ФЕДЕРАЛЬНОЕ АГЕНТСТВО ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА

Федеральное государственное бюджетное образовательное учреждение высшего образования

«Петербургский государственный университет путей сообщения Императора Александра I»

(ФГБОУ ВО ПГУПС)

Рязанский филиал ПГУПС

УТВЕРЖДАЮ
Директор Рязанского
филиала ПГУПС
_____ О.А.Дедова
«05» марта 2024 г.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ДИСЦИПЛИНЫ

ПМ.01 НАСТРОЙКА СЕТЕВОЙ ИНФРАСТРУКТУРЫ

для специальности

09.02.06 СЕТЕВОЕ И СИСТЕМНОЕ АДМИНИСТРИРОВАНИЕ

квалификация **Системный администратор**

вид подготовки – базовая

форма обучения – очная

Рязань 2024

Фонд оценочных средств разработан на основе Федерального государственного образовательного стандарта среднего профессионального образования и рабочей программы профессионального модуля ПМ.01 Настройка сетевой инфраструктуры.

Разработчик программы:
Стрельникова Н.В., преподаватель Рязанского филиала ПГУПС

Рецензенты:
Федулов М.Н., преподаватель Рязанского филиала ПГУПС

СОДЕРЖАНИЕ

1.ПАСПОРТ ФОНДА ОЦЕНОЧНЫХ СРЕДСТВ

ПМ.01 Настройка сетевой инфраструктуры

Фонд оценочных средств (ФОС) разработан на основе Федерального государственного образовательного стандарта среднего профессионального образования по специальности 09.02.06 Сетевое и системное администрирование ПМ.01 Настройка сетевой инфраструктуры и представляет собой совокупность контрольных материалов, предназначенных для оценки промежуточной аттестации обучающихся.

2. ЦЕЛЬ И ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОСВОЕНИЯ ДИСЦИПЛИНЫ

В результате освоения ПМ.01 Настройка сетевой инфраструктуры обучающимися осваиваются умения и знания

Код ПК, ОК	Умения	Знания
ОК 01. ОК 02. ОК 03. ОК 04. ОК 05. ОК 06. ОК 07. ОК 08. ОК 09. ПК 1.1. ПК 1.2. ПК 1.3. ПК 1.4. ПК 1.5. ПК 1.6. ПК 1.7.	- проектировать локальную сеть, выбирать сетевые топологии; -использовать многофункциональные приборы мониторинга, программно-аппаратные средства технического контроля локальной сети	- общие принципы построения сетей, сетевых топологий, многослойной модели OSI, требований к компьютерным сетям; - архитектуру протоколов, стандартизации сетей, этапов проектирования сетевой инфраструктуры; - базовые протоколы и технологии локальных сетей; - принципы построения высокоскоростных локальных сетей; - стандарты кабелей, основные виды коммуникационных устройств, терминов, понятий, стандартов и типовых элементов структурированной кабельной системы.

3.ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО УЧЕБНОЙ ДИСЦИПЛИНЕ

Фонд оценочных средств (далее ФОС) позволяет оценить достижения запланированных по профессиональному модулю. Оценка освоения профессионального модуля ПМ.01 Настройка сетевой инфраструктуры предусматривает следующие формы промежуточной аттестации:

ПМ.01	**Формы промежуточной аттестации по семестрам**							
	1	2	3	4	5	6	7	8
МДК. 01.01 Компьютерные сети				Экзамен				
МДК. 01.02 Организация, принципы построения и функционирования компьютерных сетей						Экзамен		
МДК.01.03 Безопасность компьютерных сетей						Экзамен		
Учебная практика УП.01.01						Дифференцированный зачет		
Производственная практика (по профилю специальности) ПП.01.01						Дифференцированный зачет		
Профессиональный модуль ПМ.01.ЭК	Экзамен (квалификационный) 6 семестр							

ЭКЗАМЕН

1. **Условия аттестации**: аттестация проводится в форме экзамена по частичному или полному освоению учебного материала междисциплинарного курса.
2. **Время аттестации:** на проведение аттестации отводится 2 часа, на подготовку – 30 минут.
3. **Общие условия оценивания:**

оценка по промежуточной аттестации носит *комплексный характер и может включать в себя:*

- результаты выполнения аттестационных заданий;
- оценку портфолио;
- оценку прочих достижений обучающегося.

4. Критерии оценки

Оценка «5», «отлично» «отл.» исчерпывающий, точный ответ, демонстрирующий хорошее знание вопроса, умение использовать критические материалы для аргументации и самостоятельных выводов; свободное владение научной терминологией; умение излагать материал последовательно, делать обобщения и выводы.

Оценка «4», «хорошо», «хор.» ответ, обнаруживающий хорошее знание и понимание учебного материала, умение анализировать, приводя примеры; умение излагать материал последовательно и грамотно. В ответе может быть недостаточно полно развернута аргументация, возможны отдельные недостатки в формулировке выводов; допускаются отдельные погрешности в речи.

Оценка 3 «удовлетворительно», «удовл.» ответ, в котором материал раскрыт в основном правильно, но схематично или недостаточно полно, с отклонениями от последовательности изложения. Нет полноценных обобщений и выводов; допущены ошибки в речевом оформлении высказывания.

Оценка 2 «неудовлетворительно». «неуд.» ответ обнаруживает незнание материала и неумение его анализировать; в ответе отсутствуют примеры; нарушена логика в изложении материала, нет необходимых обобщений и выводов; недостаточно сформированы навыки устной речи.

5. Перечень вопросов и практических заданий для проведения экзамена по МДК. 01.01 «Компьютерные сети»

Вопросы:

1. Классификация компьютерных сетей.
2. Модель взаимодействия открытых систем. Уровни модели OSI.
3. Методы защиты информации от ошибок. Классификация помехоустойчивых кодов
4. Помехоустойчивое кодирование. Кодирование с контролем четности
5. Помехоустойчивое кодирование. Код Хэмминга
6. Использование обратной связи. Основные термины.
7. Система с информационной обратной связью.
8. Система с решающей обратной связью.
9. Понятие коммутации. Коммутация каналов.
10. Понятие коммутации. Коммутация сообщений.
11. Понятие коммутации. Коммутация пакетов.
12. Способ передачи пакетов в сетях.
13. Протоколы. Стандартные стеки коммуникационных протоколов.
14. Стек протоколов TCP/IP.
15. Классы IP-адресов. Особые IP-адреса.
16. Стек протоколов IPX/SPX.
17. Семейство сетевых технологий Ethernet. Принцип работы Ethernet.
18. Принцип работы Ethernet. Взаимодействие на подуровнях LLC и MAC.
19. Характеристики физической среды передачи данных.
20. Коаксиальный кабель. Конструкция и характеристики.
21. Витая пара. Конструкция и характеристики.
22. Оптоволокно. Конструкция и характеристики.
23. Стандарты беспроводных сетей
24. Основные режимы работы беспроводных сетей

25.Область применения сетей Wi-Fi. Примеры использования.

Практические задания:

ЗАДАНИЕ № 1

Текст задания: Создать сеть для трех ПК, разделенной на две подсети с использованием двух сетевых интерфейсов на одном из узлов. При монтаже сети необходимо использовать коммутационную панель, сетевую розетку и коммутатор/маршрутизатор. Используя сетевые утилиты проверить работоспособность подсети.

Конфигурация сети:

IP – адрес первой подсети **192.168.0.0**

IP – адрес второй подсети **10.101.120.0**

Максимальное количество IP-адресов – 6

Количество используемых хостов - 4

ЗАДАНИЕ № 2

Текст задания:Создать сеть для трех ПК, разделенной на две подсети с использованием двух сетевых интерфейсов на одном из узлов. При монтаже сети необходимо использовать коммутационную панель, сетевую розетку и коммутатор/маршрутизатор. Используя сетевые утилиты проверить работоспособность подсети.

Конфигурация сети:

IP – адрес первой подсети **156.140.125.0**

IP – адрес второй подсети **130.120.110.16**

Максимальное количество IP-адресов – 6

Количество используемых хостов - 4

ЗАДАНИЕ № 3

Текст задания: Создать сеть для трех ПК, разделенной на две подсети с использованием двух сетевых интерфейсов на одном из узлов. При монтаже сети необходимо использовать коммутационную панель, сетевую розетку и коммутатор/маршрутизатор. Используя сетевые утилиты проверить работоспособность подсети.

Конфигурация сети:

IP – адрес первой подсети **113.240.23.24**

IP – адрес второй подсети **120.4.110.200**

Максимальное количество IP-адресов – 6

Количество используемых хостов - 4

ЗАДАНИЕ № 4

Текст задания:Создать сеть для трех ПК, разделенной на две подсети с использованием двух сетевых интерфейсов на одном из узлов. При монтаже сети необходимо использовать коммутационную панель, сетевую розетку и коммутатор/маршрутизатор. Используя сетевые утилиты проверить работоспособность подсети.

Конфигурация сети:

IP – адрес первой подсети **119.4.155.16**

IP – адрес второй подсети **120.4.155.200**

Максимальное количество IP-адресов – 6
Количество используемых хостов - 4

ЗАДАНИЕ № 5

Текст задания:Создать сеть для трех ПК, разделенной на две подсети с использованием двух сетевых интерфейсов на одном из узлов. При монтаже сети необходимо использовать коммутационную панель, сетевую розетку и коммутатор/маршрутизатор. Используя сетевые утилиты проверить работоспособность подсети.

Конфигурация сети:

IP – адрес первой подсети **112.26.23.64**
IP – адрес второй подсети **145.68.23.56**
Максимальное количество IP-адресов – 6
Количество используемых хостов - 4

ЗАДАНИЕ № 6

Текст задания:Создать сеть для трех ПК, разделенной на две подсети с использованием двух сетевых интерфейсов на одном из узлов. При монтаже сети необходимо использовать коммутационную панель, сетевую розетку и коммутатор/маршрутизатор. Используя сетевые утилиты проверить работоспособность подсети.

Конфигурация сети:

IP – адрес первой подсети **100.45.25.80**
IP – адрес второй подсети **12.26.85.40**
Максимальное количество IP-адресов – 6
Количество используемых хостов - 4

ЗАДАНИЕ № 7

Текст задания:Создать сеть для трех ПК, разделенной на две подсети с использованием двух сетевых интерфейсов на одном из узлов. При монтаже сети необходимо использовать коммутационную панель, сетевую розетку и коммутатор/маршрутизатор. Используя сетевые утилиты проверить работоспособность подсети.

Конфигурация сети:

IP – адрес первой подсети **13.75.96.56**
IP – адрес второй подсети **12.26.185.40**
Максимальное количество IP-адресов – 6
Количество используемых хостов - 4

ЗАДАНИЕ № 8

Текст задания:Создать сеть для трех ПК, разделенной на две подсети с использованием двух сетевых интерфейсов на одном из узлов. При монтаже сети необходимо использовать коммутационную панель, сетевую розетку и коммутатор/маршрутизатор. Используя сетевые утилиты проверить работоспособность подсети.

Конфигурация сети:

IP – адрес первой подсети **30.56.82.16**
IP – адрес второй подсети **177.12.19.80**
Максимальное количество IP-адресов – 6

Количество используемых хостов - 4

ЗАДАНИЕ № 9

Текст задания:Создать сеть для трех ПК, разделенной на две подсети с использованием двух сетевых интерфейсов на одном из узлов. При монтаже сети необходимо использовать коммутационную панель, сетевую розетку и коммутатор/маршрутизатор. Используя сетевые утилиты проверить работоспособность подсети.

Конфигурация сети:

IP – адрес первой подсети **188.52.195.72**

IP – адрес второй подсети **111.45.32.16**

Максимальное количество IP-адресов – 6

Количество используемых хостов - 4

ЗАДАНИЕ № 10

Текст задания:Создать сеть для трех ПК, разделенной на две подсети с использованием двух сетевых интерфейсов на одном из узлов. При монтаже сети необходимо использовать коммутационную панель, сетевую розетку и коммутатор/маршрутизатор. Используя сетевые утилиты проверить работоспособность подсети.

Конфигурация сети:

IP – адрес первой подсети **11.52.74.80**

IP – адрес второй подсети **177.52.69.80**

Максимальное количество IP-адресов – 6

Количество используемых хостов - 4

ЗАДАНИЕ № 11

Текст задания:Создать сеть для трех ПК, разделенной на две подсети с использованием двух сетевых интерфейсов на одном из узлов. При монтаже сети необходимо использовать коммутационную панель, сетевую розетку и коммутатор/маршрутизатор. Используя сетевые утилиты проверить работоспособность подсети.

Конфигурация сети:

IP – адрес первой подсети **112.126.123.64**

IP – адрес второй подсети **25.45.85.56**

Максимальное количество IP-адресов – 6

Количество используемых хостов - 4

ЗАДАНИЕ № 12

Текст задания:Создать сеть для трех ПК, разделенной на две подсети с использованием двух сетевых интерфейсов на одном из узлов. При монтаже сети необходимо использовать коммутационную панель, сетевую розетку и коммутатор/маршрутизатор. Используя сетевые утилиты проверить работоспособность подсети.

Конфигурация сети:

IP – адрес первой подсети **201.45.75.96**

IP – адрес второй подсети **177.152.169.80**

Максимальное количество IP-адресов – 6

Количество используемых хостов - 4

ЗАДАНИЕ № 13

Текст задания:Создать сеть для трех ПК, разделенной на две подсети с использованием двух сетевых интерфейсов на одном из узлов. При монтаже сети необходимо использовать коммутационную панель, сетевую розетку и коммутатор/маршрутизатор. Используя сетевые утилиты проверить работоспособность подсети.

Конфигурация сети:

IP – адрес первой подсети **155.45.85.112**

IP – адрес второй подсети **201.125.63.16**

Максимальное количество IP-адресов – 6

Количество используемых хостов - 4

ЗАДАНИЕ № 14

Текст задания:Создать сеть для трех ПК, разделенной на две подсети с использованием двух сетевых интерфейсов на одном из узлов. При монтаже сети необходимо использовать коммутационную панель, сетевую розетку и коммутатор/маршрутизатор. Используя сетевые утилиты проверить работоспособность подсети.

Конфигурация сети:

IP – адрес первой подсети **188.52.95.72**

IP – адрес второй подсети **201.125.163.16**

Максимальное количество IP-адресов – 6

Количество используемых хостов - 4

ЗАДАНИЕ № 15

Текст задания:Создать сеть для трех ПК, разделенной на две подсети с использованием двух сетевых интерфейсов на одном из узлов. При монтаже сети необходимо использовать коммутационную панель, сетевую розетку и коммутатор/маршрутизатор. Используя сетевые утилиты проверить работоспособность подсети.

Конфигурация сети:

IP – адрес первой подсети **37.45.95.32**

IP – адрес второй подсети **192.158.56.96**

Максимальное количество IP-адресов – 6

Количество используемых хостов - 4

ЗАДАНИЕ № 16

Текст задания:Создать сеть для трех ПК, разделенной на две подсети с использованием двух сетевых интерфейсов на одном из узлов. При монтаже сети необходимо использовать коммутационную панель, сетевую розетку и коммутатор/маршрутизатор. Используя сетевые утилиты проверить работоспособность подсети.

Конфигурация сети:

IP – адрес первой подсети **137.145.95.32**

IP – адрес второй подсети **192.58.56.96**

Максимальное количество IP-адресов – 6

Количество используемых хостов - 4

ЗАДАНИЕ № 17

Текст задания:Создать сеть для трех ПК, разделенной на две подсети с использованием двух сетевых интерфейсов на одном из узлов. При монтаже сети необходимо использовать коммутационную панель, сетевую розетку и коммутатор/маршрутизатор. Используя сетевые утилиты проверить работоспособность подсети.

Конфигурация сети:

IP – адрес первой подсети **10.10.25.72**

IP – адрес второй подсети **112.56.35.80**

Максимальное количество IP-адресов – 6

Количество используемых хостов - 4

ЗАДАНИЕ № 18

Текст задания:Создать сеть для трех ПК, разделенной на две подсети с использованием двух сетевых интерфейсов на одном из узлов. При монтаже сети необходимо использовать коммутационную панель, сетевую розетку и коммутатор/маршрутизатор. Используя сетевые утилиты проверить работоспособность подсети.

Конфигурация сети:

IP – адрес первой подсети **180.10.215.72**

IP – адрес второй подсети **12.56.135.80**

Максимальное количество IP-адресов – 6

Количество используемых хостов - 4

ЗАДАНИЕ № 19

Текст задания:Создать сеть для трех ПК, разделенной на две подсети с использованием двух сетевых интерфейсов на одном из узлов. При монтаже сети необходимо использовать коммутационную панель, сетевую розетку и коммутатор/маршрутизатор. Используя сетевые утилиты проверить работоспособность подсети.

Конфигурация сети:

IP – адрес первой подсети **187.140.115.72**

IP – адрес второй подсети **12.156.15.80**

Максимальное количество IP-адресов – 6

Количество используемых хостов - 4

ЗАДАНИЕ № 20

Текст задания:Создать сеть для трех ПК, разделенной на две подсети с использованием двух сетевых интерфейсов на одном из узлов. При монтаже сети необходимо использовать коммутационную панель, сетевую розетку и коммутатор/маршрутизатор. Используя сетевые утилиты проверить работоспособность подсети.

Конфигурация сети:

IP – адрес первой подсети **185.26.53.80**

IP – адрес второй подсети **124.156.18.80**

Максимальное количество IP-адресов – 6

Количество используемых хостов - 4

ЗАДАНИЕ № 21

Текст задания:Создать сеть для трех ПК, разделенной на две подсети с использованием двух сетевых интерфейсов на одном из узлов. При монтаже сети необходимо использовать коммутационную панель, сетевую розетку и коммутатор/маршрутизатор. Используя сетевые утилиты проверить работоспособность подсети.

Конфигурация сети:

IP – адрес первой подсети **12.45.85.144**

IP – адрес второй подсети **112.45.96.8**

Максимальное количество IP-адресов – 6

Количество используемых хостов - 4

ЗАДАНИЕ № 22

Текст задания:Создать сеть для трех ПК, разделенной на две подсети с использованием двух сетевых интерфейсов на одном из узлов. При монтаже сети необходимо использовать коммутационную панель, сетевую розетку и коммутатор/маршрутизатор. Используя сетевые утилиты проверить работоспособность подсети.

Конфигурация сети:

IP – адрес первой подсети **12.145.83.144**

IP – адрес второй подсети **112.145.196.8**

Максимальное количество IP-адресов – 6

Количество используемых хостов - 4

ЗАДАНИЕ № 23

Текст задания:Создать сеть для трех ПК, разделенной на две подсети с использованием двух сетевых интерфейсов на одном из узлов. При монтаже сети необходимо использовать коммутационную панель, сетевую розетку и коммутатор/маршрутизатор. Используя сетевые утилиты проверить работоспособность подсети.

Конфигурация сети:

IP – адрес первой подсети **112.135.103.144**

IP – адрес второй подсети **112.135.0.8**

Максимальное количество IP-адресов – 6

Количество используемых хостов - 4

ЗАДАНИЕ № 24

Текст задания:Создать сеть для трех ПК, разделенной на две подсети с использованием двух сетевых интерфейсов на одном из узлов. При монтаже сети необходимо использовать коммутационную панель, сетевую розетку и коммутатор/маршрутизатор. Используя сетевые утилиты проверить работоспособность подсети.

Конфигурация сети:

IP – адрес первой подсети **26.85.73.8**

IP – адрес второй подсети **135.63.59.8**

Максимальное количество IP-адресов – 6

Количество используемых хостов - 4

ЗАДАНИЕ № 25

Текст задания:Создать сеть для трех ПК, разделенной на две подсети с использованием двух сетевых интерфейсов на одном из узлов. При монтаже сети необходимо использовать коммутационную панель, сетевую розетку и коммутатор/маршрутизатор. Используя сетевые утилиты проверить работоспособность подсети.

Конфигурация сети:

IP – адрес первой подсети **26.85.73.8**

IP – адрес второй подсети **123.61.81.16**

Максимальное количество IP-адресов – 6

Количество используемых хостов - 4

ЗАДАНИЕ № 26

Текст задания:Создать сеть для трех ПК, разделенной на две подсети с использованием двух сетевых интерфейсов на одном из узлов. При монтаже сети необходимо использовать коммутационную панель, сетевую розетку и коммутатор/маршрутизатор. Используя сетевые утилиты проверить работоспособность подсети.

Конфигурация сети:

IP – адрес первой подсети **166.75.173.8**

IP – адрес второй подсети **123.166.81.16**

Максимальное количество IP-адресов – 6

Количество используемых хостов - 4

ЗАДАНИЕ № 27

Текст задания:Создать сеть для трех ПК, разделенной на две подсети с использованием двух сетевых интерфейсов на одном из узлов. При монтаже сети необходимо использовать коммутационную панель, сетевую розетку и коммутатор/маршрутизатор. Используя сетевые утилиты проверить работоспособность подсети.

Конфигурация сети:

IP – адрес первой подсети **126.75.73.8**

IP – адрес второй подсети **153.161.81.16**

Максимальное количество IP-адресов – 6

Количество используемых хостов - 4

ЗАДАНИЕ № 28

Текст задания:Создать сеть для трех ПК, разделенной на две подсети с использованием двух сетевых интерфейсов на одном из узлов. При монтаже сети необходимо использовать коммутационную панель, сетевую розетку и коммутатор/маршрутизатор. Используя сетевые утилиты проверить работоспособность подсети.

Конфигурация сети:

IP – адрес первой подсети **146.75.73.8**

IP – адрес второй подсети **10.121.181.16**

Максимальное количество IP-адресов – 6

Количество используемых хостов – 4

6.Перечень вопросов и практических заданий для проведения экзамена по МДК.01.02 «Организация, принципы построения и функционирования компьютерных сетей»

Вопросы:

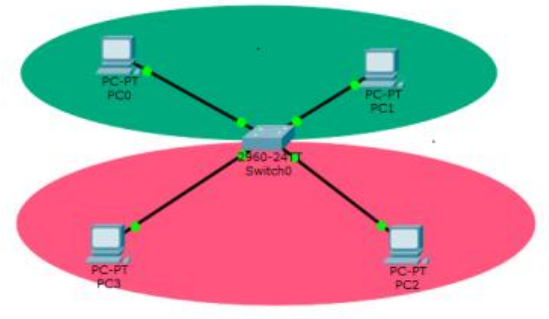
1. Основные компоненты сетей, сетевая среда и сетевые устройства. Перечислите основные компоненты сетей и различные виды сетевых устройств.
2. Планирование структуры сети Методика и начальные этапы проектирования сети.
3. Протокол разрешения адресов (ARP). Сформулируйте назначение протокола ARP и его применение в компьютерных сетях.
4. Протокол разрешения адресов (ARP). Параметр протокола ARP по которому определяется Мак адрес устройства.
5. Схемы адресов. Перечислите существующие протоколы ip адресации их принципиальные различия.
6. Сетевые протоколы и стандарты. Перечислите несколько уровней модели TCP/IP и опишите их функции.
7. Сетевые протоколы и стандарты. Перечислите несколько уровней модели OSI и опишите их функции.
8. Передача данных в сети. Перечислите и опишите функции двух основных протоколов, служащие для передачи данных в сети интернет.
9. Протоколы физического уровня. Перечислите протоколы физического уровня и их функции.
10. Протоколы канального уровня. Опишите назначение протокола канального уровня Point-to-Point Protocol over Ethernet (PPPoE)
11. Управление доступом к среде. Уровень модели OSI к которому можно соотнести подуровень «управление доступом к среде».
12. Управление доступом к среде. Опишите назначение под уровня модели OSI управление доступом к среде.
13. Протокол Ethernet .Опишите назначение технологии Ethernet, на каком уровне модели OSI работает технология Ethernet.
14. Коммутаторы локальных сетей. Опишите назначение коммутаторов локальных сетей и их отличие от маршрутизаторов.
15. Протокол разрешения адресов (ARP). Опишите схему работы протокола ARP.
16. Протоколы сетевого уровня. Опишите назначение и функции сетевого протокола RIP.
17. Маршрутизация. Перечислите существующие виды маршрутизации и способы их применения.
18. Маршрутизаторы.Опишите назначение маршрутизаторов и их отличие от коммутаторов.

19. Настройка маршрутизатора Cisco. Опишите принцип настройки маршрутизатора Cisco, приведите пример настройки ip адресации и настройки vlan.
20. IP – адресация. Сформулируйте определение, IP-адрес это…
21. Разделение IP-сетей на подсети. Опишите назначение маски подсети и ее свойства. Запишите маску подсети 255.255.255.0 в двоичной форме.
22. Протоколы транспортного уровня. Опишите назначение протоколов транспортного уровня TCP, UDP.
23. Протоколы уровня приложений. Опишите назначение и функции протокола уровня приложений DNS.
24. Проектирование небольшой сети. Перечислите приложения для проектирования локальных сетей.
25. Поиск и устранение неполадок. Сформулируйте методы средства поиска и устранения неполадок в сети.
26. Cisco IOS. Базовая настройка устройств. Опишите базовую настройку маршрутизатора под управлением Cisco IOS, настраиваемые параметры и необходимые команды.
27. Концепция маршрутизации. Опишите концепцию динамической маршрутизации.
28. Конфигурация маршрутизатора. Сформулируйте пример базовой настройки маршрутизатора, а так же основные настройки.
29. Статическая маршрутизация. Какую маршрутизацию называют статической?
30. Настройка статических маршрутов. Опишите методы настройки статических маршрутов, а также команды применяемые для настройки маршрутов.
31. Динамическая маршрутизация. Опишите методы настройки динамической маршрутизации, а также команды применяемые для настройки маршрутизации. Перечислите протоколы динамической маршрутизации и их функции.
32. Сегментация IP-сетей. Перечислите протоколы которые используются для сегментирования IP-сетей и опишите их роли и функции.
33. Коммутируемые сети. Опишите вид коммутации сети на уровне ядра. Опишите вид коммутации сети на уровне распределения.
34. Конфигурация коммутатора. Сформулируйте пример базовой настройки коммутатора, а так же его основные настройки.
35. Сети VLAN. Опишите назначение сетей VLAN в крупных сетях.
37. Маршрутизация между сетями VLAN. Как включить маршрутизацию между сетями VLAN на коммутаторе.
38. Списки контроля доступа. Опишите назначение списков контроля доступа, а также их преимущества и недостатки.
39. Настройка стандартных ACL – списков. Опишите методы настройки стандартных ACL – списков на маршрутизаторе.
40. DHCPv4. Опишите методологию настройки DHCPv4 на роутере.
41. DHCPv6. Опишите методологию настройки DHCPv6 на роутере.

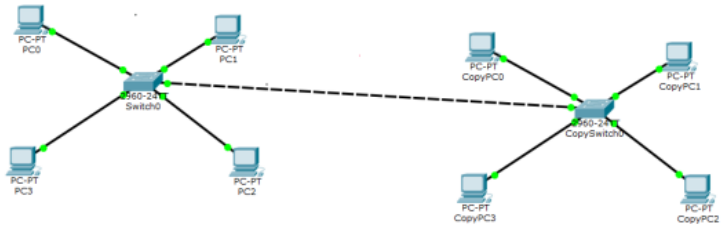
42. Преобразование NAT для IPv4. Опишите назначение технологии NAT, ее принцип действия, а также преимущества и недостатки данной технологии.
43. Настройка NAT. Опишите принцип настройки технологии NAT на маршрутизаторе.
44. Различные типы сети Ethernet. Перечислите существующие типы сети Ethernet и опишите характеристики этих сетей.
45. Беспроводная сеть. Перечислите существующие технологии беспроводных сетей и их характеристики.
46. Установка и подключение сетевого оборудования. Установка и подключение сетевого оборудования.
47. Настройка сети в Windows Server. Опишите назначение компонента Active Directory в Windows Server.
48. RAID-технологии. Опишите существующие RAID-технологии и принципы их работы.

Практические задания:

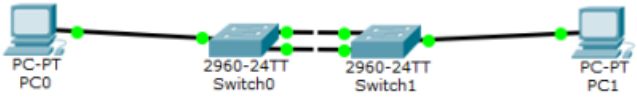
1. Выполните подключение к сетевому оборудованию в программе Cisco Packet Tracer. Добавьте в схему коммутатор Cisco 2960 и один компьютер, после настройте сеть. Настройте коммутатор с помощью консольного кабеля RS 232-Console.
   Выполните первичную настройку коммутатора, установите пароль на enable, зашифруйте пароль, настройте транспортный протокол Telnet, подключитесь к Telnet по консоли.
2. Выполните настройку технологии VIRTUAL LOCAL AREA NETWORK в программе Cisco Packet Tracer. Сконфигурируйте схему подставленную на рисунке, в данном случае необходимо выбрать коммутатор Cisco 2960, изолируйте две подсети с помощью vlan, настройте IP адресацию.



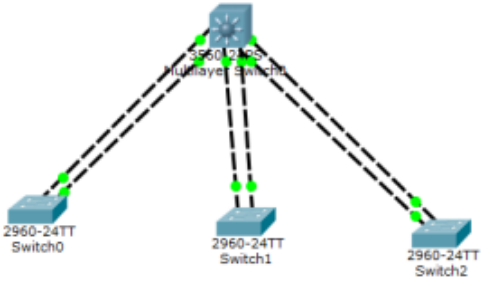
1. Выполните настройку технологии Virtual Local Area Network в программе Cisco Packet Tracer. Сконфигурируйте схему подставленную на рисунке, в данном случае необходимо выбрать коммутатор Cisco 2960, изолируйте две подсети с помощью vlan, настройте IP адресацию.



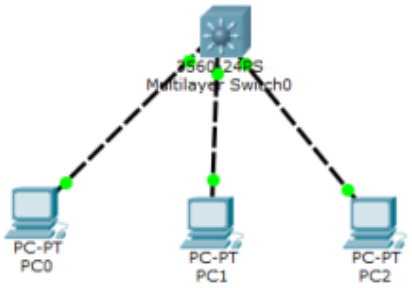
2. Выполните настройку агрегации каналов etherchannel в программе Cisco Packet Tracer. Сконфигурируйте схему подставленную на рисунке, добавьте 2 коммутатора и 2 компьютера, настройте IP адресацию, соедините коммутаторы в агрегированный канал и выполите настройку. Для проверки отказоустойчивости от отключите один из портов.



3. Выполните настройку динамической агрегации каналов etherchannel в программе Cisco Packet Tracer. Сконфигурируйте схему подставленную на рисунке, добавьте 3 коммутатора l-2 уровня и 1 коммутатор L-3 уровня, соедините коммутаторы в агрегированный канал и выполите настройку. Для проверки отказоустойчивости от отключите один из портов.

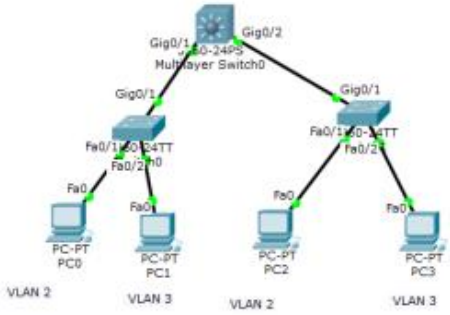


4. Выполните настройку коммутатора L3 уровня в программе Cisco Packet Tracer. Создать локальную сеть, состоящую из нескольких подсетей на основе коммутатора 3 уровня Cisco 3650, схема представлена на рисунке. Изолируйте сети с помощью технологии Vlan, для каждого компьютера создайте свою изолированную сеть, настройте IP адресацию. Выполите настройку по маршрутизации трафика между Vlan.

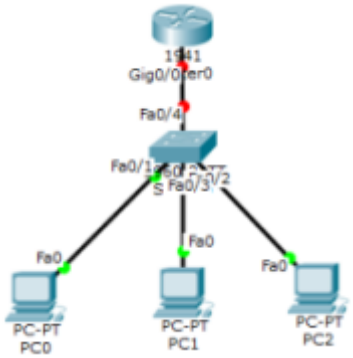


5. Выполните настройку трёх коммутаторов L3 и L2 уровня в программе Cisco Packet Tracer. Создать локальную сеть, состоящую из нескольких

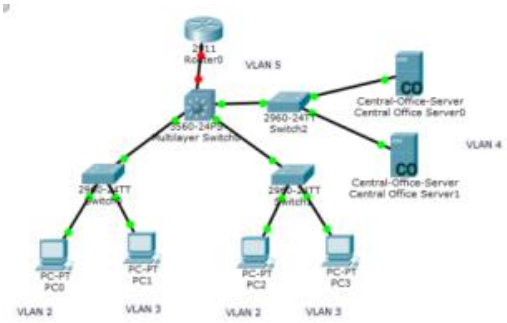
подсетей на основе коммутатора 3 уровня Cisco 3650, схема представлена на рисунке. Изолируйте сети с помощью технологии Vlan, для каждого компьютера создайте свою изолированную сеть, настройте IP адресацию. Выполите настройку по маршрутизации трафика между Vlan. Для настройке Vlan используйте команды access и trunk.



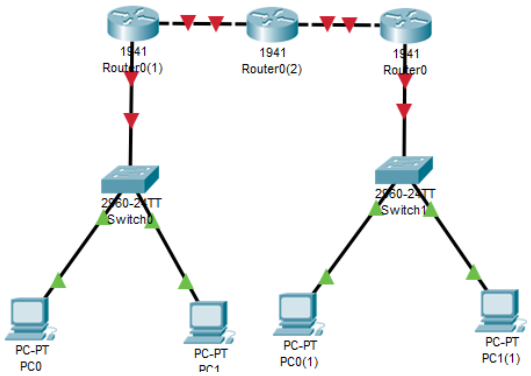
6. Выполните настройку маршрутизатора в программе Cisco Packet Tracer. Постройте маршрутизируемую IP-сеть, сконфигурируйте 3 компьютера, один коммутатор Cisco 2960, маршрутизатор Cisco 1941, для каждого компьютера создайте свою изолированную сеть Vlan, на маршрутизаторе создайте виртуальные саб интерфейсы с привязкой IP адресов, настройте IP адресацию на компьютерах.



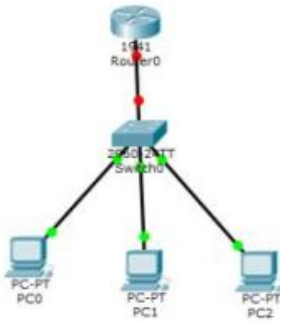
7. Выполните настройку маршрутизатора и коммутатора в программе Cisco Packet Tracer. Схема приведена на рисунке. Постройте маршрутизируемую IP-сеть, сконфигурируйте 4 компьютера, 2 сервера, 3 коммутатора Cisco 2960, маршрутизатор Cisco 1941, для каждого компьютера создайте свою изолированную сеть Vlan, на маршрутизаторе создайте виртуальные интерфейсы Vlan с привязкой IP адресов, настройте IP адресацию на компьютерах.



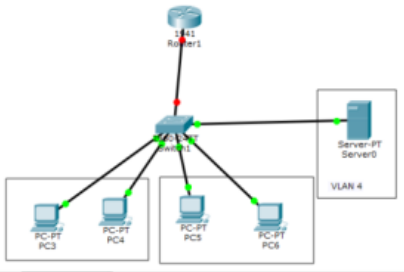
8. Выполните настройку статической маршрутизации в программе Cisco Packet Tracer. Схема приведена на рисунке. Постройте маршрутизируемую IP-сеть, сконфигурируйте 4 компьютера, 2 коммутатора Cisco 2960, 3 маршрутизатора Cisco 1941, для каждого компьютера создайте свою изолированную сеть Vlan, на маршрутизаторе создайте виртуальные интерфейсы Vlan с привязкой IP адресов, настройте IP адресацию на компьютерах. Пропишите статические маршруты на роутерах.



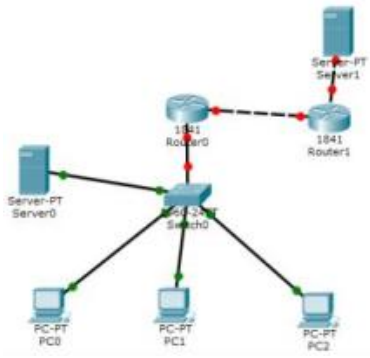
9. Выполните настройку DHCP протокола на роутере в программе Cisco Packet Tracer. Схема приведена на рисунке. Постройте маршрутизируемую IP-сеть, сконфигурируйте 3 компьютера, 1 коммутатор Cisco 2960, 1 маршрутизатор Cisco 1941, выполите настройку DHCP на роутере с пулом адресов 192,168,1,1-192,168,1,100.
Включите протокол DHCP на компьютерах.



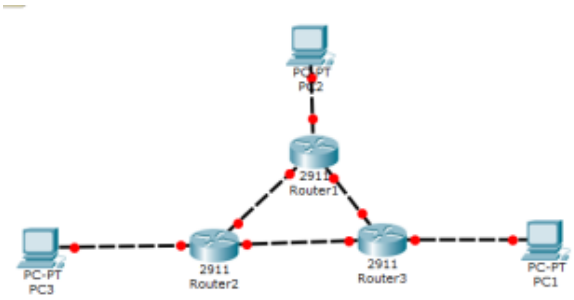
10. Выполните настройку DHCP протокола на сервере в программе Cisco Packet Tracer. Схема приведена на рисунке. Постройте маршрутизируемую IP-сеть, сконфигурируйте 4 компьютера, 1 сервер, 1 коммутатор Cisco 2960, 1 маршрутизатор Cisco 1941, изолируйте все сети с помощью Vlan, на роутере создайте виртуальные саб интерфейсы с привязанными IP адресами, выполите настройку DHCP на сервере.



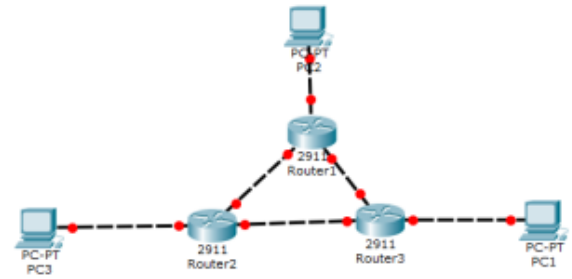
11. Выполните настройку протокола Network Address Tranclation (NAT) в программе Cisco Packet Tracer. Схема приведена на рисунке. Постройте маршрутизируемую IP-сеть, сконфигурируйте 3 компьютера, 1 сервер, 1 коммутатор Cisco 2960, 2 маршрутизатора Cisco 1941, изолируйте все сети с помощью Vlan, на роутере создайте виртуальные саб интерфейсы с привязанными IP адресами, назначьте белые IP адреса на роутере провайдера и на внешнем интерфейсе вашего роутера, так же необходимо прописать статические маршруты. Выполите настройку протокола NAT на роутере.



12. Выполните настройку протокола динамической маршрутизации OSPF в программе Cisco Packet Tracer. Схема приведена на рисунке. Постройте маршрутизируемую IP-сеть, сконфигурируйте 3 компьютера, 3 маршрутизатора Cisco 2911, настройте ip адресацию, настройте loopback, далее настройте протокол OSPF.

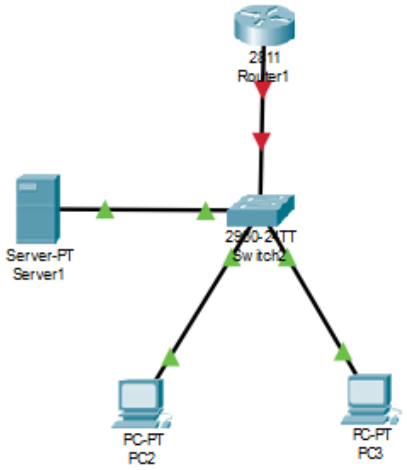


13. Выполните настройку протокола динамической маршрутизации EIGRP в программе Cisco Packet Tracer. Схема приведена на рисунке. Постройте маршрутизируемую IP-сеть, сконфигурируйте 3 компьютера, 3 маршрутизатора Cisco 2911, настройте ip адресацию, настройте loopback, далее настройте протокол EIGRP.

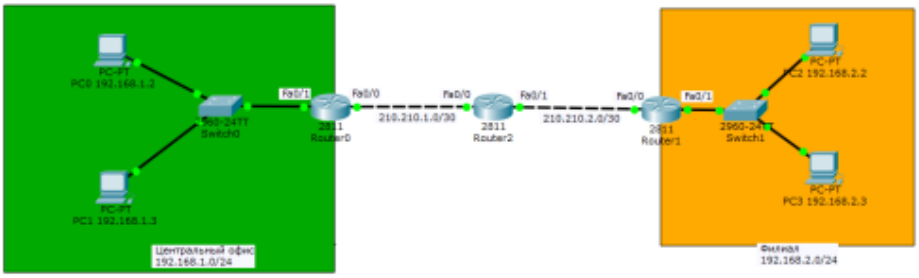


14. Выполните настройку списков контроля доступа (access list) в программе Cisco Packet Tracer. Схема приведена на рисунке. Постройте

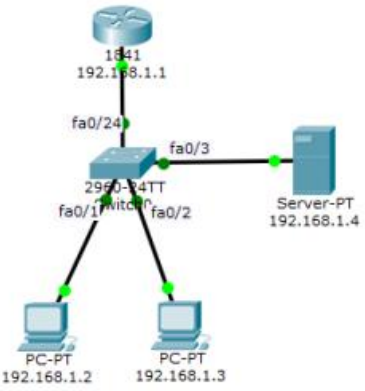
маршрутизируемую IP-сеть, сконфигурируйте 2 компьютера, 1 сервер, 1 коммутатор, 1 маршрутизатор. Изолируйте все компьютеры с помощью Vlan, настройте виртуальные интерфейсы на роутере с IP адресами. Настройте Access листы таким образом, доступ для сервера должен иметь только компьютер бухгалтеров слева.



15. Выполните настройку Virtual Private Network (VPN) в программе Cisco Packet Tracer. Схема приведена на рисунке. Постройте маршрутизируемую IP-сеть, сконфигурируйте 4 компьютера, 2 коммутатора, 3 маршрутизатора. Настройте IP адресацию, настройте белую IP адресацию во внешней сети, настройте статические маршруты, настройте NAT, настройте протокол VPN.

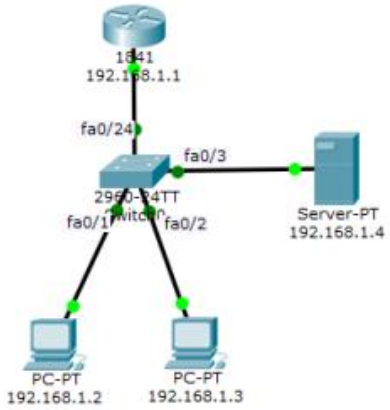


16. Выполните настройку протоколов syslog и ntp в программе Cisco Packet Tracer. Схема приведена на рисунке. Постройте IP-сеть, сконфигурируйте 2 компьютера, 1 коммутатор, 1 маршрутизатор. Настройте IP адресацию и протоколы SYSLOG, NTP.

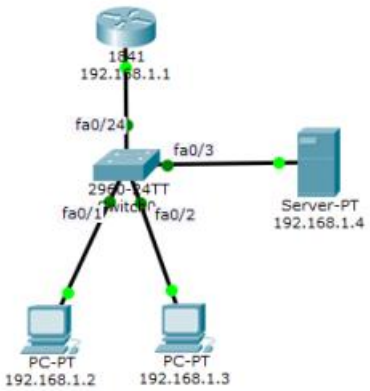


17. Выполните настройку протокола AAA на сервере в программе Cisco Packet Tracer. Схема приведена на рисунке. Постройте IP-сеть, сконфигурируйте

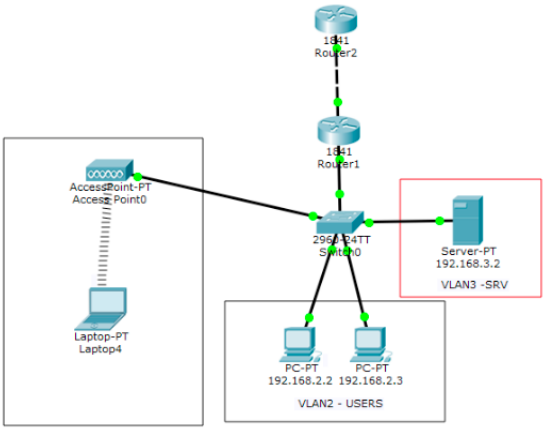
2 компьютера, 1 сервер, 1 коммутатор, 1 маршрутизатор. Настройте IP адресацию и протокол AAA на сервере.



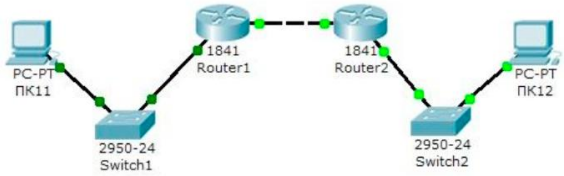
18. Выполните настройку протокола Trivial File Transfer Protocol (TFTP) на сервере в программе Cisco Packet Tracer. Схема приведена на рисунке. Постройте IP-сеть, сконфигурируйте 2 компьютера, 1 сервер, 1 коммутатор, 1 маршрутизатор. Настройте IP адресацию и протокол TFTP на сервере.



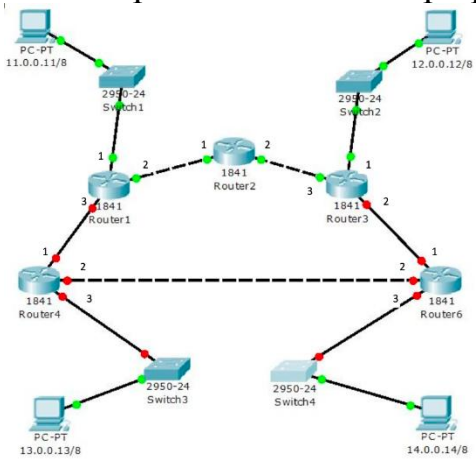
19. Выполните настройку протокола WIFI как точку доступа в программе Cisco Packet Tracer. Схема приведена на рисунке. Постройте IP-сеть, сконфигурируйте 2 компьютера, 1 ноутбук с WIFI, 1 точка доступа, 2 маршрутизатора. Настройте IP адресацию изолируйте все компьютеры с помощью Vlan, настройте виртуальные саб интрефейсы с адресами и WIFI.



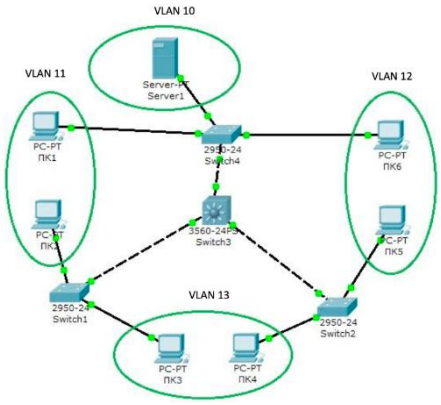
20. Выполните настройку протокола RIP в программе Cisco Packet Tracer. Схема приведена на рисунке. Постройте IP-сеть, сконфигурируйте 2 компьютера, 2 коммутатора, 2 маршрутизатора. Настройте IP адресацию и протокол RIP на маршрутизаторах.



21. Выполните настройку протокола RIP в корпоративной сети в программе Cisco Packet Tracer. Схема приведена на рисунке. Постройте IP-сеть, сконфигурируйте 4 компьютера, 4 коммутатора, 6 маршрутизаторов. Настройте IP адресацию и протокол RIP на маршрутизаторах.



22. Выполните настройку протокола Vlan в корпоративной сети в программе Cisco Packet Tracer. Схема приведена на рисунке. Постройте IP-сеть, сконфигурируйте 6 компьютеров, 3 коммутатора L2, 1 коммутатор L3. Настройте IP адресацию, каждый компьютер изолируйте сетью Vlan.



7.Перечень вопросов и практических заданий для проведения экзамена по МДК.01.03 «Безопасность компьютерных сетей»

1.Основы информационной безопасности

2. Фундаментальные принципы безопасной сети. Современные угрозы сетевой безопасности

3. Вирусы, черви и троянские кони

4. Методы атак.

5. Безопасность сетевых устройств OSI. Безопасный доступ к устройствам.

6. Назначение административных ролей. Мониторинг и управление устройствами. Использование функция автоматизированной настройки безопасности.

7. Авторизация, аутентификация и учет доступа (AAA).

8. Свойства AAA. Локальная AAA аутентификация. Server-based AAA

9. Реализация технологий брандмауэра. ACL. Технология брандмауэра.

10. Контекстный контроль доступа (CBAC). Политики брандмауэра, основанные на зонах

11. Реализация технологий предотвращения вторжения**.** IPS технологии.

12. IPS сигнатуры. Реализация IPS. Проверка и мониторинг IPS

13. Безопасность локальной сети. Обеспечение безопасности пользовательских компьютеров. Соображения по безопасности второго уровня (Layer-2)**.**

14. Конфигурация безопасности второго уровня. Безопасность беспроводных сетей, VoIP и SAN

15. Реализация технологий VPN. VPN. GRE VPN. Компоненты и функционирование IPSec VPN.

16. Реализация Site-to-siteIPSec VPN с использованием CLI. Реализация Site-to-siteIPSec VPN с использованием CCP. Реализация Remote-access VPN

17. Криптографические системы. Криптографические сервисы. Базовая целостность и аутентичность. Конфиденциальность. Криптография открытых ключей.

18. Управление безопасной сетью. Принципы безопасности сетевого дизайна. Безопасная архитектура.

19. Управление процессами и безопасность. Тестирование сети на уязвимости. Непрерывность бизнеса, планирование восстановления аварийных ситуаций.

20. Жизненный цикл сети и планирование. Разработка регламентов компании и политик безопасности

21. Cisco ASA. Введение в Адаптивное устройство безопасности ASA

22. Конфигурация файрвола на базе ASA с использованием графического интерфейса ASDM

23. Конфигурация VPN на базе ASA с использованием графического интерфейса ASDM

24. Использование Microsoft System Center для мониторинга информационной инфраструктуры и реагирования на инциденты безопасности

Применение криптопровайдера КриптоПро CSP в стандартных приложен

25. Использование системы Zabbix для мониторинга информационной инфраструктуры и реагирования на инциденты безопасности
26. Классы атак в сетях на основе TCP/IP. Атаки на сетевом и транспортном уровне: Ping, flood, IP spoofing, пассивное сканирование. MITM атаки. Способы предотвращение атак
27. DOS и DDOS атаки. Атаки отказа в обслуживании DDOS. Виды DDOS атак. Предотвращение DDOS атак.
28. Обеспечение безопасности канального уровня. MITM атаки канального уровня: ARP-spoofing, DHCP-spoofing, VLAN-hopping
29. MAC-flooding, атаки на протокол STP. Способы предотвращения атак на канальном уровне
30. Протоколы SSL/TLS. Основные понятия протоколов SSL и TLS. Устройство, принцип работы протокола SSL Цифровые сертификаты. Аутентификация и обмен ключами

Практические задания:

1. Необходимо сохранить резервную копию документов не на физическом носителе. Создайте резервную копию 2 документов из папки в «облачном пространстве» на «яндекс диске».

2. Необходимо сохранить резервную копию документов не на физическом носителе. Создайте резервную копию 2 документов из папки в «облачном пространстве» на «Mail.ru».

3. Используя средства криптографической защиты зашифровать системой шифрования Цезаря свою фамилию, имя, отчество.

4. Используя средства криптографической защиты зашифровать алгоритмом двойных перестановок свою фамилию, имя, отчество.

5. Используя средства криптографической защиты используя шифр перестановки зашифровать название своей специальности и название изучаемого модуля.

6. Используя средства криптографической защиты зашифровать системой шифрования Цезаря название своей специальности и название изучаемого модуля.

7. Используя средства криптографической защиты зашифровать алгоритмом двойных перестановок название своей специальности и название изучаемого модуля.

8. Используя средства криптографической защиты используя шифр перестановки зашифровать название своей специальности и название изучаемого модуля.

Филиал федерального государственного бюджетного образовательного учреждения высшего образования «Петербургский государственный университет путей сообщения Императора Александра I» в г.Рязани

Рассмотрено ЦК по специальности 09.02.06 Сетевое и системное администрирование Председатель_____ « ___»_____20____ г	Экзаменационный билет № 1 специальность 09.02.06 Сетевое и системное администрирование группа СС 411 Экзамен по МДК. 01.01 Компьютерные сети 20____- 20_____ учебный год	Утверждаю: Зам. директора по УМР _____ «_____» _____20____ г

1.

2.

Преподаватель _____

8. КОНТРОЛЬНО-ОЦЕНОЧНЫЕ СРЕДСТВА ЭКЗАМЕНА (КВАЛИФИКАЦИОННОГО) по ПМ.01 Настройка сетевой инфраструктуры

Экзамен (квалификационный) проводится непосредственно после завершения освоения программы профессионального модуля, т. е после изучения междисциплинарных курсов и прохождения учебной и (или) производственной практики в составе профессионального модуля. Экзамен (квалификационный) представляет собой форму независимой оценки результатов обучения с участием работодателей.

1. **Назначение**

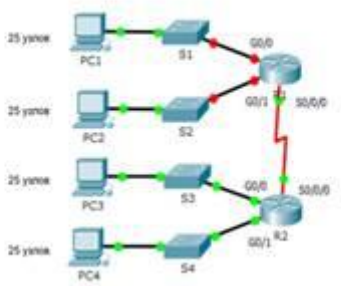
Экзамен (квалификационный) является формой промежуточной аттестации по профессиональному модулю ПМ. 01 Настройка сетевой инфраструктуры, проводится с целью проверки готовности обучающегося к выполнению вида деятельности: Настройка сетевой инфраструктуры. Спецификацией устанавливается состав оценочных средств, используемых при организации экзамена (квалификационного) по ПМ. 01 Настройка сетевой инфраструктуры.

2. Время аттестации: на проведение аттестации отводится 4 часа, на подготовку – 30 минут .

1. **Выполните базовую настройку устройств S1, R1, R2**

а. Подключитесь с помощью консоли и активируйте привилегированный

Топология



режим EXEC.

б. Отключите поиск DNS, чтобы предотвратить попытки маршрутизатора неверно преобразовывать введенные команды таким образом, как будто они являются именами узлов.

в. Назначьте class в качестве зашифрованного пароля привилегированного режима EXEC.

г. Назначьте cisco в качестве пароля консоли и включите режим входа в систему по паролю.

д. Назначьте cisco в качестве пароля VTY и включите вход по паролю.

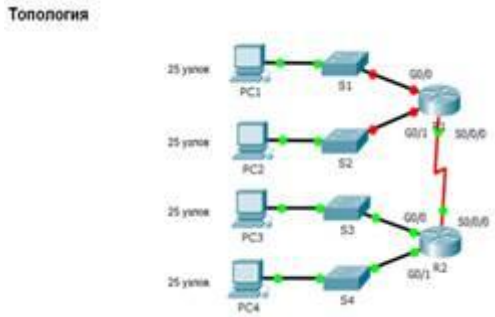
е. Зашифруйте открытые пароли.

ж. Создайте баннер, который предупреждает о запрете несанкционированного доступа (Используйте слово Warninng).

з. Сохраните текущую конфигурацию в файл загрузочной конфигурации

2. **Настроите доступ по протоколу SSH на S1 и R2**.

Измените имя домена на ccna.com



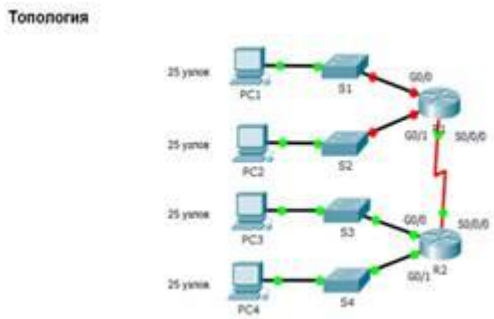
Создайте ключ RSA длиной 1024 бит.

Настройте линии VTY для доступа по протоколу SSH.

Используйте локальные профили пользователей для аутентификации.

Создайте пользователя admin с 15-м уровнем привилегированного доступа и зашифрованным паролем Adminp@ss.

3. Разбейте сеть на подсети



Разбейте сеть 192.168.0.0/24 на нужное количество подсетей:

a. Назначьте подсеть 0 локальной сети (LAN1), подключенной к интерфейсу GigabitEthernet 0/0 маршрутизатора R1.

b. Назначьте подсеть 1 локальной сети (LAN2), подключенной к интерфейсу GigabitEthernet 0/1 маршрутизатора R1.

e. Назначьте подсеть 4 каналу WAN между маршрутизаторами R1 и R2.

Завершите документирование схемы адресации в соответствии со следующими рекомендациями.

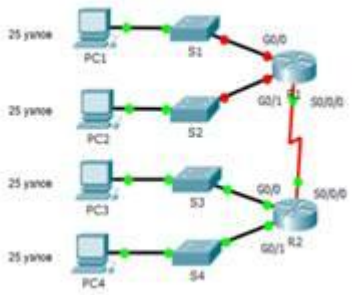
Назначьте первые используемые IP-адреса маршрутизатору R1 для двух каналов локальной сети (LAN) и одного канала сети WAN.

Второй из используемых IP-адресов назначьте коммутаторам.

Последний из используемых IP-адресов назначьте узлам.

4. Выполните базовую настройку устройств S1, R1, R2

Топология



а. Подключитесь с помощью консоли и активируйте привилегированный режим EXEC.

б. Отключите поиск DNS, чтобы предотвратить попытки маршрутизатора неверно преобразовывать введенные команды таким образом, как будто они являются именами узлов.

в. Назначьте class в качестве зашифрованного пароля привилегированного режима EXEC.

г. Назначьте cisco в качестве пароля консоли и включите режим входа в систему по паролю.

д. Назначьте cisco в качестве пароля VTY и включите вход по паролю.

е. Зашифруйте открытые пароли.

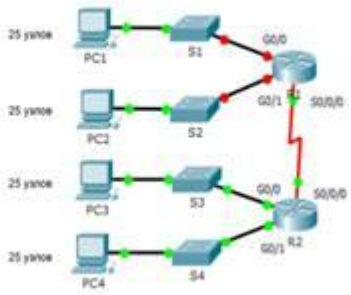
ж. Создайте баннер, который предупреждает о запрете несанкционированного доступа (Используйте слово Warninng).

з. Сохраните текущую конфигурацию в файл загрузочной конфигурации

5. Настроите доступ по протоколу SSH на S1 и R2.

Измените имя домена на ccna.com

Топология



Создайте ключ RSA длиной 1024 бит.

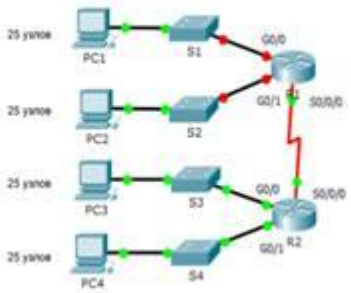
Настройте линии VTY для доступа по протоколу SSH.

Используйте локальные профили пользователей для аутентификации.

Создайте пользователя admin1 с 15-м уровнем привилегированного доступа и зашифрованным паролем Admin1p@ss.

6. Разбейте сеть на подсети

Топология



Разбейте сеть 192.168.10.0/24 на нужное количество подсетей:

a. Назначьте подсеть 0 локальной сети (LAN1), подключенной к интерфейсу GigabitEthernet 0/0 маршрутизатора R1.

b. Назначьте подсеть 1 локальной сети (LAN2), подключенной к интерфейсу GigabitEthernet 0/1 маршрутизатора R1.

e. Назначьте подсеть 4 каналу WAN между маршрутизаторами R1 и R2.

Завершите документирование схемы адресации в соответствии со следующими рекомендациями.

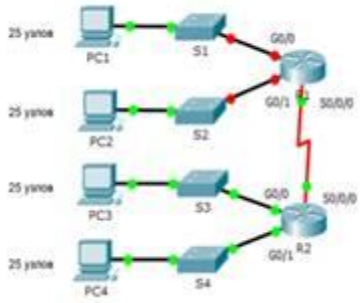
Назначьте первые используемые IP-адреса маршрутизатору R1 для двух каналов локальной сети (LAN) и одного канала сети WAN.

Второй из используемых IP-адресов назначьте коммутаторам.

Последний из используемых IP-адресов назначьте узлам.

7. Выполните базовую настройку устройств S1, R1, R2

Топология



a. Подключитесь с помощью консоли и активируйте привилегированный режим EXEC.

б. Отключите поиск DNS, чтобы предотвратить попытки маршрутизатора неверно преобразовывать введенные команды таким образом, как будто они являются именами узлов.

в. Назначьте class в качестве зашифрованного пароля привилегированного режима EXEC.

г. Назначьте cisco в качестве пароля консоли и включите режим входа в систему по паролю.

д. Назначьте cisco в качестве пароля VTY и включите вход по паролю.

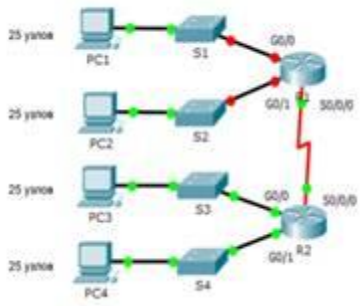
е. Зашифруйте открытые пароли.

ж. Создайте баннер, который предупреждает о запрете несанкционированного доступа(Используйте слово Warninng).

з. Сохраните текущую конфигурацию в файл загрузочной конфигурации

8. Настроите доступ по протоколу SSH на S1 и R2.

Топология



Измените имя домена на ccna.com

Создайте ключ RSA длиной 1024 бит.

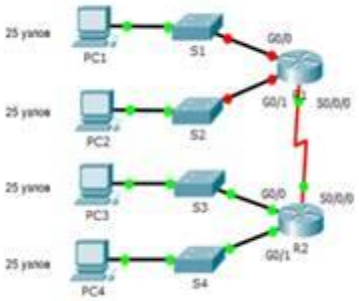
Настройте линии VTY для доступа по протоколу SSH.

Используйте локальные профили пользователей для аутентификации.

Создайте пользователя admin2 с 15-м уровнем привилегированного доступа и зашифрованным паролем Admin2p@ss.

9. Разбейте сеть на подсети

Топология



Разбейте сеть 192.168.1.0/24 на нужное количество подсетей:

a. Назначьте подсеть 0 локальной сети (LAN 1), подключенной к интерфейсу GigabitEthernet 0/0 маршрутизатора R1.

b. Назначьте подсеть 1 локальной сети (LAN2), подключенной к интерфейсу GigabitEthernet 0/1 маршрутизатора R1.

e. Назначьте подсеть 4 каналу WAN между маршрутизаторами R1 и R2.

Завершите документирование схемы адресации в соответствии со следующими рекомендациями.

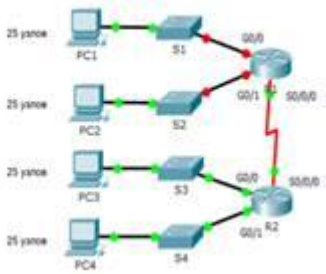
Назначьте первые используемые IP-адреса маршрутизатору R1 для двух каналов локальной сети (LAN) и одного канала сети WAN.

Второй из используемых IP-адресов назначьте коммутаторам.

Последний из используемых IP-адресов назначьте узлам.

10.Выполните базовую настройку устройств S1, R1, R2

Топология



а. Подключитесь с помощью консоли и активируйте привилегированный режим EXEC.

б. Отключите поиск DNS, чтобы предотвратить попытки маршрутизатора неверно преобразовывать введенные команды таким образом, как будто они являются именами узлов.

в. Назначьте class в качестве зашифрованного пароля привилегированного режима EXEC.

г. Назначьте cisco в качестве пароля консоли и включите режим входа в систему по паролю.

д. Назначьте cisco в качестве пароля VTY и включите вход по паролю.

е. Зашифруйте открытые пароли.

ж. Создайте баннер, который предупреждает о запрете несанкционированного доступа(Используйте слово Warninng).

з. Сохраните текущую конфигурацию в файл загрузочной конфигурации

11.Настроите доступ по протоколу SSH на S1 и R2.

Измените имя домена на ccna.com

Создайте ключ RSA длиной 1024 бит.

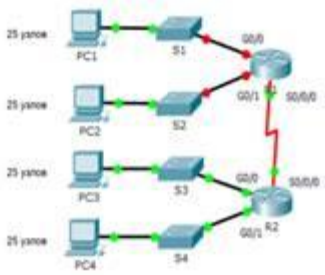
Настройте линии VTY для доступа по протоколу SSH.

Используйте локальные профили пользователей для аутентификации.

Создайте пользователя admin3 с 15-м уровнем привилегированного доступа и зашифрованным паролем Admin3p@ss.

12.Разбейте сеть на подсети

Топология



Разбейте сеть 192.168.3.0/24 на нужное количество подсетей:

a. Назначьте подсеть 0 локальной сети (LAN1), подключенной к интерфейсу GigabitEthernet 0/0 маршрутизатора R1.

b. Назначьте подсеть 1 локальной сети (LAN2), подключенной к интерфейсу GigabitEthernet 0/1 маршрутизатора R1.

е. Назначьте подсеть 4 каналу WAN между маршрутизаторами R1 и R2.

Завершите документирование схемы адресации в соответствии со следующими рекомендациями.

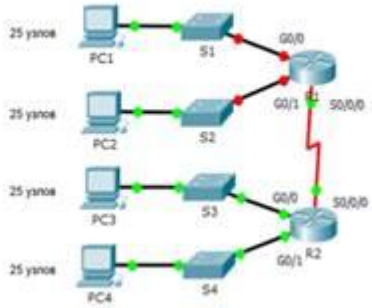
Назначьте первые используемые IP-адреса маршрутизатору R1 для двух каналов локальной сети (LAN) и одного канала сети WAN.

Второй из используемых IP-адресов назначьте коммутаторам.

Последний из используемых IP-адресов назначьте узлам.

13.Выполните базовую настройку устройств S1, R1, R2

Топология



а. Подключитесь с помощью консоли и активируйте привилегированный режим EXEC.

б. Отключите поиск DNS, чтобы предотвратить попытки маршрутизатора неверно преобразовывать введенные команды таким образом, как будто они являются именами узлов.

в. Назначьте class в качестве зашифрованного пароля привилегированного режима EXEC.

г. Назначьте cisco в качестве пароля консоли и включите режим входа в систему по паролю.

д. Назначьте cisco в качестве пароля VTY и включите вход по паролю.

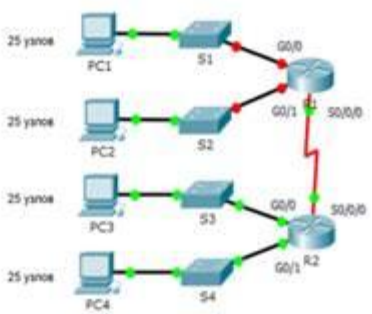
е. Зашифруйте открытые пароли.

ж. Создайте баннер, который предупреждает о запрете несанкционированного доступа(Используйте слово Warninng).

з. Сохраните текущую конфигурацию в файл загрузочной конфигурации

14.Настройте доступ по протоколу SSH на S1 и R2.

Топология



Измените имя домена на ccna.com

Создайте ключ RSA длиной 1024 бит.

Настройте линии VTY для доступа по протоколу SSH.

Используйте локальные профили пользователей для аутентификации.

Создайте пользователя admin4 с 15-м уровнем привилегированного доступа и зашифрованным паролем Admin4p@ss.

3. Разбейте сеть на подсети

Разбейте сеть 192.168.0.0/24 на нужное количество подсетей:

a. Назначьте подсеть 0 локальной сети (LAN 1), подключенной к интерфейсу GigabitEthernet 0/0 маршрутизатора R1.

b. Назначьте подсеть 1 локальной сети (LAN2), подключенной к интерфейсу GigabitEthernet 0/1 маршрутизатора R1.

e. Назначьте подсеть 3 каналу WAN между маршрутизаторами R1 и R2.

Завершите документирование схемы адресации в соответствии со следующими рекомендациями.

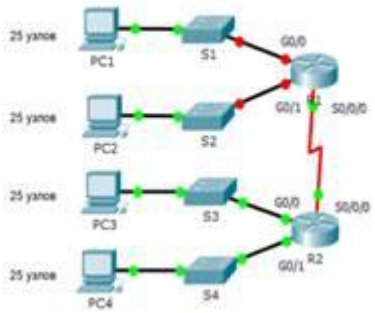
Назначьте первые используемые IP-адреса маршрутизатору R1 для двух каналов локальной сети (LAN) и одного канала сети WAN.

Второй из используемых IP-адресов назначьте коммутаторам.

Последний из используемых IP-адресов назначьте узлам.

15.Выполните базовую настройку устройств S1, R1, R2

Топология



a. Подключитесь с помощью консоли и активируйте привилегированный режим EXEC.

б. Отключите поиск DNS, чтобы предотвратить попытки маршрутизатора неверно преобразовывать введенные команды таким образом, как будто они являются именами узлов.

в. Назначьте class в качестве зашифрованного пароля привилегированного режима EXEC.

г. Назначьте cisco в качестве пароля консоли и включите режим входа в систему по паролю.

д. Назначьте cisco в качестве пароля VTY и включите вход по паролю.

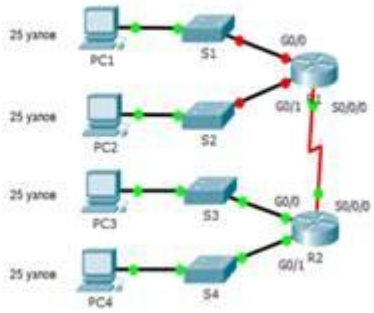
е. Зашифруйте открытые пароли.

ж. Создайте баннер, который предупреждает о запрете несанкционированного доступа(Используйте слово Warninng).

з. Сохраните текущую конфигурацию в файл загрузочной конфигурации

16.Настроите доступ по протоколу SSH на S1 и R2.

Топология



Измените имя домена на ccna.com

Создайте ключ RSA длиной 1024 бит.

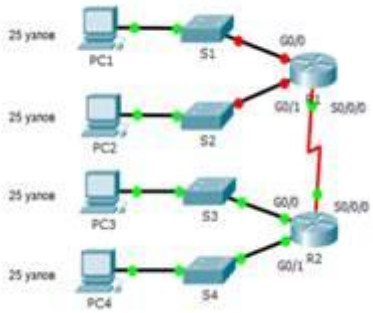
Настройте линии VTY для доступа по протоколу SSH.

Используйте локальные профили пользователей для аутентификации.

Создайте пользователя admin5 с 15-м уровнем привилегированного доступа и зашифрованным паролем Admin5p@ss.

17.Разбейте сеть на подсети

Топология



Разбейте сеть 192.168.12.0/24 на нужное количество подсетей:

a. Назначьте подсеть 0 локальной сети (LAN 1), подключенной к интерфейсу GigabitEthernet 0/0 маршрутизатора R1.

b. Назначьте подсеть 1 локальной сети (LAN2), подключенной к интерфейсу GigabitEthernet 0/1 маршрутизатора R1.

e. Назначьте подсеть 3 каналу WAN между маршрутизаторами R1 и R2.

Завершите документирование схемы адресации в соответствии со следующими рекомендациями.

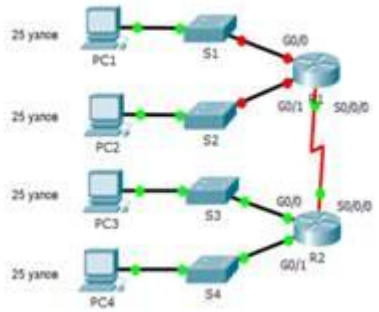
Назначьте первые используемые IP-адреса маршрутизатору R1 для двух каналов локальной сети (LAN) и одного канала сети WAN.

Второй из используемых IP-адресов назначьте коммутаторам.

Последний из используемых IP-адресов назначьте узлам.

18.Выполните базовую настройку устройств S1, R1, R2

Топология



а. Подключитесь с помощью консоли и активируйте привилегированный режим EXEC.

б. Отключите поиск DNS, чтобы предотвратить попытки маршрутизатора неверно преобразовывать введенные команды таким образом, как будто они являются именами узлов.

в. Назначьте class в качестве зашифрованного пароля привилегированного режима EXEC.

г. Назначьте cisco в качестве пароля консоли и включите режим входа в систему по паролю.

д. Назначьте cisco в качестве пароля VTY и включите вход по паролю.

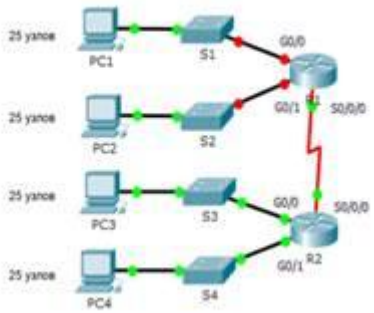
е. Зашифруйте открытые пароли.

ж. Создайте баннер, который предупреждает о запрете несанкционированного доступа(Используйте слово Warninng).

з. Сохраните текущую конфигурацию в файл загрузочной конфигурации

19.Настройте доступ по протоколу SSH на S1 и R2.

Топология



Измените имя домена на ccna.com

Создайте ключ RSA длиной 1024 бит.

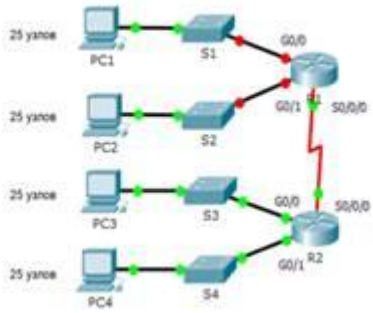
Настройте линии VTY для доступа по протоколу SSH.

Используйте локальные профили пользователей для аутентификации.

Создайте пользователя admin6 с 15-м уровнем привилегированного доступа и зашифрованным паролем Admin6p@ss.

20.Разбейте сеть на подсети

Топология



Разбейте сеть 172.16.6.0/24 на нужное количество подсетей:

a. Назначьте подсеть 0 локальной сети (LAN 1), подключенной к интерфейсу GigabitEthernet 0/0 маршрутизатора R1.

b. Назначьте подсеть 1 локальной сети (LAN2), подключенной к интерфейсу GigabitEthernet 0/1 маршрутизатора R1.

e. Назначьте подсеть 4 каналу WAN между маршрутизаторами R1 и R2.

Завершите документирование схемы адресации в соответствии со следующими рекомендациями.

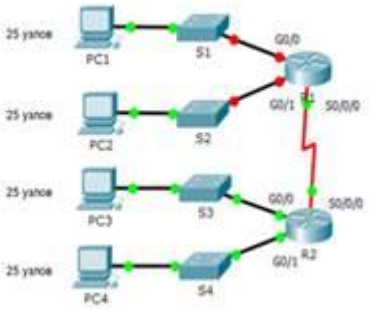
Назначьте первые используемые IP-адреса маршрутизатору R1 для двух каналов локальной сети (LAN) и одного канала сети WAN.

Второй из используемых IP-адресов назначьте коммутаторам.

Последний из используемых IP-адресов назначьте узлам.

21.Выполните базовую настройку устройств S1, R1, R2

Топология



а. Подключитесь с помощью консоли и активируйте привилегированный режим EXEC.

б. Отключите поиск DNS, чтобы предотвратить попытки маршрутизатора неверно преобразовывать введенные команды таким образом, как будто они являются именами узлов.

в. Назначьте class в качестве зашифрованного пароля привилегированного режима EXEC.

г. Назначьте cisco в качестве пароля консоли и включите режим входа в систему по паролю.

д. Назначьте cisco в качестве пароля VTY и включите вход по паролю.

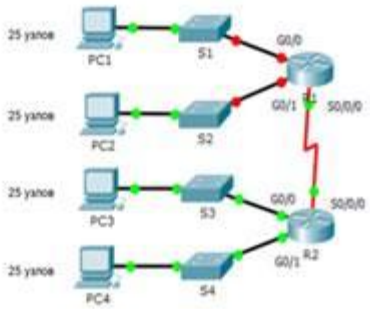
е. Зашифруйте открытые пароли.

ж. Создайте баннер, который предупреждает о запрете несанкционированного доступа(Используйте слово Warninng).

з. Сохраните текущую конфигурацию в файл загрузочной конфигурации

22. Настройте доступ по протоколу SSH на S1 и R2.

Топология



Измените имя домена на ccna.com

Создайте ключ RSA длиной 1024 бит.

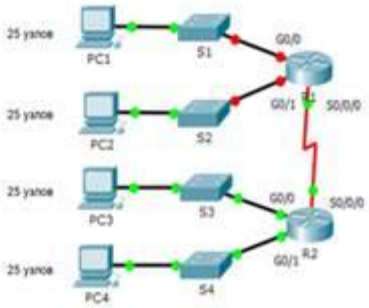
Настройте линии VTY для доступа по протоколу SSH.

Используйте локальные профили пользователей для аутентификации.

Создайте пользователя admin7 с 15-м уровнем привилегированного доступа и зашифрованным паролем Admin7p@ss.

23. Разбейте сеть на подсети

Топология



Разбейте сеть 192.168.7.0/24 на нужное количество подсетей:

a. Назначьте подсеть 0 локальной сети (LAN 1), подключенной к интерфейсу GigabitEthernet 0/0 маршрутизатора R1.

b. Назначьте подсеть 1 локальной сети (LAN2), подключенной к интерфейсу GigabitEthernet 0/1 маршрутизатора R1.

e. Назначьте подсеть 4 каналу WAN между маршрутизаторами R1 и R2.

Завершите документирование схемы адресации в соответствии со следующими рекомендациями.

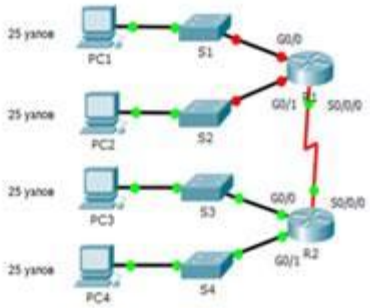
Назначьте первые используемые IP-адреса маршрутизатору R1 для двух каналов локальной сети (LAN) и одного канала сети WAN.

Второй из используемых IP-адресов назначьте коммутаторам.

Последний из используемых IP-адресов назначьте узлам.

24. Выполните базовую настройку устройств S1, R1, R2

Топология



а. Подключитесь с помощью консоли и активируйте привилегированный режим EXEC.

б. Отключите поиск DNS, чтобы предотвратить попытки маршрутизатора неверно преобразовывать введенные команды таким образом, как будто они являются именами узлов.

в. Назначьте class в качестве зашифрованного пароля привилегированного режима EXEC.

г. Назначьте cisco в качестве пароля консоли и включите режим входа в систему по паролю.

д. Назначьте cisco в качестве пароля VTY и включите вход по паролю.

е. Зашифруйте открытые пароли.

ж. Создайте баннер, который предупреждает о запрете несанкционированного доступа(Используйте слово Warninng).

з. Сохраните текущую конфигурацию в файл загрузочной конфигурации

2. Настройте доступ по протоколу SSH на S1 и R2.

Измените имя домена на ccna.com

Создайте ключ RSA длиной 1024 бит.

Настройте линии VTY для доступа по протоколу SSH.

Используйте локальные профили пользователей для аутентификации.

Создайте пользователя admin8 с 15-м уровнем привилегированного доступа и зашифрованным паролем Admin8p@ss.

25. Разбейте сеть на подсети

Разбейте сеть 192.168.8.0/24 на нужное количество подсетей:

a. Назначьте подсеть 0 локальной сети (LAN 1), подключенной к интерфейсу GigabitEthernet 0/0 маршрутизатора R1.

b. Назначьте подсеть 1 локальной сети (LAN2), подключенной к интерфейсу GigabitEthernet 0/1 маршрутизатора R1.

e. Назначьте подсеть 4 каналу WAN между маршрутизаторами R1 и R2.

Завершите документирование схемы адресации в соответствии со следующими рекомендациями.

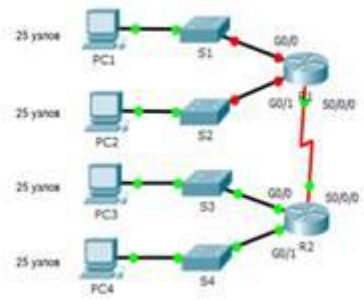
Назначьте первые используемые IP-адреса маршрутизатору R1 для двух каналов локальной сети (LAN) и одного канала сети WAN.

Второй из используемых IP-адресов назначьте коммутаторам.

Последний из используемых IP-адресов назначьте узлам.

26. Выполните базовую настройку устройств S1, R1, R2

Топология



а. Подключитесь с помощью консоли и активируйте привилегированный режим EXEC.

б. Отключите поиск DNS, чтобы предотвратить попытки маршрутизатора неверно преобразовывать введенные команды таким образом, как будто они являются именами узлов.

в. Назначьте class в качестве зашифрованного пароля привилегированного режима EXEC.

г. Назначьте cisco в качестве пароля консоли и включите режим входа в систему по паролю.

д. Назначьте cisco в качестве пароля VTY и включите вход по паролю.

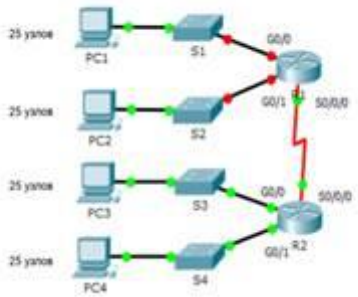
е. Зашифруйте открытые пароли.

ж. Создайте баннер, который предупреждает о запрете несанкционированного доступа(Используйте слово Warninng).

з. Сохраните текущую конфигурацию в файл загрузочной конфигурации

27. Настройте доступ по протоколу SSH на S1 и R2.

Топология



Измените имя домена на ccna.com

Создайте ключ RSA длиной 1024 бит.

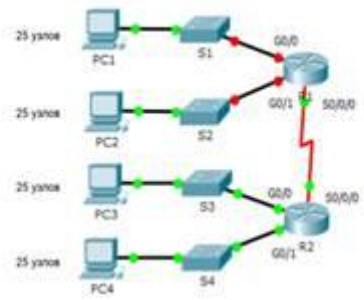
Настройте линии VTY для доступа по протоколу SSH.

Используйте локальные профили пользователей для аутентификации.

Создайте пользователя admin9 с 15-м уровнем привилегированного доступа и зашифрованным паролем Admin9p@ss.

28. Разбейте сеть на подсети

Топология



Разбейте сеть 192.168.9.0/24 на нужное количество подсетей:

a. Назначьте подсеть 0 локальной сети (LAN 1), подключенной к интерфейсу GigabitEthernet 0/0 маршрутизатора R1.

b. Назначьте подсеть 1 локальной сети (LAN2), подключенной к интерфейсу GigabitEthernet 0/1 маршрутизатора R1.

e. Назначьте подсеть 4 каналу WAN между маршрутизаторами R1 и R2.

Завершите документирование схемы адресации в соответствии со следующими рекомендациями.

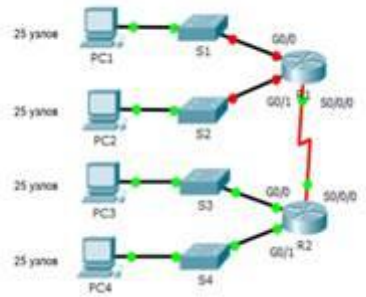
Назначьте первые используемые IP-адреса маршрутизатору R1 для двух каналов локальной сети (LAN) и одного канала сети WAN.

Второй из используемых IP-адресов назначьте коммутаторам.

Последний из используемых IP-адресов назначьте узлам.

29. Выполните базовую настройку устройств S1, R1, R2

Топология



a. Подключитесь с помощью консоли и активируйте привилегированный режим EXEC.

б. Отключите поиск DNS, чтобы предотвратить попытки маршрутизатора неверно преобразовывать введенные команды таким образом, как будто они являются именами узлов.

в. Назначьте class в качестве зашифрованного пароля привилегированного режима EXEC.

г. Назначьте cisco в качестве пароля консоли и включите режим входа в систему по паролю.

д. Назначьте cisco в качестве пароля VTY и включите вход по паролю.

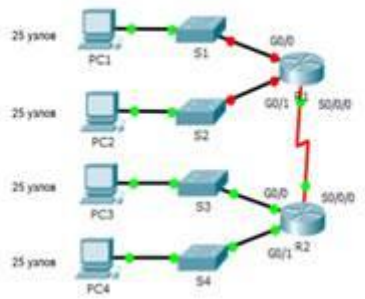
е. Зашифруйте открытые пароли.

ж. Создайте баннер, который предупреждает о запрете несанкционированного доступа(Используйте слово Warninng).

з. Сохраните текущую конфигурацию в файл загрузочной конфигурации

30. Настройте доступ по протоколу SSH на S1 и R2.

Топология



Измените имя домена на ccna.com

Создайте ключ RSA длиной 1024 бит.

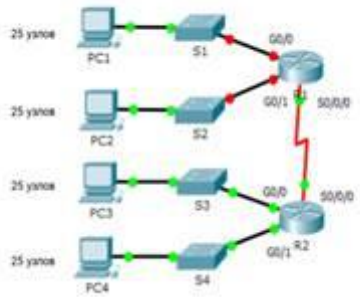
Настройте линии VTY для доступа по протоколу SSH.

Используйте локальные профили пользователей для аутентификации.

Создайте пользователя admin10 с 15-м уровнем привилегированного доступа и зашифрованным паролем Admin10p@ss.

31. Разбейте сеть на подсети

Топология



Разбейте сеть 172.16.10.0/24 на нужное количество подсетей:

a. Назначьте подсеть 0 локальной сети (LAN 1), подключенной к интерфейсу GigabitEthernet 0/0 маршрутизатора R1.

b. Назначьте подсеть 1 локальной сети (LAN2), подключенной к интерфейсу GigabitEthernet 0/1 маршрутизатора R1.

e. Назначьте подсеть 4 каналу WAN между маршрутизаторами R1 и R2.

Завершите документирование схемы адресации в соответствии со следующими рекомендациями.

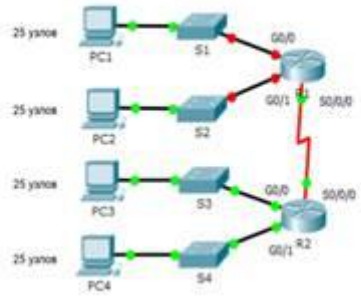
Назначьте первые используемые IP-адреса маршрутизатору R1 для двух каналов локальной сети (LAN) и одного канала сети WAN.

Второй из используемых IP-адресов назначьте коммутаторам.

Последний из используемых IP-адресов назначьте узлам.

32. Выполните базовую настройку устройств S1, R1, R2

Топология



а. Подключитесь с помощью консоли и активируйте привилегированный режим EXEC.

б. Отключите поиск DNS, чтобы предотвратить попытки маршрутизатора неверно преобразовывать введенные команды таким образом, как будто они являются именами узлов.

в. Назначьте class в качестве зашифрованного пароля привилегированного режима EXEC.

г. Назначьте cisco в качестве пароля консоли и включите режим входа в систему по паролю.

д. Назначьте cisco в качестве пароля VTY и включите вход по паролю.

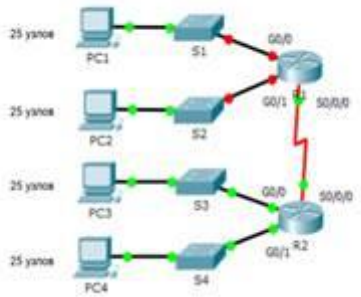
е. Зашифруйте открытые пароли.

ж. Создайте баннер, который предупреждает о запрете несанкционированного доступа(Используйте слово Warninng).

з. Сохраните текущую конфигурацию в файл загрузочной конфигурации

33. Настройте доступ по протоколу SSH на S1 и R2.

Топология



Измените имя домена на ccna.com

Создайте ключ RSA длиной 1024 бит.

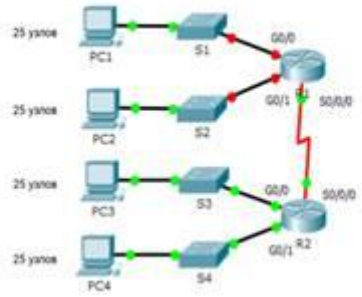
Настройте линии VTY для доступа по протоколу SSH.

Используйте локальные профили пользователей для аутентификации.

Создайте пользователя admin11 с 15-м уровнем привилегированного доступа и зашифрованным паролем Admin11p@ss.

34. Разбейте сеть на подсети

Топология



Разбейте сеть 192.168.11.0/24 на нужное количество подсетей:

a. Назначьте подсеть 0 локальной сети (LAN 1), подключенной к интерфейсу GigabitEthernet 0/0 маршрутизатора R1.

b. Назначьте подсеть 1 локальной сети (LAN2), подключенной к интерфейсу GigabitEthernet 0/1 маршрутизатора R1.

e. Назначьте подсеть 4 каналу WAN между маршрутизаторами R1 и R2.

Завершите документирование схемы адресации в соответствии со следующими рекомендациями.

Назначьте первые используемые IP-адреса маршрутизатору R1 для двух каналов локальной сети (LAN) и одного канала сети WAN.

Второй из используемых IP-адресов назначьте коммутаторам.

Последний из используемых IP-адресов назначьте узлам.

Филиал федерального государственного бюджетного образовательного учреждения высшего образования «Петербургский государственный университет путей сообщения Императора Александра I» в г.Рязани

Рассмотрено ЦК по специальности 09.02.06 Сетевое и системное администрирование Председатель_____ « ___»_____20____ г	Экзаменационный билет № 1 специальность 09.02.06 Сетевое и системное администрирование группа СС 411 Экзамен (квалификационный) по ПМ. 01 Настройка сетевой инфраструктуры 20____- 20_____ учебный год	Утверждаю: Зам. директора по УМР _____ «_____» _____20____ г

1.

2.

3.

Заведующий отделением _____

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО УЧЕБНОЙ ПРАКТИКЕ УП. 01.01

1.Описание

Обучающиеся допускаются к сдаче дифференцированного зачета по учебной практике при условии выполнения всех видов работ на практике, предусмотренных программой и своевременном предоставлении портфолио по учебной практике, включающего в себя:

- титульный лист;
- индивидуальное задание;
- дневник учебной практики;
- отчет по практике;
- выполненное индивидуальное задание;

-положительный аттестационный лист и характеристики руководителей практики от организации прохождения практики и образовательной организации об уровне освоения профессиональных компетенций. Дифференцированный зачет проходит в форме письменного опроса.

На проведения дифференцированного зачета отводится 45 минут.

2. Контрольные вопросы:

1. Проектирование общей топологии.
2. Проектирование физической топологии.
3. Проектирование логической топологии.
4. Построение структурной схемы КС.
5. Обжим сетевого кабеля различными способами.
6. Подключение компьютеров к сети с помощью кабелей.
7. Монтаж сетевых розеток.
8. Монтаж коммуникационной панели.
9. Документирование сети.
10. Создание простой сети. Настройка основных параметров коммутатора
11. Построение простейшей компьютерной сети с использованием маршрутизатора и коммутатора
12. Участие в проектировании сетевой инфраструктуры.
13. Выполнение работ по подключению и обслуживанию сетевого оборудования.
14. Участие в модернизации сетевой инфраструктуры.
15. Настройка сетевого оборудования. Создание простой сети. Настройка основных параметров коммутатора.
16. Настройка маршрутизации.
17. Расчёт суммарных маршрутов.
18. Участие в организации сетевого администрирования.
19. Построение простейшей компьютерной сети с использованием маршрутизатора и коммутатора.
20. Сбор данных для анализа использования и функционирования программно-технических средств компьютерных сетей.
21. Проведение профилактических работ на объектах сетевой инфраструктуры

и рабочих станциях.
22. Отладка сети.
23. Поиск и устранение неполадок с использованием системного подхода.
24. Настройка динамической маршрутизации с применением протоколов RIP, BGP, EIGRP.
25. Статическая трансляция адресов NAT.
26. Настройка DHCP сервера.
27. Настройка DNSP сервера.
28. Преобразование сетевых адресов. Работа с NAT и PAT
29. Сегментирование сети с помощью VLAN.
30. Trunk, настройка протоколов VTP и DTP.
31. Настройка ACL-списков.
32. Настройка Syslog. SNMP. Принцип работы SNMP. Настройка SNMP.
33. Резервное копирование и восстановление конфигураций сетевых
34. Сетевая безопасность.
35. Настройка безопасного доступа к устройствам в сети.
36. Назначение административных и других ролей.
37. Настройка безопасности на сетевых устройствах.
38. Организация и безопасного доступа к сетевым устройствам.
39. Настройка безопасности на прикладном, транспортном и канальном и сетевом уровне.
40. Настройка базового протокола PPP с аутентификацией.
41. Настройка туннелирования с помощью протокола L2TP.
42. Настройка туннелирования с помощью протокола IPsec.
43. Настройка туннелирования с помощью протокола SSTP.
44. Реализация технологий VPN Настройка туннелирования с помощью OpenVPN.
45. Авторизация клиентов в посредством SSL сертификатов.
46. Использование сервисов криптографической защиты информации.
47. Локальная аутентификация, авторизация и аудит
48. Настройка политики безопасности межсетевых экранов.
49. Настройка защиты от DOS и DDOS атаки.
50. Настройка шифрования информации различными методами.

Информационное обеспечение обучения

Перечень рекомендуемых учебных изданий, Интернет-ресурсов, дополнительной литературы

Основная литература

1. Максимов, Н. В. Компьютерные сети : учебное пособие / Н.В. Максимов, И.И. Попов. — 6-е изд., перераб. и доп. — Москва : ФОРУМ : ИНФРА-М, 2021. — 464 с. — (Сред-нее профессиональное образование). - ISBN 978-5-00091-454-0. Электронный ресурс. Режим доступа: сетевой - URL: https://znanium.com/catalog/product/1189333 (дата об-ращения: 08.04.2021).
2. Дибров, М. В. Компьютерные сети и телекоммуникации. Маршрутизация в IP-сетях в 2 ч. Часть 1 : учебник и практикум для среднего профессионального образования / М. В. Дибров. — Москва : Издательство Юрайт, 2020. — 333 с. — (Профессиональное образование). — ISBN 978-5-534-04638-0. Электронный ресурс. Режим доступа: сете-вой URL: https://urait.ru/bcode/452574 (дата обращения: 08.04.2021).
3. Дибров, М. В. Компьютерные сети и телекоммуникации. Маршрутизация в IP-сетях в 2 ч. Часть 2 : учебник и практикум для среднего профессионального образования / М. В. Дибров. — Москва : Издательство Юрайт, 2020. — 351 с. — (Профессиональное образование). — ISBN 978-5-534-04635-9. Электронный ресурс. Режим доступа: сете-вой URL: https://urait.ru/bcode/453065 (дата обращения: 08.04.2021).
4. Гольдштейн Б. С. Системы коммутации. / Гольдштейн Б. С. — СПб.: БХВ – Санкт-Петербург, 2003.— 318 с. - ISBN 5-8206-0108-4. - Текст: электронный. - URL: https://kunegin.com/nata/sk.pdf
5. Семёнов Ю. В. Проектирование сетей связи следующего поколения. / Семёнов Ю.В. — СПб.: Наука и техника, 2005. — 240 с. — Текст: электронный. - URL: https://www.proektant.org/arh/1590.html

Дополнительная литература

1. Сети и телекоммуникации : учебник и практикум для вузов / К. Е. Самуйлов [и др.] ; под редакцией К. Е. Самуйлова, И. А. Шалимова, Д. С. Кулябова. — Москва : Изда-тельство Юрайт, 2020. — 363 с. — (Высшее образование). — ISBN 978-5-534-00949-1.— Электронный ресурс. Режим доступа: сетевой URL: https://urait.ru/bcode/450234 (дата обращения: 08.04.2021).
2. Исаченко, О. В. Программное обеспечение компьютерных сетей : учебное пособие / О.В. Исаченко. — 2-е изд., испр. и доп. — Москва : ИНФРА-М, 2021. — 158 с. — (Среднее профессиональное образование). - ISBN 978-5-16-015447-3. Электронный ре-сурс. Режим доступа: сетевой - URL: https://znanium.com/catalog/product/1189344 (дата обращения: 08.04.2021).
3. Лисьев, Г.А. Программное обеспечение компьютерных сетей и web-

серверов : учебное пособие / Г. А. Лисьев, П. Ю. Романов, Ю. И. Аскерко. — Москва : ИНФРА-М, 2020. — 145 с. — (Высшее образование: Бакалавриат). - ISBN 978-5-16-013565-6.Электронный ресурс. Режим доступа: сетевой URL: https://znanium.com/catalog/product/1068576 (дата обращения: 08.04.2021).

4. Основы моделирования : учебное пособие для среднего профессионального образова-ния / О. М. Замятина. — Москва : Издательство Юрайт, 2020. — 159 с. — (Профессио-нальное образование). — ISBN 978-5-534-10682-4. — Электронный ресурс. Режим до-ступа: сетевой URL: https://urait.ru/bcode/456799 (дата обращения: 08.04.2021).
5. Тепляков И. М. Основы построения телекоммуникационных систем и сетей. Учебное пособие образования / Тепляков И.М. — Москва : Радио и связь, 2004.— 323 с. — Текст: электронный— URL: https://zlibrary-asia.se/book/2937663/43bc8a