Министерство образования Красноярского края

краевое государственное бюджетное профессиональное образовательное учреждение

«Красноярский колледж радиоэлектроники и информационных технологий»

**ФОНД ОЦЕНОЧНЫХ СРЕДСТВ**

для проведения текущей и промежуточной аттестации

**ПО УЧЕБНОЙ ДИСЦИПЛИНЕ МДК.01.02 Организация, принципы построения и функционирования компьютерных сетей**

для студентов специальности

09.02.06 Сетевое и системное администрирование

г. Красноярск, 2023

Фонд оценочных средств разработан на основе федерального государственного образовательного стандарта среднего профессионального образования по специальности 09.02.06 Сетевое и системное администрирование и рабочей программы МДК 01.02 Организация, принципы построения и функционирования компьютерных сетей

|  |  |
| --- | --- |
| ОДОБРЕНО  Старший методист  \_\_\_\_\_\_\_\_\_\_\_\_\_\_Т.В. Клачкова  «\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 2023г. | УТВЕРЖДАЮ  Заместитель директора  по учебной работе  \_\_\_\_\_\_\_\_\_\_\_\_М.А. Полютова  «\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_ 2023г. |

РАССМОТРЕНО

на заседании цикловой комиссии

преподавателей профессионального цикла

технического профиля

Протокол №\_\_\_ от «\_\_\_»\_\_\_\_\_\_\_\_\_\_\_ 2023 г.

Председатель ЦК \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Е.В. Харитонова

Скиляжнов А.О., преподаватель КГБПОУ «ККРИТ»

ПРОВЕРЕНО

Методист

\_\_\_\_\_\_\_\_\_\_\_\_\_\_Е.И. Макарова

«\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 2023г

|  |  |  |
| --- | --- | --- |
|  | СОДЕРЖАНИЕ |  |
|  |  | стр. |
| 1 | ПАСПОРТ ФОНДА ОЦЕНОЧНЫХ СРЕДСТВ | 4 |
| 2 | ОРГАНИЗАЦИЯ КОНТРОЛЯ И ОЦЕНКИ ОСВОЕНИЯ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ | 7 |
| 3 | КОНТРОЛЬНО-ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ | 8 |
| 4 | КОНТРОЛЬНО-ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ | 16 |
| 5 | ПЕРЕЧНЬ ПЕЧАТНЫХ ИЗДАНИЙ, ЭЛЕКТРОННЫХ ИЗДАНИЙ (ЭЛЕКТРОННЫХ РЕСУРСОВ), ДОПОЛНИТЕЛЬНЫХ ИСТОЧНИКОВ | 113 |

1. **ПАСПОРТ ФОНДА ОЦЕНОЧНЫХ СРЕДСТВ**
   1. Область применения

Фонд оценочных средств предназначен для проверки результатов освоения дисциплины МДК.01.02 Организация, принципы построения и функционирования компьютерных сетей основной профессиональной образовательной программы среднего профессионального образования по специальности 09.02.06 Сетевое и системное администрирование

Фонд оценочных средств позволяет оценить:

* + 1. Освоенные умения и усвоенные знания:

У1 Проектировать локальную сеть;

У2 Выбирать сетевые топологии;

У3 Рассчитывать основные параметры локальной сети;

У4 Читать техническую и проектную документацию по организации сегментов сети;

У5 Контролировать соответствие разрабатываемого проекта нормативно-технической документации;

У6 Настраивать стек протоколов TCP/IP и использовать встроенные утилиты операционной системы для диагностики работоспособности сети;

У7 Использовать многофункциональные приборы и программные средства мониторинга;

У8 Использовать программно-аппаратные средства технического контроля;

У9 Использовать техническую литературу и информационно-справочные системы для замены (поиска аналогов) устаревшего оборудования.

З1 Общие принципы построения сетей;

З2 Сетевые топологии;

З3 Многослойную модель OSI;

З4 Требования к компьютерным сетям;

З5 Архитектуру протоколов;

З6 Стандартизацию сетей;

З7 Этапы проектирования сетевой инфраструктуры;

З8 Требования к сетевой безопасности;

З9 Организацию работ по вводу в эксплуатацию объектов и сегментов компьютерных сетей;

З10 Системы топологического анализа защищенности компьютерной сети;

З11 Архитектуру сканера безопасности;

З12 Экспертные системы;

З13 Базовые протоколы и технологии локальных сетей;

З14 Принципы построения высокоскоростных локальных сетей;

З15 Основы проектирования локальных сетей, беспроводные локальные сети;

З16 Стандарты кабелей, основные виды коммуникационных устройств, термины, понятия, стандарты и типовые элементы структурированной кабельной системы: монтаж, тестирование;

З17 Средства тестирования и анализа;

З18 Программно-аппаратные средства технического контроля;

З19 Основы диагностики жестких дисков;

З20 Основы и порядок резервного копирования информации, RAID технологии, хранилища данных.

З21 Принципы и стандарты оформления технической документации.

З22 Принципы создания и оформления топологии сети.

З23 Информационно-справочные системы для замены (поиска) технического оборудования.

1.1.2. Освоение общих и профессиональных компетенций по учебной дисциплине:

ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам

ОК 02. Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.

ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие.

ОК 04. Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.

ОК 05. Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.

ОК 06. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей.

ОК 07. Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.

ОК 08. Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности.

ОК 09. Использовать информационные технологии в профессиональной деятельности.

ОК 10. Пользоваться профессиональной документацией на государственном и иностранном языках

ОК 11. Планировать предпринимательскую деятельность в профессиональной сфере

ПК 1.1. Выполнять проектирование кабельной структуры компьютерной сети

ПК 1.2. Осуществлять выбор технологии, инструментальных средств и средств вычислительной техники при организации процесса разработки и исследования объектов профессиональной деятельности

ПК 1.3. Обеспечивать защиту информации в сети с использованием программно-аппаратных средств.

ПК 1.4. Принимать участие в приемо-сдаточных испытаниях компьютерных сетей и сетевого оборудования различного уровня и в оценке качества и экономической эффективности сетевой топологии

ПК 1.5. Выполнять требования нормативно-технической документации, иметь опыт оформления проектной документации

Формой промежуточной аттестации в соответствии с учебным планом специальности является экзамен в 4 и экзамен в 5 семестрах.

**1.2 Система контроля и оценки освоения программы учебной дисциплины МДК 01.02 Организация, принципы построения**

**и функционирования компьютерных сетей**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Контролируемые элементы учебной дисциплины (темы) | Контролируемые знания, умения | Вид контроля | Форма контроля | Контрольно-оценочные  материалы |
| **Тема 2.1. Маршрутизация и коммутация. Масштабирование сетей** | У1, У2, У4, У5, У6, У7, У8, У9,  З1, З2, З3, З4, З5, З6, З7, З8, З9, З10, З12, З13, З15, З16, З17, З18, З19, З20, З21, З22, З23 | Текущий | Устный опрос  Проверка отчета | Задания для устного опроса (пункт 3)  Практические работы №1-36  (пункт 3) |
| **Тема 2.2. Соединение сетей** | У1, У2, У3, У4, У5, У6, У7, У8, У9,  З1, З2, З3, З4, З5, З6, З7, З8, З9, З10, З11, З12, З13, З14, З15, З16, З17, З18, З19, З20, З21, З22, З23 | Текущий | Устный опрос  Проверка отчёта | Задания для устного опроса (пункт3)  Практические работы №37-64 (пункт 3) |
| Учебная дисциплина МДК 01.02 Организация, принципы построения и функционирования компьютерных сетей | У1, У2, У3, У4, У5, У6, У7, У8, У9,  З1, З2, З3, З4, З5, З6, З7, З8, З9, З10, З11, З12, З13, З14, З15, З16, З17, З18, З19, З20, З21, З22, З23 | Промежуточный | Экзамен 4 семестр  Экзамен 5 семестр | Контрольно-оценочные материалы для промежуточной аттестации (Пункт 4). |

**2. ОРГАНИЗАЦИЯ КОНТРОЛЯ И ОЦЕНКИ ОСВОЕНИЯ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ МДК 01.02 ОРГАНИЗАЦИЯ, ПРИНЦИПЫ ПОСТРОЕНИЯ И ФУНКЦИОНИРОВАНИЯ КОМПЬЮТЕРНЫХ СЕТЕЙ**

Формой промежуточной аттестации по учебной дисциплине МДК 01.02 Организация, принципы построения и функционирования компьютерных сетей в соответствии с учебным планом специальности 09.02.06 Сетевое и системное администрирование является экзамен в 4 и 5 семестрах.

Экзаменационные материалы составляются на основе рабочей программы учебной дисциплины и охватывают ее наиболее актуальные разделы и темы. Экзаменационныематериалы должны целостно отражать объем проверяемых теоретических знаний и умений.

Перечень вопросов, тестовых и практических заданий входит в состав ФОС, являются его составной частью и доводятся до сведения студентов в течение первых двух месяцев от начала обучения.

Количество вопросов, тестовых и практических заданий в перечне должно превышать количество вопросов и практических задач, необходимых для составления экзаменационных билетов.

На основе разработанного и объявленного студентам перечня вопросов, тестовых и практических заданий, рекомендуемых для подготовки к экзамену, составляются экзаменационные билеты, содержание которых до студентов не доводится. Вопросы, тестовые и практические задания носят равноценный характер. Формулировки вопросов должны быть четкими, краткими, понятными, исключающими двойное толкование.

Условием допуска к экзамену является положительный результат в ходе текущего контроля в процессе изучения дисциплины и выполнения всех практических занятий и лабораторных работ, предусмотренных рабочей программой.

Экзамен проводится в форме устного опроса обучающегося по билету, включающему теоретические вопросы и практических заданий по МДК 01.02. Вопросы к экзамену охватывают наиболее значимые из тем, предусмотренных рабочей программой.

Критерии оценки для промежуточной аттестации:

Промежуточная аттестация предназначена для определения уровня освоения всего объема междисциплинарного курса. Для оценивания результатов обучения при проведении промежуточной аттестации используется шкала.

Основные виды систем оценивания

|  |  |
| --- | --- |
| 4-балльная | 2-балльная |
| Отлично | Зачтено |
| Хорошо |
| Удовлетворительно |
| Неудовлетворительно | Не зачтено |

Экзамен

При определении уровня достижений обучающих на экзамене обращается особое внимание на следующее:

* дан полный, развернутый ответ на поставленный вопрос;
* показана совокупность осознанных знаний об объекте, проявляющаяся в свободном оперировании понятиями, умении выделить существенные и несущественные признаки, причинно-следственные связи;
* знание об объекте демонстрируются на фоне понимания его в системе данной дисциплины и междисциплинарных связей;
* ответ формулируется в терминах дисциплины, изложен литературным языком, логичен, доказателен, демонстрирует авторскую позицию обучающегося;
* теоретические постулаты подтверждаются примерами из практики.

**3 КОНТРОЛЬНО-ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ**

Текущий контроль предназначен для проверки хода и качества формирования компетенций, стимулирования учебной работы обучаемых и совершенствования методики освоения новых знаний. Он обеспечивается проведением семинаров, оцениванием контрольных заданий, проверкой конспектов лекций, выполнением индивидуальных и творческих заданий, периодическим опросом обучающихся на занятиях.

В соответствии с рабочей программой учебной дисциплины МДК 01.02 Организация, принципы построения и функционирования компьютерных сетей представлено следующее распределение оценочных средств:

**Тема 2.1. Маршрутизация и коммутация. Масштабирование сетей**

Перечень вопросов для устного опроса.

1. Работа протокола Rapid-PVST между коммутаторами Extreme Networks и Cisco.

2. Принцип работы RSTP.

3. Состояния портов. Роли портов.

4. Дополнения к протоколу STP (EhterChannel, PortFast).

5. [Агрегирование каналов в Cisco](http://xgu.ru/wiki/%D0%90%D0%B3%D1%80%D0%B5%D0%B3%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5_%D0%BA%D0%B0%D0%BD%D0%B0%D0%BB%D0%BE%D0%B2#.D0.90.D0.B3.D1.80.D0.B5.D0.B3.D0.B8.D1.80.D0.BE.D0.B2.D0.B0.D0.BD.D0.B8.D0.B5_.D0.BA.D0.B0.D0.BD.D0.B0.D0.BB.D0.BE.D0.B2_.D0.B2_Cisco). [Терминология и настройка](http://xgu.ru/wiki/%D0%90%D0%B3%D1%80%D0%B5%D0%B3%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5_%D0%BA%D0%B0%D0%BD%D0%B0%D0%BB%D0%BE%D0%B2#.D0.A2.D0.B5.D1.80.D0.BC.D0.B8.D0.BD.D0.BE.D0.BB.D0.BE.D0.B3.D0.B8.D1.8F_.D0.B8_.D0.BD.D0.B0.D1.81.D1.82.D1.80.D0.BE.D0.B9.D0.BA.D0.B0).

6. [Общие правила настройки EtherChannel](http://xgu.ru/wiki/%D0%90%D0%B3%D1%80%D0%B5%D0%B3%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5_%D0%BA%D0%B0%D0%BD%D0%B0%D0%BB%D0%BE%D0%B2#.D0.9E.D0.B1.D1.89.D0.B8.D0.B5_.D0.BF.D1.80.D0.B0.D0.B2.D0.B8.D0.BB.D0.B0_.D0.BD.D0.B0.D1.81.D1.82.D1.80.D0.BE.D0.B9.D0.BA.D0.B8_EtherChannel).

7. [Синтаксис команды channel-group](http://xgu.ru/wiki/%D0%90%D0%B3%D1%80%D0%B5%D0%B3%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5_%D0%BA%D0%B0%D0%BD%D0%B0%D0%BB%D0%BE%D0%B2#.D0.A1.D0.B8.D0.BD.D1.82.D0.B0.D0.BA.D1.81.D0.B8.D1.81_.D0.BA.D0.BE.D0.BC.D0.B0.D0.BD.D0.B4.D1.8B_channel-group).

8. [Интерфейсы в состоянии suspended](http://xgu.ru/wiki/%D0%90%D0%B3%D1%80%D0%B5%D0%B3%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5_%D0%BA%D0%B0%D0%BD%D0%B0%D0%BB%D0%BE%D0%B2#.D0.98.D0.BD.D1.82.D0.B5.D1.80.D1.84.D0.B5.D0.B9.D1.81.D1.8B_.D0.B2_.D1.81.D0.BE.D1.81.D1.82.D0.BE.D1.8F.D0.BD.D0.B8.D0.B8_suspended).

9. [Команды просмотра информации](http://xgu.ru/wiki/%D0%90%D0%B3%D1%80%D0%B5%D0%B3%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5_%D0%BA%D0%B0%D0%BD%D0%B0%D0%BB%D0%BE%D0%B2#.D0.9A.D0.BE.D0.BC.D0.B0.D0.BD.D0.B4.D1.8B_.D0.BF.D1.80.D0.BE.D1.81.D0.BC.D0.BE.D1.82.D1.80.D0.B0_.D0.B8.D0.BD.D1.84.D0.BE.D1.80.D0.BC.D0.B0.D1.86.D0.B8.D0.B8).

10. [Настройка EtherChannel 2го уровня](http://xgu.ru/wiki/%D0%90%D0%B3%D1%80%D0%B5%D0%B3%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5_%D0%BA%D0%B0%D0%BD%D0%B0%D0%BB%D0%BE%D0%B2#.D0.9D.D0.B0.D1.81.D1.82.D1.80.D0.BE.D0.B9.D0.BA.D0.B0_EtherChannel_2.D0.B3.D0.BE_.D1.83.D1.80.D0.BE.D0.B2.D0.BD.D1.8F).

11. [Настройка статического EtherChannel 2го уровня](http://xgu.ru/wiki/%D0%90%D0%B3%D1%80%D0%B5%D0%B3%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5_%D0%BA%D0%B0%D0%BD%D0%B0%D0%BB%D0%BE%D0%B2#.D0.9D.D0.B0.D1.81.D1.82.D1.80.D0.BE.D0.B9.D0.BA.D0.B0_.D1.81.D1.82.D0.B0.D1.82.D0.B8.D1.87.D0.B5.D1.81.D0.BA.D0.BE.D0.B3.D0.BE_EtherChannel_2.D0.B3.D0.BE_.D1.83.D1.80.D0.BE.D0.B2.D0.BD.D1.8F).

12. [Standby-интерфейсы](http://xgu.ru/wiki/%D0%90%D0%B3%D1%80%D0%B5%D0%B3%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5_%D0%BA%D0%B0%D0%BD%D0%B0%D0%BB%D0%BE%D0%B2#Standby-.D0.B8.D0.BD.D1.82.D0.B5.D1.80.D1.84.D0.B5.D0.B9.D1.81.D1.8B). [Настройка EtherChannel 2го уровня с помощью PAgP](http://xgu.ru/wiki/%D0%90%D0%B3%D1%80%D0%B5%D0%B3%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5_%D0%BA%D0%B0%D0%BD%D0%B0%D0%BB%D0%BE%D0%B2#.D0.9D.D0.B0.D1.81.D1.82.D1.80.D0.BE.D0.B9.D0.BA.D0.B0_EtherChannel_2.D0.B3.D0.BE_.D1.83.D1.80.D0.BE.D0.B2.D0.BD.D1.8F_.D1.81_.D0.BF.D0.BE.D0.BC.D0.BE.D1.89.D1.8C.D1.8E_PAgP).

13. [Настройка EtherChannel 3го уровня](http://xgu.ru/wiki/%D0%90%D0%B3%D1%80%D0%B5%D0%B3%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5_%D0%BA%D0%B0%D0%BD%D0%B0%D0%BB%D0%BE%D0%B2#.D0.9D.D0.B0.D1.81.D1.82.D1.80.D0.BE.D0.B9.D0.BA.D0.B0_EtherChannel_3.D0.B3.D0.BE_.D1.83.D1.80.D0.BE.D0.B2.D0.BD.D1.8F).

14. [Настройка агрегирования каналов на маршрутизаторе](http://xgu.ru/wiki/%D0%90%D0%B3%D1%80%D0%B5%D0%B3%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5_%D0%BA%D0%B0%D0%BD%D0%B0%D0%BB%D0%BE%D0%B2#.D0.9D.D0.B0.D1.81.D1.82.D1.80.D0.BE.D0.B9.D0.BA.D0.B0_.D0.B0.D0.B3.D1.80.D0.B5.D0.B3.D0.B8.D1.80.D0.BE.D0.B2.D0.B0.D0.BD.D0.B8.D1.8F_.D0.BA.D0.B0.D0.BD.D0.B0.D0.BB.D0.BE.D0.B2_.D0.BD.D0.B0_.D0.BC.D0.B0.D1.80.D1.88.D1.80.D1.83.D1.82.D0.B8.D0.B7.D0.B0.D1.82.D0.BE.D1.80.D0.B5).

15. [Пример настройки агрегирования каналов между коммутатором и маршрутизатором](http://xgu.ru/wiki/%D0%90%D0%B3%D1%80%D0%B5%D0%B3%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5_%D0%BA%D0%B0%D0%BD%D0%B0%D0%BB%D0%BE%D0%B2#.D0.9F.D1.80.D0.B8.D0.BC.D0.B5.D1.80_.D0.BD.D0.B0.D1.81.D1.82.D1.80.D0.BE.D0.B9.D0.BA.D0.B8_.D0.B0.D0.B3.D1.80.D0.B5.D0.B3.D0.B8.D1.80.D0.BE.D0.B2.D0.B0.D0.BD.D0.B8.D1.8F_.D0.BA.D0.B0.D0.BD.D0.B0.D0.BB.D0.BE.D0.B2_.D0.BC.D0.B5.D0.B6.D0.B4.D1.83_.D0.BA.D0.BE.D0.BC.D0.BC.D1.83.D1.82.D0.B0.D1.82.D0.BE.D1.80.D0.BE.D0.BC_.D0.B8_.D0.BC.D0.B0.D1.80.D1.88.D1.80.D1.83.D1.82.D0.B8.D0.B7.D0.B0.D1.82.D0.BE.D1.80.D0.BE.D0.BC).

16. [Балансировка нагрузки](http://xgu.ru/wiki/%D0%90%D0%B3%D1%80%D0%B5%D0%B3%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5_%D0%BA%D0%B0%D0%BD%D0%B0%D0%BB%D0%BE%D0%B2#.D0.91.D0.B0.D0.BB.D0.B0.D0.BD.D1.81.D0.B8.D1.80.D0.BE.D0.B2.D0.BA.D0.B0_.D0.BD.D0.B0.D0.B3.D1.80.D1.83.D0.B7.D0.BA.D0.B8).

17. [Тестирование балансировки нагрузки](http://xgu.ru/wiki/%D0%90%D0%B3%D1%80%D0%B5%D0%B3%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5_%D0%BA%D0%B0%D0%BD%D0%B0%D0%BB%D0%BE%D0%B2#.D0.A2.D0.B5.D1.81.D1.82.D0.B8.D1.80.D0.BE.D0.B2.D0.B0.D0.BD.D0.B8.D0.B5_.D0.B1.D0.B0.D0.BB.D0.B0.D0.BD.D1.81.D0.B8.D1.80.D0.BE.D0.B2.D0.BA.D0.B8_.D0.BD.D0.B0.D0.B3.D1.80.D1.83.D0.B7.D0.BA.D0.B8).

18. [Взаимодействие Etherchannel с другими функциями](http://xgu.ru/wiki/%D0%90%D0%B3%D1%80%D0%B5%D0%B3%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5_%D0%BA%D0%B0%D0%BD%D0%B0%D0%BB%D0%BE%D0%B2#.D0.92.D0.B7.D0.B0.D0.B8.D0.BC.D0.BE.D0.B4.D0.B5.D0.B9.D1.81.D1.82.D0.B2.D0.B8.D0.B5_Etherchannel_.D1.81_.D0.B4.D1.80.D1.83.D0.B3.D0.B8.D0.BC.D0.B8_.D1.84.D1.83.D0.BD.D0.BA.D1.86.D0.B8.D1.8F.D0.BC.D0.B8).

19. [Статическое агрегирование каналов без использования протоколов](http://xgu.ru/wiki/%D0%90%D0%B3%D1%80%D0%B5%D0%B3%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5_%D0%BA%D0%B0%D0%BD%D0%B0%D0%BB%D0%BE%D0%B2#.D0.A1.D1.82.D0.B0.D1.82.D0.B8.D1.87.D0.B5.D1.81.D0.BA.D0.BE.D0.B5_.D0.B0.D0.B3.D1.80.D0.B5.D0.B3.D0.B8.D1.80.D0.BE.D0.B2.D0.B0.D0.BD.D0.B8.D0.B5_.D0.BA.D0.B0.D0.BD.D0.B0.D0.BB.D0.BE.D0.B2_.D0.B1.D0.B5.D0.B7_.D0.B8.D1.81.D0.BF.D0.BE.D0.BB.D1.8C.D0.B7.D0.BE.D0.B2.D0.B0.D0.BD.D0.B8.D1.8F_.D0.BF.D1.80.D0.BE.D1.82.D0.BE.D0.BA.D0.BE.D0.BB.D0.BE.D0.B2).

20. [Статическое агрегирование каналов с помощью LACP](http://xgu.ru/wiki/%D0%90%D0%B3%D1%80%D0%B5%D0%B3%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5_%D0%BA%D0%B0%D0%BD%D0%B0%D0%BB%D0%BE%D0%B2#.D0.A1.D1.82.D0.B0.D1.82.D0.B8.D1.87.D0.B5.D1.81.D0.BA.D0.BE.D0.B5_.D0.B0.D0.B3.D1.80.D0.B5.D0.B3.D0.B8.D1.80.D0.BE.D0.B2.D0.B0.D0.BD.D0.B8.D0.B5_.D0.BA.D0.B0.D0.BD.D0.B0.D0.BB.D0.BE.D0.B2_.D1.81_.D0.BF.D0.BE.D0.BC.D0.BE.D1.89.D1.8C.D1.8E_LACP).

21. [Динамическое агрегирование каналов с помощью LACP](http://xgu.ru/wiki/%D0%90%D0%B3%D1%80%D0%B5%D0%B3%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5_%D0%BA%D0%B0%D0%BD%D0%B0%D0%BB%D0%BE%D0%B2#.D0.94.D0.B8.D0.BD.D0.B0.D0.BC.D0.B8.D1.87.D0.B5.D1.81.D0.BA.D0.BE.D0.B5_.D0.B0.D0.B3.D1.80.D0.B5.D0.B3.D0.B8.D1.80.D0.BE.D0.B2.D0.B0.D0.BD.D0.B8.D0.B5_.D0.BA.D0.B0.D0.BD.D0.B0.D0.BB.D0.BE.D0.B2_.D1.81_.D0.BF.D0.BE.D0.BC.D0.BE.D1.89.D1.8C.D1.8E_LACP).

22. [Балансировка нагрузки](http://xgu.ru/wiki/%D0%90%D0%B3%D1%80%D0%B5%D0%B3%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5_%D0%BA%D0%B0%D0%BD%D0%B0%D0%BB%D0%BE%D0%B2#.D0.91.D0.B0.D0.BB.D0.B0.D0.BD.D1.81.D0.B8.D1.80.D0.BE.D0.B2.D0.BA.D0.B0_.D0.BD.D0.B0.D0.B3.D1.80.D1.83.D0.B7.D0.BA.D0.B8_2). [Балансировка нагрузки по MAC-адресам или IP-адресам](http://xgu.ru/wiki/%D0%90%D0%B3%D1%80%D0%B5%D0%B3%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5_%D0%BA%D0%B0%D0%BD%D0%B0%D0%BB%D0%BE%D0%B2#.D0.91.D0.B0.D0.BB.D0.B0.D0.BD.D1.81.D0.B8.D1.80.D0.BE.D0.B2.D0.BA.D0.B0_.D0.BD.D0.B0.D0.B3.D1.80.D1.83.D0.B7.D0.BA.D0.B8_.D0.BF.D0.BE_MAC-.D0.B0.D0.B4.D1.80.D0.B5.D1.81.D0.B0.D0.BC_.D0.B8.D0.BB.D0.B8_IP-.D0.B0.D0.B4.D1.80.D0.B5.D1.81.D0.B0.D0.BC).

23. [Балансировка нагрузки по портам](http://xgu.ru/wiki/%D0%90%D0%B3%D1%80%D0%B5%D0%B3%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5_%D0%BA%D0%B0%D0%BD%D0%B0%D0%BB%D0%BE%D0%B2#.D0.91.D0.B0.D0.BB.D0.B0.D0.BD.D1.81.D0.B8.D1.80.D0.BE.D0.B2.D0.BA.D0.B0_.D0.BD.D0.B0.D0.B3.D1.80.D1.83.D0.B7.D0.BA.D0.B8_.D0.BF.D0.BE_.D0.BF.D0.BE.D1.80.D1.82.D0.B0.D0.BC).

24. [Тестирование балансировки](http://xgu.ru/wiki/%D0%90%D0%B3%D1%80%D0%B5%D0%B3%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5_%D0%BA%D0%B0%D0%BD%D0%B0%D0%BB%D0%BE%D0%B2#.D0.A2.D0.B5.D1.81.D1.82.D0.B8.D1.80.D0.BE.D0.B2.D0.B0.D0.BD.D0.B8.D0.B5_.D0.B1.D0.B0.D0.BB.D0.B0.D0.BD.D1.81.D0.B8.D1.80.D0.BE.D0.B2.D0.BA.D0.B8).

25. [Просмотр информации об агрегированных каналах](http://xgu.ru/wiki/%D0%90%D0%B3%D1%80%D0%B5%D0%B3%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5_%D0%BA%D0%B0%D0%BD%D0%B0%D0%BB%D0%BE%D0%B2#.D0.9F.D1.80.D0.BE.D1.81.D0.BC.D0.BE.D1.82.D1.80_.D0.B8.D0.BD.D1.84.D0.BE.D1.80.D0.BC.D0.B0.D1.86.D0.B8.D0.B8_.D0.BE.D0.B1_.D0.B0.D0.B3.D1.80.D0.B5.D0.B3.D0.B8.D1.80.D0.BE.D0.B2.D0.B0.D0.BD.D0.BD.D1.8B.D1.85_.D0.BA.D0.B0.D0.BD.D0.B0.D0.BB.D0.B0.D1.85).

26. [Взаимодействие с другими функциями](http://xgu.ru/wiki/%D0%90%D0%B3%D1%80%D0%B5%D0%B3%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5_%D0%BA%D0%B0%D0%BD%D0%B0%D0%BB%D0%BE%D0%B2#.D0.92.D0.B7.D0.B0.D0.B8.D0.BC.D0.BE.D0.B4.D0.B5.D0.B9.D1.81.D1.82.D0.B2.D0.B8.D0.B5_.D1.81_.D0.B4.D1.80.D1.83.D0.B3.D0.B8.D0.BC.D0.B8_.D1.84.D1.83.D0.BD.D0.BA.D1.86.D0.B8.D1.8F.D0.BC.D0.B8) [Spanning-Tree](http://xgu.ru/wiki/%D0%90%D0%B3%D1%80%D0%B5%D0%B3%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5_%D0%BA%D0%B0%D0%BD%D0%B0%D0%BB%D0%BE%D0%B2#Spanning-Tree), [VLAN](http://xgu.ru/wiki/%D0%90%D0%B3%D1%80%D0%B5%D0%B3%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5_%D0%BA%D0%B0%D0%BD%D0%B0%D0%BB%D0%BE%D0%B2#VLAN), [Port Security](http://xgu.ru/wiki/%D0%90%D0%B3%D1%80%D0%B5%D0%B3%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5_%D0%BA%D0%B0%D0%BD%D0%B0%D0%BB%D0%BE%D0%B2#Port_Security).

27. [ISC-интерфейс](http://xgu.ru/wiki/%D0%90%D0%B3%D1%80%D0%B5%D0%B3%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5_%D0%BA%D0%B0%D0%BD%D0%B0%D0%BB%D0%BE%D0%B2#ISC-.D0.B8.D0.BD.D1.82.D0.B5.D1.80.D1.84.D0.B5.D0.B9.D1.81).

28. [Keepalive-интерфейс](http://xgu.ru/wiki/%D0%90%D0%B3%D1%80%D0%B5%D0%B3%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5_%D0%BA%D0%B0%D0%BD%D0%B0%D0%BB%D0%BE%D0%B2#Keepalive-.D0.B8.D0.BD.D1.82.D0.B5.D1.80.D1.84.D0.B5.D0.B9.D1.81).

29. [Передача трафика через распределенный транк](http://xgu.ru/wiki/%D0%90%D0%B3%D1%80%D0%B5%D0%B3%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5_%D0%BA%D0%B0%D0%BD%D0%B0%D0%BB%D0%BE%D0%B2#.D0.9F.D0.B5.D1.80.D0.B5.D0.B4.D0.B0.D1.87.D0.B0_.D1.82.D1.80.D0.B0.D1.84.D0.B8.D0.BA.D0.B0_.D1.87.D0.B5.D1.80.D0.B5.D0.B7_.D1.80.D0.B0.D1.81.D0.BF.D1.80.D0.B5.D0.B4.D0.B5.D0.BB.D0.B5.D0.BD.D0.BD.D1.8B.D0.B9_.D1.82.D1.80.D0.B0.D0.BD.D0.BA).

30. [Настройка распределенного агрегирования](http://xgu.ru/wiki/%D0%90%D0%B3%D1%80%D0%B5%D0%B3%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5_%D0%BA%D0%B0%D0%BD%D0%B0%D0%BB%D0%BE%D0%B2#.D0.9D.D0.B0.D1.81.D1.82.D1.80.D0.BE.D0.B9.D0.BA.D0.B0_.D1.80.D0.B0.D1.81.D0.BF.D1.80.D0.B5.D0.B4.D0.B5.D0.BB.D0.B5.D0.BD.D0.BD.D0.BE.D0.B3.D0.BE_.D0.B0.D0.B3.D1.80.D0.B5.D0.B3.D0.B8.D1.80.D0.BE.D0.B2.D0.B0.D0.BD.D0.B8.D1.8F). [Просмотр информации](http://xgu.ru/wiki/%D0%90%D0%B3%D1%80%D0%B5%D0%B3%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5_%D0%BA%D0%B0%D0%BD%D0%B0%D0%BB%D0%BE%D0%B2#.D0.9F.D1.80.D0.BE.D1.81.D0.BC.D0.BE.D1.82.D1.80_.D0.B8.D0.BD.D1.84.D0.BE.D1.80.D0.BC.D0.B0.D1.86.D0.B8.D0.B8_5). [Проверка согласованности настроек](http://xgu.ru/wiki/%D0%90%D0%B3%D1%80%D0%B5%D0%B3%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5_%D0%BA%D0%B0%D0%BD%D0%B0%D0%BB%D0%BE%D0%B2#.D0.9F.D1.80.D0.BE.D0.B2.D0.B5.D1.80.D0.BA.D0.B0_.D1.81.D0.BE.D0.B3.D0.BB.D0.B0.D1.81.D0.BE.D0.B2.D0.B0.D0.BD.D0.BD.D0.BE.D1.81.D1.82.D0.B8_.D0.BD.D0.B0.D1.81.D1.82.D1.80.D0.BE.D0.B5.D0.BA).

31. [Распределенное агрегирование и маршрутизация](http://xgu.ru/wiki/%D0%90%D0%B3%D1%80%D0%B5%D0%B3%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5_%D0%BA%D0%B0%D0%BD%D0%B0%D0%BB%D0%BE%D0%B2#.D0.A0.D0.B0.D1.81.D0.BF.D1.80.D0.B5.D0.B4.D0.B5.D0.BB.D0.B5.D0.BD.D0.BD.D0.BE.D0.B5_.D0.B0.D0.B3.D1.80.D0.B5.D0.B3.D0.B8.D1.80.D0.BE.D0.B2.D0.B0.D0.BD.D0.B8.D0.B5_.D0.B8_.D0.BC.D0.B0.D1.80.D1.88.D1.80.D1.83.D1.82.D0.B8.D0.B7.D0.B0.D1.86.D0.B8.D1.8F).

32. Протоколы динамической маршрутизации – назначение, принципы работы и история развития.

33. Сравнение динамической и статической маршрутизации.

34. Принципы работы протоколов маршрутизации: пуск после включения питания, сетевое обнаружение, обмен данными маршрутизации, обеспечение сходимости.

35. Классификация протоколов маршрутизации.

36. Дистанционно-векторный протокол RIP.

37. Дистанционно-векторный протокол IGRP.

38. Протокол маршрутизации по состоянию канала OSPF.

39. Протокол маршрутизации по состоянию канала IS-IS.

40. Классовые и бесклассовые протоколы маршрутизации.

41. Характеристики и метрики протоколов.

42. Дистанционно-векторный алгоритм.

43. Механизмы отправки и получения данных маршрутизации, расчёта оптимальных путей и добавления маршрутов в таблицу маршрутизации, обнаружения и реагирования на изменения в топологии.

44. Настройка протокола RIP: включение RIPv2, отключение автоматического объединения, настройка пассивных интерфейсов, передача маршрута по умолчанию по сети.

45. Настройка протокола RIPng.

46. Процесс маршрутизации по состоянию канала. Hello протокол. пакет состояния канала (LSP).

47. Лавинная рассылка пакетов состояния канала.

48. Лавинная рассылка пакетов состояния канала.

49. Создание дерева кратчайших путей SPF.

50. Добавление маршрутов OSPF в таблицу маршрутизации.

51. Недостатки протоколов маршрутизации по состоянию канала.

52. Таблица маршрутизации. Записи с прямым подключением и удалённой сети.

53. Динамически получаемые маршруты IPv4/6.

54. Процесс поиска маршрута.

55. Семейство протоколов OSPF. Характеристики, принципы работы и компоненты OSPF.

56. Особенности OSPF для одной и нескольких областей.

57. Магистральная область. Инкапсуляция сообщений OSPF.

58. Типы пакетов OSPF: пакет приветствия (hello), пакет описания базы данных (DBD), пакет запроса состояния канала (LSR), пакет обновления состояния канала (LSU). пакет подтверждения состояния канала (LSAck). Обновления состояния канала.

59. Рабочие состояния OSPF. Выделенный (DR) и резервный выделенный маршрутизатор (BDR).

60. Синхронизация баз данных OSPF.

61. Настройка OSPFv2 для одной области. Режим конфигурации идентификаторы маршрутизатора.

62. Использование интерфейса loopback.

63. Включение OSPF на интерфейсах. Шаблонная маска. Команда «network».

64. Настройка пассивных интерфейсов. Формула расчёта метрики стоимости OSPF.

65. Настройка значений пропускной способности интерфейса.

66. Проверка соседних устройств, настроек протокола, данных процесса и других характеристик OSPF.

67. Сравнение OSPFv2 и OSPFv3.

68. Адреса типа link-local. Топология сети OSPFv3.

69. Настройка идентификатора маршрутизатора OSPFv3. Включение OSPFv3 на интерфейсах.

70. Списки контроля доступа (ACL). Принцип работы ACL списков.

71. Типы ACL-списков Cisco для IPv4.

72. Присваивание номеров и имён ACL-спискам.

73. Расчёт шаблонной маски в ACL-списках.

74. Рекомендации по созданию и размещению ACL-списков.

75. Защита портов VTY с помощью стандартного ACL-списка IPv4.

76. Структура и настройка расширенных ACL-списков для IPv4.

77. Фильтрация трафика с использованием расширенных ACL-списков.

78. Поиск и устранение неполадок ACL-списков.

79. Распространённые ошибки ACL-списков.

80. Сравнение ACL-списков для IPv4 и IPv6.

81. Настройка и проверка ACL-списков для IPv6.

82. Протокол DHCPv4: базовая операция, формат сообщений, сообщения обнаружения и предложения.

83. Настройка, проверка и ретрансляция простого DHCPv4-сервера.

84. Настройка маршрутизатора в качестве DHCPv4-клиента.

85. Настройка маршрутизатора класса SOHO.

86. Поиск и устранение неполадок в работе маршрутизатора DHCPv4.

87. Автоматическая настройка адреса без отслеживания состояния (SLAAC).

88. Принцип работы SLAAC с DHCPv6.

89. DHCPv6 с и без отслеживания состояния. Процессы DHCPv6.

90. Настройка маршрутизатора в качестве DHCPv6-сервера и DHCPv6-клиента.

91. Поиск и устранение неполадок в работе DHCPv6.

92. Преобразование сетевых адресов IPv4. Концептуальное преобразование сетевых адресов (NAT).

93. Терминология и принципы работы NAT.

94. Пространство частных IPv4-адресов.

95. Статическое и динамическое преобразование сетевых адресов (NAT).

96. Преобразование адресов портов (PAT).

97. Сравнение NAT и PAT.

98. Анализ статического преобразования NAT.

99. Принцип работы динамического NAT.

100. Настройка и проверка NAT, PAT. Переадресация портов.

101. Настройка NAT и протокола IPv6.

102. Поиск и устранение неполадок в работе NAT.

103. Реализация проекта сети. Проект иерархической сети.

104. Расширение сети. Выбор сетевых устройств.

105. Коммутационное оборудование. Маршрутизаторы. Управляющие устройства.

106. Понятия протокола spanning-tree. Предназначение протокола spanning-tree.

107. Принцип работы STP.

108. Типы протоколов STP.

109. Настройка протокола STP.

110. Настройка PVST+.

111. Настройка Rapid PVST+.

112. Проблемы настройки STP.

113. Беспроводные локальные сети

114. Концепции беспроводной связи. Введение в беспроводную связь.

115. Компоненты сетей WLAN. Топологии сетей WLAN 802.11.

116. Принципы работы беспроводной локальной сети.

117. Структура кадра 802.11. Функционирование беспроводной связи. Управление каналами.

118. Угрозы для сетей WLAN. Обеспечение безопасности WLAN.

119. Настройка беспроводных локальных сетей. Настройка беспроводного маршрутизатора.

120. Настройка беспроводных клиентов. Поиск и устранение неполадок в работе сетей WLAN.

121. Расширенные параметры протокола OSPF для одной области. Маршрутизация на уровнях распределения и ядра. OSPF в сетях с множественным доступом.

122. Распространение маршрута по умолчанию. Точная настройка интерфейсов OSPF. Защита OSPF.

123. Составляющие процедуры поиска и устранения неполадок в работе OSPF для одной области.

124. Настройка OSPF для нескольких областей. Объединение маршрутов OSPF. Проверка OSPF для нескольких областей.

125. [Основные версии протокола](https://www.cisco.com/c/ru_ru/support/docs/ip/enhanced-interior-gateway-routing-protocol-eigrp/16406-eigrp-toc.html#anc2). [Теоретические сведения](https://www.cisco.com/c/ru_ru/support/docs/ip/enhanced-interior-gateway-routing-protocol-eigrp/16406-eigrp-toc.html#anc3). [Обнаружение и обслуживание соседей](https://www.cisco.com/c/ru_ru/support/docs/ip/enhanced-interior-gateway-routing-protocol-eigrp/16406-eigrp-toc.html#anc4). [Создание таблицы топологии](https://www.cisco.com/c/ru_ru/support/docs/ip/enhanced-interior-gateway-routing-protocol-eigrp/16406-eigrp-toc.html#anc5). [Метрика протокола EIGRP](https://www.cisco.com/c/ru_ru/support/docs/ip/enhanced-interior-gateway-routing-protocol-eigrp/16406-eigrp-toc.html#anc6).

126. [Возможное расстояние, фактическое расстояние и возможный следующий элемент](https://www.cisco.com/c/ru_ru/support/docs/ip/enhanced-interior-gateway-routing-protocol-eigrp/16406-eigrp-toc.html#anc7). [Определение беспетлевого пути](https://www.cisco.com/c/ru_ru/support/docs/ip/enhanced-interior-gateway-routing-protocol-eigrp/16406-eigrp-toc.html#anc8) [EIGRP](https://www.cisco.com/c/ru_ru/support/docs/ip/enhanced-interior-gateway-routing-protocol-eigrp/16406-eigrp-toc.html#anc6).

127. [Расщепление горизонта и обратное исправление](https://www.cisco.com/c/ru_ru/support/docs/ip/enhanced-interior-gateway-routing-protocol-eigrp/16406-eigrp-toc.html#anc9). [Режим запуска](https://www.cisco.com/c/ru_ru/support/docs/ip/enhanced-interior-gateway-routing-protocol-eigrp/16406-eigrp-toc.html#anc10). [Изменение таблицы топологии](https://www.cisco.com/c/ru_ru/support/docs/ip/enhanced-interior-gateway-routing-protocol-eigrp/16406-eigrp-toc.html#anc11). [Запросы](https://www.cisco.com/c/ru_ru/support/docs/ip/enhanced-interior-gateway-routing-protocol-eigrp/16406-eigrp-toc.html#anc12) [EIGRP](https://www.cisco.com/c/ru_ru/support/docs/ip/enhanced-interior-gateway-routing-protocol-eigrp/16406-eigrp-toc.html#anc6).

128. [Перераспределение между двумя автономными системами EIGRP](https://www.cisco.com/c/ru_ru/support/docs/ip/enhanced-interior-gateway-routing-protocol-eigrp/16406-eigrp-toc.html#anc16). [Перераспределение между EIGRP и IGRP в двух разных автономных системах](https://www.cisco.com/c/ru_ru/support/docs/ip/enhanced-interior-gateway-routing-protocol-eigrp/16406-eigrp-toc.html#anc17)

129. [Перераспределение между EIGRP и IGRP в одной автономной системе](https://www.cisco.com/c/ru_ru/support/docs/ip/enhanced-interior-gateway-routing-protocol-eigrp/16406-eigrp-toc.html#anc21). [Двустороннее перераспределение для других протоколов](https://www.cisco.com/c/ru_ru/support/docs/ip/enhanced-interior-gateway-routing-protocol-eigrp/16406-eigrp-toc.html#anc25). [Перераспределение статических маршрутов к интерфейсам](https://www.cisco.com/c/ru_ru/support/docs/ip/enhanced-interior-gateway-routing-protocol-eigrp/16406-eigrp-toc.html#anc26).

130. [Устранение неполадок маршрутов SIA](https://www.cisco.com/c/ru_ru/support/docs/ip/enhanced-interior-gateway-routing-protocol-eigrp/16406-eigrp-toc.html#anc14). [Перераспределение между двумя автономными системами EIGRP](https://www.cisco.com/c/ru_ru/support/docs/ip/enhanced-interior-gateway-routing-protocol-eigrp/16406-eigrp-toc.html#anc16). [Перераспределение между EIGRP и IGRP в двух разных автономных системах](https://www.cisco.com/c/ru_ru/support/docs/ip/enhanced-interior-gateway-routing-protocol-eigrp/16406-eigrp-toc.html#anc17)

131. [Группы сторон BGP](https://www.cisco.com/c/ru_ru/support/docs/ip/border-gateway-protocol-bgp/13755-29.html#bgppgrp). [Требования к группам сторон](https://www.cisco.com/c/ru_ru/support/docs/ip/border-gateway-protocol-bgp/13755-29.html#pgrpreqs). [Ограничения для групп сторон](https://www.cisco.com/c/ru_ru/support/docs/ip/border-gateway-protocol-bgp/13755-29.html#pgrplimits). [Использование групп сторон](https://www.cisco.com/c/ru_ru/support/docs/ip/border-gateway-protocol-bgp/13755-29.html#usepgrp).

132. [Формат сообщения](https://ru.wikipedia.org/wiki/Border_Gateway_Protocol#%D0%A4%D0%BE%D1%80%D0%BC%D0%B0%D1%82_%D1%81%D0%BE%D0%BE%D0%B1%D1%89%D0%B5%D0%BD%D0%B8%D1%8F). [Обновление информации](https://ru.wikipedia.org/wiki/Border_Gateway_Protocol#%D0%9E%D0%B1%D0%BD%D0%BE%D0%B2%D0%BB%D0%B5%D0%BD%D0%B8%D0%B5_%D0%B8%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%B8). [Сохранение соединения](https://ru.wikipedia.org/wiki/Border_Gateway_Protocol#%D0%A1%D0%BE%D1%85%D1%80%D0%B0%D0%BD%D0%B5%D0%BD%D0%B8%D0%B5_%D1%81%D0%BE%D0%B5%D0%B4%D0%B8%D0%BD%D0%B5%D0%BD%D0%B8%D1%8F). [Оповещение](https://ru.wikipedia.org/wiki/Border_Gateway_Protocol#%D0%9E%D0%BF%D0%BE%D0%B2%D0%B5%D1%89%D0%B5%D0%BD%D0%B8%D0%B5). [Используемые компоненты](https://www.cisco.com/c/ru_ru/support/docs/ip/border-gateway-protocol-bgp/13755-29.html#hw). [Условные обозначения](https://www.cisco.com/c/ru_ru/support/docs/ip/border-gateway-protocol-bgp/13755-29.html#conv)

133. [Устранение проблем с перегрузкой CPU, вызываемой процессом сканера или маршрутизатора BGP](https://www.cisco.com/en/US/tech/tk365/technologies_tech_note09186a00809d16f0.shtml). [Обеспечение оптимальной маршрутизации и сокращение объема памяти, используемой протоколом BGP](https://www.cisco.com/en/US/tech/tk365/technologies_tech_note09186a0080094a83.shtml).

134. [Отличие от HTTP](https://ru.wikipedia.org/wiki/FTP#%D0%9E%D1%82%D0%BB%D0%B8%D1%87%D0%B8%D0%B5_%D0%BE%D1%82_HTTP). [Соединение и передача данных](https://ru.wikipedia.org/wiki/FTP#%D0%A1%D0%BE%D0%B5%D0%B4%D0%B8%D0%BD%D0%B5%D0%BD%D0%B8%D0%B5_%D0%B8_%D0%BF%D0%B5%D1%80%D0%B5%D0%B4%D0%B0%D1%87%D0%B0_%D0%B4%D0%B0%D0%BD%D0%BD%D1%8B%D1%85). [Аутентификация](https://ru.wikipedia.org/wiki/FTP#%D0%90%D1%83%D1%82%D0%B5%D0%BD%D1%82%D0%B8%D1%84%D0%B8%D0%BA%D0%B0%D1%86%D0%B8%D1%8F). [FTP-ALG](https://ru.wikipedia.org/wiki/FTP#FTP-ALG). [NAT и обход брандмауэров](https://ru.wikipedia.org/wiki/FTP#NAT_%D0%B8_%D0%BE%D0%B1%D1%85%D0%BE%D0%B4_%D0%B1%D1%80%D0%B0%D0%BD%D0%B4%D0%BC%D0%B0%D1%83%D1%8D%D1%80%D0%BE%D0%B2). [Безопасный FTP](https://ru.wikipedia.org/wiki/FTP#%D0%91%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D1%8B%D0%B9_FTP). [FTPS](https://ru.wikipedia.org/wiki/FTP#FTPS). [SFTP](https://ru.wikipedia.org/wiki/FTP#SFTP). [Основные команды](https://ru.wikipedia.org/wiki/FTP#%D0%9E%D1%81%D0%BD%D0%BE%D0%B2%D0%BD%D1%8B%D0%B5_%D0%BA%D0%BE%D0%BC%D0%B0%D0%BD%D0%B4%D1%8B). [Коды ответов FTP](https://ru.wikipedia.org/wiki/FTP#%D0%9A%D0%BE%D0%B4%D1%8B_%D0%BE%D1%82%D0%B2%D0%B5%D1%82%D0%BE%D0%B2_FTP).

135. [Протокол IS-IS: объединение плоскости состояния и вектора пути](https://wiki.merionet.ru/seti/72/protokol-is-is-obedinenie-ploskosti-sostoyaniya-i-vektora-puti/). Сравнение с OSPF. Метрики IS-IS. Маршрутизация IS-IS.

136. Диагностика жестких дисков и восстановление данных. Диагностика. [Визуальный осмотр](https://habr.com/ru/post/476734/#1). [Тестовый запуск](https://habr.com/ru/post/476734/#2). [Подготовка к тестированию](https://habr.com/ru/post/476734/#3). [Тестирование](https://habr.com/ru/post/476734/#4). [Посекторная копия](https://habr.com/ru/post/476734/#5).

137. Диагностика данных. Методы восстановления данных. [Типовые случаи и рекомендуемые действия](https://habr.com/ru/post/476734/#7).  [Проверка целостности файлов](https://habr.com/ru/post/476734/#8). [Частые ошибки пользователей](https://habr.com/ru/post/476734/#9).

138. Уровни RAID. Преимущества и недостатки основных уровней RAID.

139. Архитектура хранилищ данных: традиционная и облачная.

140. Основные понятия и определения экспертных систем.

141. Этапы проектирования сетевой инфраструктуры.

142. Обоснование проектирования ЛВС. Подготовка к проектированию ЛВС. Топология сети.

143. Этапы проектирования ЛВС. Программы для проектирования ЛВС.

144. Средства тестирования и анализа.

146. Инструменты мониторинга и анализа сети.

147. Классификация средств мониторинга и анализа.

148. Встроенные средства мониторинга и анализа сетей.

**Тема 2.2. Соединение сетей**

Перечень вопросов для устного опроса.

1. [Цель создания глобальных сетей](https://static-course-assets.s3.amazonaws.com/CN503/ru/index.html#2.1.1).

2. [Принцип работы глобальной сети](https://static-course-assets.s3.amazonaws.com/CN503/ru/index.html#2.1.2).

3. В[ыбор технологии глобальной сети](https://static-course-assets.s3.amazonaws.com/CN503/ru/index.html#2.2)

4. [Инфраструктуры частных глобальных сетей](https://static-course-assets.s3.amazonaws.com/CN503/ru/index.html#2.2.2).

5. [Инфраструктура общедоступной глобальной сети](https://static-course-assets.s3.amazonaws.com/CN503/ru/index.html#2.2.3).

6. [Выбор сервисов глобальной сети](https://static-course-assets.s3.amazonaws.com/CN503/ru/index.html#2.2.4).

7. [Обзор последовательного соединения «точка-точка»](https://static-course-assets.s3.amazonaws.com/CN503/ru/index.html#3.1).

8. [Связь по последовательному каналу](https://static-course-assets.s3.amazonaws.com/CN503/ru/index.html#3.1.1).

9. [Инкапсуляция HDLC](https://static-course-assets.s3.amazonaws.com/CN503/ru/index.html#3.1.2).

10. Стандарты WAN. Общепринятая терминология глобальных сетей.

11. Устройства глобальной сети. Последовательная связь.

12. Сеть с коммутацией каналов.

13. Сеть с коммутацией пакетов. SDH, SONET и DWDM

14. Варианты коммутации каналов.

15. Варианты сети с коммутацией пакетов.

16. WAN на основе Ethernet.

17. WAN на основе MPLS.

18. [Преимущества протокола PPP](https://static-course-assets.s3.amazonaws.com/CN503/ru/index.html#3.2.1). [LCP и NCP](https://static-course-assets.s3.amazonaws.com/CN503/ru/index.html#3.2.2).

19. [Сеансы PPP](https://static-course-assets.s3.amazonaws.com/CN503/ru/index.html#3.2.3).

43. [Настройка протокола PPP](https://static-course-assets.s3.amazonaws.com/CN503/ru/index.html#3.3.1).

44. [Аутентификация PPP](https://static-course-assets.s3.amazonaws.com/CN503/ru/index.html#3.3.2).

45. [Отладка соединений WAN](https://static-course-assets.s3.amazonaws.com/CN503/ru/index.html#3.4). [Отладка PPP](https://static-course-assets.s3.amazonaws.com/CN503/ru/index.html#3.4.1).

46. Решения широкополосного доступа.

47. [Удалённая работа](https://static-course-assets.s3.amazonaws.com/CN503/ru/index.html#6.1). [Преимущества удалённой работы](https://static-course-assets.s3.amazonaws.com/CN503/ru/index.html#6.1.1).

48. [Бизнес-требования для удалённых работников](https://static-course-assets.s3.amazonaws.com/CN503/ru/index.html#6.1.2).

50. [Сравнение решений широкополосного доступа](https://static-course-assets.s3.amazonaws.com/CN503/ru/index.html#6.2)

51. [Беспроводные широкополосные сети](https://static-course-assets.s3.amazonaws.com/CN503/ru/index.html#6.2.3). [Выбор решений широкополосного доступа](https://static-course-assets.s3.amazonaws.com/CN503/ru/index.html#6.2.4).

52. [Настройка подключений xDSL](https://static-course-assets.s3.amazonaws.com/CN503/ru/index.html#6.3).

47. Протокол PPPoE.

48. [Обзор PPPoE](https://static-course-assets.s3.amazonaws.com/CN503/ru/index.html#6.3.1). [Настройка PPPoE](https://static-course-assets.s3.amazonaws.com/CN503/ru/index.html#6.3.2).

49. Технология создания виртуальных частных сетей.

50. Преимущество сети VPN. [Основы сетей VPN](https://static-course-assets.s3.amazonaws.com/CN503/ru/index.html#7.1.1).

51. [Типы сетей VPN](https://static-course-assets.s3.amazonaws.com/CN503/ru/index.html#7.1.2). Site-to-Site VPN и VPN для удаленного доступа.

52. VPN для крупных компаний и операторов связи.

53. SSL VPN. GRE через IPSec.

54. Динамическая многоточечная VPN-сеть (DMVPN).

55.Интерфейс виртуальных туннелей IPsec.

56. MPLS VPN уровня провайдера

57. Защита межфилиальной связи

58. [Туннели GRE между объектами](https://static-course-assets.s3.amazonaws.com/CN503/ru/index.html#7.2).

59. [Основы GRE](https://static-course-assets.s3.amazonaws.com/CN503/ru/index.html#7.2.1). [Настройка туннелей GRE](https://static-course-assets.s3.amazonaws.com/CN503/ru/index.html#7.2.2).

60. Протокол IPsec. [Общие сведения об IPsec](https://static-course-assets.s3.amazonaws.com/CN503/ru/index.html#7.3).

61. IPSec технологии. Инкапсуляция протокола IPSec.

62. Конфиденциальность. Целостность. Аутентификация.

63. Безопасный обмен ключами с Диффи-Хеллманом.

64. Транспортный и туннельный режим IPSec.

65. [Структура протокола IPsec](https://static-course-assets.s3.amazonaws.com/CN503/ru/index.html#7.3.2)

66. [Удалённый доступ](https://static-course-assets.s3.amazonaws.com/CN503/ru/index.html#7.4). [Решения VPN для удалённого доступа](https://static-course-assets.s3.amazonaws.com/CN503/ru/index.html#7.4.1).

67. [Сети VPN удалённого доступа с использованием IPsec](https://static-course-assets.s3.amazonaws.com/CN503/ru/index.html#7.4.2).

68. Мониторинг сети [Syslog](https://static-course-assets.s3.amazonaws.com/CN503/ru/index.html#8.1). 69. [Принцип работы Syslog](https://static-course-assets.s3.amazonaws.com/CN503/ru/index.html#8.1.1). [Настройка Syslog](https://static-course-assets.s3.amazonaws.com/CN503/ru/index.html#8.1.2).

69. Протокол [SNMP](https://static-course-assets.s3.amazonaws.com/CN503/ru/index.html#8.2). [Принцип работы SNMP](https://static-course-assets.s3.amazonaws.com/CN503/ru/index.html#8.2.1). [Настройка SNMP](https://static-course-assets.s3.amazonaws.com/CN503/ru/index.html#8.2.2).

70. Протокол [NetFlow](https://static-course-assets.s3.amazonaws.com/CN503/ru/index.html#8.3). [Принцип работы NetFlow](https://static-course-assets.s3.amazonaws.com/CN503/ru/index.html#8.3.1). [Настройка NetFlow](https://static-course-assets.s3.amazonaws.com/CN503/ru/index.html#8.3.2). [Проверка моделей трафика](https://static-course-assets.s3.amazonaws.com/CN503/ru/index.html#8.3.3).

71. [Поиск и устранение неполадок с использованием системного подхода](https://static-course-assets.s3.amazonaws.com/CN503/ru/index.html#9.1). [Документация по сети](https://static-course-assets.s3.amazonaws.com/CN503/ru/index.html#9.1.1). [Процедура поиска и устранения неполадок](https://static-course-assets.s3.amazonaws.com/CN503/ru/index.html#9.1.2).

72. [Изоляция проблемы с помощью многоуровневых моделей](https://static-course-assets.s3.amazonaws.com/CN503/ru/index.html#9.1.3).

73. [Отладка сети](https://static-course-assets.s3.amazonaws.com/CN503/ru/index.html#9.2). [Средства поиска и устранения неполадок](https://static-course-assets.s3.amazonaws.com/CN503/ru/index.html#9.2.1).

74. [Симптомы и причины отладки сети](https://static-course-assets.s3.amazonaws.com/CN503/ru/index.html#9.2.2). [Поиск и устранение неполадок связи в сетях IP](https://static-course-assets.s3.amazonaws.com/CN503/ru/index.html#9.2.3)

75. Принципы обеспечения безопасности сети

76. Текущий уровень кибербезопасности. Векторы сетевых атак.

77. Потеря данных. Злоумышленники. Инструменты злоумышленников.

78. Вредоносное программное обеспечение.

79. Типы вредоносного ПО. Вирусы и «троянские кони».

80. Угрозы и уязвимости IP.

81. Распространенные сетевые атаки.

82. Разведывательные атаки.

83. Атаки доступа.

84. Атаки методами социальной инженерии.

85. DoS- и DDoS-атаки.

86. Атаки на основе ICMP.

87. Атаки по методу умножения и отражения.

88. Атаки с подменой адреса.

89. Уязвимости TCP и UDP.

90. Сервисы TCP. Атаки TCP.

91. Атаки с использованием UDP.

92. Уяязвимости ARP. Подделка записей кеша ARP.

93. Спуфинг ARP.

94. Атаки DNS.

95. Туннелирование DNS.

96. Атаки, связанные с DHCP.

97. Качество передачи данных по сети QoS. Установка приоритетов трафика.

98. Пропускная способность, перегрузка, задержка и джиттер. Характеристики трафика.

99. Тенденции сетевого трафика. Оптимизация передачи.

100.  Алгоритмы QoS. Взвешенная организация очередей (WFQ).

101. Взвешенная организация очередей на основе классов (CBWFQ).

102. Организация очередей с малой задержкой (LLQ).

103. Модели обеспечения качества обслуживания. Модели QoS.

104. Выбор подходящей модели политики качества обслуживания.

105. Негарантированная доставка. Интегрированные сервисы. Дифференцированные услуги

106. Способы обеспечения качества обслуживания

107. Методы внедрения QoS. Предотвращение потери пакетов. Классификация и маркировка.

108. Поле «Тип обслуживания / Класс трафика». Значения DSCP.

109. Средство выбора класса (CS). Границы доверия.

110. Предотвращение затора. Руководящие принципы политики QoS.

111. Настройка и проверка CDP. Поиск устройств с помощью CDP. Инструмент проверки синтаксиса: настройка и проверка протокола CDP.

112. Общие сведения о протоколе LLDP Настройка и проверка протокола LLDP. Поиск устройств с помощью LLDP. Инструмент проверки синтаксиса: настройка и проверка протокола LLDP.

113. Обзор облачных вычислений. Облачные вычисления и центр обработки данных. Облачные вычисления и виртуализация.

114. Виртуализация серверов. Уровни абстракции.

115. Установка виртуальной машины на гипервизоре. Сложность виртуализации сети.

116. Программно-определяемые сети. Традиционная архитектура и архитектура SDN.

117. Контроллер и операции SDN. Типы SDN.

118. Автоматизация сети. Рост автоматизации. Умные устройства.

119. Концепция форматов данных. Формат данных JSON. Формат данных YAML. Формат данных XML.

120. API – интерфейсы. Основы API. Открытые, внутренние и партнерские API.

121. Типы веб-сервисов API.

122. REST и RESTful API. URI, URN и URL.

123. Приложения RESTful API.

124. Традиционная конфигурация сети. Инструменты управления конфигурацией.

125. Compare Ansible, Chef, Puppet, и SaltStack.

126. Политики DNA Center и контроль

**Критерии оценки устного опроса:**

**-**оценка «отлично» ставится за ответ без ошибок и недочетов или имеющий не более одного недочета;

* оценка «хорошо» ставится за правильный ответ, но при наличии в ней не более одной негрубой ошибки и одного недочета или не более двух недочетов;
* оценка «удовлетворительно» ставится в том случае, если студент правильно ответил не менее половины вопроса или допустил:

а) не более двух грубых ошибок;

б) не более одной грубой ошибки и одного недочета;

в) не более двух-трех негрубых ошибок;

г) не более одной негрубой ошибки и трех недочетов;

д) при отсутствии ошибок, но при наличии 4-5 недочетов;

* оценка «неудовлетворительно» ставится, когда число ошибок и недочетов превосходит норму, при которой может быть выставлена оценка «3», или если правильно ответил менее половины вопроса.

Грубыми являются ошибки, свидетельствующие о том, что студент не усвоил основные понятия темы, последовательность выполнения задания, не умеет формулировать выводы по результатам расчетов.

Негрубыми ошибками являются неточности расчетов, пропуск или неполное описание алгоритмов, неполное отражение результатов исследования в выводе.

К недочетам относятся небрежное выполнение заданий, отдельные погрешности в формулировке ответа.

**Критерии оценки практического занятия:**

**-**оценка «отлично» ставится за практическое занятие, выполненное без ошибок и недочетов или имеющее не более одного недочета;

* оценка «хорошо», ставится за практическое занятие, выполненное полностью, но при наличии в ней не более одной негрубой ошибки и одного недочета или не более двух недочетов;
* оценка «удовлетворительно» ставится в том случае, если студент правильно выполнил не менее половины практического занятия или допустил:

а) не более двух грубых ошибок;

б) не более одной грубой ошибки и одного недочета;

в) не более двух-трех негрубых ошибок;

г) не более одной негрубой ошибки и трех недочетов;

д) при отсутствии ошибок, но при наличии 4-5 недочетов;

* оценка «неудовлетворительно» ставится, когда число ошибок и недочетов превосходит норму, при которой может быть выставлена оценка «3», или если правильно выполнено менее половины практического занятия.

Грубыми являются ошибки, свидетельствующие о том, что студент не усвоил основные понятия темы, последовательность выполнения задания, не умеет формулировать выводы по результатам расчетов, незнание расчетов адресации сетей.

Негрубыми ошибками являются неточности расчетов; неполное отражение результатов исследования в выводе.

К недочетам относятся небрежное выполнение заданий к практическому занятию, отдельные погрешности при определении расчетов адресации.

**4 КОНТРОЛЬНО-ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ**

**Экзаменационные вопросы по МДК 01.02 Организация, принципы построения и функционирования компьютерных сетей**

**Тема 2.1**

1. Принцип работы RSTP, STP.

2. [Агрегирование каналов в Cisco](http://xgu.ru/wiki/%D0%90%D0%B3%D1%80%D0%B5%D0%B3%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5_%D0%BA%D0%B0%D0%BD%D0%B0%D0%BB%D0%BE%D0%B2#.D0.90.D0.B3.D1.80.D0.B5.D0.B3.D0.B8.D1.80.D0.BE.D0.B2.D0.B0.D0.BD.D0.B8.D0.B5_.D0.BA.D0.B0.D0.BD.D0.B0.D0.BB.D0.BE.D0.B2_.D0.B2_Cisco). [Терминология и настройка](http://xgu.ru/wiki/%D0%90%D0%B3%D1%80%D0%B5%D0%B3%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5_%D0%BA%D0%B0%D0%BD%D0%B0%D0%BB%D0%BE%D0%B2#.D0.A2.D0.B5.D1.80.D0.BC.D0.B8.D0.BD.D0.BE.D0.BB.D0.BE.D0.B3.D0.B8.D1.8F_.D0.B8_.D0.BD.D0.B0.D1.81.D1.82.D1.80.D0.BE.D0.B9.D0.BA.D0.B0). [Общие правила настройки EtherChannel](http://xgu.ru/wiki/%D0%90%D0%B3%D1%80%D0%B5%D0%B3%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5_%D0%BA%D0%B0%D0%BD%D0%B0%D0%BB%D0%BE%D0%B2#.D0.9E.D0.B1.D1.89.D0.B8.D0.B5_.D0.BF.D1.80.D0.B0.D0.B2.D0.B8.D0.BB.D0.B0_.D0.BD.D0.B0.D1.81.D1.82.D1.80.D0.BE.D0.B9.D0.BA.D0.B8_EtherChannel). [Синтаксис команды channel-group](http://xgu.ru/wiki/%D0%90%D0%B3%D1%80%D0%B5%D0%B3%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5_%D0%BA%D0%B0%D0%BD%D0%B0%D0%BB%D0%BE%D0%B2#.D0.A1.D0.B8.D0.BD.D1.82.D0.B0.D0.BA.D1.81.D0.B8.D1.81_.D0.BA.D0.BE.D0.BC.D0.B0.D0.BD.D0.B4.D1.8B_channel-group). [Интерфейсы в состоянии suspended](http://xgu.ru/wiki/%D0%90%D0%B3%D1%80%D0%B5%D0%B3%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5_%D0%BA%D0%B0%D0%BD%D0%B0%D0%BB%D0%BE%D0%B2#.D0.98.D0.BD.D1.82.D0.B5.D1.80.D1.84.D0.B5.D0.B9.D1.81.D1.8B_.D0.B2_.D1.81.D0.BE.D1.81.D1.82.D0.BE.D1.8F.D0.BD.D0.B8.D0.B8_suspended). [Команды просмотра информации](http://xgu.ru/wiki/%D0%90%D0%B3%D1%80%D0%B5%D0%B3%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5_%D0%BA%D0%B0%D0%BD%D0%B0%D0%BB%D0%BE%D0%B2#.D0.9A.D0.BE.D0.BC.D0.B0.D0.BD.D0.B4.D1.8B_.D0.BF.D1.80.D0.BE.D1.81.D0.BC.D0.BE.D1.82.D1.80.D0.B0_.D0.B8.D0.BD.D1.84.D0.BE.D1.80.D0.BC.D0.B0.D1.86.D0.B8.D0.B8).

3. [Standby-интерфейсы](http://xgu.ru/wiki/%D0%90%D0%B3%D1%80%D0%B5%D0%B3%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5_%D0%BA%D0%B0%D0%BD%D0%B0%D0%BB%D0%BE%D0%B2#Standby-.D0.B8.D0.BD.D1.82.D0.B5.D1.80.D1.84.D0.B5.D0.B9.D1.81.D1.8B). [Настройка EtherChannel 2го уровня с помощью PAgP](http://xgu.ru/wiki/%D0%90%D0%B3%D1%80%D0%B5%D0%B3%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5_%D0%BA%D0%B0%D0%BD%D0%B0%D0%BB%D0%BE%D0%B2#.D0.9D.D0.B0.D1.81.D1.82.D1.80.D0.BE.D0.B9.D0.BA.D0.B0_EtherChannel_2.D0.B3.D0.BE_.D1.83.D1.80.D0.BE.D0.B2.D0.BD.D1.8F_.D1.81_.D0.BF.D0.BE.D0.BC.D0.BE.D1.89.D1.8C.D1.8E_PAgP). [Настройка EtherChannel 3го уровня](http://xgu.ru/wiki/%D0%90%D0%B3%D1%80%D0%B5%D0%B3%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5_%D0%BA%D0%B0%D0%BD%D0%B0%D0%BB%D0%BE%D0%B2#.D0.9D.D0.B0.D1.81.D1.82.D1.80.D0.BE.D0.B9.D0.BA.D0.B0_EtherChannel_3.D0.B3.D0.BE_.D1.83.D1.80.D0.BE.D0.B2.D0.BD.D1.8F).

4. [Балансировка нагрузки](http://xgu.ru/wiki/%D0%90%D0%B3%D1%80%D0%B5%D0%B3%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5_%D0%BA%D0%B0%D0%BD%D0%B0%D0%BB%D0%BE%D0%B2#.D0.91.D0.B0.D0.BB.D0.B0.D0.BD.D1.81.D0.B8.D1.80.D0.BE.D0.B2.D0.BA.D0.B0_.D0.BD.D0.B0.D0.B3.D1.80.D1.83.D0.B7.D0.BA.D0.B8). [Тестирование балансировки нагрузки](http://xgu.ru/wiki/%D0%90%D0%B3%D1%80%D0%B5%D0%B3%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5_%D0%BA%D0%B0%D0%BD%D0%B0%D0%BB%D0%BE%D0%B2#.D0.A2.D0.B5.D1.81.D1.82.D0.B8.D1.80.D0.BE.D0.B2.D0.B0.D0.BD.D0.B8.D0.B5_.D0.B1.D0.B0.D0.BB.D0.B0.D0.BD.D1.81.D0.B8.D1.80.D0.BE.D0.B2.D0.BA.D0.B8_.D0.BD.D0.B0.D0.B3.D1.80.D1.83.D0.B7.D0.BA.D0.B8).

5. [Статическое агрегирование каналов с помощью LACP](http://xgu.ru/wiki/%D0%90%D0%B3%D1%80%D0%B5%D0%B3%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5_%D0%BA%D0%B0%D0%BD%D0%B0%D0%BB%D0%BE%D0%B2#.D0.A1.D1.82.D0.B0.D1.82.D0.B8.D1.87.D0.B5.D1.81.D0.BA.D0.BE.D0.B5_.D0.B0.D0.B3.D1.80.D0.B5.D0.B3.D0.B8.D1.80.D0.BE.D0.B2.D0.B0.D0.BD.D0.B8.D0.B5_.D0.BA.D0.B0.D0.BD.D0.B0.D0.BB.D0.BE.D0.B2_.D1.81_.D0.BF.D0.BE.D0.BC.D0.BE.D1.89.D1.8C.D1.8E_LACP). [Динамическое агрегирование каналов с помощью LACP](http://xgu.ru/wiki/%D0%90%D0%B3%D1%80%D0%B5%D0%B3%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5_%D0%BA%D0%B0%D0%BD%D0%B0%D0%BB%D0%BE%D0%B2#.D0.94.D0.B8.D0.BD.D0.B0.D0.BC.D0.B8.D1.87.D0.B5.D1.81.D0.BA.D0.BE.D0.B5_.D0.B0.D0.B3.D1.80.D0.B5.D0.B3.D0.B8.D1.80.D0.BE.D0.B2.D0.B0.D0.BD.D0.B8.D0.B5_.D0.BA.D0.B0.D0.BD.D0.B0.D0.BB.D0.BE.D0.B2_.D1.81_.D0.BF.D0.BE.D0.BC.D0.BE.D1.89.D1.8C.D1.8E_LACP).

6. [Балансировка нагрузки](http://xgu.ru/wiki/%D0%90%D0%B3%D1%80%D0%B5%D0%B3%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5_%D0%BA%D0%B0%D0%BD%D0%B0%D0%BB%D0%BE%D0%B2#.D0.91.D0.B0.D0.BB.D0.B0.D0.BD.D1.81.D0.B8.D1.80.D0.BE.D0.B2.D0.BA.D0.B0_.D0.BD.D0.B0.D0.B3.D1.80.D1.83.D0.B7.D0.BA.D0.B8_2). [Балансировка нагрузки по MAC-адресам или IP-адресам](http://xgu.ru/wiki/%D0%90%D0%B3%D1%80%D0%B5%D0%B3%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5_%D0%BA%D0%B0%D0%BD%D0%B0%D0%BB%D0%BE%D0%B2#.D0.91.D0.B0.D0.BB.D0.B0.D0.BD.D1.81.D0.B8.D1.80.D0.BE.D0.B2.D0.BA.D0.B0_.D0.BD.D0.B0.D0.B3.D1.80.D1.83.D0.B7.D0.BA.D0.B8_.D0.BF.D0.BE_MAC-.D0.B0.D0.B4.D1.80.D0.B5.D1.81.D0.B0.D0.BC_.D0.B8.D0.BB.D0.B8_IP-.D0.B0.D0.B4.D1.80.D0.B5.D1.81.D0.B0.D0.BC). [Балансировка нагрузки по портам](http://xgu.ru/wiki/%D0%90%D0%B3%D1%80%D0%B5%D0%B3%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5_%D0%BA%D0%B0%D0%BD%D0%B0%D0%BB%D0%BE%D0%B2#.D0.91.D0.B0.D0.BB.D0.B0.D0.BD.D1.81.D0.B8.D1.80.D0.BE.D0.B2.D0.BA.D0.B0_.D0.BD.D0.B0.D0.B3.D1.80.D1.83.D0.B7.D0.BA.D0.B8_.D0.BF.D0.BE_.D0.BF.D0.BE.D1.80.D1.82.D0.B0.D0.BC). [Тестирование балансировки](http://xgu.ru/wiki/%D0%90%D0%B3%D1%80%D0%B5%D0%B3%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5_%D0%BA%D0%B0%D0%BD%D0%B0%D0%BB%D0%BE%D0%B2#.D0.A2.D0.B5.D1.81.D1.82.D0.B8.D1.80.D0.BE.D0.B2.D0.B0.D0.BD.D0.B8.D0.B5_.D0.B1.D0.B0.D0.BB.D0.B0.D0.BD.D1.81.D0.B8.D1.80.D0.BE.D0.B2.D0.BA.D0.B8).

7. Протоколы динамической маршрутизации – назначение, принципы работы и история развития. Сравнение динамической и статической маршрутизации. Принципы работы протоколов маршрутизации: пуск после включения питания, сетевое обнаружение, обмен данными маршрутизации, обеспечение сходимости.

8. Классификация протоколов маршрутизации. Дистанционно-векторный протокол RIP.

9. Классификация протоколов маршрутизации. Дистанционно-векторный протокол IGRP.

10. Классификация протоколов маршрутизации. Протокол маршрутизации по состоянию канала OSPF.

11. Классификация протоколов маршрутизации. Протокол маршрутизации по состоянию канала IS-IS.

12. Классовые и бесклассовые протоколы маршрутизации. Характеристики и метрики протоколов. Дистанционно-векторный алгоритм.

13. Семейство протоколов OSPF. Характеристики, принципы работы и компоненты OSPF. Особенности OSPF для одной и нескольких областей. Магистральная область. Инкапсуляция сообщений OSPF.

14. Типы пакетов OSPF: пакет приветствия (hello), пакет описания базы данных (DBD), пакет запроса состояния канала (LSR), пакет обновления состояния канала (LSU). пакет подтверждения состояния канала (LSAck). Обновления состояния канала.

15. Рабочие состояния OSPF. Выделенный (DR) и резервный выделенный маршрутизатор (BDR). Синхронизация баз данных OSPF.

16. Списки контроля доступа (ACL). Принцип работы ACL списков. Типы ACL-списков Cisco для IPv4. Присваивание номеров и имён ACL-спискам.

17. Расчёт шаблонной маски в ACL-списках. Рекомендации по созданию и размещению ACL-списков. Защита портов VTY с помощью стандартного ACL-списка IPv4.

18. Структура и настройка расширенных ACL-списков для IPv4. Фильтрация трафика с использованием расширенных ACL-списков. Сравнение ACL-списков для IPv4 и IPv6.

19. Протокол DHCPv4: базовая операция, формат сообщений, сообщения обнаружения и предложения. Настройка, проверка и ретрансляция простого DHCPv4-сервера. Настройка маршрутизатора в качестве DHCPv4-клиента.

20. Автоматическая настройка адреса без отслеживания состояния (SLAAC). Принцип работы SLAAC с DHCPv6. DHCPv6 с и без отслеживания состояния. Процессы DHCPv6.

21. Преобразование сетевых адресов IPv4. Концептуальное преобразование сетевых адресов (NAT). Терминология и принципы работы NAT. Пространство частных IPv4-адресов.

22. Статическое и динамическое преобразование сетевых адресов (NAT). Преобразование адресов портов (PAT). Сравнение NAT и PAT.

23. Понятия протокола spanning-tree. Предназначение протокола spanning-tree. Принцип работы STP. Типы протоколов STP. Настройка PVST+. Настройка Rapid PVST+.

24. Концепции беспроводной связи. Введение в беспроводную связь. Компоненты сетей WLAN. Топологии сетей WLAN 802.11. Принципы работы беспроводной локальной сети.

25. [Основные версии протокола](https://www.cisco.com/c/ru_ru/support/docs/ip/enhanced-interior-gateway-routing-protocol-eigrp/16406-eigrp-toc.html#anc2). [Теоретические сведения](https://www.cisco.com/c/ru_ru/support/docs/ip/enhanced-interior-gateway-routing-protocol-eigrp/16406-eigrp-toc.html#anc3). [Обнаружение и обслуживание соседей](https://www.cisco.com/c/ru_ru/support/docs/ip/enhanced-interior-gateway-routing-protocol-eigrp/16406-eigrp-toc.html#anc4). [Создание таблицы топологии](https://www.cisco.com/c/ru_ru/support/docs/ip/enhanced-interior-gateway-routing-protocol-eigrp/16406-eigrp-toc.html#anc5). [Метрика протокола EIGRP](https://www.cisco.com/c/ru_ru/support/docs/ip/enhanced-interior-gateway-routing-protocol-eigrp/16406-eigrp-toc.html#anc6). [Определение беспетлевого пути](https://www.cisco.com/c/ru_ru/support/docs/ip/enhanced-interior-gateway-routing-protocol-eigrp/16406-eigrp-toc.html#anc8) [EIGRP](https://www.cisco.com/c/ru_ru/support/docs/ip/enhanced-interior-gateway-routing-protocol-eigrp/16406-eigrp-toc.html#anc6).

26. [Группы сторон BGP](https://www.cisco.com/c/ru_ru/support/docs/ip/border-gateway-protocol-bgp/13755-29.html#bgppgrp). [Требования к группам сторон](https://www.cisco.com/c/ru_ru/support/docs/ip/border-gateway-protocol-bgp/13755-29.html#pgrpreqs). [Ограничения для групп сторон](https://www.cisco.com/c/ru_ru/support/docs/ip/border-gateway-protocol-bgp/13755-29.html#pgrplimits). [Использование групп сторон](https://www.cisco.com/c/ru_ru/support/docs/ip/border-gateway-protocol-bgp/13755-29.html#usepgrp). [Формат сообщения](https://ru.wikipedia.org/wiki/Border_Gateway_Protocol#%D0%A4%D0%BE%D1%80%D0%BC%D0%B0%D1%82_%D1%81%D0%BE%D0%BE%D0%B1%D1%89%D0%B5%D0%BD%D0%B8%D1%8F). [Обновление информации](https://ru.wikipedia.org/wiki/Border_Gateway_Protocol#%D0%9E%D0%B1%D0%BD%D0%BE%D0%B2%D0%BB%D0%B5%D0%BD%D0%B8%D0%B5_%D0%B8%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%B8). [Сохранение соединения](https://ru.wikipedia.org/wiki/Border_Gateway_Protocol#%D0%A1%D0%BE%D1%85%D1%80%D0%B0%D0%BD%D0%B5%D0%BD%D0%B8%D0%B5_%D1%81%D0%BE%D0%B5%D0%B4%D0%B8%D0%BD%D0%B5%D0%BD%D0%B8%D1%8F). [Оповещение](https://ru.wikipedia.org/wiki/Border_Gateway_Protocol#%D0%9E%D0%BF%D0%BE%D0%B2%D0%B5%D1%89%D0%B5%D0%BD%D0%B8%D0%B5).

27. [Протокол IS-IS: объединение плоскости состояния и вектора пути](https://wiki.merionet.ru/seti/72/protokol-is-is-obedinenie-ploskosti-sostoyaniya-i-vektora-puti/). Сравнение с OSPF. Метрики IS-IS. Маршрутизация IS-IS.

28. Уровни RAID. Преимущества и недостатки основных уровней RAID. Архитектура хранилищ данных: традиционная и облачная.

**Тема 2.2**

1. [Цель создания глобальных сетей](https://static-course-assets.s3.amazonaws.com/CN503/ru/index.html#2.1.1). [Принцип работы глобальной сети](https://static-course-assets.s3.amazonaws.com/CN503/ru/index.html#2.1.2). В[ыбор технологии глобальной сети](https://static-course-assets.s3.amazonaws.com/CN503/ru/index.html#2.2). [Инфраструктуры частных глобальных сетей](https://static-course-assets.s3.amazonaws.com/CN503/ru/index.html#2.2.2). [Инфраструктура общедоступной глобальной сети](https://static-course-assets.s3.amazonaws.com/CN503/ru/index.html#2.2.3). [Выбор сервисов глобальной сети](https://static-course-assets.s3.amazonaws.com/CN503/ru/index.html#2.2.4).

2. [Обзор последовательного соединения «точка-точка»](https://static-course-assets.s3.amazonaws.com/CN503/ru/index.html#3.1). [Связь по последовательному каналу](https://static-course-assets.s3.amazonaws.com/CN503/ru/index.html#3.1.1). [Инкапсуляция HDLC](https://static-course-assets.s3.amazonaws.com/CN503/ru/index.html#3.1.2).

3. Стандарты WAN. Общепринятая терминология глобальных сетей. Устройства глобальной сети. Последовательная связь. Сеть с коммутацией каналов. Сеть с коммутацией пакетов. SDH, SONET и DWDM

4. [Преимущества протокола PPP](https://static-course-assets.s3.amazonaws.com/CN503/ru/index.html#3.2.1). [LCP и NCP](https://static-course-assets.s3.amazonaws.com/CN503/ru/index.html#3.2.2). [Сеансы PPP](https://static-course-assets.s3.amazonaws.com/CN503/ru/index.html#3.2.3). [Настройка протокола PPP](https://static-course-assets.s3.amazonaws.com/CN503/ru/index.html#3.3.1). [Аутентификация PPP](https://static-course-assets.s3.amazonaws.com/CN503/ru/index.html#3.3.2). [Отладка соединений WAN](https://static-course-assets.s3.amazonaws.com/CN503/ru/index.html#3.4). [Отладка PPP](https://static-course-assets.s3.amazonaws.com/CN503/ru/index.html#3.4.1).

5. Решения широкополосного доступа. [Сравнение решений широкополосного доступа](https://static-course-assets.s3.amazonaws.com/CN503/ru/index.html#6.2). [Беспроводные широкополосные сети](https://static-course-assets.s3.amazonaws.com/CN503/ru/index.html#6.2.3). [Выбор решений широкополосного доступа](https://static-course-assets.s3.amazonaws.com/CN503/ru/index.html#6.2.4).

6. Протокол PPPoE. [Обзор PPPoE](https://static-course-assets.s3.amazonaws.com/CN503/ru/index.html#6.3.1). [Настройка PPPoE](https://static-course-assets.s3.amazonaws.com/CN503/ru/index.html#6.3.2).

7. Технология создания виртуальных частных сетей. Преимущество сети VPN. [Основы сетей VPN](https://static-course-assets.s3.amazonaws.com/CN503/ru/index.html#7.1.1). [Типы сетей VPN](https://static-course-assets.s3.amazonaws.com/CN503/ru/index.html#7.1.2). Site-to-Site VPN и VPN для удаленного доступа. VPN для крупных компаний и операторов связи.

8. SSL VPN. GRE через IPSec. Динамическая многоточечная VPN-сеть (DMVPN).

9. [Туннели GRE между объектами](https://static-course-assets.s3.amazonaws.com/CN503/ru/index.html#7.2). [Основы GRE](https://static-course-assets.s3.amazonaws.com/CN503/ru/index.html#7.2.1). [Настройка туннелей GRE](https://static-course-assets.s3.amazonaws.com/CN503/ru/index.html#7.2.2).

10. Протокол IPsec. [Общие сведения об IPsec](https://static-course-assets.s3.amazonaws.com/CN503/ru/index.html#7.3). Интерфейс виртуальных туннелей IPsec. IPSec технологии. Инкапсуляция протокола IPSec.

11. [Структура протокола IPsec](https://static-course-assets.s3.amazonaws.com/CN503/ru/index.html#7.3.2). Транспортный и туннельный режим. Безопасный обмен ключами с Диффи-Хеллманом.

12. [Удалённый доступ](https://static-course-assets.s3.amazonaws.com/CN503/ru/index.html#7.4). [Решения VPN для удалённого доступа](https://static-course-assets.s3.amazonaws.com/CN503/ru/index.html#7.4.1). [Сети VPN удалённого доступа с использованием IPsec](https://static-course-assets.s3.amazonaws.com/CN503/ru/index.html#7.4.2).

13. Мониторинг сети [Syslog](https://static-course-assets.s3.amazonaws.com/CN503/ru/index.html#8.1). [Принцип работы Syslog](https://static-course-assets.s3.amazonaws.com/CN503/ru/index.html#8.1.1). [Настройка Syslog](https://static-course-assets.s3.amazonaws.com/CN503/ru/index.html#8.1.2).

14. Протокол [SNMP](https://static-course-assets.s3.amazonaws.com/CN503/ru/index.html#8.2). [Принцип работы SNMP](https://static-course-assets.s3.amazonaws.com/CN503/ru/index.html#8.2.1). [Настройка SNMP](https://static-course-assets.s3.amazonaws.com/CN503/ru/index.html#8.2.2).

15. Протокол [NetFlow](https://static-course-assets.s3.amazonaws.com/CN503/ru/index.html#8.3). [Принцип работы NetFlow](https://static-course-assets.s3.amazonaws.com/CN503/ru/index.html#8.3.1). [Настройка NetFlow](https://static-course-assets.s3.amazonaws.com/CN503/ru/index.html#8.3.2). [Проверка моделей трафика](https://static-course-assets.s3.amazonaws.com/CN503/ru/index.html#8.3.3).

16. Текущий уровень кибербезопасности. Векторы сетевых атак. Потеря данных. Злоумышленники. Инструменты злоумышленников.

17. Вредоносное программное обеспечение. Типы вредоносного ПО. Вирусы и «троянские кони».

18. Угрозы и уязвимости IP. Распространенные сетевые атаки. Разведывательные атаки. Атаки доступа. Атаки методами социальной инженерии.

19. Угрозы и уязвимости IP. DoS- и DDoS-атаки. Атаки на основе ICMP. Атаки по методу умножения и отражения. Атаки с подменой адреса.

20. Уязвимости TCP и UDP. Сервисы TCP. Атаки TCP. Атаки с использованием UDP.

21. Уяязвимости ARP. Подделка записей кеша ARP. Спуфинг ARP. Атаки DNS. Туннелирование DNS. Атаки, связанные с DHCP.

22. Качество передачи данных по сети QoS. Установка приоритетов трафика. Пропускная способность, перегрузка, задержка и джиттер. Характеристики трафика. Тенденции сетевого трафика. Оптимизация передачи.

23.  Алгоритмы QoS. Взвешенная организация очередей (WFQ). Взвешенная организация очередей на основе классов (CBWFQ). Организация очередей с малой задержкой (LLQ).

24. Модели обеспечения качества обслуживания. Модели QoS. Выбор подходящей модели политики качества обслуживания. Негарантированная доставка. Интегрированные сервисы. Дифференцированные услуги. Способы обеспечения качества обслуживания

25. Методы внедрения QoS. Предотвращение потери пакетов. Классификация и маркировка. Поле «Тип обслуживания / Класс трафика». Значения DSCP.

26. Средство выбора класса (CS). Границы доверия. Предотвращение затора. Руководящие принципы политики QoS.

27. Настройка и проверка CDP. Поиск устройств с помощью CDP. Инструмент проверки синтаксиса: настройка и проверка протокола CDP.

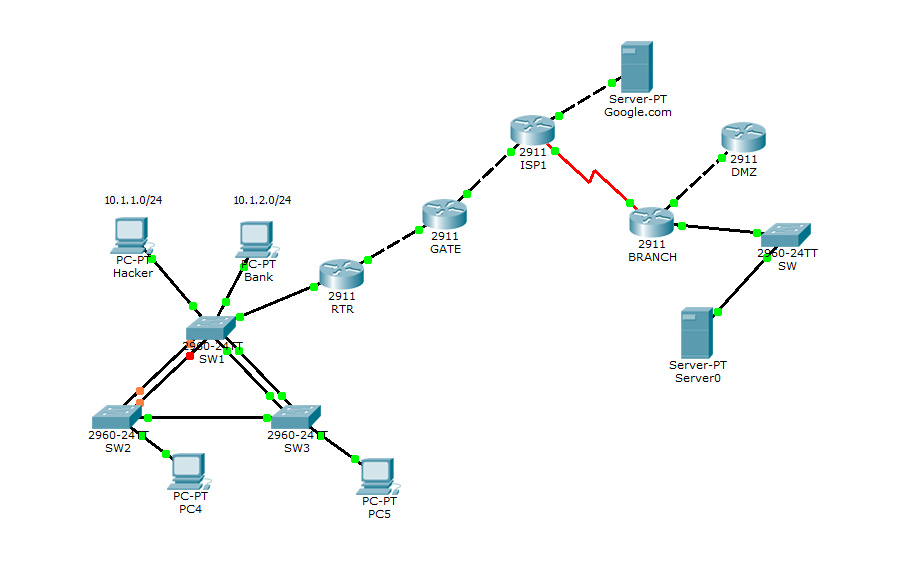
28. Общие сведения о протоколе LLDP Настройка и проверка протокола LLDP. Поиск устройств с помощью LLDP. Инструмент проверки синтаксиса: настройка и проверка протокола LLDP.

29. Обзор облачных вычислений. Облачные вычисления и центр обработки данных. Облачные вычисления и виртуализация. Виртуализация серверов. Уровни абстракции. Установка виртуальной машины на гипервизоре. Сложность виртуализации сети.

30. Программно-определяемые сети. Традиционная архитектура и архитектура SDN. Контроллер и операции SDN. Типы SDN. Автоматизация сети. Рост автоматизации. Умные устройства.

**ВАРИАНТ ПРАКТИЧЕСКОГО ЗАДАНИЯ**

**ТЕМА 2.1.**

Схема сети.

Если параметры настройки не указаны в задании, необходимо выбрать любые значения, позволяющие выполнить задание (например номера портов в портовых группах).

**Базовые настройки**

1. Для всего активного сетевого оборудования настройте доменное имя wsr2020.wsr

2. Настройте имена устройств в соответствии с диаграммой

3. Создайте локального пользователя admin с паролем Pass

- пользователь должен обладать максимальным уровнем привилегий.

- пароль должен храниться в виде результата хэш функции.

3. Для всех сетевых устройств сконфигурируйте пароль wsr2020 для входа в привилегированный режим.

4. Все сетевые устройства должны быть доступны для управления по протоколу SSHv2.

5. IP адреса устройств взять с таблицы (или с настроек примера).

**Настройка коммутации**

1. Таблица VLAN офиса HQ должна содержать следующие подсети:

VLAN10:CLIENT

VLAN20:SERV

VLAN1000:MANAGE

2. Транки между коммутаторами должны быть согласованы с использованием DTP. SW1 должен инициировать согласование, SW2 и SW3 должны быть настроены в пассивном режиме

3. Транк между SW2 и SW3 должен быть согласован без использования протокола DTP

4. На портах f0/10 коммутаторов SW2 и SW3 сконфигурируйте магистральные каналы без использования динамического согласования. Отключите протокол DTP явным образом.

**Конфигурация портовых групп.**

1. Между коммутаторами SW1 и SW2 настройте агрегирование по протоколу LACP. SW1 должен работать в активном режиме, SW2 в пассивном

2. Между коммутаторами SW1 и SW3 настройте агрегирование по протоколу PAgP. SW1 должен работать в активном режиме, SW3 в пассивном

3. На SW2 настройте балансировку нагрузки по MAC адресу источника + назначения, на SW3 настройте балансировку по IP адресу источника + назначения

**Сконфигурируйте протокол остовного дерева**

1. На всех коммутаторах используйте протокол, совместимый со стандартом 802.1w

2. Корнем для всех VLAN является SW1. При отказе SW1 корнем должен стать SW2. При отказе SW2 корнем должен стать SW3.

3. На портах f0/10 SW2 и SW3 обеспечьте быструю сходимость, без ожидания протокола 802.1w. Аналогичную настройку произведите на магистральном канале между этими двумя коммутаторами.

**Подключение ISP**

1. Для подключения левого офиса использовать обыкновенный Ethernet

2. Подключение правого офиса выполнить по протоколу PPP

- инкапсуляция PPP

- авторизация по протоколу CHAP

- пароль pass

3. Настроить GRE-туннель между правой и левой частью сети.

**Маршрутизация**

1. Обеспечьте маршрутизацию между сетями VLAN с использованием технологии Router-on-a-Stick.

2. В левой части сети настроить протокол OSPF.

3. В правой части сети настроить протокол EIGRP с автономной системой 65001.

4. Маршрут по умолчанию настроить статически в сторону ISP, настроить автомматическое распространение маршрута по умолчанию по сети.

5. Между маршрутизаторами GATE и BRANCH настроить проткол BPG, для GATE автономная система 45002 для BRANCH 45001.

6. Настроить передачу маршрутов для полного согласования сети.

**Подключение к сети интернет**

1. Настроить ретрансляцию адресов на GATE и BRANCH.

**Настройка сервисов**

1. На всех устройствах настроить согласование времени с сервером Google.

2. На RTR настроить DHCP сервер

- распределять сеть для VLAN CLIENT

- в качестве DNS использовать адрес 8.8.8.8

- в качестве шлюза адрес RTR

- первые 20 адресов сети запретить к выдаче.

**Настройка DHCP сервера**

На маршрутизаторе BRANCH сконфигурируйте DHCP сервер.

Обеспечьте возможность доступа в сеть интернет для главного офиса и офиса Branch.

Анонсируйте все сети, необходимые для достижения полной связанности в соответствии со схемой маршрутизации

Настройте аутентификацию.

**ВАРИАНТ ПРАКТИЧЕСКОГО ЗАДАНИЯ**

**ТЕМА 2.2.**

У некоторой компании есть главный офис, который подключается в Интернет. Пограничный маршрутизатор Border подключен к провайдеру, который предоставляет услуги Интернет. Также существует второй офис компании, который таже подключен к публичной сети. И между ними проброшен VPN туннель. Между роутерами установлен OSPF, а между роутерами интернет компании и главным офисом установлена статическая маршрутизация. На основных коммутаторах офиса установлены по триVLAN, на роутерах сабинтерфейсы.

Для всего активного сетевого оборудования настройте доменное имя wsr2020.wsr. Создайте локального пользователя admin с паролем Pa$$w0rd.

Для активного сетевого оборудования: пользователь должен обладать максимальным уровнем привилегий, пароль должен храниться в виде результата хэш функции, используйте алгоритм scrypt.

Для всех сетевых устройств сконфигурируйте пароль wsr2020 для входа в привилегированный режим.

Все сетевые устройства должны быть доступны для управления по протоколу SSHv2.

Зашифруйте все открытые пароли.

Таблица VLAN двух офисов должна содержать следующие подсети:

VLAN10:CLIENT

VLAN20:SERV

VLAN30:DMZ

Сконфигурируйте магистральные каналы.

Настройте подключение Border к провайдеру ISP с помощью протокола PPP. Адрес необходимо получить при помощи IPCP. Аутентификация не требуется.

Транспортный адрес необходимо получить при помощи протокола SLARP на соответствующий Serial интерфейс.

Устройства проходят аутентификацию по протоколу CHAP в одностороннем порядке. Только ISP аутентифицирует роутер Border. Для аутентификации используйте данные client65010 и пароль P@ssw0rd. Явно сконфигурируйте корректное значение MTU.

Сконфигурируйте GRE туннель между BRANCH1 и BRANCH2. В качестве адресов источника и назначения используйте адреса соответствующих loopback интерфейсов. Используйте номер туннельного интерфейса 1.

Обеспечьте возможность входа на Border c использованием доменных реквизитов. Группа MAdmins должна получать максимальный уровень привилегий при входе. Группа SAdmins должна получать при входе уровень привилегий. Обеспечьте возможность входа пользователя, созданного локально при доступности RADIUS сервера. Для 5 уровня привилегий сконфигурируйте расширенный набор команд. Добавьте возможность использования команд reload, debug и sh.

В главном офисе на сервере установлен DHCP, который раздает адресацию на все сетевые устройства. Здесь же установлены службы ААА, DNS, HTTP.

Во втором офисе компании установленWeb-server и DMZ.

На роутере Border установлена служба NAT.

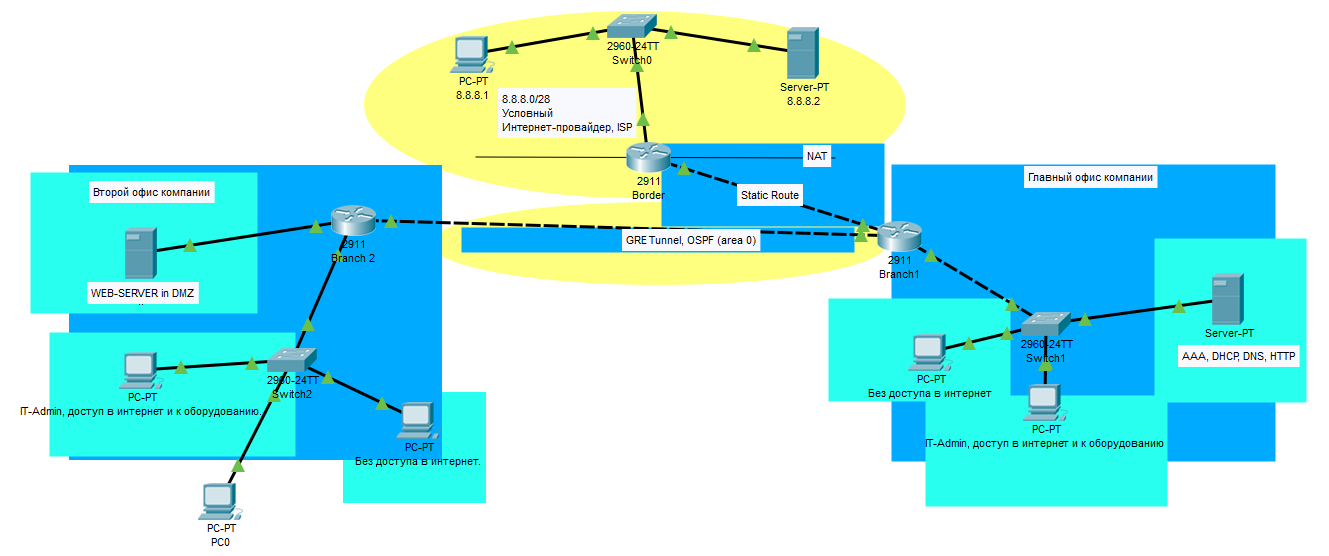


Схема сети

Министерство образования Красноярского края

краевое государственное бюджетное профессиональное образовательное учреждение «Красноярский колледж радиоэлектроники информационных технологий»

|  |  |
| --- | --- |
| РАССМОТРЕНО  на заседании цикловой комиссии  преподавателей профессионального цикла  технического профиля  Протокол № \_\_\_ от «\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_ 2023г  Председатель \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Е.В. Харитонова | УТВЕРЖДАЮ  Заместитель директора  по учебной работе  \_\_\_\_\_\_\_\_\_\_\_\_\_ М.А. Полютова  «\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 2023 г |

**ЭКЗАМЕНАЦИОННЫЕ БИЛЕТЫ**

**для проверки уровня подготовки студентов в соответствии**

**с требованиями федерального государственного образовательного стандарта СПО**

|  |  |
| --- | --- |
| Дисциплина | МДК 01.02 Организация, принципы построения и функционирования компьютерных сетей |
| Специальность | 09.02.06 Сетевое и системное администрирование |
| Курс | 2 |
| Форма обучения | очная |
| Количество билетов | 28 |
| Преподаватель | Скиляжнов А.О. |

Красноярск, 2023

Министерство образования Красноярского края

краевое государственное бюджетное профессиональное образовательное учреждение «Красноярский колледж радиоэлектроники и

информационных технологий»

|  |  |
| --- | --- |
| РАССМОТРЕНО  на заседании цикловой комиссии  преподавателей профессионального  цикла технического профиля  Протокол №\_\_ от «\_\_\_»\_\_\_\_\_\_ 2021 г .  Председатель ЦК \_\_\_\_\_ Е. В. Харитонова | УТВЕРЖДАЮ  Заместитель директора  по учебной работе  \_\_\_\_\_\_\_\_\_\_\_ М. А. Полютова  «\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 2021 г |

Экзаменационные билеты

Для проверки уровня подготовки студентов в соответствии с требованиями государственного образовательного стандарта

МДК 01.02 Организация, принципы построения и функционирования компьютерных сетей

**ПМ 01 «УЧАСТИЕ В ПРОЕКТИРОВАНИИ СЕТЕВОЙ ИНФРАСТРУКТУРЫ**

курс, семестр

для студентов специальности (ей)

09.02.06 «Сетевое и системное администрирование», базовой подготовки

Разработал

преподаватель КГБПОУ «ККРИТ»

Скиляжнов А.О.

Красноярск, 2023

Министерство образования Красноярского края

краевое государственное бюджетное профессиональное образовательное учреждение «Красноярский колледж радиоэлектроники и информационных технологий»

|  |  |  |  |
| --- | --- | --- | --- |
| |  |  |  | | --- | --- | --- | | |  | | --- | | РАССМОТРЕНО  на заседании цикловой комиссии  преподавателей профессионального  цикла технического профиля  Протокол №\_\_ от «\_\_\_»\_\_\_\_\_\_ 2021 г.  Председатель ЦК \_\_\_\_\_ Е. В. Харитонова | | ДИСЦИПЛИНА  МДК01.02 Организация, принципы построения и функционирования  компьютерных сетей  для специальности  09.02.06 Сетевое и системное\_\_\_\_\_\_\_\_  администрирование\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |   **ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №**  1  1. Уровни RAID. Преимущества и недостатки основных уровней RAID. Архитектура хранилищ данных: традиционная и облачная.   1. Практическое задание. Можно пользоваться Интернет. Схема сети.   Если параметры настройки не указаны в задании, необходимо выбрать любые значения, позволяющие выполнить задание (например номера портов в портовых группах).  **Базовые настройки**  1. Для всего активного сетевого оборудования настройте доменное имя wsr2020.wsr  2. Настройте имена устройств в соответствии с диаграммой  3. Создайте локального пользователя admin с паролем Pass  - пользователь должен обладать максимальным уровнем привилегий.  - пароль должен храниться в виде результата хэш функции.  3. Для всех сетевых устройств сконфигурируйте пароль wsr2020 для входа в привилегированный режим.  4. Все сетевые устройства должны быть доступны для управления по протоколу SSHv2.  5. IP адреса устройств взять с таблицы (или с настроек примера).  **Настройка коммутации**  1. Таблица VLAN офиса HQ должна содержать следующие подсети:  VLAN10:CLIENT  VLAN20:SERV  VLAN1000:MANAGE  2. Транки между коммутаторами должны быть согласованы с использованием DTP. SW1 должен инициировать согласование, SW2 и SW3 должны быть настроены в пассивном режиме  3. Транк между SW2 и SW3 должен быть согласован без использования протокола DTP  4. На портах f0/10 коммутаторов SW2 и SW3 сконфигурируйте магистральные каналы без использования динамического согласования. Отключите протокол DTP явным образом.  **Конфигурация портовых групп.**  1. Между коммутаторами SW1 и SW2 настройте агрегирование по протоколу LACP. SW1 должен работать в активном режиме, SW2 в пассивном  2. Между коммутаторами SW1 и SW3 настройте агрегирование по протоколу PAgP. SW1 должен работать в активном режиме, SW3 в пассивном  3. На SW2 настройте балансировку нагрузки по MAC адресу источника + назначения, на SW3 настройте балансировку по IP адресу источника + назначения  **Сконфигурируйте протокол остовного дерева**  1. На всех коммутаторах используйте протокол, совместимый со стандартом 802.1w  2. Корнем для всех VLAN является SW1. При отказе SW1 корнем должен стать SW2. При отказе SW2 корнем должен стать SW3.  3. На портах f0/10 SW2 и SW3 обеспечьте быструю сходимость, без ожидания протокола 802.1w. Аналогичную настройку произведите на магистральном канале между этими двумя коммутаторами.  **Подключение ISP**  1. Для подключения левого офиса использовать обыкновенный Ethernet  2. Подключение правого офиса выполнить по протоколу PPP  - инкапсуляция PPP  - авторизация по протоколу CHAP  - пароль pass  3. Настроить GRE-туннель между правой и левой частью сети.  **Маршрутизация**  1. Обеспечьте маршрутизацию между сетями VLAN с использованием технологии Router-on-a-Stick.  2. В левой части сети настроить протокол OSPF.  3. В правой части сети настроить протокол EIGRP с автономной системой 65001.  4. Маршрут по умолчанию настроить статически в сторону ISP, настроить автомматическое распространение маршрута по умолчанию по сети.  5. Между маршрутизаторами GATE и BRANCH настроить проткол BPG, для GATE автономная система 45002 для BRANCH 45001.  6. Настроить передачу маршрутов для полного согласования сети.  **Подключение к сети интернет**  1. Настроить ретрансляцию адресов на GATE и BRANCH.  **Настройка сервисов**  1. На всех устройствах настроить согласование времени с сервером Google.  2. На RTR настроить DHCP сервер  - распределять сеть для VLAN CLIENT  - в качестве DNS использовать адрес 8.8.8.8  - в качестве шлюза адрес RTR  - первые 20 адресов сети запретить к выдаче.  **Настройка DHCP сервера**  На маршрутизаторе BRANCH сконфигурируйте DHCP сервер.  Обеспечьте возможность доступа в сеть интернет для главного офиса и офиса Branch.  Анонсируйте все сети, необходимые для достижения полной связанности в соответствии со схемой маршрутизации  Настройте аутентификацию.  Преподаватель\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Скиляжнов А.О. |

Министерство образования Красноярского края

краевое государственное бюджетное профессиональное образовательное учреждение «Красноярский колледж радиоэлектроники и информационных технологий»

|  |  |  |  |
| --- | --- | --- | --- |
| |  |  |  | | --- | --- | --- | | |  | | --- | | РАССМОТРЕНО  на заседании цикловой комиссии  преподавателей профессионального  цикла технического профиля  Протокол №\_\_ от «\_\_\_»\_\_\_\_\_\_ 2021 г.  Председатель ЦК \_\_\_\_\_ Е. В. Харитонова | | ДИСЦИПЛИНА  МДК01.02 Организация, принципы построения и функционирования  компьютерных сетей  для специальности  09.02.06 Сетевое и системное\_\_\_\_\_\_\_\_  администрирование\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |   **ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №**  2  1. [Протокол IS-IS: объединение плоскости состояния и вектора пути](https://wiki.merionet.ru/seti/72/protokol-is-is-obedinenie-ploskosti-sostoyaniya-i-vektora-puti/). Сравнение с OSPF. Метрики IS-IS. Маршрутизация IS-IS.  2. Практическое задание. Можно пользоваться Интернет. Схема сети.  Если параметры настройки не указаны в задании, необходимо выбрать любые значения, позволяющие выполнить задание (например номера портов в портовых группах).  **Базовые настройки**  1. Для всего активного сетевого оборудования настройте доменное имя wsr2020.wsr  2. Настройте имена устройств в соответствии с диаграммой  3. Создайте локального пользователя admin с паролем Pass  - пользователь должен обладать максимальным уровнем привилегий.  - пароль должен храниться в виде результата хэш функции.  3. Для всех сетевых устройств сконфигурируйте пароль wsr2020 для входа в привилегированный режим.  4. Все сетевые устройства должны быть доступны для управления по протоколу SSHv2.  5. IP адреса устройств взять с таблицы (или с настроек примера).  **Настройка коммутации**  1. Таблица VLAN офиса HQ должна содержать следующие подсети:  VLAN10:CLIENT  VLAN20:SERV  VLAN1000:MANAGE  2. Транки между коммутаторами должны быть согласованы с использованием DTP. SW1 должен инициировать согласование, SW2 и SW3 должны быть настроены в пассивном режиме  3. Транк между SW2 и SW3 должен быть согласован без использования протокола DTP  4. На портах f0/10 коммутаторов SW2 и SW3 сконфигурируйте магистральные каналы без использования динамического согласования. Отключите протокол DTP явным образом.  **Конфигурация портовых групп.**  1. Между коммутаторами SW1 и SW2 настройте агрегирование по протоколу LACP. SW1 должен работать в активном режиме, SW2 в пассивном  2. Между коммутаторами SW1 и SW3 настройте агрегирование по протоколу PAgP. SW1 должен работать в активном режиме, SW3 в пассивном  3. На SW2 настройте балансировку нагрузки по MAC адресу источника + назначения, на SW3 настройте балансировку по IP адресу источника + назначения  **Сконфигурируйте протокол остовного дерева**  1. На всех коммутаторах используйте протокол, совместимый со стандартом 802.1w  2. Корнем для всех VLAN является SW1. При отказе SW1 корнем должен стать SW2. При отказе SW2 корнем должен стать SW3.  3. На портах f0/10 SW2 и SW3 обеспечьте быструю сходимость, без ожидания протокола 802.1w. Аналогичную настройку произведите на магистральном канале между этими двумя коммутаторами.  **Подключение ISP**  1. Для подключения левого офиса использовать обыкновенный Ethernet  2. Подключение правого офиса выполнить по протоколу PPP  - инкапсуляция PPP  - авторизация по протоколу CHAP  - пароль pass  3. Настроить GRE-туннель между правой и левой частью сети.  **Маршрутизация**  1. Обеспечьте маршрутизацию между сетями VLAN с использованием технологии Router-on-a-Stick.  2. В левой части сети настроить протокол OSPF.  3. В правой части сети настроить протокол EIGRP с автономной системой 65001.  4. Маршрут по умолчанию настроить статически в сторону ISP, настроить автомматическое распространение маршрута по умолчанию по сети.  5. Между маршрутизаторами GATE и BRANCH настроить проткол BPG, для GATE автономная система 45002 для BRANCH 45001.  6. Настроить передачу маршрутов для полного согласования сети.  **Подключение к сети интернет**  1. Настроить ретрансляцию адресов на GATE и BRANCH.  **Настройка сервисов**  1. На всех устройствах настроить согласование времени с сервером Google.  2. На RTR настроить DHCP сервер  - распределять сеть для VLAN CLIENT  - в качестве DNS использовать адрес 8.8.8.8  - в качестве шлюза адрес RTR  - первые 20 адресов сети запретить к выдаче.  **Настройка DHCP сервера**  На маршрутизаторе BRANCH сконфигурируйте DHCP сервер.  Обеспечьте возможность доступа в сеть интернет для главного офиса и офиса Branch.  Анонсируйте все сети, необходимые для достижения полной связанности в соответствии со схемой маршрутизации  Настройте аутентификацию.  Преподаватель\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Скиляжнов А.О. |

Министерство образования Красноярского края

краевое государственное бюджетное профессиональное образовательное учреждение «Красноярский колледж радиоэлектроники и информационных технологий»

|  |  |  |  |
| --- | --- | --- | --- |
| |  |  |  | | --- | --- | --- | | |  | | --- | | РАССМОТРЕНО  на заседании цикловой комиссии  преподавателей профессионального  цикла технического профиля  Протокол №\_\_ от «\_\_\_»\_\_\_\_\_\_ 2021 г.  Председатель ЦК \_\_\_\_\_ Е. В. Харитонова | | ДИСЦИПЛИНА  МДК01.02 Организация, принципы построения и функционирования  компьютерных сетей  для специальности  09.02.06 Сетевое и системное\_\_\_\_\_\_\_\_  администрирование\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |   **ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №**  3   1. [Группы сторон BGP](https://www.cisco.com/c/ru_ru/support/docs/ip/border-gateway-protocol-bgp/13755-29.html#bgppgrp). [Требования к группам сторон](https://www.cisco.com/c/ru_ru/support/docs/ip/border-gateway-protocol-bgp/13755-29.html#pgrpreqs). [Ограничения для групп сторон](https://www.cisco.com/c/ru_ru/support/docs/ip/border-gateway-protocol-bgp/13755-29.html#pgrplimits). [Использование групп сторон](https://www.cisco.com/c/ru_ru/support/docs/ip/border-gateway-protocol-bgp/13755-29.html#usepgrp). [Формат сообщения](https://ru.wikipedia.org/wiki/Border_Gateway_Protocol#%D0%A4%D0%BE%D1%80%D0%BC%D0%B0%D1%82_%D1%81%D0%BE%D0%BE%D0%B1%D1%89%D0%B5%D0%BD%D0%B8%D1%8F). [Обновление информации](https://ru.wikipedia.org/wiki/Border_Gateway_Protocol#%D0%9E%D0%B1%D0%BD%D0%BE%D0%B2%D0%BB%D0%B5%D0%BD%D0%B8%D0%B5_%D0%B8%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%B8). [Сохранение соединения](https://ru.wikipedia.org/wiki/Border_Gateway_Protocol#%D0%A1%D0%BE%D1%85%D1%80%D0%B0%D0%BD%D0%B5%D0%BD%D0%B8%D0%B5_%D1%81%D0%BE%D0%B5%D0%B4%D0%B8%D0%BD%D0%B5%D0%BD%D0%B8%D1%8F). [Оповещение](https://ru.wikipedia.org/wiki/Border_Gateway_Protocol#%D0%9E%D0%BF%D0%BE%D0%B2%D0%B5%D1%89%D0%B5%D0%BD%D0%B8%D0%B5). 2. Практическое задание. Можно пользоваться Интернет. Схема сети.   Если параметры настройки не указаны в задании, необходимо выбрать любые значения, позволяющие выполнить задание (например номера портов в портовых группах).  **Базовые настройки**  1. Для всего активного сетевого оборудования настройте доменное имя wsr2020.wsr  2. Настройте имена устройств в соответствии с диаграммой  3. Создайте локального пользователя admin с паролем Pass  - пользователь должен обладать максимальным уровнем привилегий.  - пароль должен храниться в виде результата хэш функции.  3. Для всех сетевых устройств сконфигурируйте пароль wsr2020 для входа в привилегированный режим.  4. Все сетевые устройства должны быть доступны для управления по протоколу SSHv2.  5. IP адреса устройств взять с таблицы (или с настроек примера).  **Настройка коммутации**  1. Таблица VLAN офиса HQ должна содержать следующие подсети:  VLAN10:CLIENT  VLAN20:SERV  VLAN1000:MANAGE  2. Транки между коммутаторами должны быть согласованы с использованием DTP. SW1 должен инициировать согласование, SW2 и SW3 должны быть настроены в пассивном режиме  3. Транк между SW2 и SW3 должен быть согласован без использования протокола DTP  4. На портах f0/10 коммутаторов SW2 и SW3 сконфигурируйте магистральные каналы без использования динамического согласования. Отключите протокол DTP явным образом.  **Конфигурация портовых групп.**  1. Между коммутаторами SW1 и SW2 настройте агрегирование по протоколу LACP. SW1 должен работать в активном режиме, SW2 в пассивном  2. Между коммутаторами SW1 и SW3 настройте агрегирование по протоколу PAgP. SW1 должен работать в активном режиме, SW3 в пассивном  3. На SW2 настройте балансировку нагрузки по MAC адресу источника + назначения, на SW3 настройте балансировку по IP адресу источника + назначения  **Сконфигурируйте протокол остовного дерева**  1. На всех коммутаторах используйте протокол, совместимый со стандартом 802.1w  2. Корнем для всех VLAN является SW1. При отказе SW1 корнем должен стать SW2. При отказе SW2 корнем должен стать SW3.  3. На портах f0/10 SW2 и SW3 обеспечьте быструю сходимость, без ожидания протокола 802.1w. Аналогичную настройку произведите на магистральном канале между этими двумя коммутаторами.  **Подключение ISP**  1. Для подключения левого офиса использовать обыкновенный Ethernet  2. Подключение правого офиса выполнить по протоколу PPP  - инкапсуляция PPP  - авторизация по протоколу CHAP  - пароль pass  3. Настроить GRE-туннель между правой и левой частью сети.  **Маршрутизация**  1. Обеспечьте маршрутизацию между сетями VLAN с использованием технологии Router-on-a-Stick.  2. В левой части сети настроить протокол OSPF.  3. В правой части сети настроить протокол EIGRP с автономной системой 65001.  4. Маршрут по умолчанию настроить статически в сторону ISP, настроить автомматическое распространение маршрута по умолчанию по сети.  5. Между маршрутизаторами GATE и BRANCH настроить проткол BPG, для GATE автономная система 45002 для BRANCH 45001.  6. Настроить передачу маршрутов для полного согласования сети.  **Подключение к сети интернет**  1. Настроить ретрансляцию адресов на GATE и BRANCH.  **Настройка сервисов**  1. На всех устройствах настроить согласование времени с сервером Google.  2. На RTR настроить DHCP сервер  - распределять сеть для VLAN CLIENT  - в качестве DNS использовать адрес 8.8.8.8  - в качестве шлюза адрес RTR  - первые 20 адресов сети запретить к выдаче.  **Настройка DHCP сервера**  На маршрутизаторе BRANCH сконфигурируйте DHCP сервер.  Обеспечьте возможность доступа в сеть интернет для главного офиса и офиса Branch.  Анонсируйте все сети, необходимые для достижения полной связанности в соответствии со схемой маршрутизации  Настройте аутентификацию.  Преподаватель\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Скиляжнов А.О.. |

Министерство образования Красноярского края

краевое государственное бюджетное профессиональное образовательное учреждение «Красноярский колледж радиоэлектроники и информационных технологий»

|  |  |  |  |
| --- | --- | --- | --- |
| |  |  |  | | --- | --- | --- | | |  | | --- | | РАССМОТРЕНО  на заседании цикловой комиссии  преподавателей профессионального  цикла технического профиля  Протокол №\_\_ от «\_\_\_»\_\_\_\_\_\_ 2021 г.  Председатель ЦК \_\_\_\_\_ Е. В. Харитонова | | ДИСЦИПЛИНА  МДК01.02 Организация, принципы построения и функционирования  компьютерных сетей  для специальности  09.02.06 Сетевое и системное\_\_\_\_\_\_\_\_  администрирование\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |   **ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №**  4   1. [Основные версии протокола](https://www.cisco.com/c/ru_ru/support/docs/ip/enhanced-interior-gateway-routing-protocol-eigrp/16406-eigrp-toc.html#anc2). [Теоретические сведения](https://www.cisco.com/c/ru_ru/support/docs/ip/enhanced-interior-gateway-routing-protocol-eigrp/16406-eigrp-toc.html#anc3). [Обнаружение и обслуживание соседей](https://www.cisco.com/c/ru_ru/support/docs/ip/enhanced-interior-gateway-routing-protocol-eigrp/16406-eigrp-toc.html#anc4). [Создание таблицы топологии](https://www.cisco.com/c/ru_ru/support/docs/ip/enhanced-interior-gateway-routing-protocol-eigrp/16406-eigrp-toc.html#anc5). [Метрика протокола EIGRP](https://www.cisco.com/c/ru_ru/support/docs/ip/enhanced-interior-gateway-routing-protocol-eigrp/16406-eigrp-toc.html#anc6). [Определение беспетлевого пути](https://www.cisco.com/c/ru_ru/support/docs/ip/enhanced-interior-gateway-routing-protocol-eigrp/16406-eigrp-toc.html#anc8) [EIGRP](https://www.cisco.com/c/ru_ru/support/docs/ip/enhanced-interior-gateway-routing-protocol-eigrp/16406-eigrp-toc.html#anc6). 2. Практическое задание. Можно пользоваться Интернет. Схема сети.   Если параметры настройки не указаны в задании, необходимо выбрать любые значения, позволяющие выполнить задание (например номера портов в портовых группах).  **Базовые настройки**  1. Для всего активного сетевого оборудования настройте доменное имя wsr2020.wsr  2. Настройте имена устройств в соответствии с диаграммой  3. Создайте локального пользователя admin с паролем Pass  - пользователь должен обладать максимальным уровнем привилегий.  - пароль должен храниться в виде результата хэш функции.  3. Для всех сетевых устройств сконфигурируйте пароль wsr2020 для входа в привилегированный режим.  4. Все сетевые устройства должны быть доступны для управления по протоколу SSHv2.  5. IP адреса устройств взять с таблицы (или с настроек примера).  **Настройка коммутации**  1. Таблица VLAN офиса HQ должна содержать следующие подсети:  VLAN10:CLIENT  VLAN20:SERV  VLAN1000:MANAGE  2. Транки между коммутаторами должны быть согласованы с использованием DTP. SW1 должен инициировать согласование, SW2 и SW3 должны быть настроены в пассивном режиме  3. Транк между SW2 и SW3 должен быть согласован без использования протокола DTP  4. На портах f0/10 коммутаторов SW2 и SW3 сконфигурируйте магистральные каналы без использования динамического согласования. Отключите протокол DTP явным образом.  **Конфигурация портовых групп.**  1. Между коммутаторами SW1 и SW2 настройте агрегирование по протоколу LACP. SW1 должен работать в активном режиме, SW2 в пассивном  2. Между коммутаторами SW1 и SW3 настройте агрегирование по протоколу PAgP. SW1 должен работать в активном режиме, SW3 в пассивном  3. На SW2 настройте балансировку нагрузки по MAC адресу источника + назначения, на SW3 настройте балансировку по IP адресу источника + назначения  **Сконфигурируйте протокол остовного дерева**  1. На всех коммутаторах используйте протокол, совместимый со стандартом 802.1w  2. Корнем для всех VLAN является SW1. При отказе SW1 корнем должен стать SW2. При отказе SW2 корнем должен стать SW3.  3. На портах f0/10 SW2 и SW3 обеспечьте быструю сходимость, без ожидания протокола 802.1w. Аналогичную настройку произведите на магистральном канале между этими двумя коммутаторами.  **Подключение ISP**  1. Для подключения левого офиса использовать обыкновенный Ethernet  2. Подключение правого офиса выполнить по протоколу PPP  - инкапсуляция PPP  - авторизация по протоколу CHAP  - пароль pass  3. Настроить GRE-туннель между правой и левой частью сети.  **Маршрутизация**  1. Обеспечьте маршрутизацию между сетями VLAN с использованием технологии Router-on-a-Stick.  2. В левой части сети настроить протокол OSPF.  3. В правой части сети настроить протокол EIGRP с автономной системой 65001.  4. Маршрут по умолчанию настроить статически в сторону ISP, настроить автомматическое распространение маршрута по умолчанию по сети.  5. Между маршрутизаторами GATE и BRANCH настроить проткол BPG, для GATE автономная система 45002 для BRANCH 45001.  6. Настроить передачу маршрутов для полного согласования сети.  **Подключение к сети интернет**  1. Настроить ретрансляцию адресов на GATE и BRANCH.  **Настройка сервисов**  1. На всех устройствах настроить согласование времени с сервером Google.  2. На RTR настроить DHCP сервер  - распределять сеть для VLAN CLIENT  - в качестве DNS использовать адрес 8.8.8.8  - в качестве шлюза адрес RTR  - первые 20 адресов сети запретить к выдаче.  **Настройка DHCP сервера**  На маршрутизаторе BRANCH сконфигурируйте DHCP сервер.  Обеспечьте возможность доступа в сеть интернет для главного офиса и офиса Branch.  Анонсируйте все сети, необходимые для достижения полной связанности в соответствии со схемой маршрутизации  Настройте аутентификацию.  Преподаватель\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Скиляжнов А.О. |

Министерство образования Красноярского края

краевое государственное бюджетное профессиональное образовательное учреждение «Красноярский колледж радиоэлектроники и информационных технологий»

|  |  |  |  |
| --- | --- | --- | --- |
| |  |  |  | | --- | --- | --- | | |  | | --- | | РАССМОТРЕНО  на заседании цикловой комиссии  преподавателей профессионального  цикла технического профиля  Протокол №\_\_ от «\_\_\_»\_\_\_\_\_\_ 2021 г.  Председатель ЦК \_\_\_\_\_ Е. В. Харитонова | | ДИСЦИПЛИНА  МДК01.02 Организация, принципы построения и функционирования  компьютерных сетей  для специальности  09.02.06 Сетевое и системное\_\_\_\_\_\_\_\_  администрирование\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |   **ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №**  5  1. Концепции беспроводной связи. Введение в беспроводную связь. Компоненты сетей WLAN. Топологии сетей WLAN 802.11. Принципы работы беспроводной локальной сети.  2. Практическое задание. Можно пользоваться Интернет. Схема сети.  Если параметры настройки не указаны в задании, необходимо выбрать любые значения, позволяющие выполнить задание (например номера портов в портовых группах).  **Базовые настройки**  1. Для всего активного сетевого оборудования настройте доменное имя wsr2020.wsr  2. Настройте имена устройств в соответствии с диаграммой  3. Создайте локального пользователя admin с паролем Pass  - пользователь должен обладать максимальным уровнем привилегий.  - пароль должен храниться в виде результата хэш функции.  3. Для всех сетевых устройств сконфигурируйте пароль wsr2020 для входа в привилегированный режим.  4. Все сетевые устройства должны быть доступны для управления по протоколу SSHv2.  5. IP адреса устройств взять с таблицы (или с настроек примера).  **Настройка коммутации**  1. Таблица VLAN офиса HQ должна содержать следующие подсети:  VLAN10:CLIENT  VLAN20:SERV  VLAN1000:MANAGE  2. Транки между коммутаторами должны быть согласованы с использованием DTP. SW1 должен инициировать согласование, SW2 и SW3 должны быть настроены в пассивном режиме  3. Транк между SW2 и SW3 должен быть согласован без использования протокола DTP  4. На портах f0/10 коммутаторов SW2 и SW3 сконфигурируйте магистральные каналы без использования динамического согласования. Отключите протокол DTP явным образом.  **Конфигурация портовых групп.**  1. Между коммутаторами SW1 и SW2 настройте агрегирование по протоколу LACP. SW1 должен работать в активном режиме, SW2 в пассивном  2. Между коммутаторами SW1 и SW3 настройте агрегирование по протоколу PAgP. SW1 должен работать в активном режиме, SW3 в пассивном  3. На SW2 настройте балансировку нагрузки по MAC адресу источника + назначения, на SW3 настройте балансировку по IP адресу источника + назначения  **Сконфигурируйте протокол остовного дерева**  1. На всех коммутаторах используйте протокол, совместимый со стандартом 802.1w  2. Корнем для всех VLAN является SW1. При отказе SW1 корнем должен стать SW2. При отказе SW2 корнем должен стать SW3.  3. На портах f0/10 SW2 и SW3 обеспечьте быструю сходимость, без ожидания протокола 802.1w. Аналогичную настройку произведите на магистральном канале между этими двумя коммутаторами.  **Подключение ISP**  1. Для подключения левого офиса использовать обыкновенный Ethernet  2. Подключение правого офиса выполнить по протоколу PPP  - инкапсуляция PPP  - авторизация по протоколу CHAP  - пароль pass  3. Настроить GRE-туннель между правой и левой частью сети.  **Маршрутизация**  1. Обеспечьте маршрутизацию между сетями VLAN с использованием технологии Router-on-a-Stick.  2. В левой части сети настроить протокол OSPF.  3. В правой части сети настроить протокол EIGRP с автономной системой 65001.  4. Маршрут по умолчанию настроить статически в сторону ISP, настроить автомматическое распространение маршрута по умолчанию по сети.  5. Между маршрутизаторами GATE и BRANCH настроить проткол BPG, для GATE автономная система 45002 для BRANCH 45001.  6. Настроить передачу маршрутов для полного согласования сети.  **Подключение к сети интернет**  1. Настроить ретрансляцию адресов на GATE и BRANCH.  **Настройка сервисов**  1. На всех устройствах настроить согласование времени с сервером Google.  2. На RTR настроить DHCP сервер  - распределять сеть для VLAN CLIENT  - в качестве DNS использовать адрес 8.8.8.8  - в качестве шлюза адрес RTR  - первые 20 адресов сети запретить к выдаче.  **Настройка DHCP сервера**  На маршрутизаторе BRANCH сконфигурируйте DHCP сервер.  Обеспечьте возможность доступа в сеть интернет для главного офиса и офиса Branch.  Анонсируйте все сети, необходимые для достижения полной связанности в соответствии со схемой маршрутизации  Настройте аутентификацию.  Преподаватель\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Скиляжнов А.О. |

Министерство образования Красноярского края

краевое государственное бюджетное профессиональное образовательное учреждение «Красноярский колледж радиоэлектроники и информационных технологий»

|  |  |  |  |
| --- | --- | --- | --- |
| |  |  |  | | --- | --- | --- | | |  | | --- | | РАССМОТРЕНО  на заседании цикловой комиссии  преподавателей профессионального  цикла технического профиля  Протокол №\_\_ от «\_\_\_»\_\_\_\_\_\_ 2021 г.  Председатель ЦК \_\_\_\_\_ Е. В. Харитонова | | ДИСЦИПЛИНА  МДК01.02 Организация, принципы построения и функционирования  компьютерных сетей  для специальности  09.02.06 Сетевое и системное\_\_\_\_\_\_\_\_  администрирование\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |   **ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №**  6  1. Понятия протокола spanning-tree. Предназначение протокола spanning-tree. Принцип работы STP. Типы протоколов STP. Настройка PVST+. Настройка Rapid PVST+.  2. Практическое задание. Можно пользоваться Интернет. Схема сети.  Если параметры настройки не указаны в задании, необходимо выбрать любые значения, позволяющие выполнить задание (например номера портов в портовых группах).  **Базовые настройки**  1. Для всего активного сетевого оборудования настройте доменное имя wsr2020.wsr  2. Настройте имена устройств в соответствии с диаграммой  3. Создайте локального пользователя admin с паролем Pass  - пользователь должен обладать максимальным уровнем привилегий.  - пароль должен храниться в виде результата хэш функции.  3. Для всех сетевых устройств сконфигурируйте пароль wsr2020 для входа в привилегированный режим.  4. Все сетевые устройства должны быть доступны для управления по протоколу SSHv2.  5. IP адреса устройств взять с таблицы (или с настроек примера).  **Настройка коммутации**  1. Таблица VLAN офиса HQ должна содержать следующие подсети:  VLAN10:CLIENT  VLAN20:SERV  VLAN1000:MANAGE  2. Транки между коммутаторами должны быть согласованы с использованием DTP. SW1 должен инициировать согласование, SW2 и SW3 должны быть настроены в пассивном режиме  3. Транк между SW2 и SW3 должен быть согласован без использования протокола DTP  4. На портах f0/10 коммутаторов SW2 и SW3 сконфигурируйте магистральные каналы без использования динамического согласования. Отключите протокол DTP явным образом.  **Конфигурация портовых групп.**  1. Между коммутаторами SW1 и SW2 настройте агрегирование по протоколу LACP. SW1 должен работать в активном режиме, SW2 в пассивном  2. Между коммутаторами SW1 и SW3 настройте агрегирование по протоколу PAgP. SW1 должен работать в активном режиме, SW3 в пассивном  3. На SW2 настройте балансировку нагрузки по MAC адресу источника + назначения, на SW3 настройте балансировку по IP адресу источника + назначения  **Сконфигурируйте протокол остовного дерева**  1. На всех коммутаторах используйте протокол, совместимый со стандартом 802.1w  2. Корнем для всех VLAN является SW1. При отказе SW1 корнем должен стать SW2. При отказе SW2 корнем должен стать SW3.  3. На портах f0/10 SW2 и SW3 обеспечьте быструю сходимость, без ожидания протокола 802.1w. Аналогичную настройку произведите на магистральном канале между этими двумя коммутаторами.  **Подключение ISP**  1. Для подключения левого офиса использовать обыкновенный Ethernet  2. Подключение правого офиса выполнить по протоколу PPP  - инкапсуляция PPP  - авторизация по протоколу CHAP  - пароль pass  3. Настроить GRE-туннель между правой и левой частью сети.  **Маршрутизация**  1. Обеспечьте маршрутизацию между сетями VLAN с использованием технологии Router-on-a-Stick.  2. В левой части сети настроить протокол OSPF.  3. В правой части сети настроить протокол EIGRP с автономной системой 65001.  4. Маршрут по умолчанию настроить статически в сторону ISP, настроить автомматическое распространение маршрута по умолчанию по сети.  5. Между маршрутизаторами GATE и BRANCH настроить проткол BPG, для GATE автономная система 45002 для BRANCH 45001.  6. Настроить передачу маршрутов для полного согласования сети.  **Подключение к сети интернет**  1. Настроить ретрансляцию адресов на GATE и BRANCH.  **Настройка сервисов**  1. На всех устройствах настроить согласование времени с сервером Google.  2. На RTR настроить DHCP сервер  - распределять сеть для VLAN CLIENT  - в качестве DNS использовать адрес 8.8.8.8  - в качестве шлюза адрес RTR  - первые 20 адресов сети запретить к выдаче.  **Настройка DHCP сервера**  На маршрутизаторе BRANCH сконфигурируйте DHCP сервер.  Обеспечьте возможность доступа в сеть интернет для главного офиса и офиса Branch.  Анонсируйте все сети, необходимые для достижения полной связанности в соответствии со схемой маршрутизации  Настройте аутентификацию.  Преподаватель\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Скиляжнов А.О. |

Министерство образования Красноярского края

краевое государственное бюджетное профессиональное образовательное учреждение «Красноярский колледж радиоэлектроники и информационных технологий»

|  |  |  |  |
| --- | --- | --- | --- |
| |  |  |  | | --- | --- | --- | | |  | | --- | | РАССМОТРЕНО  на заседании цикловой комиссии  преподавателей профессионального  цикла технического профиля  Протокол №\_\_ от «\_\_\_»\_\_\_\_\_\_ 2021 г.  Председатель ЦК \_\_\_\_\_ Е. В. Харитонова | | ДИСЦИПЛИНА  МДК01.02 Организация, принципы построения и функционирования  компьютерных сетей  для специальности  09.02.06 Сетевое и системное\_\_\_\_\_\_\_\_  администрирование\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |   **ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №**  7  1. Статическое и динамическое преобразование сетевых адресов (NAT). Преобразование адресов портов (PAT). Сравнение NAT и PAT.  2. Практическое задание. Можно пользоваться Интернет. Схема сети.  Если параметры настройки не указаны в задании, необходимо выбрать любые значения, позволяющие выполнить задание (например номера портов в портовых группах).  **Базовые настройки**  1. Для всего активного сетевого оборудования настройте доменное имя wsr2020.wsr  2. Настройте имена устройств в соответствии с диаграммой  3. Создайте локального пользователя admin с паролем Pass  - пользователь должен обладать максимальным уровнем привилегий.  - пароль должен храниться в виде результата хэш функции.  3. Для всех сетевых устройств сконфигурируйте пароль wsr2020 для входа в привилегированный режим.  4. Все сетевые устройства должны быть доступны для управления по протоколу SSHv2.  5. IP адреса устройств взять с таблицы (или с настроек примера).  **Настройка коммутации**  1. Таблица VLAN офиса HQ должна содержать следующие подсети:  VLAN10:CLIENT  VLAN20:SERV  VLAN1000:MANAGE  2. Транки между коммутаторами должны быть согласованы с использованием DTP. SW1 должен инициировать согласование, SW2 и SW3 должны быть настроены в пассивном режиме  3. Транк между SW2 и SW3 должен быть согласован без использования протокола DTP  4. На портах f0/10 коммутаторов SW2 и SW3 сконфигурируйте магистральные каналы без использования динамического согласования. Отключите протокол DTP явным образом.  **Конфигурация портовых групп.**  1. Между коммутаторами SW1 и SW2 настройте агрегирование по протоколу LACP. SW1 должен работать в активном режиме, SW2 в пассивном  2. Между коммутаторами SW1 и SW3 настройте агрегирование по протоколу PAgP. SW1 должен работать в активном режиме, SW3 в пассивном  3. На SW2 настройте балансировку нагрузки по MAC адресу источника + назначения, на SW3 настройте балансировку по IP адресу источника + назначения  **Сконфигурируйте протокол остовного дерева**  1. На всех коммутаторах используйте протокол, совместимый со стандартом 802.1w  2. Корнем для всех VLAN является SW1. При отказе SW1 корнем должен стать SW2. При отказе SW2 корнем должен стать SW3.  3. На портах f0/10 SW2 и SW3 обеспечьте быструю сходимость, без ожидания протокола 802.1w. Аналогичную настройку произведите на магистральном канале между этими двумя коммутаторами.  **Подключение ISP**  1. Для подключения левого офиса использовать обыкновенный Ethernet  2. Подключение правого офиса выполнить по протоколу PPP  - инкапсуляция PPP  - авторизация по протоколу CHAP  - пароль pass  3. Настроить GRE-туннель между правой и левой частью сети.  **Маршрутизация**  1. Обеспечьте маршрутизацию между сетями VLAN с использованием технологии Router-on-a-Stick.  2. В левой части сети настроить протокол OSPF.  3. В правой части сети настроить протокол EIGRP с автономной системой 65001.  4. Маршрут по умолчанию настроить статически в сторону ISP, настроить автомматическое распространение маршрута по умолчанию по сети.  5. Между маршрутизаторами GATE и BRANCH настроить проткол BPG, для GATE автономная система 45002 для BRANCH 45001.  6. Настроить передачу маршрутов для полного согласования сети.  **Подключение к сети интернет**  1. Настроить ретрансляцию адресов на GATE и BRANCH.  **Настройка сервисов**  1. На всех устройствах настроить согласование времени с сервером Google.  2. На RTR настроить DHCP сервер  - распределять сеть для VLAN CLIENT  - в качестве DNS использовать адрес 8.8.8.8  - в качестве шлюза адрес RTR  - первые 20 адресов сети запретить к выдаче.  **Настройка DHCP сервера**  На маршрутизаторе BRANCH сконфигурируйте DHCP сервер.  Обеспечьте возможность доступа в сеть интернет для главного офиса и офиса Branch.  Анонсируйте все сети, необходимые для достижения полной связанности в соответствии со схемой маршрутизации  Настройте аутентификацию.  Преподаватель\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Скиляжнов А.О. |

Министерство образования Красноярского края

краевое государственное бюджетное профессиональное образовательное учреждение «Красноярский колледж радиоэлектроники и информационных технологий»

|  |  |  |  |
| --- | --- | --- | --- |
| |  |  |  | | --- | --- | --- | | |  | | --- | | РАССМОТРЕНО  на заседании цикловой комиссии  преподавателей профессионального  цикла технического профиля  Протокол №\_\_ от «\_\_\_»\_\_\_\_\_\_ 2021 г.  Председатель ЦК \_\_\_\_\_ Е. В. Харитонова | | ДИСЦИПЛИНА  МДК01.02 Организация, принципы построения и функционирования  компьютерных сетей  для специальности  09.02.06 Сетевое и системное\_\_\_\_\_\_\_\_  администрирование\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |   **ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №**  8  1. Преобразование сетевых адресов IPv4. Концептуальное преобразование сетевых адресов (NAT). Терминология и принципы работы NAT. Пространство частных IPv4-адресов.  2. Практическое задание. Можно пользоваться Интернет. Схема сети.  Если параметры настройки не указаны в задании, необходимо выбрать любые значения, позволяющие выполнить задание (например номера портов в портовых группах).  **Базовые настройки**  1. Для всего активного сетевого оборудования настройте доменное имя wsr2020.wsr  2. Настройте имена устройств в соответствии с диаграммой  3. Создайте локального пользователя admin с паролем Pass  - пользователь должен обладать максимальным уровнем привилегий.  - пароль должен храниться в виде результата хэш функции.  3. Для всех сетевых устройств сконфигурируйте пароль wsr2020 для входа в привилегированный режим.  4. Все сетевые устройства должны быть доступны для управления по протоколу SSHv2.  5. IP адреса устройств взять с таблицы (или с настроек примера).  **Настройка коммутации**  1. Таблица VLAN офиса HQ должна содержать следующие подсети:  VLAN10:CLIENT  VLAN20:SERV  VLAN1000:MANAGE  2. Транки между коммутаторами должны быть согласованы с использованием DTP. SW1 должен инициировать согласование, SW2 и SW3 должны быть настроены в пассивном режиме  3. Транк между SW2 и SW3 должен быть согласован без использования протокола DTP  4. На портах f0/10 коммутаторов SW2 и SW3 сконфигурируйте магистральные каналы без использования динамического согласования. Отключите протокол DTP явным образом.  **Конфигурация портовых групп.**  1. Между коммутаторами SW1 и SW2 настройте агрегирование по протоколу LACP. SW1 должен работать в активном режиме, SW2 в пассивном  2. Между коммутаторами SW1 и SW3 настройте агрегирование по протоколу PAgP. SW1 должен работать в активном режиме, SW3 в пассивном  3. На SW2 настройте балансировку нагрузки по MAC адресу источника + назначения, на SW3 настройте балансировку по IP адресу источника + назначения  **Сконфигурируйте протокол остовного дерева**  1. На всех коммутаторах используйте протокол, совместимый со стандартом 802.1w  2. Корнем для всех VLAN является SW1. При отказе SW1 корнем должен стать SW2. При отказе SW2 корнем должен стать SW3.  3. На портах f0/10 SW2 и SW3 обеспечьте быструю сходимость, без ожидания протокола 802.1w. Аналогичную настройку произведите на магистральном канале между этими двумя коммутаторами.  **Подключение ISP**  1. Для подключения левого офиса использовать обыкновенный Ethernet  2. Подключение правого офиса выполнить по протоколу PPP  - инкапсуляция PPP  - авторизация по протоколу CHAP  - пароль pass  3. Настроить GRE-туннель между правой и левой частью сети.  **Маршрутизация**  1. Обеспечьте маршрутизацию между сетями VLAN с использованием технологии Router-on-a-Stick.  2. В левой части сети настроить протокол OSPF.  3. В правой части сети настроить протокол EIGRP с автономной системой 65001.  4. Маршрут по умолчанию настроить статически в сторону ISP, настроить автомматическое распространение маршрута по умолчанию по сети.  5. Между маршрутизаторами GATE и BRANCH настроить проткол BPG, для GATE автономная система 45002 для BRANCH 45001.  6. Настроить передачу маршрутов для полного согласования сети.  **Подключение к сети интернет**  1. Настроить ретрансляцию адресов на GATE и BRANCH.  **Настройка сервисов**  1. На всех устройствах настроить согласование времени с сервером Google.  2. На RTR настроить DHCP сервер  - распределять сеть для VLAN CLIENT  - в качестве DNS использовать адрес 8.8.8.8  - в качестве шлюза адрес RTR  - первые 20 адресов сети запретить к выдаче.  **Настройка DHCP сервера**  На маршрутизаторе BRANCH сконфигурируйте DHCP сервер.  Обеспечьте возможность доступа в сеть интернет для главного офиса и офиса Branch.  Анонсируйте все сети, необходимые для достижения полной связанности в соответствии со схемой маршрутизации  Настройте аутентификацию.  Преподаватель\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Скиляжнов А.О. |

Министерство образования Красноярского края

краевое государственное бюджетное профессиональное образовательное учреждение «Красноярский колледж радиоэлектроники и информационных технологий»

|  |  |  |  |
| --- | --- | --- | --- |
| |  |  |  | | --- | --- | --- | | |  | | --- | | РАССМОТРЕНО  на заседании цикловой комиссии  преподавателей профессионального  цикла технического профиля  Протокол №\_\_ от «\_\_\_»\_\_\_\_\_\_ 2021 г.  Председатель ЦК \_\_\_\_\_ Е. В. Харитонова | | ДИСЦИПЛИНА  МДК01.02 Организация, принципы построения и функционирования  компьютерных сетей  для специальности  09.02.06 Сетевое и системное\_\_\_\_\_\_\_\_  администрирование\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Семестр 4 группа 9САД1.20, 9САД2.20 |   **ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №**  9  1. Автоматическая настройка адреса без отслеживания состояния (SLAAC). Принцип работы SLAAC с DHCPv6. DHCPv6 с и без отслеживания состояния. Процессы DHCPv6.  2. Практическое задание. Можно пользоваться Интернет. Схема сети.  Если параметры настройки не указаны в задании, необходимо выбрать любые значения, позволяющие выполнить задание (например номера портов в портовых группах).  **Базовые настройки**  1. Для всего активного сетевого оборудования настройте доменное имя wsr2020.wsr  2. Настройте имена устройств в соответствии с диаграммой  3. Создайте локального пользователя admin с паролем Pass  - пользователь должен обладать максимальным уровнем привилегий.  - пароль должен храниться в виде результата хэш функции.  3. Для всех сетевых устройств сконфигурируйте пароль wsr2020 для входа в привилегированный режим.  4. Все сетевые устройства должны быть доступны для управления по протоколу SSHv2.  5. IP адреса устройств взять с таблицы (или с настроек примера).  **Настройка коммутации**  1. Таблица VLAN офиса HQ должна содержать следующие подсети:  VLAN10:CLIENT  VLAN20:SERV  VLAN1000:MANAGE  2. Транки между коммутаторами должны быть согласованы с использованием DTP. SW1 должен инициировать согласование, SW2 и SW3 должны быть настроены в пассивном режиме  3. Транк между SW2 и SW3 должен быть согласован без использования протокола DTP  4. На портах f0/10 коммутаторов SW2 и SW3 сконфигурируйте магистральные каналы без использования динамического согласования. Отключите протокол DTP явным образом.  **Конфигурация портовых групп.**  1. Между коммутаторами SW1 и SW2 настройте агрегирование по протоколу LACP. SW1 должен работать в активном режиме, SW2 в пассивном  2. Между коммутаторами SW1 и SW3 настройте агрегирование по протоколу PAgP. SW1 должен работать в активном режиме, SW3 в пассивном  3. На SW2 настройте балансировку нагрузки по MAC адресу источника + назначения, на SW3 настройте балансировку по IP адресу источника + назначения  **Сконфигурируйте протокол остовного дерева**  1. На всех коммутаторах используйте протокол, совместимый со стандартом 802.1w  2. Корнем для всех VLAN является SW1. При отказе SW1 корнем должен стать SW2. При отказе SW2 корнем должен стать SW3.  3. На портах f0/10 SW2 и SW3 обеспечьте быструю сходимость, без ожидания протокола 802.1w. Аналогичную настройку произведите на магистральном канале между этими двумя коммутаторами.  **Подключение ISP**  1. Для подключения левого офиса использовать обыкновенный Ethernet  2. Подключение правого офиса выполнить по протоколу PPP  - инкапсуляция PPP  - авторизация по протоколу CHAP  - пароль pass  3. Настроить GRE-туннель между правой и левой частью сети.  **Маршрутизация**  1. Обеспечьте маршрутизацию между сетями VLAN с использованием технологии Router-on-a-Stick.  2. В левой части сети настроить протокол OSPF.  3. В правой части сети настроить протокол EIGRP с автономной системой 65001.  4. Маршрут по умолчанию настроить статически в сторону ISP, настроить автомматическое распространение маршрута по умолчанию по сети.  5. Между маршрутизаторами GATE и BRANCH настроить проткол BPG, для GATE автономная система 45002 для BRANCH 45001.  6. Настроить передачу маршрутов для полного согласования сети.  **Подключение к сети интернет**  1. Настроить ретрансляцию адресов на GATE и BRANCH.  **Настройка сервисов**  1. На всех устройствах настроить согласование времени с сервером Google.  2. На RTR настроить DHCP сервер  - распределять сеть для VLAN CLIENT  - в качестве DNS использовать адрес 8.8.8.8  - в качестве шлюза адрес RTR  - первые 20 адресов сети запретить к выдаче.  **Настройка DHCP сервера**  На маршрутизаторе BRANCH сконфигурируйте DHCP сервер.  Обеспечьте возможность доступа в сеть интернет для главного офиса и офиса Branch.  Анонсируйте все сети, необходимые для достижения полной связанности в соответствии со схемой маршрутизации  Настройте аутентификацию.  Преподаватель\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Скиляжнов А.О. |

Министерство образования Красноярского края

краевое государственное бюджетное профессиональное образовательное учреждение «Красноярский колледж радиоэлектроники и информационных технологий»

|  |  |  |  |
| --- | --- | --- | --- |
| |  |  |  | | --- | --- | --- | | |  | | --- | | РАССМОТРЕНО  на заседании цикловой комиссии  преподавателей профессионального  цикла технического профиля  Протокол №\_\_ от «\_\_\_»\_\_\_\_\_\_ 2021 г.  Председатель ЦК \_\_\_\_\_ Е. В. Харитонова | | ДИСЦИПЛИНА  МДК01.02 Организация, принципы построения и функционирования  компьютерных сетей  для специальности  09.02.06 Сетевое и системное\_\_\_\_\_\_\_\_  администрирование\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Семестр 4 группа 9САД1.20, 9САД2.20 |   **ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №**  10  1. Протокол DHCPv4: базовая операция, формат сообщений, сообщения обнаружения и предложения. Настройка, проверка и ретрансляция простого DHCPv4-сервера. Настройка маршрутизатора в качестве DHCPv4-клиента.  2. Практическое задание. Можно пользоваться Интернет. Схема сети.  Если параметры настройки не указаны в задании, необходимо выбрать любые значения, позволяющие выполнить задание (например номера портов в портовых группах).  **Базовые настройки**  1. Для всего активного сетевого оборудования настройте доменное имя wsr2020.wsr  2. Настройте имена устройств в соответствии с диаграммой  3. Создайте локального пользователя admin с паролем Pass  - пользователь должен обладать максимальным уровнем привилегий.  - пароль должен храниться в виде результата хэш функции.  3. Для всех сетевых устройств сконфигурируйте пароль wsr2020 для входа в привилегированный режим.  4. Все сетевые устройства должны быть доступны для управления по протоколу SSHv2.  5. IP адреса устройств взять с таблицы (или с настроек примера).  **Настройка коммутации**  1. Таблица VLAN офиса HQ должна содержать следующие подсети:  VLAN10:CLIENT  VLAN20:SERV  VLAN1000:MANAGE  2. Транки между коммутаторами должны быть согласованы с использованием DTP. SW1 должен инициировать согласование, SW2 и SW3 должны быть настроены в пассивном режиме  3. Транк между SW2 и SW3 должен быть согласован без использования протокола DTP  4. На портах f0/10 коммутаторов SW2 и SW3 сконфигурируйте магистральные каналы без использования динамического согласования. Отключите протокол DTP явным образом.  **Конфигурация портовых групп.**  1. Между коммутаторами SW1 и SW2 настройте агрегирование по протоколу LACP. SW1 должен работать в активном режиме, SW2 в пассивном  2. Между коммутаторами SW1 и SW3 настройте агрегирование по протоколу PAgP. SW1 должен работать в активном режиме, SW3 в пассивном  3. На SW2 настройте балансировку нагрузки по MAC адресу источника + назначения, на SW3 настройте балансировку по IP адресу источника + назначения  **Сконфигурируйте протокол остовного дерева**  1. На всех коммутаторах используйте протокол, совместимый со стандартом 802.1w  2. Корнем для всех VLAN является SW1. При отказе SW1 корнем должен стать SW2. При отказе SW2 корнем должен стать SW3.  3. На портах f0/10 SW2 и SW3 обеспечьте быструю сходимость, без ожидания протокола 802.1w. Аналогичную настройку произведите на магистральном канале между этими двумя коммутаторами.  **Подключение ISP**  1. Для подключения левого офиса использовать обыкновенный Ethernet  2. Подключение правого офиса выполнить по протоколу PPP  - инкапсуляция PPP  - авторизация по протоколу CHAP  - пароль pass  3. Настроить GRE-туннель между правой и левой частью сети.  **Маршрутизация**  1. Обеспечьте маршрутизацию между сетями VLAN с использованием технологии Router-on-a-Stick.  2. В левой части сети настроить протокол OSPF.  3. В правой части сети настроить протокол EIGRP с автономной системой 65001.  4. Маршрут по умолчанию настроить статически в сторону ISP, настроить автомматическое распространение маршрута по умолчанию по сети.  5. Между маршрутизаторами GATE и BRANCH настроить проткол BPG, для GATE автономная система 45002 для BRANCH 45001.  6. Настроить передачу маршрутов для полного согласования сети.  **Подключение к сети интернет**  1. Настроить ретрансляцию адресов на GATE и BRANCH.  **Настройка сервисов**  1. На всех устройствах настроить согласование времени с сервером Google.  2. На RTR настроить DHCP сервер  - распределять сеть для VLAN CLIENT  - в качестве DNS использовать адрес 8.8.8.8  - в качестве шлюза адрес RTR  - первые 20 адресов сети запретить к выдаче.  **Настройка DHCP сервера**  На маршрутизаторе BRANCH сконфигурируйте DHCP сервер.  Обеспечьте возможность доступа в сеть интернет для главного офиса и офиса Branch.  Анонсируйте все сети, необходимые для достижения полной связанности в соответствии со схемой маршрутизации  Настройте аутентификацию.  Преподаватель\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Скиляжнов А.О. |

Министерство образования Красноярского края

краевое государственное бюджетное профессиональное образовательное учреждение «Красноярский колледж радиоэлектроники и информационных технологий»

|  |  |  |  |
| --- | --- | --- | --- |
| |  |  |  | | --- | --- | --- | | |  | | --- | | РАССМОТРЕНО  на заседании цикловой комиссии  преподавателей профессионального  цикла технического профиля  Протокол №\_\_ от «\_\_\_»\_\_\_\_\_\_ 2021 г.  Председатель ЦК \_\_\_\_\_ Е. В. Харитонова | | ДИСЦИПЛИНА  МДК01.02 Организация, принципы построения и функционирования  компьютерных сетей  для специальности  09.02.06 Сетевое и системное\_\_\_\_\_\_\_\_  администрирование\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Семестр 4 группа 9САД1.20, 9САД2.20 |   **ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №**  11  1. Структура и настройка расширенных ACL-списков для IPv4. Фильтрация трафика с использованием расширенных ACL-списков. Сравнение ACL-списков для IPv4 и IPv6.  2. Практическое задание. Можно пользоваться Интернет. Схема сети.  Если параметры настройки не указаны в задании, необходимо выбрать любые значения, позволяющие выполнить задание (например номера портов в портовых группах).  **Базовые настройки**  1. Для всего активного сетевого оборудования настройте доменное имя wsr2020.wsr  2. Настройте имена устройств в соответствии с диаграммой  3. Создайте локального пользователя admin с паролем Pass  - пользователь должен обладать максимальным уровнем привилегий.  - пароль должен храниться в виде результата хэш функции.  3. Для всех сетевых устройств сконфигурируйте пароль wsr2020 для входа в привилегированный режим.  4. Все сетевые устройства должны быть доступны для управления по протоколу SSHv2.  5. IP адреса устройств взять с таблицы (или с настроек примера).  **Настройка коммутации**  1. Таблица VLAN офиса HQ должна содержать следующие подсети:  VLAN10:CLIENT  VLAN20:SERV  VLAN1000:MANAGE  2. Транки между коммутаторами должны быть согласованы с использованием DTP. SW1 должен инициировать согласование, SW2 и SW3 должны быть настроены в пассивном режиме  3. Транк между SW2 и SW3 должен быть согласован без использования протокола DTP  4. На портах f0/10 коммутаторов SW2 и SW3 сконфигурируйте магистральные каналы без использования динамического согласования. Отключите протокол DTP явным образом.  **Конфигурация портовых групп.**  1. Между коммутаторами SW1 и SW2 настройте агрегирование по протоколу LACP. SW1 должен работать в активном режиме, SW2 в пассивном  2. Между коммутаторами SW1 и SW3 настройте агрегирование по протоколу PAgP. SW1 должен работать в активном режиме, SW3 в пассивном  3. На SW2 настройте балансировку нагрузки по MAC адресу источника + назначения, на SW3 настройте балансировку по IP адресу источника + назначения  **Сконфигурируйте протокол остовного дерева**  1. На всех коммутаторах используйте протокол, совместимый со стандартом 802.1w  2. Корнем для всех VLAN является SW1. При отказе SW1 корнем должен стать SW2. При отказе SW2 корнем должен стать SW3.  3. На портах f0/10 SW2 и SW3 обеспечьте быструю сходимость, без ожидания протокола 802.1w. Аналогичную настройку произведите на магистральном канале между этими двумя коммутаторами.  **Подключение ISP**  1. Для подключения левого офиса использовать обыкновенный Ethernet  2. Подключение правого офиса выполнить по протоколу PPP  - инкапсуляция PPP  - авторизация по протоколу CHAP  - пароль pass  3. Настроить GRE-туннель между правой и левой частью сети.  **Маршрутизация**  1. Обеспечьте маршрутизацию между сетями VLAN с использованием технологии Router-on-a-Stick.  2. В левой части сети настроить протокол OSPF.  3. В правой части сети настроить протокол EIGRP с автономной системой 65001.  4. Маршрут по умолчанию настроить статически в сторону ISP, настроить автомматическое распространение маршрута по умолчанию по сети.  5. Между маршрутизаторами GATE и BRANCH настроить проткол BPG, для GATE автономная система 45002 для BRANCH 45001.  6. Настроить передачу маршрутов для полного согласования сети.  **Подключение к сети интернет**  1. Настроить ретрансляцию адресов на GATE и BRANCH.  **Настройка сервисов**  1. На всех устройствах настроить согласование времени с сервером Google.  2. На RTR настроить DHCP сервер  - распределять сеть для VLAN CLIENT  - в качестве DNS использовать адрес 8.8.8.8  - в качестве шлюза адрес RTR  - первые 20 адресов сети запретить к выдаче.  **Настройка DHCP сервера**  На маршрутизаторе BRANCH сконфигурируйте DHCP сервер.  Обеспечьте возможность доступа в сеть интернет для главного офиса и офиса Branch.  Анонсируйте все сети, необходимые для достижения полной связанности в соответствии со схемой маршрутизации  Настройте аутентификацию.  Преподаватель\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Скиляжнов А.О. |

Министерство образования Красноярского края

краевое государственное бюджетное профессиональное образовательное учреждение «Красноярский колледж радиоэлектроники и информационных технологий»

|  |  |  |  |
| --- | --- | --- | --- |
| |  |  |  | | --- | --- | --- | | |  | | --- | | РАССМОТРЕНО  на заседании цикловой комиссии  преподавателей профессионального  цикла технического профиля  Протокол №\_\_ от «\_\_\_»\_\_\_\_\_\_ 2021 г.  Председатель ЦК \_\_\_\_\_ Е. В. Харитонова | | ДИСЦИПЛИНА  МДК01.02 Организация, принципы построения и функционирования  компьютерных сетей  для специальности  09.02.06 Сетевое и системное\_\_\_\_\_\_\_\_  администрирование\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Семестр 4 группа 9САД1.20, 9САД2.20 |   **ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №**  12  1. Расчёт шаблонной маски в ACL-списках. Рекомендации по созданию и размещению ACL-списков. Защита портов VTY с помощью стандартного ACL-списка IPv4.  2. Практическое задание. Можно пользоваться Интернет. Схема сети.  Если параметры настройки не указаны в задании, необходимо выбрать любые значения, позволяющие выполнить задание (например номера портов в портовых группах).  **Базовые настройки**  1. Для всего активного сетевого оборудования настройте доменное имя wsr2020.wsr  2. Настройте имена устройств в соответствии с диаграммой  3. Создайте локального пользователя admin с паролем Pass  - пользователь должен обладать максимальным уровнем привилегий.  - пароль должен храниться в виде результата хэш функции.  3. Для всех сетевых устройств сконфигурируйте пароль wsr2020 для входа в привилегированный режим.  4. Все сетевые устройства должны быть доступны для управления по протоколу SSHv2.  5. IP адреса устройств взять с таблицы (или с настроек примера).  **Настройка коммутации**  1. Таблица VLAN офиса HQ должна содержать следующие подсети:  VLAN10:CLIENT  VLAN20:SERV  VLAN1000:MANAGE  2. Транки между коммутаторами должны быть согласованы с использованием DTP. SW1 должен инициировать согласование, SW2 и SW3 должны быть настроены в пассивном режиме  3. Транк между SW2 и SW3 должен быть согласован без использования протокола DTP  4. На портах f0/10 коммутаторов SW2 и SW3 сконфигурируйте магистральные каналы без использования динамического согласования. Отключите протокол DTP явным образом.  **Конфигурация портовых групп.**  1. Между коммутаторами SW1 и SW2 настройте агрегирование по протоколу LACP. SW1 должен работать в активном режиме, SW2 в пассивном  2. Между коммутаторами SW1 и SW3 настройте агрегирование по протоколу PAgP. SW1 должен работать в активном режиме, SW3 в пассивном  3. На SW2 настройте балансировку нагрузки по MAC адресу источника + назначения, на SW3 настройте балансировку по IP адресу источника + назначения  **Сконфигурируйте протокол остовного дерева**  1. На всех коммутаторах используйте протокол, совместимый со стандартом 802.1w  2. Корнем для всех VLAN является SW1. При отказе SW1 корнем должен стать SW2. При отказе SW2 корнем должен стать SW3.  3. На портах f0/10 SW2 и SW3 обеспечьте быструю сходимость, без ожидания протокола 802.1w. Аналогичную настройку произведите на магистральном канале между этими двумя коммутаторами.  **Подключение ISP**  1. Для подключения левого офиса использовать обыкновенный Ethernet  2. Подключение правого офиса выполнить по протоколу PPP  - инкапсуляция PPP  - авторизация по протоколу CHAP  - пароль pass  3. Настроить GRE-туннель между правой и левой частью сети.  **Маршрутизация**  1. Обеспечьте маршрутизацию между сетями VLAN с использованием технологии Router-on-a-Stick.  2. В левой части сети настроить протокол OSPF.  3. В правой части сети настроить протокол EIGRP с автономной системой 65001.  4. Маршрут по умолчанию настроить статически в сторону ISP, настроить автомматическое распространение маршрута по умолчанию по сети.  5. Между маршрутизаторами GATE и BRANCH настроить проткол BPG, для GATE автономная система 45002 для BRANCH 45001.  6. Настроить передачу маршрутов для полного согласования сети.  **Подключение к сети интернет**  1. Настроить ретрансляцию адресов на GATE и BRANCH.  **Настройка сервисов**  1. На всех устройствах настроить согласование времени с сервером Google.  2. На RTR настроить DHCP сервер  - распределять сеть для VLAN CLIENT  - в качестве DNS использовать адрес 8.8.8.8  - в качестве шлюза адрес RTR  - первые 20 адресов сети запретить к выдаче.  **Настройка DHCP сервера**  На маршрутизаторе BRANCH сконфигурируйте DHCP сервер.  Обеспечьте возможность доступа в сеть интернет для главного офиса и офиса Branch.  Анонсируйте все сети, необходимые для достижения полной связанности в соответствии со схемой маршрутизации  Настройте аутентификацию.  Преподаватель\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Скиляжнов А.О. |

Министерство образования Красноярского края

краевое государственное бюджетное профессиональное образовательное учреждение «Красноярский колледж радиоэлектроники и информационных технологий»

|  |  |  |  |
| --- | --- | --- | --- |
| |  |  |  | | --- | --- | --- | | |  | | --- | | РАССМОТРЕНО  на заседании цикловой комиссии  преподавателей профессионального  цикла технического профиля  Протокол №\_\_ от «\_\_\_»\_\_\_\_\_\_ 2021 г.  Председатель ЦК \_\_\_\_\_ Е. В. Харитонова | | ДИСЦИПЛИНА  МДК01.02 Организация, принципы построения и функционирования  компьютерных сетей  для специальности  09.02.06 Сетевое и системное\_\_\_\_\_\_\_\_  администрирование\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Семестр 4 группа 9САД1.20, 9САД2.20 |   **ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №**  13  1. Списки контроля доступа (ACL). Принцип работы ACL списков. Типы ACL-списков Cisco для IPv4. Присваивание номеров и имён ACL-спискам.  2. Практическое задание. Можно пользоваться Интернет. Схема сети.  Если параметры настройки не указаны в задании, необходимо выбрать любые значения, позволяющие выполнить задание (например номера портов в портовых группах).  **Базовые настройки**  1. Для всего активного сетевого оборудования настройте доменное имя wsr2020.wsr  2. Настройте имена устройств в соответствии с диаграммой  3. Создайте локального пользователя admin с паролем Pass  - пользователь должен обладать максимальным уровнем привилегий.  - пароль должен храниться в виде результата хэш функции.  3. Для всех сетевых устройств сконфигурируйте пароль wsr2020 для входа в привилегированный режим.  4. Все сетевые устройства должны быть доступны для управления по протоколу SSHv2.  5. IP адреса устройств взять с таблицы (или с настроек примера).  **Настройка коммутации**  1. Таблица VLAN офиса HQ должна содержать следующие подсети:  VLAN10:CLIENT  VLAN20:SERV  VLAN1000:MANAGE  2. Транки между коммутаторами должны быть согласованы с использованием DTP. SW1 должен инициировать согласование, SW2 и SW3 должны быть настроены в пассивном режиме  3. Транк между SW2 и SW3 должен быть согласован без использования протокола DTP  4. На портах f0/10 коммутаторов SW2 и SW3 сконфигурируйте магистральные каналы без использования динамического согласования. Отключите протокол DTP явным образом.  **Конфигурация портовых групп.**  1. Между коммутаторами SW1 и SW2 настройте агрегирование по протоколу LACP. SW1 должен работать в активном режиме, SW2 в пассивном  2. Между коммутаторами SW1 и SW3 настройте агрегирование по протоколу PAgP. SW1 должен работать в активном режиме, SW3 в пассивном  3. На SW2 настройте балансировку нагрузки по MAC адресу источника + назначения, на SW3 настройте балансировку по IP адресу источника + назначения  **Сконфигурируйте протокол остовного дерева**  1. На всех коммутаторах используйте протокол, совместимый со стандартом 802.1w  2. Корнем для всех VLAN является SW1. При отказе SW1 корнем должен стать SW2. При отказе SW2 корнем должен стать SW3.  3. На портах f0/10 SW2 и SW3 обеспечьте быструю сходимость, без ожидания протокола 802.1w. Аналогичную настройку произведите на магистральном канале между этими двумя коммутаторами.  **Подключение ISP**  1. Для подключения левого офиса использовать обыкновенный Ethernet  2. Подключение правого офиса выполнить по протоколу PPP  - инкапсуляция PPP  - авторизация по протоколу CHAP  - пароль pass  3. Настроить GRE-туннель между правой и левой частью сети.  **Маршрутизация**  1. Обеспечьте маршрутизацию между сетями VLAN с использованием технологии Router-on-a-Stick.  2. В левой части сети настроить протокол OSPF.  3. В правой части сети настроить протокол EIGRP с автономной системой 65001.  4. Маршрут по умолчанию настроить статически в сторону ISP, настроить автомматическое распространение маршрута по умолчанию по сети.  5. Между маршрутизаторами GATE и BRANCH настроить проткол BPG, для GATE автономная система 45002 для BRANCH 45001.  6. Настроить передачу маршрутов для полного согласования сети.  **Подключение к сети интернет**  1. Настроить ретрансляцию адресов на GATE и BRANCH.  **Настройка сервисов**  1. На всех устройствах настроить согласование времени с сервером Google.  2. На RTR настроить DHCP сервер  - распределять сеть для VLAN CLIENT  - в качестве DNS использовать адрес 8.8.8.8  - в качестве шлюза адрес RTR  - первые 20 адресов сети запретить к выдаче.  **Настройка DHCP сервера**  На маршрутизаторе BRANCH сконфигурируйте DHCP сервер.  Обеспечьте возможность доступа в сеть интернет для главного офиса и офиса Branch.  Анонсируйте все сети, необходимые для достижения полной связанности в соответствии со схемой маршрутизации  Настройте аутентификацию.  Преподаватель\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Скиляжнов А.О. |

Министерство образования Красноярского края

краевое государственное бюджетное профессиональное образовательное учреждение «Красноярский колледж радиоэлектроники и информационных технологий»

|  |  |  |  |
| --- | --- | --- | --- |
| |  |  |  | | --- | --- | --- | | |  | | --- | | РАССМОТРЕНО  на заседании цикловой комиссии  преподавателей профессионального  цикла технического профиля  Протокол №\_\_ от «\_\_\_»\_\_\_\_\_\_ 2021 г.  Председатель ЦК \_\_\_\_\_ Е. В. Харитонова | | ДИСЦИПЛИНА  МДК01.02 Организация, принципы построения и функционирования  компьютерных сетей  для специальности  09.02.06 Сетевое и системное\_\_\_\_\_\_\_\_  администрирование\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Семестр 4 группа 9САД1.20, 9САД2.20 |   **ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №**  14  1. Рабочие состояния OSPF. Выделенный (DR) и резервный выделенный маршрутизатор (BDR). Синхронизация баз данных OSPF.  2. Практическое задание. Можно пользоваться Интернет. Схема сети.  Если параметры настройки не указаны в задании, необходимо выбрать любые значения, позволяющие выполнить задание (например номера портов в портовых группах).  **Базовые настройки**  1. Для всего активного сетевого оборудования настройте доменное имя wsr2020.wsr  2. Настройте имена устройств в соответствии с диаграммой  3. Создайте локального пользователя admin с паролем Pass  - пользователь должен обладать максимальным уровнем привилегий.  - пароль должен храниться в виде результата хэш функции.  3. Для всех сетевых устройств сконфигурируйте пароль wsr2020 для входа в привилегированный режим.  4. Все сетевые устройства должны быть доступны для управления по протоколу SSHv2.  5. IP адреса устройств взять с таблицы (или с настроек примера).  **Настройка коммутации**  1. Таблица VLAN офиса HQ должна содержать следующие подсети:  VLAN10:CLIENT  VLAN20:SERV  VLAN1000:MANAGE  2. Транки между коммутаторами должны быть согласованы с использованием DTP. SW1 должен инициировать согласование, SW2 и SW3 должны быть настроены в пассивном режиме  3. Транк между SW2 и SW3 должен быть согласован без использования протокола DTP  4. На портах f0/10 коммутаторов SW2 и SW3 сконфигурируйте магистральные каналы без использования динамического согласования. Отключите протокол DTP явным образом.  **Конфигурация портовых групп.**  1. Между коммутаторами SW1 и SW2 настройте агрегирование по протоколу LACP. SW1 должен работать в активном режиме, SW2 в пассивном  2. Между коммутаторами SW1 и SW3 настройте агрегирование по протоколу PAgP. SW1 должен работать в активном режиме, SW3 в пассивном  3. На SW2 настройте балансировку нагрузки по MAC адресу источника + назначения, на SW3 настройте балансировку по IP адресу источника + назначения  **Сконфигурируйте протокол остовного дерева**  1. На всех коммутаторах используйте протокол, совместимый со стандартом 802.1w  2. Корнем для всех VLAN является SW1. При отказе SW1 корнем должен стать SW2. При отказе SW2 корнем должен стать SW3.  3. На портах f0/10 SW2 и SW3 обеспечьте быструю сходимость, без ожидания протокола 802.1w. Аналогичную настройку произведите на магистральном канале между этими двумя коммутаторами.  **Подключение ISP**  1. Для подключения левого офиса использовать обыкновенный Ethernet  2. Подключение правого офиса выполнить по протоколу PPP  - инкапсуляция PPP  - авторизация по протоколу CHAP  - пароль pass  3. Настроить GRE-туннель между правой и левой частью сети.  **Маршрутизация**  1. Обеспечьте маршрутизацию между сетями VLAN с использованием технологии Router-on-a-Stick.  2. В левой части сети настроить протокол OSPF.  3. В правой части сети настроить протокол EIGRP с автономной системой 65001.  4. Маршрут по умолчанию настроить статически в сторону ISP, настроить автомматическое распространение маршрута по умолчанию по сети.  5. Между маршрутизаторами GATE и BRANCH настроить проткол BPG, для GATE автономная система 45002 для BRANCH 45001.  6. Настроить передачу маршрутов для полного согласования сети.  **Подключение к сети интернет**  1. Настроить ретрансляцию адресов на GATE и BRANCH.  **Настройка сервисов**  1. На всех устройствах настроить согласование времени с сервером Google.  2. На RTR настроить DHCP сервер  - распределять сеть для VLAN CLIENT  - в качестве DNS использовать адрес 8.8.8.8  - в качестве шлюза адрес RTR  - первые 20 адресов сети запретить к выдаче.  **Настройка DHCP сервера**  На маршрутизаторе BRANCH сконфигурируйте DHCP сервер.  Обеспечьте возможность доступа в сеть интернет для главного офиса и офиса Branch.  Анонсируйте все сети, необходимые для достижения полной связанности в соответствии со схемой маршрутизации  Настройте аутентификацию.  Преподаватель\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Скиляжнов А.О. |

Министерство образования Красноярского края

краевое государственное бюджетное профессиональное образовательное учреждение «Красноярский колледж радиоэлектроники и информационных технологий»

|  |  |  |  |
| --- | --- | --- | --- |
| |  |  |  | | --- | --- | --- | | |  | | --- | | РАССМОТРЕНО  на заседании цикловой комиссии  преподавателей профессионального  цикла технического профиля  Протокол №\_\_ от «\_\_\_»\_\_\_\_\_\_ 2021 г.  Председатель ЦК \_\_\_\_\_ Е. В. Харитонова | | ДИСЦИПЛИНА  МДК01.02 Организация, принципы построения и функционирования  компьютерных сетей  для специальности  09.02.06 Сетевое и системное\_\_\_\_\_\_\_\_  администрирование\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Семестр 4 группа 9САД1.20, 9САД2.20 |   **ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №**  15  1. Типы пакетов OSPF: пакет приветствия (hello), пакет описания базы данных (DBD), пакет запроса состояния канала (LSR), пакет обновления состояния канала (LSU). пакет подтверждения состояния канала (LSAck). Обновления состояния канала.  2. Практическое задание. Можно пользоваться Интернет. Схема сети.  Если параметры настройки не указаны в задании, необходимо выбрать любые значения, позволяющие выполнить задание (например номера портов в портовых группах).  **Базовые настройки**  1. Для всего активного сетевого оборудования настройте доменное имя wsr2020.wsr  2. Настройте имена устройств в соответствии с диаграммой  3. Создайте локального пользователя admin с паролем Pass  - пользователь должен обладать максимальным уровнем привилегий.  - пароль должен храниться в виде результата хэш функции.  3. Для всех сетевых устройств сконфигурируйте пароль wsr2020 для входа в привилегированный режим.  4. Все сетевые устройства должны быть доступны для управления по протоколу SSHv2.  5. IP адреса устройств взять с таблицы (или с настроек примера).  **Настройка коммутации**  1. Таблица VLAN офиса HQ должна содержать следующие подсети:  VLAN10:CLIENT  VLAN20:SERV  VLAN1000:MANAGE  2. Транки между коммутаторами должны быть согласованы с использованием DTP. SW1 должен инициировать согласование, SW2 и SW3 должны быть настроены в пассивном режиме  3. Транк между SW2 и SW3 должен быть согласован без использования протокола DTP  4. На портах f0/10 коммутаторов SW2 и SW3 сконфигурируйте магистральные каналы без использования динамического согласования. Отключите протокол DTP явным образом.  **Конфигурация портовых групп.**  1. Между коммутаторами SW1 и SW2 настройте агрегирование по протоколу LACP. SW1 должен работать в активном режиме, SW2 в пассивном  2. Между коммутаторами SW1 и SW3 настройте агрегирование по протоколу PAgP. SW1 должен работать в активном режиме, SW3 в пассивном  3. На SW2 настройте балансировку нагрузки по MAC адресу источника + назначения, на SW3 настройте балансировку по IP адресу источника + назначения  **Сконфигурируйте протокол остовного дерева**  1. На всех коммутаторах используйте протокол, совместимый со стандартом 802.1w  2. Корнем для всех VLAN является SW1. При отказе SW1 корнем должен стать SW2. При отказе SW2 корнем должен стать SW3.  3. На портах f0/10 SW2 и SW3 обеспечьте быструю сходимость, без ожидания протокола 802.1w. Аналогичную настройку произведите на магистральном канале между этими двумя коммутаторами.  **Подключение ISP**  1. Для подключения левого офиса использовать обыкновенный Ethernet  2. Подключение правого офиса выполнить по протоколу PPP  - инкапсуляция PPP  - авторизация по протоколу CHAP  - пароль pass  3. Настроить GRE-туннель между правой и левой частью сети.  **Маршрутизация**  1. Обеспечьте маршрутизацию между сетями VLAN с использованием технологии Router-on-a-Stick.  2. В левой части сети настроить протокол OSPF.  3. В правой части сети настроить протокол EIGRP с автономной системой 65001.  4. Маршрут по умолчанию настроить статически в сторону ISP, настроить автомматическое распространение маршрута по умолчанию по сети.  5. Между маршрутизаторами GATE и BRANCH настроить проткол BPG, для GATE автономная система 45002 для BRANCH 45001.  6. Настроить передачу маршрутов для полного согласования сети.  **Подключение к сети интернет**  1. Настроить ретрансляцию адресов на GATE и BRANCH.  **Настройка сервисов**  1. На всех устройствах настроить согласование времени с сервером Google.  2. На RTR настроить DHCP сервер  - распределять сеть для VLAN CLIENT  - в качестве DNS использовать адрес 8.8.8.8  - в качестве шлюза адрес RTR  - первые 20 адресов сети запретить к выдаче.  **Настройка DHCP сервера**  На маршрутизаторе BRANCH сконфигурируйте DHCP сервер.  Обеспечьте возможность доступа в сеть интернет для главного офиса и офиса Branch.  Анонсируйте все сети, необходимые для достижения полной связанности в соответствии со схемой маршрутизации  Настройте аутентификацию.  Преподаватель\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Скиляжнов А.О. |

Министерство образования Красноярского края

краевое государственное бюджетное профессиональное образовательное учреждение «Красноярский колледж радиоэлектроники и информационных технологий»

|  |  |  |  |
| --- | --- | --- | --- |
| |  |  |  | | --- | --- | --- | | |  | | --- | | РАССМОТРЕНО  на заседании цикловой комиссии  преподавателей профессионального  цикла технического профиля  Протокол №\_\_ от «\_\_\_»\_\_\_\_\_\_ 2021 г.  Председатель ЦК \_\_\_\_\_ Е. В. Харитонова | | ДИСЦИПЛИНА  МДК01.02 Организация, принципы построения и функционирования  компьютерных сетей  для специальности  09.02.06 Сетевое и системное\_\_\_\_\_\_\_\_  администрирование\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Семестр 4 группа 9САД1.20, 9САД2.20 |   **ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №**  16   1. Семейство протоколов OSPF. Характеристики, принципы работы и компоненты OSPF. Особенности OSPF для одной и нескольких областей. Магистральная область. Инкапсуляция сообщений OSPF. 2. Практическое задание. Можно пользоваться Интернет. Схема сети.   Если параметры настройки не указаны в задании, необходимо выбрать любые значения, позволяющие выполнить задание (например номера портов в портовых группах).  **Базовые настройки**  1. Для всего активного сетевого оборудования настройте доменное имя wsr2020.wsr  2. Настройте имена устройств в соответствии с диаграммой  3. Создайте локального пользователя admin с паролем Pass  - пользователь должен обладать максимальным уровнем привилегий.  - пароль должен храниться в виде результата хэш функции.  3. Для всех сетевых устройств сконфигурируйте пароль wsr2020 для входа в привилегированный режим.  4. Все сетевые устройства должны быть доступны для управления по протоколу SSHv2.  5. IP адреса устройств взять с таблицы (или с настроек примера).  **Настройка коммутации**  1. Таблица VLAN офиса HQ должна содержать следующие подсети:  VLAN10:CLIENT  VLAN20:SERV  VLAN1000:MANAGE  2. Транки между коммутаторами должны быть согласованы с использованием DTP. SW1 должен инициировать согласование, SW2 и SW3 должны быть настроены в пассивном режиме  3. Транк между SW2 и SW3 должен быть согласован без использования протокола DTP  4. На портах f0/10 коммутаторов SW2 и SW3 сконфигурируйте магистральные каналы без использования динамического согласования. Отключите протокол DTP явным образом.  **Конфигурация портовых групп.**  1. Между коммутаторами SW1 и SW2 настройте агрегирование по протоколу LACP. SW1 должен работать в активном режиме, SW2 в пассивном  2. Между коммутаторами SW1 и SW3 настройте агрегирование по протоколу PAgP. SW1 должен работать в активном режиме, SW3 в пассивном  3. На SW2 настройте балансировку нагрузки по MAC адресу источника + назначения, на SW3 настройте балансировку по IP адресу источника + назначения  **Сконфигурируйте протокол остовного дерева**  1. На всех коммутаторах используйте протокол, совместимый со стандартом 802.1w  2. Корнем для всех VLAN является SW1. При отказе SW1 корнем должен стать SW2. При отказе SW2 корнем должен стать SW3.  3. На портах f0/10 SW2 и SW3 обеспечьте быструю сходимость, без ожидания протокола 802.1w. Аналогичную настройку произведите на магистральном канале между этими двумя коммутаторами.  **Подключение ISP**  1. Для подключения левого офиса использовать обыкновенный Ethernet  2. Подключение правого офиса выполнить по протоколу PPP  - инкапсуляция PPP  - авторизация по протоколу CHAP  - пароль pass  3. Настроить GRE-туннель между правой и левой частью сети.  **Маршрутизация**  1. Обеспечьте маршрутизацию между сетями VLAN с использованием технологии Router-on-a-Stick.  2. В левой части сети настроить протокол OSPF.  3. В правой части сети настроить протокол EIGRP с автономной системой 65001.  4. Маршрут по умолчанию настроить статически в сторону ISP, настроить автомматическое распространение маршрута по умолчанию по сети.  5. Между маршрутизаторами GATE и BRANCH настроить проткол BPG, для GATE автономная система 45002 для BRANCH 45001.  6. Настроить передачу маршрутов для полного согласования сети.  **Подключение к сети интернет**  1. Настроить ретрансляцию адресов на GATE и BRANCH.  **Настройка сервисов**  1. На всех устройствах настроить согласование времени с сервером Google.  2. На RTR настроить DHCP сервер  - распределять сеть для VLAN CLIENT  - в качестве DNS использовать адрес 8.8.8.8  - в качестве шлюза адрес RTR  - первые 20 адресов сети запретить к выдаче.  **Настройка DHCP сервера**  На маршрутизаторе BRANCH сконфигурируйте DHCP сервер.  Обеспечьте возможность доступа в сеть интернет для главного офиса и офиса Branch.  Анонсируйте все сети, необходимые для достижения полной связанности в соответствии со схемой маршрутизации  Настройте аутентификацию.  Преподаватель\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Скиляжнов А.О. |

Министерство образования Красноярского края

краевое государственное бюджетное профессиональное образовательное учреждение «Красноярский колледж радиоэлектроники и информационных технологий»

|  |  |  |  |
| --- | --- | --- | --- |
| |  |  |  | | --- | --- | --- | | |  | | --- | | РАССМОТРЕНО  на заседании цикловой комиссии  преподавателей профессионального  цикла технического профиля  Протокол №\_\_ от «\_\_\_»\_\_\_\_\_\_ 2021 г.  Председатель ЦК \_\_\_\_\_ Е. В. Харитонова | | ДИСЦИПЛИНА  МДК01.02 Организация, принципы построения и функционирования  компьютерных сетей  для специальности  09.02.06 Сетевое и системное\_\_\_\_\_\_\_\_  администрирование\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Семестр 4 группа 9САД1.20, 9САД2.20 |   **ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №**  17  1. Классовые и бесклассовые протоколы маршрутизации. Характеристики и метрики протоколов. Дистанционно-векторный алгоритм.  2. Практическое задание. Можно пользоваться Интернет. Схема сети.  Если параметры настройки не указаны в задании, необходимо выбрать любые значения, позволяющие выполнить задание (например номера портов в портовых группах).  **Базовые настройки**  1. Для всего активного сетевого оборудования настройте доменное имя wsr2020.wsr  2. Настройте имена устройств в соответствии с диаграммой  3. Создайте локального пользователя admin с паролем Pass  - пользователь должен обладать максимальным уровнем привилегий.  - пароль должен храниться в виде результата хэш функции.  3. Для всех сетевых устройств сконфигурируйте пароль wsr2020 для входа в привилегированный режим.  4. Все сетевые устройства должны быть доступны для управления по протоколу SSHv2.  5. IP адреса устройств взять с таблицы (или с настроек примера).  **Настройка коммутации**  1. Таблица VLAN офиса HQ должна содержать следующие подсети:  VLAN10:CLIENT  VLAN20:SERV  VLAN1000:MANAGE  2. Транки между коммутаторами должны быть согласованы с использованием DTP. SW1 должен инициировать согласование, SW2 и SW3 должны быть настроены в пассивном режиме  3. Транк между SW2 и SW3 должен быть согласован без использования протокола DTP  4. На портах f0/10 коммутаторов SW2 и SW3 сконфигурируйте магистральные каналы без использования динамического согласования. Отключите протокол DTP явным образом.  **Конфигурация портовых групп.**  1. Между коммутаторами SW1 и SW2 настройте агрегирование по протоколу LACP. SW1 должен работать в активном режиме, SW2 в пассивном  2. Между коммутаторами SW1 и SW3 настройте агрегирование по протоколу PAgP. SW1 должен работать в активном режиме, SW3 в пассивном  3. На SW2 настройте балансировку нагрузки по MAC адресу источника + назначения, на SW3 настройте балансировку по IP адресу источника + назначения  **Сконфигурируйте протокол остовного дерева**  1. На всех коммутаторах используйте протокол, совместимый со стандартом 802.1w  2. Корнем для всех VLAN является SW1. При отказе SW1 корнем должен стать SW2. При отказе SW2 корнем должен стать SW3.  3. На портах f0/10 SW2 и SW3 обеспечьте быструю сходимость, без ожидания протокола 802.1w. Аналогичную настройку произведите на магистральном канале между этими двумя коммутаторами.  **Подключение ISP**  1. Для подключения левого офиса использовать обыкновенный Ethernet  2. Подключение правого офиса выполнить по протоколу PPP  - инкапсуляция PPP  - авторизация по протоколу CHAP  - пароль pass  3. Настроить GRE-туннель между правой и левой частью сети.  **Маршрутизация**  1. Обеспечьте маршрутизацию между сетями VLAN с использованием технологии Router-on-a-Stick.  2. В левой части сети настроить протокол OSPF.  3. В правой части сети настроить протокол EIGRP с автономной системой 65001.  4. Маршрут по умолчанию настроить статически в сторону ISP, настроить автомматическое распространение маршрута по умолчанию по сети.  5. Между маршрутизаторами GATE и BRANCH настроить проткол BPG, для GATE автономная система 45002 для BRANCH 45001.  6. Настроить передачу маршрутов для полного согласования сети.  **Подключение к сети интернет**  1. Настроить ретрансляцию адресов на GATE и BRANCH.  **Настройка сервисов**  1. На всех устройствах настроить согласование времени с сервером Google.  2. На RTR настроить DHCP сервер  - распределять сеть для VLAN CLIENT  - в качестве DNS использовать адрес 8.8.8.8  - в качестве шлюза адрес RTR  - первые 20 адресов сети запретить к выдаче.  **Настройка DHCP сервера**  На маршрутизаторе BRANCH сконфигурируйте DHCP сервер.  Обеспечьте возможность доступа в сеть интернет для главного офиса и офиса Branch.  Анонсируйте все сети, необходимые для достижения полной связанности в соответствии со схемой маршрутизации  Настройте аутентификацию.  Преподаватель\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Скиляжнов А.О. |

Министерство образования Красноярского края

краевое государственное бюджетное профессиональное образовательное учреждение «Красноярский колледж радиоэлектроники и информационных технологий»

|  |  |  |  |
| --- | --- | --- | --- |
| |  |  |  | | --- | --- | --- | | |  | | --- | | РАССМОТРЕНО  на заседании цикловой комиссии  преподавателей профессионального  цикла технического профиля  Протокол №\_\_ от «\_\_\_»\_\_\_\_\_\_ 2021 г.  Председатель ЦК \_\_\_\_\_ Е. В. Харитонова | | ДИСЦИПЛИНА  МДК01.02 Организация, принципы построения и функционирования  компьютерных сетей  для специальности  09.02.06 Сетевое и системное\_\_\_\_\_\_\_\_  администрирование\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Семестр 4 группа 9САД1.20, 9САД2.20 |   **ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №**  18  1. Классификация протоколов маршрутизации. Протокол маршрутизации по состоянию канала IS-IS.  2. Практическое задание. Можно пользоваться Интернет. Схема сети.  Если параметры настройки не указаны в задании, необходимо выбрать любые значения, позволяющие выполнить задание (например номера портов в портовых группах).  **Базовые настройки**  1. Для всего активного сетевого оборудования настройте доменное имя wsr2020.wsr  2. Настройте имена устройств в соответствии с диаграммой  3. Создайте локального пользователя admin с паролем Pass  - пользователь должен обладать максимальным уровнем привилегий.  - пароль должен храниться в виде результата хэш функции.  3. Для всех сетевых устройств сконфигурируйте пароль wsr2020 для входа в привилегированный режим.  4. Все сетевые устройства должны быть доступны для управления по протоколу SSHv2.  5. IP адреса устройств взять с таблицы (или с настроек примера).  **Настройка коммутации**  1. Таблица VLAN офиса HQ должна содержать следующие подсети:  VLAN10:CLIENT  VLAN20:SERV  VLAN1000:MANAGE  2. Транки между коммутаторами должны быть согласованы с использованием DTP. SW1 должен инициировать согласование, SW2 и SW3 должны быть настроены в пассивном режиме  3. Транк между SW2 и SW3 должен быть согласован без использования протокола DTP  4. На портах f0/10 коммутаторов SW2 и SW3 сконфигурируйте магистральные каналы без использования динамического согласования. Отключите протокол DTP явным образом.  **Конфигурация портовых групп.**  1. Между коммутаторами SW1 и SW2 настройте агрегирование по протоколу LACP. SW1 должен работать в активном режиме, SW2 в пассивном  2. Между коммутаторами SW1 и SW3 настройте агрегирование по протоколу PAgP. SW1 должен работать в активном режиме, SW3 в пассивном  3. На SW2 настройте балансировку нагрузки по MAC адресу источника + назначения, на SW3 настройте балансировку по IP адресу источника + назначения  **Сконфигурируйте протокол остовного дерева**  1. На всех коммутаторах используйте протокол, совместимый со стандартом 802.1w  2. Корнем для всех VLAN является SW1. При отказе SW1 корнем должен стать SW2. При отказе SW2 корнем должен стать SW3.  3. На портах f0/10 SW2 и SW3 обеспечьте быструю сходимость, без ожидания протокола 802.1w. Аналогичную настройку произведите на магистральном канале между этими двумя коммутаторами.  **Подключение ISP**  1. Для подключения левого офиса использовать обыкновенный Ethernet  2. Подключение правого офиса выполнить по протоколу PPP  - инкапсуляция PPP  - авторизация по протоколу CHAP  - пароль pass  3. Настроить GRE-туннель между правой и левой частью сети.  **Маршрутизация**  1. Обеспечьте маршрутизацию между сетями VLAN с использованием технологии Router-on-a-Stick.  2. В левой части сети настроить протокол OSPF.  3. В правой части сети настроить протокол EIGRP с автономной системой 65001.  4. Маршрут по умолчанию настроить статически в сторону ISP, настроить автомматическое распространение маршрута по умолчанию по сети.  5. Между маршрутизаторами GATE и BRANCH настроить проткол BPG, для GATE автономная система 45002 для BRANCH 45001.  6. Настроить передачу маршрутов для полного согласования сети.  **Подключение к сети интернет**  1. Настроить ретрансляцию адресов на GATE и BRANCH.  **Настройка сервисов**  1. На всех устройствах настроить согласование времени с сервером Google.  2. На RTR настроить DHCP сервер  - распределять сеть для VLAN CLIENT  - в качестве DNS использовать адрес 8.8.8.8  - в качестве шлюза адрес RTR  - первые 20 адресов сети запретить к выдаче.  **Настройка DHCP сервера**  На маршрутизаторе BRANCH сконфигурируйте DHCP сервер.  Обеспечьте возможность доступа в сеть интернет для главного офиса и офиса Branch.  Анонсируйте все сети, необходимые для достижения полной связанности в соответствии со схемой маршрутизации  Настройте аутентификацию.  Преподаватель\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Скиляжнов А.О. |

Министерство образования Красноярского края

краевое государственное бюджетное профессиональное образовательное учреждение «Красноярский колледж радиоэлектроники и информационных технологий»

|  |  |  |  |
| --- | --- | --- | --- |
| |  |  |  | | --- | --- | --- | | |  | | --- | | РАССМОТРЕНО  на заседании цикловой комиссии  преподавателей профессионального  цикла технического профиля  Протокол №\_\_ от «\_\_\_»\_\_\_\_\_\_ 2021 г.  Председатель ЦК \_\_\_\_\_ Е. В. Харитонова | | ДИСЦИПЛИНА  МДК01.02 Организация, принципы построения и функционирования  компьютерных сетей  для специальности  09.02.06 Сетевое и системное\_\_\_\_\_\_\_\_  администрирование\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Семестр 4 группа 9САД1.20, 9САД2.20 |   **ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №**  19   1. Классификация протоколов маршрутизации. Протокол маршрутизации по состоянию канала OSPF. 2. Практическое задание. Можно пользоваться Интернет. Схема сети.   Если параметры настройки не указаны в задании, необходимо выбрать любые значения, позволяющие выполнить задание (например номера портов в портовых группах).  **Базовые настройки**  1. Для всего активного сетевого оборудования настройте доменное имя wsr2020.wsr  2. Настройте имена устройств в соответствии с диаграммой  3. Создайте локального пользователя admin с паролем Pass  - пользователь должен обладать максимальным уровнем привилегий.  - пароль должен храниться в виде результата хэш функции.  3. Для всех сетевых устройств сконфигурируйте пароль wsr2020 для входа в привилегированный режим.  4. Все сетевые устройства должны быть доступны для управления по протоколу SSHv2.  5. IP адреса устройств взять с таблицы (или с настроек примера).  **Настройка коммутации**  1. Таблица VLAN офиса HQ должна содержать следующие подсети:  VLAN10:CLIENT  VLAN20:SERV  VLAN1000:MANAGE  2. Транки между коммутаторами должны быть согласованы с использованием DTP. SW1 должен инициировать согласование, SW2 и SW3 должны быть настроены в пассивном режиме  3. Транк между SW2 и SW3 должен быть согласован без использования протокола DTP  4. На портах f0/10 коммутаторов SW2 и SW3 сконфигурируйте магистральные каналы без использования динамического согласования. Отключите протокол DTP явным образом.  **Конфигурация портовых групп.**  1. Между коммутаторами SW1 и SW2 настройте агрегирование по протоколу LACP. SW1 должен работать в активном режиме, SW2 в пассивном  2. Между коммутаторами SW1 и SW3 настройте агрегирование по протоколу PAgP. SW1 должен работать в активном режиме, SW3 в пассивном  3. На SW2 настройте балансировку нагрузки по MAC адресу источника + назначения, на SW3 настройте балансировку по IP адресу источника + назначения  **Сконфигурируйте протокол остовного дерева**  1. На всех коммутаторах используйте протокол, совместимый со стандартом 802.1w  2. Корнем для всех VLAN является SW1. При отказе SW1 корнем должен стать SW2. При отказе SW2 корнем должен стать SW3.  3. На портах f0/10 SW2 и SW3 обеспечьте быструю сходимость, без ожидания протокола 802.1w. Аналогичную настройку произведите на магистральном канале между этими двумя коммутаторами.  **Подключение ISP**  1. Для подключения левого офиса использовать обыкновенный Ethernet  2. Подключение правого офиса выполнить по протоколу PPP  - инкапсуляция PPP  - авторизация по протоколу CHAP  - пароль pass  3. Настроить GRE-туннель между правой и левой частью сети.  **Маршрутизация**  1. Обеспечьте маршрутизацию между сетями VLAN с использованием технологии Router-on-a-Stick.  2. В левой части сети настроить протокол OSPF.  3. В правой части сети настроить протокол EIGRP с автономной системой 65001.  4. Маршрут по умолчанию настроить статически в сторону ISP, настроить автомматическое распространение маршрута по умолчанию по сети.  5. Между маршрутизаторами GATE и BRANCH настроить проткол BPG, для GATE автономная система 45002 для BRANCH 45001.  6. Настроить передачу маршрутов для полного согласования сети.  **Подключение к сети интернет**  1. Настроить ретрансляцию адресов на GATE и BRANCH.  **Настройка сервисов**  1. На всех устройствах настроить согласование времени с сервером Google.  2. На RTR настроить DHCP сервер  - распределять сеть для VLAN CLIENT  - в качестве DNS использовать адрес 8.8.8.8  - в качестве шлюза адрес RTR  - первые 20 адресов сети запретить к выдаче.  **Настройка DHCP сервера**  На маршрутизаторе BRANCH сконфигурируйте DHCP сервер.  Обеспечьте возможность доступа в сеть интернет для главного офиса и офиса Branch.  Анонсируйте все сети, необходимые для достижения полной связанности в соответствии со схемой маршрутизации  Настройте аутентификацию.  Преподаватель\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Скиляжнов А.О. |

Министерство образования Красноярского края

краевое государственное бюджетное профессиональное образовательное учреждение «Красноярский колледж радиоэлектроники и информационных технологий»

|  |  |  |  |
| --- | --- | --- | --- |
| |  |  |  | | --- | --- | --- | | |  | | --- | | РАССМОТРЕНО  на заседании цикловой комиссии  преподавателей профессионального  цикла технического профиля  Протокол №\_\_ от «\_\_\_»\_\_\_\_\_\_ 2021 г.  Председатель ЦК \_\_\_\_\_ Е. В. Харитонова | | ДИСЦИПЛИНА  МДК01.02 Организация, принципы построения и функционирования  компьютерных сетей  для специальности  09.02.06 Сетевое и системное\_\_\_\_\_\_\_\_  администрирование\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Семестр 4 группа 9САД1.20, 9САД2.20 |   **ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №**  20  1. Классификация протоколов маршрутизации. Дистанционно-векторный протокол IGRP.  2. Практическое задание. Можно пользоваться Интернет. Схема сети.  Если параметры настройки не указаны в задании, необходимо выбрать любые значения, позволяющие выполнить задание (например номера портов в портовых группах).  **Базовые настройки**  1. Для всего активного сетевого оборудования настройте доменное имя wsr2020.wsr  2. Настройте имена устройств в соответствии с диаграммой  3. Создайте локального пользователя admin с паролем Pass  - пользователь должен обладать максимальным уровнем привилегий.  - пароль должен храниться в виде результата хэш функции.  3. Для всех сетевых устройств сконфигурируйте пароль wsr2020 для входа в привилегированный режим.  4. Все сетевые устройства должны быть доступны для управления по протоколу SSHv2.  5. IP адреса устройств взять с таблицы (или с настроек примера).  **Настройка коммутации**  1. Таблица VLAN офиса HQ должна содержать следующие подсети:  VLAN10:CLIENT  VLAN20:SERV  VLAN1000:MANAGE  2. Транки между коммутаторами должны быть согласованы с использованием DTP. SW1 должен инициировать согласование, SW2 и SW3 должны быть настроены в пассивном режиме  3. Транк между SW2 и SW3 должен быть согласован без использования протокола DTP  4. На портах f0/10 коммутаторов SW2 и SW3 сконфигурируйте магистральные каналы без использования динамического согласования. Отключите протокол DTP явным образом.  **Конфигурация портовых групп.**  1. Между коммутаторами SW1 и SW2 настройте агрегирование по протоколу LACP. SW1 должен работать в активном режиме, SW2 в пассивном  2. Между коммутаторами SW1 и SW3 настройте агрегирование по протоколу PAgP. SW1 должен работать в активном режиме, SW3 в пассивном  3. На SW2 настройте балансировку нагрузки по MAC адресу источника + назначения, на SW3 настройте балансировку по IP адресу источника + назначения  **Сконфигурируйте протокол остовного дерева**  1. На всех коммутаторах используйте протокол, совместимый со стандартом 802.1w  2. Корнем для всех VLAN является SW1. При отказе SW1 корнем должен стать SW2. При отказе SW2 корнем должен стать SW3.  3. На портах f0/10 SW2 и SW3 обеспечьте быструю сходимость, без ожидания протокола 802.1w. Аналогичную настройку произведите на магистральном канале между этими двумя коммутаторами.  **Подключение ISP**  1. Для подключения левого офиса использовать обыкновенный Ethernet  2. Подключение правого офиса выполнить по протоколу PPP  - инкапсуляция PPP  - авторизация по протоколу CHAP  - пароль pass  3. Настроить GRE-туннель между правой и левой частью сети.  **Маршрутизация**  1. Обеспечьте маршрутизацию между сетями VLAN с использованием технологии Router-on-a-Stick.  2. В левой части сети настроить протокол OSPF.  3. В правой части сети настроить протокол EIGRP с автономной системой 65001.  4. Маршрут по умолчанию настроить статически в сторону ISP, настроить автомматическое распространение маршрута по умолчанию по сети.  5. Между маршрутизаторами GATE и BRANCH настроить проткол BPG, для GATE автономная система 45002 для BRANCH 45001.  6. Настроить передачу маршрутов для полного согласования сети.  **Подключение к сети интернет**  1. Настроить ретрансляцию адресов на GATE и BRANCH.  **Настройка сервисов**  1. На всех устройствах настроить согласование времени с сервером Google.  2. На RTR настроить DHCP сервер  - распределять сеть для VLAN CLIENT  - в качестве DNS использовать адрес 8.8.8.8  - в качестве шлюза адрес RTR  - первые 20 адресов сети запретить к выдаче.  **Настройка DHCP сервера**  На маршрутизаторе BRANCH сконфигурируйте DHCP сервер.  Обеспечьте возможность доступа в сеть интернет для главного офиса и офиса Branch.  Анонсируйте все сети, необходимые для достижения полной связанности в соответствии со схемой маршрутизации  Настройте аутентификацию.  Преподаватель\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Скиляжнов А.О. |

Министерство образования Красноярского края

краевое государственное бюджетное профессиональное образовательное учреждение «Красноярский колледж радиоэлектроники и информационных технологий»

|  |  |  |  |
| --- | --- | --- | --- |
| |  |  |  | | --- | --- | --- | | |  | | --- | | РАССМОТРЕНО  на заседании цикловой комиссии  преподавателей профессионального  цикла технического профиля  Протокол №\_\_ от «\_\_\_»\_\_\_\_\_\_ 2021 г.  Председатель ЦК \_\_\_\_\_ Е. В. Харитонова | | ДИСЦИПЛИНА  МДК01.02 Организация, принципы построения и функционирования  компьютерных сетей  для специальности  09.02.06 Сетевое и системное\_\_\_\_\_\_\_\_  администрирование\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Семестр 4 группа 9САД1.20, 9САД2.20 |   **ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №**  21  1. Классификация протоколов маршрутизации. Дистанционно-векторный протокол RIP.  2. Практическое задание. Можно пользоваться Интернет. Схема сети.  Если параметры настройки не указаны в задании, необходимо выбрать любые значения, позволяющие выполнить задание (например номера портов в портовых группах).  **Базовые настройки**  1. Для всего активного сетевого оборудования настройте доменное имя wsr2020.wsr  2. Настройте имена устройств в соответствии с диаграммой  3. Создайте локального пользователя admin с паролем Pass  - пользователь должен обладать максимальным уровнем привилегий.  - пароль должен храниться в виде результата хэш функции.  3. Для всех сетевых устройств сконфигурируйте пароль wsr2020 для входа в привилегированный режим.  4. Все сетевые устройства должны быть доступны для управления по протоколу SSHv2.  5. IP адреса устройств взять с таблицы (или с настроек примера).  **Настройка коммутации**  1. Таблица VLAN офиса HQ должна содержать следующие подсети:  VLAN10:CLIENT  VLAN20:SERV  VLAN1000:MANAGE  2. Транки между коммутаторами должны быть согласованы с использованием DTP. SW1 должен инициировать согласование, SW2 и SW3 должны быть настроены в пассивном режиме  3. Транк между SW2 и SW3 должен быть согласован без использования протокола DTP  4. На портах f0/10 коммутаторов SW2 и SW3 сконфигурируйте магистральные каналы без использования динамического согласования. Отключите протокол DTP явным образом.  **Конфигурация портовых групп.**  1. Между коммутаторами SW1 и SW2 настройте агрегирование по протоколу LACP. SW1 должен работать в активном режиме, SW2 в пассивном  2. Между коммутаторами SW1 и SW3 настройте агрегирование по протоколу PAgP. SW1 должен работать в активном режиме, SW3 в пассивном  3. На SW2 настройте балансировку нагрузки по MAC адресу источника + назначения, на SW3 настройте балансировку по IP адресу источника + назначения  **Сконфигурируйте протокол остовного дерева**  1. На всех коммутаторах используйте протокол, совместимый со стандартом 802.1w  2. Корнем для всех VLAN является SW1. При отказе SW1 корнем должен стать SW2. При отказе SW2 корнем должен стать SW3.  3. На портах f0/10 SW2 и SW3 обеспечьте быструю сходимость, без ожидания протокола 802.1w. Аналогичную настройку произведите на магистральном канале между этими двумя коммутаторами.  **Подключение ISP**  1. Для подключения левого офиса использовать обыкновенный Ethernet  2. Подключение правого офиса выполнить по протоколу PPP  - инкапсуляция PPP  - авторизация по протоколу CHAP  - пароль pass  3. Настроить GRE-туннель между правой и левой частью сети.  **Маршрутизация**  1. Обеспечьте маршрутизацию между сетями VLAN с использованием технологии Router-on-a-Stick.  2. В левой части сети настроить протокол OSPF.  3. В правой части сети настроить протокол EIGRP с автономной системой 65001.  4. Маршрут по умолчанию настроить статически в сторону ISP, настроить автомматическое распространение маршрута по умолчанию по сети.  5. Между маршрутизаторами GATE и BRANCH настроить проткол BPG, для GATE автономная система 45002 для BRANCH 45001.  6. Настроить передачу маршрутов для полного согласования сети.  **Подключение к сети интернет**  1. Настроить ретрансляцию адресов на GATE и BRANCH.  **Настройка сервисов**  1. На всех устройствах настроить согласование времени с сервером Google.  2. На RTR настроить DHCP сервер  - распределять сеть для VLAN CLIENT  - в качестве DNS использовать адрес 8.8.8.8  - в качестве шлюза адрес RTR  - первые 20 адресов сети запретить к выдаче.  **Настройка DHCP сервера**  На маршрутизаторе BRANCH сконфигурируйте DHCP сервер.  Обеспечьте возможность доступа в сеть интернет для главного офиса и офиса Branch.  Анонсируйте все сети, необходимые для достижения полной связанности в соответствии со схемой маршрутизации  Настройте аутентификацию.  Преподаватель\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Скиляжнов А.О. |

Министерство образования Красноярского края

краевое государственное бюджетное профессиональное образовательное учреждение «Красноярский колледж радиоэлектроники и информационных технологий»

|  |  |  |  |
| --- | --- | --- | --- |
| |  |  |  | | --- | --- | --- | | |  | | --- | | РАССМОТРЕНО  на заседании цикловой комиссии  преподавателей профессионального  цикла технического профиля  Протокол №\_\_ от «\_\_\_»\_\_\_\_\_\_ 2021 г.  Председатель ЦК \_\_\_\_\_ Е. В. Харитонова | | ДИСЦИПЛИНА  МДК01.02 Организация, принципы построения и функционирования  компьютерных сетей  для специальности  09.02.06 Сетевое и системное\_\_\_\_\_\_\_\_  администрирование\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Семестр 4 группа 9САД1.20, 9САД2.20 |   **ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №**  22   1. Протоколы динамической маршрутизации – назначение, принципы работы и история развития. Сравнение динамической и статической маршрутизации. Принципы работы протоколов маршрутизации: пуск после включения питания, сетевое обнаружение, обмен данными маршрутизации, обеспечение сходимости. 2. Практическое задание. Можно пользоваться Интернет. Схема сети.   Если параметры настройки не указаны в задании, необходимо выбрать любые значения, позволяющие выполнить задание (например номера портов в портовых группах).  **Базовые настройки**  1. Для всего активного сетевого оборудования настройте доменное имя wsr2020.wsr  2. Настройте имена устройств в соответствии с диаграммой  3. Создайте локального пользователя admin с паролем Pass  - пользователь должен обладать максимальным уровнем привилегий.  - пароль должен храниться в виде результата хэш функции.  3. Для всех сетевых устройств сконфигурируйте пароль wsr2020 для входа в привилегированный режим.  4. Все сетевые устройства должны быть доступны для управления по протоколу SSHv2.  5. IP адреса устройств взять с таблицы (или с настроек примера).  **Настройка коммутации**  1. Таблица VLAN офиса HQ должна содержать следующие подсети:  VLAN10:CLIENT  VLAN20:SERV  VLAN1000:MANAGE  2. Транки между коммутаторами должны быть согласованы с использованием DTP. SW1 должен инициировать согласование, SW2 и SW3 должны быть настроены в пассивном режиме  3. Транк между SW2 и SW3 должен быть согласован без использования протокола DTP  4. На портах f0/10 коммутаторов SW2 и SW3 сконфигурируйте магистральные каналы без использования динамического согласования. Отключите протокол DTP явным образом.  **Конфигурация портовых групп.**  1. Между коммутаторами SW1 и SW2 настройте агрегирование по протоколу LACP. SW1 должен работать в активном режиме, SW2 в пассивном  2. Между коммутаторами SW1 и SW3 настройте агрегирование по протоколу PAgP. SW1 должен работать в активном режиме, SW3 в пассивном  3. На SW2 настройте балансировку нагрузки по MAC адресу источника + назначения, на SW3 настройте балансировку по IP адресу источника + назначения  **Сконфигурируйте протокол остовного дерева**  1. На всех коммутаторах используйте протокол, совместимый со стандартом 802.1w  2. Корнем для всех VLAN является SW1. При отказе SW1 корнем должен стать SW2. При отказе SW2 корнем должен стать SW3.  3. На портах f0/10 SW2 и SW3 обеспечьте быструю сходимость, без ожидания протокола 802.1w. Аналогичную настройку произведите на магистральном канале между этими двумя коммутаторами.  **Подключение ISP**  1. Для подключения левого офиса использовать обыкновенный Ethernet  2. Подключение правого офиса выполнить по протоколу PPP  - инкапсуляция PPP  - авторизация по протоколу CHAP  - пароль pass  3. Настроить GRE-туннель между правой и левой частью сети.  **Маршрутизация**  1. Обеспечьте маршрутизацию между сетями VLAN с использованием технологии Router-on-a-Stick.  2. В левой части сети настроить протокол OSPF.  3. В правой части сети настроить протокол EIGRP с автономной системой 65001.  4. Маршрут по умолчанию настроить статически в сторону ISP, настроить автомматическое распространение маршрута по умолчанию по сети.  5. Между маршрутизаторами GATE и BRANCH настроить проткол BPG, для GATE автономная система 45002 для BRANCH 45001.  6. Настроить передачу маршрутов для полного согласования сети.  **Подключение к сети интернет**  1. Настроить ретрансляцию адресов на GATE и BRANCH.  **Настройка сервисов**  1. На всех устройствах настроить согласование времени с сервером Google.  2. На RTR настроить DHCP сервер  - распределять сеть для VLAN CLIENT  - в качестве DNS использовать адрес 8.8.8.8  - в качестве шлюза адрес RTR  - первые 20 адресов сети запретить к выдаче.  **Настройка DHCP сервера**  На маршрутизаторе BRANCH сконфигурируйте DHCP сервер.  Обеспечьте возможность доступа в сеть интернет для главного офиса и офиса Branch.  Анонсируйте все сети, необходимые для достижения полной связанности в соответствии со схемой маршрутизации  Настройте аутентификацию.  Преподаватель\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Скиляжнов А.О. |

Министерство образования Красноярского края

краевое государственное бюджетное профессиональное образовательное учреждение «Красноярский колледж радиоэлектроники и информационных технологий»

|  |  |  |  |
| --- | --- | --- | --- |
| |  |  |  | | --- | --- | --- | | |  | | --- | | РАССМОТРЕНО  на заседании цикловой комиссии  преподавателей профессионального  цикла технического профиля  Протокол №\_\_ от «\_\_\_»\_\_\_\_\_\_ 2021 г.  Председатель ЦК \_\_\_\_\_ Е. В. Харитонова | | ДИСЦИПЛИНА  МДК01.02 Организация, принципы построения и функционирования  компьютерных сетей  для специальности  09.02.06 Сетевое и системное\_\_\_\_\_\_\_\_  администрирование\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Семестр 4 группа 9САД1.20, 9САД2.20 |   **ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №**  23   1. [Балансировка нагрузки](http://xgu.ru/wiki/%D0%90%D0%B3%D1%80%D0%B5%D0%B3%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5_%D0%BA%D0%B0%D0%BD%D0%B0%D0%BB%D0%BE%D0%B2#.D0.91.D0.B0.D0.BB.D0.B0.D0.BD.D1.81.D0.B8.D1.80.D0.BE.D0.B2.D0.BA.D0.B0_.D0.BD.D0.B0.D0.B3.D1.80.D1.83.D0.B7.D0.BA.D0.B8_2). [Балансировка нагрузки по MAC-адресам или IP-адресам](http://xgu.ru/wiki/%D0%90%D0%B3%D1%80%D0%B5%D0%B3%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5_%D0%BA%D0%B0%D0%BD%D0%B0%D0%BB%D0%BE%D0%B2#.D0.91.D0.B0.D0.BB.D0.B0.D0.BD.D1.81.D0.B8.D1.80.D0.BE.D0.B2.D0.BA.D0.B0_.D0.BD.D0.B0.D0.B3.D1.80.D1.83.D0.B7.D0.BA.D0.B8_.D0.BF.D0.BE_MAC-.D0.B0.D0.B4.D1.80.D0.B5.D1.81.D0.B0.D0.BC_.D0.B8.D0.BB.D0.B8_IP-.D0.B0.D0.B4.D1.80.D0.B5.D1.81.D0.B0.D0.BC). [Балансировка нагрузки по портам](http://xgu.ru/wiki/%D0%90%D0%B3%D1%80%D0%B5%D0%B3%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5_%D0%BA%D0%B0%D0%BD%D0%B0%D0%BB%D0%BE%D0%B2#.D0.91.D0.B0.D0.BB.D0.B0.D0.BD.D1.81.D0.B8.D1.80.D0.BE.D0.B2.D0.BA.D0.B0_.D0.BD.D0.B0.D0.B3.D1.80.D1.83.D0.B7.D0.BA.D0.B8_.D0.BF.D0.BE_.D0.BF.D0.BE.D1.80.D1.82.D0.B0.D0.BC). [Тестирование балансировки](http://xgu.ru/wiki/%D0%90%D0%B3%D1%80%D0%B5%D0%B3%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5_%D0%BA%D0%B0%D0%BD%D0%B0%D0%BB%D0%BE%D0%B2#.D0.A2.D0.B5.D1.81.D1.82.D0.B8.D1.80.D0.BE.D0.B2.D0.B0.D0.BD.D0.B8.D0.B5_.D0.B1.D0.B0.D0.BB.D0.B0.D0.BD.D1.81.D0.B8.D1.80.D0.BE.D0.B2.D0.BA.D0.B8). 2. Практическое задание. Можно пользоваться Интернет. Схема сети.   Если параметры настройки не указаны в задании, необходимо выбрать любые значения, позволяющие выполнить задание (например номера портов в портовых группах).  **Базовые настройки**  1. Для всего активного сетевого оборудования настройте доменное имя wsr2020.wsr  2. Настройте имена устройств в соответствии с диаграммой  3. Создайте локального пользователя admin с паролем Pass  - пользователь должен обладать максимальным уровнем привилегий.  - пароль должен храниться в виде результата хэш функции.  3. Для всех сетевых устройств сконфигурируйте пароль wsr2020 для входа в привилегированный режим.  4. Все сетевые устройства должны быть доступны для управления по протоколу SSHv2.  5. IP адреса устройств взять с таблицы (или с настроек примера).  **Настройка коммутации**  1. Таблица VLAN офиса HQ должна содержать следующие подсети:  VLAN10:CLIENT  VLAN20:SERV  VLAN1000:MANAGE  2. Транки между коммутаторами должны быть согласованы с использованием DTP. SW1 должен инициировать согласование, SW2 и SW3 должны быть настроены в пассивном режиме  3. Транк между SW2 и SW3 должен быть согласован без использования протокола DTP  4. На портах f0/10 коммутаторов SW2 и SW3 сконфигурируйте магистральные каналы без использования динамического согласования. Отключите протокол DTP явным образом.  **Конфигурация портовых групп.**  1. Между коммутаторами SW1 и SW2 настройте агрегирование по протоколу LACP. SW1 должен работать в активном режиме, SW2 в пассивном  2. Между коммутаторами SW1 и SW3 настройте агрегирование по протоколу PAgP. SW1 должен работать в активном режиме, SW3 в пассивном  3. На SW2 настройте балансировку нагрузки по MAC адресу источника + назначения, на SW3 настройте балансировку по IP адресу источника + назначения  **Сконфигурируйте протокол остовного дерева**  1. На всех коммутаторах используйте протокол, совместимый со стандартом 802.1w  2. Корнем для всех VLAN является SW1. При отказе SW1 корнем должен стать SW2. При отказе SW2 корнем должен стать SW3.  3. На портах f0/10 SW2 и SW3 обеспечьте быструю сходимость, без ожидания протокола 802.1w. Аналогичную настройку произведите на магистральном канале между этими двумя коммутаторами.  **Подключение ISP**  1. Для подключения левого офиса использовать обыкновенный Ethernet  2. Подключение правого офиса выполнить по протоколу PPP  - инкапсуляция PPP  - авторизация по протоколу CHAP  - пароль pass  3. Настроить GRE-туннель между правой и левой частью сети.  **Маршрутизация**  1. Обеспечьте маршрутизацию между сетями VLAN с использованием технологии Router-on-a-Stick.  2. В левой части сети настроить протокол OSPF.  3. В правой части сети настроить протокол EIGRP с автономной системой 65001.  4. Маршрут по умолчанию настроить статически в сторону ISP, настроить автомматическое распространение маршрута по умолчанию по сети.  5. Между маршрутизаторами GATE и BRANCH настроить проткол BPG, для GATE автономная система 45002 для BRANCH 45001.  6. Настроить передачу маршрутов для полного согласования сети.  **Подключение к сети интернет**  1. Настроить ретрансляцию адресов на GATE и BRANCH.  **Настройка сервисов**  1. На всех устройствах настроить согласование времени с сервером Google.  2. На RTR настроить DHCP сервер  - распределять сеть для VLAN CLIENT  - в качестве DNS использовать адрес 8.8.8.8  - в качестве шлюза адрес RTR  - первые 20 адресов сети запретить к выдаче.  **Настройка DHCP сервера**  На маршрутизаторе BRANCH сконфигурируйте DHCP сервер.  Обеспечьте возможность доступа в сеть интернет для главного офиса и офиса Branch.  Анонсируйте все сети, необходимые для достижения полной связанности в соответствии со схемой маршрутизации  Настройте аутентификацию.  Преподаватель\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Скиляжнов А.О. |

Министерство образования Красноярского края

краевое государственное бюджетное профессиональное образовательное учреждение «Красноярский колледж радиоэлектроники и информационных технологий»

|  |  |  |  |
| --- | --- | --- | --- |
| |  |  |  | | --- | --- | --- | | |  | | --- | | РАССМОТРЕНО  на заседании цикловой комиссии  преподавателей профессионального  цикла технического профиля  Протокол №\_\_ от «\_\_\_»\_\_\_\_\_\_ 2021 г.  Председатель ЦК \_\_\_\_\_ Е. В. Харитонова | | ДИСЦИПЛИНА  МДК01.02 Организация, принципы построения и функционирования  компьютерных сетей  для специальности  09.02.06 Сетевое и системное\_\_\_\_\_\_\_\_  администрирование\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Семестр 4 группа 9САД1.20, 9САД2.20 |   **ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №**  24  1. [Статическое агрегирование каналов с помощью LACP](http://xgu.ru/wiki/%D0%90%D0%B3%D1%80%D0%B5%D0%B3%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5_%D0%BA%D0%B0%D0%BD%D0%B0%D0%BB%D0%BE%D0%B2#.D0.A1.D1.82.D0.B0.D1.82.D0.B8.D1.87.D0.B5.D1.81.D0.BA.D0.BE.D0.B5_.D0.B0.D0.B3.D1.80.D0.B5.D0.B3.D0.B8.D1.80.D0.BE.D0.B2.D0.B0.D0.BD.D0.B8.D0.B5_.D0.BA.D0.B0.D0.BD.D0.B0.D0.BB.D0.BE.D0.B2_.D1.81_.D0.BF.D0.BE.D0.BC.D0.BE.D1.89.D1.8C.D1.8E_LACP). [Динамическое агрегирование каналов с помощью LACP](http://xgu.ru/wiki/%D0%90%D0%B3%D1%80%D0%B5%D0%B3%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5_%D0%BA%D0%B0%D0%BD%D0%B0%D0%BB%D0%BE%D0%B2#.D0.94.D0.B8.D0.BD.D0.B0.D0.BC.D0.B8.D1.87.D0.B5.D1.81.D0.BA.D0.BE.D0.B5_.D0.B0.D0.B3.D1.80.D0.B5.D0.B3.D0.B8.D1.80.D0.BE.D0.B2.D0.B0.D0.BD.D0.B8.D0.B5_.D0.BA.D0.B0.D0.BD.D0.B0.D0.BB.D0.BE.D0.B2_.D1.81_.D0.BF.D0.BE.D0.BC.D0.BE.D1.89.D1.8C.D1.8E_LACP).  2. Практическое задание. Можно пользоваться Интернет. Схема сети.  Если параметры настройки не указаны в задании, необходимо выбрать любые значения, позволяющие выполнить задание (например номера портов в портовых группах).  **Базовые настройки**  1. Для всего активного сетевого оборудования настройте доменное имя wsr2020.wsr  2. Настройте имена устройств в соответствии с диаграммой  3. Создайте локального пользователя admin с паролем Pass  - пользователь должен обладать максимальным уровнем привилегий.  - пароль должен храниться в виде результата хэш функции.  3. Для всех сетевых устройств сконфигурируйте пароль wsr2020 для входа в привилегированный режим.  4. Все сетевые устройства должны быть доступны для управления по протоколу SSHv2.  5. IP адреса устройств взять с таблицы (или с настроек примера).  **Настройка коммутации**  1. Таблица VLAN офиса HQ должна содержать следующие подсети:  VLAN10:CLIENT  VLAN20:SERV  VLAN1000:MANAGE  2. Транки между коммутаторами должны быть согласованы с использованием DTP. SW1 должен инициировать согласование, SW2 и SW3 должны быть настроены в пассивном режиме  3. Транк между SW2 и SW3 должен быть согласован без использования протокола DTP  4. На портах f0/10 коммутаторов SW2 и SW3 сконфигурируйте магистральные каналы без использования динамического согласования. Отключите протокол DTP явным образом.  **Конфигурация портовых групп.**  1. Между коммутаторами SW1 и SW2 настройте агрегирование по протоколу LACP. SW1 должен работать в активном режиме, SW2 в пассивном  2. Между коммутаторами SW1 и SW3 настройте агрегирование по протоколу PAgP. SW1 должен работать в активном режиме, SW3 в пассивном  3. На SW2 настройте балансировку нагрузки по MAC адресу источника + назначения, на SW3 настройте балансировку по IP адресу источника + назначения  **Сконфигурируйте протокол остовного дерева**  1. На всех коммутаторах используйте протокол, совместимый со стандартом 802.1w  2. Корнем для всех VLAN является SW1. При отказе SW1 корнем должен стать SW2. При отказе SW2 корнем должен стать SW3.  3. На портах f0/10 SW2 и SW3 обеспечьте быструю сходимость, без ожидания протокола 802.1w. Аналогичную настройку произведите на магистральном канале между этими двумя коммутаторами.  **Подключение ISP**  1. Для подключения левого офиса использовать обыкновенный Ethernet  2. Подключение правого офиса выполнить по протоколу PPP  - инкапсуляция PPP  - авторизация по протоколу CHAP  - пароль pass  3. Настроить GRE-туннель между правой и левой частью сети.  **Маршрутизация**  1. Обеспечьте маршрутизацию между сетями VLAN с использованием технологии Router-on-a-Stick.  2. В левой части сети настроить протокол OSPF.  3. В правой части сети настроить протокол EIGRP с автономной системой 65001.  4. Маршрут по умолчанию настроить статически в сторону ISP, настроить автомматическое распространение маршрута по умолчанию по сети.  5. Между маршрутизаторами GATE и BRANCH настроить проткол BPG, для GATE автономная система 45002 для BRANCH 45001.  6. Настроить передачу маршрутов для полного согласования сети.  **Подключение к сети интернет**  1. Настроить ретрансляцию адресов на GATE и BRANCH.  **Настройка сервисов**  1. На всех устройствах настроить согласование времени с сервером Google.  2. На RTR настроить DHCP сервер  - распределять сеть для VLAN CLIENT  - в качестве DNS использовать адрес 8.8.8.8  - в качестве шлюза адрес RTR  - первые 20 адресов сети запретить к выдаче.  **Настройка DHCP сервера**  На маршрутизаторе BRANCH сконфигурируйте DHCP сервер.  Обеспечьте возможность доступа в сеть интернет для главного офиса и офиса Branch.  Анонсируйте все сети, необходимые для достижения полной связанности в соответствии со схемой маршрутизации  Настройте аутентификацию.  Преподаватель\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Скиляжнов А.О. |

Министерство образования Красноярского края

краевое государственное бюджетное профессиональное образовательное учреждение «Красноярский колледж радиоэлектроники и информационных технологий»

|  |  |  |  |
| --- | --- | --- | --- |
| |  |  |  | | --- | --- | --- | | |  | | --- | | РАССМОТРЕНО  на заседании цикловой комиссии  преподавателей профессионального  цикла технического профиля  Протокол №\_\_ от «\_\_\_»\_\_\_\_\_\_ 2021 г.  Председатель ЦК \_\_\_\_\_ Е. В. Харитонова | | ДИСЦИПЛИНА  МДК01.02 Организация, принципы построения и функционирования  компьютерных сетей  для специальности  09.02.06 Сетевое и системное\_\_\_\_\_\_\_\_  администрирование\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Семестр 4 группа 9САД1.20, 9САД2.20 |   **ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №**  25  1. [Балансировка нагрузки](http://xgu.ru/wiki/%D0%90%D0%B3%D1%80%D0%B5%D0%B3%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5_%D0%BA%D0%B0%D0%BD%D0%B0%D0%BB%D0%BE%D0%B2#.D0.91.D0.B0.D0.BB.D0.B0.D0.BD.D1.81.D0.B8.D1.80.D0.BE.D0.B2.D0.BA.D0.B0_.D0.BD.D0.B0.D0.B3.D1.80.D1.83.D0.B7.D0.BA.D0.B8). [Тестирование балансировки нагрузки](http://xgu.ru/wiki/%D0%90%D0%B3%D1%80%D0%B5%D0%B3%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5_%D0%BA%D0%B0%D0%BD%D0%B0%D0%BB%D0%BE%D0%B2#.D0.A2.D0.B5.D1.81.D1.82.D0.B8.D1.80.D0.BE.D0.B2.D0.B0.D0.BD.D0.B8.D0.B5_.D0.B1.D0.B0.D0.BB.D0.B0.D0.BD.D1.81.D0.B8.D1.80.D0.BE.D0.B2.D0.BA.D0.B8_.D0.BD.D0.B0.D0.B3.D1.80.D1.83.D0.B7.D0.BA.D0.B8).  2. Практическое задание. Можно пользоваться Интернет. Схема сети.  Если параметры настройки не указаны в задании, необходимо выбрать любые значения, позволяющие выполнить задание (например номера портов в портовых группах).  **Базовые настройки**  1. Для всего активного сетевого оборудования настройте доменное имя wsr2020.wsr  2. Настройте имена устройств в соответствии с диаграммой  3. Создайте локального пользователя admin с паролем Pass  - пользователь должен обладать максимальным уровнем привилегий.  - пароль должен храниться в виде результата хэш функции.  3. Для всех сетевых устройств сконфигурируйте пароль wsr2020 для входа в привилегированный режим.  4. Все сетевые устройства должны быть доступны для управления по протоколу SSHv2.  5. IP адреса устройств взять с таблицы (или с настроек примера).  **Настройка коммутации**  1. Таблица VLAN офиса HQ должна содержать следующие подсети:  VLAN10:CLIENT  VLAN20:SERV  VLAN1000:MANAGE  2. Транки между коммутаторами должны быть согласованы с использованием DTP. SW1 должен инициировать согласование, SW2 и SW3 должны быть настроены в пассивном режиме  3. Транк между SW2 и SW3 должен быть согласован без использования протокола DTP  4. На портах f0/10 коммутаторов SW2 и SW3 сконфигурируйте магистральные каналы без использования динамического согласования. Отключите протокол DTP явным образом.  **Конфигурация портовых групп.**  1. Между коммутаторами SW1 и SW2 настройте агрегирование по протоколу LACP. SW1 должен работать в активном режиме, SW2 в пассивном  2. Между коммутаторами SW1 и SW3 настройте агрегирование по протоколу PAgP. SW1 должен работать в активном режиме, SW3 в пассивном  3. На SW2 настройте балансировку нагрузки по MAC адресу источника + назначения, на SW3 настройте балансировку по IP адресу источника + назначения  **Сконфигурируйте протокол остовного дерева**  1. На всех коммутаторах используйте протокол, совместимый со стандартом 802.1w  2. Корнем для всех VLAN является SW1. При отказе SW1 корнем должен стать SW2. При отказе SW2 корнем должен стать SW3.  3. На портах f0/10 SW2 и SW3 обеспечьте быструю сходимость, без ожидания протокола 802.1w. Аналогичную настройку произведите на магистральном канале между этими двумя коммутаторами.  **Подключение ISP**  1. Для подключения левого офиса использовать обыкновенный Ethernet  2. Подключение правого офиса выполнить по протоколу PPP  - инкапсуляция PPP  - авторизация по протоколу CHAP  - пароль pass  3. Настроить GRE-туннель между правой и левой частью сети.  **Маршрутизация**  1. Обеспечьте маршрутизацию между сетями VLAN с использованием технологии Router-on-a-Stick.  2. В левой части сети настроить протокол OSPF.  3. В правой части сети настроить протокол EIGRP с автономной системой 65001.  4. Маршрут по умолчанию настроить статически в сторону ISP, настроить автомматическое распространение маршрута по умолчанию по сети.  5. Между маршрутизаторами GATE и BRANCH настроить проткол BPG, для GATE автономная система 45002 для BRANCH 45001.  6. Настроить передачу маршрутов для полного согласования сети.  **Подключение к сети интернет**  1. Настроить ретрансляцию адресов на GATE и BRANCH.  **Настройка сервисов**  1. На всех устройствах настроить согласование времени с сервером Google.  2. На RTR настроить DHCP сервер  - распределять сеть для VLAN CLIENT  - в качестве DNS использовать адрес 8.8.8.8  - в качестве шлюза адрес RTR  - первые 20 адресов сети запретить к выдаче.  **Настройка DHCP сервера**  На маршрутизаторе BRANCH сконфигурируйте DHCP сервер.  Обеспечьте возможность доступа в сеть интернет для главного офиса и офиса Branch.  Анонсируйте все сети, необходимые для достижения полной связанности в соответствии со схемой маршрутизации  Настройте аутентификацию.  Преподаватель\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Скиляжнов А.О. |

Министерство образования Красноярского края

краевое государственное бюджетное профессиональное образовательное учреждение «Красноярский колледж радиоэлектроники и информационных технологий»

|  |  |  |  |
| --- | --- | --- | --- |
| |  |  |  | | --- | --- | --- | | |  | | --- | | РАССМОТРЕНО  на заседании цикловой комиссии  преподавателей профессионального  цикла технического профиля  Протокол №\_\_ от «\_\_\_»\_\_\_\_\_\_ 2021 г.  Председатель ЦК \_\_\_\_\_ Е. В. Харитонова | | ДИСЦИПЛИНА  МДК01.02 Организация, принципы построения и функционирования  компьютерных сетей  для специальности  09.02.06 Сетевое и системное\_\_\_\_\_\_\_\_  администрирование\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Семестр 4 группа 9САД1.20, 9САД2.20 |   **ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №**  26  1. [Standby-интерфейсы](http://xgu.ru/wiki/%D0%90%D0%B3%D1%80%D0%B5%D0%B3%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5_%D0%BA%D0%B0%D0%BD%D0%B0%D0%BB%D0%BE%D0%B2#Standby-.D0.B8.D0.BD.D1.82.D0.B5.D1.80.D1.84.D0.B5.D0.B9.D1.81.D1.8B). [Настройка EtherChannel 2го уровня с помощью PAgP](http://xgu.ru/wiki/%D0%90%D0%B3%D1%80%D0%B5%D0%B3%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5_%D0%BA%D0%B0%D0%BD%D0%B0%D0%BB%D0%BE%D0%B2#.D0.9D.D0.B0.D1.81.D1.82.D1.80.D0.BE.D0.B9.D0.BA.D0.B0_EtherChannel_2.D0.B3.D0.BE_.D1.83.D1.80.D0.BE.D0.B2.D0.BD.D1.8F_.D1.81_.D0.BF.D0.BE.D0.BC.D0.BE.D1.89.D1.8C.D1.8E_PAgP). [Настройка EtherChannel 3го уровня](http://xgu.ru/wiki/%D0%90%D0%B3%D1%80%D0%B5%D0%B3%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5_%D0%BA%D0%B0%D0%BD%D0%B0%D0%BB%D0%BE%D0%B2#.D0.9D.D0.B0.D1.81.D1.82.D1.80.D0.BE.D0.B9.D0.BA.D0.B0_EtherChannel_3.D0.B3.D0.BE_.D1.83.D1.80.D0.BE.D0.B2.D0.BD.D1.8F).  2. Практическое задание. Можно пользоваться Интернет. Схема сети.  Если параметры настройки не указаны в задании, необходимо выбрать любые значения, позволяющие выполнить задание (например номера портов в портовых группах).  **Базовые настройки**  1. Для всего активного сетевого оборудования настройте доменное имя wsr2020.wsr  2. Настройте имена устройств в соответствии с диаграммой  3. Создайте локального пользователя admin с паролем Pass  - пользователь должен обладать максимальным уровнем привилегий.  - пароль должен храниться в виде результата хэш функции.  3. Для всех сетевых устройств сконфигурируйте пароль wsr2020 для входа в привилегированный режим.  4. Все сетевые устройства должны быть доступны для управления по протоколу SSHv2.  5. IP адреса устройств взять с таблицы (или с настроек примера).  **Настройка коммутации**  1. Таблица VLAN офиса HQ должна содержать следующие подсети:  VLAN10:CLIENT  VLAN20:SERV  VLAN1000:MANAGE  2. Транки между коммутаторами должны быть согласованы с использованием DTP. SW1 должен инициировать согласование, SW2 и SW3 должны быть настроены в пассивном режиме  3. Транк между SW2 и SW3 должен быть согласован без использования протокола DTP  4. На портах f0/10 коммутаторов SW2 и SW3 сконфигурируйте магистральные каналы без использования динамического согласования. Отключите протокол DTP явным образом.  **Конфигурация портовых групп.**  1. Между коммутаторами SW1 и SW2 настройте агрегирование по протоколу LACP. SW1 должен работать в активном режиме, SW2 в пассивном  2. Между коммутаторами SW1 и SW3 настройте агрегирование по протоколу PAgP. SW1 должен работать в активном режиме, SW3 в пассивном  3. На SW2 настройте балансировку нагрузки по MAC адресу источника + назначения, на SW3 настройте балансировку по IP адресу источника + назначения  **Сконфигурируйте протокол остовного дерева**  1. На всех коммутаторах используйте протокол, совместимый со стандартом 802.1w  2. Корнем для всех VLAN является SW1. При отказе SW1 корнем должен стать SW2. При отказе SW2 корнем должен стать SW3.  3. На портах f0/10 SW2 и SW3 обеспечьте быструю сходимость, без ожидания протокола 802.1w. Аналогичную настройку произведите на магистральном канале между этими двумя коммутаторами.  **Подключение ISP**  1. Для подключения левого офиса использовать обыкновенный Ethernet  2. Подключение правого офиса выполнить по протоколу PPP  - инкапсуляция PPP  - авторизация по протоколу CHAP  - пароль pass  3. Настроить GRE-туннель между правой и левой частью сети.  **Маршрутизация**  1. Обеспечьте маршрутизацию между сетями VLAN с использованием технологии Router-on-a-Stick.  2. В левой части сети настроить протокол OSPF.  3. В правой части сети настроить протокол EIGRP с автономной системой 65001.  4. Маршрут по умолчанию настроить статически в сторону ISP, настроить автомматическое распространение маршрута по умолчанию по сети.  5. Между маршрутизаторами GATE и BRANCH настроить проткол BPG, для GATE автономная система 45002 для BRANCH 45001.  6. Настроить передачу маршрутов для полного согласования сети.  **Подключение к сети интернет**  1. Настроить ретрансляцию адресов на GATE и BRANCH.  **Настройка сервисов**  1. На всех устройствах настроить согласование времени с сервером Google.  2. На RTR настроить DHCP сервер  - распределять сеть для VLAN CLIENT  - в качестве DNS использовать адрес 8.8.8.8  - в качестве шлюза адрес RTR  - первые 20 адресов сети запретить к выдаче.  **Настройка DHCP сервера**  На маршрутизаторе BRANCH сконфигурируйте DHCP сервер.  Обеспечьте возможность доступа в сеть интернет для главного офиса и офиса Branch.  Анонсируйте все сети, необходимые для достижения полной связанности в соответствии со схемой маршрутизации  Настройте аутентификацию.  Преподаватель\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Скиляжнов А.О. |

Министерство образования Красноярского края

краевое государственное бюджетное профессиональное образовательное учреждение «Красноярский колледж радиоэлектроники и информационных технологий»

|  |  |  |  |
| --- | --- | --- | --- |
| |  |  |  | | --- | --- | --- | | |  | | --- | | РАССМОТРЕНО  на заседании цикловой комиссии  преподавателей профессионального  цикла технического профиля  Протокол №\_\_ от «\_\_\_»\_\_\_\_\_\_ 2021 г.  Председатель ЦК \_\_\_\_\_ Е. В. Харитонова | | ДИСЦИПЛИНА  МДК01.02 Организация, принципы построения и функционирования  компьютерных сетей  для специальности  09.02.06 Сетевое и системное\_\_\_\_\_\_\_\_  администрирование\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Семестр 4 группа 9САД1.20, 9САД2.20 |   **ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №**  27  1. [Агрегирование каналов в Cisco](http://xgu.ru/wiki/%D0%90%D0%B3%D1%80%D0%B5%D0%B3%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5_%D0%BA%D0%B0%D0%BD%D0%B0%D0%BB%D0%BE%D0%B2#.D0.90.D0.B3.D1.80.D0.B5.D0.B3.D0.B8.D1.80.D0.BE.D0.B2.D0.B0.D0.BD.D0.B8.D0.B5_.D0.BA.D0.B0.D0.BD.D0.B0.D0.BB.D0.BE.D0.B2_.D0.B2_Cisco). [Терминология и настройка](http://xgu.ru/wiki/%D0%90%D0%B3%D1%80%D0%B5%D0%B3%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5_%D0%BA%D0%B0%D0%BD%D0%B0%D0%BB%D0%BE%D0%B2#.D0.A2.D0.B5.D1.80.D0.BC.D0.B8.D0.BD.D0.BE.D0.BB.D0.BE.D0.B3.D0.B8.D1.8F_.D0.B8_.D0.BD.D0.B0.D1.81.D1.82.D1.80.D0.BE.D0.B9.D0.BA.D0.B0). [Общие правила настройки EtherChannel](http://xgu.ru/wiki/%D0%90%D0%B3%D1%80%D0%B5%D0%B3%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5_%D0%BA%D0%B0%D0%BD%D0%B0%D0%BB%D0%BE%D0%B2#.D0.9E.D0.B1.D1.89.D0.B8.D0.B5_.D0.BF.D1.80.D0.B0.D0.B2.D0.B8.D0.BB.D0.B0_.D0.BD.D0.B0.D1.81.D1.82.D1.80.D0.BE.D0.B9.D0.BA.D0.B8_EtherChannel). [Синтаксис команды channel-group](http://xgu.ru/wiki/%D0%90%D0%B3%D1%80%D0%B5%D0%B3%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5_%D0%BA%D0%B0%D0%BD%D0%B0%D0%BB%D0%BE%D0%B2#.D0.A1.D0.B8.D0.BD.D1.82.D0.B0.D0.BA.D1.81.D0.B8.D1.81_.D0.BA.D0.BE.D0.BC.D0.B0.D0.BD.D0.B4.D1.8B_channel-group). [Интерфейсы в состоянии suspended](http://xgu.ru/wiki/%D0%90%D0%B3%D1%80%D0%B5%D0%B3%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5_%D0%BA%D0%B0%D0%BD%D0%B0%D0%BB%D0%BE%D0%B2#.D0.98.D0.BD.D1.82.D0.B5.D1.80.D1.84.D0.B5.D0.B9.D1.81.D1.8B_.D0.B2_.D1.81.D0.BE.D1.81.D1.82.D0.BE.D1.8F.D0.BD.D0.B8.D0.B8_suspended). [Команды просмотра информации](http://xgu.ru/wiki/%D0%90%D0%B3%D1%80%D0%B5%D0%B3%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5_%D0%BA%D0%B0%D0%BD%D0%B0%D0%BB%D0%BE%D0%B2#.D0.9A.D0.BE.D0.BC.D0.B0.D0.BD.D0.B4.D1.8B_.D0.BF.D1.80.D0.BE.D1.81.D0.BC.D0.BE.D1.82.D1.80.D0.B0_.D0.B8.D0.BD.D1.84.D0.BE.D1.80.D0.BC.D0.B0.D1.86.D0.B8.D0.B8).  2. Практическое задание. Можно пользоваться Интернет. Схема сети.  Если параметры настройки не указаны в задании, необходимо выбрать любые значения, позволяющие выполнить задание (например номера портов в портовых группах).  **Базовые настройки**  1. Для всего активного сетевого оборудования настройте доменное имя wsr2020.wsr  2. Настройте имена устройств в соответствии с диаграммой  3. Создайте локального пользователя admin с паролем Pass  - пользователь должен обладать максимальным уровнем привилегий.  - пароль должен храниться в виде результата хэш функции.  3. Для всех сетевых устройств сконфигурируйте пароль wsr2020 для входа в привилегированный режим.  4. Все сетевые устройства должны быть доступны для управления по протоколу SSHv2.  5. IP адреса устройств взять с таблицы (или с настроек примера).  **Настройка коммутации**  1. Таблица VLAN офиса HQ должна содержать следующие подсети:  VLAN10:CLIENT  VLAN20:SERV  VLAN1000:MANAGE  2. Транки между коммутаторами должны быть согласованы с использованием DTP. SW1 должен инициировать согласование, SW2 и SW3 должны быть настроены в пассивном режиме  3. Транк между SW2 и SW3 должен быть согласован без использования протокола DTP  4. На портах f0/10 коммутаторов SW2 и SW3 сконфигурируйте магистральные каналы без использования динамического согласования. Отключите протокол DTP явным образом.  **Конфигурация портовых групп.**  1. Между коммутаторами SW1 и SW2 настройте агрегирование по протоколу LACP. SW1 должен работать в активном режиме, SW2 в пассивном  2. Между коммутаторами SW1 и SW3 настройте агрегирование по протоколу PAgP. SW1 должен работать в активном режиме, SW3 в пассивном  3. На SW2 настройте балансировку нагрузки по MAC адресу источника + назначения, на SW3 настройте балансировку по IP адресу источника + назначения  **Сконфигурируйте протокол остовного дерева**  1. На всех коммутаторах используйте протокол, совместимый со стандартом 802.1w  2. Корнем для всех VLAN является SW1. При отказе SW1 корнем должен стать SW2. При отказе SW2 корнем должен стать SW3.  3. На портах f0/10 SW2 и SW3 обеспечьте быструю сходимость, без ожидания протокола 802.1w. Аналогичную настройку произведите на магистральном канале между этими двумя коммутаторами.  **Подключение ISP**  1. Для подключения левого офиса использовать обыкновенный Ethernet  2. Подключение правого офиса выполнить по протоколу PPP  - инкапсуляция PPP  - авторизация по протоколу CHAP  - пароль pass  3. Настроить GRE-туннель между правой и левой частью сети.  **Маршрутизация**  1. Обеспечьте маршрутизацию между сетями VLAN с использованием технологии Router-on-a-Stick.  2. В левой части сети настроить протокол OSPF.  3. В правой части сети настроить протокол EIGRP с автономной системой 65001.  4. Маршрут по умолчанию настроить статически в сторону ISP, настроить автомматическое распространение маршрута по умолчанию по сети.  5. Между маршрутизаторами GATE и BRANCH настроить проткол BPG, для GATE автономная система 45002 для BRANCH 45001.  6. Настроить передачу маршрутов для полного согласования сети.  **Подключение к сети интернет**  1. Настроить ретрансляцию адресов на GATE и BRANCH.  **Настройка сервисов**  1. На всех устройствах настроить согласование времени с сервером Google.  2. На RTR настроить DHCP сервер  - распределять сеть для VLAN CLIENT  - в качестве DNS использовать адрес 8.8.8.8  - в качестве шлюза адрес RTR  - первые 20 адресов сети запретить к выдаче.  **Настройка DHCP сервера**  На маршрутизаторе BRANCH сконфигурируйте DHCP сервер.  Обеспечьте возможность доступа в сеть интернет для главного офиса и офиса Branch.  Анонсируйте все сети, необходимые для достижения полной связанности в соответствии со схемой маршрутизации  Настройте аутентификацию.  Преподаватель\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Скиляжнов А.О. |

Министерство образования Красноярского края

краевое государственное бюджетное профессиональное образовательное учреждение «Красноярский колледж радиоэлектроники и информационных технологий»

|  |  |  |  |
| --- | --- | --- | --- |
| |  |  |  | | --- | --- | --- | | |  | | --- | | РАССМОТРЕНО  на заседании цикловой комиссии  преподавателей профессионального  цикла технического профиля  Протокол №\_\_ от «\_\_\_»\_\_\_\_\_\_ 2021 г.  Председатель ЦК \_\_\_\_\_ Е. В. Харитонова | | ДИСЦИПЛИНА  МДК01.02 Организация, принципы построения и функционирования  компьютерных сетей  для специальности  09.02.06 Сетевое и системное\_\_\_\_\_\_\_\_  администрирование\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Семестр 4 группа 9САД1.20, 9САД2.20 |   **ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №**  28  1. Принцип работы RSTP, STP.  2. Практическое задание. Можно пользоваться Интернет. Схема сети.  Если параметры настройки не указаны в задании, необходимо выбрать любые значения, позволяющие выполнить задание (например номера портов в портовых группах).  **Базовые настройки**  1. Для всего активного сетевого оборудования настройте доменное имя wsr2020.wsr  2. Настройте имена устройств в соответствии с диаграммой  3. Создайте локального пользователя admin с паролем Pass  - пользователь должен обладать максимальным уровнем привилегий.  - пароль должен храниться в виде результата хэш функции.  3. Для всех сетевых устройств сконфигурируйте пароль wsr2020 для входа в привилегированный режим.  4. Все сетевые устройства должны быть доступны для управления по протоколу SSHv2.  5. IP адреса устройств взять с таблицы (или с настроек примера).  **Настройка коммутации**  1. Таблица VLAN офиса HQ должна содержать следующие подсети:  VLAN10:CLIENT  VLAN20:SERV  VLAN1000:MANAGE  2. Транки между коммутаторами должны быть согласованы с использованием DTP. SW1 должен инициировать согласование, SW2 и SW3 должны быть настроены в пассивном режиме  3. Транк между SW2 и SW3 должен быть согласован без использования протокола DTP  4. На портах f0/10 коммутаторов SW2 и SW3 сконфигурируйте магистральные каналы без использования динамического согласования. Отключите протокол DTP явным образом.  **Конфигурация портовых групп.**  1. Между коммутаторами SW1 и SW2 настройте агрегирование по протоколу LACP. SW1 должен работать в активном режиме, SW2 в пассивном  2. Между коммутаторами SW1 и SW3 настройте агрегирование по протоколу PAgP. SW1 должен работать в активном режиме, SW3 в пассивном  3. На SW2 настройте балансировку нагрузки по MAC адресу источника + назначения, на SW3 настройте балансировку по IP адресу источника + назначения  **Сконфигурируйте протокол остовного дерева**  1. На всех коммутаторах используйте протокол, совместимый со стандартом 802.1w  2. Корнем для всех VLAN является SW1. При отказе SW1 корнем должен стать SW2. При отказе SW2 корнем должен стать SW3.  3. На портах f0/10 SW2 и SW3 обеспечьте быструю сходимость, без ожидания протокола 802.1w. Аналогичную настройку произведите на магистральном канале между этими двумя коммутаторами.  **Подключение ISP**  1. Для подключения левого офиса использовать обыкновенный Ethernet  2. Подключение правого офиса выполнить по протоколу PPP  - инкапсуляция PPP  - авторизация по протоколу CHAP  - пароль pass  3. Настроить GRE-туннель между правой и левой частью сети.  **Маршрутизация**  1. Обеспечьте маршрутизацию между сетями VLAN с использованием технологии Router-on-a-Stick.  2. В левой части сети настроить протокол OSPF.  3. В правой части сети настроить протокол EIGRP с автономной системой 65001.  4. Маршрут по умолчанию настроить статически в сторону ISP, настроить автомматическое распространение маршрута по умолчанию по сети.  5. Между маршрутизаторами GATE и BRANCH настроить проткол BPG, для GATE автономная система 45002 для BRANCH 45001.  6. Настроить передачу маршрутов для полного согласования сети.  **Подключение к сети интернет**  1. Настроить ретрансляцию адресов на GATE и BRANCH.  **Настройка сервисов**  1. На всех устройствах настроить согласование времени с сервером Google.  2. На RTR настроить DHCP сервер  - распределять сеть для VLAN CLIENT  - в качестве DNS использовать адрес 8.8.8.8  - в качестве шлюза адрес RTR  - первые 20 адресов сети запретить к выдаче.  **Настройка DHCP сервера**  На маршрутизаторе BRANCH сконфигурируйте DHCP сервер.  Обеспечьте возможность доступа в сеть интернет для главного офиса и офиса Branch.  Анонсируйте все сети, необходимые для достижения полной связанности в соответствии со схемой маршрутизации  Настройте аутентификацию.  Преподаватель\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Скиляжнов А.О. |

Министерство образования Красноярского края

краевое государственное бюджетное профессиональное образовательное учреждение «Красноярский колледж радиоэлектроники информационных технологий»

|  |  |
| --- | --- |
| РАССМОТРЕНО  на заседании цикловой комиссии  преподавателей профессионального цикла  технического профиля  Протокол № \_\_\_ от «\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_ 2021г  Председатель \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Е.В. Харитонова | УТВЕРЖДАЮ  Заместитель директора  по учебной работе  \_\_\_\_\_\_\_\_\_\_\_\_\_ М.А. Полютова  «\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 2021 г |

**ЭКЗАМЕНАЦИОННЫЕ БИЛЕТЫ**

**для проверки уровня подготовки студентов в соответствии**

**с требованиями федерального государственного образовательного стандарта СПО**

|  |  |
| --- | --- |
| Дисциплина | МДК 01.02 Организация, принципы построения и функционирования компьютерных сетей |
| Специальность | 09.02.06 Сетевое и системное администрирование |
| Курс | 3 |
| Форма обучения | очная |
| Количество билетов | 30 |
| Преподаватель | Скиляжнов А.О. |

Красноярск, 2023

Министерство образования Красноярского края

краевое государственное бюджетное профессиональное образовательное учреждение «Красноярский колледж радиоэлектроники и

информационных технологий»

|  |  |
| --- | --- |
| РАССМОТРЕНО  на заседании цикловой комиссии  преподавателей профессионального  цикла технического профиля  Протокол №\_\_ от «\_\_\_»\_\_\_\_\_\_ 2023 г .  Председатель ЦК \_\_\_\_\_ Е. В. Харитонова | УТВЕРЖДАЮ  Заместитель директора  по учебной работе  \_\_\_\_\_\_\_\_\_\_\_ М. А. Полютова  «\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 2023 г |

Экзаменационные билеты

Для проверки уровня подготовки студентов в соответствии с требованиями государственного образовательного стандарта

МДК 01.02 Организация, принципы построения и функционирования компьютерных сетей

**ПМ 01 «УЧАСТИЕ В ПРОЕКТИРОВАНИИ СЕТЕВОЙ ИНФРАСТРУКТУРЫ**

для студентов специальности (ей)

09.02.06 «Сетевое и системное администрирование», базовой подготовки

Разработал

преподаватель КГБПОУ «ККРИТ»

Скиляжнов А.О.

Красноярск, 2023

Министерство образования Красноярского края

краевое государственное бюджетное профессиональное образовательное учреждение «Красноярский колледж радиоэлектроники и информационных технологий»

|  |  |  |  |
| --- | --- | --- | --- |
| |  |  |  | | --- | --- | --- | | |  | | --- | | РАССМОТРЕНО  на заседании цикловой комиссии  преподавателей профессионального  цикла технического профиля  Протокол №\_\_ от «\_\_\_»\_\_\_\_\_\_ 2021 г.  Председатель ЦК \_\_\_\_\_ Е. В. Харитонова | | ДИСЦИПЛИНА  МДК01.02 Организация, принципы построения и функционирования  компьютерных сетей  для специальности  09.02.06 Сетевое и системное\_\_\_\_\_\_\_\_  администрирование\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Семестр 5 группа 9САД1.20, 9САД2.20 |   **ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №**  1  1. Программно-определяемые сети. Традиционная архитектура и архитектура SDN. Контроллер и операции SDN. Типы SDN. Автоматизация сети. Рост автоматизации. Умные устройства.  2. Практическое задание. Можно пользоваться Интернет. Схема сети.  У некоторой компании есть главный офис, который подключается в Интернет. Пограничный маршрутизатор Border подключен к провайдеру, который предоставляет услуги Интернет. Также существует второй офис компании, который таже подключен к публичной сети. И между ними проброшен VPN туннель. Между роутерами установлен OSPF, а между роутерами интернет компании и главным офисом установлена статическая маршрутизация. На основных коммутаторах офиса установлены по триVLAN, на роутерах сабинтерфейсы.  Для всего активного сетевого оборудования настройте доменное имя wsr2020.wsr. Создайте локального пользователя admin с паролем Pa$$w0rd. Для активного сетевого оборудования: пользователь должен обладать максимальным уровнем привилегий, пароль должен храниться в виде результата хэш функции, используйте алгоритм scrypt. Для всех сетевых устройств сконфигурируйте пароль wsr2020 для входа в привилегированный режим. Все сетевые устройства должны быть доступны для управления по протоколу SSHv2. Зашифруйте все открытые пароли.  Таблица VLAN двух офисов должна содержать следующие подсети: VLAN10:CLIENT, VLAN20:SERV, VLAN30:DMZ. Сконфигурируйте магистральные каналы.  Настройте подключение Border к провайдеру ISP с помощью протокола PPP. Адрес необходимо получить при помощи IPCP. Аутентификация не требуется.  Транспортный адрес необходимо получить при помощи протокола SLARP на соответствующий Serial интерфейс.  Устройства проходят аутентификацию по протоколу CHAP в одностороннем порядке. Только ISP аутентифицирует роутер Border. Для аутентификации используйте данные client65010 и пароль P@ssw0rd. Явно сконфигурируйте корректное значение MTU.  Сконфигурируйте GRE туннель между BRANCH1 и BRANCH2. В качестве адресов источника и назначения используйте адреса соответствующих loopback интерфейсов. Используйте номер туннельного интерфейса 1.  Обеспечьте возможность входа на Border c использованием доменных реквизитов. Группа MAdmins должна получать максимальный уровень привилегий при входе. Группа SAdmins должна получать при входе уровень привилегий. Обеспечьте возможность входа пользователя, созданного локально при доступности RADIUS сервера. Для 5 уровня привилегий сконфигурируйте расширенный набор команд. Добавьте возможность использования команд reload, debug и sh.  В главном офисе на сервере установлен DHCP, который раздает адресацию на все сетевые устройства. Здесь же установлены службы ААА, DNS, HTTP. Во втором офисе компании установленWeb-server и DMZ. На роутере Border установлена служба NAT.  Преподаватель\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Скиляжнов А.О. |

Министерство образования Красноярского края

краевое государственное бюджетное профессиональное образовательное учреждение «Красноярский колледж радиоэлектроники и информационных технологий»

|  |  |  |  |
| --- | --- | --- | --- |
| |  |  |  | | --- | --- | --- | | |  | | --- | | РАССМОТРЕНО  на заседании цикловой комиссии  преподавателей профессионального  цикла технического профиля  Протокол №\_\_ от «\_\_\_»\_\_\_\_\_\_ 2021 г.  Председатель ЦК \_\_\_\_\_ Е. В. Харитонова | | ДИСЦИПЛИНА  МДК01.02 Организация, принципы построения и функционирования  компьютерных сетей  для специальности  09.02.06 Сетевое и системное\_\_\_\_\_\_\_\_  администрирование\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Семестр 5 группа 9САД1.20, 9САД2.20 |   **ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №**  2  1. Обзор облачных вычислений. Облачные вычисления и центр обработки данных. Облачные вычисления и виртуализация. Виртуализация серверов. Уровни абстракции. Установка виртуальной машины на гипервизоре. Сложность виртуализации сети.  2. Практическое задание. Можно пользоваться Интернет. Схема сети.  У некоторой компании есть главный офис, который подключается в Интернет. Пограничный маршрутизатор Border подключен к провайдеру, который предоставляет услуги Интернет. Также существует второй офис компании, который таже подключен к публичной сети. И между ними проброшен VPN туннель. Между роутерами установлен OSPF, а между роутерами интернет компании и главным офисом установлена статическая маршрутизация. На основных коммутаторах офиса установлены по триVLAN, на роутерах сабинтерфейсы.  Для всего активного сетевого оборудования настройте доменное имя wsr2020.wsr. Создайте локального пользователя admin с паролем Pa$$w0rd. Для активного сетевого оборудования: пользователь должен обладать максимальным уровнем привилегий, пароль должен храниться в виде результата хэш функции, используйте алгоритм scrypt. Для всех сетевых устройств сконфигурируйте пароль wsr2020 для входа в привилегированный режим. Все сетевые устройства должны быть доступны для управления по протоколу SSHv2. Зашифруйте все открытые пароли.  Таблица VLAN двух офисов должна содержать следующие подсети: VLAN10:CLIENT, VLAN20:SERV, VLAN30:DMZ. Сконфигурируйте магистральные каналы.  Настройте подключение Border к провайдеру ISP с помощью протокола PPP. Адрес необходимо получить при помощи IPCP. Аутентификация не требуется.  Транспортный адрес необходимо получить при помощи протокола SLARP на соответствующий Serial интерфейс.  Устройства проходят аутентификацию по протоколу CHAP в одностороннем порядке. Только ISP аутентифицирует роутер Border. Для аутентификации используйте данные client65010 и пароль P@ssw0rd. Явно сконфигурируйте корректное значение MTU.  Сконфигурируйте GRE туннель между BRANCH1 и BRANCH2. В качестве адресов источника и назначения используйте адреса соответствующих loopback интерфейсов. Используйте номер туннельного интерфейса 1.  Обеспечьте возможность входа на Border c использованием доменных реквизитов. Группа MAdmins должна получать максимальный уровень привилегий при входе. Группа SAdmins должна получать при входе уровень привилегий. Обеспечьте возможность входа пользователя, созданного локально при доступности RADIUS сервера. Для 5 уровня привилегий сконфигурируйте расширенный набор команд. Добавьте возможность использования команд reload, debug и sh.  В главном офисе на сервере установлен DHCP, который раздает адресацию на все сетевые устройства. Здесь же установлены службы ААА, DNS, HTTP. Во втором офисе компании установленWeb-server и DMZ. На роутере Border установлена служба NAT.  Преподаватель\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Скиляжнов А.О. |

Министерство образования Красноярского края

краевое государственное бюджетное профессиональное образовательное учреждение «Красноярский колледж радиоэлектроники и информационных технологий»

|  |  |  |  |
| --- | --- | --- | --- |
| |  |  |  | | --- | --- | --- | | |  | | --- | | РАССМОТРЕНО  на заседании цикловой комиссии  преподавателей профессионального  цикла технического профиля  Протокол №\_\_ от «\_\_\_»\_\_\_\_\_\_ 2021 г.  Председатель ЦК \_\_\_\_\_ Е. В. Харитонова | | ДИСЦИПЛИНА  МДК01.02 Организация, принципы построения и функционирования  компьютерных сетей  для специальности  09.02.06 Сетевое и системное\_\_\_\_\_\_\_\_  администрирование\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Семестр 5 группа 9САД1.20, 9САД2.20 |   **ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №**  3  1. Общие сведения о протоколе LLDP Настройка и проверка протокола LLDP. Поиск устройств с помощью LLDP. Инструмент проверки синтаксиса: настройка и проверка протокола LLDP.  2. Практическое задание. Можно пользоваться Интернет. Схема сети.  У некоторой компании есть главный офис, который подключается в Интернет. Пограничный маршрутизатор Border подключен к провайдеру, который предоставляет услуги Интернет. Также существует второй офис компании, который таже подключен к публичной сети. И между ними проброшен VPN туннель. Между роутерами установлен OSPF, а между роутерами интернет компании и главным офисом установлена статическая маршрутизация. На основных коммутаторах офиса установлены по триVLAN, на роутерах сабинтерфейсы.  Для всего активного сетевого оборудования настройте доменное имя wsr2020.wsr. Создайте локального пользователя admin с паролем Pa$$w0rd. Для активного сетевого оборудования: пользователь должен обладать максимальным уровнем привилегий, пароль должен храниться в виде результата хэш функции, используйте алгоритм scrypt. Для всех сетевых устройств сконфигурируйте пароль wsr2020 для входа в привилегированный режим. Все сетевые устройства должны быть доступны для управления по протоколу SSHv2. Зашифруйте все открытые пароли.  Таблица VLAN двух офисов должна содержать следующие подсети: VLAN10:CLIENT, VLAN20:SERV, VLAN30:DMZ. Сконфигурируйте магистральные каналы.  Настройте подключение Border к провайдеру ISP с помощью протокола PPP. Адрес необходимо получить при помощи IPCP. Аутентификация не требуется.  Транспортный адрес необходимо получить при помощи протокола SLARP на соответствующий Serial интерфейс.  Устройства проходят аутентификацию по протоколу CHAP в одностороннем порядке. Только ISP аутентифицирует роутер Border. Для аутентификации используйте данные client65010 и пароль P@ssw0rd. Явно сконфигурируйте корректное значение MTU.  Сконфигурируйте GRE туннель между BRANCH1 и BRANCH2. В качестве адресов источника и назначения используйте адреса соответствующих loopback интерфейсов. Используйте номер туннельного интерфейса 1.  Обеспечьте возможность входа на Border c использованием доменных реквизитов. Группа MAdmins должна получать максимальный уровень привилегий при входе. Группа SAdmins должна получать при входе уровень привилегий. Обеспечьте возможность входа пользователя, созданного локально при доступности RADIUS сервера. Для 5 уровня привилегий сконфигурируйте расширенный набор команд. Добавьте возможность использования команд reload, debug и sh.  В главном офисе на сервере установлен DHCP, который раздает адресацию на все сетевые устройства. Здесь же установлены службы ААА, DNS, HTTP. Во втором офисе компании установленWeb-server и DMZ. На роутере Border установлена служба NAT.  Преподаватель\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Скиляжнов А.О. |

Министерство образования Красноярского края

краевое государственное бюджетное профессиональное образовательное учреждение «Красноярский колледж радиоэлектроники и информационных технологий»

|  |  |  |  |
| --- | --- | --- | --- |
| |  |  |  | | --- | --- | --- | | |  | | --- | | РАССМОТРЕНО  на заседании цикловой комиссии  преподавателей профессионального  цикла технического профиля  Протокол №\_\_ от «\_\_\_»\_\_\_\_\_\_ 2021 г.  Председатель ЦК \_\_\_\_\_ Е. В. Харитонова | | ДИСЦИПЛИНА  МДК01.02 Организация, принципы построения и функционирования  компьютерных сетей  для специальности  09.02.06 Сетевое и системное\_\_\_\_\_\_\_\_  администрирование\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Семестр 5 группа 9САД1.20, 9САД2.20 |   **ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №**  4  1. Настройка и проверка CDP. Поиск устройств с помощью CDP. Инструмент проверки синтаксиса: настройка и проверка протокола CDP.  2. Практическое задание. Можно пользоваться Интернет. Схема сети.  У некоторой компании есть главный офис, который подключается в Интернет. Пограничный маршрутизатор Border подключен к провайдеру, который предоставляет услуги Интернет. Также существует второй офис компании, который таже подключен к публичной сети. И между ними проброшен VPN туннель. Между роутерами установлен OSPF, а между роутерами интернет компании и главным офисом установлена статическая маршрутизация. На основных коммутаторах офиса установлены по триVLAN, на роутерах сабинтерфейсы.  Для всего активного сетевого оборудования настройте доменное имя wsr2020.wsr. Создайте локального пользователя admin с паролем Pa$$w0rd. Для активного сетевого оборудования: пользователь должен обладать максимальным уровнем привилегий, пароль должен храниться в виде результата хэш функции, используйте алгоритм scrypt. Для всех сетевых устройств сконфигурируйте пароль wsr2020 для входа в привилегированный режим. Все сетевые устройства должны быть доступны для управления по протоколу SSHv2. Зашифруйте все открытые пароли.  Таблица VLAN двух офисов должна содержать следующие подсети: VLAN10:CLIENT, VLAN20:SERV, VLAN30:DMZ. Сконфигурируйте магистральные каналы.  Настройте подключение Border к провайдеру ISP с помощью протокола PPP. Адрес необходимо получить при помощи IPCP. Аутентификация не требуется.  Транспортный адрес необходимо получить при помощи протокола SLARP на соответствующий Serial интерфейс.  Устройства проходят аутентификацию по протоколу CHAP в одностороннем порядке. Только ISP аутентифицирует роутер Border. Для аутентификации используйте данные client65010 и пароль P@ssw0rd. Явно сконфигурируйте корректное значение MTU.  Сконфигурируйте GRE туннель между BRANCH1 и BRANCH2. В качестве адресов источника и назначения используйте адреса соответствующих loopback интерфейсов. Используйте номер туннельного интерфейса 1.  Обеспечьте возможность входа на Border c использованием доменных реквизитов. Группа MAdmins должна получать максимальный уровень привилегий при входе. Группа SAdmins должна получать при входе уровень привилегий. Обеспечьте возможность входа пользователя, созданного локально при доступности RADIUS сервера. Для 5 уровня привилегий сконфигурируйте расширенный набор команд. Добавьте возможность использования команд reload, debug и sh.  В главном офисе на сервере установлен DHCP, который раздает адресацию на все сетевые устройства. Здесь же установлены службы ААА, DNS, HTTP. Во втором офисе компании установленWeb-server и DMZ. На роутере Border установлена служба NAT.  Преподаватель\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Скиляжнов А.О. |

Министерство образования Красноярского края

краевое государственное бюджетное профессиональное образовательное учреждение «Красноярский колледж радиоэлектроники и информационных технологий»

|  |  |  |  |
| --- | --- | --- | --- |
| |  |  |  | | --- | --- | --- | | |  | | --- | | РАССМОТРЕНО  на заседании цикловой комиссии  преподавателей профессионального  цикла технического профиля  Протокол №\_\_ от «\_\_\_»\_\_\_\_\_\_ 2021 г.  Председатель ЦК \_\_\_\_\_ Е. В. Харитонова | | ДИСЦИПЛИНА  МДК01.02 Организация, принципы построения и функционирования  компьютерных сетей  для специальности  09.02.06 Сетевое и системное\_\_\_\_\_\_\_\_  администрирование\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Семестр 5 группа 9САД1.20, 9САД2.20 |   **ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №**  5  1. Средство выбора класса (CS). Границы доверия. Предотвращение затора. Руководящие принципы политики QoS.  2. Практическое задание. Можно пользоваться Интернет. Схема сети.  У некоторой компании есть главный офис, который подключается в Интернет. Пограничный маршрутизатор Border подключен к провайдеру, который предоставляет услуги Интернет. Также существует второй офис компании, который таже подключен к публичной сети. И между ними проброшен VPN туннель. Между роутерами установлен OSPF, а между роутерами интернет компании и главным офисом установлена статическая маршрутизация. На основных коммутаторах офиса установлены по триVLAN, на роутерах сабинтерфейсы.  Для всего активного сетевого оборудования настройте доменное имя wsr2020.wsr. Создайте локального пользователя admin с паролем Pa$$w0rd. Для активного сетевого оборудования: пользователь должен обладать максимальным уровнем привилегий, пароль должен храниться в виде результата хэш функции, используйте алгоритм scrypt. Для всех сетевых устройств сконфигурируйте пароль wsr2020 для входа в привилегированный режим. Все сетевые устройства должны быть доступны для управления по протоколу SSHv2. Зашифруйте все открытые пароли.  Таблица VLAN двух офисов должна содержать следующие подсети: VLAN10:CLIENT, VLAN20:SERV, VLAN30:DMZ. Сконфигурируйте магистральные каналы.  Настройте подключение Border к провайдеру ISP с помощью протокола PPP. Адрес необходимо получить при помощи IPCP. Аутентификация не требуется.  Транспортный адрес необходимо получить при помощи протокола SLARP на соответствующий Serial интерфейс.  Устройства проходят аутентификацию по протоколу CHAP в одностороннем порядке. Только ISP аутентифицирует роутер Border. Для аутентификации используйте данные client65010 и пароль P@ssw0rd. Явно сконфигурируйте корректное значение MTU.  Сконфигурируйте GRE туннель между BRANCH1 и BRANCH2. В качестве адресов источника и назначения используйте адреса соответствующих loopback интерфейсов. Используйте номер туннельного интерфейса 1.  Обеспечьте возможность входа на Border c использованием доменных реквизитов. Группа MAdmins должна получать максимальный уровень привилегий при входе. Группа SAdmins должна получать при входе уровень привилегий. Обеспечьте возможность входа пользователя, созданного локально при доступности RADIUS сервера. Для 5 уровня привилегий сконфигурируйте расширенный набор команд. Добавьте возможность использования команд reload, debug и sh.  В главном офисе на сервере установлен DHCP, который раздает адресацию на все сетевые устройства. Здесь же установлены службы ААА, DNS, HTTP. Во втором офисе компании установленWeb-server и DMZ. На роутере Border установлена служба NAT.  Преподаватель\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Скиляжнов А.О. |

Министерство образования Красноярского края

краевое государственное бюджетное профессиональное образовательное учреждение «Красноярский колледж радиоэлектроники и информационных технологий»

|  |  |  |  |
| --- | --- | --- | --- |
| |  |  |  | | --- | --- | --- | | |  | | --- | | РАССМОТРЕНО  на заседании цикловой комиссии  преподавателей профессионального  цикла технического профиля  Протокол №\_\_ от «\_\_\_»\_\_\_\_\_\_ 2021 г.  Председатель ЦК \_\_\_\_\_ Е. В. Харитонова | | ДИСЦИПЛИНА  МДК01.02 Организация, принципы построения и функционирования  компьютерных сетей  для специальности  09.02.06 Сетевое и системное\_\_\_\_\_\_\_\_  администрирование\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Семестр 5 группа 9САД1.20, 9САД2.20 |   **ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №**  6  1. Методы внедрения QoS. Предотвращение потери пакетов. Классификация и маркировка. Поле «Тип обслуживания / Класс трафика». Значения DSCP.  2. Практическое задание. Можно пользоваться Интернет. Схема сети.  У некоторой компании есть главный офис, который подключается в Интернет. Пограничный маршрутизатор Border подключен к провайдеру, который предоставляет услуги Интернет. Также существует второй офис компании, который таже подключен к публичной сети. И между ними проброшен VPN туннель. Между роутерами установлен OSPF, а между роутерами интернет компании и главным офисом установлена статическая маршрутизация. На основных коммутаторах офиса установлены по триVLAN, на роутерах сабинтерфейсы.  Для всего активного сетевого оборудования настройте доменное имя wsr2020.wsr. Создайте локального пользователя admin с паролем Pa$$w0rd. Для активного сетевого оборудования: пользователь должен обладать максимальным уровнем привилегий, пароль должен храниться в виде результата хэш функции, используйте алгоритм scrypt. Для всех сетевых устройств сконфигурируйте пароль wsr2020 для входа в привилегированный режим. Все сетевые устройства должны быть доступны для управления по протоколу SSHv2. Зашифруйте все открытые пароли.  Таблица VLAN двух офисов должна содержать следующие подсети: VLAN10:CLIENT, VLAN20:SERV, VLAN30:DMZ. Сконфигурируйте магистральные каналы.  Настройте подключение Border к провайдеру ISP с помощью протокола PPP. Адрес необходимо получить при помощи IPCP. Аутентификация не требуется.  Транспортный адрес необходимо получить при помощи протокола SLARP на соответствующий Serial интерфейс.  Устройства проходят аутентификацию по протоколу CHAP в одностороннем порядке. Только ISP аутентифицирует роутер Border. Для аутентификации используйте данные client65010 и пароль P@ssw0rd. Явно сконфигурируйте корректное значение MTU.  Сконфигурируйте GRE туннель между BRANCH1 и BRANCH2. В качестве адресов источника и назначения используйте адреса соответствующих loopback интерфейсов. Используйте номер туннельного интерфейса 1.  Обеспечьте возможность входа на Border c использованием доменных реквизитов. Группа MAdmins должна получать максимальный уровень привилегий при входе. Группа SAdmins должна получать при входе уровень привилегий. Обеспечьте возможность входа пользователя, созданного локально при доступности RADIUS сервера. Для 5 уровня привилегий сконфигурируйте расширенный набор команд. Добавьте возможность использования команд reload, debug и sh.  В главном офисе на сервере установлен DHCP, который раздает адресацию на все сетевые устройства. Здесь же установлены службы ААА, DNS, HTTP. Во втором офисе компании установленWeb-server и DMZ. На роутере Border установлена служба NAT.  Преподаватель\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Скиляжнов А.О. |

Министерство образования Красноярского края

краевое государственное бюджетное профессиональное образовательное учреждение «Красноярский колледж радиоэлектроники и информационных технологий»

|  |  |  |  |
| --- | --- | --- | --- |
| |  |  |  | | --- | --- | --- | | |  | | --- | | РАССМОТРЕНО  на заседании цикловой комиссии  преподавателей профессионального  цикла технического профиля  Протокол №\_\_ от «\_\_\_»\_\_\_\_\_\_ 2021 г.  Председатель ЦК \_\_\_\_\_ Е. В. Харитонова | | ДИСЦИПЛИНА  МДК01.02 Организация, принципы построения и функционирования  компьютерных сетей  для специальности  09.02.06 Сетевое и системное\_\_\_\_\_\_\_\_  администрирование\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Семестр 5 группа 9САД1.20, 9САД2.20 |   **ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №**  7  1. Модели обеспечения качества обслуживания. Модели QoS. Выбор подходящей модели политики качества обслуживания. Негарантированная доставка. Интегрированные сервисы. Дифференцированные услуги. Способы обеспечения качества обслуживания.  2. Практическое задание. Можно пользоваться Интернет. Схема сети.  У некоторой компании есть главный офис, который подключается в Интернет. Пограничный маршрутизатор Border подключен к провайдеру, который предоставляет услуги Интернет. Также существует второй офис компании, который таже подключен к публичной сети. И между ними проброшен VPN туннель. Между роутерами установлен OSPF, а между роутерами интернет компании и главным офисом установлена статическая маршрутизация. На основных коммутаторах офиса установлены по триVLAN, на роутерах сабинтерфейсы.  Для всего активного сетевого оборудования настройте доменное имя wsr2020.wsr. Создайте локального пользователя admin с паролем Pa$$w0rd. Для активного сетевого оборудования: пользователь должен обладать максимальным уровнем привилегий, пароль должен храниться в виде результата хэш функции, используйте алгоритм scrypt. Для всех сетевых устройств сконфигурируйте пароль wsr2020 для входа в привилегированный режим. Все сетевые устройства должны быть доступны для управления по протоколу SSHv2. Зашифруйте все открытые пароли.  Таблица VLAN двух офисов должна содержать следующие подсети: VLAN10:CLIENT, VLAN20:SERV, VLAN30:DMZ. Сконфигурируйте магистральные каналы.  Настройте подключение Border к провайдеру ISP с помощью протокола PPP. Адрес необходимо получить при помощи IPCP. Аутентификация не требуется.  Транспортный адрес необходимо получить при помощи протокола SLARP на соответствующий Serial интерфейс.  Устройства проходят аутентификацию по протоколу CHAP в одностороннем порядке. Только ISP аутентифицирует роутер Border. Для аутентификации используйте данные client65010 и пароль P@ssw0rd. Явно сконфигурируйте корректное значение MTU.  Сконфигурируйте GRE туннель между BRANCH1 и BRANCH2. В качестве адресов источника и назначения используйте адреса соответствующих loopback интерфейсов. Используйте номер туннельного интерфейса 1.  Обеспечьте возможность входа на Border c использованием доменных реквизитов. Группа MAdmins должна получать максимальный уровень привилегий при входе. Группа SAdmins должна получать при входе уровень привилегий. Обеспечьте возможность входа пользователя, созданного локально при доступности RADIUS сервера. Для 5 уровня привилегий сконфигурируйте расширенный набор команд. Добавьте возможность использования команд reload, debug и sh.  В главном офисе на сервере установлен DHCP, который раздает адресацию на все сетевые устройства. Здесь же установлены службы ААА, DNS, HTTP. Во втором офисе компании установленWeb-server и DMZ. На роутере Border установлена служба NAT.  Преподаватель\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Скиляжнов А.О. |

Министерство образования Красноярского края

краевое государственное бюджетное профессиональное образовательное учреждение «Красноярский колледж радиоэлектроники и информационных технологий»

|  |  |  |  |
| --- | --- | --- | --- |
| |  |  |  | | --- | --- | --- | | |  | | --- | | РАССМОТРЕНО  на заседании цикловой комиссии  преподавателей профессионального  цикла технического профиля  Протокол №\_\_ от «\_\_\_»\_\_\_\_\_\_ 2021 г.  Председатель ЦК \_\_\_\_\_ Е. В. Харитонова | | ДИСЦИПЛИНА  МДК01.02 Организация, принципы построения и функционирования  компьютерных сетей  для специальности  09.02.06 Сетевое и системное\_\_\_\_\_\_\_\_  администрирование\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Семестр 5 группа 9САД1.20, 9САД2.20 |   **ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №**  8  1. Алгоритмы QoS. Взвешенная организация очередей (WFQ). Взвешенная организация очередей на основе классов (CBWFQ). Организация очередей с малой задержкой (LLQ).  2. Практическое задание. Можно пользоваться Интернет. Схема сети.  У некоторой компании есть главный офис, который подключается в Интернет. Пограничный маршрутизатор Border подключен к провайдеру, который предоставляет услуги Интернет. Также существует второй офис компании, который таже подключен к публичной сети. И между ними проброшен VPN туннель. Между роутерами установлен OSPF, а между роутерами интернет компании и главным офисом установлена статическая маршрутизация. На основных коммутаторах офиса установлены по триVLAN, на роутерах сабинтерфейсы.  Для всего активного сетевого оборудования настройте доменное имя wsr2020.wsr. Создайте локального пользователя admin с паролем Pa$$w0rd. Для активного сетевого оборудования: пользователь должен обладать максимальным уровнем привилегий, пароль должен храниться в виде результата хэш функции, используйте алгоритм scrypt. Для всех сетевых устройств сконфигурируйте пароль wsr2020 для входа в привилегированный режим. Все сетевые устройства должны быть доступны для управления по протоколу SSHv2. Зашифруйте все открытые пароли.  Таблица VLAN двух офисов должна содержать следующие подсети: VLAN10:CLIENT, VLAN20:SERV, VLAN30:DMZ. Сконфигурируйте магистральные каналы.  Настройте подключение Border к провайдеру ISP с помощью протокола PPP. Адрес необходимо получить при помощи IPCP. Аутентификация не требуется.  Транспортный адрес необходимо получить при помощи протокола SLARP на соответствующий Serial интерфейс.  Устройства проходят аутентификацию по протоколу CHAP в одностороннем порядке. Только ISP аутентифицирует роутер Border. Для аутентификации используйте данные client65010 и пароль P@ssw0rd. Явно сконфигурируйте корректное значение MTU.  Сконфигурируйте GRE туннель между BRANCH1 и BRANCH2. В качестве адресов источника и назначения используйте адреса соответствующих loopback интерфейсов. Используйте номер туннельного интерфейса 1.  Обеспечьте возможность входа на Border c использованием доменных реквизитов. Группа MAdmins должна получать максимальный уровень привилегий при входе. Группа SAdmins должна получать при входе уровень привилегий. Обеспечьте возможность входа пользователя, созданного локально при доступности RADIUS сервера. Для 5 уровня привилегий сконфигурируйте расширенный набор команд. Добавьте возможность использования команд reload, debug и sh.  В главном офисе на сервере установлен DHCP, который раздает адресацию на все сетевые устройства. Здесь же установлены службы ААА, DNS, HTTP. Во втором офисе компании установленWeb-server и DMZ. На роутере Border установлена служба NAT.  Преподаватель\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Скиляжнов А.О. |

Министерство образования Красноярского края

краевое государственное бюджетное профессиональное образовательное учреждение «Красноярский колледж радиоэлектроники и информационных технологий»

|  |  |  |  |
| --- | --- | --- | --- |
| |  |  |  | | --- | --- | --- | | |  | | --- | | РАССМОТРЕНО  на заседании цикловой комиссии  преподавателей профессионального  цикла технического профиля  Протокол №\_\_ от «\_\_\_»\_\_\_\_\_\_ 2021 г.  Председатель ЦК \_\_\_\_\_ Е. В. Харитонова | | ДИСЦИПЛИНА  МДК01.02 Организация, принципы построения и функционирования  компьютерных сетей  для специальности  09.02.06 Сетевое и системное\_\_\_\_\_\_\_\_  администрирование\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Семестр 5 группа 9САД1.20, 9САД2.20 |   **ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №**  9  1. Качество передачи данных по сети QoS. Установка приоритетов трафика. Пропускная способность, перегрузка, задержка и джиттер. Характеристики трафика. Тенденции сетевого трафика. Оптимизация передачи.  2. Практическое задание. Можно пользоваться Интернет. Схема сети.  У некоторой компании есть главный офис, который подключается в Интернет. Пограничный маршрутизатор Border подключен к провайдеру, который предоставляет услуги Интернет. Также существует второй офис компании, который таже подключен к публичной сети. И между ними проброшен VPN туннель. Между роутерами установлен OSPF, а между роутерами интернет компании и главным офисом установлена статическая маршрутизация. На основных коммутаторах офиса установлены по триVLAN, на роутерах сабинтерфейсы.  Для всего активного сетевого оборудования настройте доменное имя wsr2020.wsr. Создайте локального пользователя admin с паролем Pa$$w0rd. Для активного сетевого оборудования: пользователь должен обладать максимальным уровнем привилегий, пароль должен храниться в виде результата хэш функции, используйте алгоритм scrypt. Для всех сетевых устройств сконфигурируйте пароль wsr2020 для входа в привилегированный режим. Все сетевые устройства должны быть доступны для управления по протоколу SSHv2. Зашифруйте все открытые пароли.  Таблица VLAN двух офисов должна содержать следующие подсети: VLAN10:CLIENT, VLAN20:SERV, VLAN30:DMZ. Сконфигурируйте магистральные каналы.  Настройте подключение Border к провайдеру ISP с помощью протокола PPP. Адрес необходимо получить при помощи IPCP. Аутентификация не требуется.  Транспортный адрес необходимо получить при помощи протокола SLARP на соответствующий Serial интерфейс.  Устройства проходят аутентификацию по протоколу CHAP в одностороннем порядке. Только ISP аутентифицирует роутер Border. Для аутентификации используйте данные client65010 и пароль P@ssw0rd. Явно сконфигурируйте корректное значение MTU.  Сконфигурируйте GRE туннель между BRANCH1 и BRANCH2. В качестве адресов источника и назначения используйте адреса соответствующих loopback интерфейсов. Используйте номер туннельного интерфейса 1.  Обеспечьте возможность входа на Border c использованием доменных реквизитов. Группа MAdmins должна получать максимальный уровень привилегий при входе. Группа SAdmins должна получать при входе уровень привилегий. Обеспечьте возможность входа пользователя, созданного локально при доступности RADIUS сервера. Для 5 уровня привилегий сконфигурируйте расширенный набор команд. Добавьте возможность использования команд reload, debug и sh.  В главном офисе на сервере установлен DHCP, который раздает адресацию на все сетевые устройства. Здесь же установлены службы ААА, DNS, HTTP. Во втором офисе компании установленWeb-server и DMZ. На роутере Border установлена служба NAT.  Преподаватель\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Скиляжнов А.О. |

Министерство образования Красноярского края

краевое государственное бюджетное профессиональное образовательное учреждение «Красноярский колледж радиоэлектроники и информационных технологий»

|  |  |  |  |
| --- | --- | --- | --- |
| |  |  |  | | --- | --- | --- | | |  | | --- | | РАССМОТРЕНО  на заседании цикловой комиссии  преподавателей профессионального  цикла технического профиля  Протокол №\_\_ от «\_\_\_»\_\_\_\_\_\_ 2021 г.  Председатель ЦК \_\_\_\_\_ Е. В. Харитонова | | ДИСЦИПЛИНА  МДК01.02 Организация, принципы построения и функционирования  компьютерных сетей  для специальности  09.02.06 Сетевое и системное\_\_\_\_\_\_\_\_  администрирование\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Семестр 5 группа 9САД1.20, 9САД2.20 |   **ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №**  10  1. Уязвимости ARP. Подделка записей кеша ARP. Спуфинг ARP. Атаки DNS. Туннелирование DNS. Атаки, связанные с DHCP.  2. Практическое задание. Можно пользоваться Интернет. Схема сети.  У некоторой компании есть главный офис, который подключается в Интернет. Пограничный маршрутизатор Border подключен к провайдеру, который предоставляет услуги Интернет. Также существует второй офис компании, который таже подключен к публичной сети. И между ними проброшен VPN туннель. Между роутерами установлен OSPF, а между роутерами интернет компании и главным офисом установлена статическая маршрутизация. На основных коммутаторах офиса установлены по триVLAN, на роутерах сабинтерфейсы.  Для всего активного сетевого оборудования настройте доменное имя wsr2020.wsr. Создайте локального пользователя admin с паролем Pa$$w0rd. Для активного сетевого оборудования: пользователь должен обладать максимальным уровнем привилегий, пароль должен храниться в виде результата хэш функции, используйте алгоритм scrypt. Для всех сетевых устройств сконфигурируйте пароль wsr2020 для входа в привилегированный режим. Все сетевые устройства должны быть доступны для управления по протоколу SSHv2. Зашифруйте все открытые пароли.  Таблица VLAN двух офисов должна содержать следующие подсети: VLAN10:CLIENT, VLAN20:SERV, VLAN30:DMZ. Сконфигурируйте магистральные каналы.  Настройте подключение Border к провайдеру ISP с помощью протокола PPP. Адрес необходимо получить при помощи IPCP. Аутентификация не требуется.  Транспортный адрес необходимо получить при помощи протокола SLARP на соответствующий Serial интерфейс.  Устройства проходят аутентификацию по протоколу CHAP в одностороннем порядке. Только ISP аутентифицирует роутер Border. Для аутентификации используйте данные client65010 и пароль P@ssw0rd. Явно сконфигурируйте корректное значение MTU.  Сконфигурируйте GRE туннель между BRANCH1 и BRANCH2. В качестве адресов источника и назначения используйте адреса соответствующих loopback интерфейсов. Используйте номер туннельного интерфейса 1.  Обеспечьте возможность входа на Border c использованием доменных реквизитов. Группа MAdmins должна получать максимальный уровень привилегий при входе. Группа SAdmins должна получать при входе уровень привилегий. Обеспечьте возможность входа пользователя, созданного локально при доступности RADIUS сервера. Для 5 уровня привилегий сконфигурируйте расширенный набор команд. Добавьте возможность использования команд reload, debug и sh.  В главном офисе на сервере установлен DHCP, который раздает адресацию на все сетевые устройства. Здесь же установлены службы ААА, DNS, HTTP. Во втором офисе компании установленWeb-server и DMZ. На роутере Border установлена служба NAT.  Преподаватель\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Скиляжнов А.О. |

Министерство образования Красноярского края

краевое государственное бюджетное профессиональное образовательное учреждение «Красноярский колледж радиоэлектроники и информационных технологий»

|  |  |  |  |
| --- | --- | --- | --- |
| |  |  |  | | --- | --- | --- | | |  | | --- | | РАССМОТРЕНО  на заседании цикловой комиссии  преподавателей профессионального  цикла технического профиля  Протокол №\_\_ от «\_\_\_»\_\_\_\_\_\_ 2021 г.  Председатель ЦК \_\_\_\_\_ Е. В. Харитонова | | ДИСЦИПЛИНА  МДК01.02 Организация, принципы построения и функционирования  компьютерных сетей  для специальности  09.02.06 Сетевое и системное\_\_\_\_\_\_\_\_  администрирование\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Семестр 5 группа 9САД1.20, 9САД2.20 |   **ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №**  11  1. Уязвимости TCP и UDP. Сервисы TCP. Атаки TCP. Атаки с использованием UDP.  2. Практическое задание. Можно пользоваться Интернет. Схема сети.  У некоторой компании есть главный офис, который подключается в Интернет. Пограничный маршрутизатор Border подключен к провайдеру, который предоставляет услуги Интернет. Также существует второй офис компании, который таже подключен к публичной сети. И между ними проброшен VPN туннель. Между роутерами установлен OSPF, а между роутерами интернет компании и главным офисом установлена статическая маршрутизация. На основных коммутаторах офиса установлены по триVLAN, на роутерах сабинтерфейсы.  Для всего активного сетевого оборудования настройте доменное имя wsr2020.wsr. Создайте локального пользователя admin с паролем Pa$$w0rd. Для активного сетевого оборудования: пользователь должен обладать максимальным уровнем привилегий, пароль должен храниться в виде результата хэш функции, используйте алгоритм scrypt. Для всех сетевых устройств сконфигурируйте пароль wsr2020 для входа в привилегированный режим. Все сетевые устройства должны быть доступны для управления по протоколу SSHv2. Зашифруйте все открытые пароли.  Таблица VLAN двух офисов должна содержать следующие подсети: VLAN10:CLIENT, VLAN20:SERV, VLAN30:DMZ. Сконфигурируйте магистральные каналы.  Настройте подключение Border к провайдеру ISP с помощью протокола PPP. Адрес необходимо получить при помощи IPCP. Аутентификация не требуется.  Транспортный адрес необходимо получить при помощи протокола SLARP на соответствующий Serial интерфейс.  Устройства проходят аутентификацию по протоколу CHAP в одностороннем порядке. Только ISP аутентифицирует роутер Border. Для аутентификации используйте данные client65010 и пароль P@ssw0rd. Явно сконфигурируйте корректное значение MTU.  Сконфигурируйте GRE туннель между BRANCH1 и BRANCH2. В качестве адресов источника и назначения используйте адреса соответствующих loopback интерфейсов. Используйте номер туннельного интерфейса 1.  Обеспечьте возможность входа на Border c использованием доменных реквизитов. Группа MAdmins должна получать максимальный уровень привилегий при входе. Группа SAdmins должна получать при входе уровень привилегий. Обеспечьте возможность входа пользователя, созданного локально при доступности RADIUS сервера. Для 5 уровня привилегий сконфигурируйте расширенный набор команд. Добавьте возможность использования команд reload, debug и sh.  В главном офисе на сервере установлен DHCP, который раздает адресацию на все сетевые устройства. Здесь же установлены службы ААА, DNS, HTTP. Во втором офисе компании установленWeb-server и DMZ. На роутере Border установлена служба NAT.  Преподаватель\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Скиляжнов А.О. |

Министерство образования Красноярского края

краевое государственное бюджетное профессиональное образовательное учреждение «Красноярский колледж радиоэлектроники и информационных технологий»

|  |  |  |  |
| --- | --- | --- | --- |
| |  |  |  | | --- | --- | --- | | |  | | --- | | РАССМОТРЕНО  на заседании цикловой комиссии  преподавателей профессионального  цикла технического профиля  Протокол №\_\_ от «\_\_\_»\_\_\_\_\_\_ 2021 г.  Председатель ЦК \_\_\_\_\_ Е. В. Харитонова | | ДИСЦИПЛИНА  МДК01.02 Организация, принципы построения и функционирования  компьютерных сетей  для специальности  09.02.06 Сетевое и системное\_\_\_\_\_\_\_\_  администрирование\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Семестр 5 группа 9САД1.20, 9САД2.20 |   **ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №**  12  1. Угрозы и уязвимости IP. DoS- и DDoS-атаки. Атаки на основе ICMP. Атаки по методу умножения и отражения. Атаки с подменой адреса.  2. Практическое задание. Можно пользоваться Интернет. Схема сети.  У некоторой компании есть главный офис, который подключается в Интернет. Пограничный маршрутизатор Border подключен к провайдеру, который предоставляет услуги Интернет. Также существует второй офис компании, который таже подключен к публичной сети. И между ними проброшен VPN туннель. Между роутерами установлен OSPF, а между роутерами интернет компании и главным офисом установлена статическая маршрутизация. На основных коммутаторах офиса установлены по триVLAN, на роутерах сабинтерфейсы.  Для всего активного сетевого оборудования настройте доменное имя wsr2020.wsr. Создайте локального пользователя admin с паролем Pa$$w0rd. Для активного сетевого оборудования: пользователь должен обладать максимальным уровнем привилегий, пароль должен храниться в виде результата хэш функции, используйте алгоритм scrypt. Для всех сетевых устройств сконфигурируйте пароль wsr2020 для входа в привилегированный режим. Все сетевые устройства должны быть доступны для управления по протоколу SSHv2. Зашифруйте все открытые пароли.  Таблица VLAN двух офисов должна содержать следующие подсети: VLAN10:CLIENT, VLAN20:SERV, VLAN30:DMZ. Сконфигурируйте магистральные каналы.  Настройте подключение Border к провайдеру ISP с помощью протокола PPP. Адрес необходимо получить при помощи IPCP. Аутентификация не требуется.  Транспортный адрес необходимо получить при помощи протокола SLARP на соответствующий Serial интерфейс.  Устройства проходят аутентификацию по протоколу CHAP в одностороннем порядке. Только ISP аутентифицирует роутер Border. Для аутентификации используйте данные client65010 и пароль P@ssw0rd. Явно сконфигурируйте корректное значение MTU.  Сконфигурируйте GRE туннель между BRANCH1 и BRANCH2. В качестве адресов источника и назначения используйте адреса соответствующих loopback интерфейсов. Используйте номер туннельного интерфейса 1.  Обеспечьте возможность входа на Border c использованием доменных реквизитов. Группа MAdmins должна получать максимальный уровень привилегий при входе. Группа SAdmins должна получать при входе уровень привилегий. Обеспечьте возможность входа пользователя, созданного локально при доступности RADIUS сервера. Для 5 уровня привилегий сконфигурируйте расширенный набор команд. Добавьте возможность использования команд reload, debug и sh.  В главном офисе на сервере установлен DHCP, который раздает адресацию на все сетевые устройства. Здесь же установлены службы ААА, DNS, HTTP. Во втором офисе компании установленWeb-server и DMZ. На роутере Border установлена служба NAT.  Преподаватель\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Скиляжнов А.О. |

Министерство образования Красноярского края

краевое государственное бюджетное профессиональное образовательное учреждение «Красноярский колледж радиоэлектроники и информационных технологий»

|  |  |  |  |
| --- | --- | --- | --- |
| |  |  |  | | --- | --- | --- | | |  | | --- | | РАССМОТРЕНО  на заседании цикловой комиссии  преподавателей профессионального  цикла технического профиля  Протокол №\_\_ от «\_\_\_»\_\_\_\_\_\_ 2021 г.  Председатель ЦК \_\_\_\_\_ Е. В. Харитонова | | ДИСЦИПЛИНА  МДК01.02 Организация, принципы построения и функционирования  компьютерных сетей  для специальности  09.02.06 Сетевое и системное\_\_\_\_\_\_\_\_  администрирование\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Семестр 5 группа 9САД1.20, 9САД2.20 |   **ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №**  13  1. Угрозы и уязвимости IP. Распространенные сетевые атаки. Разведывательные атаки. Атаки доступа. Атаки методами социальной инженерии.  2. Практическое задание. Можно пользоваться Интернет. Схема сети.  У некоторой компании есть главный офис, который подключается в Интернет. Пограничный маршрутизатор Border подключен к провайдеру, который предоставляет услуги Интернет. Также существует второй офис компании, который таже подключен к публичной сети. И между ними проброшен VPN туннель. Между роутерами установлен OSPF, а между роутерами интернет компании и главным офисом установлена статическая маршрутизация. На основных коммутаторах офиса установлены по триVLAN, на роутерах сабинтерфейсы.  Для всего активного сетевого оборудования настройте доменное имя wsr2020.wsr. Создайте локального пользователя admin с паролем Pa$$w0rd. Для активного сетевого оборудования: пользователь должен обладать максимальным уровнем привилегий, пароль должен храниться в виде результата хэш функции, используйте алгоритм scrypt. Для всех сетевых устройств сконфигурируйте пароль wsr2020 для входа в привилегированный режим. Все сетевые устройства должны быть доступны для управления по протоколу SSHv2. Зашифруйте все открытые пароли.  Таблица VLAN двух офисов должна содержать следующие подсети: VLAN10:CLIENT, VLAN20:SERV, VLAN30:DMZ. Сконфигурируйте магистральные каналы.  Настройте подключение Border к провайдеру ISP с помощью протокола PPP. Адрес необходимо получить при помощи IPCP. Аутентификация не требуется.  Транспортный адрес необходимо получить при помощи протокола SLARP на соответствующий Serial интерфейс.  Устройства проходят аутентификацию по протоколу CHAP в одностороннем порядке. Только ISP аутентифицирует роутер Border. Для аутентификации используйте данные client65010 и пароль P@ssw0rd. Явно сконфигурируйте корректное значение MTU.  Сконфигурируйте GRE туннель между BRANCH1 и BRANCH2. В качестве адресов источника и назначения используйте адреса соответствующих loopback интерфейсов. Используйте номер туннельного интерфейса 1.  Обеспечьте возможность входа на Border c использованием доменных реквизитов. Группа MAdmins должна получать максимальный уровень привилегий при входе. Группа SAdmins должна получать при входе уровень привилегий. Обеспечьте возможность входа пользователя, созданного локально при доступности RADIUS сервера. Для 5 уровня привилегий сконфигурируйте расширенный набор команд. Добавьте возможность использования команд reload, debug и sh.  В главном офисе на сервере установлен DHCP, который раздает адресацию на все сетевые устройства. Здесь же установлены службы ААА, DNS, HTTP. Во втором офисе компании установленWeb-server и DMZ. На роутере Border установлена служба NAT.  Преподаватель\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Скиляжнов А.О. |

Министерство образования Красноярского края

краевое государственное бюджетное профессиональное образовательное учреждение «Красноярский колледж радиоэлектроники и информационных технологий»

|  |  |  |  |
| --- | --- | --- | --- |
| |  |  |  | | --- | --- | --- | | |  | | --- | | РАССМОТРЕНО  на заседании цикловой комиссии  преподавателей профессионального  цикла технического профиля  Протокол №\_\_ от «\_\_\_»\_\_\_\_\_\_ 2021 г.  Председатель ЦК \_\_\_\_\_ Е. В. Харитонова | | ДИСЦИПЛИНА  МДК01.02 Организация, принципы построения и функционирования  компьютерных сетей  для специальности  09.02.06 Сетевое и системное\_\_\_\_\_\_\_\_  администрирование\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Семестр 5 группа 9САД1.20, 9САД2.20 |   **ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №**  14  1. Вредоносное программное обеспечение. Типы вредоносного ПО. Вирусы и «троянские кони».  2. Практическое задание. Можно пользоваться Интернет. Схема сети.  У некоторой компании есть главный офис, который подключается в Интернет. Пограничный маршрутизатор Border подключен к провайдеру, который предоставляет услуги Интернет. Также существует второй офис компании, который таже подключен к публичной сети. И между ними проброшен VPN туннель. Между роутерами установлен OSPF, а между роутерами интернет компании и главным офисом установлена статическая маршрутизация. На основных коммутаторах офиса установлены по триVLAN, на роутерах сабинтерфейсы.  Для всего активного сетевого оборудования настройте доменное имя wsr2020.wsr. Создайте локального пользователя admin с паролем Pa$$w0rd. Для активного сетевого оборудования: пользователь должен обладать максимальным уровнем привилегий, пароль должен храниться в виде результата хэш функции, используйте алгоритм scrypt. Для всех сетевых устройств сконфигурируйте пароль wsr2020 для входа в привилегированный режим. Все сетевые устройства должны быть доступны для управления по протоколу SSHv2. Зашифруйте все открытые пароли.  Таблица VLAN двух офисов должна содержать следующие подсети: VLAN10:CLIENT, VLAN20:SERV, VLAN30:DMZ. Сконфигурируйте магистральные каналы.  Настройте подключение Border к провайдеру ISP с помощью протокола PPP. Адрес необходимо получить при помощи IPCP. Аутентификация не требуется.  Транспортный адрес необходимо получить при помощи протокола SLARP на соответствующий Serial интерфейс.  Устройства проходят аутентификацию по протоколу CHAP в одностороннем порядке. Только ISP аутентифицирует роутер Border. Для аутентификации используйте данные client65010 и пароль P@ssw0rd. Явно сконфигурируйте корректное значение MTU.  Сконфигурируйте GRE туннель между BRANCH1 и BRANCH2. В качестве адресов источника и назначения используйте адреса соответствующих loopback интерфейсов. Используйте номер туннельного интерфейса 1.  Обеспечьте возможность входа на Border c использованием доменных реквизитов. Группа MAdmins должна получать максимальный уровень привилегий при входе. Группа SAdmins должна получать при входе уровень привилегий. Обеспечьте возможность входа пользователя, созданного локально при доступности RADIUS сервера. Для 5 уровня привилегий сконфигурируйте расширенный набор команд. Добавьте возможность использования команд reload, debug и sh.  В главном офисе на сервере установлен DHCP, который раздает адресацию на все сетевые устройства. Здесь же установлены службы ААА, DNS, HTTP. Во втором офисе компании установленWeb-server и DMZ. На роутере Border установлена служба NAT.  Преподаватель\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Скиляжнов А.О. |

Министерство образования Красноярского края

краевое государственное бюджетное профессиональное образовательное учреждение «Красноярский колледж радиоэлектроники и информационных технологий»

|  |  |  |  |
| --- | --- | --- | --- |
| |  |  |  | | --- | --- | --- | | |  | | --- | | РАССМОТРЕНО  на заседании цикловой комиссии  преподавателей профессионального  цикла технического профиля  Протокол №\_\_ от «\_\_\_»\_\_\_\_\_\_ 2021 г.  Председатель ЦК \_\_\_\_\_ Е. В. Харитонова | | ДИСЦИПЛИНА  МДК01.02 Организация, принципы построения и функционирования  компьютерных сетей  для специальности  09.02.06 Сетевое и системное\_\_\_\_\_\_\_\_  администрирование\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Семестр 5 группа 9САД1.20, 9САД2.20 |   **ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №**  15  1. Текущий уровень кибербезопасности. Векторы сетевых атак. Потеря данных. Злоумышленники. Инструменты злоумышленников.  2. Практическое задание. Можно пользоваться Интернет. Схема сети.  У некоторой компании есть главный офис, который подключается в Интернет. Пограничный маршрутизатор Border подключен к провайдеру, который предоставляет услуги Интернет. Также существует второй офис компании, который таже подключен к публичной сети. И между ними проброшен VPN туннель. Между роутерами установлен OSPF, а между роутерами интернет компании и главным офисом установлена статическая маршрутизация. На основных коммутаторах офиса установлены по триVLAN, на роутерах сабинтерфейсы.  Для всего активного сетевого оборудования настройте доменное имя wsr2020.wsr. Создайте локального пользователя admin с паролем Pa$$w0rd. Для активного сетевого оборудования: пользователь должен обладать максимальным уровнем привилегий, пароль должен храниться в виде результата хэш функции, используйте алгоритм scrypt. Для всех сетевых устройств сконфигурируйте пароль wsr2020 для входа в привилегированный режим. Все сетевые устройства должны быть доступны для управления по протоколу SSHv2. Зашифруйте все открытые пароли.  Таблица VLAN двух офисов должна содержать следующие подсети: VLAN10:CLIENT, VLAN20:SERV, VLAN30:DMZ. Сконфигурируйте магистральные каналы.  Настройте подключение Border к провайдеру ISP с помощью протокола PPP. Адрес необходимо получить при помощи IPCP. Аутентификация не требуется.  Транспортный адрес необходимо получить при помощи протокола SLARP на соответствующий Serial интерфейс.  Устройства проходят аутентификацию по протоколу CHAP в одностороннем порядке. Только ISP аутентифицирует роутер Border. Для аутентификации используйте данные client65010 и пароль P@ssw0rd. Явно сконфигурируйте корректное значение MTU.  Сконфигурируйте GRE туннель между BRANCH1 и BRANCH2. В качестве адресов источника и назначения используйте адреса соответствующих loopback интерфейсов. Используйте номер туннельного интерфейса 1.  Обеспечьте возможность входа на Border c использованием доменных реквизитов. Группа MAdmins должна получать максимальный уровень привилегий при входе. Группа SAdmins должна получать при входе уровень привилегий. Обеспечьте возможность входа пользователя, созданного локально при доступности RADIUS сервера. Для 5 уровня привилегий сконфигурируйте расширенный набор команд. Добавьте возможность использования команд reload, debug и sh.  В главном офисе на сервере установлен DHCP, который раздает адресацию на все сетевые устройства. Здесь же установлены службы ААА, DNS, HTTP. Во втором офисе компании установленWeb-server и DMZ. На роутере Border установлена служба NAT.  Преподаватель\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Скиляжнов А.О. |

Министерство образования Красноярского края

краевое государственное бюджетное профессиональное образовательное учреждение «Красноярский колледж радиоэлектроники и информационных технологий»

|  |  |  |  |
| --- | --- | --- | --- |
| |  |  |  | | --- | --- | --- | | |  | | --- | | РАССМОТРЕНО  на заседании цикловой комиссии  преподавателей профессионального  цикла технического профиля  Протокол №\_\_ от «\_\_\_»\_\_\_\_\_\_ 2021 г.  Председатель ЦК \_\_\_\_\_ Е. В. Харитонова | | ДИСЦИПЛИНА  МДК01.02 Организация, принципы построения и функционирования  компьютерных сетей  для специальности  09.02.06 Сетевое и системное\_\_\_\_\_\_\_\_  администрирование\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Семестр 5 группа 9САД1.20, 9САД2.20 |   **ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №**  16  1. Протокол [NetFlow](https://static-course-assets.s3.amazonaws.com/CN503/ru/index.html#8.3). [Принцип работы NetFlow](https://static-course-assets.s3.amazonaws.com/CN503/ru/index.html#8.3.1). [Настройка NetFlow](https://static-course-assets.s3.amazonaws.com/CN503/ru/index.html#8.3.2). [Проверка моделей трафика](https://static-course-assets.s3.amazonaws.com/CN503/ru/index.html#8.3.3).  2. Практическое задание. Можно пользоваться Интернет. Схема сети.  У некоторой компании есть главный офис, который подключается в Интернет. Пограничный маршрутизатор Border подключен к провайдеру, который предоставляет услуги Интернет. Также существует второй офис компании, который таже подключен к публичной сети. И между ними проброшен VPN туннель. Между роутерами установлен OSPF, а между роутерами интернет компании и главным офисом установлена статическая маршрутизация. На основных коммутаторах офиса установлены по триVLAN, на роутерах сабинтерфейсы.  Для всего активного сетевого оборудования настройте доменное имя wsr2020.wsr. Создайте локального пользователя admin с паролем Pa$$w0rd. Для активного сетевого оборудования: пользователь должен обладать максимальным уровнем привилегий, пароль должен храниться в виде результата хэш функции, используйте алгоритм scrypt. Для всех сетевых устройств сконфигурируйте пароль wsr2020 для входа в привилегированный режим. Все сетевые устройства должны быть доступны для управления по протоколу SSHv2. Зашифруйте все открытые пароли.  Таблица VLAN двух офисов должна содержать следующие подсети: VLAN10:CLIENT, VLAN20:SERV, VLAN30:DMZ. Сконфигурируйте магистральные каналы.  Настройте подключение Border к провайдеру ISP с помощью протокола PPP. Адрес необходимо получить при помощи IPCP. Аутентификация не требуется.  Транспортный адрес необходимо получить при помощи протокола SLARP на соответствующий Serial интерфейс.  Устройства проходят аутентификацию по протоколу CHAP в одностороннем порядке. Только ISP аутентифицирует роутер Border. Для аутентификации используйте данные client65010 и пароль P@ssw0rd. Явно сконфигурируйте корректное значение MTU.  Сконфигурируйте GRE туннель между BRANCH1 и BRANCH2. В качестве адресов источника и назначения используйте адреса соответствующих loopback интерфейсов. Используйте номер туннельного интерфейса 1.  Обеспечьте возможность входа на Border c использованием доменных реквизитов. Группа MAdmins должна получать максимальный уровень привилегий при входе. Группа SAdmins должна получать при входе уровень привилегий. Обеспечьте возможность входа пользователя, созданного локально при доступности RADIUS сервера. Для 5 уровня привилегий сконфигурируйте расширенный набор команд. Добавьте возможность использования команд reload, debug и sh.  В главном офисе на сервере установлен DHCP, который раздает адресацию на все сетевые устройства. Здесь же установлены службы ААА, DNS, HTTP. Во втором офисе компании установленWeb-server и DMZ. На роутере Border установлена служба NAT.  Преподаватель\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Скиляжнов А.О. |

Министерство образования Красноярского края

краевое государственное бюджетное профессиональное образовательное учреждение «Красноярский колледж радиоэлектроники и информационных технологий»

|  |  |  |  |
| --- | --- | --- | --- |
| |  |  |  | | --- | --- | --- | | |  | | --- | | РАССМОТРЕНО  на заседании цикловой комиссии  преподавателей профессионального  цикла технического профиля  Протокол №\_\_ от «\_\_\_»\_\_\_\_\_\_ 2021 г.  Председатель ЦК \_\_\_\_\_ Е. В. Харитонова | | ДИСЦИПЛИНА  МДК01.02 Организация, принципы построения и функционирования  компьютерных сетей  для специальности  09.02.06 Сетевое и системное\_\_\_\_\_\_\_\_  администрирование\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Семестр 5 группа 9САД1.20, 9САД2.20 |   **ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №**  17  1. Протокол [SNMP](https://static-course-assets.s3.amazonaws.com/CN503/ru/index.html#8.2). [Принцип работы SNMP](https://static-course-assets.s3.amazonaws.com/CN503/ru/index.html#8.2.1). [Настройка SNMP](https://static-course-assets.s3.amazonaws.com/CN503/ru/index.html#8.2.2).  2. Практическое задание. Можно пользоваться Интернет. Схема сети.  У некоторой компании есть главный офис, который подключается в Интернет. Пограничный маршрутизатор Border подключен к провайдеру, который предоставляет услуги Интернет. Также существует второй офис компании, который таже подключен к публичной сети. И между ними проброшен VPN туннель. Между роутерами установлен OSPF, а между роутерами интернет компании и главным офисом установлена статическая маршрутизация. На основных коммутаторах офиса установлены по триVLAN, на роутерах сабинтерфейсы.  Для всего активного сетевого оборудования настройте доменное имя wsr2020.wsr. Создайте локального пользователя admin с паролем Pa$$w0rd. Для активного сетевого оборудования: пользователь должен обладать максимальным уровнем привилегий, пароль должен храниться в виде результата хэш функции, используйте алгоритм scrypt. Для всех сетевых устройств сконфигурируйте пароль wsr2020 для входа в привилегированный режим. Все сетевые устройства должны быть доступны для управления по протоколу SSHv2. Зашифруйте все открытые пароли.  Таблица VLAN двух офисов должна содержать следующие подсети: VLAN10:CLIENT, VLAN20:SERV, VLAN30:DMZ. Сконфигурируйте магистральные каналы.  Настройте подключение Border к провайдеру ISP с помощью протокола PPP. Адрес необходимо получить при помощи IPCP. Аутентификация не требуется.  Транспортный адрес необходимо получить при помощи протокола SLARP на соответствующий Serial интерфейс.  Устройства проходят аутентификацию по протоколу CHAP в одностороннем порядке. Только ISP аутентифицирует роутер Border. Для аутентификации используйте данные client65010 и пароль P@ssw0rd. Явно сконфигурируйте корректное значение MTU.  Сконфигурируйте GRE туннель между BRANCH1 и BRANCH2. В качестве адресов источника и назначения используйте адреса соответствующих loopback интерфейсов. Используйте номер туннельного интерфейса 1.  Обеспечьте возможность входа на Border c использованием доменных реквизитов. Группа MAdmins должна получать максимальный уровень привилегий при входе. Группа SAdmins должна получать при входе уровень привилегий. Обеспечьте возможность входа пользователя, созданного локально при доступности RADIUS сервера. Для 5 уровня привилегий сконфигурируйте расширенный набор команд. Добавьте возможность использования команд reload, debug и sh.  В главном офисе на сервере установлен DHCP, который раздает адресацию на все сетевые устройства. Здесь же установлены службы ААА, DNS, HTTP. Во втором офисе компании установленWeb-server и DMZ. На роутере Border установлена служба NAT.  Преподаватель\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Скиляжнов А.О. |

Министерство образования Красноярского края

краевое государственное бюджетное профессиональное образовательное учреждение «Красноярский колледж радиоэлектроники и информационных технологий»

|  |  |  |  |
| --- | --- | --- | --- |
| |  |  |  | | --- | --- | --- | | |  | | --- | | РАССМОТРЕНО  на заседании цикловой комиссии  преподавателей профессионального  цикла технического профиля  Протокол №\_\_ от «\_\_\_»\_\_\_\_\_\_ 2021 г.  Председатель ЦК \_\_\_\_\_ Е. В. Харитонова | | ДИСЦИПЛИНА  МДК01.02 Организация, принципы построения и функционирования  компьютерных сетей  для специальности  09.02.06 Сетевое и системное\_\_\_\_\_\_\_\_  администрирование\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Семестр 5 группа 9САД1.20, 9САД2.20 |   **ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №**  18  1. Мониторинг сети [Syslog](https://static-course-assets.s3.amazonaws.com/CN503/ru/index.html#8.1). [Принцип работы Syslog](https://static-course-assets.s3.amazonaws.com/CN503/ru/index.html#8.1.1). [Настройка Syslog](https://static-course-assets.s3.amazonaws.com/CN503/ru/index.html#8.1.2).  2. Практическое задание. Можно пользоваться Интернет. Схема сети.  У некоторой компании есть главный офис, который подключается в Интернет. Пограничный маршрутизатор Border подключен к провайдеру, который предоставляет услуги Интернет. Также существует второй офис компании, который таже подключен к публичной сети. И между ними проброшен VPN туннель. Между роутерами установлен OSPF, а между роутерами интернет компании и главным офисом установлена статическая маршрутизация. На основных коммутаторах офиса установлены по триVLAN, на роутерах сабинтерфейсы.  Для всего активного сетевого оборудования настройте доменное имя wsr2020.wsr. Создайте локального пользователя admin с паролем Pa$$w0rd. Для активного сетевого оборудования: пользователь должен обладать максимальным уровнем привилегий, пароль должен храниться в виде результата хэш функции, используйте алгоритм scrypt. Для всех сетевых устройств сконфигурируйте пароль wsr2020 для входа в привилегированный режим. Все сетевые устройства должны быть доступны для управления по протоколу SSHv2. Зашифруйте все открытые пароли.  Таблица VLAN двух офисов должна содержать следующие подсети: VLAN10:CLIENT, VLAN20:SERV, VLAN30:DMZ. Сконфигурируйте магистральные каналы.  Настройте подключение Border к провайдеру ISP с помощью протокола PPP. Адрес необходимо получить при помощи IPCP. Аутентификация не требуется.  Транспортный адрес необходимо получить при помощи протокола SLARP на соответствующий Serial интерфейс.  Устройства проходят аутентификацию по протоколу CHAP в одностороннем порядке. Только ISP аутентифицирует роутер Border. Для аутентификации используйте данные client65010 и пароль P@ssw0rd. Явно сконфигурируйте корректное значение MTU.  Сконфигурируйте GRE туннель между BRANCH1 и BRANCH2. В качестве адресов источника и назначения используйте адреса соответствующих loopback интерфейсов. Используйте номер туннельного интерфейса 1.  Обеспечьте возможность входа на Border c использованием доменных реквизитов. Группа MAdmins должна получать максимальный уровень привилегий при входе. Группа SAdmins должна получать при входе уровень привилегий. Обеспечьте возможность входа пользователя, созданного локально при доступности RADIUS сервера. Для 5 уровня привилегий сконфигурируйте расширенный набор команд. Добавьте возможность использования команд reload, debug и sh.  В главном офисе на сервере установлен DHCP, который раздает адресацию на все сетевые устройства. Здесь же установлены службы ААА, DNS, HTTP. Во втором офисе компании установленWeb-server и DMZ. На роутере Border установлена служба NAT.  Преподаватель\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Скиляжнов А.О. |

Министерство образования Красноярского края

краевое государственное бюджетное профессиональное образовательное учреждение «Красноярский колледж радиоэлектроники и информационных технологий»

|  |  |  |  |
| --- | --- | --- | --- |
| |  |  |  | | --- | --- | --- | | |  | | --- | | РАССМОТРЕНО  на заседании цикловой комиссии  преподавателей профессионального  цикла технического профиля  Протокол №\_\_ от «\_\_\_»\_\_\_\_\_\_ 2021 г.  Председатель ЦК \_\_\_\_\_ Е. В. Харитонова | | ДИСЦИПЛИНА  МДК01.02 Организация, принципы построения и функционирования  компьютерных сетей  для специальности  09.02.06 Сетевое и системное\_\_\_\_\_\_\_\_  администрирование\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Семестр 5 группа 9САД1.20, 9САД2.20 |   **ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №**  19  1. [Удалённый доступ](https://static-course-assets.s3.amazonaws.com/CN503/ru/index.html#7.4). [Решения VPN для удалённого доступа](https://static-course-assets.s3.amazonaws.com/CN503/ru/index.html#7.4.1). [Сети VPN удалённого доступа с использованием IPsec](https://static-course-assets.s3.amazonaws.com/CN503/ru/index.html#7.4.2).  2. Практическое задание. Можно пользоваться Интернет. Схема сети.  У некоторой компании есть главный офис, который подключается в Интернет. Пограничный маршрутизатор Border подключен к провайдеру, который предоставляет услуги Интернет. Также существует второй офис компании, который таже подключен к публичной сети. И между ними проброшен VPN туннель. Между роутерами установлен OSPF, а между роутерами интернет компании и главным офисом установлена статическая маршрутизация. На основных коммутаторах офиса установлены по триVLAN, на роутерах сабинтерфейсы.  Для всего активного сетевого оборудования настройте доменное имя wsr2020.wsr. Создайте локального пользователя admin с паролем Pa$$w0rd. Для активного сетевого оборудования: пользователь должен обладать максимальным уровнем привилегий, пароль должен храниться в виде результата хэш функции, используйте алгоритм scrypt. Для всех сетевых устройств сконфигурируйте пароль wsr2020 для входа в привилегированный режим. Все сетевые устройства должны быть доступны для управления по протоколу SSHv2. Зашифруйте все открытые пароли.  Таблица VLAN двух офисов должна содержать следующие подсети: VLAN10:CLIENT, VLAN20:SERV, VLAN30:DMZ. Сконфигурируйте магистральные каналы.  Настройте подключение Border к провайдеру ISP с помощью протокола PPP. Адрес необходимо получить при помощи IPCP. Аутентификация не требуется.  Транспортный адрес необходимо получить при помощи протокола SLARP на соответствующий Serial интерфейс.  Устройства проходят аутентификацию по протоколу CHAP в одностороннем порядке. Только ISP аутентифицирует роутер Border. Для аутентификации используйте данные client65010 и пароль P@ssw0rd. Явно сконфигурируйте корректное значение MTU.  Сконфигурируйте GRE туннель между BRANCH1 и BRANCH2. В качестве адресов источника и назначения используйте адреса соответствующих loopback интерфейсов. Используйте номер туннельного интерфейса 1.  Обеспечьте возможность входа на Border c использованием доменных реквизитов. Группа MAdmins должна получать максимальный уровень привилегий при входе. Группа SAdmins должна получать при входе уровень привилегий. Обеспечьте возможность входа пользователя, созданного локально при доступности RADIUS сервера. Для 5 уровня привилегий сконфигурируйте расширенный набор команд. Добавьте возможность использования команд reload, debug и sh.  В главном офисе на сервере установлен DHCP, который раздает адресацию на все сетевые устройства. Здесь же установлены службы ААА, DNS, HTTP. Во втором офисе компании установленWeb-server и DMZ. На роутере Border установлена служба NAT.  Преподаватель\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Скиляжнов А.О. |

Министерство образования Красноярского края

краевое государственное бюджетное профессиональное образовательное учреждение «Красноярский колледж радиоэлектроники и информационных технологий»

|  |  |  |  |
| --- | --- | --- | --- |
| |  |  |  | | --- | --- | --- | | |  | | --- | | РАССМОТРЕНО  на заседании цикловой комиссии  преподавателей профессионального  цикла технического профиля  Протокол №\_\_ от «\_\_\_»\_\_\_\_\_\_ 2021 г.  Председатель ЦК \_\_\_\_\_ Е. В. Харитонова | | ДИСЦИПЛИНА  МДК01.02 Организация, принципы построения и функционирования  компьютерных сетей  для специальности  09.02.06 Сетевое и системное\_\_\_\_\_\_\_\_  администрирование\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Семестр 5 группа 9САД1.20, 9САД2.20 |   **ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №**  20  1. [Структура протокола IPsec](https://static-course-assets.s3.amazonaws.com/CN503/ru/index.html#7.3.2). Транспортный и туннельный режим. Безопасный обмен ключами с Диффи-Хеллманом.  2. Практическое задание. Можно пользоваться Интернет. Схема сети.  У некоторой компании есть главный офис, который подключается в Интернет. Пограничный маршрутизатор Border подключен к провайдеру, который предоставляет услуги Интернет. Также существует второй офис компании, который таже подключен к публичной сети. И между ними проброшен VPN туннель. Между роутерами установлен OSPF, а между роутерами интернет компании и главным офисом установлена статическая маршрутизация. На основных коммутаторах офиса установлены по триVLAN, на роутерах сабинтерфейсы.  Для всего активного сетевого оборудования настройте доменное имя wsr2020.wsr. Создайте локального пользователя admin с паролем Pa$$w0rd. Для активного сетевого оборудования: пользователь должен обладать максимальным уровнем привилегий, пароль должен храниться в виде результата хэш функции, используйте алгоритм scrypt. Для всех сетевых устройств сконфигурируйте пароль wsr2020 для входа в привилегированный режим. Все сетевые устройства должны быть доступны для управления по протоколу SSHv2. Зашифруйте все открытые пароли.  Таблица VLAN двух офисов должна содержать следующие подсети: VLAN10:CLIENT, VLAN20:SERV, VLAN30:DMZ. Сконфигурируйте магистральные каналы.  Настройте подключение Border к провайдеру ISP с помощью протокола PPP. Адрес необходимо получить при помощи IPCP. Аутентификация не требуется.  Транспортный адрес необходимо получить при помощи протокола SLARP на соответствующий Serial интерфейс.  Устройства проходят аутентификацию по протоколу CHAP в одностороннем порядке. Только ISP аутентифицирует роутер Border. Для аутентификации используйте данные client65010 и пароль P@ssw0rd. Явно сконфигурируйте корректное значение MTU.  Сконфигурируйте GRE туннель между BRANCH1 и BRANCH2. В качестве адресов источника и назначения используйте адреса соответствующих loopback интерфейсов. Используйте номер туннельного интерфейса 1.  Обеспечьте возможность входа на Border c использованием доменных реквизитов. Группа MAdmins должна получать максимальный уровень привилегий при входе. Группа SAdmins должна получать при входе уровень привилегий. Обеспечьте возможность входа пользователя, созданного локально при доступности RADIUS сервера. Для 5 уровня привилегий сконфигурируйте расширенный набор команд. Добавьте возможность использования команд reload, debug и sh.  В главном офисе на сервере установлен DHCP, который раздает адресацию на все сетевые устройства. Здесь же установлены службы ААА, DNS, HTTP. Во втором офисе компании установленWeb-server и DMZ. На роутере Border установлена служба NAT.  Преподаватель\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Скиляжнов А.О. |

Министерство образования Красноярского края

краевое государственное бюджетное профессиональное образовательное учреждение «Красноярский колледж радиоэлектроники и информационных технологий»

|  |  |  |  |
| --- | --- | --- | --- |
| |  |  |  | | --- | --- | --- | | |  | | --- | | РАССМОТРЕНО  на заседании цикловой комиссии  преподавателей профессионального  цикла технического профиля  Протокол №\_\_ от «\_\_\_»\_\_\_\_\_\_ 2021 г.  Председатель ЦК \_\_\_\_\_ Е. В. Харитонова | | ДИСЦИПЛИНА  МДК01.02 Организация, принципы построения и функционирования  компьютерных сетей  для специальности  09.02.06 Сетевое и системное\_\_\_\_\_\_\_\_  администрирование\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Семестр 5 группа 9САД1.20, 9САД2.20 |   **ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №**  21  1. Протокол IPsec. [Общие сведения об IPsec](https://static-course-assets.s3.amazonaws.com/CN503/ru/index.html#7.3). Интерфейс виртуальных туннелей IPsec. IPSec технологии. Инкапсуляция протокола IPSec.  2. Практическое задание. Можно пользоваться Интернет. Схема сети.  У некоторой компании есть главный офис, который подключается в Интернет. Пограничный маршрутизатор Border подключен к провайдеру, который предоставляет услуги Интернет. Также существует второй офис компании, который таже подключен к публичной сети. И между ними проброшен VPN туннель. Между роутерами установлен OSPF, а между роутерами интернет компании и главным офисом установлена статическая маршрутизация. На основных коммутаторах офиса установлены по триVLAN, на роутерах сабинтерфейсы.  Для всего активного сетевого оборудования настройте доменное имя wsr2020.wsr. Создайте локального пользователя admin с паролем Pa$$w0rd. Для активного сетевого оборудования: пользователь должен обладать максимальным уровнем привилегий, пароль должен храниться в виде результата хэш функции, используйте алгоритм scrypt. Для всех сетевых устройств сконфигурируйте пароль wsr2020 для входа в привилегированный режим. Все сетевые устройства должны быть доступны для управления по протоколу SSHv2. Зашифруйте все открытые пароли.  Таблица VLAN двух офисов должна содержать следующие подсети: VLAN10:CLIENT, VLAN20:SERV, VLAN30:DMZ. Сконфигурируйте магистральные каналы.  Настройте подключение Border к провайдеру ISP с помощью протокола PPP. Адрес необходимо получить при помощи IPCP. Аутентификация не требуется.  Транспортный адрес необходимо получить при помощи протокола SLARP на соответствующий Serial интерфейс.  Устройства проходят аутентификацию по протоколу CHAP в одностороннем порядке. Только ISP аутентифицирует роутер Border. Для аутентификации используйте данные client65010 и пароль P@ssw0rd. Явно сконфигурируйте корректное значение MTU.  Сконфигурируйте GRE туннель между BRANCH1 и BRANCH2. В качестве адресов источника и назначения используйте адреса соответствующих loopback интерфейсов. Используйте номер туннельного интерфейса 1.  Обеспечьте возможность входа на Border c использованием доменных реквизитов. Группа MAdmins должна получать максимальный уровень привилегий при входе. Группа SAdmins должна получать при входе уровень привилегий. Обеспечьте возможность входа пользователя, созданного локально при доступности RADIUS сервера. Для 5 уровня привилегий сконфигурируйте расширенный набор команд. Добавьте возможность использования команд reload, debug и sh.  В главном офисе на сервере установлен DHCP, который раздает адресацию на все сетевые устройства. Здесь же установлены службы ААА, DNS, HTTP. Во втором офисе компании установленWeb-server и DMZ. На роутере Border установлена служба NAT.  Преподаватель\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Скиляжнов А.О. |

Министерство образования Красноярского края

краевое государственное бюджетное профессиональное образовательное учреждение «Красноярский колледж радиоэлектроники и информационных технологий»

|  |  |  |  |
| --- | --- | --- | --- |
| |  |  |  | | --- | --- | --- | | |  | | --- | | РАССМОТРЕНО  на заседании цикловой комиссии  преподавателей профессионального  цикла технического профиля  Протокол №\_\_ от «\_\_\_»\_\_\_\_\_\_ 2021 г.  Председатель ЦК \_\_\_\_\_ Е. В. Харитонова | | ДИСЦИПЛИНА  МДК01.02 Организация, принципы построения и функционирования  компьютерных сетей  для специальности  09.02.06 Сетевое и системное\_\_\_\_\_\_\_\_  администрирование\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Семестр 5 группа 9САД1.20, 9САД2.20 |   **ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №**  22  1. [Туннели GRE между объектами](https://static-course-assets.s3.amazonaws.com/CN503/ru/index.html#7.2). [Основы GRE](https://static-course-assets.s3.amazonaws.com/CN503/ru/index.html#7.2.1). [Настройка туннелей GRE](https://static-course-assets.s3.amazonaws.com/CN503/ru/index.html#7.2.2).  2. Практическое задание. Можно пользоваться Интернет. Схема сети.  У некоторой компании есть главный офис, который подключается в Интернет. Пограничный маршрутизатор Border подключен к провайдеру, который предоставляет услуги Интернет. Также существует второй офис компании, который таже подключен к публичной сети. И между ними проброшен VPN туннель. Между роутерами установлен OSPF, а между роутерами интернет компании и главным офисом установлена статическая маршрутизация. На основных коммутаторах офиса установлены по триVLAN, на роутерах сабинтерфейсы.  Для всего активного сетевого оборудования настройте доменное имя wsr2020.wsr. Создайте локального пользователя admin с паролем Pa$$w0rd. Для активного сетевого оборудования: пользователь должен обладать максимальным уровнем привилегий, пароль должен храниться в виде результата хэш функции, используйте алгоритм scrypt. Для всех сетевых устройств сконфигурируйте пароль wsr2020 для входа в привилегированный режим. Все сетевые устройства должны быть доступны для управления по протоколу SSHv2. Зашифруйте все открытые пароли.  Таблица VLAN двух офисов должна содержать следующие подсети: VLAN10:CLIENT, VLAN20:SERV, VLAN30:DMZ. Сконфигурируйте магистральные каналы.  Настройте подключение Border к провайдеру ISP с помощью протокола PPP. Адрес необходимо получить при помощи IPCP. Аутентификация не требуется.  Транспортный адрес необходимо получить при помощи протокола SLARP на соответствующий Serial интерфейс.  Устройства проходят аутентификацию по протоколу CHAP в одностороннем порядке. Только ISP аутентифицирует роутер Border. Для аутентификации используйте данные client65010 и пароль P@ssw0rd. Явно сконфигурируйте корректное значение MTU.  Сконфигурируйте GRE туннель между BRANCH1 и BRANCH2. В качестве адресов источника и назначения используйте адреса соответствующих loopback интерфейсов. Используйте номер туннельного интерфейса 1.  Обеспечьте возможность входа на Border c использованием доменных реквизитов. Группа MAdmins должна получать максимальный уровень привилегий при входе. Группа SAdmins должна получать при входе уровень привилегий. Обеспечьте возможность входа пользователя, созданного локально при доступности RADIUS сервера. Для 5 уровня привилегий сконфигурируйте расширенный набор команд. Добавьте возможность использования команд reload, debug и sh.  В главном офисе на сервере установлен DHCP, который раздает адресацию на все сетевые устройства. Здесь же установлены службы ААА, DNS, HTTP. Во втором офисе компании установленWeb-server и DMZ. На роутере Border установлена служба NAT.  Преподаватель\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Скиляжнов А.О. |

Министерство образования Красноярского края

краевое государственное бюджетное профессиональное образовательное учреждение «Красноярский колледж радиоэлектроники и информационных технологий»

|  |  |  |  |
| --- | --- | --- | --- |
| |  |  |  | | --- | --- | --- | | |  | | --- | | РАССМОТРЕНО  на заседании цикловой комиссии  преподавателей профессионального  цикла технического профиля  Протокол №\_\_ от «\_\_\_»\_\_\_\_\_\_ 2021 г.  Председатель ЦК \_\_\_\_\_ Е. В. Харитонова | | ДИСЦИПЛИНА  МДК01.02 Организация, принципы построения и функционирования  компьютерных сетей  для специальности  09.02.06 Сетевое и системное\_\_\_\_\_\_\_\_  администрирование\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Семестр 5 группа 9САД1.20, 9САД2.20 |   **ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №**  23  1. SSL VPN. GRE через IPSec. Динамическая многоточечная VPN-сеть (DMVPN).  2. Практическое задание. Можно пользоваться Интернет. Схема сети.  У некоторой компании есть главный офис, который подключается в Интернет. Пограничный маршрутизатор Border подключен к провайдеру, который предоставляет услуги Интернет. Также существует второй офис компании, который таже подключен к публичной сети. И между ними проброшен VPN туннель. Между роутерами установлен OSPF, а между роутерами интернет компании и главным офисом установлена статическая маршрутизация. На основных коммутаторах офиса установлены по триVLAN, на роутерах сабинтерфейсы.  Для всего активного сетевого оборудования настройте доменное имя wsr2020.wsr. Создайте локального пользователя admin с паролем Pa$$w0rd. Для активного сетевого оборудования: пользователь должен обладать максимальным уровнем привилегий, пароль должен храниться в виде результата хэш функции, используйте алгоритм scrypt. Для всех сетевых устройств сконфигурируйте пароль wsr2020 для входа в привилегированный режим. Все сетевые устройства должны быть доступны для управления по протоколу SSHv2. Зашифруйте все открытые пароли.  Таблица VLAN двух офисов должна содержать следующие подсети: VLAN10:CLIENT, VLAN20:SERV, VLAN30:DMZ. Сконфигурируйте магистральные каналы.  Настройте подключение Border к провайдеру ISP с помощью протокола PPP. Адрес необходимо получить при помощи IPCP. Аутентификация не требуется.  Транспортный адрес необходимо получить при помощи протокола SLARP на соответствующий Serial интерфейс.  Устройства проходят аутентификацию по протоколу CHAP в одностороннем порядке. Только ISP аутентифицирует роутер Border. Для аутентификации используйте данные client65010 и пароль P@ssw0rd. Явно сконфигурируйте корректное значение MTU.  Сконфигурируйте GRE туннель между BRANCH1 и BRANCH2. В качестве адресов источника и назначения используйте адреса соответствующих loopback интерфейсов. Используйте номер туннельного интерфейса 1.  Обеспечьте возможность входа на Border c использованием доменных реквизитов. Группа MAdmins должна получать максимальный уровень привилегий при входе. Группа SAdmins должна получать при входе уровень привилегий. Обеспечьте возможность входа пользователя, созданного локально при доступности RADIUS сервера. Для 5 уровня привилегий сконфигурируйте расширенный набор команд. Добавьте возможность использования команд reload, debug и sh.  В главном офисе на сервере установлен DHCP, который раздает адресацию на все сетевые устройства. Здесь же установлены службы ААА, DNS, HTTP. Во втором офисе компании установленWeb-server и DMZ. На роутере Border установлена служба NAT.  Преподаватель\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Скиляжнов А.О.. |

Министерство образования Красноярского края

краевое государственное бюджетное профессиональное образовательное учреждение «Красноярский колледж радиоэлектроники и информационных технологий»

|  |  |  |  |
| --- | --- | --- | --- |
| |  |  |  | | --- | --- | --- | | |  | | --- | | РАССМОТРЕНО  на заседании цикловой комиссии  преподавателей профессионального  цикла технического профиля  Протокол №\_\_ от «\_\_\_»\_\_\_\_\_\_ 2021 г.  Председатель ЦК \_\_\_\_\_ Е. В. Харитонова | | ДИСЦИПЛИНА  МДК01.02 Организация, принципы построения и функционирования  компьютерных сетей  для специальности  09.02.06 Сетевое и системное\_\_\_\_\_\_\_\_  администрирование\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Семестр 5 группа 9САД1.20, 9САД2.20 |   **ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №**  24  1. Технология создания виртуальных частных сетей. Преимущество сети VPN. [Основы сетей VPN](https://static-course-assets.s3.amazonaws.com/CN503/ru/index.html#7.1.1). [Типы сетей VPN](https://static-course-assets.s3.amazonaws.com/CN503/ru/index.html#7.1.2). Site-to-Site VPN и VPN для удаленного доступа. VPN для крупных компаний и операторов связи.  2. Практическое задание. Можно пользоваться Интернет. Схема сети.  У некоторой компании есть главный офис, который подключается в Интернет. Пограничный маршрутизатор Border подключен к провайдеру, который предоставляет услуги Интернет. Также существует второй офис компании, который таже подключен к публичной сети. И между ними проброшен VPN туннель. Между роутерами установлен OSPF, а между роутерами интернет компании и главным офисом установлена статическая маршрутизация. На основных коммутаторах офиса установлены по триVLAN, на роутерах сабинтерфейсы.  Для всего активного сетевого оборудования настройте доменное имя wsr2020.wsr. Создайте локального пользователя admin с паролем Pa$$w0rd. Для активного сетевого оборудования: пользователь должен обладать максимальным уровнем привилегий, пароль должен храниться в виде результата хэш функции, используйте алгоритм scrypt. Для всех сетевых устройств сконфигурируйте пароль wsr2020 для входа в привилегированный режим. Все сетевые устройства должны быть доступны для управления по протоколу SSHv2. Зашифруйте все открытые пароли.  Таблица VLAN двух офисов должна содержать следующие подсети: VLAN10:CLIENT, VLAN20:SERV, VLAN30:DMZ. Сконфигурируйте магистральные каналы.  Настройте подключение Border к провайдеру ISP с помощью протокола PPP. Адрес необходимо получить при помощи IPCP. Аутентификация не требуется.  Транспортный адрес необходимо получить при помощи протокола SLARP на соответствующий Serial интерфейс.  Устройства проходят аутентификацию по протоколу CHAP в одностороннем порядке. Только ISP аутентифицирует роутер Border. Для аутентификации используйте данные client65010 и пароль P@ssw0rd. Явно сконфигурируйте корректное значение MTU.  Сконфигурируйте GRE туннель между BRANCH1 и BRANCH2. В качестве адресов источника и назначения используйте адреса соответствующих loopback интерфейсов. Используйте номер туннельного интерфейса 1.  Обеспечьте возможность входа на Border c использованием доменных реквизитов. Группа MAdmins должна получать максимальный уровень привилегий при входе. Группа SAdmins должна получать при входе уровень привилегий. Обеспечьте возможность входа пользователя, созданного локально при доступности RADIUS сервера. Для 5 уровня привилегий сконфигурируйте расширенный набор команд. Добавьте возможность использования команд reload, debug и sh.  В главном офисе на сервере установлен DHCP, который раздает адресацию на все сетевые устройства. Здесь же установлены службы ААА, DNS, HTTP. Во втором офисе компании установленWeb-server и DMZ. На роутере Border установлена служба NAT.  Преподаватель\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Скиляжнов А.О. |

Министерство образования Красноярского края

краевое государственное бюджетное профессиональное образовательное учреждение «Красноярский колледж радиоэлектроники и информационных технологий»

|  |  |  |  |
| --- | --- | --- | --- |
| |  |  |  | | --- | --- | --- | | |  | | --- | | РАССМОТРЕНО  на заседании цикловой комиссии  преподавателей профессионального  цикла технического профиля  Протокол №\_\_ от «\_\_\_»\_\_\_\_\_\_ 2021 г.  Председатель ЦК \_\_\_\_\_ Е. В. Харитонова | | ДИСЦИПЛИНА  МДК01.02 Организация, принципы построения и функционирования  компьютерных сетей  для специальности  09.02.06 Сетевое и системное\_\_\_\_\_\_\_\_  администрирование\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Семестр 5 группа 9САД1.20, 9САД2.20 |   **ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №**  25  1. Протокол PPPoE. [Обзор PPPoE](https://static-course-assets.s3.amazonaws.com/CN503/ru/index.html#6.3.1). [Настройка PPPoE](https://static-course-assets.s3.amazonaws.com/CN503/ru/index.html#6.3.2).  2. Практическое задание. Можно пользоваться Интернет. Схема сети.  У некоторой компании есть главный офис, который подключается в Интернет. Пограничный маршрутизатор Border подключен к провайдеру, который предоставляет услуги Интернет. Также существует второй офис компании, который таже подключен к публичной сети. И между ними проброшен VPN туннель. Между роутерами установлен OSPF, а между роутерами интернет компании и главным офисом установлена статическая маршрутизация. На основных коммутаторах офиса установлены по триVLAN, на роутерах сабинтерфейсы.  Для всего активного сетевого оборудования настройте доменное имя wsr2020.wsr. Создайте локального пользователя admin с паролем Pa$$w0rd. Для активного сетевого оборудования: пользователь должен обладать максимальным уровнем привилегий, пароль должен храниться в виде результата хэш функции, используйте алгоритм scrypt. Для всех сетевых устройств сконфигурируйте пароль wsr2020 для входа в привилегированный режим. Все сетевые устройства должны быть доступны для управления по протоколу SSHv2. Зашифруйте все открытые пароли.  Таблица VLAN двух офисов должна содержать следующие подсети: VLAN10:CLIENT, VLAN20:SERV, VLAN30:DMZ. Сконфигурируйте магистральные каналы.  Настройте подключение Border к провайдеру ISP с помощью протокола PPP. Адрес необходимо получить при помощи IPCP. Аутентификация не требуется.  Транспортный адрес необходимо получить при помощи протокола SLARP на соответствующий Serial интерфейс.  Устройства проходят аутентификацию по протоколу CHAP в одностороннем порядке. Только ISP аутентифицирует роутер Border. Для аутентификации используйте данные client65010 и пароль P@ssw0rd. Явно сконфигурируйте корректное значение MTU.  Сконфигурируйте GRE туннель между BRANCH1 и BRANCH2. В качестве адресов источника и назначения используйте адреса соответствующих loopback интерфейсов. Используйте номер туннельного интерфейса 1.  Обеспечьте возможность входа на Border c использованием доменных реквизитов. Группа MAdmins должна получать максимальный уровень привилегий при входе. Группа SAdmins должна получать при входе уровень привилегий. Обеспечьте возможность входа пользователя, созданного локально при доступности RADIUS сервера. Для 5 уровня привилегий сконфигурируйте расширенный набор команд. Добавьте возможность использования команд reload, debug и sh.  В главном офисе на сервере установлен DHCP, который раздает адресацию на все сетевые устройства. Здесь же установлены службы ААА, DNS, HTTP. Во втором офисе компании установленWeb-server и DMZ. На роутере Border установлена служба NAT.  Преподаватель\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Скиляжнов А.О. |

Министерство образования Красноярского края

краевое государственное бюджетное профессиональное образовательное учреждение «Красноярский колледж радиоэлектроники и информационных технологий»

|  |  |  |  |
| --- | --- | --- | --- |
| |  |  |  | | --- | --- | --- | | |  | | --- | | РАССМОТРЕНО  на заседании цикловой комиссии  преподавателей профессионального  цикла технического профиля  Протокол №\_\_ от «\_\_\_»\_\_\_\_\_\_ 2021 г.  Председатель ЦК \_\_\_\_\_ Е. В. Харитонова | | ДИСЦИПЛИНА  МДК01.02 Организация, принципы построения и функционирования  компьютерных сетей  для специальности  09.02.06 Сетевое и системное\_\_\_\_\_\_\_\_  администрирование\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Семестр 5 группа 9САД1.20, 9САД2.20 |   **ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №**  26  1. Решения широкополосного доступа. [Сравнение решений широкополосного доступа](https://static-course-assets.s3.amazonaws.com/CN503/ru/index.html#6.2). [Беспроводные широкополосные сети](https://static-course-assets.s3.amazonaws.com/CN503/ru/index.html#6.2.3). [Выбор решений широкополосного доступа](https://static-course-assets.s3.amazonaws.com/CN503/ru/index.html#6.2.4).  2. Практическое задание. Можно пользоваться Интернет. Схема сети.  У некоторой компании есть главный офис, который подключается в Интернет. Пограничный маршрутизатор Border подключен к провайдеру, который предоставляет услуги Интернет. Также существует второй офис компании, который таже подключен к публичной сети. И между ними проброшен VPN туннель. Между роутерами установлен OSPF, а между роутерами интернет компании и главным офисом установлена статическая маршрутизация. На основных коммутаторах офиса установлены по триVLAN, на роутерах сабинтерфейсы.  Для всего активного сетевого оборудования настройте доменное имя wsr2020.wsr. Создайте локального пользователя admin с паролем Pa$$w0rd. Для активного сетевого оборудования: пользователь должен обладать максимальным уровнем привилегий, пароль должен храниться в виде результата хэш функции, используйте алгоритм scrypt. Для всех сетевых устройств сконфигурируйте пароль wsr2020 для входа в привилегированный режим. Все сетевые устройства должны быть доступны для управления по протоколу SSHv2. Зашифруйте все открытые пароли.  Таблица VLAN двух офисов должна содержать следующие подсети: VLAN10:CLIENT, VLAN20:SERV, VLAN30:DMZ. Сконфигурируйте магистральные каналы.  Настройте подключение Border к провайдеру ISP с помощью протокола PPP. Адрес необходимо получить при помощи IPCP. Аутентификация не требуется.  Транспортный адрес необходимо получить при помощи протокола SLARP на соответствующий Serial интерфейс.  Устройства проходят аутентификацию по протоколу CHAP в одностороннем порядке. Только ISP аутентифицирует роутер Border. Для аутентификации используйте данные client65010 и пароль P@ssw0rd. Явно сконфигурируйте корректное значение MTU.  Сконфигурируйте GRE туннель между BRANCH1 и BRANCH2. В качестве адресов источника и назначения используйте адреса соответствующих loopback интерфейсов. Используйте номер туннельного интерфейса 1.  Обеспечьте возможность входа на Border c использованием доменных реквизитов. Группа MAdmins должна получать максимальный уровень привилегий при входе. Группа SAdmins должна получать при входе уровень привилегий. Обеспечьте возможность входа пользователя, созданного локально при доступности RADIUS сервера. Для 5 уровня привилегий сконфигурируйте расширенный набор команд. Добавьте возможность использования команд reload, debug и sh.  В главном офисе на сервере установлен DHCP, который раздает адресацию на все сетевые устройства. Здесь же установлены службы ААА, DNS, HTTP. Во втором офисе компании установленWeb-server и DMZ. На роутере Border установлена служба NAT.  Преподаватель\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Скиляжнов А.О. |

Министерство образования Красноярского края

краевое государственное бюджетное профессиональное образовательное учреждение «Красноярский колледж радиоэлектроники и информационных технологий»

|  |  |  |  |
| --- | --- | --- | --- |
| |  |  |  | | --- | --- | --- | | |  | | --- | | РАССМОТРЕНО  на заседании цикловой комиссии  преподавателей профессионального  цикла технического профиля  Протокол №\_\_ от «\_\_\_»\_\_\_\_\_\_ 2021 г.  Председатель ЦК \_\_\_\_\_ Е. В. Харитонова | | ДИСЦИПЛИНА  МДК01.02 Организация, принципы построения и функционирования  компьютерных сетей  для специальности  09.02.06 Сетевое и системное\_\_\_\_\_\_\_\_  администрирование\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Семестр 5 группа 9САД1.20, 9САД2.20 |   **ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №**  27  1. [Преимущества протокола PPP](https://static-course-assets.s3.amazonaws.com/CN503/ru/index.html#3.2.1). [LCP и NCP](https://static-course-assets.s3.amazonaws.com/CN503/ru/index.html#3.2.2). [Сеансы PPP](https://static-course-assets.s3.amazonaws.com/CN503/ru/index.html#3.2.3). [Настройка протокола PPP](https://static-course-assets.s3.amazonaws.com/CN503/ru/index.html#3.3.1). [Аутентификация PPP](https://static-course-assets.s3.amazonaws.com/CN503/ru/index.html#3.3.2). [Отладка соединений WAN](https://static-course-assets.s3.amazonaws.com/CN503/ru/index.html#3.4). [Отладка PPP](https://static-course-assets.s3.amazonaws.com/CN503/ru/index.html#3.4.1).  2. Практическое задание. Можно пользоваться Интернет. Схема сети.  У некоторой компании есть главный офис, который подключается в Интернет. Пограничный маршрутизатор Border подключен к провайдеру, который предоставляет услуги Интернет. Также существует второй офис компании, который таже подключен к публичной сети. И между ними проброшен VPN туннель. Между роутерами установлен OSPF, а между роутерами интернет компании и главным офисом установлена статическая маршрутизация. На основных коммутаторах офиса установлены по триVLAN, на роутерах сабинтерфейсы.  Для всего активного сетевого оборудования настройте доменное имя wsr2020.wsr. Создайте локального пользователя admin с паролем Pa$$w0rd. Для активного сетевого оборудования: пользователь должен обладать максимальным уровнем привилегий, пароль должен храниться в виде результата хэш функции, используйте алгоритм scrypt. Для всех сетевых устройств сконфигурируйте пароль wsr2020 для входа в привилегированный режим. Все сетевые устройства должны быть доступны для управления по протоколу SSHv2. Зашифруйте все открытые пароли.  Таблица VLAN двух офисов должна содержать следующие подсети: VLAN10:CLIENT, VLAN20:SERV, VLAN30:DMZ. Сконфигурируйте магистральные каналы.  Настройте подключение Border к провайдеру ISP с помощью протокола PPP. Адрес необходимо получить при помощи IPCP. Аутентификация не требуется.  Транспортный адрес необходимо получить при помощи протокола SLARP на соответствующий Serial интерфейс.  Устройства проходят аутентификацию по протоколу CHAP в одностороннем порядке. Только ISP аутентифицирует роутер Border. Для аутентификации используйте данные client65010 и пароль P@ssw0rd. Явно сконфигурируйте корректное значение MTU.  Сконфигурируйте GRE туннель между BRANCH1 и BRANCH2. В качестве адресов источника и назначения используйте адреса соответствующих loopback интерфейсов. Используйте номер туннельного интерфейса 1.  Обеспечьте возможность входа на Border c использованием доменных реквизитов. Группа MAdmins должна получать максимальный уровень привилегий при входе. Группа SAdmins должна получать при входе уровень привилегий. Обеспечьте возможность входа пользователя, созданного локально при доступности RADIUS сервера. Для 5 уровня привилегий сконфигурируйте расширенный набор команд. Добавьте возможность использования команд reload, debug и sh.  В главном офисе на сервере установлен DHCP, который раздает адресацию на все сетевые устройства. Здесь же установлены службы ААА, DNS, HTTP. Во втором офисе компании установленWeb-server и DMZ. На роутере Border установлена служба NAT.  Преподаватель\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Скиляжнов А.О. |

Министерство образования Красноярского края

краевое государственное бюджетное профессиональное образовательное учреждение «Красноярский колледж радиоэлектроники и информационных технологий»

|  |  |  |  |
| --- | --- | --- | --- |
| |  |  |  | | --- | --- | --- | | |  | | --- | | РАССМОТРЕНО  на заседании цикловой комиссии  преподавателей профессионального  цикла технического профиля  Протокол №\_\_ от «\_\_\_»\_\_\_\_\_\_ 2021 г.  Председатель ЦК \_\_\_\_\_ Е. В. Харитонова | | ДИСЦИПЛИНА  МДК01.02 Организация, принципы построения и функционирования  компьютерных сетей  для специальности  09.02.06 Сетевое и системное\_\_\_\_\_\_\_\_  администрирование\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Семестр 5 группа 9САД1.20, 9САД2.20 |   **ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №**  28  1. Стандарты WAN. Общепринятая терминология глобальных сетей. Устройства глобальной сети. Последовательная связь. Сеть с коммутацией каналов. Сеть с коммутацией пакетов. SDH, SONET и DWDM.  2. Практическое задание. Можно пользоваться Интернет. Схема сети.  У некоторой компании есть главный офис, который подключается в Интернет. Пограничный маршрутизатор Border подключен к провайдеру, который предоставляет услуги Интернет. Также существует второй офис компании, который таже подключен к публичной сети. И между ними проброшен VPN туннель. Между роутерами установлен OSPF, а между роутерами интернет компании и главным офисом установлена статическая маршрутизация. На основных коммутаторах офиса установлены по триVLAN, на роутерах сабинтерфейсы.  Для всего активного сетевого оборудования настройте доменное имя wsr2020.wsr. Создайте локального пользователя admin с паролем Pa$$w0rd. Для активного сетевого оборудования: пользователь должен обладать максимальным уровнем привилегий, пароль должен храниться в виде результата хэш функции, используйте алгоритм scrypt. Для всех сетевых устройств сконфигурируйте пароль wsr2020 для входа в привилегированный режим. Все сетевые устройства должны быть доступны для управления по протоколу SSHv2. Зашифруйте все открытые пароли.  Таблица VLAN двух офисов должна содержать следующие подсети: VLAN10:CLIENT, VLAN20:SERV, VLAN30:DMZ. Сконфигурируйте магистральные каналы.  Настройте подключение Border к провайдеру ISP с помощью протокола PPP. Адрес необходимо получить при помощи IPCP. Аутентификация не требуется.  Транспортный адрес необходимо получить при помощи протокола SLARP на соответствующий Serial интерфейс.  Устройства проходят аутентификацию по протоколу CHAP в одностороннем порядке. Только ISP аутентифицирует роутер Border. Для аутентификации используйте данные client65010 и пароль P@ssw0rd. Явно сконфигурируйте корректное значение MTU.  Сконфигурируйте GRE туннель между BRANCH1 и BRANCH2. В качестве адресов источника и назначения используйте адреса соответствующих loopback интерфейсов. Используйте номер туннельного интерфейса 1.  Обеспечьте возможность входа на Border c использованием доменных реквизитов. Группа MAdmins должна получать максимальный уровень привилегий при входе. Группа SAdmins должна получать при входе уровень привилегий. Обеспечьте возможность входа пользователя, созданного локально при доступности RADIUS сервера. Для 5 уровня привилегий сконфигурируйте расширенный набор команд. Добавьте возможность использования команд reload, debug и sh.  В главном офисе на сервере установлен DHCP, который раздает адресацию на все сетевые устройства. Здесь же установлены службы ААА, DNS, HTTP. Во втором офисе компании установленWeb-server и DMZ. На роутере Border установлена служба NAT.  Преподаватель\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Скиляжнов А.О. |

Министерство образования Красноярского края

краевое государственное бюджетное профессиональное образовательное учреждение «Красноярский колледж радиоэлектроники и информационных технологий»

|  |  |  |  |
| --- | --- | --- | --- |
| |  |  |  | | --- | --- | --- | | |  | | --- | | РАССМОТРЕНО  на заседании цикловой комиссии  преподавателей профессионального  цикла технического профиля  Протокол №\_\_ от «\_\_\_»\_\_\_\_\_\_ 2021 г.  Председатель ЦК \_\_\_\_\_ Е. В. Харитонова | | ДИСЦИПЛИНА  МДК01.02 Организация, принципы построения и функционирования  компьютерных сетей  для специальности  09.02.06 Сетевое и системное\_\_\_\_\_\_\_\_  администрирование\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Семестр 5 группа 9САД1.20, 9САД2.20 |   **ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №**  29  1. [Обзор последовательного соединения «точка-точка»](https://static-course-assets.s3.amazonaws.com/CN503/ru/index.html#3.1). [Связь по последовательному каналу](https://static-course-assets.s3.amazonaws.com/CN503/ru/index.html#3.1.1). [Инкапсуляция HDLC](https://static-course-assets.s3.amazonaws.com/CN503/ru/index.html#3.1.2).  2. Практическое задание. Можно пользоваться Интернет. Схема сети.  У некоторой компании есть главный офис, который подключается в Интернет. Пограничный маршрутизатор Border подключен к провайдеру, который предоставляет услуги Интернет. Также существует второй офис компании, который таже подключен к публичной сети. И между ними проброшен VPN туннель. Между роутерами установлен OSPF, а между роутерами интернет компании и главным офисом установлена статическая маршрутизация. На основных коммутаторах офиса установлены по триVLAN, на роутерах сабинтерфейсы.  Для всего активного сетевого оборудования настройте доменное имя wsr2020.wsr. Создайте локального пользователя admin с паролем Pa$$w0rd. Для активного сетевого оборудования: пользователь должен обладать максимальным уровнем привилегий, пароль должен храниться в виде результата хэш функции, используйте алгоритм scrypt. Для всех сетевых устройств сконфигурируйте пароль wsr2020 для входа в привилегированный режим. Все сетевые устройства должны быть доступны для управления по протоколу SSHv2. Зашифруйте все открытые пароли.  Таблица VLAN двух офисов должна содержать следующие подсети: VLAN10:CLIENT, VLAN20:SERV, VLAN30:DMZ. Сконфигурируйте магистральные каналы.  Настройте подключение Border к провайдеру ISP с помощью протокола PPP. Адрес необходимо получить при помощи IPCP. Аутентификация не требуется.  Транспортный адрес необходимо получить при помощи протокола SLARP на соответствующий Serial интерфейс.  Устройства проходят аутентификацию по протоколу CHAP в одностороннем порядке. Только ISP аутентифицирует роутер Border. Для аутентификации используйте данные client65010 и пароль P@ssw0rd. Явно сконфигурируйте корректное значение MTU.  Сконфигурируйте GRE туннель между BRANCH1 и BRANCH2. В качестве адресов источника и назначения используйте адреса соответствующих loopback интерфейсов. Используйте номер туннельного интерфейса 1.  Обеспечьте возможность входа на Border c использованием доменных реквизитов. Группа MAdmins должна получать максимальный уровень привилегий при входе. Группа SAdmins должна получать при входе уровень привилегий. Обеспечьте возможность входа пользователя, созданного локально при доступности RADIUS сервера. Для 5 уровня привилегий сконфигурируйте расширенный набор команд. Добавьте возможность использования команд reload, debug и sh.  В главном офисе на сервере установлен DHCP, который раздает адресацию на все сетевые устройства. Здесь же установлены службы ААА, DNS, HTTP. Во втором офисе компании установленWeb-server и DMZ. На роутере Border установлена служба NAT.  Преподаватель\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Скиляжнов А.О. |

Министерство образования Красноярского края

краевое государственное бюджетное профессиональное образовательное учреждение «Красноярский колледж радиоэлектроники и информационных технологий»

|  |  |  |  |
| --- | --- | --- | --- |
| |  |  |  | | --- | --- | --- | | |  | | --- | | РАССМОТРЕНО  на заседании цикловой комиссии  преподавателей профессионального  цикла технического профиля  Протокол №\_\_ от «\_\_\_»\_\_\_\_\_\_ 2021 г.  Председатель ЦК \_\_\_\_\_ Е. В. Харитонова | | ДИСЦИПЛИНА  МДК01.02 Организация, принципы построения и функционирования  компьютерных сетей  для специальности  09.02.06 Сетевое и системное\_\_\_\_\_\_\_\_  администрирование\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Семестр 5 группа 9САД1.20, 9САД2.20 |   **ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №**  30  1. [Цель создания глобальных сетей](https://static-course-assets.s3.amazonaws.com/CN503/ru/index.html#2.1.1). [Принцип работы глобальной сети](https://static-course-assets.s3.amazonaws.com/CN503/ru/index.html#2.1.2). В[ыбор технологии глобальной сети](https://static-course-assets.s3.amazonaws.com/CN503/ru/index.html#2.2). [Инфраструктуры частных глобальных сетей](https://static-course-assets.s3.amazonaws.com/CN503/ru/index.html#2.2.2). [Инфраструктура общедоступной глобальной сети](https://static-course-assets.s3.amazonaws.com/CN503/ru/index.html#2.2.3). [Выбор сервисов глобальной сети](https://static-course-assets.s3.amazonaws.com/CN503/ru/index.html#2.2.4).  2. Практическое задание. Можно пользоваться Интернет. Схема сети.  У некоторой компании есть главный офис, который подключается в Интернет. Пограничный маршрутизатор Border подключен к провайдеру, который предоставляет услуги Интернет. Также существует второй офис компании, который таже подключен к публичной сети. И между ними проброшен VPN туннель. Между роутерами установлен OSPF, а между роутерами интернет компании и главным офисом установлена статическая маршрутизация. На основных коммутаторах офиса установлены по триVLAN, на роутерах сабинтерфейсы.  Для всего активного сетевого оборудования настройте доменное имя wsr2020.wsr. Создайте локального пользователя admin с паролем Pa$$w0rd. Для активного сетевого оборудования: пользователь должен обладать максимальным уровнем привилегий, пароль должен храниться в виде результата хэш функции, используйте алгоритм scrypt. Для всех сетевых устройств сконфигурируйте пароль wsr2020 для входа в привилегированный режим. Все сетевые устройства должны быть доступны для управления по протоколу SSHv2. Зашифруйте все открытые пароли.  Таблица VLAN двух офисов должна содержать следующие подсети: VLAN10:CLIENT, VLAN20:SERV, VLAN30:DMZ. Сконфигурируйте магистральные каналы.  Настройте подключение Border к провайдеру ISP с помощью протокола PPP. Адрес необходимо получить при помощи IPCP. Аутентификация не требуется.  Транспортный адрес необходимо получить при помощи протокола SLARP на соответствующий Serial интерфейс.  Устройства проходят аутентификацию по протоколу CHAP в одностороннем порядке. Только ISP аутентифицирует роутер Border. Для аутентификации используйте данные client65010 и пароль P@ssw0rd. Явно сконфигурируйте корректное значение MTU.  Сконфигурируйте GRE туннель между BRANCH1 и BRANCH2. В качестве адресов источника и назначения используйте адреса соответствующих loopback интерфейсов. Используйте номер туннельного интерфейса 1.  Обеспечьте возможность входа на Border c использованием доменных реквизитов. Группа MAdmins должна получать максимальный уровень привилегий при входе. Группа SAdmins должна получать при входе уровень привилегий. Обеспечьте возможность входа пользователя, созданного локально при доступности RADIUS сервера. Для 5 уровня привилегий сконфигурируйте расширенный набор команд. Добавьте возможность использования команд reload, debug и sh.  В главном офисе на сервере установлен DHCP, который раздает адресацию на все сетевые устройства. Здесь же установлены службы ААА, DNS, HTTP. Во втором офисе компании установленWeb-server и DMZ. На роутере Border установлена служба NAT.  Преподаватель\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Скиляжнов А.О. |

* + 1. **ПЕРЕЧНЬ ПЕЧАТНЫХ ИЗДАНИЙ, ЭЛЕКТРОННЫХ ИЗДАНИЙ (ЭЛЕКТРОННЫХ РЕСУРСОВ), ДОПОЛНИТЕЛЬНЫХ ИСТОЧНИКОВ**

Основные источники:

# Кузин, А.В. Компьютерные сети: учеб. пособие / А.В. Кузин, Д.А. Кузин. – 4-е изд. – М.: ФОРУМ: ИНФРА-М, 2020. – 190 с;

1. Максимов, Н.В. Компьютерные сети: уч. Пособие для студентов учреждений среднего проф. образования. [Текст] /Н.В. Максимов,  
    И.И. Попов – М.: ФОРУМ, 2015, - 464 с.;

# Новожилов, Е.О. Компьютерные сети: учеб. пособие для студ. Учреждений сред. Проф. образования / Е.О. Новожилов, О.П. Новожилов. – 5-е изд. – М.: издательский центр «Академия», 2017. – 224с;

# Олифер, В. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов.5-е изд. [Текст] /В.Олифер – С-Пб.: Питер, 2016, – 992 с.;

1. Пескова, С.А. Сети и телекоммуникации: учеб. пособие для студ. высш. учеб. заведений. – 3-е изд. [Текст] / С. А. Пескова, А. В. Кузин,   
   А. Н. Волков – М.: Издат. центр «Академия», 2012, – 352 с.;
2. Самуйлов, К.Е. Сети и телекоммуникации: учебник и практикум для академического бакалавриата / под ред. К.Е. Самуйлова,  
    И.А. Шалимова, Д.С. Кулябова. – М.: Издательство Юрайт, 2019. – 363 с;
3. Пруцков А.В., Математическая логика и теория алгоритмов :Уч. / А.В.Пруцков-М.:КУРС, НИЦ ИНФРА-М,2018.-152 с.;
4. Спирина М.С., Теория вероятностей и математическая статистика :учебник для студ.учреждений сред. проф. образования / М.С. Спирина, П.А. Спирин. – 8-е изд., стер. – М.: Издательский центр «Академия», 2017.-352с.

Дополнительные источники:

1. Костров, Б. В. Сети и системы передачи информации: учеб. для студ. учреждений сред. проф. образования / Б.В. Костров, В.Н. Ручкин. – М.: Издательский центр «Академия», 2018. – 256 с;
2. Костров, Б. В. Технологии физического уровня передачи данных: учебник / Б.В. Костров, А.В. Кистрин, А.И Ефимов, Д.И. Устюков. – М.: Издательский центр «Академия», 2018. – 224 с;
3. Семенов, А.Б. Проектирование и расчет структурированных кабельных систем и их компонентов / А.Б. Семенов. – М.: ДМК:Пресс, 2017. – 416с.

Информационные ресурсы:

http://www.netacad.com/

http://www.cisco.com/

https://www.huaweicup.ru/

<https://e.huawei.com/>