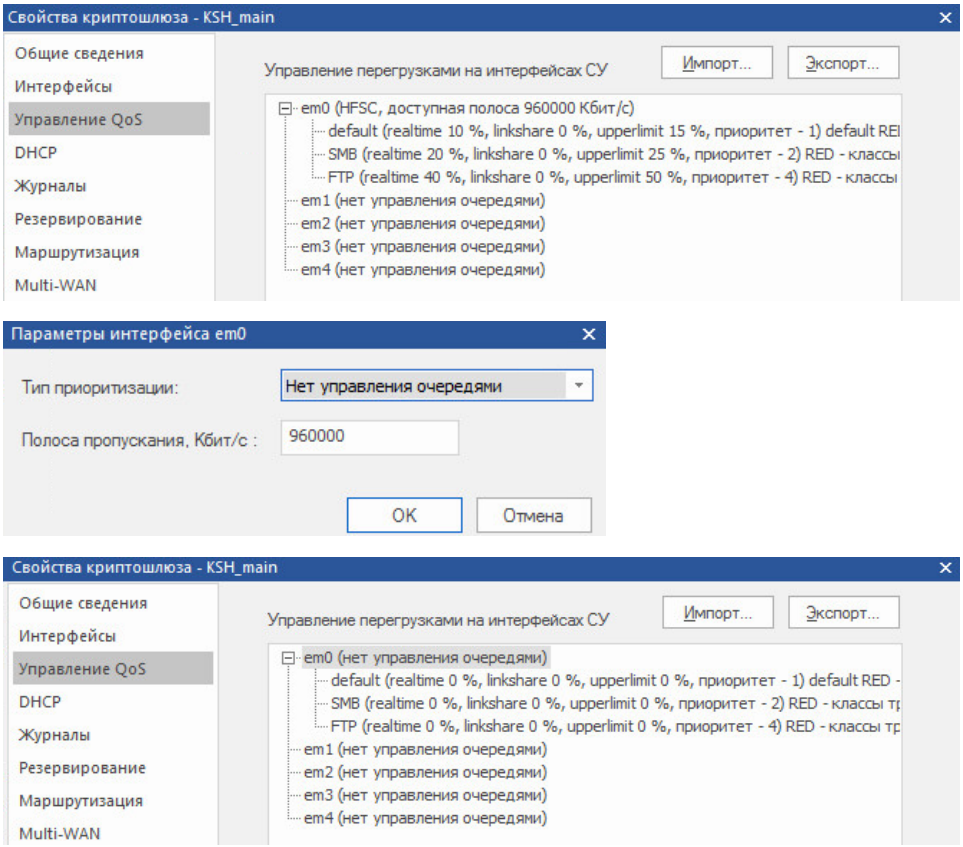




  - также следует помнить, что учебный стенд построен в виртуальной среде, и поэтому абсолютные значения показателей скорости зависят от степени загруженности ESXi-сервера и будут отличаться от тех значений, которые могут быть получены на реальном оборудовании;
- на ВМ WS1 и AP удалите скопированный файл (<Shift>+<Del>) из локальной папки "C:\test\down".

9. Таким образом, в ходе проверки работы механизма QoS на узлах "Континент" описаны параметры очередей для приоритизации сетевого трафика и протестировано их влияние на скорость межсетевого взаимодействия.

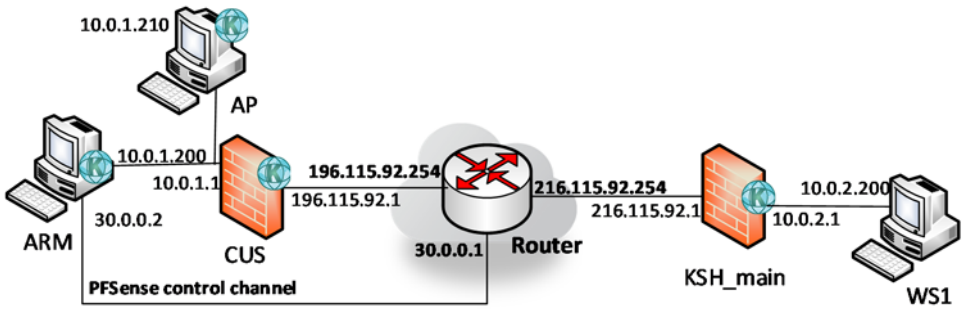
В ПУ ЦУС, используя описание п. 7, на сетевых узлах KSH_main и КШ с ЦУСом для внешних интерфейсов "em0" отключите приоритизацию трафика (настройки очередей при этом можно не удалять).



Выполнение лабораторной работы завершено.

Лабораторная работа №2 "Оценка производительности КШ «Континент» в режиме шифрования (L3VPN)"

В данной лабораторной работе демонстрируется влияние распределения потоков шифрования по ядрам процессора на КШ "Континент" на производительность сетевого взаимодействия между абонентами L3VPN-соединения. Ниже на рисунке показаны виртуальные машины, которые будут при этом задействованы.



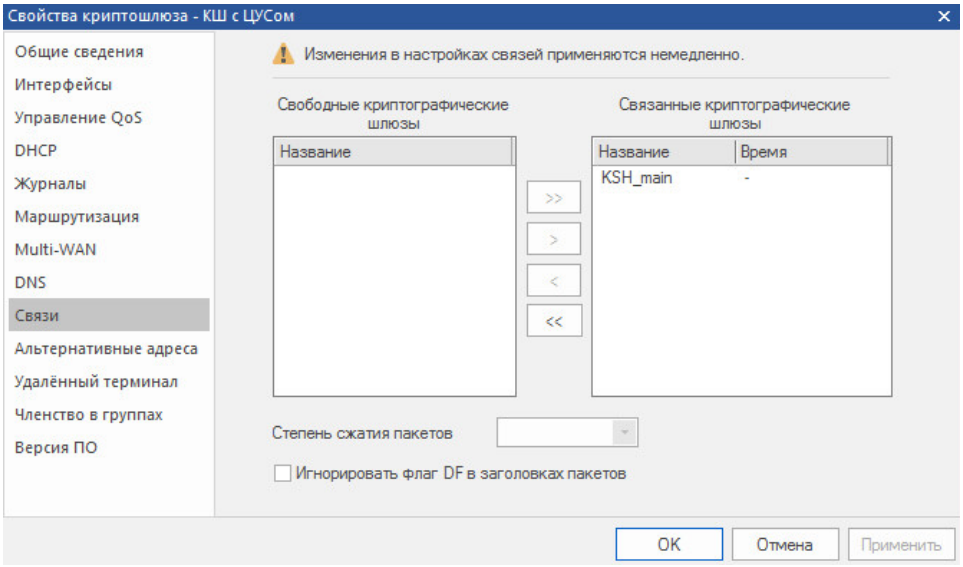
Оценка влияния распределения потоков шифрования по ядрам процессора на скорость межсетевого взаимодействия будет проводиться в следующем порядке:

1. Оценивается скорость передачи шифрованного трафика между сетевыми узлами "Континент" в одном направлении (один поток шифрования).
2. На связанных КШ "Континент" в настройках шифрования отключить распределение потоков по ядрам процессора.
3. Провести оценку скорости передачи шифрованного трафика между связанными КШ в двух направлениях одновременно (два потока шифрования).
4. На связанных КШ включить в настройках шифрования распределение потоков по ядрам процессора.

5. Провести оценку скорости передачи шифрованного трафика между связанными КШ в двух направлениях одновременно (два потока шифрования) и сравнить показатели с полученными в п. 3.

Далее приведены задания лабораторной работы.

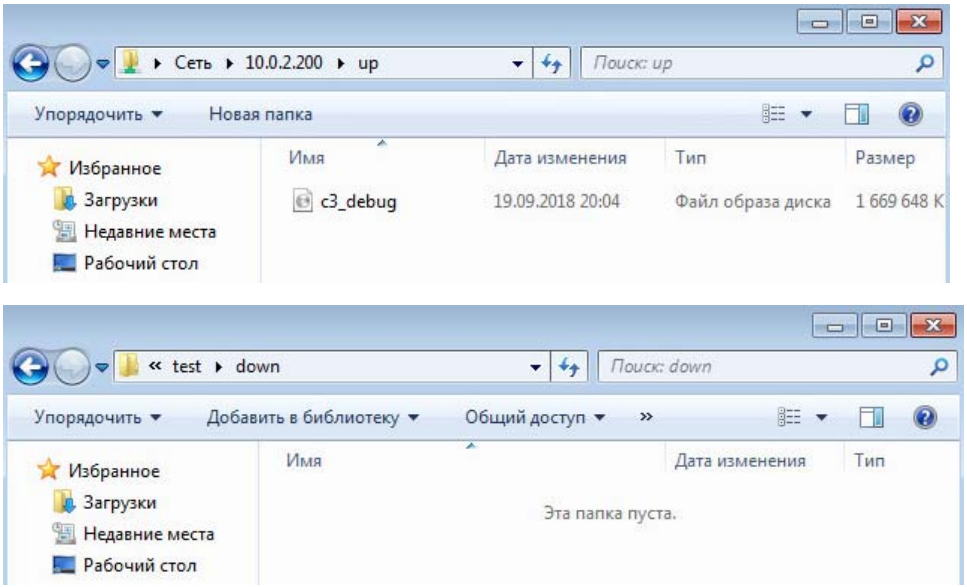
1. Включите шифрование между КШ с ЦУСом и KSH_main. Для этого в разделе "Сетевые устройства Континент / Криптошлюзы" ПУ ЦУС из контекстного меню одного из этих КШ (любого) выберите опцию "Свойства" и на вкладке "Связи" переместите имя другого устройства из списка "Свободные криптографические шлюзы" в список "Связанные криптографические шлюзы".



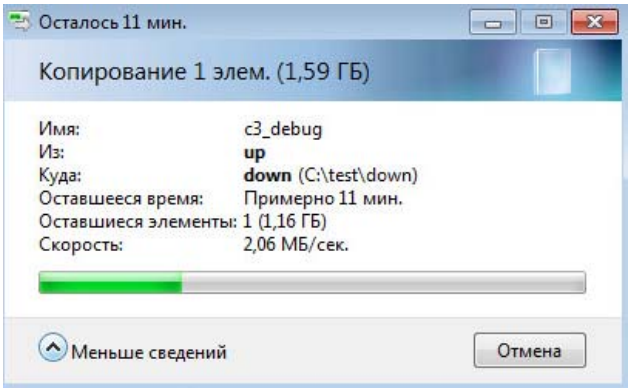
Обратите внимание, что изменения настроек применяются немедленно. Нажмите кнопку "ОК".

2. Проведите оценку скорости передачи шифрованного трафика между сетевыми узлами "Континент" в одном направлении (один поток шифрования). Для этого сделайте следующее:

- переключитесь в окно консоли ВМ AP и запустите копирование файла из общедоступной папки "up" на ВМ WS1 (10.0.2.200) в локальную папку "C:\test\down";



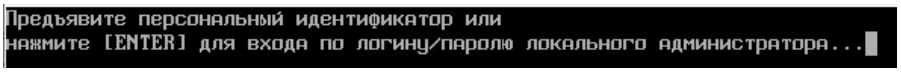
- оцените скорость передачи одного потока шифрованного трафика. Как отмечалось в главе 1, на одной сессии (один поток шифрования) невозможно добиться максимальной производительности узла "Континент" (также помните, что учебный стенд построен в виртуальной среде, и поэтому абсолютные значения показателей скорости зависят от степени загруженности ESXi-сервера и будут отличаться от тех значений, которые могут быть получены на реальном оборудовании).



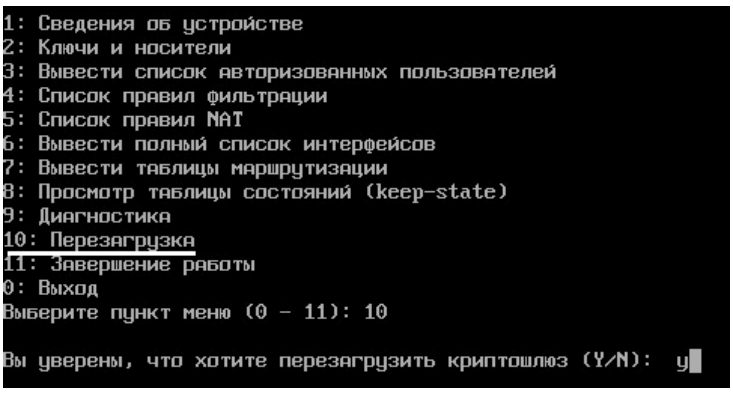
- в окне консоли ВМ АР удалите скопированный файл (<Shift>+<Del>) из локальной папки "C:\test\down".

3. Просмотрите текущее состояние локальных настроек шифрования на КШ и на КШ с ЦУСом. Для этого сделайте следующее:

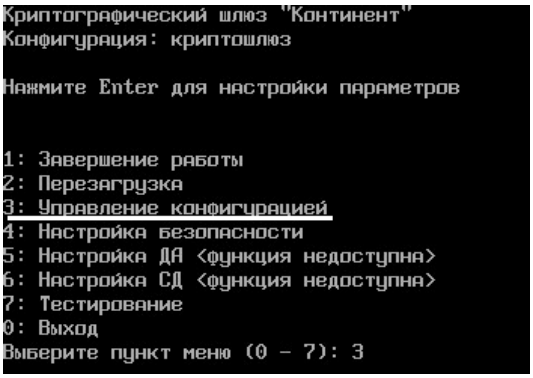
- откройте консоль ВМ KSH_main, нажмите комбинацию клавиш <Alt>+<F2> и авторизуйтесь с учетной записью локального администратора **kshadmin / P@ssword**;

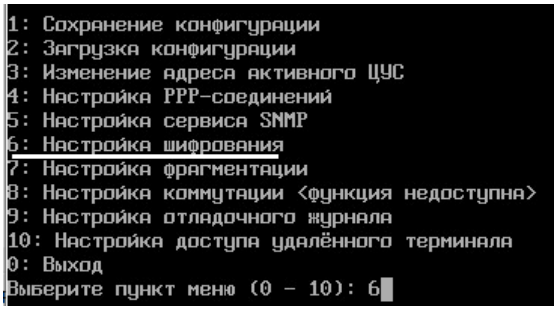


- в локальном меню введите команду **10** "Перезагрузка" и подтвердите операцию;



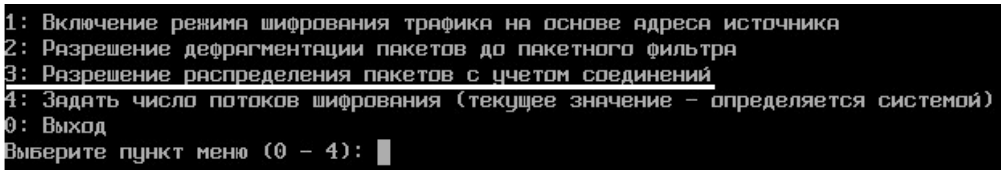
- дождитесь появления приглашения "Нажмите Enter для настройки параметров", нажмите клавишу <Enter> и в открывшемся локальном меню введите: **3** "Управление конфигурацией", а затем – **6** "Настройка шифрования";





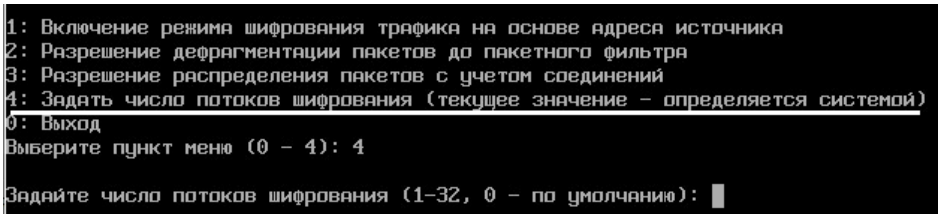
- в открывшемся подменю настроек обратите внимание на состояние опции **3**. Как отмечалось в главе 1, на КШ по умолчанию данный параметр включен, т.е. разрешено распределение потоков по ядрам и значение данной опции должно быть – "Запрет распределения пакетов с учетом соединения". Однако на виртуальном учебном стенде состояние данного параметра может быть любым.

  В целях данной лабораторной работы отключите распределение потоков по ядрам – установите для опции **3** значение "Разрешение распределения пакетов с учетом соединения" (т.е. текущее ее состояние – запрет распределения);



> **Для сведения.** В настройках шифратора данная установка отображается строкой net.inet.ipcrypt.l3_hash:0.

- обратите внимание на состояние опции **4** "Задать число потоков шифрования…" – по умолчанию данный параметр определен системой (см. главу 1). При необходимости можно указать нужное количество потоков, которое затем будет отображаться в локальном меню. Если же ввести значение **0**, то данный параметр будет установлен в значение по умолчанию.

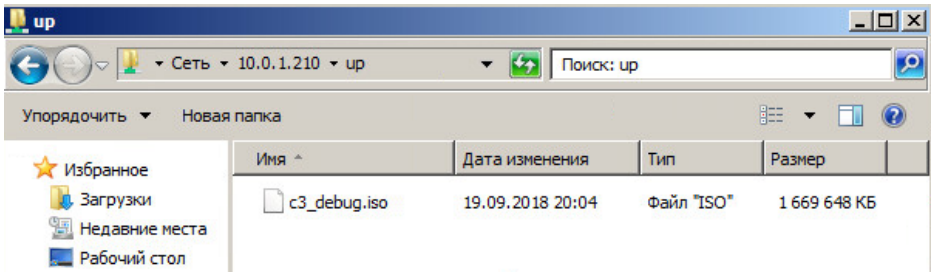


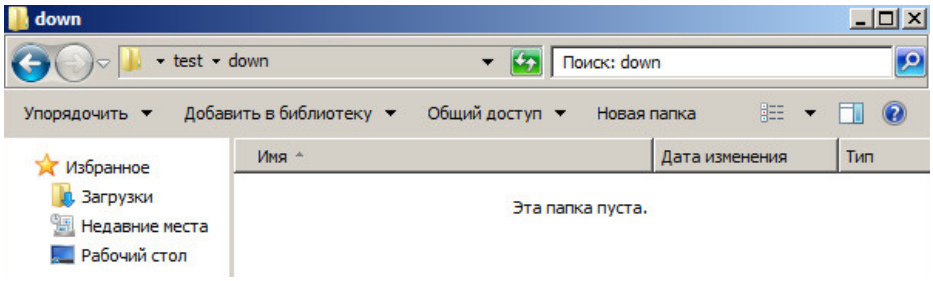
  Не изменяйте текущее значение числа потоков шифрования;

- используя описание подпунктов данного пункта 3, просмотрите текущее состояние локальных настроек шифрования на КШ с ЦУСом (учетная запись локального администратора **admin / 11111111**) и также отключите на данном узле распределение потоков по ядрам (установите для опции 3 локального меню настроек шифратора значение "Разрешение распределения пакетов с учетом соединения").

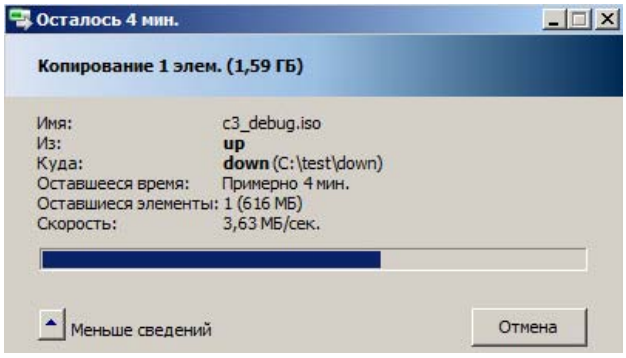
4. Проведите оценку скорости передачи шифрованного трафика между сетевыми узлами "Континент" в двух направлениях одновременно (два потока шифрования). Для этого:

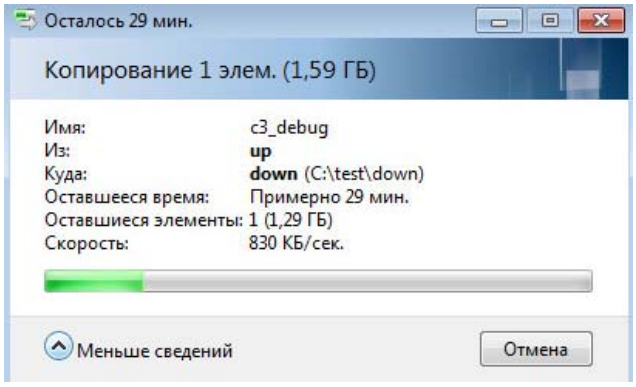
- переключитесь в окно консоли ВМ WS1 и откройте расположенную на ВМ АР (10.0.1.210) общедоступную папку "up" (локальный путь – "C:\test\up"), содержащую файл размером 1,6 Гбайт, а также локальную пустую папку "C:\test\down";





- в окне консоли ВМ WS1 запустите копирование файла из общедоступной папки "up" на ВМ АР (10.0.1.210) в локальную папку "C:\test\down";
- переключитесь в окно консоли ВМ АР и также запустите копирование файла из общедоступной папки "up" на ВМ WS1 (10.0.2.200) в локальную папку "C:\test\down";
- по ходу выполнения процессов копирования оцените совокупную скорость передачи шифрованного трафика в двух направлениях. Поскольку распределение потоков по ядрам было отключено, то совокупная скорость должна приблизительно соответствовать удвоенному показателю из п. 2;



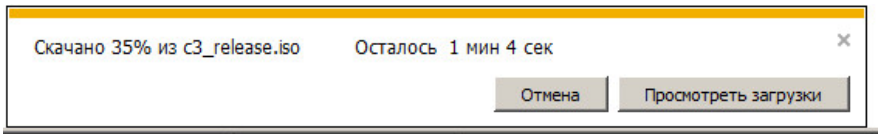


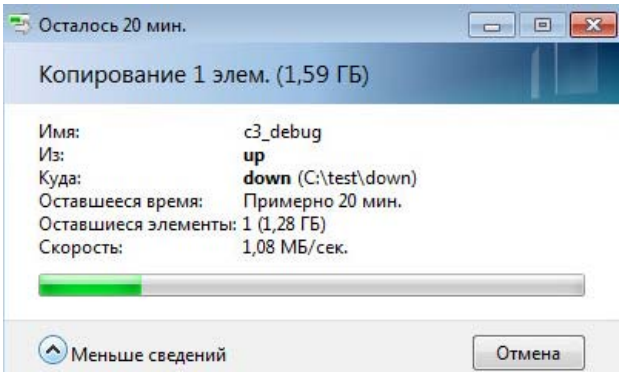
- на ВМ АР и WS1 удалите скопированный файл (<Shift>+<Del>) из локальной папки "C:\test\down".

5. Проведите оценку производительности при передаче между сетевыми узлами "Континент" одновременно двух потоков шифрованного трафика с разными приоритетами шифрования (SMB- и FTP-трафика, см. описание классов и правил фильтрации в п. 5 лабораторной работы №1). Для этого:

- в окне консоли ВМ АР запустите копирование файла из общедоступной папки "up" на ВМ WS1 в локальную папку "C:\test\down";

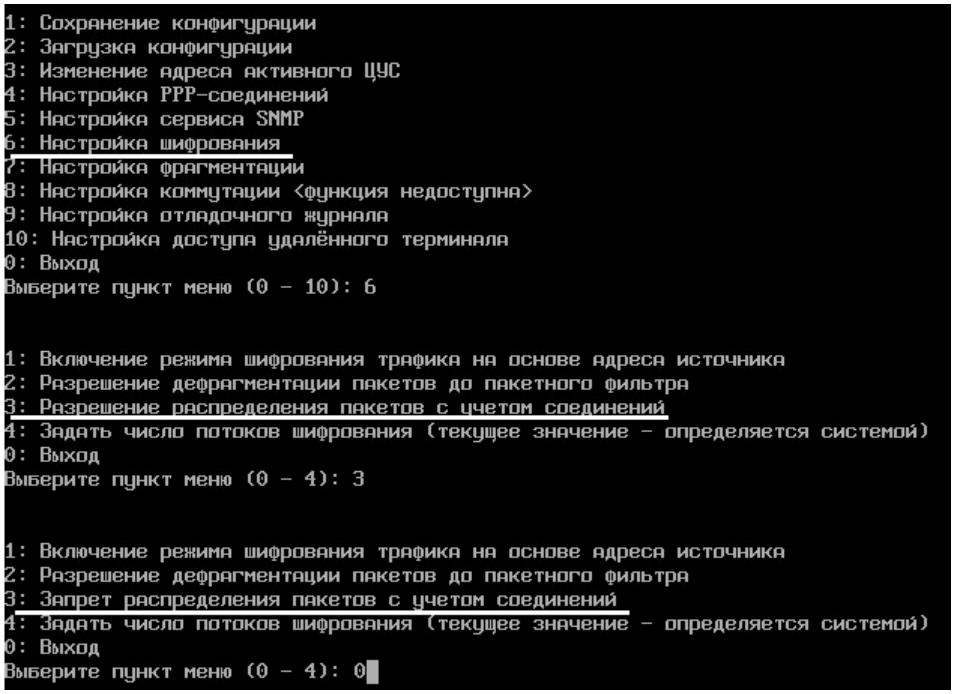
- переключитесь в окно консоли ВМ WS1 и в браузере IE запустите сохранение файла с FTP-сервера (ВМ ARM, 10.0.1.200) в локальную папку "C:\test\down";
- по ходу выполнения запущенных процессов скачивания файлов оцените совокупную скорость передачи трафика шифрованного трафика в двух направлениях. Поскольку на узлах стенда распределение потоков по ядрам было отключено, совокупная скорость должна приблизительно соответствовать удвоенному показателю из п. 2. При этом, поскольку в параметрах правил фильтрации для FTP-трафика указан более высокий приоритет шифрования, обмен по FTP-протоколу выполняется существенно быстрее;





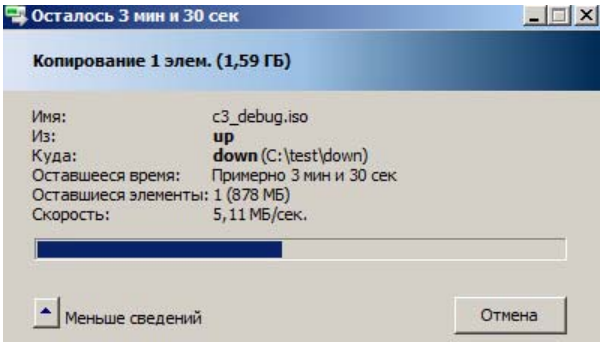
- на ВМ WS1 и АР удалите скопированный файл (<Shift>+<Del>) из локальной папки "C:\test\down".

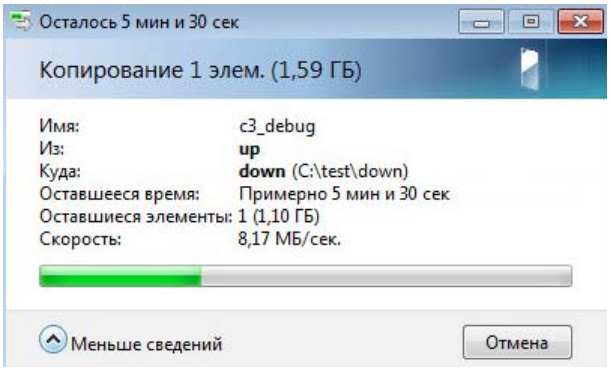
6. Используя описание п. 3, включите на КШ и на КШ с ЦУСом распределение потоков по ядрам (установите для опции 3 локального меню настроек шифратора значение "Запрет распределения пакетов с учетом соединения").



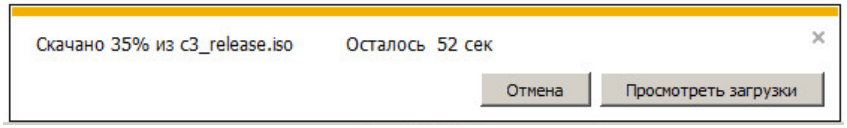
Для сведения. В настройках шифратора данная установка отображается строкой net.inet.ipcrypt.l3_hash:1.

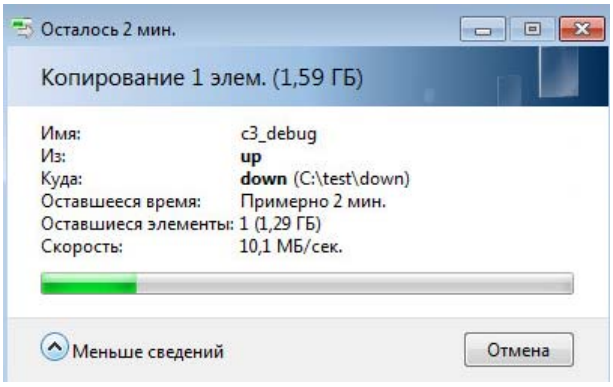
7. Используя описание п. 4, проведите оценку скорости передачи шифрованного трафика между сетевыми узлами "Континент" в двух направлениях одновременно (два потока шифрования, распределение потоков по ядрам включено). По ходу выполнения процессов копирования оцените совокупную скорость передачи и обратите внимание, что по сравнению с показателями из п. 4 она существенно выше.





8. Используя описание п. 5, проведите оценку производительности при передаче между сетевыми узлами "Континент" одновременно двух потоков шифрованного трафика с разными приоритетами шифрования (SMB- и FTP-трафик, два потока шифрования, распределение потоков по ядрам включено). По ходу выполнения процессов копирования оцените совокупную скорость передачи и обратите внимание, что по сравнению с показателями из п. 5 она тоже значительно выше. При этом, поскольку в параметрах правил фильтрации для FTP-трафика указан более высокий приоритет шифрования, обмен по FTP-протоколу выполняется быстрее.



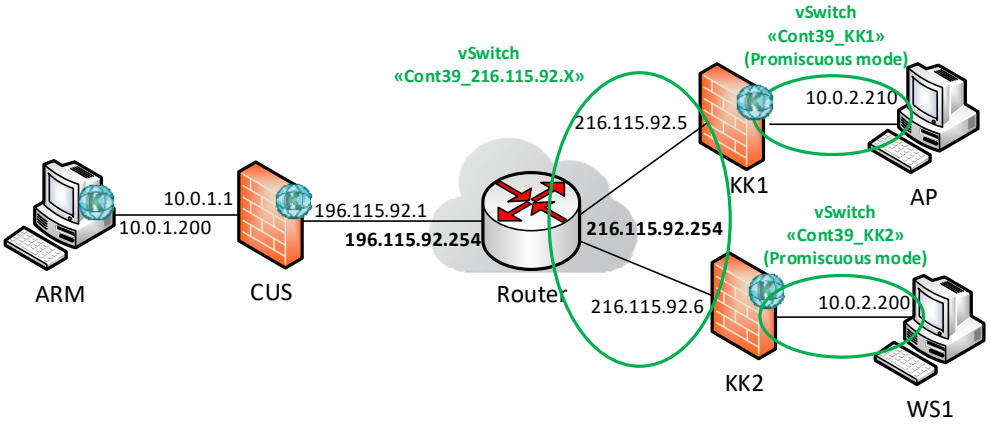


9. Таким образом, протестировано влияние распределения потоков шифрования по ядрам процессора на криптошлюзах "Континент" на скорость сетевого взаимодействия между абонентами L3VPN-соединения.

   Выполнение лабораторной работы завершено.

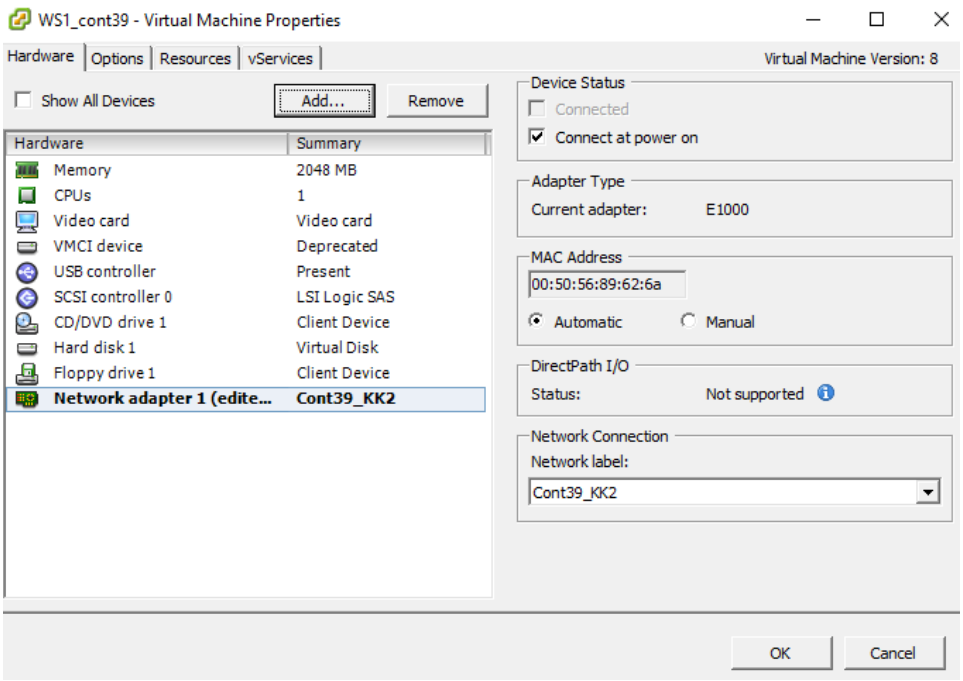
Лабораторная работа №3 "Оценка производительности КК «Континент» (L2VPN)"

В данной лабораторной работе проводится оценка производительности криптокоммутаторов "Континент" при взаимодействии между абонентами защищаемых сегментов одной подсети (L2VPN). Предварительно для этого необходимо сделать соответствующие изменения в конфигурации учебного стенда и включить криптокоммутаторы КК1 и КК2 (инициализация, ввод в эксплуатацию и настройка этих сетевых узлов проводились в рамках основного учебного курса "Администрирование АПКШ «Континент» версии 3.9"). На рисунке показаны виртуальные машины, которые будут использоваться.

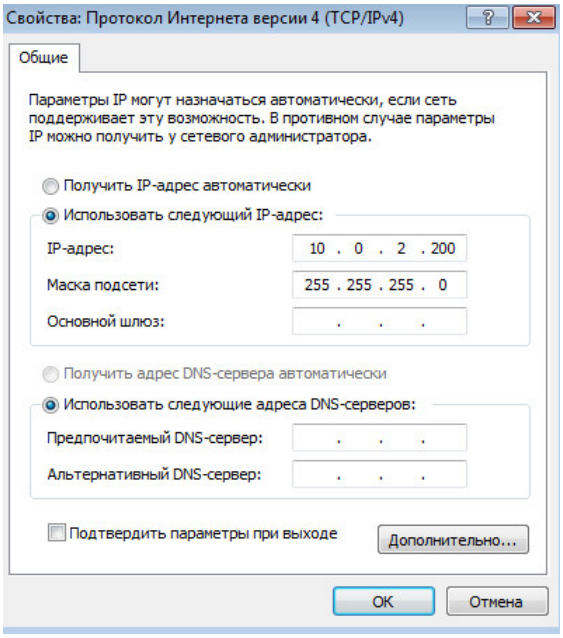


Перед началом выполнения лабораторной работы внесите в конфигурацию учебного стенда следующие изменения:

1. Выключите виртуальную машину KSH_main.
2. На ВМ WS1 сделайте следующее:
   - в настройках ВМ переподключите сетевой интерфейс к виртуальному коммутатору, к которому подключен порт коммутации криптокоммутатора КК2 (данный виртуальный коммутатор должен работать в режиме "Promiscuous mode");

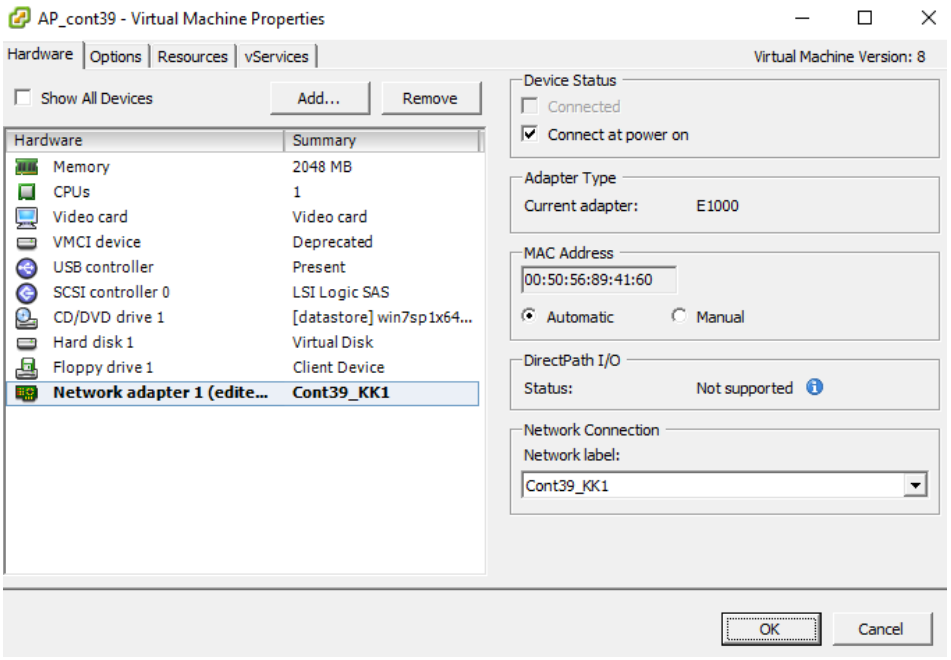


   - в настройках сетевого подключения в ОС Windows уберите установку шлюза по умолчанию.

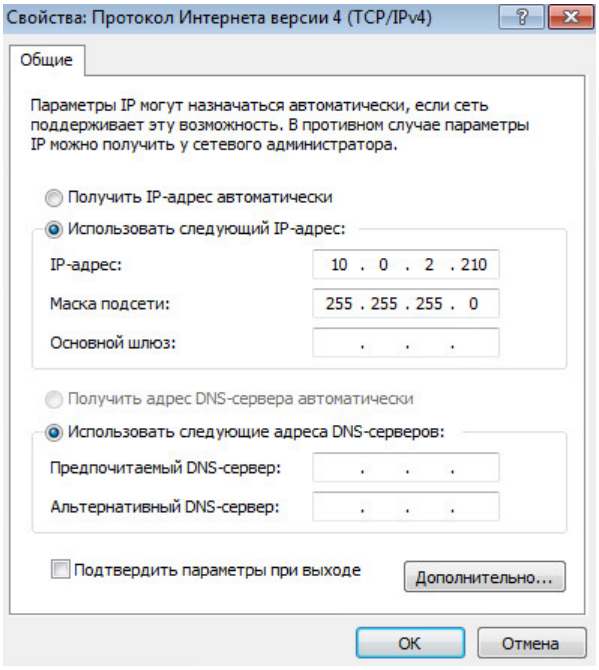


3. На ВМ AP сделайте следующее:

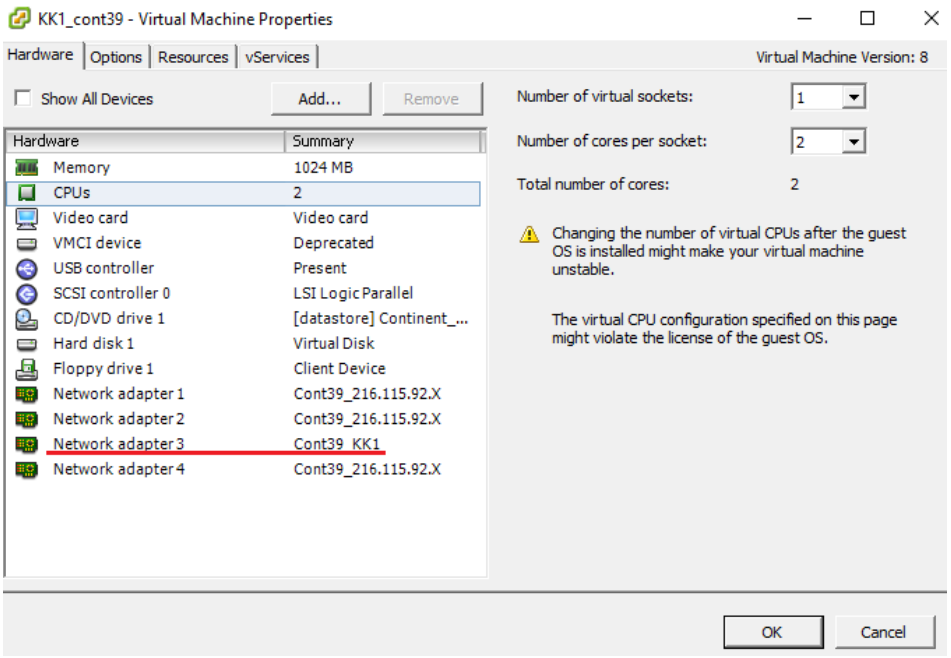
   - в настройках ВМ переподключите сетевой интерфейс к виртуальному коммутатору, к которому подключен порт коммутации криптокоммутатора KK1 (данный виртуальный коммутатор должен работать в режиме "Promiscuous mode");

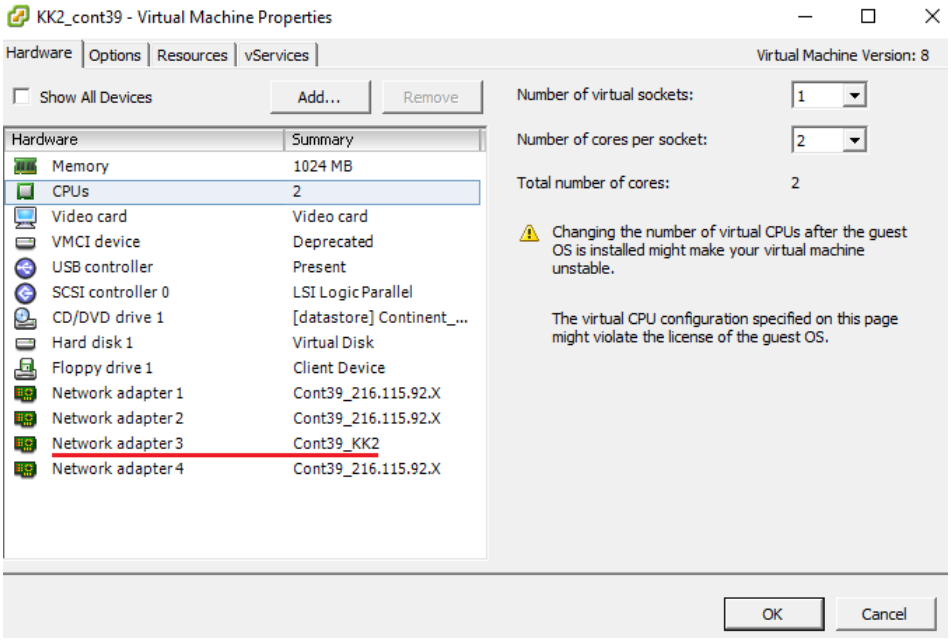


   - в настройках сетевого подключения в ОС Windows измените IP-адрес на **10.0.2.210/255.255.255.0** и уберите установку шлюза по умолчанию. Это необходимо сделать для того, чтобы виртуальные машины AP и WS1 находились в одной подсети.



4. Убедитесь, что на виртуальных машинах КК1 и КК2 сетевые интерфейсы коммутации являются недоступными друг для друга, то есть подключены к разным виртуальным коммутаторам, работающим в режиме "Promiscuous mode".





5. Включите ВМ криптокоммутаторов КК1 и КК2.

Примечание. Предполагается, что инициализация, ввод в эксплуатацию и настройка этих сетевых узлов проведены в рамках основного учебного курса "Администрирование АПКШ «Континент» версии 3.9".

6. Убедитесь, что криптокоммутаторы КК1 и КК2 являются связанными, и проверьте работоспособность канала шифрования между сегментами подсети (виртуальными машинами AP и WS1) с помощью утилиты **ping**.

Далее приведены задания лабораторной работы.

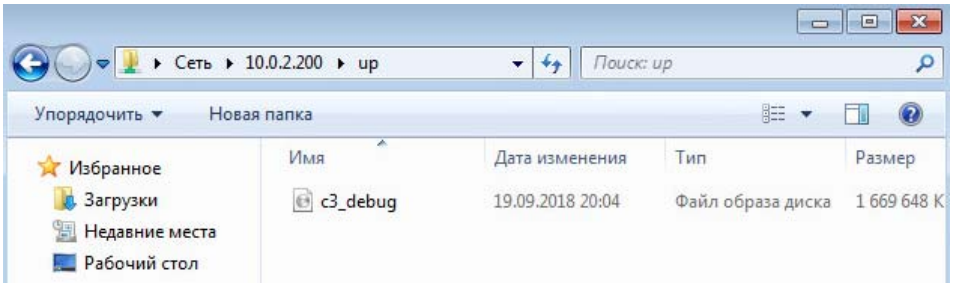
1. Используя описание п. 3 лабораторной работы №2, просмотрите текущее состояние локальных настроек шифрования на КК1 и КК2 (учетные записи локальных администраторов – **kk1admin / P@ssword** и **kk2admin / P@ssword** соответственно) и убедитесь, что, как отмечалось в главе 1, на КК по умолчанию запрещено распределение потоков по ядрам процессора, т.е. в настройках шифрования опция 3 имеет значение "Разрешение распределения пакетов с учетом соединений".

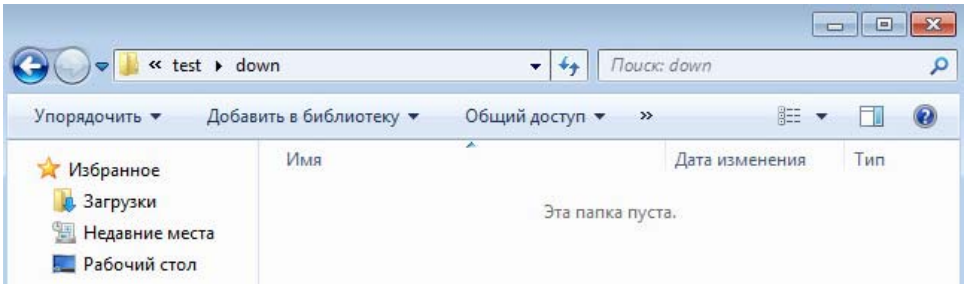
```
Криптографический коммутатор "Континент"
Конфигурация: криптокоммутатор

Нажмите Enter для настройки параметров


1: Завершение работы
2: Перезагрузка
3: Управление конфигурацией
4: Настройка безопасности
5: Настройка ДА <функция недоступна>
6: Настройка СД <функция недоступна>
7: Тестирование
0: Выход
Выберите пункт меню (0 - 7): 3


1: Сохранение конфигурации
2: Загрузка конфигурации
3: Изменение адреса активного ЦУС
4: Настройка PPP-соединений
5: Настройка сервиса SNMP
6: Настройка шифрования
7: Настройка фрагментации
8: Настройка коммутации
9: Настройка отладочного журнала
10: Настройка доступа удалённого терминала
0: Выход
Выберите пункт меню (0 - 10): 6


1: Включение режима шифрования трафика на основе адреса источника
2: Разрешение дефрагментации пакетов до пакетного фильтра
3: Разрешение распределения пакетов с учетом соединений
4: Задать число потоков шифрования (текущее значение - определяется системой)
0: Выход
Выберите пункт меню (0 - 4): 0
```

Для сведения. В настройках шифратора данная установка отображается строкой: net.inet.ipcrypt.l2_hash:0.

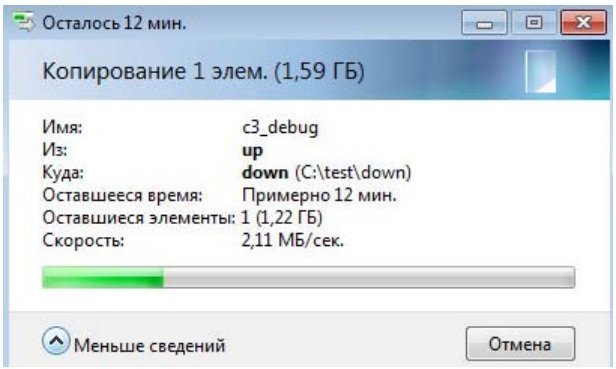
2. Проведите оценку скорости передачи шифрованного трафика между KK1 и KK2 в одном направлении (один поток шифрования). Для этого сделайте следующее:

- переключитесь в окно консоли BM AP и запустите копирование файла из общедоступной папки "up" на BM WS1 (10.0.2.200) в локальную папку "C:\test\down";





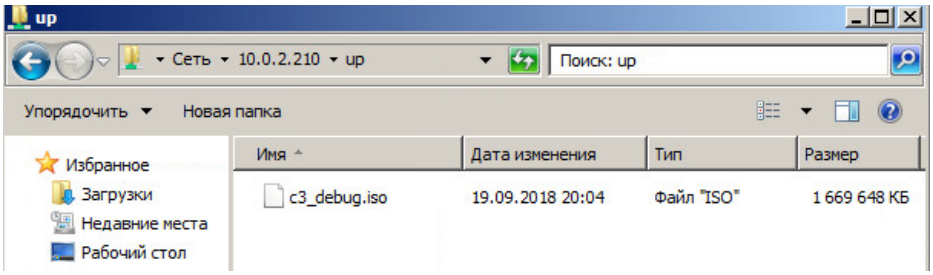
- оцените скорость передачи шифрованного трафика. Как отмечалось в главе 1, на одной сессии (один поток шифрования) невозможно добиться максимальной производительности узла "Континент". Однако по сравнению с КШ в аналогичной ситуации (см. п. 2 лабораторной работы №2) производительность КК должна быть выше, поскольку коммутатор работает на L2-уровне и не выполняет маршрутизацию и фильтрацию пакетов;

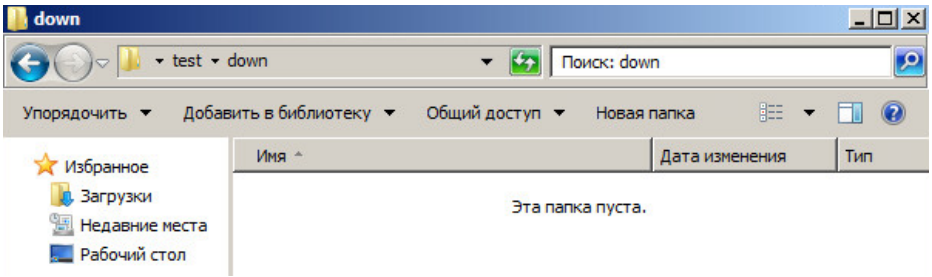


- в окне консоли ВМ АР удалите скопированный файл (<Shift>+<Del>) из локальной папки "C:\test\down".

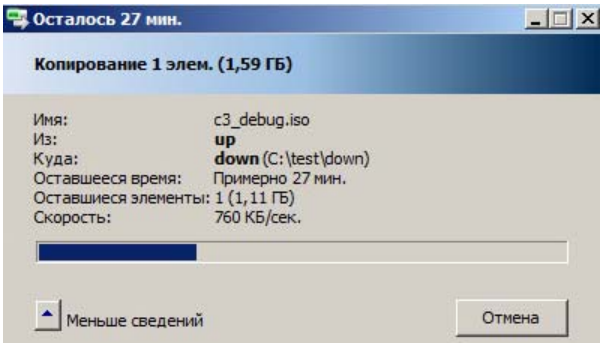
3. Проведите оценку скорости передачи шифрованного трафика между КК1 и КК2 в двух направлениях одновременно (для криптокоммутаторов это будет по-прежнему один поток шифрования – см. главу 1). Для этого:

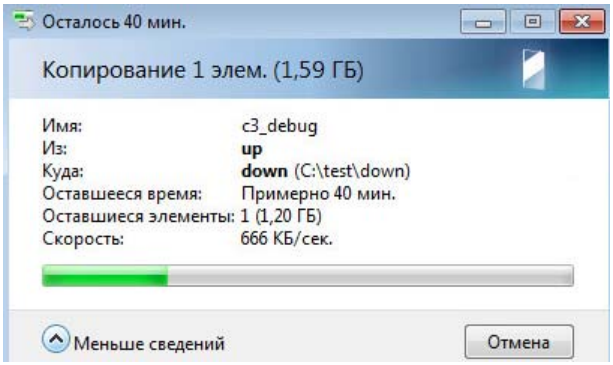
- переключитесь в окно консоли ВМ WS1 и откройте расположенную на ВМ АР (10.0.2.210) общедоступную папку "up" (локальный путь – "C:\test\up"), содержащую файл размером 1,6 Гбайт, а также локальную пустую папку "C:\test\down";





- в окне консоли ВМ WS1 запустите копирование файла из общедоступной папки "up" на ВМ АР (10.0.2.210) в локальную папку "C:\test\down";
- переключитесь в окно консоли ВМ АР и также запустите копирование файла из общедоступной папки "up" на ВМ WS1 (10.0.2.200) в локальную папку "C:\test\down";
- по ходу выполнения копирования оцените совокупную скорость передачи шифрованного трафика в двух направлениях и заметьте, что она не превышает показателя из п. 2 (см. описание работы КК в главе 1);

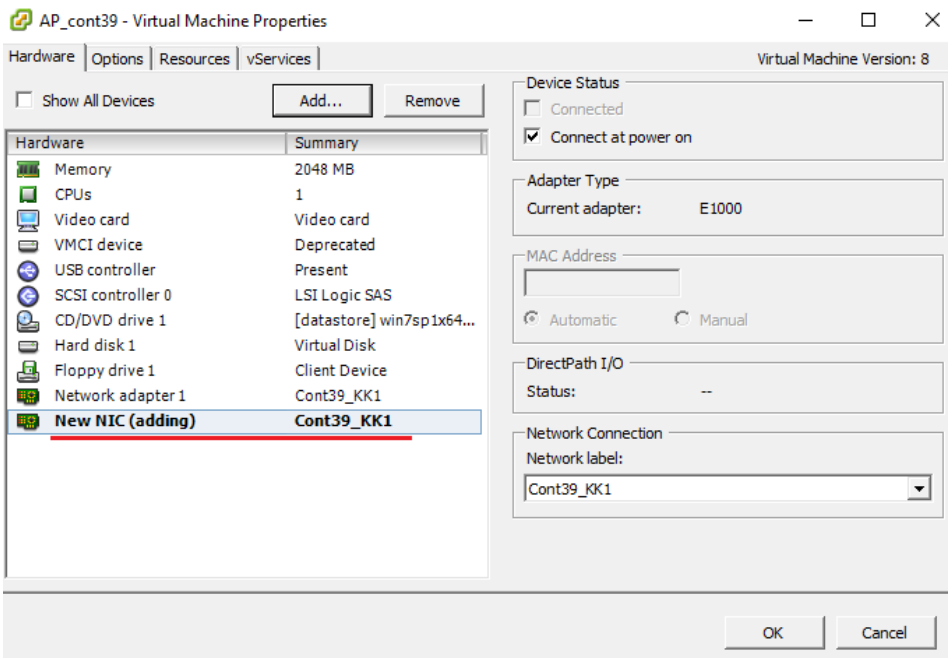




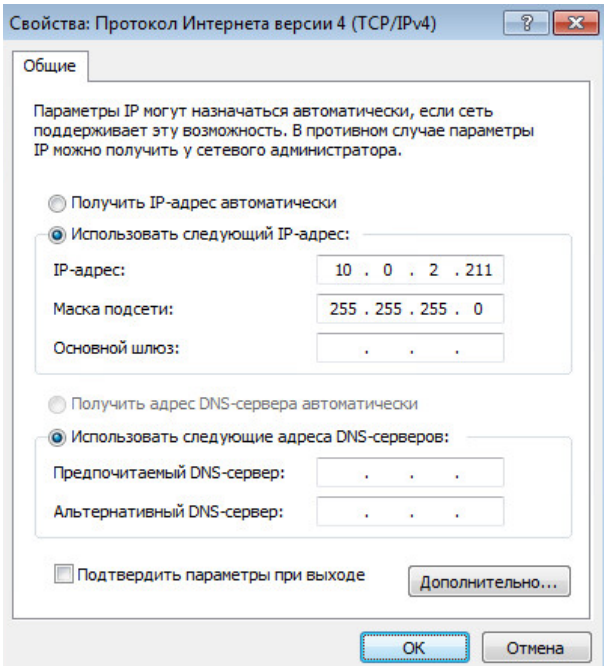
- на ВМ АР и WS1 удалите скопированный файл (<Shift>+<Del>) из локальной папки "C:\test\down".

4. Для достижения более оптимального использования ресурсов КК и канала передачи данных выполните следующие действия:

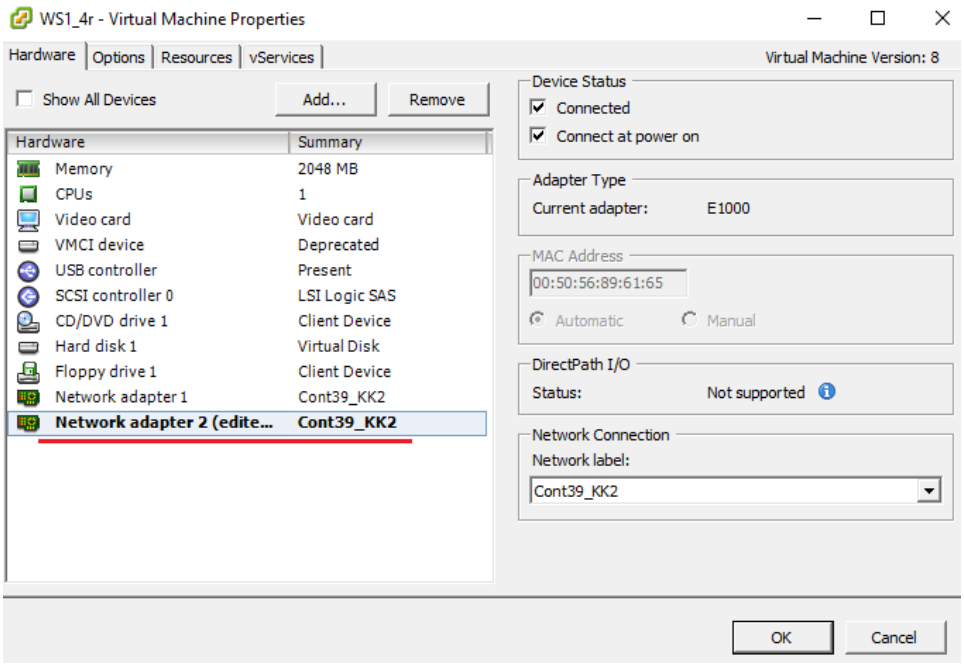
- в свойствах ВМ АР добавьте дополнительный сетевой интерфейс и подключите его к виртуальному коммутатору, к которому подключен порт коммутации криптокоммутатора КК1 (на данной ВМ теперь два интерфейса подключены к одному виртуальному коммутатору);



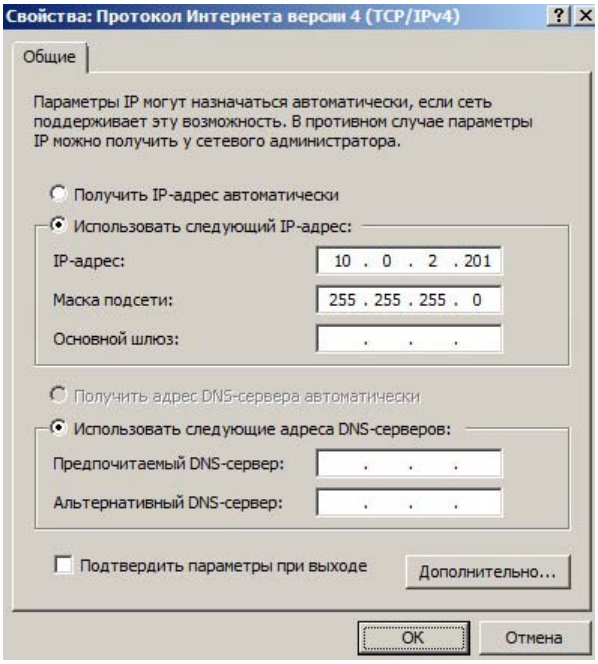
- в настройках сетевого подключения в ОС Windows установите для дополнительного интерфейса IP-адрес/маску **10.0.2.211/24** без адреса шлюза по умолчанию;



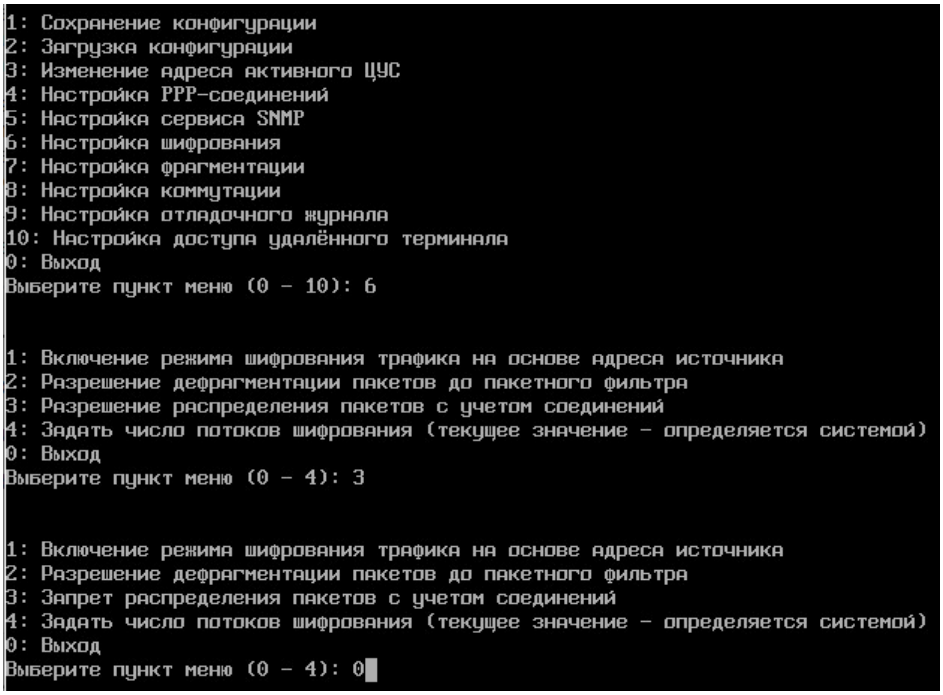
- в настройках ВМ WS1 добавьте дополнительный сетевой интерфейс и подключите его к виртуальному коммутатору, к которому подключен порт коммутации криптокоммутатора KK2 (на данной ВМ теперь тоже два интерфейса подключены к одному виртуальному коммутатору);



- в настройках сетевого подключения в ОС Windows установите для дополнительного интерфейса IP-адрес/маску **10.0.2.201/24** без адреса шлюза по умолчанию;

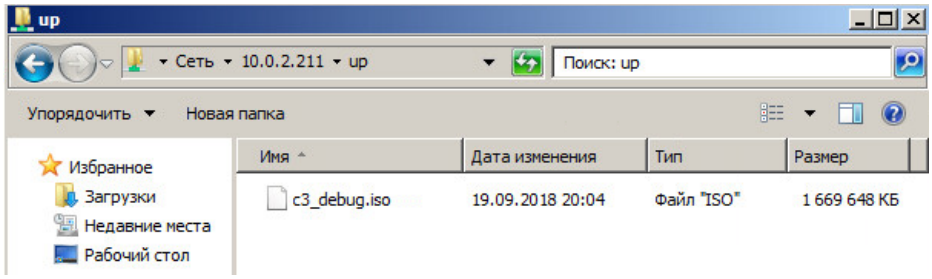


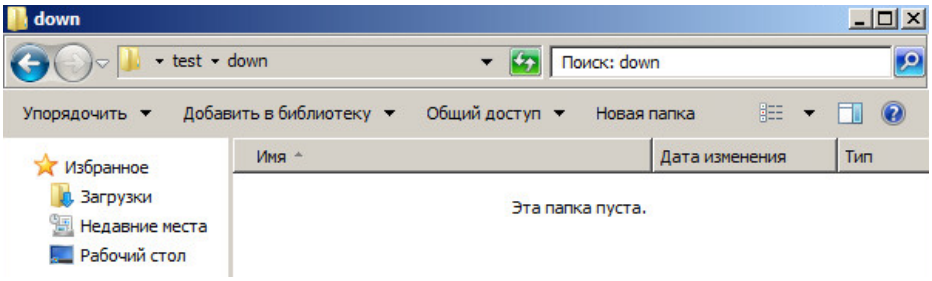
- на KK1 и KK2 в локальных настройках шифрования (учетные записи локальных администраторов – **kk1admin / P@ssword** и **kk2admin / P@ssword** соответственно) включите распределение потоков по ядрам процессора (т.е. опция 3 должна отображаться со значением "Запрет распределения пакетов с учетом соединений");



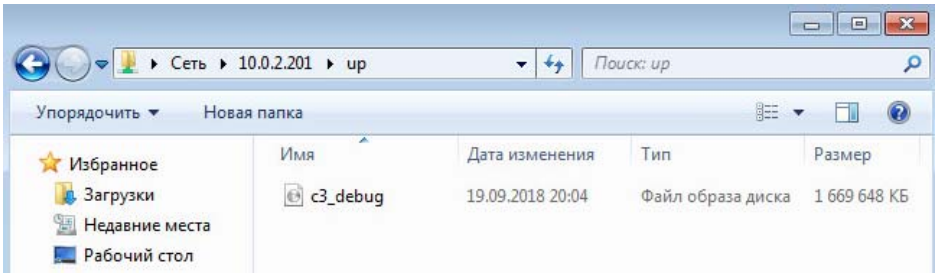
> **Для сведения.** В настройках шифратора данная установка отображается строкой net.inet.ipcrypt.l2_hash:1.

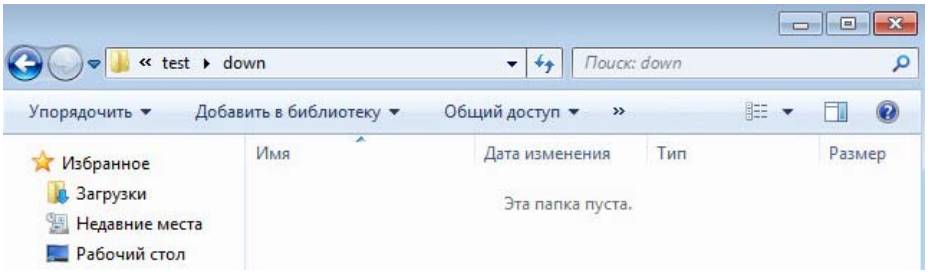
- переключитесь в окно консоли ВМ WS1 и откройте расположенную на ВМ AP (**по дополнительному адресу 10.0.2.211**) общедоступную папку "up" (локальный путь – "C:\test\up"), содержащую файл размером 1,6 Гбайт, а также локальную пустую папку "C:\test\down";



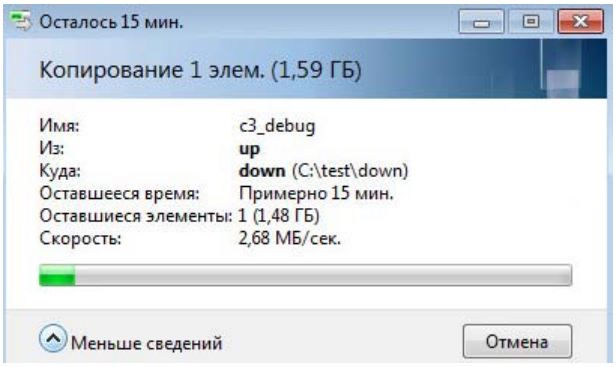


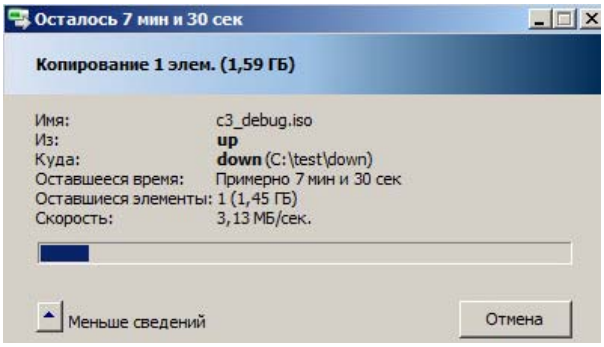
- переключитесь в окно консоли ВМ АР и откройте расположенную на ВМ WS1 (**по дополнительному адресу 10.0.2.201**) общедоступную папку "up" (локальный путь – "C:\test\up"), содержащую файл размером 1,6 Гбайт, а также локальную пустую папку "C:\test\down";





- в окне консоли ВМ АР запустите копирование файла из общедоступной папки "up" на ВМ WS1 (с адреса **10.0.2.201**) в локальную папку "C:\test\down";
- переключитесь в окно консоли ВМ WS1 и также запустите копирование файла из общедоступной папки "up" на ВМ АР (с адреса **10.0.2.211**) в локальную папку "C:\test\down";
- по ходу выполнения копирования оцените совокупную скорость передачи шифрованного трафика в двух направлениях (теперь для криптокоммутаторов это будут два потока шифрования по разным парам MAC-адресов при включенном распределении по ядрам – см. главу 1) и сравните результат с показателями, полученными в п. 3.





Таким образом, как отмечалось в главе 1, чтобы достигнуть оптимально максимального использования ресурсов КК и канала передачи данных при подключении защищаемых хостов к портам криптокоммутатора без промежуточного L3-оборудования (т.е. КК "видит" всю защищаемую сеть, много сессий по MAC-адресам), оптимальным будет разрешить распределение пакетов с учетом соединений (изменить настройку по умолчанию).

5. На ВМ AP и WS1 удалите скопированный файл (<Shift>+<Del>) из локальной папки "C:\test\down".
6. Восстановите конфигурацию учебного стенда:
   - выключите виртуальные машины KK1 и KK2;
   - на ВМ WS1 и AP восстановите конфигурацию сетевых параметров и переподключите сетевые интерфейсы к исходным виртуальным коммутаторам (см. описание учебного стенда);
   - включите виртуальную машину KSH_main.

   Проведена оценка производительности криптокоммутаторов "Континент" при взаимодействии между абонентами защищаемых сегментов одной подсети (L2VPN).

   Выполнение лабораторной работы завершено.

Контрольные вопросы

1. На чем основана возможность приоритизации трафика в комплексе?
2. Какие планировщики очередей поддерживаются в комплексе?
3. Какие настройки предусмотрены в комплексе для оптимизации работы шифратора и управления распределением шифрования сессий?
4. Какое состояние настройки "Разрешение / Запрет распределения пакетов с учетом соединений" является оптимальным для КШ, если в VPN-канале между защищаемыми сетями активны несколько сетевых соединений?
5. Какое состояние настройки "Разрешение / Запрет распределения пакетов с учетом соединений" является оптимальным для КК при подключении к портам криптокоммутатора защищаемых хостов без промежуточного L3-оборудования?

Глава 2
Поддержка динамической маршрутизации в АПКШ "Континент"

Протоколы динамической маршрутизации

Помимо статической, в АПКШ "Континент" поддерживается также динамическая маршрутизация. Правила динамической маршрутизации определяются поддерживаемыми протоколами: OSPF, RIP и BGP. Для их настройки необходимо сформировать конфигурационный файл "zebra.conf", а также конфигурационные файлы тех протоколов, которые будут использоваться ("ospfd.conf", "bgpd.conf", "ripd.conf").

Поддерживаются следующие версии протоколов:

- OSPF – версия 2;
- BGP – версия 4;
- RIP – версии 1 и 2.

Описание форматов и примеры файлов конфигурации см. в приложении "Формат и примеры конфигурационных файлов" к документу "АПКШ «Континент». Версия 3.9. Руководство администратора. Управление комплексом".

Динамическая маршрутизация не поддерживается в следующих случаях:

- включен режим привязки маршрутизаторов к MAC-адресам, что позволяет запретить на сетевом устройстве действие протокола ARP и осуществлять маршрутизацию по MAC-адресам маршрутизаторов. Такой подход обеспечивает защиту от сетевых атак типа ARP-spoofing. При использовании этой функции в случае замены маршрутизатора (сетевых карт узлов, выполняющих функции маршрутизатора) необходимо выполнить принудительное обновление зафиксированных в конфигурации сетевого устройства аппаратных адресов (подробнее см. раздел "Привязка аппаратных адресов маршрутизаторов" в документе "АПКШ «Континент». Версия 3.9. Руководство администратора. Управление комплексом");
- включен один из режимов Multi-WAN (см. главу 9 основного учебного курса "Администрирование АПКШ «Континент» версии 3.9").

Настройка динамической маршрутизации выполняется в следующем порядке:

1. Создание конфигурационного файла.
2. Настройка параметров динамической маршрутизации.

Поддержка протоколов динамической маршрутизации в комплексе реализована на базе платформы Quagga. Каждый из протоколов обслуживается отдельным процессом с последующим формированием таблиц маршрутизации. Одновременно могут работать несколько разных процессов под контролем управляющего процесса zebra, который служит для формирования таблицы маршрутизации и перераспределения маршрутов между различными протоколами.

Для просмотра информации о работе протоколов, таблиц маршрутизации и сведений о полученных/анонсируемых маршрутах следует подключаться к соответствующим управляющим консолям процессов по следующим портам:

- zebra – TCP/2601;
- ripd – TCP/2602, 2603;
- ospfd – TCP/2604;
- bgpd – TCP/2605.

Ниже в таблице приведен перечень некоторых команд для просмотра информации о работе соответствующих протоколов.

Команда	Описание
show running-config	отобразить конфигурацию
sh ip route	показать таблицу маршрутизации
sh ip rip status	показать общую информацию о работе RIP
sh ip rip	отобразить полученные по RIP маршруты
sh ip ospf	показать общую информацию о работе OSPF

Команда	Описание
sh ip ospf database	отобразить LSDB
sh ip ospf neighbors	показать информацию о соседях
sh ip ospf route	отобразить полученные маршруты
sh ip bgp	отобразить таблицу BGP
sh bgp neighbors	показать информацию о соседях
sh ip bgp nei <IP-пира> received-routes	показать полученные от соседа маршруты*
sh ip bgp nei <IP-пира> advertised-routes	отобразить анонсируемые соседу маршруты*

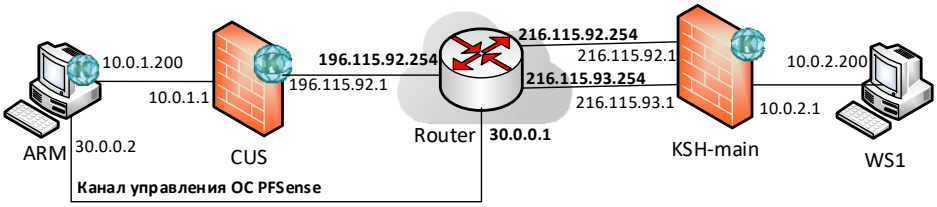
*Для выполнения этой команды необходимо в файл конфигурации "bgpd.conf" добавить строку **neighbor <IP-пира> soft-reconfiguration inbound**.

Лабораторный модуль №2 "Поддержка динамической маршрутизации в АПКШ "Континент"

Лабораторная работа №1 "Настройка динамической маршрутизации по протоколу BGP"

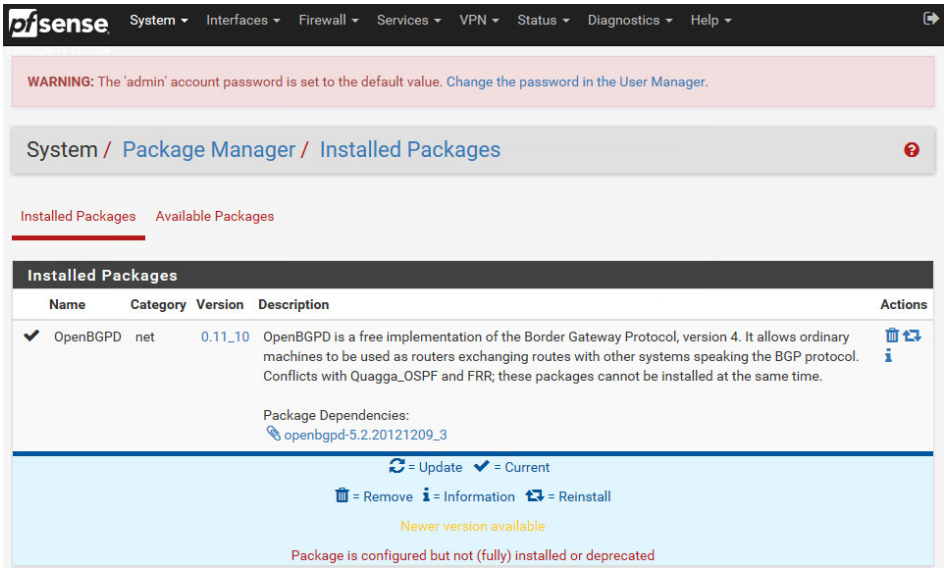
Сценарий. Для того чтобы обеспечить взаимодействие между защищаемыми подсетями 10.0.1.0/24 и 10.0.2.0/24, разделенными сетью общего доступа с маршрутизаторами, поддерживающими BGP-протокол, администратор выполняет настройку динамической маршрутизации на сетевых узлах "Континент" и проверяет работу сети.

В данной лабораторной работе задействованы ВМ, которые показаны на рисунке ниже. Роль стороннего BGP-маршрутизатора выполняет ВМ Router.



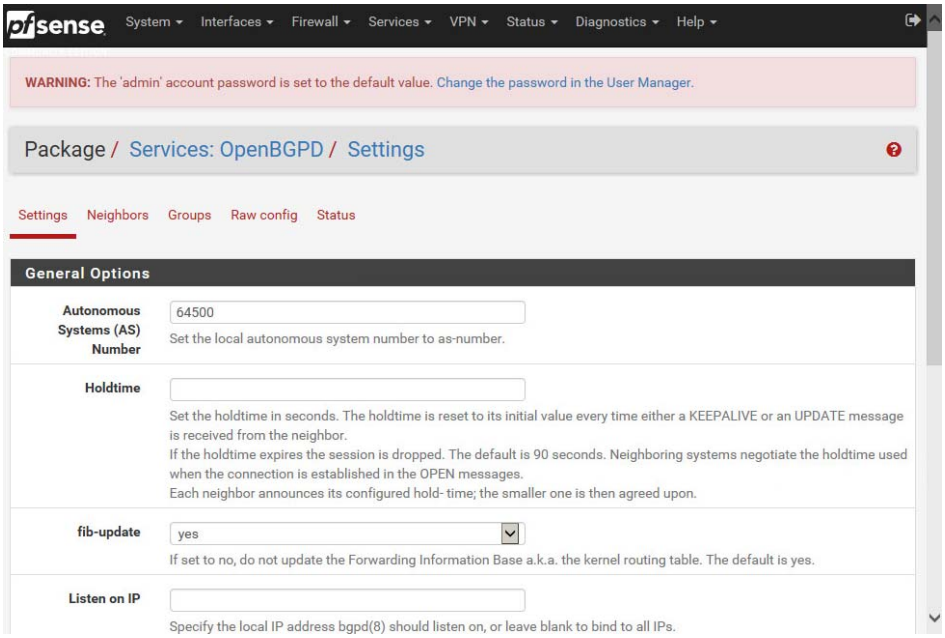
Перед началом выполнения лабораторной работы проведите минимально необходимую настройку протокола BGP на ВМ Router. Для этого:

1. В окне консоли ВМ ARM запустите обозреватель IE и подключитесь через веб-интерфейс к маршрутизатору: адрес – **https://30.0.0.1**, логин – **admin**, пароль – **pfsense**.
2. Выберите страницу "System / Package Manager" и на вкладке "Installed Packages" убедитесь, что на маршрутизаторе установлен пакет "OpenBGPD".

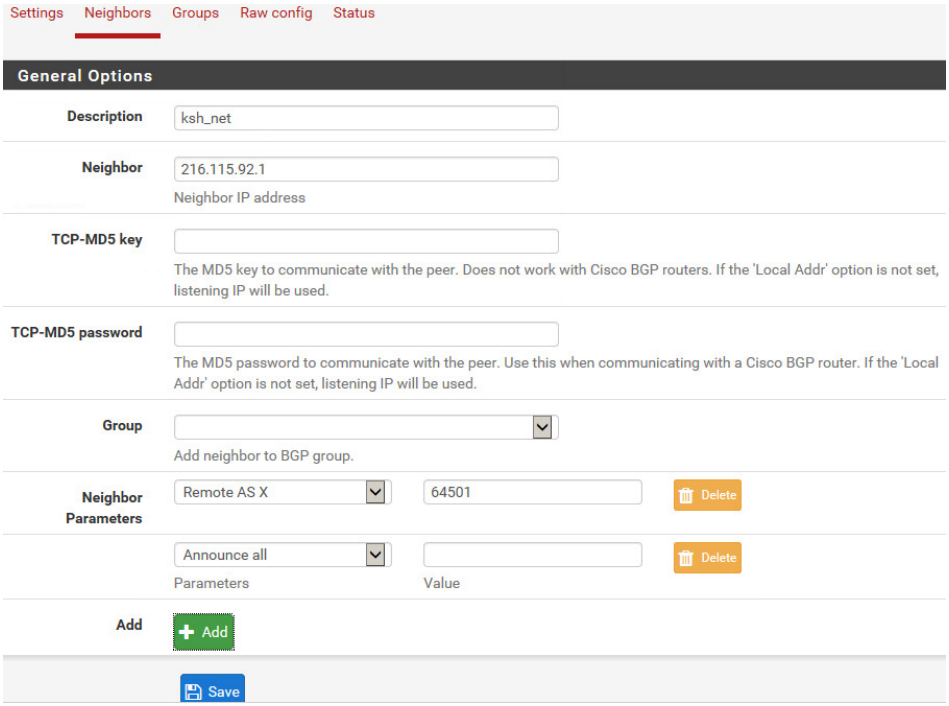


Обратите внимание, что данный пакет не поддерживает совместную работу с расширениями "Quagga_OSPF" и "FRR".

3. Выберите страницу настроек "Services / OpenBGPD" и на вкладке "Settings" установите следующие параметры:
   - "Autonomous Systems (AS) Number" – **64500**;
   - "Holdtime" – не заполняйте (по умолчанию);
   - "Listen to IP" – не заполняйте (будут прослушиваться все подключенные к маршрутизатору сети);
   - "Router IP" – **216.115.92.254**;
   - "Networks" – с помощью кнопки "Add" добавьте два значения: **196.115.92.0/24** и **216.115.92.0/24**;
   - для сохранения настроек нажмите кнопку "Save".



4. Выберите вкладку "Neighbors", нажмите кнопку "Add" и введите следующие параметры соседнего BGP-узла:
   - "Description" – **ksh_net** (произвольно);
   - "Neighbor" – **216.115.92.1**;
   - "Neighbor Parameters" – в выпадающем списке выберите параметр "Remote AS X" и введите значение **64501**;
   - с помощью кнопки "Add" добавьте в раздел "Neighbor Parameters" еще один параметр "Announce all";



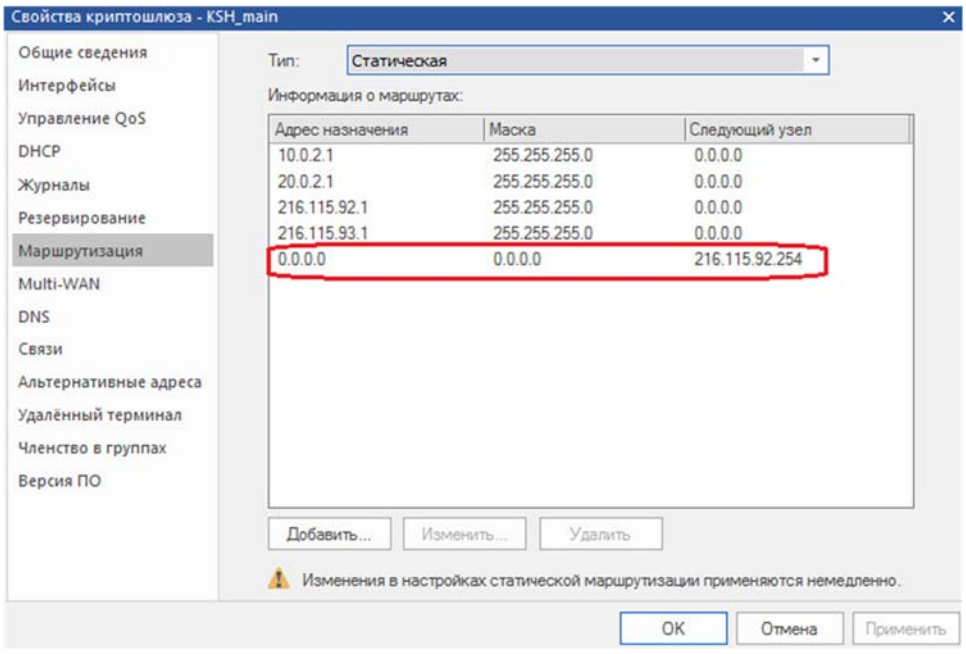
- для сохранения настроек нажмите кнопку "Save".

5. Выберите страницу настроек "Diagnostics / Reboot", перезагрузите BM Router и после загрузки системы снова откройте страницу "Services / OpenBGPD". Результат сделанных настроек будет проверен по ходу лабораторной работы.

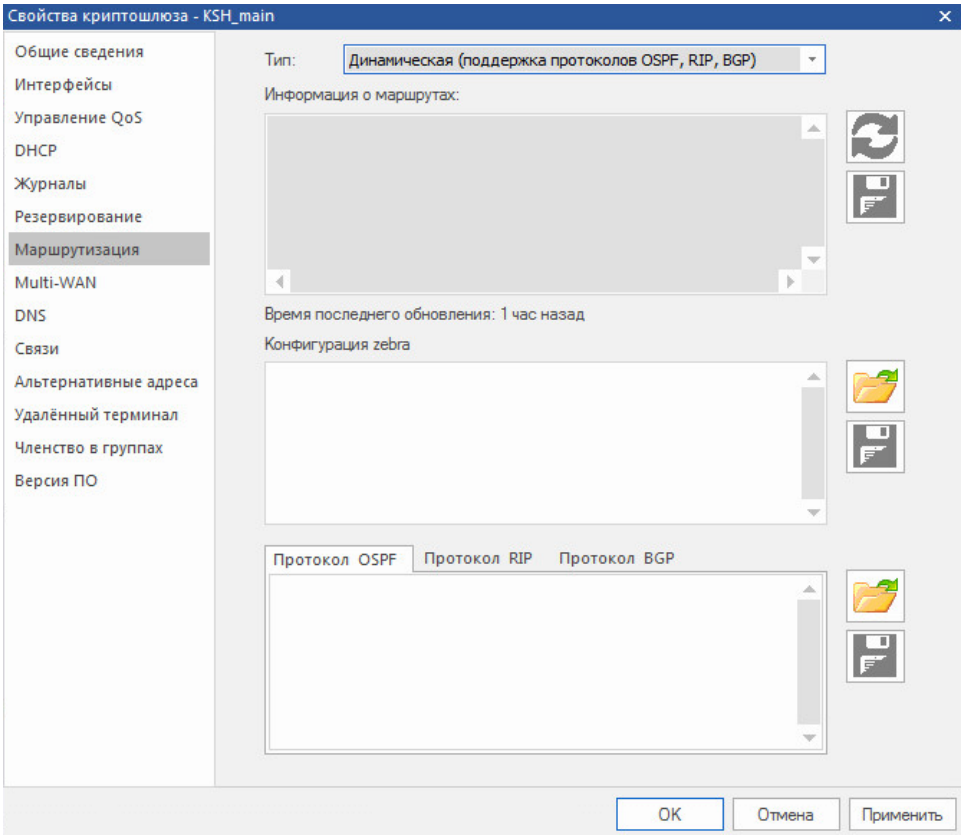
Далее по ходу лабораторной работы будет проведена настройка динамической маршрутизации по протоколу BGP на КШ KSH_main и проверка сохранения взаимодействия между защищаемыми подсетями при внесении изменений в схему маршрутов на стенде.

1. Для настройки на KSH_main динамической маршрутизации в ПУ ЦУС сделайте следующее:

- в области объектов управления выберите "Сетевые устройства Континент / Криптошлюзы" и через контекстное меню криптошлюза KSH_main откройте окно его свойств;
- выберите категорию "Маршрутизация". Обратите внимание, что в параметрах статической маршрутизации на данный момент присутствует единственный заданный вручную статический маршрут – адрес шлюза по умолчанию 216.115.92.254;



- в выпадающем списке "Тип" выберите "Динамическая (поддержка протоколов OSPF, RIP, BGP)". Обратите внимание, что при необходимости можно загрузить конфигурационный файл нужного протокола с помощью кнопок "Загрузить конфигурацию из файла" ;



- в поле "Конфигурация zebra" введите следующий текст конфигурационного файла:

  hostname ksh_main

  password P@ssw0rd

  log stdout

  ip route 0.0.0.0/0 216.115.92.254

  Примите к сведению. В реальной работе в конфигурации zebra следует описать все действующие на данном узле статические маршруты (строки "ip route …").

- в нижнем тестовом поле выберите вкладку "Протокол BGP" и введите следующий текст конфигурационного файла:

  hostname ksh_main

  password P@ssw0rd

  router bgp 64501

  bgp router –id 216.115.92.1

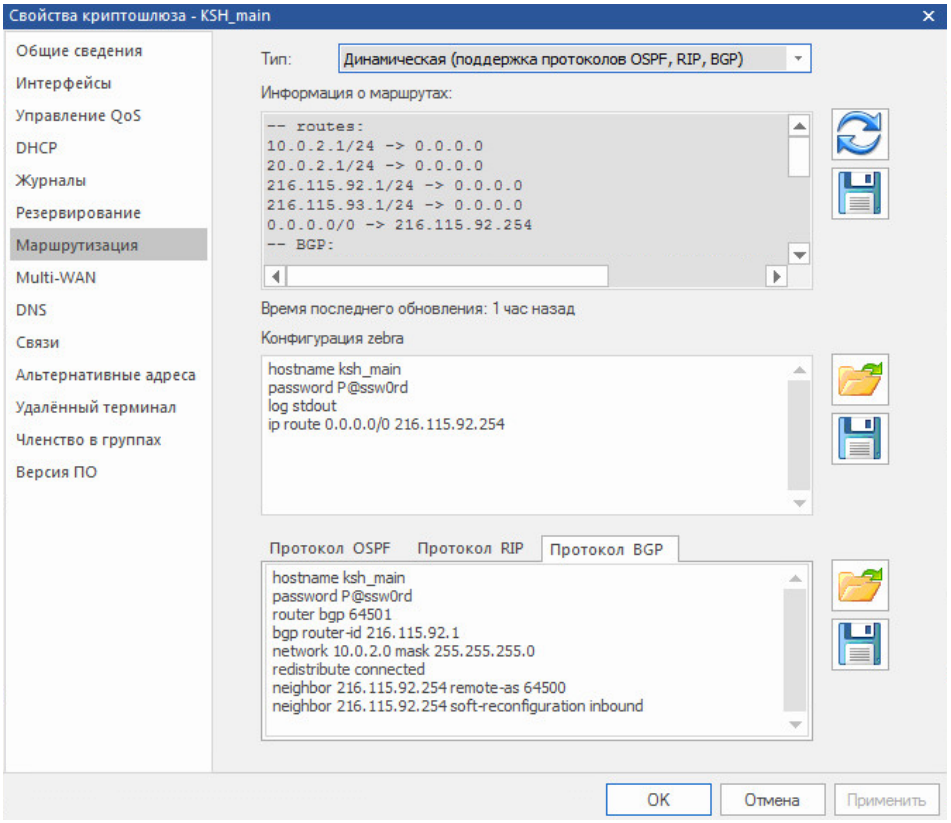
  network 10.0.2.0 mask 255.255.255.0

  redistribute connected

  neighbor 216.115.92.254 remote-as 64500

  neighbor 216.115.92.254 soft-reconfiguration inbound

- нажмите кнопку "Применить". Сетевому устройству будет отправлена команда на загрузку в ЦУС списка маршрутов, и в ЦУС начнется обновление информации о сетевом устройстве – ход этого процесса будет отображаться в поле "Информация о маршрутах". После завершения обновления список маршрутов данного сетевого устройства поступит из ЦУС в ПУ и будет отображен в этом поле;



Примечание. В реальной работе при достаточно большом количестве маршрутов обновление информации на ЦУС может потребовать дополнительного времени. При этом кнопка прерывания обновления в течение примерно 50 секунд будет недоступна.

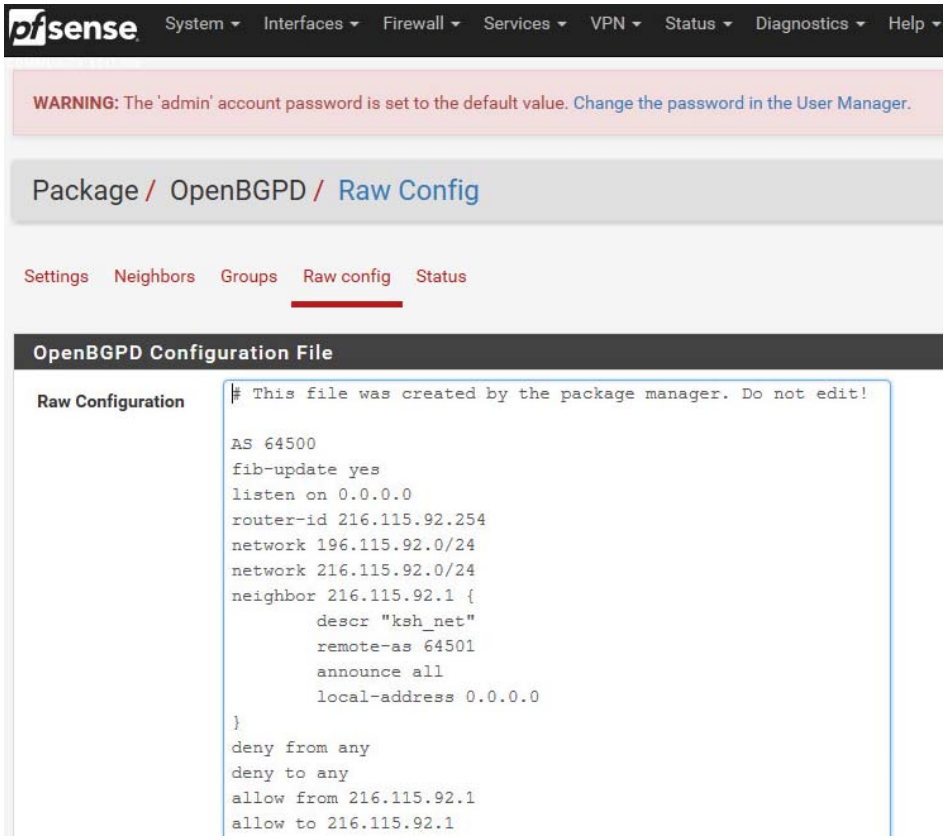
Если необходимо сохранить в виде текстового файла информацию о маршрутах или конфигурациях, используйте кнопку "Сохранить..."  , расположенную справа от соответствующего раздела.

- нажмите кнопку "ОК" и вернитесь к списку криптошлюзов.

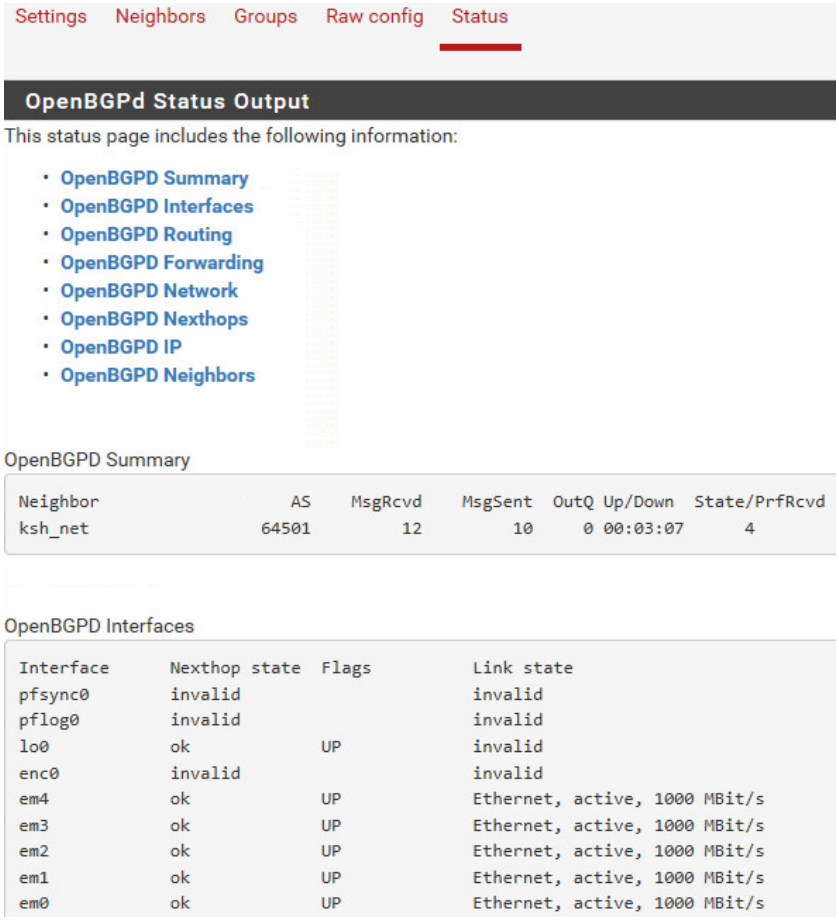
Примечание. После закрытия окна свойств сетевого устройства информация о маршрутах, отображаемая на вкладке "Маршрутизация", не сохраняется. При следующем открытии окна на вкладке "Маршрутизация" раздел "Информация о маршрутах" будет обновлен заново.

2. Для просмотра информации о текущих BGP-сессиях, соседях, действующих маршрутах на маршрутизаторе Router переключитесь в окно браузера IE, в веб-интерфейсе маршрутизатора откройте страницу "Services / OpenBGPD" и просмотрите следующие вкладки:

- "Raw config" – автоматически сгенерированный в результате сделанных настроек текст конфигурационного файла (возможен только просмотр!);



- "Status" – текущие сведения о конфигурации BGP на маршрутизаторе.



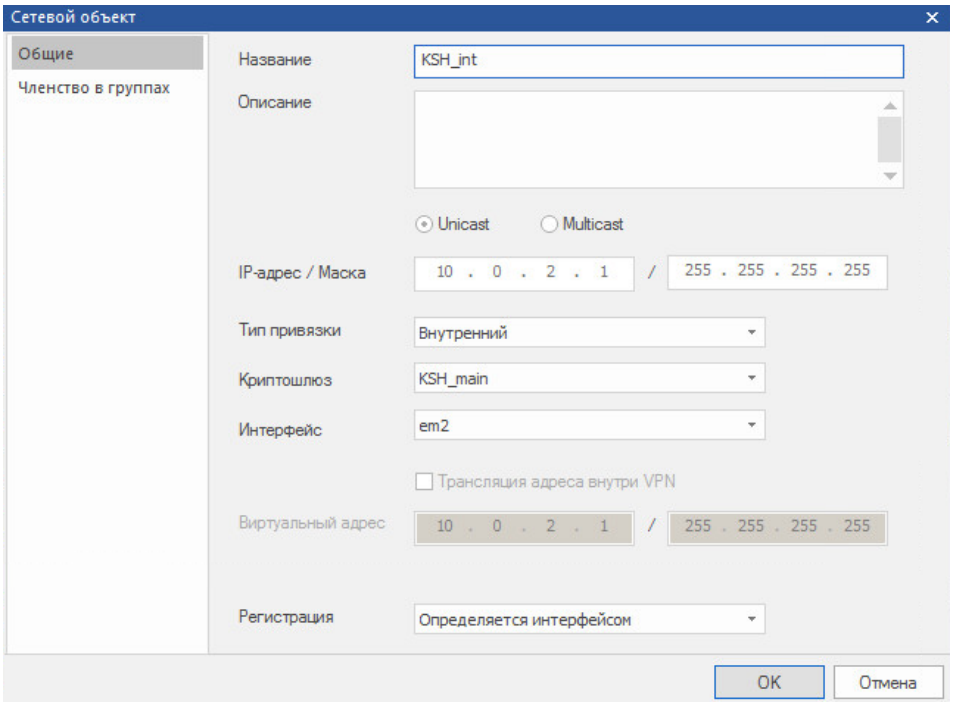
3. Для просмотра на KSH_main сведений о текущих BGP-сессиях, соседях, полученных или анонсируемых маршрутах следует использовать удаленное подключение на соответствующий порт управляющей консоли процесса:

- zebra – TCP/2601;
- bgpd – TCP/2605.

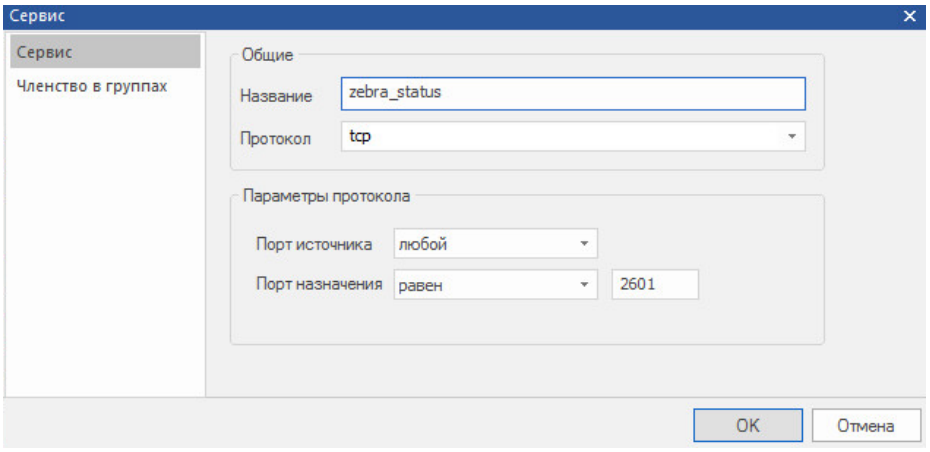
Для того чтобы обеспечить удаленное подключение к KSH_main по указанным портам, создайте:

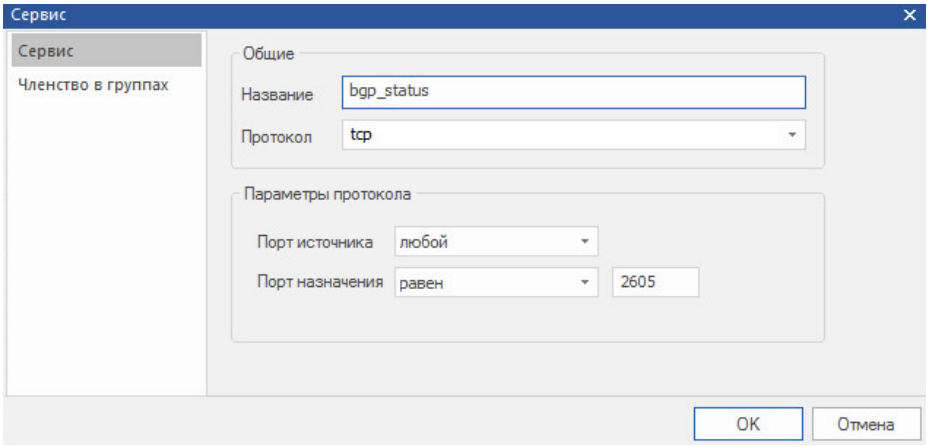
- новый сетевой объект с реквизитами согласно представленной ниже таблице;

Наименование поля	Значение
Название	KSH_int
IP-адрес/маска	10.0.2.1/255.255.255.255
Тип привязки	Внутренний
Криптошлюз	KSH_main
Интерфейс	em2



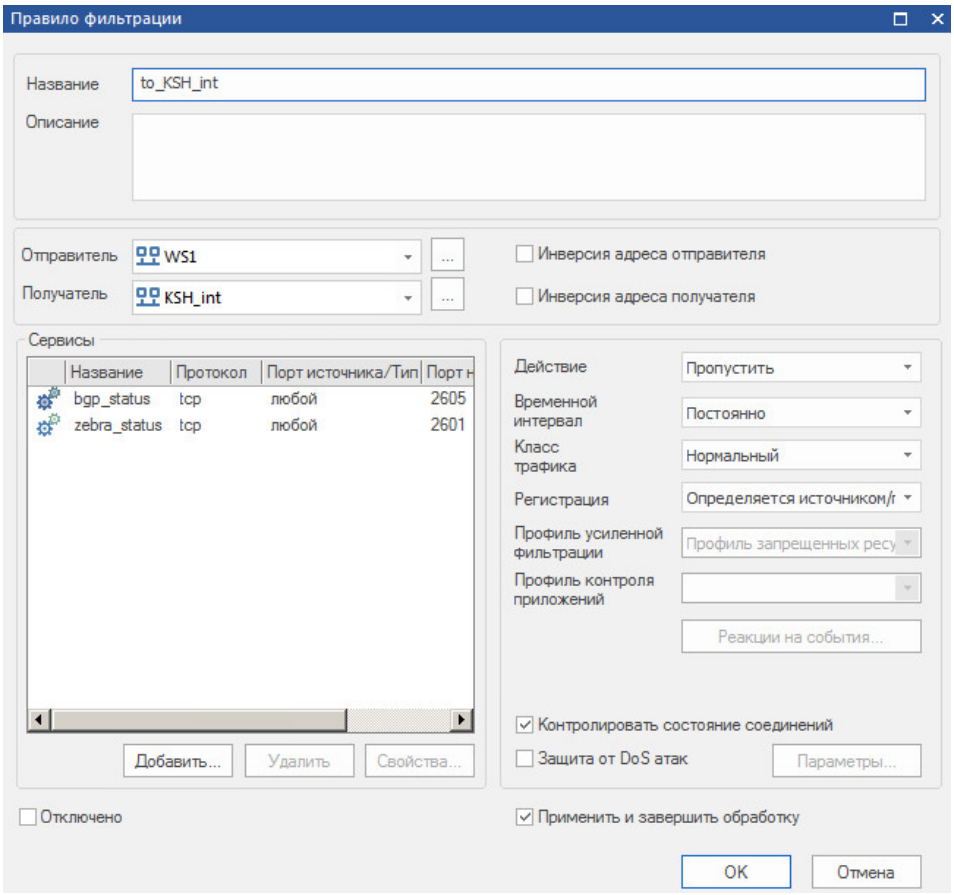
- сетевые сервисы с реквизитами согласно представленным ниже рисункам;





- правило фильтрации (или внесите изменения в уже существующие) с реквизитами согласно представленной ниже таблице, а затем – сохраните сделанные изменения.

Наименование поля	Значение
Название	to KSH_int
Отправитель	WS1
Получатель	KSH_int
Сервисы	zebra_status, bgp_status
Действие	Пропустить
Класс трафика	"Нормальный"
Контролировать состояние соединений	Включить
Применить и завершить обработку	Включить

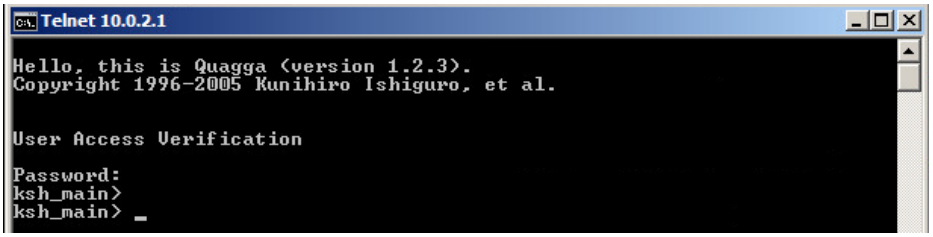


4. Для просмотра на KSH_main сведений о текущих BGP-сессиях, соседях, полученных или анонсируемых маршрутах переключитесь в окно консоли WS1 и выполните следующие действия:

- запустите утилиту командной строки и подключитесь к порту 2601 управляющей консоли zebra на KSH_main командой:

  telnet 10.0.2.1 2601

  на запрос пароля введите **P@ssw0rd**

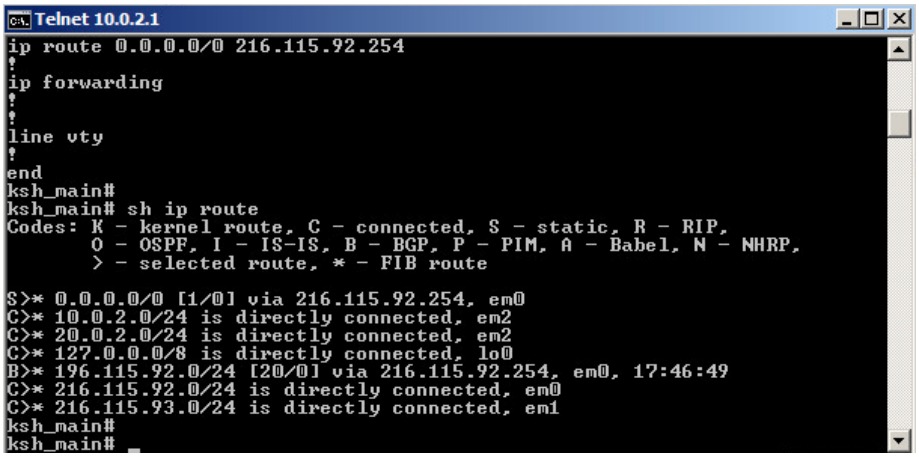


- для просмотра конфигурации и таблицы маршрутов последовательно введите команды:

  enable

  show running-config

  sh ip route



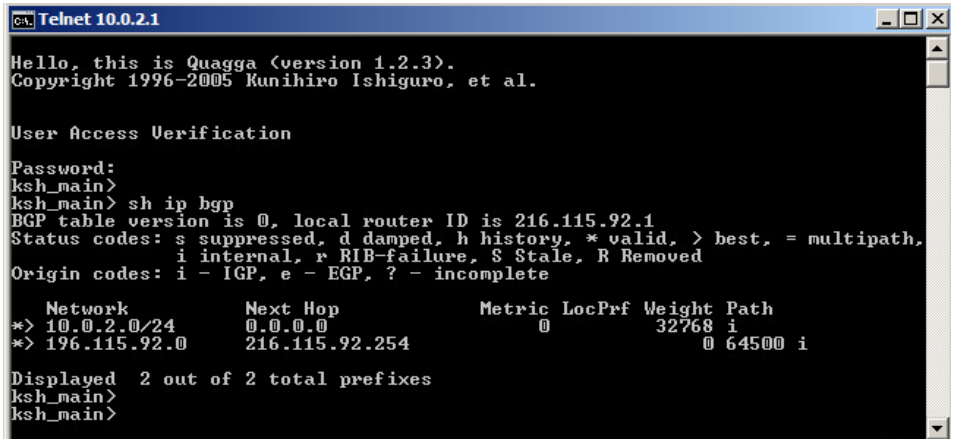
- завершите telnet-сеанс командой **exit** и подключитесь к порту 2605 управляющей консоли bgpd на KSH_main командой:

  telnet 10.0.2.1 2605

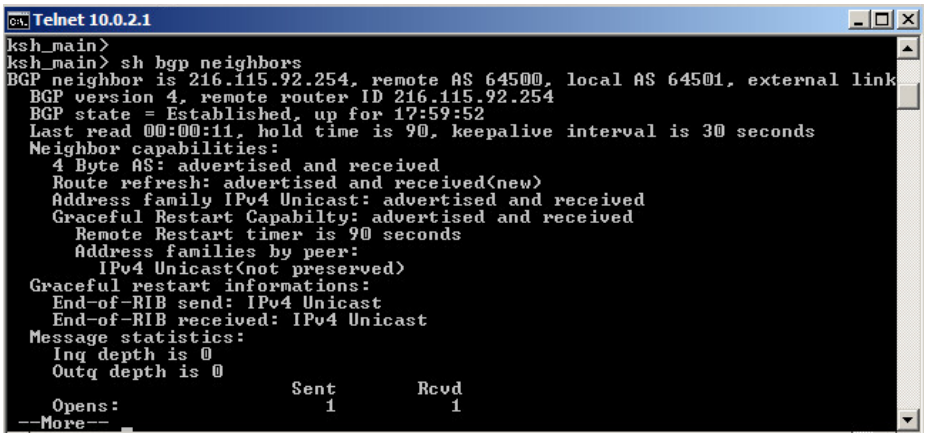
  на запрос пароля введите **P@ssw0rd**

- для просмотра bgp-таблицы, информации о соседях, полученных и анонсируемых маршрутах последовательно введите команды:

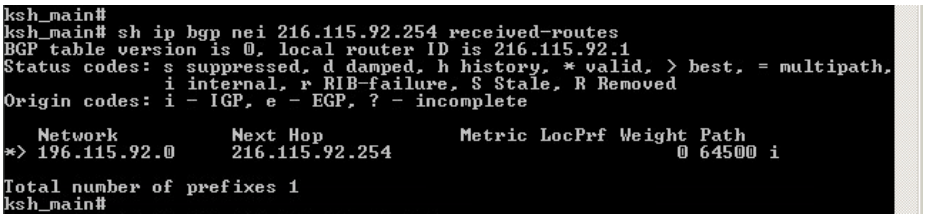
  sh ip bgp



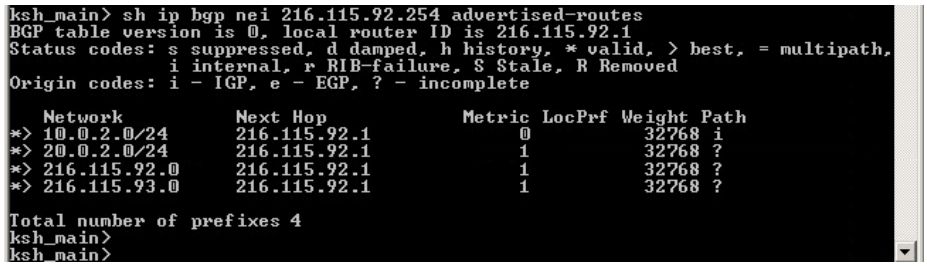
  sh bgp neighbors



sh ip bgp nei 216.115.92.254 received-routes

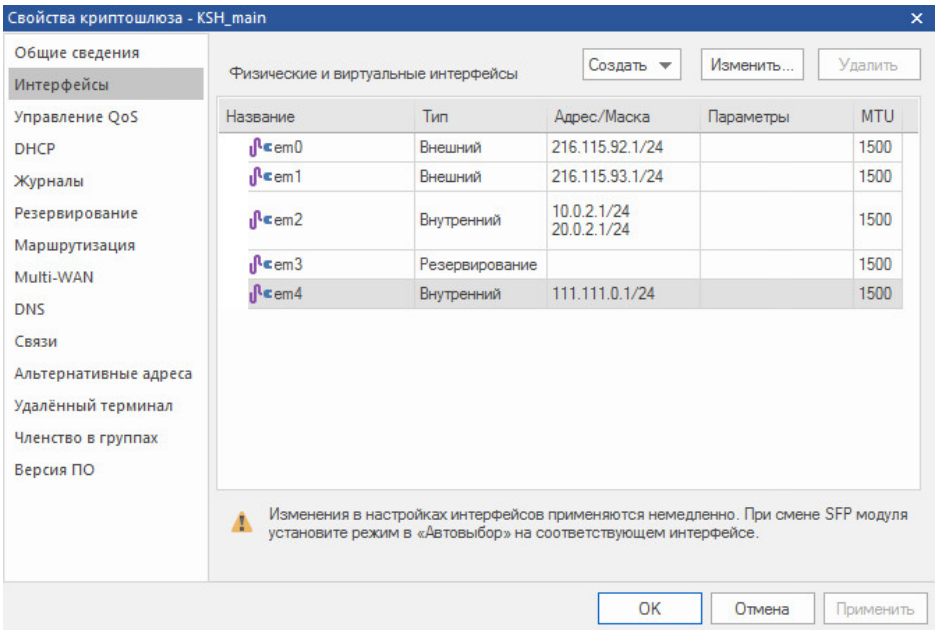


sh ip bgp nei 216.115.92.254 advertised-routes

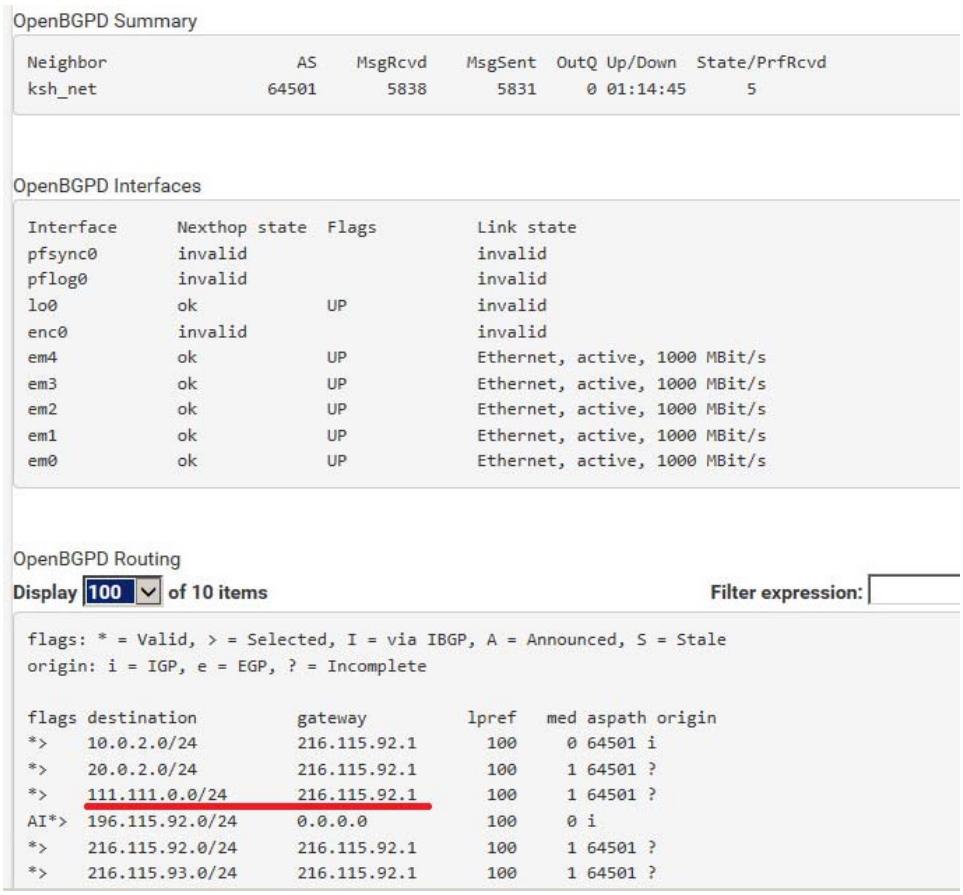


exit

5. Для того чтобы протестировать передачу сведений о вновь появившихся маршрутах между BGP-соседями, выполните следующие действия:
   - переключитесь в окно ВМ ARM и в ПУ ЦУС через контекстное меню крип-тошлюза KSH_main откройте окно его свойств;
   - выберите категорию "Интерфейсы" и для интерфейса "em4" установите: "Тип" – "Внутренний", "Адрес/Маска" – **111.111.0.1/24**;



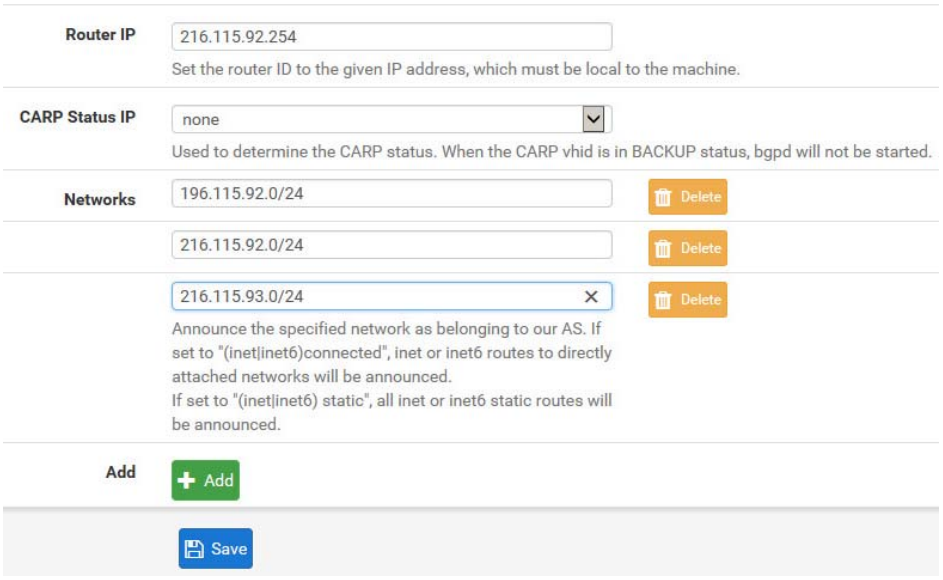
- нажмите кнопку "ОК";
- переключитесь в окно браузера IE, в веб-интерфейсе маршрутизатора откройте страницу "Services / OpenBGPD" и выберите вкладку "Status". Дождитесь обновления сведений и убедитесь, что на маршрутизаторе появился маршрут к вновь добавленной на КШ подсети 111.111.0.0/24.



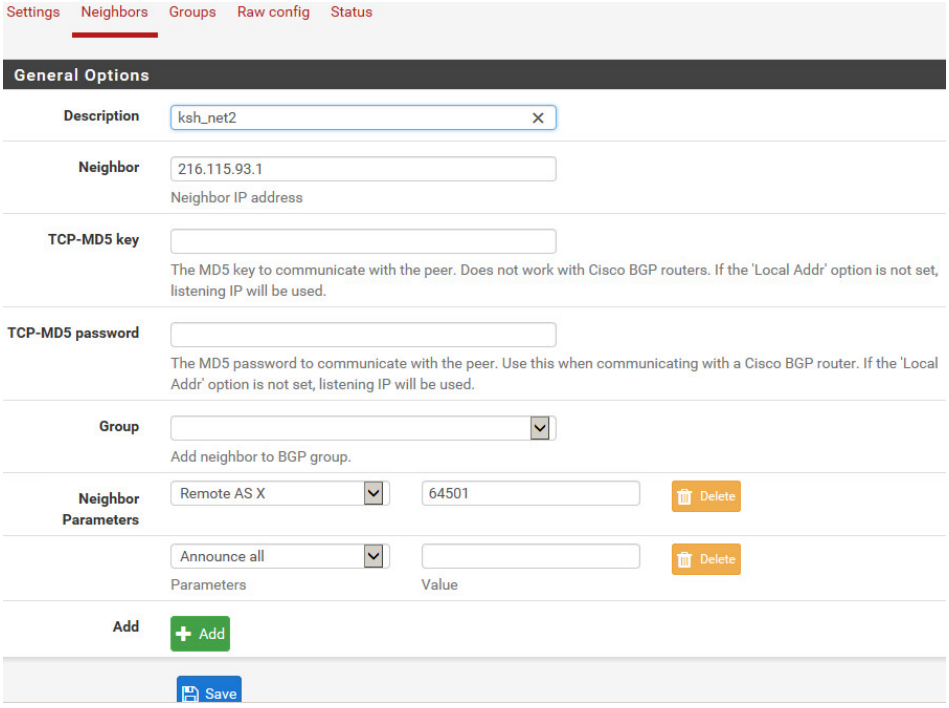
6. Для того чтобы протестировать взаимодействие сетевых узлов "Континент", работающих в режиме динамической маршрутизации, необходимо внести соответствующие изменения в конфигурацию маршрутизатора Router и сетевых узлов комплекса.

Для внесения изменений в конфигурацию маршрутизатора Router выполните следующие действия:

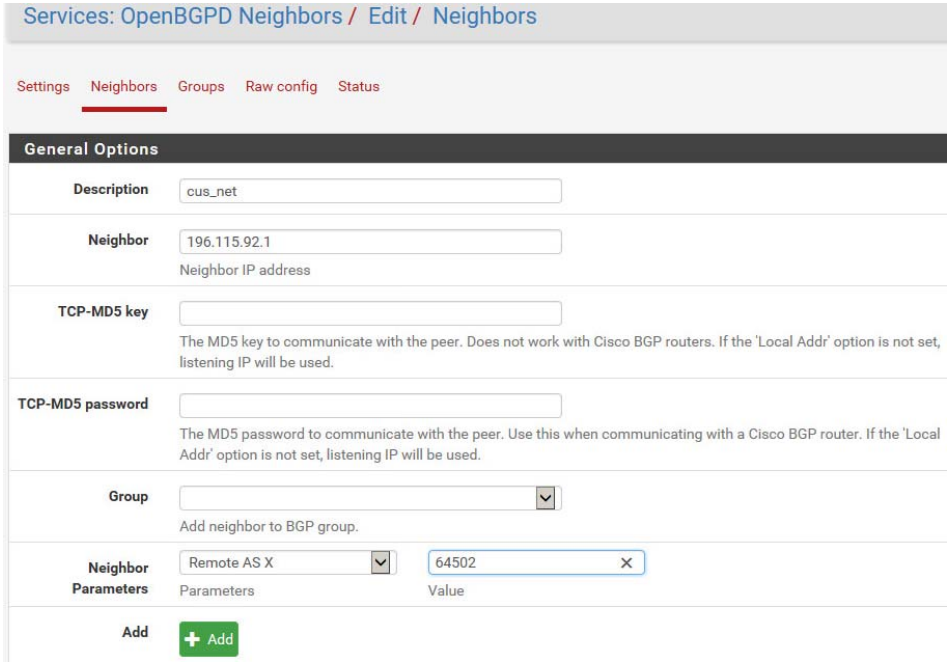
- переключитесь на вкладку "Settings" и в разделе "Networks" с помощью кнопки "Add" добавьте еще одно значение **216.115.93.0/24**;



- нажмите кнопку "Save" и переключитесь на вкладку "Neighbors";
- через кнопку "Add" добавьте еще один соседний BGP-узел со следующими параметрами:
  - "Description" – **ksh_net2** (произвольно);
  - "Neighbor" – **216.115.93.1**;
  - в разделе "Neighbor Parameters" добавьте параметры: "Remote AS X" со значением **64501** и "Announce all";



- нажмите кнопку "Save". На вкладке "Neighbors" через кнопку "Add" добавьте еще один соседний BGP-узел со следующими параметрами:
  - "Description" – **cus_net** (произвольно);
  - "Neighbor" – **196.115.92.1**;
  - в разделе "Neighbor Parameters" добавьте параметры: "Remote AS X" со значением **64502** и "Announce all";



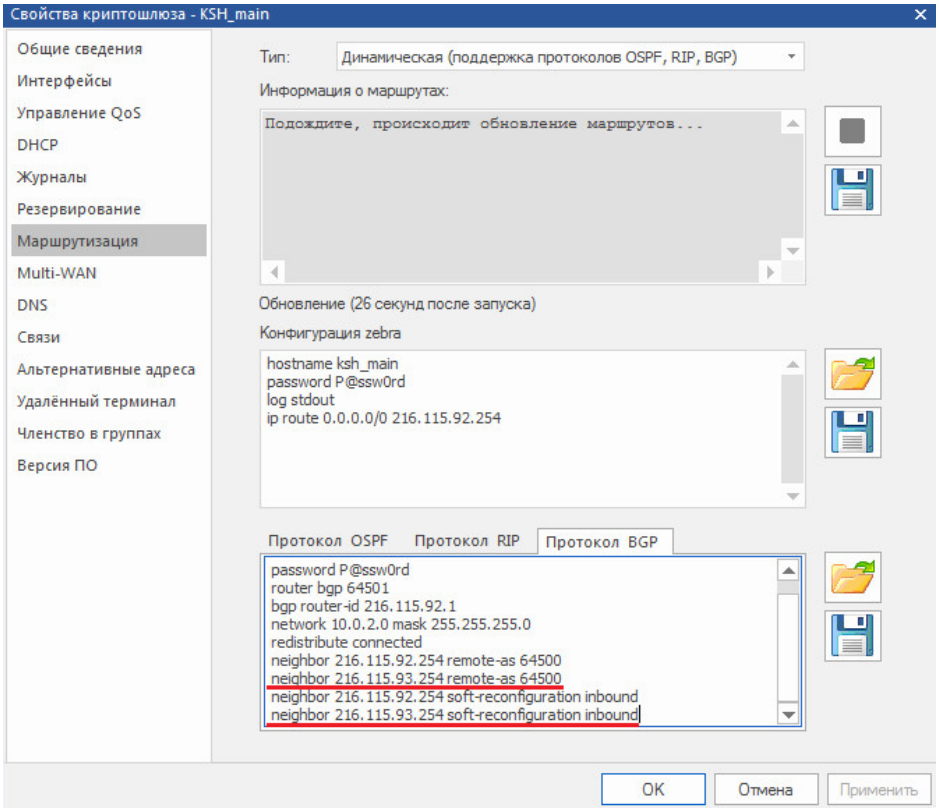
- сохраните сделанные настройки на маршрутизаторе Router.

7. Для настройки динамической маршрутизации на сетевых узлах "Континент" переключитесь в окно ПУ ЦУС и выполните следующие действия:

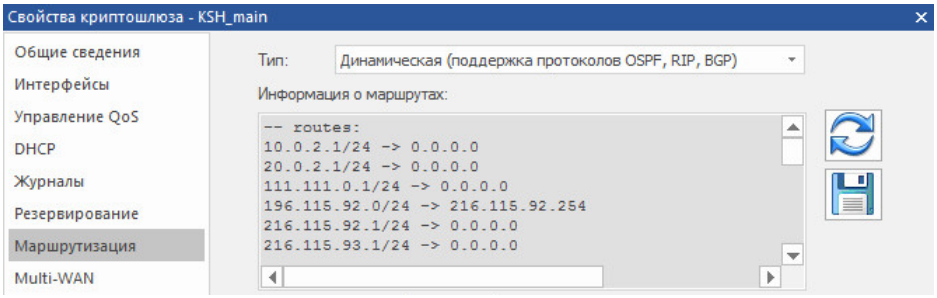
- откройте окно свойств криптошлюза KSH_main и в категории настроек "Маршрутизация" в нижнем тестовом поле выберите вкладку "Протокол BGP". Добавьте в текст конфигурационного файла следующие строки:

  neighbor 216.115.93.254 remote-as 64500

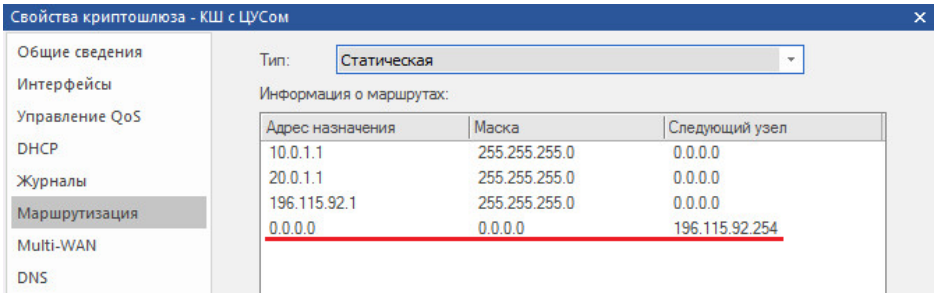
  neighbor 216.115.93.254 soft-reconfiguration inbound



- нажмите кнопку "Применить", дождитесь завершения обновления списка маршрутов данного сетевого устройства и отображения сведений в поле "Информация о маршрутах";



- закройте окно свойств криптошлюза KSH_main, вызовите окно свойств КШ с ЦУСом и выберите категорию "Маршрутизация". Обратите внимание, что в параметрах статической маршрутизации на данный момент присутствует единственный заданный вручную статический маршрут – адрес шлюза по умолчанию 196.115.92.254;



- в выпадающем списке "Тип" выберите "Динамическая (поддержка протоколов OSPF, RIP, BGP)". В поле "Конфигурация zebra" введите следующий текст конфигурационного файла:

  hostname cus

  password 11111111

  log stdout

  ip route 0.0.0.0/0 196.115.92.254

  Примите к сведению. В реальной работе в конфигурации zebra следует описать все действующие на данном узле статические маршруты (строки "ip route …").

- в нижнем тестовом поле выберите вкладку "Протокол BGP" и введите следующий текст конфигурационного файла:

  hostname cus

  password 11111111

  router bgp 64502

  bgp router–id 196.115.92.1

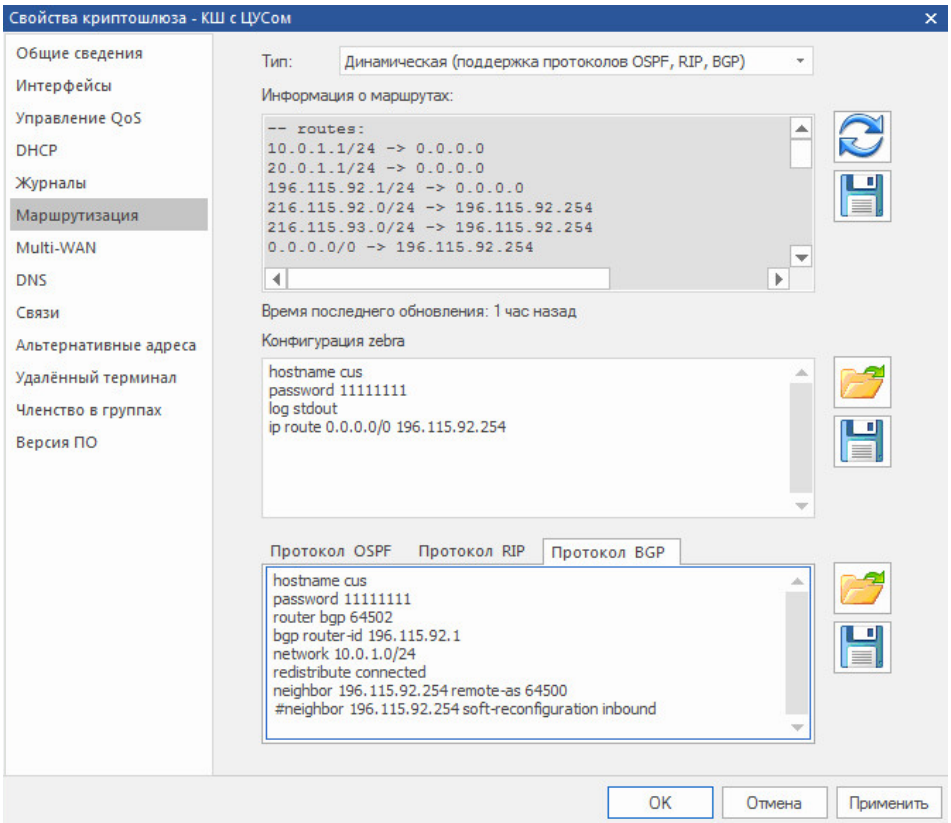
  network 10.0.1.0 mask 255.255.255.0

  redistribute connected

  neighbor 196.115.92.254 remote-as 64500

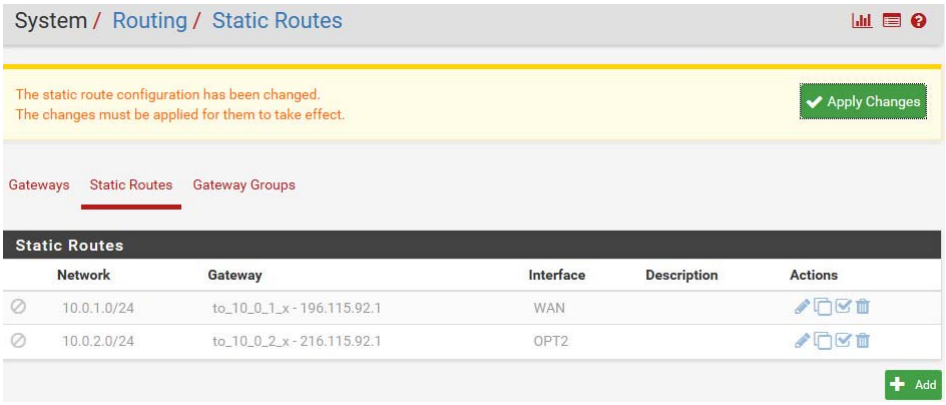
  neighbor 196.115.92.254 soft-reconfiguration inbound

- нажмите кнопку "Применить". Дождитесь завершения обновления списка маршрутов данного сетевого устройства и отображения изменений в поле "Информация о маршрутах".

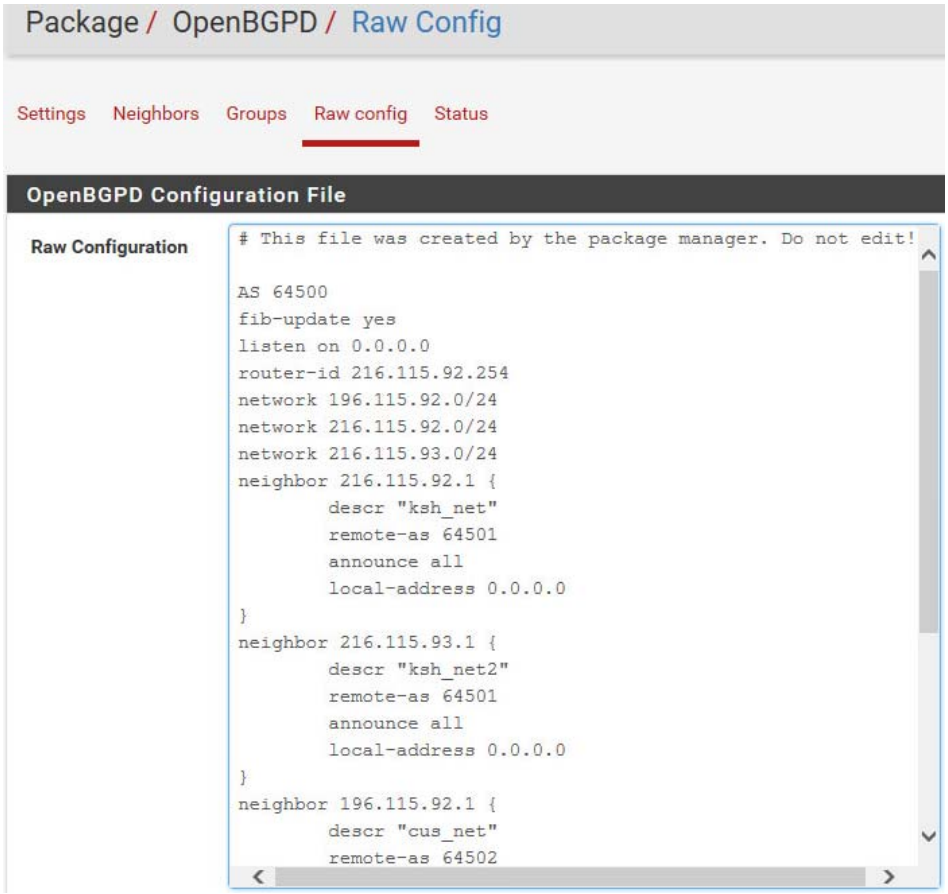


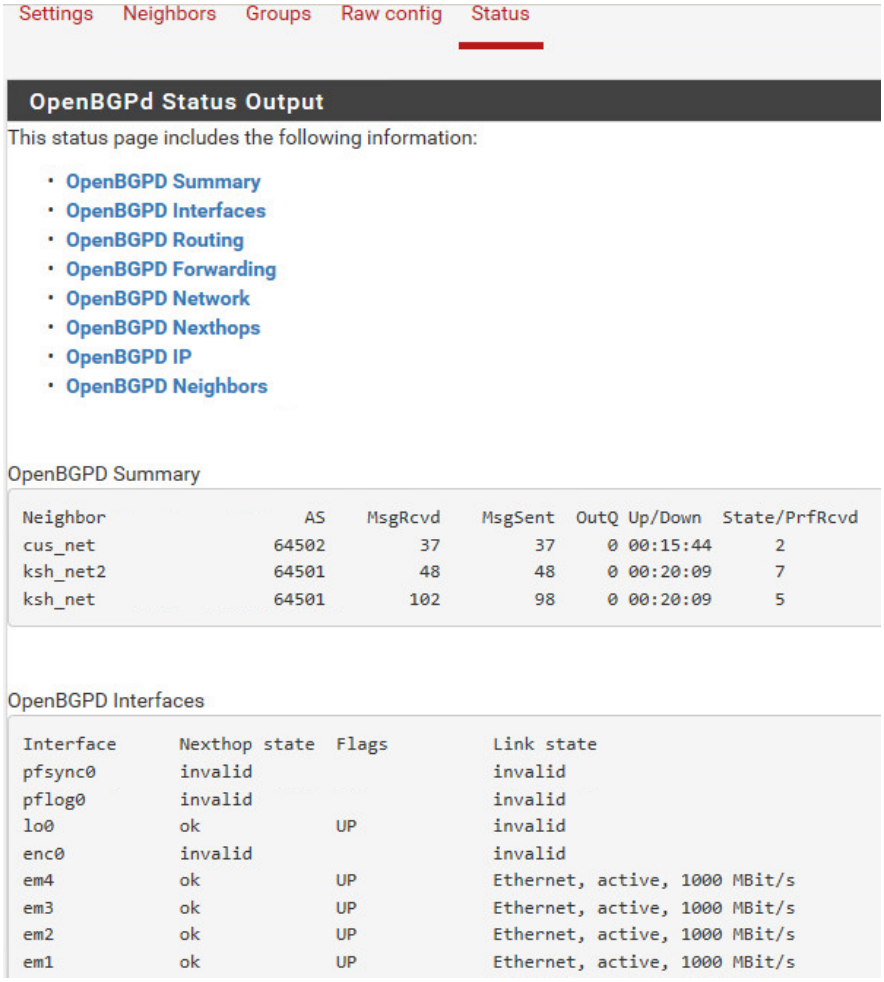
8. Переключитесь в окно браузера IE и в веб-интерфейсе маршрутизатора выполните следующие действия:

- откройте страницу "System / Routing", выберите вкладку "Static Routes" и, используя кнопку "Disable route"  , отключите действующие статические маршруты, примените сделанные изменения, а затем перезагрузите Router с помощью опции "Diagnostic / Reboot";



- используя описание п. 2, просмотрите информацию о текущих BGP-сессиях, соседях и действующих маршрутах на маршрутизаторе Router (вкладки "Raw config" и "Status" на странице "Services / OpenBGPD" в окне веб-интерфейса маршрутизатора).

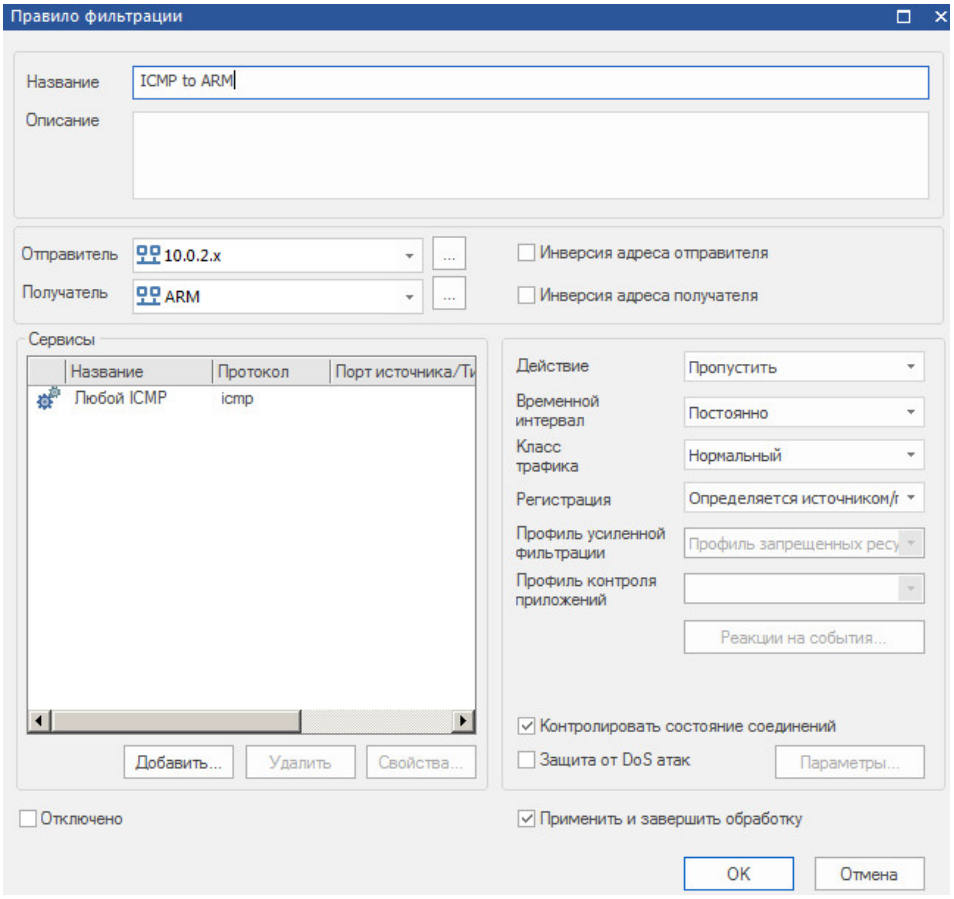




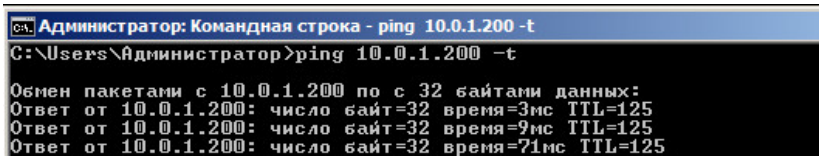
9. Для того чтобы протестировать взаимодействие сетевых узлов "Континент", работающих в режиме динамической маршрутизации, выполните следующие действия:

- самостоятельно, используя описание пп. 3, 4, создайте аналогичные сетевой объект CUS_int и правило фильтрации, а затем просмотрите из окна консоли ARM сведения о текущих BGP-сессиях, соседях, полученных или анонсируемых маршрутах на CUS;
- создайте правило фильтрации (или внесите изменения в уже существующее) с реквизитами согласно представленной ниже таблице, а затем – сохраните сделанные изменения;

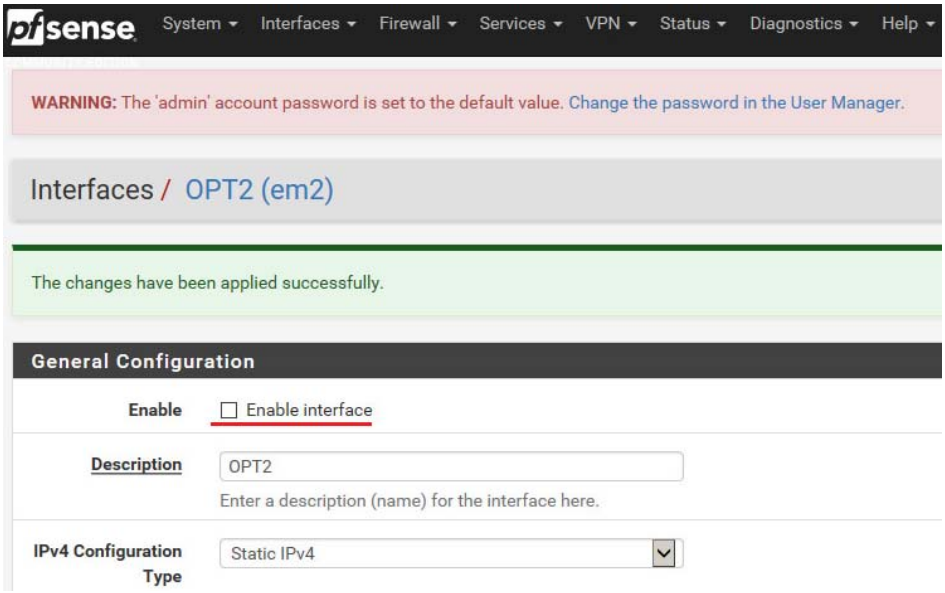
Наименование поля	**Значение**
Название	ICMP to ARM
Отправитель	10.0.2.x
Получатель	ARM
Сервисы	Любой ICMP
Действие	Пропустить
Класс трафика	"Нормальный"
Контролировать состояние соединений	Включить
Применить и завершить обработку	Включить



- переключитесь в окно консоли ВМ WS1, запустите утилиту командной строки и с помощью команды **ping 10.0.1.200 -t** активируйте постоянную проверку доступности компьютера ARM;



- переключитесь в окно консоли ВМ ARM и в веб-интерфейсе маршрутизатора откройте страницу "Interfaces / OPT2". Отключите интерфейс OPT2 (216.115.92.254), сняв отметку в поле "Enable interface", а затем – сохраните и примените сделанные изменения;



- переключитесь в окно консоли BM WS1 и по отклику утилиты ping убедитесь, что после сбоя основного канала на маршрутизаторе Router компьютер ARM остается доступным, поскольку трафик передается через другой интерфейс.

В окне утилиты командной строки остановите выполнение команды ping.

Проведена настройка BGP-протокола на сетевых узлах "Континент" и протестировано сетевое взаимодействие между ними.

Выполнение лабораторной работы завершено.

Контрольные вопросы

1. Какие версии протоколов динамической маршрутизации поддерживаются в комплексе?
2. Какие порты для подключения к узлу "Континент" следует использовать для просмотра информации о работе протоколов, таблиц маршрутизации и сведений о полученных/анонсируемых маршрутах?