

# Администрирование АПКШ "Континент" версии 3.9. Дополнительные настройки

Учебно-методическое пособие



### © Компания "Код Безопасности", 2019. Все права защищены.

Все авторские права на методическое пособие защищены.

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

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

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

# Оглавление

Список сокращений	. 4
Введение	. 5
Глава 1. Управление QoS	. 6
Определение классов трафика	. 6
Настройка приоритизации трафика	. 6
Настройки шифрования для оптимизации работы комплекса при организаци L2 и L3VPN	и .7
Лабораторный модуль №1 "Управление QoS"	. 9
Краткое описание учебного стенда	9
Лабораторная работа №1 "Настройка QoS на сетевых интерфейсах узлов "Континент"	11
Лабораторная работа №2 "Оценка производительности КШ «Континент» в режиме шифрования (L3VPN)"	25
Лабораторная работа №3 "Оценка производительности КК «Континент» (L2VPN)"	32
Контрольные вопросы	42
Глава 2. Поддержка динамической маршрутизации в АПКШ "Континент"	43
Протоколы динамической маршрутизации	43
Лабораторный модуль №2 "Поддержка динамической маршрутизации в АПКІ "Континент"	Ш 44
Лабораторная работа №1 "Настройка динамической маршрутизации по протоколу BGP"	44
Контрольные вопросы	61

# Список сокращений

FPGA	Field-Programmable Gate Array — программируемая логическая интегральная схема (ПЛИС)		
ICMP	Internet Control Message Protocol		
IP	Internet Protocol		
ТСР	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		
OC	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 ИТслужб, 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".

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

> 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:



Условные

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 (<u>info@securitycode.ru</u>).

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 "Hyperthreading" (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.

#### Ceccия: "Source\_ip:proto:port – Destination\_ip:proto:port"



У КК сессия – это обмен между хостами по МАС-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 SMBпротоколу) 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.



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 HTTPсоединения – 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.Х/24 имитирует внутреннюю/защищаемую сеть организации;
- 196.115.92.Х/24 и 196.115.93.Х/24 имитируют внешние сети организации;
- 216.115.92.Х/24 и 216.115.93.Х/24 имитируют внешние сети филиала;
- 10.0.2.X/24 имитирует внутреннюю/защищаемую сеть филиала;
- 30.0.0.Х/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 OC 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 "С:\" 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 **КК1** и **КК2** 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 **АР** 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@sswOrd;
- 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 BM 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:

- Для последующего сравнения оценивается средняя скорость передачи трафика (SMB-протокол) при прямом сетевом взаимодействии (без промежуточных сетевых узлов) в разных направлениях.
- 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.
- 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.
- 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 BM AP сделайте следующее:
  - в настройках ВМ переподключите сетевой интерфейс на тот, к которому подключена BM WS1;

	Show All Devices	Add Remove	Device Status Connected
Haro	lware	Summary	Connect at power on
	Memory CPUs Video card VMCI device USB controller SCSI controller 0 CD/DVD drive 1 Hard disk 1 Floppy drive 1 Network adapter 1 (edite	2048 MB 1 Video card Deprecated Present LSI Logic SAS [datastore] win7sp1x64 Virtual Disk Client Device Cont39_10.0.2.X	Adapter Type Current adapter: E1000 MAC Address 00:50:56:89:41:60 © Automatic © Manual DirectPath I/O Status: Not supported 💿
			Network Connection Network label: Cont39_10.0.2.X

 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;

Свойства: Протокол Интернета верс	ии 4 (ТСР/	/IPv4)		? <mark>×</mark>
Общие				
Параметры IP могут назначаться ав поддерживает эту возможность. В г IP можно получить у сетевого адми	атоматичеся противном нистратора	ки, есл случае а.	и сеть параме	тры
Получить IP-адрес автоматиче	ски			
<ul> <li>Оспользовать следующий IP-а,</li> </ul>	дрес:			
IP-адрес:	10 . 0	. 2	. 210	
Маска подсети:	255 . 25	5.25	5.0	
Основной шлюз:	10 . 0	. 2	. 1	
Получить адрес DNS-сервера а истористи и получить обращить обращи Обращить обращить об Обращить обращить обр Обращить обращить обр	втоматиче	ски		
о использовать следующие адре	eca DNS-cep	рверов		
Предпочитаемыи DNS-сервер:	· · ·		0.00	
Альтернативный DNS-сервер:		•	•	
Подтвердить параметры при н	выходе	До	полните	льно
		ОК		Отмена

 перезагрузите ВМ, авторизуйтесь с УЗ admin / P@sswOrd и убедитесь в сетевой доступности BM WS1.

C:\Windows\system32\cmd.exe	
Microsoft Windows [Version 6.1.7601] <c> Корпорация Майкрософт (Microsoft Corp.), 2009. Все права защищень</c>	. <u>^</u>
C:\Users\admin>ping 10.0.2.200	
Обмен пакетами с 10.0.2.200 по с 32 байтами данных: Ответ от 10.0.2.200: число байт=32 время=1мс TTL=128 Ответ от 10.0.2.200: число байт=32 время<1мс TTL=128 Ответ от 10.0.2.200: число байт=32 время<1мс TTL=128 Ответ от 10.0.2.200: число байт=32 время=2мс TTL=128	
Статистика Ping для 10.0.2.200: Пакетов: отправлено = 4, получено = 4, потеряно = 0 (0% потерь) Приблизительное время приема-передачи в мс: Минимальное = Омсек, Максимальное = 2 мсек, Среднее = 0 мсек	
C:\Users\admin>_	

- 2. Убедитесь, что на виртуальных машинах АР и WS1:
  - сетевые интерфейсы работают со скоростью 1 Гбит/с;
  - значение МТU 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 OC Windows (протокол SMB). Для этого сделайте следующее:
  - в окне консоли ВМ АР 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";

🔾 🗢 👤 🕨 Сеть 🕨	WS1 🕨 up	- + Touc	к: ир	
порядочить 👻 Нова	я папка			
7 Избранное	Имя	Дата изменения	Тип	Размер
〕 Загрузки	C3_debug	19.09.2018 20:04	Файл образа диска	1 669 64
Рабочий стол				
v use this clear ↓ ≪ test → d	own	<ul> <li>◄ 4<sub>7</sub> Поис</li> </ul>	e: down	
орядочить ▼ Доба	own вить в библиотеку 🔻	<ul> <li>✓ </li> <li< td=""><td>k: down ≋≕ ▼</td><td></td></li<></ul>	k: down ≋≕ ▼	
С	оwn вить в библиотеку ▼ Имя	<ul> <li>◄ ◄</li> <li>Общий доступ</li> <li></li> </ul>	к: down 8::: 🔻	П

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

📕 up				_ 🗆 ×
🕒 🗸 • Сеть •	AP + up	👻 🛃 Поиск:	up	<u> 9</u>
Упорядочить 👻 Новая	папка		8	= - 🔟 🕐
🔆 Избранное	Имя *	Дата изменения	Тип	Размер
脉 Загрузки 🔛 Недавние места 💻 Рабочий стол	c3_debug.iso	19.09.2018 20:04	Файл "ISO"	1 669 648 KB

13

🕌 down				
	down	🔻 🛃 Поис	ск: down	2
Упорядочить 🔻 Добав	ить в библиотеку 🔻	Общий доступ 🔻	Новая папка 🛛 🔠 🔻	
🔆 Избранное	Имя *		Дата изменения	Тип
脉 Загрузки 🕮 Недавние места 💻 Рабочий стол		Эта папка	пуста.	

 в окне консоли BM AP (OC Windows 7 SP1 x64) запустите процесс копирования файла с BM WS1 (OC 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);

Копирование 1 э	лем. (1,59 ГБ)	
Имя: Из: Куда: Оставшееся время: Оставшиеся элементи Скорость:	c3_debug up (C:\test\up) down Примерно 30 сек. ы: 1 (992 МБ) 26,5 МБ/сек.	

 в окне консоли BM WS1 (OC Windows Server 2008 R2 SP1 x64) запустите процесс копирования файла с BM AP (OC 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);

	AN (1 50 FE)	
Kolimpobanne 1 3/k	EM. (1,3310)	
Имя:	c3_debug.iso	
Из:	up	
Куда:	down (C: \test\down)	
Оставшееся время:	Примерно 45 сек.	
Оставшиеся элемент	ък: 1 (937 МБ)	
CKODOCTH:	25.6 M5/cex.	

- на BM WS1 и AP 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;

AP_cont39 - Virtual Machine Pro	operties	– – ×
Show All Devices	Add Remove	Device Status
Hardware	Summary	Connect at power on
Memory     CPUs     Video card     VMCI device     USB controller     SCSI controller 0	2048 MB 1 Video card Deprecated Present LSI Logic SAS	Adapter Type Current adapter: E1000 MAC Address 00:50:56:89:41:60
CD/DVD drive 1     Hard disk 1     Floppy drive 1	[datastore] win/sp1x64 Virtual Disk Client Device	Automatic Manual
Network adapter 1 (edite	Cont39_10.0.1.X	Network Connection Network label: Cont39_10.0.1.X
		OK Cancel

 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;

Свойства: Протокол Интернета веро	сии 4 (TCP/IPv4)
Общие	
Параметры IP могут назначаться а поддерживает эту возможность. В IP можно получить у сетевого адми	зтоматически, если сеть противном случае параметры нистратора.
Получить IP-адрес автоматиче	ески
<ul> <li>Оспользовать следующий IP-а</li> </ul>	дрес:
IP-адрес:	10 . 0 . 1 . 210
Маска подсети:	255.255.255.0
Основной шлюз:	10 . 0 . 1 . 1
🔵 Получить адрес DNS-сервера а	автоматически
Оспользовать следующие адр	еса DNS-серверов:
Предпочитаемый DNS-сервер:	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
Альтернативный DNS-сервер:	
🔲 Подтвердить параметры при	выходе Дополнительно
	ОК Отмена

- 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 BM 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	
<b>IP-адрес/маска</b> 10.0.1.200/255.255.255		10.0.2.200/255.255.255.255	
Тип привязки	Защищаемый	Внутренний	
Криптошлюз	КШ с ЦУСом	KSH_main	
Интерфейс	em2	em2	

		Kor	нтинент - Главн	ный адми	инистрат	гор - КШ с ЦУС	ом (10.0.1.1)			-	□×
•	Главная	Вид									^
Сетевой объект	руппа объектов	Удалить Сетевой объект	<ul> <li>Фильтр</li> <li>Фильтр</li> <li>Фильтрация и</li> </ul>	о ить поиск	Поля	Иерархия	Обновить	Свойст	гва		
Dec of	1.010711		Сетевые о	бъекть							
ble oo	БЕКТЫ	* ^	Название	Описа	ние	IP-адрес	Маска		Криптошлюз	Тип привязки	Интер
	тр управлен Сетевые об Группы сете	ния сетью ъекты евых объектов	Любой ARM WS1	Любо	3	0.0.0.0 10.0.1.200 10.0.2.200	0.0.0.0 255.255.25 255.255.25	55.255 55.255	КШ с ЦУСом KSH_main	Нет Защищаемый Внутренний	em2 em2
đ	Сервисы		10.0.1.210			10.0.1.210	255.255.25	5.255	КШ с ЦУСом	Защищаемый	em2
	Пользовате	ли	10.0.2.x			10.0.2.0	255.255.25	55.0	KSH_main	Защищаемый	em2
٢	Временные и	интервалы	Remote_vpn			10.0.0.0	255.255.25	55.248	КШ с ЦУСом	Защищаемый	Любо
	Классы трас	фика	AP			216.115.92.200	255.255.25	5.255		Нет	

 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	10010	10020
зашифрованного трафика		

		Ko	тинент -	Главный ад	министратор - КШ с Ц)	/Сом (10.0.1.1)		- 🗆 ×
	Главная В	ид			n ha sue l'ast			^
Зарадина	<b>Х</b> Удалить	Обновить	Свойств	a				
Создать	Класс трафика	Обновить	Свойства	a				
Все об	ъекты	-	х Кла	ассы траф	ика			
			Hase	зание	Описание	Приоритет шифрования	Порт	Маркиро
	Сополни се	1010	Hop	мальный		5	10000	Не мен:
- 66	сетевые объекть		Клас	Класс 10		10	10010	Не мен:
+	Группы сетевых	объектов	Клас	cc 20		20	10020	Не мен
0	Сервисы							0.00.00.00.00.00.00.00.00.00.00.00.00.0
-	Пользователи							
۲	Временные интер	валы						
	Классы трафика							
	Реакции на событ	гия						

• в области объектов управления выберите "Центр управления сетью /

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

Сервис	Общие					
Членство в группах	Название	SMB				
	Протокол	tcp				*
	Параметры г	протока	ла			
	Порт источ	ника	любой	¥		
	Порт назна	вчения	равен	σ	445	
				C	ж	Отмен

 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

Nº 🔺	Название	Отправите	Получатель	Сервисы	Д.	K	Η	Времен
1	from AP to ARM	Пюбой	ARM	http	0	=5	4	Постоя
2	from WS1 to ARM 10	10.0.2.x	10.0.1.210	Любой ІСМР	0	=s	4	Постоя
3	to WS1	Любой	WS1	Любой ТСР; Лю	0	=-		Постоя
4	from WS1	WS1	Любой	Любой ТСР; Лю	0	=-		Постоя
5	from WS1 to ARM 20	WS1	ARM	Любой ІСМР	0	=5	4	Постоя
6	from AP to WS1	Remote_vpn	10.0.2.x	Любой TCP; Лю	0	=15	4	Постоя
7	ICMP to ARM	Любой	ARM	Пюбой ІСМР	0	=5	4	Постоя
8	SMB to 10.0.1.210	WS1	10.0.1.210	SMB	0	=5	5	Постоя
9	SMB to 10.0.2.200	10.0.1.210	WS1	SMB	0	=5	4	Постоя
10	FTP to 10.0.1.200	10.0.2.x	ARM	ftp; tcp-high-ports	0	= 5	4	Постоя
11	FTP to 10.0.2.x	ARM	10.0.2.x	tcp-high-ports; ftp	0	=5	4	Постоя
12	from ARM to AP block	10.0.1.210	AP	Любой ТСР; Лю	0	=-	3	Постоя
13	from ARM to AP pass	10.0.1.210	AP	Пюбой ІСМР	0	=-		Постоя
14	from AP to ARM pass	AP	10.0.1.210	Любой ІСМР	6	=-		Постоя

- 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 АР 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";

🔍 🗣 🖡 🕨 Сеть 🕨	10.0.2.200 ▶ up	🕶 🐓 Поиск:	up	م
упорядочить ♥ Нов. ☆ Избранное В Загрузки Ш Недавние места ■ Рабочий стол	имя ear c3_debug	Дата изменения 19.09.2018 20:04	8== ♥ Тип Файл образа диска	Размер 1 669 648 1
▼ 📕 « test → d	own	<ul> <li>↓</li> <li>Поис</li> </ul>	к: down	, • •

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

葠 Корневой каталог FTP н	a 10.0.1.200 - Internet	Explorer					_ 🗆 🗙
	200/	+ ح	🙆 Корнев	ой каталог F	ГР на 1 ×		☆☆ 🕸
Корневой кат	алог FTP на	ı 10.0.1.2	:00				
Чтобы просмотреть эт команду Открыть FT	от FTP-сайт в про: <b>Р-сайт в проводн</b>	воднике, наж ике.	мите клав	ишу ALT,	щелкните	Вид, а зате	ем выберите
08/02/2019 02:06	Каталог <u>file</u> s	8					

🧉 Каталог FTP /files/ на 10.0.1.200 - Internet Explorer	
🚱 🕞 ♥ 🎑 ftp://10.0.1.200/files/ Р 🚽 🎸 💋 Каталог FTP /files/ на 10.0 ×	6 🛠 🔅
Каталог FTP /files/ на 10.0.1.200	
Чтобы просмотреть этот FTP-сайт в проводнике, нажмите клавищу ALT, щелкните <b>Вид</b> , а затк команду <b>Открыть FTP-сайт в проводнике</b> .	ем выберите
На один уровень вверх	
09/19/2018 08:09 1,649,418,240 <u>c3 release.iso</u>	

- запустите одновременно два параллельных процесса:
  - в окне консоли BM WS1 в браузере IE сохранение файла с FTPсервера (BM ARM, 10.0.1.200) в локальную папку "C:\test\down";
  - в окне консоли ВМ АР 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;

Скачано 27% из с3_	release.iso Осталось	а 4 мин 10 сек	×
		Отмена	Просмотреть загрузки
🛬 Осталось б мин.			
Копирование 1	элем. (1,59 ГБ)		
Имя: Из: Куда: Оставшееся время: Оставшиеся элемен Скорость:	c3_debug <b>up</b> down (C:\test\down) Примерно 6 мин. ты: 1 (955 МБ) 4,14 МБ/сек.		
Меньше сведени	й	Отмена	

- 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 BM 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";

• Главная	Допо Вид Состо	олнительно яние КШ/КК		Контин	ент - Главный адм	инистратор	о - КШ с ЦУ	/Сом (10.	0.1.1)	- 🗆 ×
Криптошлюз Группу Создать	🖌 Таблица сост 😋 Кр	ояний 😃 Холптошлюз	Группс	рвые ции Фил	♥ Фильтр ♥ Очистить ₩ Найти вътрация и поиск	Поля	Иерархия	Обно Обно	вить Св	ойства ойства
Все объекты	<b>▼</b> ×	Криптог	рафиче	ские шлн	03Ы	0:	TS.	15 54		
<ul> <li>Центр управлени</li> <li>Сетевые объ</li> <li>В Группы сетев</li> <li>Сервисы</li> </ul>	1я сетью екты зых объектов	Hase	ание LUYCom _main _reserve	Описание	Частный режим	Состояние Включен Включен Отключен	НСД	NAT	Multi-WAN	Каналы VF
よ Пользовател ⓒ Временные и स Классы траф 🌲 Реакции на си	и нтервалы ика обытия	• I Состоя	ание К	:Ш						• • ×
Профили уси. Профили кон Профили кон Сертификать	пенной фильтраци троля приложений ы	Статус КШ с	ы ЦУСом							^
<ul> <li>Правила фил</li> <li>База решаюц</li> <li>Виртуальные</li> <li>Администрат</li> <li>Э Сетевые устройх</li> </ul>	ьтрации цих правил коммутаторы оры ства Континент	Включ Введё Режим Время	іен: н в экспл и работы последн	іуатацию : него изме	: гнения БД ЦУС:	ДА ДА акт 02.	гивный 08.2019 1	15:58:37		
Криптошлюз	ы	Статис	тика по	о трафи	іку					
<ul> <li>Сринтокомму</li> <li>Детекторы а</li> <li>Отчёты</li> </ul>	так	Ин <sup>-</sup> BCE	герфейс ГО:	Кол-во 1415305	входящих байт 5973	Кол-во 5826836	исходящ	их байт	Кол-во 422357	входящі О
• Внешние криптог	рафические сети	ет(	, Динам	1304/82 1155/71 ич Пра	2570 15 ивила т Очеред	5826836 о ь Автор	изо Вне	ешние	2/5162 55005 Состоян	> > ии DHCP
	L							0	0 3	/6

 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);

Общие сведения			Созлать 💌	Изменить	Улалить
Интерфейсы	Физические и вир	туальные интерфейсы	COOLER	- Horiorian D	5 parrie
Управление QoS	Название	Тип	Адрес/Маска	Параметры	MTU
DHCP	<b>∬</b> ⊄em0	Внешний	216.115.92.1/24		1500
Журналы	<b>ீ</b> ∈em1	Внешний	216.115.93.1/24		1500
<sup>р</sup> езервирование	<b>ீ</b> em2	Внутренний	10.0.2.1/24 20.0.2.1/24		1500
маршругизация	<b>്</b> ലോ	Резервирование			1500
	പ്⊄em4	Не определён			1500
Альтернативные адреса Удалённый терминал Членство в группах Версия ПО					
	Изменения в	настройках интерфейсов	применяются неме,	дленно. При смене	SFP модул

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;

Свойства криптошлюза - KSH	L_main
Общие сведения Интерфейсы Управление QoS DHCP Журналы Резервирование Маршрутизация Multi-WAN DNS Связи Альтернативные адреса Удалённый терминал Членство в группах Велсия ПО	Управление перегрузками на интерфейсах СУ
араметры интерфейса en	Добавить очередь Удалить очередь Изменить ОК Отмена Применит
Полоса пропускания, Кбит	/c : 960000
	ОК Отмена
воиства криптошлюза - KSF Общие сведения	и таплания перегонаками на интерфейсах СУ Импорт Экспорт
Интерфейсы	Управление переі рузками на интерфейсах су

- 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);

обистов очереди		
Криптошлюз	KSH_main	
Интерфейс	em0	
Общая полоса пропу	искания, Кбит/с 960000	
Тип приоритизации	HFSC	
Название очереди	default	
🗹 Очередь по у	молчанию	
Классы трафика	1-	
Имя	Приоритет шифро	ования Порт
	Доб	бавить Удалить
Полоса пропускания	<u>По</u> б	бавить Удалить
Полоса пропускания realtime 10	Доб а. % linkshare 0	бавить Удалить upperlimit 15
Полоса пропускания realtime 10 Приоритет 1	ی ۱. % linkshare 0	бавить Удалить upperlimit 15
Полоса пропускания realtime 10 Приоритет 1 Защита от перегрузи	Inkshare 0	бавить Удалить upperlimit 15
Полоса пропускания realtime 10 Приоритет 1 Защита от перегруз ✓ RED [	ц, % linkshare 0 v ок RIO _ ECN	бавить Удалить upperlimit 15

- 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";

воиства очереди		>
Криптошлюз	KSH_main	
Интерфейс	em0	
Общая полоса пропу	ускания, Кбит/с 960000	)
Тип приоритизации	HFSC	
Название очереди	SMB	
Очередь по у	молчанию	
Имя	Приоритет шифр	ования Порт
Класс 10	10	10010
	Ло	бавить Удалить
Полоса пропускания realtime 20 Приоритет 2	a, % D linkshare 0	upperlimit 25
Полоса пропускания realtime 20 Приоритет 2 Защита от перегоуз	a, % D linkshare 0	upperlimit 25
Полоса пропускания realtime 20 Приоритет 2 Защита от перегруз	а, % Iinkshare 0	upperlimit 25
Полоса пропускания realtime 20 Приоритет 2 Защита от перегруз (RED) [	a, % D linkshare 0 v ok RIO ECN	upperlimit 25

- нажмите кнопку "ОК". В структуре интерфейса "em0" появится запись очереди "SMB". Аналогично создайте очередь для приоритизации FTPтрафика, 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";

фиптошлюз	KSH_main				
Інтерфейс	em0				
бщая полоса пропу	ускания, Кбит.	/c 9600	00		
ип приоритизации	HFSC				
азвание очереди	FTP				
🗌 Очередь по у	молчанию				
лассы трафика					
Имя	При	юритет шиф	рования	Порт	
Класс 20	20			1002	0
		I	Іобавить		Удалить
олоса пропускания	a, %	I	Іобавить	. 2	Удалить
олоса пропускания realtime 40	ı, %	L share 0	Іобавить up	. <u>1</u>	Удалить 50
юлоса пропускания realtime 40 риоритет 4	a, %	Lahare 0	Іобавить up	. <u>1</u>	Удалить
олоса пропускания realtime 40 риоритет 4 ащита от перегруз	а, % Iinks т	Linare 0	Іобавить up	. <u>s</u>	Удалить
Іолоса пропускания realtime 40 Іриоритет 4 ащита от перегруз ⊽ RED [	a, % links v ok RIO	L bhare 0	Іобавить up	. <u>s</u>	Удалить 50

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

Свойства криптошлюза - К	войства криптошлюза - KSH_main						
Общие сведения Интерфейсы	Управление перегрузками на интерфейсах СУ <u>И</u> мпорт <u>Экспорт</u>						
Управление QoS	— em0 (HFSC, доступная полоса 960000 Кбит/с) — default (realtime 10 %, linksbare 0 %, unperlimit 15 %, приоритет - 1) default В	=					
DHCP	- SMB (realtime 20 %, linkshare 0 %, upperlimit 25 %, приоритет - 2) RED - класс	51					
Журналы	— FTP (realtime 40 %, linkshare 0 %, upperlimit 50 %, приоритет - 4) RED - классе — em 1 (нет управления очередями)	al.					
Резервирование	em2 (нет управления очередями)						
Маршрутизация	… em3 (нет управления очередями)						
Multi-WAN	Emerte (нет управления очередями)						

- 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.

Свойства криптошлюза -	КШ с ЦУСом	
Общие сведения Интерфейсы	Управление перегрузками на интерфейсах СУ Импорт	<u>Э</u> кспорт
Управление QoS	⊡ ем0 (HFSC, доступная полоса 960000 Кбит/с)	rer - 1) default PEI
DHCP	- SMB (realtime 20 %, linkshare 0 %, upperlimit 25 %, приоритет	- 2) RED - классы
Журналы	— FTP (realtime 40 %, linkshare 0 %, upperlimit 50 %, приоритет	- 4) RED - классы
Маршрутизация	- em2 (нет управления очередями)	
Multi-WAN	em3 (нет управления очередями)	

- 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 BM WS1 в браузере IE сохранение файла с FTPсервера (BM ARM, 10.0.1.200) в локальную папку "C:\test\down";
    - в окне консоли ВМ АР 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 FTPсервера проходит существенно быстрее;
    - передача трафика по SMB-протоколу (копирование на BM AP файла из общедоступной папки с BM WS1) имеет более низкий приоритет и ограничена выделенной квотой – 20-25% от общей полосы пропускания канала;

Скачано 41% из с3_	release.iso Осталос	5 7 мин 8 сек	×
		Отмена	Просмотреть загрузки
📑 Осталось 26 мин.			
Копирование 1 з	лем. (1,59 ГБ)		
Имя: Из: Куда: Оставшееся время: Оставшиеся элемент Скорость:	c3_debug up down (C:\test\down) Примерно 26 мин. ы: 1 (1,19 ГБ) 0,99 МБ/сек.		
🔿 Меньше сведений	ň	Отмена	

- 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 BM 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).

войства криптошлюза - KSH_m	ain
Общие сведения	Импорт
Интерфейсы	управление перегрузками на интерфейсах Су
Управление QoS	— ето (HFSC, доступная полоса 960000 Кбит/с)     default (realtime 10.%, inkehare 0.%, uncertaint 15.%, приористот - 1) default PEI
DHCP	<ul> <li>SMB (realtime 20 %, linkshare 0 %, upperlimit 25 %, приоритет - 2) RED - классы</li> </ul>
Журналы	FTP (realtime 40 %, linkshare 0 %, upperlimit 50 %, приоритет - 4) RED - классы
Резервирование	····em1 (нет управления очередями) ····em2 (нет управления очередями)
Маршрутизация	····em3 (нет управления очередями)
Multi-WAN	ет (нет управления очередями)
]араметры интерфейса em0	×
Тип приоритизации:	Нет управления очередями 👻
Полоса пропускания, Кбит/с	960000
	ОК Отмена
івойства криптошлюза - KSH_m	ain
Общие сведения	Импорт Экспорт
Интерфейсы	Управление перегрузками на интерфейсах СУ
Управление QoS	- em0 (нет управления очередями)
DHCP	SMB (realtime 0 %, linkshare 0 %, upperlimit 0 %, приоритет - 2) RED - классы т
Журналы	— FTP (realtime 0 %, linkshare 0 %, upperlimit 0 %, приоритет - 4) RED - классы тр
Резервирование	···· ет цнет управления очередями) ···· ет 2 (нет управления очередями)
Маршрутизация	… em3 (нет управления очередями)
	····· em4 (нет управления очередями)

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).
- 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.

 Включите шифрование между КШ с ЦУСом и КSH\_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".

Общие сведения	🥼 Изменения в настройках связей г	применяются немедл	енно.	
1нтерфейсы /правление QoS	Свободные криптографические шлюзы	Связанные	криптографические шлюзы	
DHCP	Название	Название	Время	
Курналы		KSH_main	194 <sup>1</sup>	
Ларшрутизация		2		
Multi-WAN		>		
ONS		<[]		
Твязи		<		
льтернативные адреса				
/далённый терминал				
Аленство в группах	-	1000		
Зерсия ПО	Степень сжатия пакетов	*		
	🗌 Игнорировать флаг DF в заголовка	ах пакетов		

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

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

🗸 🗸 🖡 🕨 Сеть 🕨	10.0.2.200 ▶ up	✓ 4) Поиск:	up	<mark>×</mark> ا
Упорядочить 🔻 Нова	вя папка		i≡ •	
ጵ Избранное ᠾ Загрузки 똂 Недавние места 💻 Рабочий стол	Имя ightarrow c3_debug	Дата изменения 19.09.2018 20:04	Тип Файл образа диска	Размер 1 669 648
♥ ♥ ♥ ♥ ♥ ♥ ♥ ♥ ♥ ♥ ♥ ♥ ♥ ♥ ♥	own	<b>▼ 4</b>	ж: down	
/порядочить 🔻 Доба	вить в библиотеку 🔻	Общий доступ 🔻 🗙	• •	
👉 Избранное 〕 Загрузки 🖭 Недавние места 💻 Рабочий стол	Имя	<ul> <li>Эта папка пу-</li> </ul>	Дата изменения ста.	Тип

 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).

3:		
	up	
/да:	down (C:\test\down)	
ставшееся время:	Примерно 11 мин.	
ставшиеся элемент	ък. 1 (1,16 ГБ)	
сорость:	2,06 МБ/сек.	

- 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 BM KSH\_main, нажмите комбинацию клавиш <Alt>+<F2> и авторизуйтесь с учетной записью локального администратора kshadmin / P@ssword;

Предъявите персональный идентификатор или нажмите [ENTER] для входа по логину/паролю локального администратора...

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

1: Сведения об устройстве
2: Ключи и насители
3: Вывести списак автаризаванных пальзавателей
4: Списак превил фильтреции
5: Списак правил NAT
6: Вывести полный список интерфейсов
7: Вывести таблицы маршрутизации
8: Просмотр таблицы состояний (keep-state)
9: Диягностика
10: Перезагрузка
11: Завершение работы
0: Выход
Выберите пункт меню (0 – 11): 10
Вы уверены, что хотите перезагрузить криптошлюз (Y/N): у

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

Криптографический шлюз "Континент" Конфигурация: криптошлюз
Нажмите Enter для настройки параметров
1: Завершение работы
2: Перезагризка
3: Управление конфигурацией
4: Настройка безопасности
5: Настройка ДА <функция недоступна>
6: Настройка СД <функция недоступна>
7: Тестировение
0: Выхол
Выберите пункт меню (0 – 7): 3



 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);

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
Вые	5ерите пункт меню (0 – 4):

**Для сведения.** В настройках шифратора данная установка отображается строкой net.inet.ipcrypt.I3\_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.

1: Включени	е режима і	шифрования т	рафика н	а основ	е адреса	источника	
2: Разрешен	ие дефраг	ментации пак	етов до	пакетно	го фильт	PA	
3: Разрешен	ие распре,	деления паке	тов с уч	етом со	единений		
4: Задать ч	исло пото	ков шифровані	ия (теку	щее зна	чение – і	определяется	системой)
0: Выход							
Выберите пі	нкт меню	(0 - 4): 4					
Задайте чис	ло потоко	в шифрования	(1-32,	0 — па	умолчани	0):	

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").
- Проведите оценку скорости передачи шифрованного трафика между сетевыми узлами "Континент" в двух направлениях одновременно (два потока шифрования). Для этого:
  - переключитесь в окно консоли BM WS1 и откройте расположенную на BM AP (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";

📕 up				_	
<b>О</b> С 🕨 • Сеть •	10.0.1.210 • up	🔻 🚱 Поиск: и	p		2
Упорядочить 🔻 Новая	папка			= -	0
🔆 Избранное	Имя *	Дата изменения	Тип	Размер	
ᠾ Загрузки 强 Недавние места 💻 Рабочий стол	C3_debug.iso	19.09.2018 20:04	Файл "ISO"	1 669 648 K	Б
🕌 down				_	
	down	🔻 🛃 Поиск: d	lown		2
Упорядочить 🔻 Добав	ить в библиотеку 🔻	Общий доступ 👻 Нов	ая папка	= •	0
🔆 Избранное	Имя ^		Дата измен	ения Ти	п
🗼 Загрузки 🗐 Недавние места 📰 Рабочий стол		Эта папка пус	ra.		

- в окне консоли BM WS1 запустите копирование файла из общедоступной папки "up" на BM AP (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;

Осталось 4 мин.		>
Копирование 1 элем.	(1,59 ГБ)	
Имя: 0 Из: 4 Куда: 0 Оставшееся время: Г Оставшиеся элементы: 1 Скорость: 3	:3_debug.iso up Jown (C:\test\down) Примерно 4 мин. L (616 МБ) 8,63 МБ/сек.	
Меньше сведений		Отмена
Копирование 1 э	лем. (1,59 ГБ)	
Имя: Из: Куда: Оставшееся время: Оставшиеся элементи Скорость:	c3_debug up down (C:\test\down) Примерно 29 мин. ы: 1 (1,29 ГБ) 830 КБ/сек.	
Меньше сведений	1	Отмена

- 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 BM WS1 и в браузере IE запустите сохранение файла с FTP-сервера (BM 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;

Скачано 35% из с3_ге	elease.iso Осталось	1 мин 4 сек	×
		Отмена	Просмотреть загрузки
🛬 Осталось 20 мин.			
Копирование 1 э	лем. (1,59 ГБ)		
Имя: Из: Куда: Оставшееся время: Оставшиеся элементь Скорость:	c3_debug up down (C:\test\down) Примерно 20 мин. ы: 1 (1,28 ГБ) 1,08 МБ/сек.		
Меньше сведений	P.	Отмена	

- на BM WS1 и AP 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.I3 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.

Копирование 1 элег	ч. (1,59 ГБ)	-	
Имя: Из: Куда: Оставшееся время:	c3_debug.iso up down (C:\test\down) Примерно 3 мин и 30 сек 1 (сязка)		
Скорость:	5,11 МБ/сек.		
📩 Меньше сведений	i	Отмена	
Осталось 5 мин и 3	0 сек		
Осталось 5 мин и 3 Копирование 1	<sup>0 сек</sup> . элем. (1,59 ГБ)	• •	
Осталось 5 мин и 3 Копирование 1 Имя:	0 сек . элем. (1,59 ГБ) c3_debug		
Осталось 5 мин и 3 Копирование 1 Имя: Из:	0 сек . элем. (1,59 ГБ) c3_debug up		
Осталось 5 мин и 3 Копирование 1 Имя: Из: Куда:	0 сек . элем. (1,59 ГБ) c3_debug up down (C:\test\down)		
Осталось 5 мин и 3 Копирование 1 Имя: Из: Куда: Оставшееся время:	0 сек . элем. (1,59 ГБ) c3_debug up down (C:\test\down) Примерно 5 мин и 30 сек		
Осталось 5 мин и 3 Копирование 1 Имя: Из: Куда: Оставшиеся время: Оставшиеся элемен	0 сек . элем. (1,59 ГБ) c3_debug up down (C:\test\down) Примерно 5 мин и 30 сек нты: 1 (1,10 ГБ) 9 17 МГ (стр		
Осталось 5 мин и 3 Копирование 1 Имя: Из: Куда: Оставшееся время: Оставшиеся элемен Скорость:	0 сек . элем. (1,59 ГБ) c3_debug up down (C:\test\down) Примерно 5 мин и 30 сек нты: 1 (1,10 ГБ) 8,17 МБ/сек.		
Осталось 5 мин и 3 Копирование 1 Имя: Из: Куда: Оставшеся время: Оставшиеся элемен Скорость:	0 сек . Элем. (1,59 ГБ) c3_debug up down (C:\test\down) Примерно 5 мин и 30 сек нты: 1 (1,10 ГБ) 8,17 МБ/сек.		

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.

.качано 35% из с3_ге	elease.iso OCTAJOCE	52 Cek	
		Отмена	Просмотреть загрузки
Осталось 2 мин.		- • •	
Копирование 1 э	лем. (1,59 ГБ)		
Имя:	c3_debug		
Из:	up		
Куда:	down (C:\test\down)		
Оставшееся время:	Примерно 2 мин.		
Оставшиеся элементи	ы: 1 (1,29 ГБ)		
Скорость:	10,1 МБ/сек.		

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 BM 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");

2	VS1_cont39 - Virtual Machine F	Properties				_		×
Hard	ware Options Resources vSe	ervices			Virtua	l Machii	ne Version	: 8
	Show All Devices	Add	Remove	Device Status				
Hard	iware	Summary		• connect at power on				
	Memory CPUs Video card VMCI device USB controller SCSI controller 0 CD/DVD drive 1 Hard disk 1 Floopy drive 1	2048 MB 1 Video card Deprecated Present LSI Logic SAS Client Device Virtual Disk Client Device		Adapter Type Current adapter: MAC Address 00:50:56:89:62:6a • Automatic DirectPath I/O	E1000 Manual			
	Network adapter 1 (edite	Cont39_KK2		Status: Network Connection	Not supported	•		•
					ОК		Cancel	

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

бщие			
Тараметры IP могут назначаться а поддерживает эту возможность. В IP можно получить у сетевого адми	втоматически, ес противном случа нистратора.	ли сеть е парамет	гры
Получить IP-адрес автоматич	ески		
<ul> <li>Оспользовать следующий IP-а</li> </ul>	адрес:		
IP-адрес:	10 . 0 . 2	2.200	
Маска подсети:	255 . 255 . 25	55.0	
Основной шлюз:			
🔘 Получить адрес DNS-сервера	автоматически		
Оспользовать следующие адр	еса DNS-серверо	в:	
Предпочитаемый DNS-сервер:			
Альтернативный DNS-сервер:			
🔲 Подтвердить параметры при	выходе Д	ополните	льно

- 3. На ВМ АР сделайте следующее:
  - в настройках ВМ переподключите сетевой интерфейс к виртуальному коммутатору, к которому подключен порт коммутации криптокоммутатора КК1 (данный виртуальный коммутатор должен работать в режиме "Promiscuous mode");

lardware Options Resources VServ	vices	Virtual Machine Version: 8
Show All Devices	Add Remove	Device Status
Hardware	Summary	Connect at power on
<ul> <li>Memory</li> <li>CPUs</li> <li>Video card</li> <li>VMCI device</li> <li>USB controller</li> <li>SCSI controller 0</li> <li>CD/DVD drive 1</li> <li>Hard disk 1</li> <li>Floppy drive 1</li> <li>Network adapter 1 (edite</li> </ul>	2048 MB 1 Video card Deprecated Present LSI Logic SAS [datastore] win7sp1x64 Virtual Disk Client Device Cont39_KK1	Adapter Type         Current adapter:       E1000         MAC Address         00:50:56:89:41:60         (• Automatic       Manual         DirectPath I/O         Status:       Not supported         Network Connection         Network label:         Cont39_KK1

 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.

бщие					
Параметры IP могут назначаться а поддерживает эту возможность. В IP можно получить у сетевого адми	втоматиче противном инистратор	ски, 1 слу ра.	если чае	1 сеть парамет	ры
Получить IP-адрес автоматиче	ески				
Оспользовать следующий IP-а	адрес:				
IP-адрес:	10 .	ο.	2	. 210	
Маска подсети:	255.2	55.	255	. 0	
Основной шлюз:					
<ul> <li>Получить адрес DNS-сервера -</li> <li>Использовать следующие адр</li> <li>Предпочитаемый DNS-сервер:</li> <li>Альтернативный DNS-сервер:</li> </ul>	автоматич Deca DNS-co	ески ерве	DOB:	•	
Подтвердить параметры при	выходе	ſ	Доп	олнител	ъно.

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".

Shov	w All Devices	Add Remove	Num	ber of virtual sockets:	1	-	
Hardwar	e	Summary	Num	ber of cores per socket:	2	-	
Me CP	emory PUs deo card	1024 MB 2 Video card	Tota	al number of cores:	2		
VI     VI	ACI device BS controller CSI controller 0 D/DVD drive 1 and disk 1 oppy drive 1 etwork adapter 1 etwork adapter 2 etwork adapter 3 etwork adapter 4	Deprecated Present LSI Logic Parallel [datastore] Continent Virtual Disk Client Device Cont39_216.115.92.X Cont39_216.115.92.X Cont39_216.115.92.X	Â	Changing the number of virt OS is installed might make you unstable. The virtual CPU configuratio might violate the license of t	tual CPUs after our virtual mac In specified on the guest OS.	the guest hine this page	

	opuons   resources   1	//////////////////////////////////////	
<b>•</b>	Show All Devices	Add Remove	Number of virtual sockets:
Hard	ware	Summary	Number of cores per socket: 2
	Memory	1024 MB	
	CPUs	2	Total number of cores: 2
	Video card	Video card	
-	VMCI device	Deprecated	Changing the number of virtual CPUs after the guest OS is installed might make your virtual machine
3	USB controller	Present	unstable.
õ	SCSI controller 0	LSI Logic Parallel	
Đ,	CD/DVD drive 1	[datastore] Continent	The virtual CPU configuration specified on this page
-	Hard disk 1	Virtual Disk	might violate the license of the guest OS.
0	Floppy drive 1	Client Device	
2	Network adapter 1	Cont39_216.115.92.X	
10	Network adapter 2	Cont39_216.115.92.X	
12	Network adapter 3	Cont39_KK2	
10	Network adapter 4	Cont39_216.115.92.X	

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".

 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.

 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".

Криптаграфический коммутатор "Континент"
Канфигурация: криптакаммутатар
Нажмите Enter для настройки параметров
1: Завершение работы
2: Перезагрузка
3 <u>: Управление конфигурацией</u>
4: Настрайка безапаснасти
5: Настройка ДА <функция недоступна>
6: Настройка СД <функция недоступна>
7: Тестирование
0: Выход
Выберите пункт меню (0 – 7): З
1: Сохранение конфигурации
2: Загрузка конфигурации
3: Изменение адреса активного ЦУС
4: Настройка РРР-соединений
5: Настройка сервиса SNMP
6: Настройка шифрования
7: Настройка фрагментации
8: Настройка коммутации
9: Нестройке отледочного журнеле
10: Настройка доступа удалённого терминала
0: Выхад
Выберите пункт меню (0 – 10): 6
1: Включение режима шифравания 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)
О: Выход
Выберите пункт меню (0 – 4): О

**Для сведения.** В настройках шифратора данная установка отображается строкой: net.inet.ipcrypt.l2\_hash:0.

- **2.** Проведите оценку скорости передачи шифрованного трафика между КК1 и КК2 в одном направлении (один поток шифрования). Для этого сделайте следующее:
  - переключитесь в окно консоли ВМ АР и запустите копирование файла из общедоступной папки "up" на ВМ WS1 (10.0.2.200) в локальную папку "C:\test\down";

🗸 🗸 🖌 Сеть 🔸	10.0.2.200 ▶ up	✓ 49 Поиска	: up	× 🗉 م
Упорядочить 👻 Нова	ая папка			
ጵ Избранное 🙀 Загрузки 🗐 Недавние места 💻 Рабочий стол	Имя i c3_debug	Дата изменения 19.09.2018 20:04	Тип Файл образа диска	Размер 1 669 648
▼ 📕 « test ≯ d	own	<b>- ∮</b> Пои	ck: down	
/порядочить 🔻 Доба	вить в библиотеку 🔻	Общий доступ 🔻 🔹	» 🔠 🔻	
👉 Избранное 🚺 Загрузки 🗐 Недавние места	Имя	л Эта папка пу	Дата изменения иста.	Тип

 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;

Имя:	c3_debug	
Из:	up	
Куда:	down (C:\test\down)	
Оставшееся время:	Примерно 12 мин.	
Оставшиеся элемент	ък 1 (1,22 ГБ)	
Скорость:	2,11 МБ/сек.	

- 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 BM WS1 и откройте расположенную на BM AP (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";

Na				<u>_                                    </u>
	10.0.2.210 - up	👻 🏠 Поиск: up		2
Упорядочить 🔻 Новая	папка		: ::::	• 🔳 🔞
🜟 Избранное	Имя *	Дата изменения	Тип	Размер
) Загрузки 🧐 Недавние места 📃 Рабочий стол	C3_debug.iso	19.09.2018 20:04	Файл "ISO"	1 669 648 KB
<mark>le down</mark> ← Lest + test + te	down	🔻 🛃 Поиск: dou	wn	× □ 2
Упорядочить 👻 Добав	вить в библиотеку 🔻	Общий доступ 🔻 Новая	папка 🔠	- 🛯 🔞
🔆 Избранное	Имя *		Дата изменения	Тип
🗼 Загрузки 🗐 Недавние места 💻 Рабочий стол		Эта папка пуста		

- в окне консоли BM WS1 запустите копирование файла из общедоступной папки "up" на BM AP (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);

Осталось 27 мин.		
Копирование 1 эл	лем. (1,59 ГБ)	
Имя: Из: Куда: Оставшееся время: Оставшиеся элемен Скорость:	с3_debug.iso up down (C:\test\down) : Примерно 27 мин. ты: 1 (1,11 ГБ) 760 КБ/сек.	
Меньше сведен	ний	Отмена
Осталось 40 мин	l	
Осталось 40 мин Копирование	е 1 элем. (1,59 ГБ)	
Осталось 40 мин Копирования Имя: Из: Куда: Оставшееся врег Оставшееся эле Скорость:	а. е 1 элем. (1,59 ГБ) с3_debug ир down (C:\test\down) мя: Примерно 40 мин. менты: 1 (1,20 ГБ) 666 КБ/сек.	
Осталось 40 мин Копирования Имя: Из: Куда: Оставшееся врег Оставшиеся эле Скорость:	а. е 1 элем. (1,59 ГБ) с3_debug up down (C:\test\down) мя: Примерно 40 мин. менты: 1 (1,20 ГБ) 666 КБ/сек.	

- 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);

🕜 AP_cont39 -	Virtual Machine Pro	perties		-		$\times$
Hardware Option	s Resources VServ	vices		Virtual Mach	nine Versio	n: 8
Show All Devi	tes [	Add Remove	Device Status			
Hardware		Summary	<ul> <li>Connect at power on</li> </ul>			
Memory CPUs Video card VMCI devic SCSI contro SCSI contro CD/DVD dr Hard disk 1 Floppy driv Network ac	e Iler Iler 0 ive 1 e 1 lapter 1 <b>adding)</b>	2048 MB 1 Video card Deprecated Present LSI Logic SAS [datastore] win7sp1x64 Virtual Disk Client Device Cont39_KK1 Cont39_KK1	Adapter Type Current adapter: E1000 MAC Address Automatic C Manual DirectPath I/O Status: Network Connection Network label: Cont39_KK1			
				ок	Cance	

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

ющие Параметры IP могут назначаться аг поддерживает эту возможность. В IP можно получить у сетевого адми	втомати противн инистра	ческ ном с гора	и, лу	еслі чае	и сеть парам	етры
🔘 Получить IP-адрес автоматиче	ески					
Оспользовать следующий IP-а	адрес:					_
IP-адрес:	10	. 0	•	2	. 211	
Маска подсети:	255	. 255	ξ.	255	. 0	
Основной шлюз:						
Получить адрес DNS-сервера а	автомат	ичес	ки			
• Использовать следующие адр	eca DNS	-cep	ве	ров:		
Предпочитаемый DNS-сервер:						1
Альтернативный DNS-сервер:					2	1
Подтвердить параметры при	выходе	1	ſ	Лоп	олнит	entho

 в настройках BM WS1 добавьте дополнительный сетевой интерфейс и подключите его к виртуальному коммутатору, к которому подключен порт коммутации криптокоммутатора КК2 (на данной BM теперь тоже два интерфейса подключены к одному виртуальному коммутатору);

		Device Status
Show All Devices	Add Remove	Connected
lardware	Summary	Connect at power on
Memory CPUs Video card VMCI device USB controller SCSI controller 0 CD/DVD drive 1 Hard disk 1 Floppy drive 1 Network adapter 1	2048 MB 1 Video card Deprecated Present LSI Logic SAS Client Device Virtual Disk Client Device Cont39_KK2	Adapter Type Current adapter: E 1000 MAC Address 00:50:56:89:61:65 © Automatic © Manual DirectPath I/O Status: Not supported 3
Network adapter 2 (e	dite Cont39_KK2	Network Connection Network label: Cont39_KK2

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

втомати против	44 HC	ескі рм с	и, пу	еслі чае	и се пар	еть раметр	ы
нистра	т	opa.					
ески							
адрес:	-						
10	•	0		2	. 2	201	
255	•	255		255	4	0	
	•						
автома	ти	нес	КP	ŕ			
peca DN	IS-	сер	ве	ров			
	÷		4		4		
	2						
	атомати против нистра ески адрес: 10 255 автома автома ореса DN	атоматич противно нистрато ески адрес: — 10 . 255 .	атоматически противном си нистратора. ески адрес: 10 . 0 255 . 255 автоматичес реса DNS-сер	атоматически, противном слу інистратора. ески адрес: 10 0 0 255,255, 255,255, автоматически реса DNS-серве	атоматически, если противном случае інистратора. ески адрес: 10 . 0 . 2 255 . 255 . 255 255 . 255 автоматически реса DNS-серверов	атоматически, если со противном случае палически, если со противном случае палинистратора. ески адрес:	атоматически, если сеть противном случае параметри нистратора. ески адрес: 10 0 2 201 255 255 255 0 0 0 0 2 201 255 255 255 0 0 0 0 0 2 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0

 на КК1 и КК2 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");

1: Сохране 2: Загрузк 3: Изменен 4: Настрой 5: Настрой 6: Настрой	ние конфигурации а конфигурации ие адреса активного ЦУС ка РРР-соединений ка сервиса SNMP ка шифоования	
7: Настрой 8: Настрой	ка фрагментации ка коммутации	
9: Настрой 10: Настро 0: Выход Выберите п	ка отладочного журнала Ика доступа удалённого терминала ункт меню (0 – 10): 6	
1: Включен 2: Разреше 3: Разреше 4: Задать 0: Выход Выберите п	ие режима шифрования трафика на основе адреса источника ние дефрагментации пакетов до пакетного фильтра ние распределения пакетов с учетом соединений число потоков шифрования (текущее значение – определяется ункт меню (0 – 4): 3	системой)
1: Включен 2: Разреше 3: Запрет 4: Задать 0: Выход Выберите п	ие режимя шифравания трафика на аснове адреса источника ние дефрагментации пакетов да пакетного фильтра распределения пакетов с учетом соединений число потоков шифрования (текущее значение – определяется ункт меню (0 – 4): 0	системой)

**Для сведения.** В настройках шифратора данная установка отображается строкой net.inet.ipcrypt.l2\_hash:1.

 переключитесь в окно консоли BM WS1 и откройте расположенную на BM 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";

<u>N</u> up					_ 🗆 ×
🕞 🖓 🐺 • Сеть •	10.0.2.211 - up	🔻 🛃 Поиск: up	P.		2
Упорядочить 🔻 Новая	папка			•	
🔆 Избранное	Имя *	Дата изменения	Тип	Разме	p
🗼 Загрузки 🖳 Недавние места 🌉 Рабочий стол	C3_debug.iso	19.09.2018 20:04	Файл "ISO"	1 669	9 648 KB
🕌 down					<u>_     ×</u>
	own	👻 🚱 Поиск: do	wn		2
Упорядочить 🔻 Добави	ить в библиотеку 🔻 Об	щий доступ 🔻 Нова:	я папка		
🔆 Избранное	Имя *		Дата изменен	ния	Тип
🚺 Загрузки 🖅 Недавние места 💻 Рабочий стол		Эта папка пуста	1.		

 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";

/порядочить 🔻 Но	вая папка		833 •	· 🗇 🌘
ጵ Избранное 🙀 Загрузки 🗐 Недавние места 💻 Рабочий стол	Имя @ c3_debug	Дата изменения 19.09.2018 20:04	Тип Файл образа диска	Размер 1 669 648 К
🔍 🗢 📕 « test 🕨 a	down	<del>▼</del>   <b>4</b> 3	ck: down	
Горядочить ▼ Доб	Jown авить в библиотеку 🔻	<ul> <li>◄</li> <li>4</li> <li>Общий доступ ◄</li> </ul>	cx: down	

- в окне консоли BM AP запустите копирование файла из общедоступной папки "up" на BM WS1 (с адреса 10.0.2.201) в локальную папку "C:\test\down";
- переключитесь в окно консоли BM WS1 и также запустите копирование файла из общедоступной папки "up" на BM AP (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 МАСадресов при включенном распределении по ядрам – см. главу 1) и сравните результат с показателями, полученными в п. 3.

Осталось 15 мин.		
Копирование 1	элем. (1,59 ГБ)	
Имя:	c3_debug	
Из:	up	
Куда:	down (C:\test\down)	
Оставшееся время:	Примерно 15 мин.	
Оставшиеся элемен	нты: 1 (1,48 ГБ)	
Скорость:	2,68 МБ/сек.	
~		
Меньше сведен	ий	Отмена
Меньше сведен Осталось 7 мин и 3	ий ) сек	Отмена
Меньше сведен Осталось 7 мин и 3 Копирование 1 эле	ий ) сек м. (1,59 ГБ)	Отмена
Меньше сведен Осталось 7 мин и 3 Копирование 1 эле Имя:	ий ) сек м. <b>(1,59 ГБ)</b> c3 debug.iso	Отмена
Меньше сведен Осталось 7 мин и 30 Копирование 1 эле Имя: Из:	ий D сек м. (1,59 ГБ) c3_debug.iso up	Отмена
Меньше сведен Осталось 7 мин и 3 Копирование 1 эле Имя: Из: Куда:	ий D сек M. (1,59 ГБ) c3_debug.iso up down (C:\test\down)	Отмена
Меньше сведен Осталось 7 мин и 3 Копирование 1 эле Имя: Из: Куда: Оставшееся время:	ий D сек м. (1,59 ГБ) c3_debug.iso up down (C:\test\down) Примерно 7 мин и 30 сек	Отмена
Меньше сведен Осталось 7 мин и 3 Копирование 1 эле Имя: Из: Ставшееся время: Оставшиеся элементь	ий D сек c3_debug.iso up down (C:\test\down) Примерно 7 мин и 30 сек и: 1 (1,45 ГБ)	Отмена
Меньше сведен Осталось 7 мин и 3 Копирование 1 эле Имя: Из: Ставшееся время: Оставшиеся элементь Скорость:	ий D сек M. (1,59 ГБ) c3_debug.iso up down (C: \test\down) Примерно 7 мин и 30 сек и: 1 (1,45 ГБ) 3,13 МБ/сек.	Отмена
Меньше сведен Осталось 7 мин и 3 Копирование 1 эле Имя: Из: Ставшеся время: Оставшиеся элементь Скорость:	ий D сек M. (1,59 ГБ) c3_debug.iso up down (C:\test\down) Примерно 7 мин и 30 сек и: 1 (1,45 ГБ) 3,13 МБ/сек.	Отмена
Меньше сведен Осталось 7 мин и 3 Копирование 1 эле Имя: Из: Ставшеся время: Оставшиеся элементь Скорость:	ий D сек M. (1,59 ГБ) c3_debug.iso up down (C:\test\down) Примерно 7 мин и 30 сек и: 1 (1,45 ГБ) 3,13 МБ/сек.	Отмена

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 АР и WS1 удалите скопированный файл (<Shift>+<Del>) из локальной папки "C:\test\down".
- 6. Восстановите конфигурацию учебного стенда:
  - выключите виртуальные машины КК1 и КК2;
  - на BM 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 L3оборудования?

# 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 МАС-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</ip-пира>	показать полученные от соседа маршруты*
sh ip bgp nei <ip-пира> advertised-routes</ip-пира>	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 BM Router.



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

- В окне консоли ВМ ARM запустите обозреватель IE и подключитесь через вебинтерфейс 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".

Ís	ense	System -	Interfac	ses + Firewall + Services + VPN + Status + Diagnostics + Help +	(
WA	RNING: The	'admin' acc	ount pass	word is set to the default value. Change the password in the User Manager.	
Sy	stem /	Packag	je Man	ager / Installed Packages	0
nsta	alled Package	es Availa	able Packa	iges	
-		_			
Ins	talled Pa	ckages			
Ins	stalled Pao	ckages Category	Version	Description	Actions
Ins	Name OpenBGPD	ckages Category net	Version 0.11_10	Description OpenBGPD is a free implementation of the Border Gateway Protocol, version 4. It allows ordinary machines to be used as routers exchanging routes with other systems speaking the BGP protocol. Conflicts with Quagga_OSPF and FRR; these packages cannot be installed at the same time.	Actions
Ins	<b>Name</b> OpenBGPD	ckages Category net	Version 0.11_10	Description           OpenBGPD is a free implementation of the Border Gateway Protocol, version 4. It allows ordinary machines to be used as routers exchanging routes with other systems speaking the BGP protocol. Conflicts with Quagga_OSPF and FRR; these packages cannot be installed at the same time.           Package Dependencies:              % openbgpd-5.2.20121209_3	Actions
Ins	stalled Pao Name OpenBGPD	ckages Category net	Version 0.11_10	Description         OpenBGPD is a free implementation of the Border Gateway Protocol, version 4. It allows ordinary machines to be used as routers exchanging routes with other systems speaking the BGP protocol. Conflicts with Quagga_OSPF and FRR; these packages cannot be installed at the same time.         Package Dependencies:         Sopenbgpd-5.2.20121209_3         C = Update ✓ = Current	Actions
Ins	stalled Pao Name OpenBGPD	ckages Category net	Version 0.11_10	Description         OpenBGPD is a free implementation of the Border Gateway Protocol, version 4. It allows ordinary machines to be used as routers exchanging routes with other systems speaking the BGP protocol. Conflicts with Quagga_OSPF and FRR; these packages cannot be installed at the same time.         Package Dependencies:         So openbgpd-5.2.20121209_3	Actions ÎÎ 13 Î
Ins	atalled Pac	ckages Category net	Version 0.11_10	Description         OpenBGPD is a free implementation of the Border Gateway Protocol, version 4. It allows ordinary machines to be used as routers exchanging routes with other systems speaking the BGP protocol. Conflicts with Quagga_OSPF and FRR; these packages cannot be installed at the same time.         Package Dependencies:         Sopenbgpd-5.2.2012/209_3	Actions ÎII 13 i

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".

of sense, Syste	m + Interfaces + Firewall + Services + VPN + Status + Diagnostics + Help +
WARNING: The 'admir	' account password is set to the default value. Change the password in the User Manager.
Package / Ser	rvices: OpenBGPD / Settings
Settings Neighbors	Groups Raw config Status
General Options	
Autonomous	64500
Systems (AS) Number	Set the local autonomous system number to as-number.
Holdtime	
	Set the holdtime in seconds. The holdtime is reset to its initial value every time either a KEEPALIVE or an UPDATE message is received from the neighbor.
	If the holdtime expires the session is dropped. The default is 90 seconds. Neighboring systems negotiate the holdtime used
	when the connection is established in the OPEN messages. Each neighbor announces its configured hold- time; the smaller one is then agreed upon.
fib-update	yes 🗸
	If set to no, do not update the Forwarding Information Base a.k.a. the kernel routing table. The default is yes.
Listen on IP	
	Specify the local IP address bood(8) should listen on, or leave blank to bind to all IPs.

- 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";

General Options	
Description	ksh_net
Neighbor	216.115.92.1
	Neighbor IP address
TCP-MD5 key	
	The MD5 key to communicate with the peer. Does not work with Cisco BGP routers. If the 'Local Addr' option is not s listening IP will be used.
TCP-MD5 password	
	The MD5 password to communicate with the peer. Use this when communicating with a Cisco BGP router. If the 'Lo Addr' option is not set, listening IP will be used.
Group	
Group	Add neighbor to BGP group.
Group Neighbor Parameters	Add neighbor to BGP group.     Remote AS X   64501
Group Neighbor Parameters	Add neighbor to BGP group.       Remote AS X       Image: Constraint of the second secon
Group Neighbor Parameters	Add neighbor to BGP group.       Remote AS X       Image: Constraint of the second secon

- для сохранения настроек нажмите кнопку "Save".
- 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;

Общие сведения	Тип: Статиче	ская	-
Интерфейсы	Информация о мари	шрутах:	
Управление QoS	Адрес назначения	Маска	Следующий узел
DHCP	10.0.2.1	255.255.255.0	0.0.0.0
Журналы	20.0.2.1	255.255.255.0	0.0.0.0
Резервирование	216.115.92.1	255.255.255.0	0.0.0.0
	216.115.93.1	255.255.255.0	0.0.0.0
маршрутизация	0.0.00	0.0.0.0	216.115.92.254
DNS			
DNS Связи Альтернативные адреса Удалённый терминал Членство в группах Версия ПО	Добавить	Изменить Удалить	

1.

 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" 🞑

Свойства криптошлюза - KSH	main	×
Общие сведения	Тип: Динамическая (поддержка протоколов OSPF, RIP, BGP)	
Интерфейсы	Информация о маршрутах:	
Управление QoS		
DHCP		
Журналы		
Резервирование		F
Маршрутизация	-	
Multi-WAN	▲	
DNS	Время последнего обновления: 1 час назад	
Связи	Конфигурация zebra	
Альтернативные адреса	A	1
Удалённый терминал		
Членство в группах		F
Версия ПО		
	Протокол OSPF Протокол RIP Протокол BGP	
		F
	×	
	ОК Отмена	Применить

 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;

48



**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 кон-

фигурациях, 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.

- 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!);

of sense System	n 🕶 Interfaces 🕶	Firewall 🗕	Services -	VPN -	Status 🕶	Diagnostics -	Help -
WARNING: The 'admin'	account password is	s set to the d	efault value. (	Change th	e password	in the User Mana	ager.
Package / Ope	nBGPD / Rav	w Config	I				
Settings Neighbors	Groups Raw conf	ig Status					
OpenBGPD Config	uration File						
Raw Configuration	<pre># This file wa AS 64500 fib-update yes listen on 0.0. router-id 216. network 196.11 network 216.11 neighbor 216.1 descr remote annour local- } deny from any deny to any allow from 216.1</pre>	as created .0.0 .115.92.25 .5.92.0/24 .5.92.1/24 	by the pa	ackage m	anager. :	Do not edit!	

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

Settings Neighbors Groups Raw config Status

#### OpenBGPd Status Output

This status page includes the following information:

- OpenBGPD Summary
- OpenBGPD Interfaces
- OpenBGPD Routing
   OpenBGPD Forwarding
- OpenBGPD Network
- Openborb Network
- OpenBGPD Nexthops
- OpenBGPD IP
- OpenBGPD Neighbors

#### **OpenBGPD Summary**

Neighbor	AS	MsgRcvd	MsgSent	OutQ Up/Down	State/PrfRcvd
ksh_net	64501	12	10	0 00:03:07	4

OpenBGPD Interfaces

Interface	Nexthop state	Flags	Link state
pfsync0	invalid		invalid
pflog0	invalid		invalid
100	ok	UP	invalid
enc0	invalid		invalid
em4	ok	UP	Ethernet, active, 1000 MBit/s
em3	ok	UP	Ethernet, active, 1000 MBit/s
em2	ok	UP	Ethernet, active, 1000 MBit/s
em1	ok	UP	Ethernet, active, 1000 MBit/s
emØ	ok	UP	Ethernet, active, 1000 MBit/s

**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

бщие	Название	KSH_int
Іленство в группах	Описание	
		<ul> <li>✓ Unicast</li> <li>○ Unicast</li> </ul>
	IP-адрес / Маска	10 . 0 . 2 . 1 / 255 . 255 . 255
	Тип привязки	Внутренний 🔻
	Криптошлюз Интерфейс	KSH_main 👻
		em2 *
		Трансляция адреса внутри VPN
	Виртуальный адрес	10 . 0 . 2 . 1 / 255 . 255 . 255
	Регистрация	Определяется интерфейсом 👻

• сетевые сервисы с реквизитами согласно представленным ниже рисункам;

Сервис	Общие	Общие							
іленство в группах	Название	zebra_st	tatus				]		
	Протокол	tcp				*			
	Параметры	протокола	1						
	Порт исто	чника л	юбой	Ŧ					
	Порт назн	ачения р	авен	*	2601				
					1	OK	Отмена		

Сервис	Общие						
Членство в группах	Название	bgp_s	tatus				
	Протокол	tcp				*	
	Параметры	протоко	ла				
	Порт исто	чника	любой	•			
	Порт назн	ачения	равен	+	2605		

 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

Название	to_KSH_int			
Описание				
тправитель	<u>무무</u> WS1	•	Инверсия адреса	отправителя
Іолучатель	모모 KSH_int	•	Инверсия адреса	получателя
Сервисы				
Назван	ие Протокол Порт источника	/Тип Портн	Действие	Пропустить
bgp_sta	atus tcp любой status tcp любой	2605 2601	Временной интервал	Постоянно
**			Класс трафика	Нормальный
			Регистрация	Определяется источником/г
			Профиль усиленной фильтрации	Профиль запрещенных ресу
			Профиль контроля приложений	
				Реакции на события
•		F	Контролировать с	остояние соединений
	Добавить Удалить (	Свойства	🗌 Защита от DoS ат	ак Параметры
Отключено			Применить и заве	ршить обработку

**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

🕰 Telnet 10.0.2.1	
Hello, this is Quagga (version 1.2.3). Copyright 1996-2005 Kunihiro Ishiguro, et al.	
User Access Verification	
Password: ksh_main> ksh_main>	

• для просмотра конфигурации и таблицы маршрутов последовательно введите команды:

#### enable

show running-config

#### sh ip route

🔤 Telnet 10.0.2.1	_ 🗆 ×
ip route 0.0.0.0/0 216.115.92.254	-
in forwarding	
1	
line utu	
end	
ksh_main#	
ksh_main# sh ip route	
Codes: K - kernel route, C - connected, S - static, R - RIP,	
0 - OSPF, I - IS-IS, B - BGP, P - PIM, A - Babel, N - NHRP,	
> - selected route, * - FIB route	
S>* 0.0.0.0/0 [1/0] via 216.115.92.254. em0	
C > * 10.0.2.0/24 is directly connected. em2	
$C \ge 20.0.2.0/24$ is directly connected. em2	
C>* 127.0.0.0/8 is directly connected. lo0	
B>* 196.115.92.0/24 [20/0] via 216.115.92.254. em0. 17:46:49	
C>* 216.115.92.0/24 is directly connected. em0	
C>* 216.115.93.0/24 is directly connected, em1	
ksh_main#	
ksh_main# _	-

 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

Telnet 10.0.2.1					_ 0	×
Hello, this is Quag Copyright 1996-2005	ga (version 1.2.3). Kunihiro Ishiguro,	et al.				<b>^</b>
User Access Verifica	ation					
Password: ksh_main> ksh_main> sh ip bgp BGP table version i: Status codes: s supj i int Origin codes: i - IG	s O, local router ID pressed, d damped, h ernal, r RIB-failure GP, e - EGP, ? - inc	is 216.115.92 history, * va , S Stale, R Ro omplete	.1 lid, > ) emoved	best, :	= multipath,	
Network *> 10.0.2.0/24 *> 196.115.92.0	Next Hop 0.0.0.0 216.115.92.254	Metric LocPrf 0	Weight 32768 0	Path i 64500	i	
Displayed 2 out of ksh_main> ksh_main>	2 total prefixes					•

### sh bgp neighbors

🖬 Telnet 10.0.2.1	×
ksh_main>	-
ksh_main> sh bgp neighbors	
BGP neighbor is 216.115.92.254, remote AS 64500, local AS 64501, external link	
BGP version 4, remote router ID 216.115.92.254	
BGP state = Established, up for 17:59:52	
Last read UU:UU:11, hold time is 90, keepalive interval is 30 seconds	
Neighbor capabilities	
4 Byte AS: advertised and received	
Route refresh: advertised and received(new)	
Address family IPv4 Unicast: advertised and received	
Graceful Restart Capabilty: advertised and received	
Remote Restart timer is 90 seconds	
Address families by peer:	
IPv4 Unicast(not preserved)	
Graceful restart informations:	
End-of-RIB send: IPv4 Unicast	
End-of-RIB received: IPv4 Unicast	
Message statistics:	
lng depth is U	
Outq depth is U	
Sent Rovd	
Opens: 1 1	
More	-

sh ip bgp nei 216.115.92.254 received-routes

ksh_main# ksh main# sh ip	bgu nei 216.115.92.25	4 received-routes	
BGP table versio	n is O, local router	ID is 216.115.92.	1
origin codes: s 0	internal, r RIB-failu - IGP, e - EGP, ? - i	re, S Stale, R Rei ncomplete	na, / Dest, - Maitipath, moved
Network *> 196.115.92.0	Next Hop 216.115.92.254	Metric LocPrf	Weight Path 0 64500 i
Total number of ksh_main#	prefixes 1		

sh ip bgp nei 216.115.92.254 advertised-routes

ksh_main> sh ip BGP table versio Status codes: s i Origin codes: i	bgp nei 216.115.92. n is O, local route: suppressed, d damped internal, r RIB-fai - IGP, e - EGP, ? -	254 advertised-rou r ID is 216.115.92 l, h history, * va lure, S Stale, R R incomplete	tes .1 lid, > best, = emoved	multipath,
Network *> 10.0.2.0/24 *> 20.0.2.0/24 *> 216.115.92.0 *> 216.115.93.0 Total number of ksh_main>	Next Hop 216.115.92.1 216.115.92.1 216.115.92.1 216.115.92.1 216.115.92.1 prefixes 4	Metric LocPrf 0 1 1 1	Weight Path 32768 i 32768 ? 32768 ? 32768 ? 32768 ?	

exit

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

Общие сведения			Созлать 💌	Изменить	Улалить
1нтерфейсы	Физические и вирт	туальные интерфейсы	Соодано	, ionorano	5 garnero
правление QoS	Название	Тип	Адрес/Маска	Параметры	MTU
OHCP	<b>∬</b> ⊈em0	Внешний	216.115.92.1/24		1500
Курналы	¶≊em1	Внешний	216.115.93.1/24		1500
Резервирование Маршрутизация	<b>ி</b> em2	Внутренний	10.0.2.1/24 20.0.2.1/24		1500
	<b>്</b> ലേ3	Резервирование			1500
VIUIU-VVAN	<b>ி</b> ∝em4	Внутренний	111.111.0.1/24		1500
Альтернативные адреса /далённый терминал Аленство в группах Зерсия ПО					

- 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.

OpenBGPD	Summary
----------	---------

	Neighbor ksh_net	AS 64501	MsgRcvd 5838	MsgSent 5831	OutQ Up/Down 0 01:14:45	State/PrfRcvd 5	
--	---------------------	-------------	-----------------	-----------------	----------------------------	--------------------	--

OpenBGPD Interfaces

Interface	Nexthop state	Flags	Link state
pfsync0	invalid		invalid
pflog0	invalid		invalid
100	ok	UP	invalid
enc0	invalid		invalid
em4	ok	UP	Ethernet, active, 1000 MBit/s
em3	ok	UP	Ethernet, active, 1000 MBit/s
em2	ok	UP	Ethernet, active, 1000 MBit/s
em1	ok	UP	Ethernet, active, 1000 MBit/s
emØ	ok	UP	Ethernet, active, 1000 MBit/s

```
OpenBGPD Routing
Display 100 v of 10 items
```

Filter expression:

flags: \* = Valid, > = Selected, I = via IBGP, A = Announced, S = Stale
origin: i = IGP, e = EGP, ? = Incomplete

flags	destination	gateway	lpref	med	aspath origin
*>	10.0.2.0/24	216.115.92.1	100	0	64501 i
*>	20.0.2.0/24	216.115.92.1	100	1	64501 ?
*>	111.111.0.0/24	216.115.92.1	100	1	64501 ?
<*IA	196.115.92.0/24	0.0.0	100	0	i
*>	216.115.92.0/24	216.115.92.1	100	1	64501 ?
*>	216.115.93.0/24	216.115.92.1	100	1	64501 ?

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;

Router IP	216.115.92.254	
	Set the router ID to the given IP address, which must be loc	al to the machine.
CARP Status IP	none	
	Used to determine the CARP status. When the CARP vhid is	in BACKUP status, bgpd will not be started
Networks	196.115.92.0/24	🛍 Delete
	216.115.92.0/24	Delete
	216.115.93.0/24 ×	Delete
	Announce the specified network as belonging to our AS. If set to "(inet/inet6)connected", inet or inet6 routes to directly attached networks will be announced.	
	If set to "(inet inet6) static", all inet or inet6 static routes wil be announced.	
Add	+ Add	
Add	+ Add	

- 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";

Settings Neighbors	Groups Raw.config Status
General Options	
Description	ksh_net2 X
Neighbor	216.115.93.1 Neighbor IP address
TCP-MD5 key	The MD5 key to communicate with the peer. Does not work with Cisco BGP routers. If the 'Local Addr' option is not set, listening IP will be used.
TCP-MD5 password	The MD5 password to communicate with the peer. Use this when communicating with a Cisco BGP router. If the 'Local Addr' option is not set, listening IP will be used.
Group	Add neighbor to BGP group.
Neighbor Parameters	Remote AS X
	Announce all     Image: Constraint of the second seco
Add	+ Add
	P Save

- 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";

Groups Raw config Status		
cus_net		
196.115.92.1 Neighbor IP address		
The MD5 key to communicate with listening IP will be used.	the peer. Does not work with C	isco BGP routers. If the 'Local Addr' option is not se
The MD5 password to communicate Addr' option is not set, listening IP v	e with the peer. Use this when vill be used.	communicating with a Cisco BGP router. If the 'Loc
Add neighbor to BGP group.	~	
Remote AS X	64502	×
	Groups Raw config Status Cus_net Description Description Cus_net Description D	Groups       Raw config       Status         cus_net

• 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

Своиства криптошлюза - КСН	_mainX
Общие сведения Интерфейсы	Тип: Динамическая (поддержка протоколов OSPF, RIP, BGP) -
Управление QoS DHCP Журналы Резервирование Маршрутизация Multi-WAN	Информация о маршрутах: Подождите, происходит обновление маршрутов
DNS Связи	Обновление (26 секунд после запуска) Конфигурация zebra
Альтернативные адреса Удалённый терминал Членство в группах Версия ПО	hostname ksh_main password P@ssw0rd log stdout ip route 0.0.0.0/0 216.115.92.254
	Протокол OSPF Протокол RIP Протокол BGP password P@ssw0rd router bgp 64501 bgp router-id 216.115.92.1 network 10.0.2.0 mask 255.255.0 redistribute connected neighbor 216.115.92.254 remote-as 64500 neighbor 216.115.92.254 soft-reconfiguration inbound neighbor 216.115.93.254 soft-reconfiguration inbound
	ОК Отмена Применить

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

Свойства криптошлюза -	KSH_main		×
Общие сведения	Тип:	Динамическая (поддержка протоколов OSPF, RIP, BGP) 🔹	
Интерфейсы	Информ	ация о маршрутах:	
Управление QoS	ro	utes:	
DHCP	10.0.	2.1/24 -> 0.0.0.0	
Журналы	111.1	11.0.1/24 -> 0.0.0.0	
Резервирование	196.1	15.92.0/24 -> 216.115.92.254	
Маршрутизация	216.1	15.93.1/24 -> 0.0.0.0	
Multi-WAN	4		

 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;

Общие сведения	Тип: Статическая		*	
Интерфейсы	Информация о маршрута	EX:		
Управление QoS	Адрес назначения	Маска	Следующий узел	
DHCP	10.0.1.1	255.255.255.0	0.0.0.0	
Журналы	20.0.1.1	255.255.255.0	0.0.0.0	
Маршрутизация	196.115.92.1	255.255.255.0	0.0.0.0	
mapapymouthin	0.0.0.0	0.0.0.0	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".

Свойства криптошлюза - КШ с	ЦУСом	×
Общие сведения Интерфейсы	Тип: Динамическая (поддержка протоколов OSPF, RIP, BGP) • Информация о маршрутах:	
Управление QoS DHCP Журналы Маршрутизация Multi-WAN DNS Связи	routes: 10.0.1.1/24 -> 0.0.0.0 20.0.1.1/24 -> 0.0.0.0 196.115.92.1/24 -> 0.0.0.0 216.115.92.0/24 -> 196.115.92.254 216.115.93.0/24 -> 196.115.92.254 0.0.0.0/0 -> 196.115.92.254 Ф Время последнего обновления: 1 час назад	
Альтернативные адреса Удалённый терминал Членство в группах Версия ПО	Конфигурация zebra hostname cus password 11111111 log stdout ip route 0.0.0.0/0 196.115.92.254	
	Протокол OSPF Протокол RIP Протокол BGP hostname cus password 11111111 router bgp 64502 bgp router-id 196.115.92.1 network 10.0.1.0/24 redistribute connected neighbor 196.115.92.254 remote-as 64500 #neighbor 196.115.92.254 soft-reconfiguration inbound	
	ОК Отмена	Применить

- **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";

Syst					
The sta The ch	atic route configur anges must be ap	ation has been changed. plied for them to take effect.			🗸 Apply Chang
Gatewa	ys Static Routes	Gateway Groups			
Gatewa Statio	ys Static Routes	Gateway Groups			
Gatewa Statio	ys Static Routes c Routes Network	Gateway Groups	Interface	Description	Actions
Gatewa Statio	ys Static Routes c Routes Network 10.0.1.0/24	Gateway Groups Gateway to_10_0_1_x - 196.115.92.1	Interface WAN	Description	Actions

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

ettings Neighbors	Groups Raw config Status
OpenBGPD Confi	guration File
Raw Configuration	# This file was created by the package manager. Do not edit
	A5 64500
	fib-update ves
	listen on 0.0.0.0
	router-id 216.115.92.254
	network 196.115.92.0/24
	network 216.115.92.0/24
	network 216.115.93.0/24
	neighbor 216.115.92.1 {
	descr "ksh_net"
	remote-as 64501
	announce all
	local-address 0.0.0.0
	1
	neighbor 216.115.93.1 {
	descr "ksh_net2"
	remote-as 64501
	announce all
	local-address 0.0.0.0
	}
	neignbor 190.113.92.1 (

Settings	Neighbors	Groups	Raw config	Status	
OpenB	GPd Status	Output			
This status	page include	s the follow	wing information	on:	
• Oper	nBGPD Summ	ary			
• Oper	nBGPD Interfa	ces			
• Oper	nBGPD Routin	g			
• Oper	BGPD Forwa	rding			
• Oper	BGPD Netwo	rk			
• Oper	BGPD Nexthe	ops			
• Oper	BGPD IP				
Oper     Oper	nBGPD Interfa nBGPD Routin nBGPD Forwa nBGPD Netwo nBGPD Nextho nBGPD IP	ces g rding rk ops			

OpenBGPD Neighbors

OpenBGPD Summary

Neighbor	AS	MsgRcvd	MsgSent	OutQ	Up/Down	State/PrfRcvd
cus_net	64502	37	37	0	00:15:44	2
ksh_net2	64501	48	48	0	00:20:09	7
ksh_net	64501	102	98	0	00:20:09	5

OpenBGPD Interfaces

Interface	Nexthop state	Flags	Link state
pfsync0	invalid		invalid
pflog0	invalid		invalid
100	ok	UP	invalid
enc0	invalid		invalid
em4	ok	UP	Ethernet, active, 1000 MBit/s
em3	ok	UP	Ethernet, active, 1000 MBit/s
em2	ok	UP	Ethernet, active, 1000 MBit/s
em1	ok	UP	Ethernet, active, 1000 MBit/s

- **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 ІСМР
Действие	Пропустить
Класс трафика	"Нормальный"
Контролировать состояние соединений	Включить
Применить и завершить обработку	Включить

авило филь	трации					
Название )писание	ICMP to	ARM				
тправитель олучатель	<u>무</u> 민 10.0. 모모 ARM	2.x	• •	Инверсия адреса	отправителя получателя	
Сервисы			]	_		
Названи	ие	Протокол	Порт источника/Ти	Действие	Пропустить	
Пюбой ICMP істр		icmp		Временной интервал	Постоянно	+
				Класс трафика	Нормальны	ň –
				Регистрация	Определяет	тся источником/г 🔻
				Профиль усиленной фильтрации	Профиль за	прещенных ресу
				Профиль контроля приложений		-
					Реакци	и на события
•			Þ	🗸 Контролировать с	остояние сое	динений
	Добавит	ь Удали	ть Свойства	🗌 Защита от DoS ат	вк	Параметры
Отключено				🗸 Применить и заве	ршить обрабо	лку

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

📧 Администратор: Командная строка - ping 10.0.1.200 -t						
C:\Users\Администратор>ping 10.0.1.200 -t						
Обмен пакетами с 10.0.1.200 по с 32 байтами данных: Ответ от 10.0.1.200: число байт=32 время=3мс IIL=125						
Ответ от 10.0.1.200: число байт=32 время=9мс TTL=125 Ответ от 10.0.1.200: число байт=32 время=71мс TTL=125						

 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;

pf sense Syst	em 👻 Interfaces 👻	Firewall 🗕 S	Services 🕶 VP	'N 🕶 Status 🕶	Diagnostics 🕶	Help 🕶
WARNING: The 'admi	n' account password i	is set to the defa	ault value. Chan	ige the password	l in the User Man	ager.
Interfaces / C	)PT2 (em2)					
The changes have be	en applied successful	lly.				
General Configu	ration	_		_	_	
Enable	Enable interface	e				
Description	OPT2 Enter a description	(name) for the	interface here.			
IPv4 Configuration Type	Static IPv4			~		

 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?