КОМИТЕТ ОБРАЗОВАНИЯ, НАУКИ И МОЛОДЕЖНОЙ ПОЛИТИКИ ВОЛГОГРАДСКОЙ ОБЛАСТИ
ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ «КОТОВСКИЙ ПРОМЫШЛЕННО–ЭКОНОМИЧЕСКИЙ ТЕХНИКУМ»
(ГБПОУ «КОТОВСКИЙ ПРОМЫШЛЕННО–ЭКОНОМИЧЕСКИЙ ТЕХНИКУМ»)

УТВЕРЖДАЮ
Зам. директора по УР
_____ З.Ф. Дьякова
«5» 09 2022 г.

# МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО ВЫПОЛНЕНИЮ ЛАБОРАТОРНЫХ РАБОТ

МДК 01.01 Компьютерные сети

ПМ.01 ВЫПОЛНЕНИЕ РАБОТ ПО ПРОЕКТИРОВАНИЮ СЕТЕВОЙ ИНФРАСТРУКТУРЫ

**09.02.06 Сетевое и системное администрирование**

Форма обучения **ОЧНАЯ**

Котово,
2022

**Методические рекомендации по выполнению лабораторных работ по** МДК 01.01 Компьютерные сети **профессионального модуля** ПМ.01 Выполнение работ по проектированию сетевой инфраструктуры **специальности 09.02.06 Сетевое и системное администрирование.** Форма обучения **очная**

Организация-разработчик: **Государственное бюджетное профессиональное образовательное учреждение «Котовский промышленно-экономический техникум»**

Разработчики:
**Трунова Людмила Владимировна,** председатель ЦМО, преподаватель профессиональных дисциплин

РАССМОТРЕНО

На заседании ЦМО ЕН и ИТ

Протокол № 4 от 03.02 2022 г.

Председатель ЦМО Трун /Трунова Л.В/

РЕКОМЕНДОВАНО

Научно-методический совет

Заключение № 6 от 05.02 2022 г.

Председатель методического совета З.Ф.Дьякова

# Содержание

## Пояснительная записка

Методические указания по выполнению лабораторных работ по МДК 01.01 Компьютерные программы профессионального модуля **ПМ.01 Выполнение работ по проектированию сетевой инфраструктуры** разработана на основе Федерального государственного образовательного стандарта по специальности среднего профессионального образования **09.02.06 Сетевое и системное администрирование**.

В результате изучения профессионального модуля студент должен освоить основной вид деятельности Выполнение работ по проектированию сетевой инфраструктуры и соответствующие ему общие компетенции и профессиональные компетенции.

Иметь практический опыт в:

- проектировании архитектуры локальной сети в соответствии с поставленной задачей;
- установке и настройке сетевых протоколов и сетевого оборудования в соответствии с конкретной задачей;
- выборе технологии, инструментальных средств при организации процесса исследования объектов сетевой инфраструктуры;
- обеспечении безопасного хранения и передачи информации в локальной сети;
- использовании специального программного обеспечения для моделирования, проектирования и тестирования компьютерных сетей.

## Содержание учебной дисциплины

### Раздел 1. Компьютерные сети

### Тема 1.1. Введение в сетевые технологии

**1. Лекция «Компьютерные сети»**

Совместная работа, Интернет и современные сетевые технологии - область применения и назначение. Виды компьютерных сетей. Глобальные и локальные сети. Одноранговые и клиент - серверные архитектуры. Основные компоненты сетей, сетевая среда и сетевые устройства. Технологии подключения к Интернет. Конвергентные сети. Качество и надежность сетей. Основные понятия сетевой безопасности. Тенденции развития сетей.

**2. Лекция «Сетевые протоколы и коммуникации»**

Кодирование и параметры сообщения. Сетевые протоколы. Взаимодействие протоколов. Набор протоколов TCP/IP и процесс обмена данными. Организации по стандартизации: ISOC, IAB, IETF, IEEE, ISO. Многоуровневые модели OSI и TCP/IP. Инкапсуляция данных. Протокольные блоки данных (PDU). Доступ к локальным ресурсам. Сетевая адресация. MAC- и IP- адреса. Доступ к удалённым ресурсам. Шлюз по умолчанию.

**3. Лекция «Сетевой доступ»**

Протоколы и стандарты физического уровня. Способы подключения к сети. Сетевые интерфейсные платы (NIC). Среды передачи данных и их характеристики: пропускная способность, производительность. Виды медных сетевых кабелей: UTP, STP, коаксиальный. Разновидности, особенности прокладки и тестирования кабелей. Структура и особенности прокладки оптоволоконных кабелей. Беспроводные средства передачи данных. Стандарт Wi-Fi IEEE 802.11.

Канальный уровень и его подуровни: Управление логическим каналом (LLC) и Управление доступом к среде передачи данных MAC. Структура кадра канального уровня и принципы его формирования. Стандарты канального уровня. Физическая и логическая топология сети. Топологии «точка-точка», «звезда», «полносвязанная», «кольцевая».

**4. Лекция «Сетевые технологии Ethernet»**

Семейство сетевых технологий Ethernet. Принцип работы Ethernet. Взаимодействие на подуровнях LLC и MAC. Управление доступом к среде передачи данных (CSMA). MAC-адрес: идентификация Ethernet. Атрибуты кадра Ethernet. Представления MAC-адресов. Одно и много адресной, широковещательной рассылок. Сквозное подключение, MAC- и IP-адреса. Протокол разрешения адресов (ARP): принципы работы, роль в процессе

удаленного обмена данными. Таблицы ARP на сетевых устройствах.

**5. Лекция «Сетевой уровень»**

Сетевой уровень в процессе передачи данных. Протоколы сетевого уровня. Основные характеристики IP-протокола. Структура пакетов IPv4 и IPv6. Особенности и преимущества протокола Pv6. Методы маршрутизации узлов. Таблица маршрутизации узлов и маршрутизатора
для протоколов IPv4 и IPv6. Устройство маршрутизатора - Процессор, память, операционная система. Подключение к маршрутизатору через различные порты. Настройка исходных параметров, интерфейсов, шлюза по умолчанию и других характеристик маршрутизатора.

**6. Лекция «Транспортный уровень»**

Назначение и задачи транспортного уровня.
Мультиплексирование сеансов связи. Описание и сравнение протоколов TCP и UDP - надежность и производительность, область применения. Адресация портов и сегментация TCP и UDP. Обмен данными по TCP. Процессы TCP сервера. Установление TCP-соединения и его завершение. Принципы «трёхстороннего рукопожатия» TCP. Надёжность и управление потоком TCP - Подтверждение получения сегментов, потеря данных и повторная передача, управление потоком. Обмен данными с использованием UDP. Процессы и запросы UDP- сервера, UDP-датаграммы, процессы UDP-клиента. Приложения, использующие UDP и TCP.

**7. Лекция «IP-адресация»**

Структура IPv4-адресов. Сетевая и узловая часть IP-адреса. Преобразование адресов между двоичным и десятеричным представлением. Маска подсети IPv4. Сетевой адрес, адрес узла и широковещательный адрес сети IPv4. Присвоение узлу статического и динамического IPv4- адреса. Многоадресная передача. Публичные и частные IPv4-адреса. IPv4-адреса специального назначения. Присвоение IP-адресов.Совместное использование протоколов IPv4 и IPv6: двойной стек, туннелирование, преобразование. Представление IPv6-адресов.

**8. Лекция «Разделение IP-сетей на подсети»**

Сегментация IP-сетей. Обмен данными между подсетями. Планирование адресации в подсетях. Расчетные формулы для сегментации сети. Разбиение на подсети на основе требований узлов и сетей, в соответствии с требованиями сетей. Определение маски подсети. Разбиение на подсети с использованием маски переменной длины (VLSM).

**9. Лекция «Уровень приложений»**

Уровень приложений, уровень представления и сеансовый уровень. Примеры распространенных приложений. Протоколы уровня приложений. Одноранговые сети (P2P). Модель типа «клиент-сервер». Обзор протоколов HTTP, HTTPS, SMTP, POP и IMAP. Служба доменных имён (DNS). Формат сообщений и иерархия DNS. Утилита «nslookup». Служба DHCP. Протокол передачи файлов (FTP). Протокол обмена блоками серверных сообщений (SMB). Концепции «Всеобъемлющий Интернет» BYOD. Доставка данных по конвергентным сетям.

**10. Лекция «Создание и настройка небольшой компьютерной сети»**

Планирование и создание небольшой компьютерной сети: определение ключевых факторов, выбор топологии и сетевых устройств, выбор и настройка протоколов, системы адресации. Меры по обеспечению безопасности сети. Уязвимости и сетевые атаки. Разведывательные атаки, Атаки доступа, Отказ в обслуживании (DoS-атаки). Резервное копирование, обновление и установка исправлений. Межсетевые экраны. Аутентификация, авторизация и учёт. Включение протокола SSH.

**11. Лекция «Введение в коммутируемые сети»**

Объединённые сети. Иерархия в коммутируемой сети. Роль коммутируемых сетей. Коммутируемая среда. Динамическое заполнение таблицы MAC-адресов коммутатора.

Методы пересылки на коммутаторе. Коммутация с промежуточным хранением. Сквозная коммутация. Коммутационные домены. Снижение перегрузок сети.

**12. Лекция «Основные концепции и настройка коммутации»**

Основные концепции и настройка коммутации. Первоначальная настройка коммутатора и восстановление после системного сбоя. Настройка доступа для базового управления коммутатором с IPv4. Дуплексная связь. Настройка портов коммутатора на физическом уровне.

Безопасность коммутатора. Защищённый удалённый доступ. Настройка SSH. Распространённые угрозы безопасности: переполнение таблицы MAC-адресов, DHCP-спуфинг, использование уязвимостей протокола CDP, Атаки Telnet и др. Аудит и практические рекомендации по обеспечению безопасности сети.

**13. Лекция «Виртуальные локальные сети (VLAN)»**

Виртуальные локальные сети (VLAN) - классификация и основные характеристики. Транки виртуальных сетей. Контроль широковещательных доменов в сетях VLAN. Тегирование кадров Ethernet для идентификации сети VLAN. Сети native VLAN и тегирование стандарта 802.1Q. Тегирование голосовой VLAN. Реализации виртуальной локальной сети. Назначение портов сетям VLAN. Настройка транковых каналов. Протокол динамического создания транкового канала (DTP). Поиск и устранение неполадок в виртуальных локальных сетях и транковых каналах. Проблемы с IP-адресацией сети VLAN. Проектирование и обеспечение безопасности VLAN: hopping, спуфинг коммутатора, атака с двойным тегированием, Сеть PVLAN периметра.

**14. Лекция «Концепция маршрутизации»**

Настройка маршрутизатора. Механизмы пересылки пакетов. Подключение и настройка устройств. Активация и настройка IP- адресации. Проверка связности сетей с прямым подключением. Проверка настроек интерфейса. Фильтрация выходных данных команд «show». Коммутация пакетов между сетями. Функция коммутации маршрутизатора. Маршрутизация пакетов. Определение пути. Процесс принятия решения о пересылке пакетов. Выбор оптимального пути. Протоколы RIP, OSPF, EIGRP. Распределение нагрузки. Администрирование расстояние (AD) и надежность маршрута. Анализ таблиц маршрутизации - источник данных, принципы формирование возможности настройки. Записи таблицы маршрутизации для сетей с прямым подключением. Задание статических маршрутов. Протоколы динамической маршрутизации сетей IPv4 и IPv6.

**15. Лекция «Маршрутизация между VLAN»**

Принципы работы маршрутизации между VLAN. Настройка маршрутизации на базе маршрутизаторов с несколькими физическими интерфейсами, с использованием конфигурации router-on-a-stick, через многоуровневый коммутатор. Проблемы маршрутизации между VLAN. Проверка конфигурации коммутатора и настроек маршрутизатора. Неполадки в работе интерфейса. Ошибки в IP-адресах и масках подсети. Настройка и работа коммутации на 3-м уровне. Маршрутизация между VLAN через виртуальные интерфейсы коммутатора, маршрутизируемые порты.

**16. Лекция «Статическая маршрутизация»**

Преимущества и задачи статической маршрутизации. Типы статических маршрутов: стандартный, по умолчанию, суммарный, плавающий. Настройка статических маршрутов IPv4 и IPv6. Команда «ip route». Маршрут следующего перехода. Напрямую подключённый статический маршрут. Полностью заданный статический маршрут. Настройка статического маршрута по умолчанию. Классовая адресация. Классовые маски подсети. Бесклассовая междоменная маршрутизация CIDR. Объединение маршрутов. Организация суперсетей. Использование масок подсети фиксированной длины (FLSM). Маска подсети переменной длины (VLSM). Настройка суммарных и плавающих статических маршрутов. Расчёт суммарного маршрута. Объединение сетевых адресов IPv4 и IPv6.

**17. Лекция «Динамическая маршрутизация»**

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. Классификация протоколов маршрутизации. Протоколы IGP и EGP. Дистанционно-векторные протоколы RIP, IGRP. Протоколы маршрутизации по состоянию канала OSPF и IS-IS. Классовые и бесклассовые протоколы маршрутизации. Характеристики и метрики протоколов.

**18. Лекция «OSPF для одной области»**

Семейство протоколов OSPF. Характеристики, принципы работы и компоненты OSPF. Особенности OSPF для одной и нескольких областей. Магистральная область. Инкапсуляция сообщений OSPF. 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. Рабочие состояния OSPF. Выделенный (DR) и резервный выделенный маршрутизатор (BDR). Настройка OSPFv2 для одной области. Режим конфигурации идентификаторы маршрутизатора. Включение OSPF на интерфейсах. Шаблонная маска. Команда «network». Формула расчёта метрики стоимости OSPF. Настройка значений пропускной способности интерфейса. Проверка соседних устройств, настроек протокола, данных процесса и других характеристик OSPF. Сравнение OSPFv2 и OSPFv3.

**19. Лекция «Списки контроля доступа (ACL)»**

Списки контроля доступа (ACL). Принцип работы ACLсписков. Типы ACL-списков Cisco для IPv4. Присваивание номеров и имён ACL-спискам. Расчёт шаблонной маски в ACL-списках. Рекомендации по созданию и размещению ACL-списков. Размещение стандартных и расширенных ACL-списков. Настройка стандартного ACL-списка. Применение стандартных ACL-списков на интерфейсах. Комментарии к ACL-спискам. ACL-статистика. Защита портов VTY с помощью стандартного ACL-списка IPv4. Структура и настройка расширенных ACL-списков для IPv4. Фильтрация трафика с использованием расширенных ACL-списков. Настройка и проверка ACL-списков для IPv6.

**20. Лекция «Протокол DHCP»**

Протокол DHCP. DHCPv4: базовая операция, формат сообщений, сообщения обнаружения и предложения. Настройка, проверка и ретрансляция простого DHCPv4-сервера. Настройка маршрутизатора в качестве DHCPv4-клиента. Настройка маршрутизатора класса SOHO. Поиск и устранение неполадок в работе маршрутизатора DHCPv4. Протокол DHCPv6. Автоматическая настройка адреса без отслеживания состояния (SLAAC). Принцип работы SLAAC с DHCPv6. DHCPv6 с и без отслеживания состояния. Процессы DHCPv6. Настройка маршрутизатора в качестве DHCPv6-сервера и DHCPv6-клиента. Поиск и устранение неполадок в работе DHCPv6.

**21. Лекция «Преобразование сетевых адресов IPv4»**

Преобразование сетевых адресов IPv4. Концептуальное преобразование сетевых адресов (NAT). Терминология и принципы работы NAT. Пространство частных IPv4-адресов. Статическое и динамическое преобразование сетевых адресов (NAT). Преобразование адресов портов (PAT). Сравнение NAT и PAT. Преимущества и недостатки NAT. Анализ статического преобразования NAT. Принцип работы динамического NAT Настройка и проверка NAT,

PAT. Переадресация портов. Настройка NAT и протокола IPv6.

Поиск и устранение неполадок в работе NAT.

**Методические указания по выполнению лабораторных работ**

**Лабораторная работа № 1**

**Тема: Составление карты сети Интернет с помощью утилит «ping» и «traceroute»**

**Цель работы: получить практические навыки по работе с утилитами «ping» и «traceroute»**

Необходимые ресурсы 1 ПК (Windows 10 с выходом в Интернет)

**Часть 1. Проверка сетевого подключения с помощью команды ping**

a. Что такое Эхо-запрос с помощью команды ping?

b. Нажмите кнопку **Пуск** на экране компьютера, введите команду **cmd** в поле **Найти программы и файлы** и нажмите клавишу ВВОД.

c. В командной строке введите **ping www.cisco.com**.

d. Где в строке полученных данных отображается полное доменное имя (FQDN) , IP-адрес ?

e. Сколько было отправлено эхо-запросов с помощью команды ping, на каждый из которых был получен ответ.

Сколько потеренных пакетов?

Какое среднее для передачи пакетов по сети?

```
C:\>ping -n 100 www.cisco.com
```

f. Теперь отправьте эхо-запрос с помощью команды ping на веб-сайты регионального интернетрегистратора (RIR), расположенные в различных частях мира.

Африка:

C:\> **ping www.afrinic.net**

Австралия:

C:\> **ping www.apnic.net**

Европа:

C:\> **ping www.ripe.net**

Южная Америка:

C:\> **ping lacnic.net**

Что можно сказать об эхо-запросах с помощью команды ping?

**Часть 2. Трассировка маршрута к удаленному серверу с помощью команды Windows tracert**

**Определите, какой маршрут из всего интернет-трафика направлен к удалённому серверу.**

a. В командной строке введите **tracert** www.cisco.com.

b. Сохраните результаты, полученные после ввода команды «tracert», в текстовый файл, выполнив указанные ниже действия.

c. Запустите утилиту **tracert** для каждого веб-сайта назначения и сохраните полученные результаты в последовательно пронумерованные файлы.

C:\> **tracert www.afrinic.net**

C:\> **tracert www.lacnic.net**

d. Интерпретируйте данные, полученные с помощью утилиты **tracert**.

```
C:\>tracert www.cisco.com

Tracing route to e144.dscb.akamaiedge.net [23.1.144.170]
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms  dslrouter.westell.com [192.168.1.1]
  2    38 ms    38 ms    37 ms  10.18.20.1
  3    37 ms    37 ms    37 ms  G3-0-9-2204.ALBYNY-LCR-02.verizon-gni.net [130.8
1.196.190]
  4    43 ms    43 ms    42 ms  so-5-1-1-0.NY325-BB-RTR2.verizon-gni.net [130.81
.22.46]
  5    43 ms    43 ms    65 ms  0.so-4-0-2.XT2.NYC4.ALTER.NET [152.63.1.57]
  6    45 ms    45 ms    45 ms  0.so-3-2-0.XL4.EWR6.ALTER.NET [152.63.17.109]
  7    46 ms    48 ms    46 ms  TenGigE0-5-0-0.GW8.EWR6.ALTER.NET [152.63.21.14]

  8    45 ms    45 ms    45 ms  a23-1-144-170.deploy.akamaitechnologies.com [23.
1.144.170]

Trace complete.
```

Детализируем.


**Оформите отчет, сделайте вывод по работе**

**Практическая работа № 1**
**Тема: Подключение компьютеров к сети с помощью кабелей и беспроводных адаптеров**
**Цель работы: научится описывать функции и физические характеристики сетевого устройства, а так же физические характеристики сетевой среды**

**Часть 1: Определение сетевых устройств**
Преподаватель предложит вам определить различные сетевые устройства. Каждому из них будет присвоен идентификационный номер. Заполните приведённую ниже таблицу, указав идентификационный номер устройства, название производителя и модель устройства, тип (концентратор, коммутатор или маршрутизатор), функцию (беспроводное устройство, маршрутизатор, коммутатор или комбинация функций) и другие физические характеристики, например количество типов интерфейсов.

| Идентификатор | Производитель Модель | Тип | Функции | Физические характеристики |
|---|---|---|---|---|
| | | | | |
| | | | | |
| | | | | |
| | | | | |

**Часть 2: Packet Tracer: подключение проводной и беспроводной сети**
Топология:

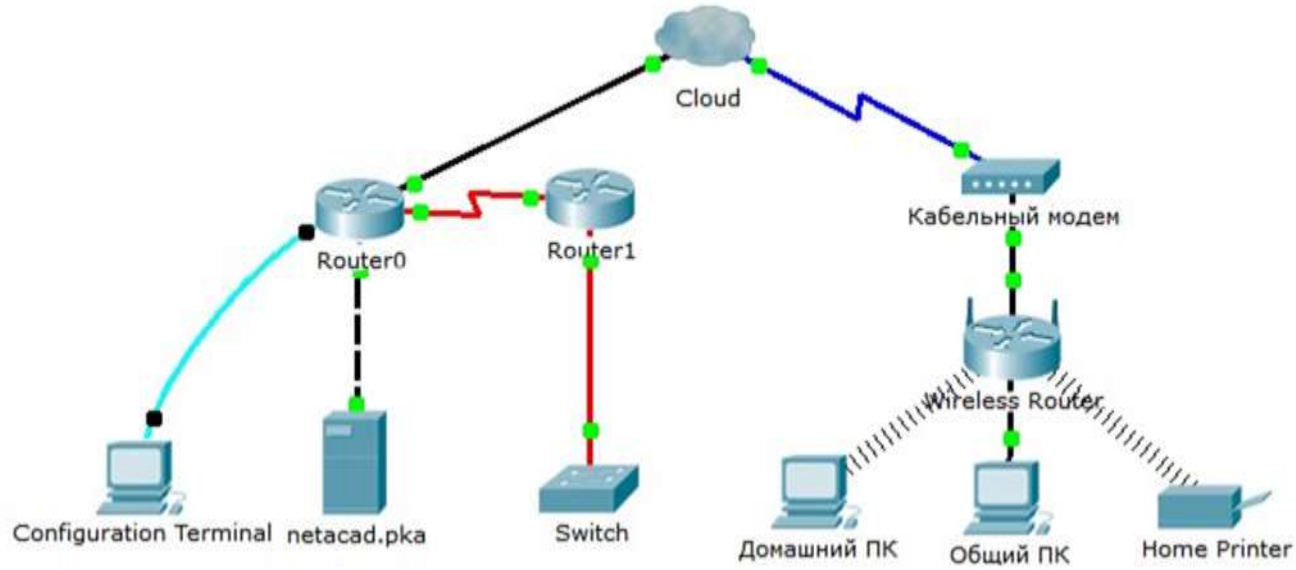



Таблица адресации

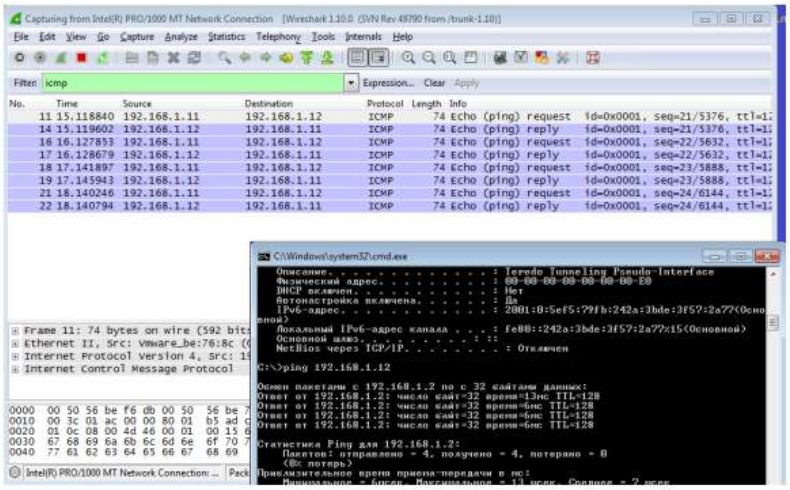
| Устройство | Интерфейс | IP-адрес | Подключается к |
|---|---|---|---|
| Cloud | Eth6 | Недоступно | Fa0/0 |
| | Coax7 | Недоступно | Port0 |
| Кабельный модем | Port0 | Недоступно | Coax7 |
| | Port1 | Недоступно | Интернет |
| Маршрутизатор0 | Консоль | Недоступно | RS232 |
| | Fa0/0 | 192.168.2.1/24 | Eth6 |
| | Fa0/1 | 10.0.0.1/24 | Fa0 |
| | Ser0/0/0 | 172.31.0.1/24 | Ser0/0 |
| Маршрутизатор1 | Ser0/0 | 172.31.0.2/24 | Ser0/0/0 |
| | Fa1/0 | 172.16.0.1/24 | Fa0/1 |
| Беспроводной маршрутизатор | Интернет | 192.168.2.2/24 | Порт 1 |
| | Eth1 | 192.168.1.1 | Fa0 |
| Общий ПК | Fa0 | 192.168.1.102 | Eth1 |
| Коммутатор | Fa0/1 | 172.16.0.2 | Fa1/0 |
| Netacad.pka | Fa0 | 10.0.0.1 | Fa0/1 |
| Терминал настройки | RS232 | Недоступно | Консоль |

**Оформите отчет, сделайте вывод по работе**

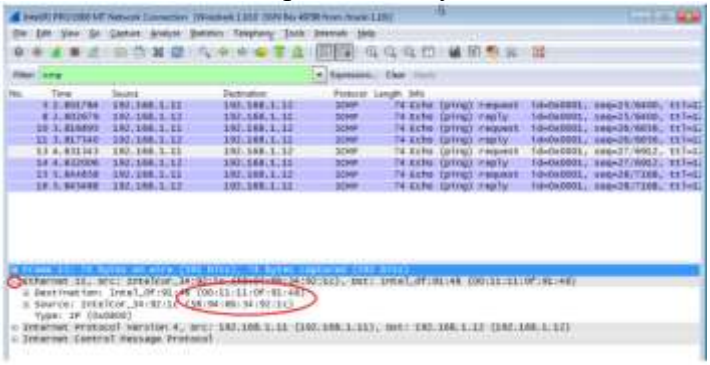
## Лабораторная работа № 2
## Тема: Просмотр сетевого трафика с помощью программы Wireshark

**Цель работы: получить практические навыки работы с программой Wireshark**
Необходимые ресурсы
• 1 ПК (Windows 10 с выходом в Интернет)
• Дополнительные ПК в локальной сети будут использоваться для ответов на эхо-запросы.
Топология:


Загрузите и установите программу Wireshark (необязательно)
Часть 1. Сбор и анализ данных протокола ICMP по локальным узлам в программе Wireshark
a. Начните и остановите сбор данных трафика эхо-запросов с помощью команды ping к локальным узлам.



b. Найдите данные об IP- и MAC-адресах в полученных PDU.



Совпадает ли MAC-адрес источника с интерфейсом вашего компьютера? Совпадает ли MAC-адрес назначения в программе Wireshark с MAC-адресом другого учащегося?
Как ваш ПК вычислил MAC-адрес ПК, на который был отправлен эхо-запрос с помощью команды ping?
**Часть 2. Сбор и анализ данных протокола ICMP по удалённым узлам в программе Wireshark**
a. Начните и остановите сбор данных трафика эхо-запросов с помощью команды ping к удалённым узлам.

Активировав перехват данных, отправьте эхо-запрос с помощью команды ping на следующие три URL-адреса: 1) www.yahoo.com 2) www.cisco.com 3) www.google.com

b. Найдите данные об IP- и MAC-адресах в полученных PDU.

Просмотрите собранные данные и изучите IP- и MAC-адреса трёх запрошенных веб-сайтов.

Ниже укажите IP- и MAC-адреса назначения для всех трех веб-сайтов.

1адрес:IP: _____._____._____._____ MAC: ____:____:____:____:____:____

2адрес:IP: _____._____._____._____ MAC: ____:____:____:____:____:____

3адрес:IP: _____._____._____._____ MAC: ____:_

c. Поясните, почему MAC-адреса удалённых узлов отличаются от MAC-адресов локальных узлов.

**Оформите отчет, сделайте вывод по работе.**

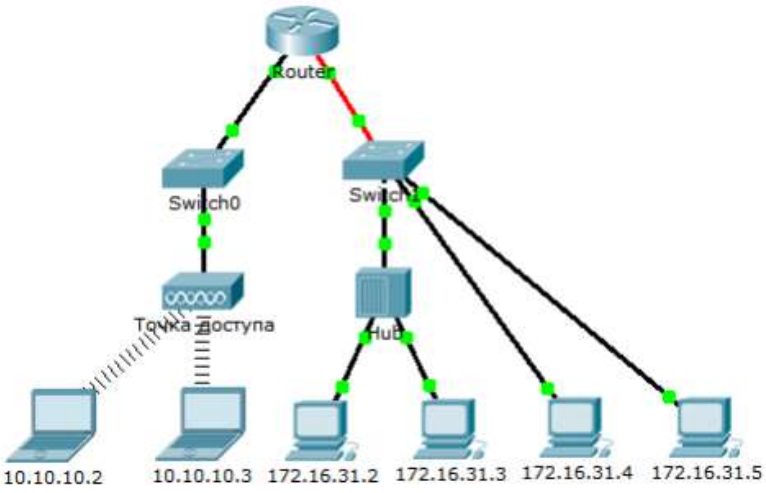
## Лабораторная работа № 3
## Тема: Изучение Ethernet-технологий

**Цель работы: получить практические навыки работы с программой Packet Tracer: определение MAC-и IP-адресов**

Необходимые ресурсы

1 ПК (Windows 10 с доступом к командной строке, доступу к Интернету и с программой Packet Tracer)

Топология:




**Часть 1: Сбор сведений о PDU**

a. Щёлкните 172.16.31.2 и откройте окно Command Prompt (Командная строка).

b. Введите команду ping 10.10.10.3.

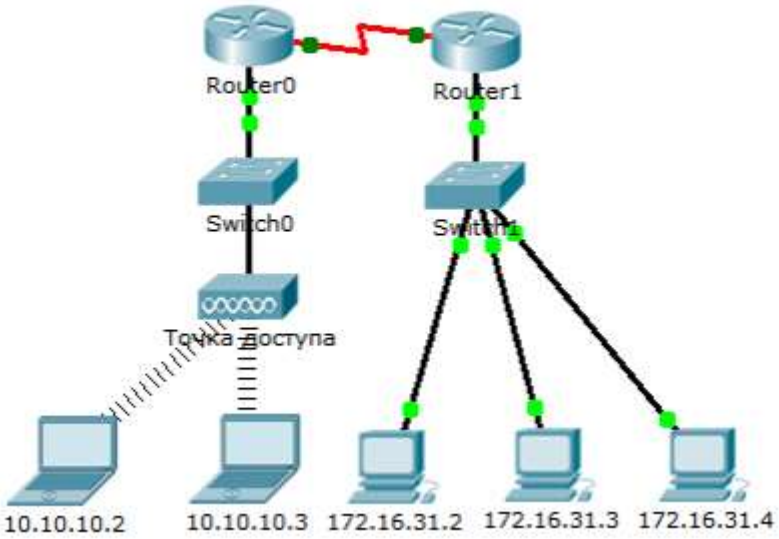
c. Перейдите в режим моделирования и повторите команду ping 10.10.10.3. PDU будет показан
рядом с 172.16.31.2.

d. Щёлкните PDU и запишите следующие данные на вкладке Outbound PDU Layer (сведения об
исходящем PDU):

– Destination MAC Address: 00D0:BA8E:741A
– Source MAC Address: 000C:85CC:1DA7

**Часть 2: Анализ запроса ARP**

Топология:




Создание запросов ARP путём отправки эхо-запросов на адрес 172.16.31.3
с 172.16.31.2.
a. Щёлкните 172.16.31.2 и откройте окно Command Prompt (Командная строка).
b. Выполните команду arp -d, чтобы очистить таблицу ARP.
c. Перейдите в режим моделирования и выполните команду ping 172.16.31.3. Будут созданы два
пакета PDU. Команда ping не может отправить ICMP-пакет, не зная MAC-адрес назначения.
Поэтому компьютер отправляет широковещательный кадр ARP, чтобы найти MAC-адрес назначения.
d. Нажмите кнопку Capture/Forward (Захватить/Переслать) один раз. ARP-пакет PDU перемещается
на коммутатор Switch1, а ICMP-пакет PDU исчезает, ожидая ARP-ответ. Откройте PDU и запишите
MAC-адрес назначения. Этот адрес есть в таблице выше?
e. Нажмите кнопку Capture/Forward (Захватить/Переслать), чтобы переместить PDU на следующее
устройство. Сколько копий PDU создал коммутатор Switch1?
f. Какой IP-адрес имеет устройство, которое приняло PDU?
g. Откройте PDU и изучите 2-й уровень. Что произошло с MAC-адресами источника и назначения?
h. Нажимайте кнопку Capture/Forward до тех пор, пока PDU не вернётся на узел 172.16.31.2. Сколько
копий PDU создал коммутатор для ответа на ARP-запрос?
Анализ таблицы ARP.
a. Обратите внимание, что пакет ICMP снова появился. Откройте PDU и взгляните на MAC-адрес.
MAC-адреса источника и назначения соответствуют их IP-адресам?
b. Вернитесь обратно в режим реального времени, и команда ping завершится.
c. Щёлкните 172.16.31.2 и выполните команду arp -a. Какому IP-адресу соответствует запись MAC-адреса?
d. В общем случае, когда оконечное устройство отправляет ARP-запрос?
**Оформите отчет, сделайте вывод по работе.**

**Лабораторная работа № 4**

**Тема: Построение сети на базе маршрутизатора**

**Цель работы: получить практические навыки в работе с программой Packet Tracer: изучение межсетевых устройств**

Необходимые ресурсы

1 ПК (Windows 10 с доступом к командной строке, доступу к Интернету и с программой Packet Tracer)

Топология:


**Часть 1: Определение физических характеристик межсетевых устройств**

Шаг 1: Определение портов управления маршрутизатора Cisco. a. Щёлкните маршрутизатор East. Вкладка Physical (Физический) должна быть активна. b. Увеличьте масштаб и разверните окно, чтобы видеть весь маршрутизатор. c. Какие порты управления доступны?

Шаг 2: Определение интерфейсов локальной и глобальной сети на маршрутизаторе Cisco

a. Какие интерфейсы ЛВС и WAN доступны на маршрутизаторе East и сколько их?

c. Откройте вкладку CLI и введите следующие команды:

East> show ip interface brief

Выходные данные подтверждают правильное количество интерфейсов и их обозначение. Интерфейс vlan1 является виртуальным и существует только в программном обеспечении. Сколько физических интерфейсов перечислено?

d. Введите следующие команды:

East> show interface gigabitethernet 0/0 Какая пропускная способность задана по умолчанию для данного интерфейса?

East> show interface serial 0/0/0

Какая пропускная способность задана по умолчанию для данного интерфейса?

Шаг 3: Определите слоты расширения для модулей в коммутаторах. a. Сколько портов расширения доступно для установки дополнительных модулей в маршрутизаторе East? b. Щёлкните Switch2 или Switch3. Сколько слотов расширения доступно?

**Часть 2: Подключение устройств**

a. Выберите соответствующий тип кабеля.

b. Щёлкните первое устройство и выберите указанный интерфейс.

c. Щёлкните второе устройство и выберите указанный интерфейс.

d. Если вы правильно подключили два устройства, вы увидите, что ваша оценка увеличилась.

| Устройство | Интерфейс | Тип кабеля | Устройство | Интерфейс |
|---|---|---|---|---|
| East | GigabitEthernet0/0 | Прямой медный кабель | Коммутатор1 | GigabitEthernet0/1 |
| East | GigabitEthernet0/1 | Прямой медный | Коммутатор4 | GigabitEthernet0/1 |

| | | | | |
|---|---|---|---|---|
| | | кабель | | |
| East | FastEthernet0/1/0 | Прямой медный кабель | ПК1 | FastEthernet0 |
| East | FastEthernet0/1/1 | Прямой медный кабель | ПК2 | FastEthernet0 |
| East | FastEthernet0/1/2 | Прямой медный кабель | ПК3 | FastEthernet0 |
| Коммутатор1 | FastEthernet0/1 | Прямой медный кабель | ПК4 | FastEthernet0 |
| Коммутатор1 | FastEthernet0/2 | Прямой медный кабель | ПК5 | FastEthernet0 |
| Коммутатор1 | FastEthernet0/3 | Прямой медный кабель | ПК6 | FastEthernet0 |
| Коммутатор4 | GigabitEthernet0/2 | Перевёрнутый медный кабель | Коммутатор3 | GigabitEthernet3/1 |
| Коммутатор3 | GigabitEthernet5/1 | Оптоволоконный кабель | Коммутатор2 | GigabitEthernet5/1 |
| Коммутатор2 | FastEthernet0/1 | Прямой медный кабель | ПК7 | FastEthernet0 |
| Коммутатор2 | FastEthernet1/1 | Прямой медный кабель | ПК8 | FastEthernet0 |
| Коммутатор2 | FastEthernet2/1 | Прямой медный кабель | ПК9 | FastEthernet0 |
| East | Serial0/0/0 | Последовательный DCE (подключается сначала к East) | West | Serial0/0/0 |

**Оформите отчет, сделайте вывод по работе.**

## Лабораторная работа № 5
## Тема: Изучение транспортного уровня

**Цель работы: выполнить наблюдение за процессом трёхстороннего рукопожатия TCP с помощью программы Wireshark**

Необходимые ресурсы

1 ПК (Windows 10 с доступом к командной строке, доступу к Интернету и установленному анализатору пакетов Wireshark)

Топология

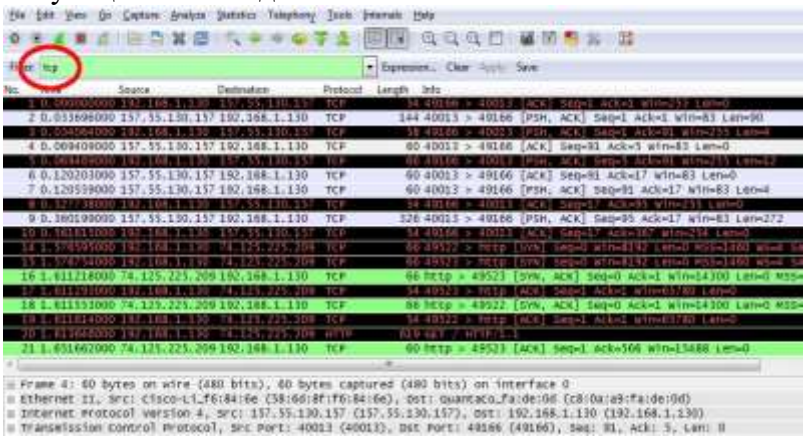

**Часть 1. Подготовка программы Wireshark к захвату пакетов**

– Выберите подходящий интерфейс сетевого адаптера для захвата пакетов.

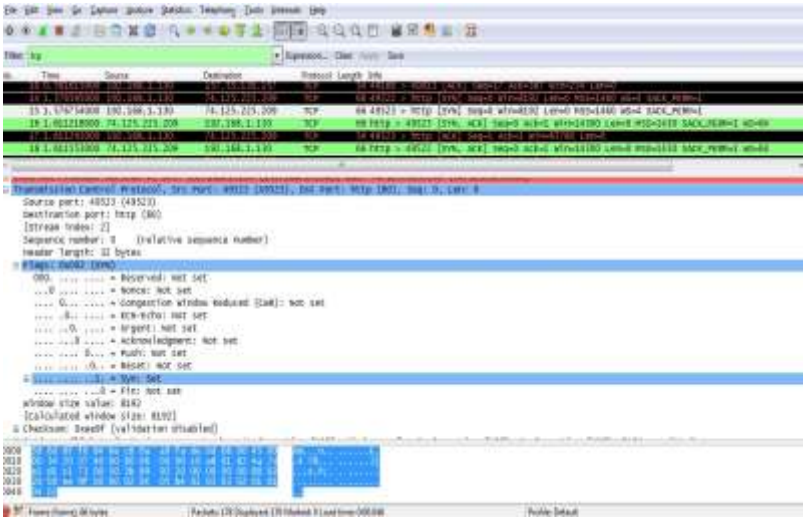
**Часть 2. Захват, поиск и изучение пакетов**

– Захватите данные веб-сеанса на узле www.google.com.

Найдите соответствующие пакеты для веб-сеанса.



– Изучите содержащиеся в пакетах данные, включая IP-адреса, номера портов TCP и флажки управления TCP.



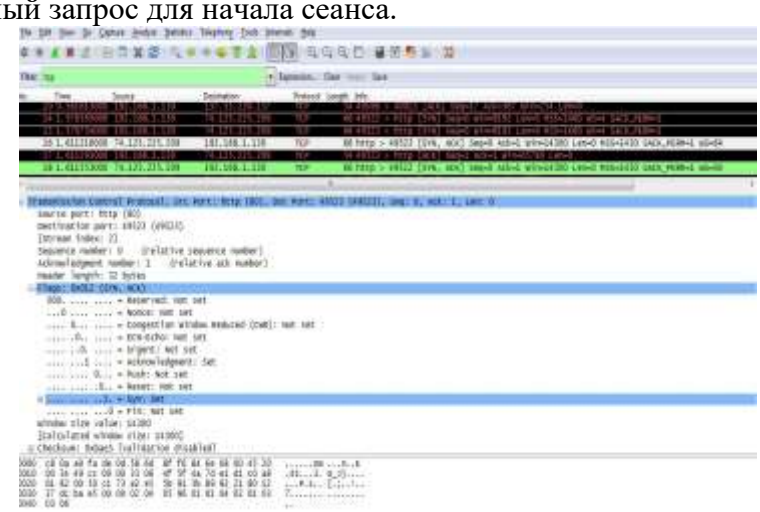
Назовите номер порта источника TCP. Как бы вы классифицировали порт источника?

Назовите номер порта назначения TCP.

Как бы вы классифицировали порт назначения? Какие установлены флажки?

На какое значение настроен относительный последовательный номер?

Чтобы выбрать следующий кадр в трёхстороннем рукопожатии, в меню программы Wireshark выберите параметр **Go** (Перейти), а затем **Next Packet In Conversation** (Следующий пакет коммуникации). В данном примере это кадр 16. Это ответ веб-сервера Google на исходный запрос для начала сеанса.



Назовите значения портов источника и назначения.

Какие установлены флажки?
На какие значения настроены относительный последовательный номер и номер подтверждения?
**Сделайте вывод по работе, выполните отчет.**

## Лабораторная работа № 6
## Тема: Настройка IP-адресации. Использование калькулятора Windows в работе с сетевыми адресами

**Цель работы: получит практические навыки по настройке IP-адресации, в использовании калькулятора Windows в работе с сетевыми адресами**

Необходимые ресурсы • Один ПК (Windows 10)

**Част 1. Использование калькулятора Windows в работе с сетевыми адресами**

a. Сотрите значение в окне, нажав на кнопку **C** над цифрой 9 на клавиатуре калькулятора.

Переведите в двоичную, десятичную и шестнадцатеричную системы счисления следующие числа:

| Десятичное | Двоичное | Шестнадцатеричное |
|---|---|---|
| 86 | | |
| 175 | | |
| 204 | | |
| | 0001 0011 | |
| | 0100 1101 | |
| | 0010 1010 | |
| | | 38 |
| | | 93 |
| | | E4 |

b. Заполняя приведённую выше таблицу, заметили вы что-либо общее между двоичными и шестнадцатеричными числами?

c. Чтобы вычислить количество узлов в сети, необходимо определить сетевую и узловую части адреса.

d. Адрес и маска подсети переводятся в двоичные числа на примере адреса 192.168.1.10 с подсетью 255.255.248.0. Записывая результаты перевода данных в двоичные числа, выставляйте биты.

| IP-адрес и маска подсети в десятичном формате | IP-адрес и маска подсети в двоичном формате |
|---|---|
| 192.168.1.10 | |
| 255.255.248.0 | |

e. Для данной маски подсети определите количество доступных узлов и запишите ответ в приведённую ниже таблицу.

| Маска подсети | Двоичная маска подсети | Количество доступных узловых битов | Количество доступных узлов |
|---|---|---|---|
| 255.255.255.0 | 11111111.11111111.11111111.00000000 | | |
| 255.255.240.0 | 11111111.11111111.11110000.00000000 | | |
| 255.255.255.128 | 11111111.11111111.11111111.10000000 | | |
| 255.255.255.252 | 11111111.11111111.11111111.11111100 | | |
| 255.255.0.0 | 11111111.11111111.00000000.00000000 | | |

Част 2. Использование побитовой операции И для определения сетевых адресов

f. Введите отсутствующую информацию в таблицу ниже:

| Описание | Десятичное | Двоичное |
|---|---|---|
| IP-адрес | 10.172.2.8 | |
| Маска подсети | 255.224.0.0 | |
| Сетевой адрес | | |

**Сделайте вывод по работе, выполните отчет.**

## Лабораторная работа № 7

## Тема: Сегментация IP-сетей. Изучение калькуляторов подсетей

**Цель работы: получить практические навыки по сегментации IP-сетей. Изучеть возможности калькуляторов подсетей**

Необходимые ресурсы Устройство с выходом в Интерне

**Часть 1: Обзор доступных калькуляторов подсетей**

– Рассмотрите некоторые программы для расчёта данных подсетей.

– Воспользуйтесь веб-калькулятором подсетей.

**Часть 2: Расчёт сетевых данных с помощью калькулятора подсетей**

**Шаг 1: Заполните приведённую ниже таблицу для адреса 10.223.23.136/10.**

| Описание | Десятичное | Двоичное |
|---|---|---|
| Адрес | 10.223.23.136 | |
| Маска подсети | | |
| Сетевой адрес | | |
| Широковещательный адрес | | |
| Адрес первого узла | | |
| Адрес последнего узла | | |
| Число доступных узлов | | Недоступно |

Общий или частный тип адреса?

**Шаг 2: Заполните приведённую ниже таблицу для адреса 172.18.255.92 с маской подсети 255.255.224.0.**

| Описание | Десятичное | Двоичное |
|---|---|---|
| Адрес | 172.18.255.92 | |
| Маска подсети | 255.255.224.0 | |
| Сетевой адрес | | |
| Широковещательный адрес | | |
| Адрес первого узла | | |
| Адрес последнего узла | | |
| Число доступных узлов | | Недоступно |

Какова в данной сети префиксная запись CIDR? Общий или частный тип адреса?

**Сделайте вывод по работе, выполните отчет.**

## Лабораторная работа № 8

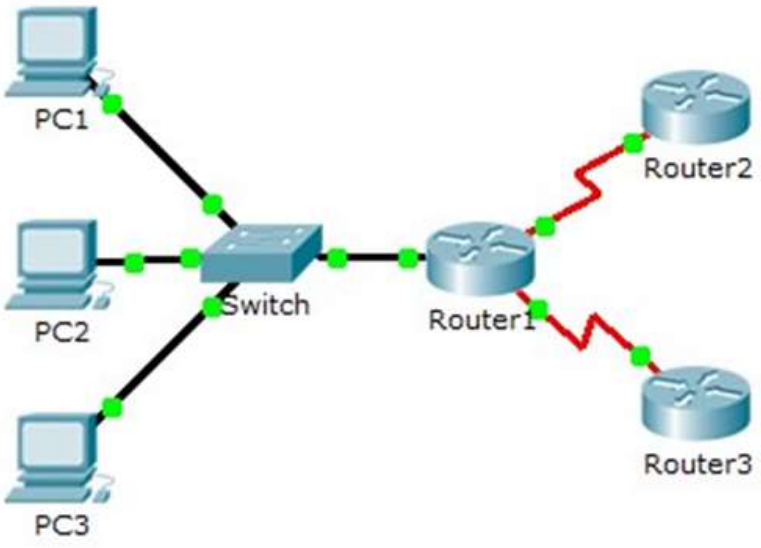
## Тема: IP-адресация. Анализ трафика одноадресной передачи, широковещательной и многоадресной рассылки

**Цель работы: получить практические навыки по работе с программой Packet Tracer: выполнение анализа трафика одноадресной передачи, широковещательной и многоадресной рассылки**

Необходимые ресурсы

1 ПК (Windows 10 с доступом к командной строке, доступу к Интернету и с программой Packet Tracer)

Топология:




**Часть 1. Генерирование трафика одноадресной передачи**

Шаг 1: Использование команды ping для генерирования трафика.

a. Щёлкните ПК1, откройте вкладку Desktop (рабочий стол) и выберите Command Prompt (командная строка).

b. Выполните команду ping 10.0.3.2. Команда ping должна быть успешно выполнена.
. Все права защищены.
Шаг 2: Переход в режим моделирования.
a. Откройте вкладку Simulation (Моделирование), чтобы перейти в режим моделирования.
b. Нажмите кнопку Edit Filters и убедитесь, что выбраны только события ICMP и EIGRP.
c. Щёлкните ПК1 и выполните команду ping 10.0.3.2.
Шаг 3: Анализ трафика одноадресной передачи.
Пакет PDU на ПК1 — это эхо-запрос ICMP, предназначенный для последовательного интерфейса на маршрутизаторе Router3.
a. Нажмите кнопку Capture/Forward ещё раз и посмотрите, как эхо-запрос отправляется на маршрутизатор Router3 и эхо-отклик возвращается на ПК1. Остановите моделирование, когда первый ответ поступит на ПК1.
Через какие устройства прошёл пакет в ходе индивидуальной рассылки?

**Часть 2. Генерирование трафика широковещательной рассылки.**

**Анализ трафика многоадресной рассылки**

**Шаг 1: Добавление сложного PDU.**

a. Нажмите кнопку **Add Complex PDU** (Добавить сложный PDU). Значок этого пакета находится на правой панели инструментов и имеет вид открытого конверта.
b. Наведите указатель мыши на топологию, и курсор примет вид конверта со знаком плюс (+).
c. Щёлкните **ПК1**, который будет источником для этого тестового сообщения. Откроется диалоговое окно **Create Complex PDU** (Создание сложного PDU). Введите следующие значения:

- Destination IP Address: **255.255.255.255** (адрес широковещательной рассылки)
- Sequence Number: 1
- One Shot Time: **0**

В параметрах PDU значение по умолчанию для **Select Application:** PING. Какие другие приложения (как минимум 3) доступны для использования?
d. Нажмите кнопку **Create PDU** (Создать PDU). Этот тестовый пакет широковещательной рассылки теперь появится в списке событий на **панели моделирования**. Он также будет показан в окне PDU List.
e. Два раза нажмите кнопку **Capture/Forward** (Захватить/Переслать). Этот пакет отправляется на коммутатор, а затем широковещательно рассылается на **ПК2**, **ПК3** и **Router1**. Изучите сведения уровня 3 для всех событий. Обратите внимание, что IP-адрес назначения — 255.255.255.255. Это широковещательный адрес, который был настроен при создании сложного PDU.
Проанализируйте данные модели OSI и скажите, какие изменения происходят в данных на уровне 3 в столбце «Out Layers» на узлах Router1, ПК2 и ПК3?
f. Нажмите кнопку **Capture/Forward** (Захватить/Переслать) ещё раз. Пересылается ли широковещательный PDU на маршрутизатор Router2 или Router3? Почему?
g. После анализа поведения широковещательной рассылки удалите тестовый пакет, нажав кнопку **Delete** под **Scenario 0**.

**Шаг 2: Проверка трафика, созданного протоколами маршрутизации.**

a. Нажмите кнопку **Capture/Forward**. Пакеты EIGRP на маршрутизаторе Router1 ожидают отправки в многоадресной рассылке на всех интерфейсах.
b. Изучите содержимое этих пакетов, открыв окно PDU Information, и нажмите ещё раз кнопку **Capture/Forward**. Пакеты отправляются на два других маршрутизатора и на коммутатор. Маршрутизаторы принимают и обрабатывают пакеты, поскольку они входят в группу мультивещания. Коммутатор перешлёт пакеты на компьютеры.

**Сделайте вывод по работе, выполните отчет.**

**Лабораторная работа № 9**

**Тема: Сегментация IP-сетей. Организация подсети по различным сценариям**

**Цель работы: получить практические навыки по работе с программой Packet Tracer: организация подсети по различным сценариям**

Необходимые ресурсы

1 ПК (Windows 10 с доступом к командной строке, доступу к Интернету и с программой Packet Tracer)

**Топология:**

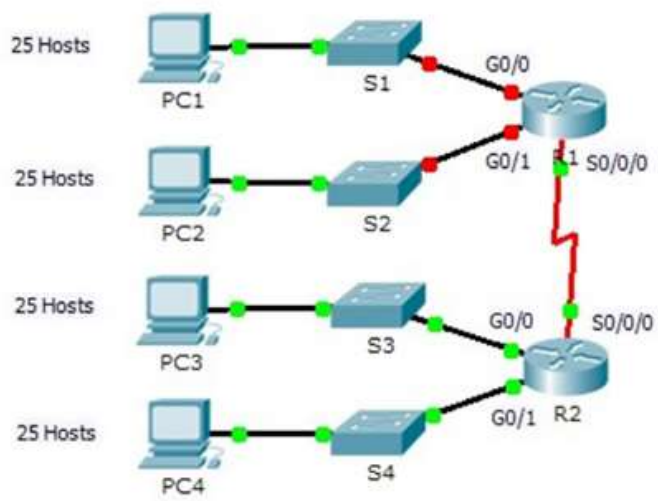



Таблица адресации

| Устройство | Интерфейс | IP-адрес | Маска подсети | Шлюз по умолчанию |
|---|---|---|---|---|
| R1 | G0/0 | | | |
| | G0/1 | | | |
| | S0/0/0 | | | |
| R2 | G0/0 | | | |
| | G0/1 | | | |
| | S0/0/0 | | | |
| S1 | VLAN 1 | | | |
| S2 | VLAN 1 | | | |
| S3 | VLAN 1 | | | |
| S4 | VLAN 1 | | | |
| ПК1 | Сетевой адаптер | | | |
| ПК2 | Сетевой адаптер | | | |
| ПК3 | Сетевой адаптер | | | |
| ПК4 | Сетевой адаптер | | | |

**Часть 1: Разработка схемы IP-адресации**

**Шаг 1: Разбиение сети 192.168.100.0/24 на нужное количество подсетей.**

a. В соответствии с имеющейся топологией сколько потребуется подсетей? Сколько необходимо заимствовать битов для поддержки нескольких подсетей в таблице топологии?

b. Сколько в результате этого создаётся подсетей?

c. Сколько при этом в каждой подсети будет доступно пригодных к использованию узлов?

d. Рассчитайте двоичное значение для первых пяти подсетей. Первая подсеть уже показана.

Net 0: 192 . 168 . 100 . 0 0 0 0 0 0 0 0

Net 1: 192 . 168 . 100 . ___ ___ ___ ___ ___ ___ ___ ___

Net 2: 192 . 168 . 100 . ___ ___ ___ ___ ___ ___ ___ ___

Net 3: 192 . 168 . 100 . ___ ___ ___ ___ ___ ___ ___ ___

Net 4: 192 . 168 . 100 . ___ ___ ___ ___ ___ ___ ___ ___ Рассчитайте двоичное и десятичное значение новой маски подсети.

11111111.11111111.11111111. ___ ___ ___ ___ ___ ___ ___ ___

255 . 255 . 255 . _____

e. Заполните **таблицу подсетей**, перечислив десятичные значения всех доступных подсетей, первый и последний используемый адрес узла и широковещательный адрес. Повторяйте действие до отображения всех адресов.

**Таблица подсети**

| Номер подсети | Адрес подсети | Первый используемый адрес узла | Последний используемый адрес узла | Широковещательный адрес |
|---|---|---|---|---|
| 0 | | | | |
| **1** | | | | |
| **2** | | | | |
| **3** | | | | |
| **4** | | | | |

**Шаг 2: Назначьте подсети для сети, отображаемой в топологии.**

a. Назначьте подсеть 0 локальной сети, подключённой к интерфейсу GigabitEthernet 0/0 маршрутизатора R1: _____

b. Назначьте подсеть 1 локальной сети, подключённой к интерфейсу GigabitEthernet 0/1 маршрутизатора R1: _____

c. Назначьте подсеть 2 локальной сети, подключённой к интерфейсу GigabitEthernet 0/0 маршрутизатора R2: _____

d. Назначьте подсеть 3 локальной сети, подключённой к интерфейсу GigabitEthernet 0/1 маршрутизатора R2: _____

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

**Шаг 3: Задокументируйте схему адресации.**

Заполните **таблицу адресации**, используя следующие рекомендации.

**Часть 2: Назначение сетевым устройствам IP-адресов и проверка подключения**

Основная часть IP-адресации на данной сети уже настроена. Выполните следующие шаги для завершения настройки адресации.

**Шаг 1: Настройка IP-адресации на интерфейсах локальной сети маршрутизатора R1.**

**Шаг 2: Настройте IP-адресацию на S3, включая шлюз по умолчанию.**

**Шаг 3: Настройте IP-адресацию на ПК4, включая шлюз по умолчанию.**

**Шаг 4: Проверка подключения.**

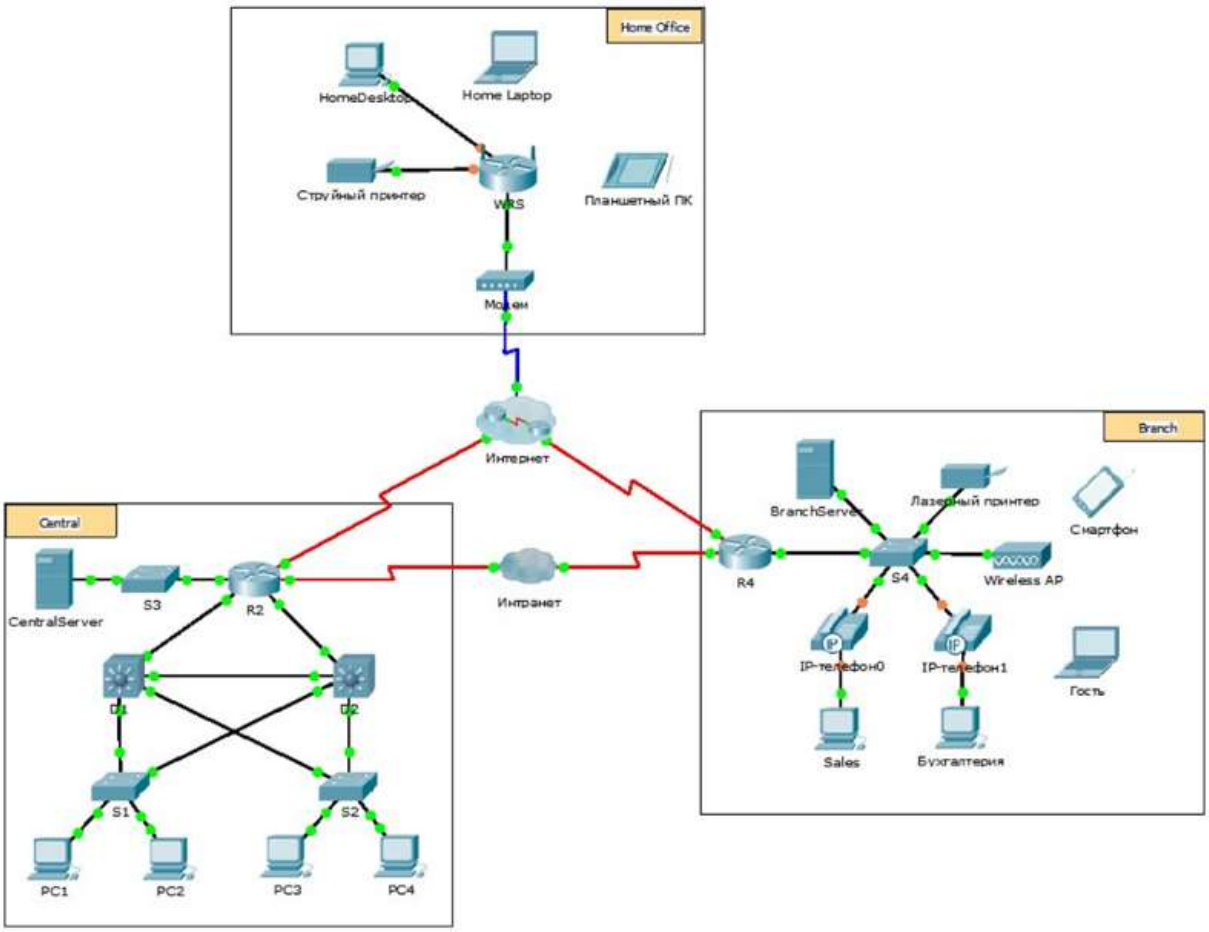
**Сделайте вывод по работе, выполните отчет.**

**Лабораторная работа № 10**
**Тема: Изучение основных сетевых служб**

**Цель работы: получить практические навыки работы с программой Packet Tracer по изучению основных сетевых служб: веб-серверы и почтовые серверы**

Необходимые ресурсы
1 ПК (Windows 10 с доступом к командной строке, доступу к Интернету и с программой Packet Tracer)

Топология




**Часть 1: Настройка и проверка веб-служб**

**Шаг 1: Настройка веб-служб на CentralServer и BranchServer.**

a. Щёлкните **CentralServer**, откройте вкладку **Config** (Настройка) и выберите раздел **HTTP**.

b. Выберите вариант **On**, чтобы включить HTTP и HTTPS.

c. Дополнительно: Измените HTML-код.

d. Повторите шаги с 1a по 1в на веб-сайте **BranchServer**.

**Шаг 2: Проверьте работоспособность веб-серверов, открыв их веб-страницы.**

В этой сети много оконечных устройств, но согласно задачам данного шага используйте **PC3**.

a. Щёлкните **PC3**, откройте вкладку **Desktop** (Рабочий стол) и выберите раздел **Web Browser** (Веббраузер).

b. В поле URL введите IP-адрес **10.10.10.2** и нажмите кнопку **Go**. Откроется веб-сайт **CentralServer**.

c. В поле URL введите IP-адрес **64.100.200.1** и нажмите кнопку **Go**. Откроется веб-сайт **BranchServer**.
d. В поле URL введите **centralserver.pt.pka** нажмите кнопку **Go**. Откроется веб-сайт **CentralServer**.
e. В поле URL введите **branchserver.pt.pka** нажмите кнопку **Go**. Откроется веб-сайт **BranchServer**.
f. Какой протокол преобразует имена **centralserver.pt.pka** и **branchserver.pt.pka** в IP-адреса?

**Часть 2: Настройка и проверка служб электронной почты на серверах**

**Шаг 1: Настройка CentralServer для отправки (SMTP) и получения сообщений электронной почты (POP3).**

a. Щёлкните **CentralServer**, откройте вкладку **Config** (Настройка) и нажмите кнопку **EMAIL**.
b. Выберите вариант **On**, чтобы включить SMTP и POP3.
c. Назначьте имя домена **centralserver.pt.pka** и нажмите кнопку **Set**.
d. Создайте пользователя с именем **central-user** и паролем **cisco**. Нажмите **+**, чтобы добавить пользователя.

**Шаг 2: Настройка BranchServer для отправки (SMTP) и получения сообщений электронной почты (POP3).**

a. Щёлкните **BranchServer**, откройте вкладку **Config** (Настройка) и выберите раздел **EMAIL**.
b. Выберите вариант **On**, чтобы включить SMTP и POP3.
c. Назначьте имя домена **branchserver.pt.pka** и нажмите кнопку **Set**.
d. Создайте пользователя с именем **branch-user** и паролем **cisco**. Нажмите **+**, чтобы добавить пользователя.

**серверы и почтовые серверы**

**Шаг 3: Настройте PC3 для использования службы электронной почты CentralServer.**

a. Щёлкните **PC3**, откройте вкладку **Desktop** (Рабочий стол) и выберите раздел **E Mail** (Электронная почта).
b. Введите следующие значения в соответствующие поля.
1) Ваше имя: **Central User**
2) Адрес электронной почты: **central-user@centralserver.pt.pka**
3) Сервер входящей почты: **10.10.10.2**
4) Сервер исходящей почты: **10.10.10.2**
5) Имя пользователя: **central-user**
6) Пароль: **cisco**
c. Нажмите кнопку **Save** (Сохранить). Отобразится окно почтового клиента.
d. Нажмите кнопку **Receive** (Получить). Если все настройки клиента и сервера выполнены правильно, в окне почтового клиента появится сообщение о подтверждении Receive Mail Success (Почта успешно получена).

**Сделайте вывод по работе, выполните отчет.**

## Лабораторная работа № 11
## Тема: Обеспечение безопасности сети

**Цель работы: получить практические навыки по работе с программой Packet Tracer: выполнение настройки протокола SSH**

Необходимые ресурсы
1 ПК (Windows 10 с доступом к командной строке, доступу к Интернету и с программой Packet Tracer)

Топология:

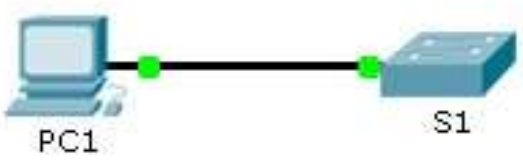



**Таблица адресации**

| Устройство | Интерфейс | IP-адрес | Маска подсети |
|---|---|---|---|
| S1 | VLAN 1 | 10.10.10.2 | 255.255.255.0 |
| PC1 | NIC | 10.10.10.10 | 255.255.255.0 |

**Часть 1. Настройка шифрования паролей**

a. С помощью командной строки на узле **PC1**, подключитесь к коммутатору **S1** через Telnet. Пароль для пользовательского и привилегированного доступа — **cisco**.

b. Сохраните текущую конфигурацию, чтобы любые допущенные вами ошибки можно было отменить, отключив питание коммутатора **S1**.

c. Отобразите текущую конфигурацию и обратите внимание на то, что пароли написаны в виде открытого текста. Введите команду, позволяющую шифровать незашифрованные пароли**:** d. Убедитесь, что пароли зашифрованы.

**Часть 2. Обеспечение защищенной коммуникации**

**Шаг 1: Настройте имя домена IP и создайте ключи шифрования.**

В принципе, использование Telnet небезопасно, поскольку текстовые данные передаются в незашифрованном виде. Поэтому рекомендуется по возможности использовать протокол SSH.

**Packet Tracer. Настройка протокола SSH**

a. Присвойте домену имя **netacad.pka.**

b. Для шифрования данных требуются ключи шифрования Создайте RSA ключи длиной 1024 бит.

**Шаг 2: Создайте пользователя SSH и перенастройте линии VTY на доступ только по протоколу SSH.**

a. Создайте пользователя-администратора (**administrator**) с паролем **cisco**.

b. Настройте линии VTY для проверки регистрационных данных в локальных базах данных имён пользователей, а также для разрешения удалённого доступа только по протоколу SSH. Удалите существующий пароль линии VTY.

**Шаг 3. Проверка реализации протокола SSH**

a. Завершите сеанс работы Telnet и попробуйте снова войти в систему через Telnet. Попытка должна завершиться неудачей.

b. Попробуйте войти в систему через протокол SSH. Введите **ssh** и нажмите **ВВОД**, не добавляя какие-либо параметры, чтобы отобразить инструкции использования команды.

**Сделайте вывод по работе, выполните отчет.**

## Лабораторная работа № 12

### Тема: Анализ компьютерной сети и настройка маршрутизатора

**Цель работы: получить практические навыки по работе с программой Packet Tracer: Выполнение настройки маршрутизатора Linksys**

Необходимые ресурсы

1 ПК (Windows 10 с доступом к командной строке, доступу к Интернету и с программой Packet Tracer)

**Топология:**


**Часть 1: Подключение к маршрутизатору Linksys**

**Шаг 1: Настройка и проверка соединения к маршрутизатору Linksys.**

a. Подключите соответствующий кабель с **Host-A** к порту Ethernet 1 на **Linksys**.

b. Дождитесь, когда индикатор связи загорится зелёным цветом. Затем откройте окно командной строки узла **Host-A**. С помощью команды **ipconfig** проверьте IP-адрес, **выданный узлу Host**.

c. С помощью команды **ping 192.168.0.1** проверьте, имеет ли узел **Host-A** доступ к шлюзу по умолчанию.

**Шаг 2: Доступ к графическому интерфейсу пользователя Linksys в веб-браузере.**

a. Для настройки маршрутизатора **Linksys** с помощью графического интерфейса пользователя нужно открыть его в **веб-браузере**. Откройте веб-браузер и выполните доступ к **Linksys**, введя в адресной строке адрес шлюза по умолчанию.

b. Введите имя пользователя **admin** и аналогичный пароль для доступа к маршрутизатору **Linksys**.

**Примечание.** Вы не увидите изменение своей оценки при настройке маршрутизатора **Linksys** до тех пор, пока не нажмёте кнопку **Save settings** (Сохранить настройки).

**Часть 2: Включение беспроводного подключения**

**Шаг 1: Настройка подключения к Интернету на маршрутизаторе Linksys.**

В этом сценарии нет подключения к Интернету, но несмотря на это, вам необходимо будет настроить параметры интерфейса, подключённого к Интернету. Для параметра **Internet Connection Type** (Тип подключения к Интернету) выберите значение **Static IP** (Статический IP-адрес) в раскрывающемся списке. Затем введите следующие данные IP-адреса:

- IP-адрес в Интернете — **198.133.219.1**;
- маска подсети — **255.255.255.0**; • шлюз по умолчанию — **198.133.219.254**;
- DNS 1 — **198.133.219.10**.

**Шаг 2: Настройте параметры внутренней сети.**

Прокрутите страницу вниз до раздела **Network Setup** (Настройка сети) и настройте следующие параметры:

- IP-адрес — **172.31.1.1**;
- маска подсети — **255.255.255.224**;
- начальный IP-адрес — для последнего октета введите значение **5**;
- максимальное количество пользователей — **25**.

**Шаг 3: Сохраните настройки и повторно подключитесь к маршрутизатору Linksys.**

a. Прокрутите страницу вниз до конца и нажмите кнопку **Save Settings** (Сохранить параметры). При переходе между вкладками без сохранения настроенные параметры будут потеряны.

b. Соединение будет разорвано, если вы нажмёте кнопку **Save Settings**. Это произошло потому, что вы изменили IP-адрес маршрутизатора.

c. Вернитесь в окно командной строки **Host-A**. Выполните команду **ipconfig /renew**, чтобы обновить IP-адрес.

d. В веб-браузере **Host-A** повторно подключитесь к **Linksys**. Вы должны будете использовать новый адрес шлюза по умолчанию. Проверьте параметры **Internet Connection** (Подключение к Интернету) на вкладке **Status** (Состояние). Параметры должны иметь значения, настроенные в части 2, шаг 1. Если значения не совпадают, повторите часть 2, шаг 1 и шаг 2.

**Шаг 4: Настройка беспроводной сети для беспроводных устройств.**

a. Откройте вкладку **Wireless** (Беспроводные сети) и изучите параметры в раскрывающемся списке **Network Mode** (Режим сети).

b. Установите режим сети **Wireless-N Only** (Только Wireless-N).

c. Измените SSID на **MyHomeNetwork.**

d. Когда беспроводной клиент опрашивает зону вокруг себя в поиске беспроводных сетей, он находит все широковещательные рассылки SSID. Широковещательные рассылки SSID включены по умолчанию.

e. Чтобы обеспечить наилучшую производительность сети с использованием Wireless-N, установите диапазон частот **Wide-40MHz.**

f. Нажмите кнопку **Save Settings**, а затем — **Continue**.

**Шаг 5: Настройте систему безопасности, чтобы клиенты прошли аутентификацию для подключения к беспроводной сети.**

a. Щёлкните параметр **Wireless Security** под вкладкой **Wireless**.

b. Установите для параметра **Security Mode** значение **WPA2 Personal**.

c. Выполните выход из режима шифрования AES и введите парольную фразу **itsasecret**.

d. Нажмите кнопку **Save Settings**, а затем — **Continue**.

**Шаг 6: Изменение пароля по умолчанию для доступа к конфигурации Linksys.**

a. Всегда изменяйте пароль по умолчанию. Откройте вкладку **Administration** и измените пароль **Router Access** на **letmein**.

b. Нажмите кнопку **Save Settings**. Введите имя пользователя **admin** и новый пароль.

**Шаг 7: Настройка ноутбука для доступа к беспроводной сети.**

a. Щёлкните **Laptop** и выберите **Desktop** > **PC Wireless**. Открывшееся окно — это графический пользовательский интерфейс Linksys для клиента.

b. Откройте вкладку **Connect** и нажмите кнопку **Refresh**, если необходимо. Вы должны увидеть **MyHomeNetwork** в поле «Wireless Network Name» (Название беспроводной сети).

c. Щёлкните **MyHomeNetwork** и выберите команду **Connect**.

d. Теперь вы должны увидеть сеть **MyHomeNetwork**. Щёлкните эту сеть и выберите команду **Connect**.

e. **Pre-shared Key** — пароль, настроенный в части 2, шаг 5c. Введите пароль и нажмите кнопку **Connect**.

f. Закройте интерфейс пользователя Linksys и щёлкните **Command Prompt**. Выполните команду **ipconfig**, чтобы убедиться, что **Laptop** получил IP-адрес.

**Шаг 8: Проверка связи между узлами Laptop и Host-A.**

a. Отправьте эхо-запрос маршрутизатору **Linksys** с узла **Laptop**.

b. Отправьте эхо-запрос узлу **Host-A** с **Laptop**.

**Сделайте вывод по работе, выполните отчет.**

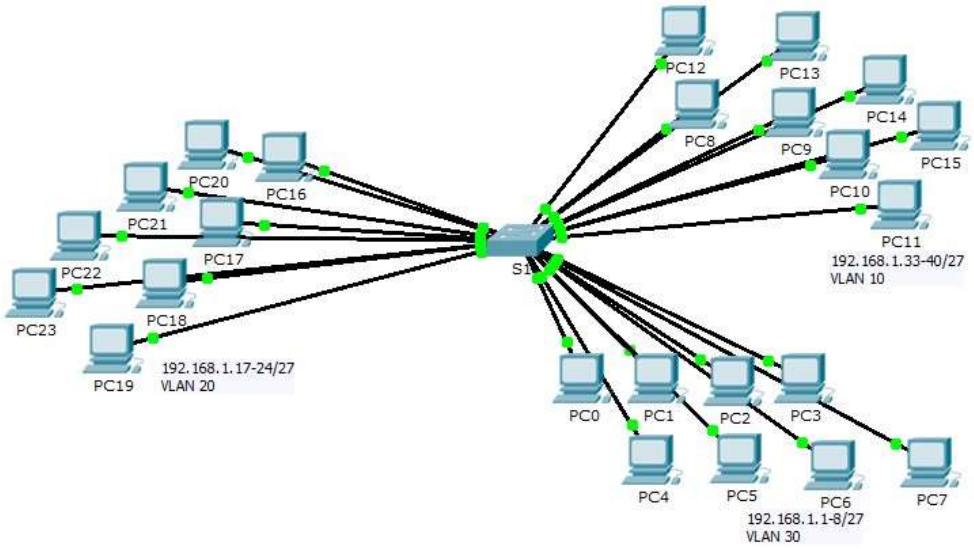
## Лабораторная работа № 13
## Тема: Настройка коммутатора

**Цель работы: получить практические навыки по работе с программой Packet Tracer: анализ широковещательных сообщений, проходящих через коммутатор**

Необходимые ресурсы

1 ПК (Windows 10 с доступом к командной строке, доступу к Интернету и с программой Packet Tracer)

**Топология:**




**Часть 1. Наблюдение за трафиком широковещательной рассылки в сети VLAN**
**Шаг 1: Для создания трафика используйте отправку эхо-запросов.**

a. Нажмите на **PC0** и выберите вкладку Desktop (**Рабочий стол**) > Command Prompt (**Командная строка**).

b. Введите команду **ping 192.168.1.8**. Эхо-запрос должен быть успешным.

В отличие от сети LAN сеть VLAN представляет собой домен широковещательной рассылки, создаваемый коммутаторами. Используя режим **Simulation (Моделирование)** в Packet Tracer, **Packet Tracer. Получатели широковещательных сообщений** отправьте эхо-запрос на оконечные устройства в пределах их сети VLAN. Ответьте на вопросы шага 2, основываясь на своих наблюдениях.

**Шаг 2: Создайте и проверьте широковещательный трафик.**

a. Перейдите в режим **Simulation (Моделирование).**

b. Нажмите кнопку **Edit Filters (Редактировать фильтры)** в Simulation Panel (Панель моделирования). Снимите флажок с пункта Show All/None (**Показывать все/ничего**). Установите флажок в поле **ICMP**.

c. Выберите инструмент **Add Complex PDU (Создать сложный PDU)** — это значок открытого конверта на панели справа.

d. Наведите курсор на топологию — стрелка курсора будет отображаться в виде конверта со знаком «плюс» (+).

e. Нажмите на **PC0**, чтобы он выполнял роль источника для данного тестового сообщения. После этого откроется диалоговое окно Add Complex PDU (**Создать сложный PDU**). Введите следующие значения:

- IP-адрес узла-назначения: 255.255.255.255 (широковещательный адрес)
- Порядковый номер: 1
- Время однократного события: 0

По умолчанию **Select Application** (Выбрать приложение) в настройках PDU настроен на PING. Назовите не менее трёх других доступных приложений.

f. Нажмите на **Create PDU(Создать PDU)**. Этот тестовый пакет широковещательной рассылки теперь появится в **Simulation Panel Event List (Список событий панели моделирования).** Пакет также отобразится в окне списка PDU. Это первый фрагмент PDU Сценария 0.

g. Нажмите дважды на **Capture/forward (Захват/Вперед)**. Что произошло с пакетом?

h. Повторите действия для **PC8** и **PC16**.

**Часть 2. Вопросы**

1. Если компьютер в сети VLAN 10 отправляет широковещательное сообщение, какие устройства его получат?
2. Если компьютер в сети VLAN 20 отправляет широковещательное сообщение, какие устройства его получат?
3. Если компьютер в сети VLAN 30 отправляет широковещательное сообщение, какие устройства его получат?
4. Что происходит с кадром, отправленным с компьютера сети VLAN 10 на компьютер сети VLAN 30?

**Сделайте вывод по работе, выполните отчет.**

## Лабораторная работа № 14
## Тема: Конфигурация сетей VLAN

**Цель работы: получить практические навыки по работе с программой Packet Tracer: выполнение поиска и устранения неполадок в реализации сети VLAN, а так же документирования сети**

Необходимые ресурсы

1 ПК (Windows 10 с доступом к командной строке, доступу к Интернету и с программой Packet Tracer)

**Топология**

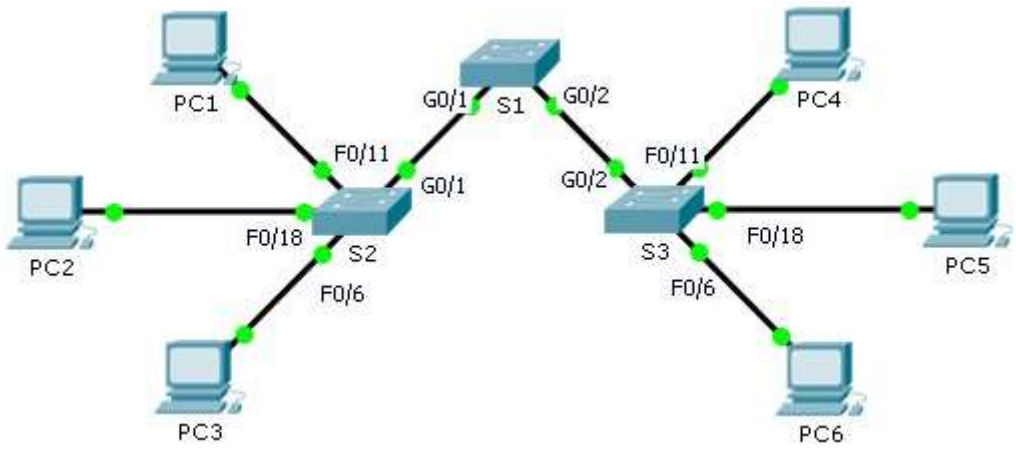



**Таблица адресации**

| Устройство | Интерфейс | IPv4-адрес | Маска подсети | Порт коммутатора | VLAN |
|---|---|---|---|---|---|
| PC1 | NIC | 172.17.10.21 | 255.255.255.0 | S1 F0/11 | 10 |
| PC2 | NIC | 172.17.20.22 | 255.255.255.0 | S1 F0/18 | 20 |
| PC3 | NIC | 172.17.30.23 | 255.255.255.0 | S1 F0/6 | 30 |
| PC4 | NIC | 172.17.10.24 | 255.255.255.0 | S2 F0/11 | 10 |
| PC5 | NIC | 172.17.20.25 | 255.255.255.0 | S2 F0/18 | 20 |
| PC6 | NIC | 172.17.30.26 | 255.255.255.0 | S2 F0/6 | 30 |

**Часть 1. Проверка подключения между компьютерами в одной и той же сети VLAN**

Из командной строки на каждом компьютере отправьте эхо-запрос на компьютеры в одной сети VLAN.

a. Успешно ли отправляется эхо-запрос от PC1 на PC4? _____

b. Успешно ли отправляется эхо-запрос от PC2 на PC5? _____
c. Успешно ли отправляется эхо-запрос от PC3 на PC6? _____

**Шаг 1: Проверьте конфигурацию на компьютерах.**

Убедитесь в правильности настроек каждого компьютера.

- IP-адрес
- Маска подсети

**Шаг 2: Проверьте конфигурацию на коммутаторах.**

Убедитесь в правильности настроек коммутаторов.

- Порты назначены верным сетям VLAN.
- Порты настроены в соответствующем режиме.
- Порты подключены к соответствующим устройствам.

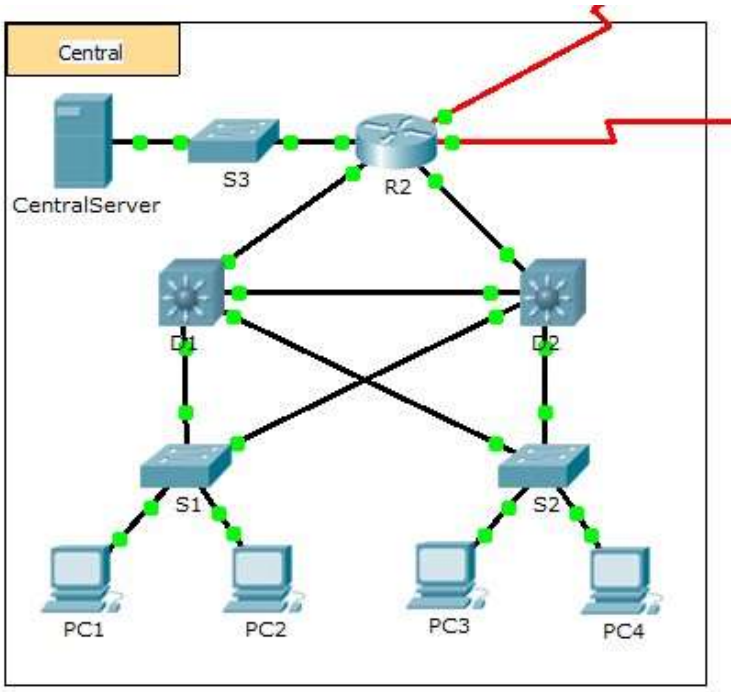
**Сделайте вывод по работе, выполните отчет.**

**Часть2. Packet Tracer. Документирование сети**

Необходимые ресурсы

1 ПК (Windows 10 с доступом к командной строке, доступу к Интернету и с программой Packet Tracer)

**Топология**




**Исходные данные**

В этом задании необходимо задокументировать схему адресации и подключения, используемые в центральной области сети (Central). Для сбора необходимой информации используйте различные команды.

**Примечание.** Пароль пользовательского режима — **cisco**. Пароль привилегированного режима — **class**.

**Требования**

- Получите доступ к командой строке на разных устройствах центральной области (Central).
- Используйте команды, чтобы собрать информацию, необходимую для таблицы **Документация схемы адресации и подключений устройств (Addressing Scheme and Device Connection Documentation)**.
- Если вы не помните необходимые команды, можно использовать встроенную справочную систему IOS.
- Если вам нужна дополнительная помощь, см. страницу **Hints (Советы)**. В программе Packet Tracer нажмите правую стрелку (>) в правой нижней части окна

инструкции. Если у вас есть печатная версия инструкций, то страница Советы — это последняя страница.

**Документация схемы адресации и подключений устройств**

| Имя устройства | Интерфейс | Адрес | Маска подсети | Подключения | |
|---|---|---|---|---|---|
| | | | | Имя устройства | Интерфейс |
| R2 | G0/0 | | | | |
| | G0/1 | | | | |
| | G0/2 | | | | |
| | S0/0/0 | 64.100.100.1 | 255.255.255.252 | Internet | N/A |
| | S0/0/1.1 | 64.100.200.2 | 255.255.255.252 | Intranet | N/A |
| S3 | VLAN 1 | 10.10.10.254 | 255.255.255.0 | N/A | N/A |
| | F0/1 | N/A | N/A | CentralServer | NIC |
| | G0/1 | N/A | N/A | | |
| CentralServer | NIC | | | | |
| D1 | VLAN2 | 10.2.0.1 | 255.255.255.0 | N/A | N/A |
| | G0/1 | | | | |
| | G0/2 | | | | |
| | F0/23 | N/A | N/A | | |
| | F0/24 | N/A | N/A | | |
| S1 | VLAN 2 | 10.2.0.2 | 255.255.255.0 | N/A | N/A |
| | F0/23 | N/A | N/A | | |
| | G0/1 | N/A | N/A | | |
| D2 | F0/23 | N/A | N/A | S1 | F0/23 |
| | F0/24 | | | | |
| | G0/1 | | | | |
| | G0/2 | | | | |
| S2 | VLAN 1 | 10.3.0.2 | 255.255.255.0 | N/A | N/A |
| | F0/23 | N/A | N/A | | |
| | G0/1 | N/A | N/A | | |

**Часть 3. Packet Tracer. Настройка и проверка небольшой сети**

Необходимые ресурсы

1 ПК (Windows 10 с доступом к командной строке, доступу к Интернету и с программой Packet Tracer)

**Топология:**

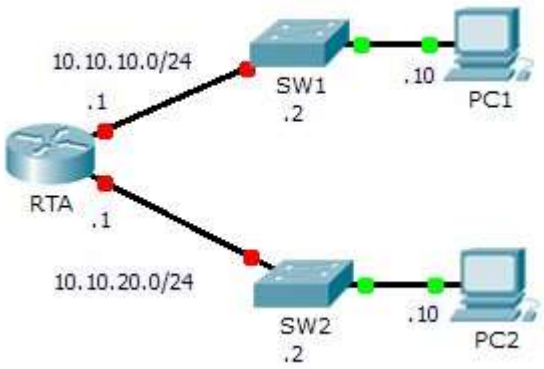



**Таблица адресации**

| Устройство | Интерфейс | IP-адрес | Маска подсети | Шлюз по умолчанию |
|---|---|---|---|---|
| RTA | G0/0 | 10.10.10.1 | 255.255.255.0 | N/A |
| | G0/1 | 10.10.20.1 | 255.255.255.0 | N/A |
| SW1 | VLAN1 | 10.10.10.2 | 255.255.255.0 | 10.10.10.1 |
| SW2 | VLAN1 | 10.10.20.2 | 255.255.255.0 | 10.10.20.1 |
| PC1 | NIC | 10.10.10.10 | 255.255.255.0 | 10.10.10.1 |
| PC2 | NIC | 10.10.20.10 | 255.255.255.0 | 10.10.20.1 |

**Исходные данные**

В этом упражнении вам предстоит настроить основные параметры на **RTA**, включая IP-адресацию. Вам также потребуется настроить SW1 для удалённого управления и настроить компьютеры. После успешной проверки подключения вам нужно будет использовать команды **show** для сбора информации о сети.

**Примечание.** Пароль пользовательского режима — **cisco**. Пароль привилегированного режима — **class**.

**Packet Tracer. Настройка и проверка небольшой сети**

**Настройка устройств и проверка подключения**

**Шаг 1: Выполните настройку основных параметров на RTA.**

a. Настройте RTA, используя следующие сведения и **Таблицу адресации**:

- Имя узла и баннер
- Пароли канала — **cisco**; зашифрованный пароль — **class**
- IP-адресация и описания на интерфейсах LAN

b. Сохраните конфигурацию.

**Шаг 2: Настройте адресацию на узлах PC1 и PC2.**

a. Используя **Таблицу адресации**, настройте IP-адресацию для узлов PC1 и PC2.

b. Проверьте подключение между узлами **PC1** и **PC2**. При необходимости выполните поиск и устранение неполадок.

**Шаг 3: Настройте SW1 для удалённого управления.**

a. Используя **Таблицу адресации**, настройте административный интерфейс для SW1.

b. Настройте адрес шлюза по умолчанию.

c. Сохраните конфигурацию.

**Сбор данных с помощью команд show**

**Шаг 1: Соберите необходимые сведения, используя выходные данные команды show interface.**

Выполните следующие команды:
**show ip interface brief**
**show interfaces show ip**
**interface**

**Дополнительное задание 1**
**Часть 1. Packet Tracer. Настройка интерфейсов IPv4 и IPv6**
Необходимые ресурсы
1 ПК (Windows 10 с доступом к командной строке, доступу к Интернету и с программой Packet Tracer)

**Топология:**

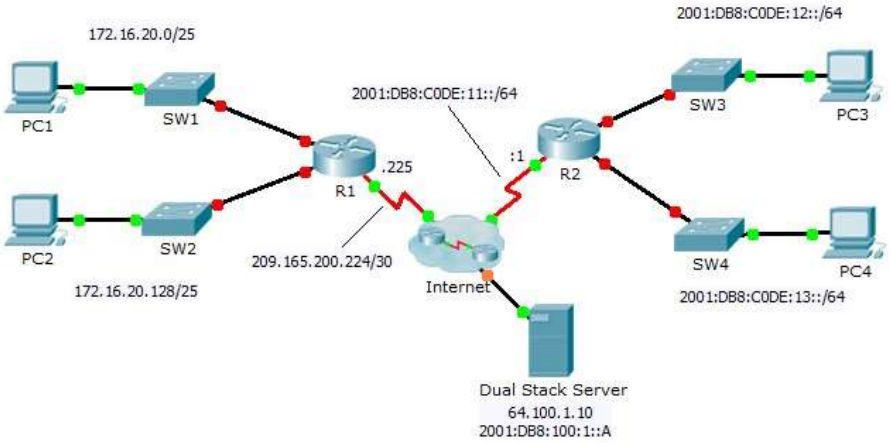



**Таблица адресации**

| Устройство | Интерфейс | IPv4-адрес / IPv6-адрес/Префикс | Маска подсети | Шлюз по умолчанию |
|---|---|---|---|---|
| R1 | G0/0 | 172.16.20.1 | 255.255.255.128 | N/A |
| | G0/1 | 172.16.20.129 | 255.255.255.128 | N/A |
| | S0/0/0 | 209.165.200.225 | 255.255.255.252 | N/A |
| PC1 | NIC | 172.16.20.10 | 255.255.255.128 | 172.16.20.1 |
| PC2 | NIC | 172.16.20.138 | 255.255.255.128 | 172.16.20.129 |
| R2 | G0/0 | 2001:DB8:C0DE:12::1/64 | | N/A |
| | G0/1 | 2001:DB8:C0DE:13::1/64 | | N/A |
| | S0/0/1 | 2001:DB8:C0DE:11::1/64 | | N/A |
| | Link-local | FE80::2 | | N/A |
| PC3 | NIC | 2001:DB8:C0DE:12::A/64 | | FE80::2 |
| PC4 | NIC | 2001:DB8:C0DE:13::A/64 | | FE80::2 |

**Исходные данные**

К маршрутизаторам R1 и R2 подключены по две локальных сети. Ваша задача — настроить соответствующую адресацию на каждом устройстве и проверить подключение между локальными сетями.

**Примечание.** Пароль пользовательского режима — **cisco**. Пароль привилегированного режима — **class**.

**1. Настройка адресации IPv4 и проверка подключения**

**Шаг 1: Назначьте IPv4-адреса маршрутизатору R1 и устройствам локальной сети.**

Руководствуясь **Таблицей адресации**, настройте IP-адресацию для интерфейсов локальной сети маршрутизатора **R1**, а также для узлов **PC1** и **PC2**. Последовательный интерфейс уже настроен.

**Шаг 2: Проверьте подключение.**

Узлы **PC1** и **PC2** должны успешно отправлять эхо-запросы друг другу и на **сервер с двойным стеком (Dual Stack Server)**.

**2. Настройка адресации IPv6 и проверка подключения**

**Шаг 1: Назначьте IPv6-адреса маршрутизатору R2 и устройствам локальной сети.**

Руководствуясь **Таблицей адресации**, настройте IP-адресацию для интерфейсов локальной сети маршрутизатора **R2**, а также для узлов **PC3** и **PC4**. Последовательный интерфейс уже настроен.

**Шаг 2: Проверьте подключение.**

Узлы **PC3** и **PC4** должны успешно отправлять эхо-запросы друг другу и на **сервер с двойным стеком (Dual Stack Server)**.

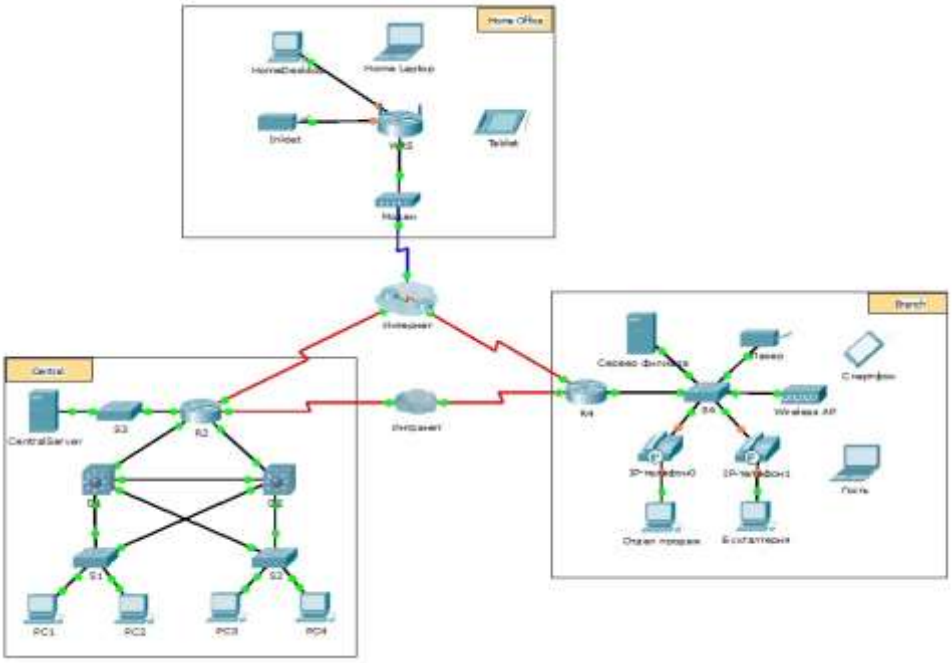
**Дополнительное задание 1**

**Часть 1. Packet Tracer. Использование команды traceroute для обнаружения сети**

Необходимые ресурсы

1 ПК (Windows 10 с доступом к командной строке, доступу к Интернету и с программой Packet Tracer)

**Топология:**



**Примечание.** Пароль пользовательского режима — **cisco**. Пароль привилегированного режима — **class**.

**Часть 1. Трассировка и документирование удалённых устройств.**

a. Нажмите на **Sales (Продажи)** и выберите вкладку **Desktop (Рабочий стол)** > **Command Prompt (Командная строка)**. Используйте команду **ipconfig**, чтобы проверить настройку IP-адреса для **Sales (Продажи)**.

b. Новый веб-адрес сервера — **b2server.pt.pka.** Введите следующую команду **nslookup**, чтобы узнать IP-адрес для **b2server**:

PC> **nslookup b2server.pt.pka**

Какой адрес команда вернула для **b2server**?

c. Введите команду **tracert**, чтобы определить путь от узла **Sales (Продажи)** до **b2server.pt.pka.**

PC> **tracert b2server.pt.pka**

d. С помощью telnet подключитесь к первому IP-адресу в выходных данных команды **tracert** и войдите в систему.

PC> **telnet 172.16.0.1**

e. Вы подключены к маршрутизатору **R4**. На маршрутизаторе выполните команду **traceroute**, используя адрес для b2server, определённый на шаге b. В чём заключаются различия между командой **traceroute** на маршрутизаторе и командой **tracert** на ПК? Что означает маршрутизатор **R4** для узла **Sales (Продажи)**?

f. Используйте команду **show ip interface brief**, чтобы отобразить состояние интерфейсов на маршрутизаторе R4. Исходя из выходных данных команды, определите, какой интерфейс используется для подключения к следующему устройству в списке выходного сообщения команды **tracert**?

Совет. Используйте команду **show running-config** для просмотра значений масок подсетей для интерфейсов.

g. С помощью telnet подключитесь ко второму IP-адресу в списке **tracert** и войдите в систему. Можно использовать число в крайнем левом столбце выходного сообщения команды **tracert**, в список которого включено ваше устройство. Укажите имя устройства, к которому вы подключены. Введите команду **show ip route** и изучите выходные данные. Какие типы маршрутов показаны в таблице маршрутизации (см. список кодов в начале выходных данных)?

h. Исходя из выходных данных команды **show ip route**, скажите, какой интерфейс является выходным для следующего IP-адреса, указанного в первоначальных выходных данных команды **tracert**? С помощью команды telnet обратитесь к третьему IP-адресу в выходном сообщении команды **tracert** и войдите в систему. Укажите имя узла данного устройства.

Выполните команду **show ip route connected**. Какие сети напрямую подключены к этому маршрутизатору?

Обратитесь к таблице **Документация схемы адресации.** Какие интерфейсы соединяют устройства между трассировкой маршрута 2 и трассировкой маршрута 3?

i. С помощью telnet подключитесь к четвёртому IP-адресу в выходном сообщении команды **tracert** и войдите в систему. Укажите имя устройства. Выполните команду, чтобы определить, к какому интерфейсу подключён **b2server.pt.pka**.

j. Если при выполнении предыдущих шагов вы использовали таблицу **Документация схемы адресации**, то теперь таблица должна быть заполнена. Если это не так, заполните таблицу.

k. Обладая полной документацией схемы адресации и знаниями о пути от узла **Sales (Продажи)** до **branch2.pt.pka**, вы сможете отобразить схему нового филиала в **Документации топологии** ниже.

**Часть 2. Документация схемы адресации**

| Идентификатор маршрута трассы | Устройство | Интерфейс | Адрес | Маска подсети |
|---|---|---|---|---|
| — | Продажи | NIC | 172.16.0.x (DHCP) | 255.255.255.0 |
| 1 | | | | |
| | | | | |
| | | S0/0/1.1 | 64.100.200.1 | 255.255.255.252 |
| 2 | | | | |
| | | G0/1 | 64.104.223.1 | 255.255.255.252 |
| | | S0/0/0 | 64.100.100.2 | |
| | | | | |
| 3 | | | | |
| | | G0/2 | | 255.255.255.0 |
| | | F0/1 | 128.107.46.1 | |
| | | | | |
| 4 | | G0/0 | | |
| | | | | |
| 5 | b2server.pt.pka | NIC | 128.107.64.254 | 255.255.255.0 |

**Сделайте вывод по работе, выполните отчет.**

**Лабораторная работа № 16**
**Тема: Настройка статической маршрутизации**

**Цель работы: получить практические навыки по работе с программой Packet Tracer: выполнить настройку статических маршрутов и маршрутов по умолчанию для IPv4**

Необходимые ресурсы
1 ПК (Windows 10 с доступом к командной строке, доступу к Интернету и с программой Packet Tracer)

**Топология:**

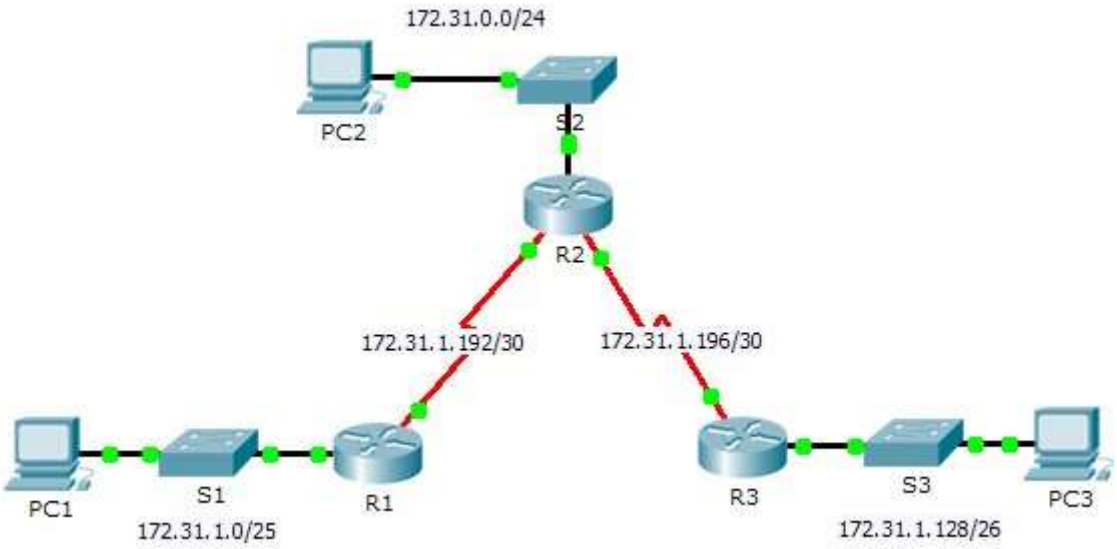



**Таблица адресации**

| Устройство | Интерфейс | IPv4-адрес | Маска подсети | Шлюз по умолчанию |
|---|---|---|---|---|
| R1 | G0/0 | 172.31.1.1 | 255.255.255.128 | N/A |
| | S0/0/0 | 172.31.1.194 | 255.255.255.252 | N/A |
| R2 | G0/0 | 172.31.0.1 | 255.255.255.0 | N/A |
| | S0/0/0 | 172.31.1.193 | 255.255.255.252 | N/A |
| | S0/0/1 | 172.31.1.197 | 255.255.255.252 | N/A |
| R3 | G0/0 | 172.31.1.129 | 255.255.255.192 | N/A |
| | S0/0/1 | 172.31.1.198 | 255.255.255.252 | N/A |
| PC1 | NIC | 172.31.1.126 | 255.255.255.128 | 172.31.1.1 |
| PC2 | NIC | 172.31.0.254 | 255.255.255.0 | 172.31.0.1 |
| PC3 | NIC | 172.31.1.190 | 255.255.255.192 | 172.31.1.129 |

**Часть 1. Исследование сети и оценка необходимости статической маршрутизации**

a. Используя схему топологии, ответьте, сколько всего имеется сетей?

b. Сколько сетей подключены напрямую к маршрутизаторам R1, R2 и R3?

c. Сколько статических маршрутов требуется каждому маршрутизатору, чтобы достичь сетей, не имеющих с ним прямого подключения?

d. Проверьте подключение к сетям LAN маршрутизаторов R2 и R3, отправив эхо-запросы на PC2 и PC3 от PC1.

Почему эхо-запросы были неудачными?

**Часть 2. Настройка статического маршрута и маршрута по умолчанию**

**Шаг 1: Настройте рекурсивные статические маршруты на маршрутизаторе R1.**

a. Что такое рекурсивный статический маршрут?
b. Почему рекурсивному статическому маршруту требуется два поиска в таблице маршрутизации?
c. Настройте рекурсивный статический маршрут для каждой сети без прямого подключения к R1, включая канал WAN между R2 и R3.
d. Проверьте подключение к сети LAN маршрутизатора R2 и отправьте эхо-запросы на IP-адреса компьютеров PC2 и PC3.
Почему эхо-запросы были неудачными?

**Шаг 2: Настройте напрямую подключенные статические маршруты на маршрутизаторе R2.**

a. Чем отличается статический маршрут с прямым подключением от рекурсивного статического маршрута?
b. Настройте напрямую подключенный статический маршрут от R2 ко всем сетям, не имеющим прямого подключения.
c. С помощью какой команды отображаются только сети с прямым подключением?
d. С помощью какой команды отображаются только статические маршруты, указанные в таблице маршрутизации?
e. При просмотре таблицы маршрутизации можете ли вы отличить напрямую подключенный статический маршрут от сети с прямым подключением?

**Шаг 3: Настройте маршрут по умолчанию для маршрутизатора R3.**

a. Чем отличается маршрут по умолчанию от обычного статического маршрута?
b. Настройте маршрут по умолчанию на маршрутизаторе R3 таким образом, чтобы была доступна каждая сеть без прямого подключения.
c. Как статический маршрут отображается в таблице маршрутизации?

**Шаг 4: Запишите команды для полностью заданных маршрутов.**

**Примечание**. В настоящее время Packet Tracer не поддерживает настройку полностью заданных статических маршрутов. Таким образом, на данном шаге необходимо задокументировать конфигурацию для полностью заданных маршрутов.

a. Объясните, что означает полностью заданный маршрут.
b. С помощью какой команды реализуется полностью заданный статический маршрут от LAN R3 к LAN R2?
Запишите полностью заданный маршрут от R3 к сети между маршрутизаторами R2 и R1. Настраивать маршрут не нужно, необходимо просто рассчитать его.
c. Запишите полностью заданный статический маршрут от LAN R3 к LAN R1. Настраивать маршрут не нужно, необходимо просто рассчитать его.

**Шаг 5: Проверьте настройки статических маршрутов.**

Для проверки настроек используйте соответствующие команды **show**.
Какие команды **show** следует использовать для проверки правильности конфигурации статических маршрутов?

**Шаг 6: Проверка подключения**

Теперь каждое устройство должно успешно отправлять эхо-запрос на любое другой устройство. Если это не так, проверьте настройки статического маршрута и маршрута по умолчанию.

**Сделайте вывод по работе, выполните отчет.**

## Лабораторная работа № 17

## Тема: Настройка динамической маршрутизации

**Цель работы: получить практические навыки по работе с программой Packet Tracer: исследовать процесс сходимости, выполнить настройку протокола RIPv2**

**Задание 1 Исследование сходимости**

Необходимые ресурсы

1 ПК (Windows 10 с доступом к командной строке, доступу к Интернету и с программой Packet Tracer)

**Топология:**

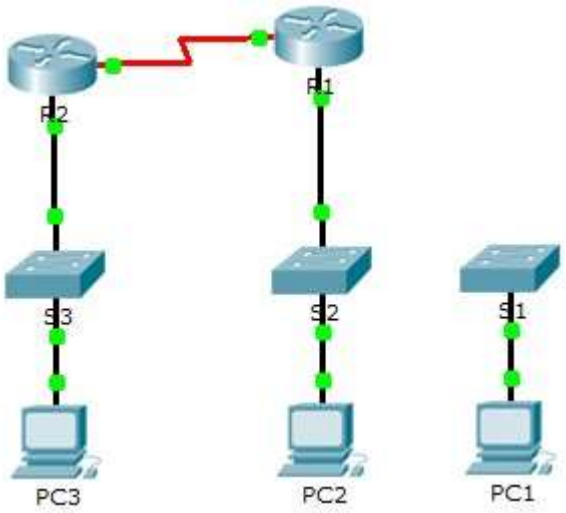



**Таблица адресации**

| Устройство | Интерфейс | IP-адрес | Маска подсети | Шлюз по умолчанию |
|---|---|---|---|---|
| R1 | G0/0 | 209.165.0.1 | 255.255.255.0 | N/A |
| | G0/1 | 64.100.0.1 | 255.0.0.0 | N/A |
| | S0/0/0 | 192.168.1.2 | 255.255.255.0 | N/A |
| R2 | G0/0 | 10.0.0.1 | 255.0.0.0 | N/A |
| | S0/0/0 | 192.168.1.1 | 255.255.255.0 | N/A |
| PC1 | NIC | 64.100.0.2 | 255.0.0.0 | 64.100.0.1 |
| PC2 | NIC | 209.165.0.2 | 255.255.255.0 | 209.165.0.1 |
| PC3 | NIC | 10.0.0.2 | 255.0.0.0 | 10.0.0.1 |

**Часть 1. Просмотр таблицы маршрутизации сошедшейся сети**

**Шаг 1: Выполните команды show и интерпретируйте выходные данные.**

a. Отобразите сети с прямым подключением маршрутизатора **R1**. Сколько маршрутов подключены к маршрутизатору **R1**? R1# **show ip route connected**

b. Отобразите текущую конфигурацию маршрутизатора **R1**. Какой протокол маршрутизации используется?

c. Совпадают ли IP-адреса в конфигурации, объявленные протоколом RIP, с подключёнными адресами?

d. Эти IP-адреса назначаемые, сетевые или широковещательные?

e. Отобразите сети маршрутизатора **R1**, полученные через RIP. Сколько этих маршрутов? R1# **show ip route rip**

f. Отобразите все сети, содержащиеся в таблице маршрутизации **R1**. Что означают начальные буквы?

R1# **show ip route**

g. Повторите действия от a до f шага 1 на маршрутизаторе **R2**. Сравните выходные данные двух маршрутизаторов.

**Шаг 2: Проверьте состояние топологии.**

a. Отправьте эхо-запрос с **PC3** на **PC2**. Эхо-запрос должен быть успешным.

b. Отобразите состояние интерфейсов на **R2**. Два интерфейса должны иметь назначенные адреса. Каждый адрес соответствует подключённой сети.

R2# **show ip interface brief**

c. Отобразите состояние интерфейсов на **R1**. Сколько интерфейсов имеют назначенные адреса?

R1# **show ip interface brief**

**Часть 2. Добавление новой сети LAN в топологию**

**Шаг 1: Добавьте в топологию ещё один кабель Ethernet.**

a. Выполните подключение кабеля Ethernet от коммутатора S1 к соответствующему порту на маршрутизаторе **R1**.

b. После того, как индикатор порта коммутатора S1 загорится зелёным цветом, отправьте эхо-запрос от **PC1** на **PC2**. Успешно ли выполнен эхо-запрос?

c. Отправьте эхо-запрос с **PC1** на **PC3**. Успешно ли выполнен эхо-запрос? Почему?

**Шаг 2: Настройте маршрут.**

a. Перейдите из режима реального времени (Realtime mode) в режим моделирования (Simulation mode).

b. На маршрутизаторе R1 добавьте новый маршрут для сети 64.0.0.0.

R1(config)# **router rip**

R1(config-router)# **network 64.0.0.0**

c. Изучите PDU, которые покидают маршрутизатор **R1**. Какого они типа?

**Наблюдение за процессом сходимости**

**Шаг 1: Используйте команды debug.**

a. Включите отладку на маршрутизаторе **R2**.

R2# **debug ip rip**

R2# **debug ip routing**

b. Для справки отобразите таблицу маршрутизации **R2**, как в шаге 1f.

c. Нажмите на **Capture/Forward (Захват/Вперед)** в режиме моделирования. Какое уведомление появилось в терминале маршрутизатора **R2**?

d. Сколько переходов разделяет маршрутизатор R2 от 64.0.0.0 согласно выходным данным отладки?

e. На какой интерфейс маршрутизатор **R2** отправляет пакеты, адресованные сети 64.0.0.0?

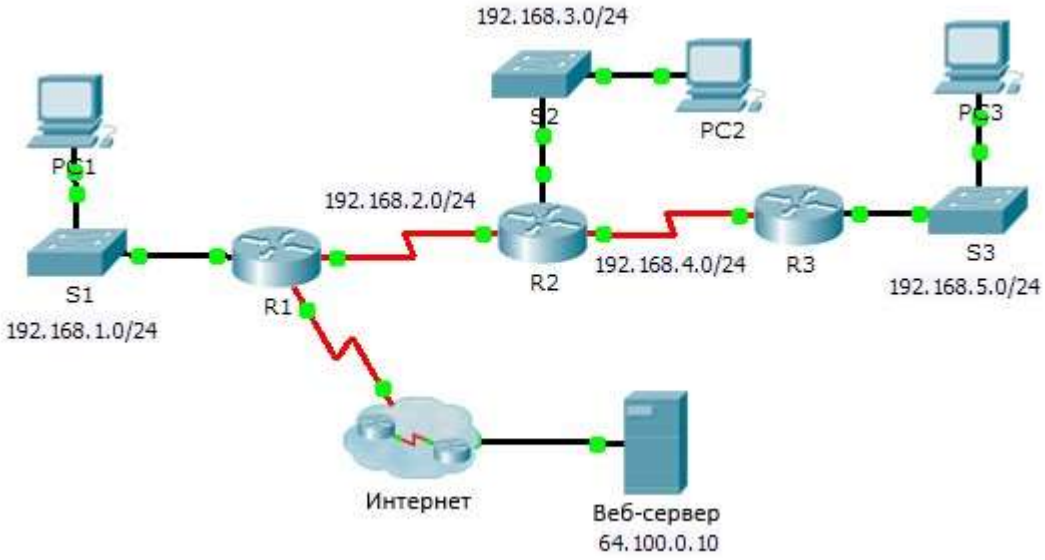
f. Отобразите таблицу маршрутизации маршрутизатора **R2**. Создайте новую запись.

**Шаг 2: Проверьте состояние топологии.**

Отправьте эхо-запрос с **PC1** на **PC3**. Успешно ли выполнен эхо-запрос? Почему?

**Задание 2 Настройка протокола RIPv2**

**Топология:**




.

**Часть 1. Настройка RIPv2**

**Шаг 1: Настройте протокол RIPv2 на маршрутизаторе R1.**

a. Используйте соответствующую команду, чтобы создать на маршрутизаторе **R1** маршрут по умолчанию, по которому весь интернет-трафик покинет сеть через интерфейс S0/0/1.

b. Войдите в режим конфигурации протокола RIP.

c. Выберите версию 2 протокола RIP и отключите суммирование сетей.

d. Настройте протокол RIP для сетей, которые подключены к маршрутизатору **R1**.

e. Настройте порт LAN таким образом, чтобы он не отправлял маршрутизирующую информацию в виде анонсов маршрутов.

f. Объявите маршрут по умолчанию, настроенный на шаге 1a с другими маршрутизаторами RIP. g. Сохраните конфигурацию.

**Packet Tracer. Настройка протокола RIPv2**

**Шаг 2: Настройте протокол RIPv2 на маршрутизаторе R2.**

a. Войдите в режим конфигурации протокола RIP.

b. Выберите версию 2 протокола RIP и отключите суммирование сетей.

c. Настройте протокол RIP для сетей с прямым подключением к маршрутизатору **R2**.

d. Настройте интерфейс без маршрутизаторов таким образом, чтобы он не отправлял никаких данных маршрутизации.

e. Сохраните конфигурацию.

**Шаг 3: Настройте протокол RIPv2 на маршрутизаторе R3**

Повторите действия шага 2 на маршрутизаторе **R3**.

**Часть 2. Проверка конфигураций**

**Шаг 1: Просмотрите таблицы маршрутизации на маршрутизаторах R1, R2 и R3.**

a. Используйте соответствующие команды, чтобы посмотреть таблицу маршрутизации **R1**. Теперь RIP (R) появляется в таблице маршрутизации вместе с подключёнными (C) и локальными (L) маршрутами. Для каждой сети существует запись. В списке также отображается маршрут по умолчанию.

b. Просмотрите таблицы маршрутизации на маршрутизаторах **R2** и **R3**. Обратите внимание, что каждый маршрутизатор имеет полный список всех сетей 192.168.x.0 и маршрут по умолчанию.

**Шаг 2: Убедитесь в наличии полного подключения ко всем местам назначения.**

Теперь каждое устройство должно успешно отправлять эхо-запрос на любое другой устройство внутри сети. Кроме того, все устройства должны успешно отправлять эхо-запросы на **веб-сервер**.

**Сделайте вывод по работе, выполните отчет.**

**Лабораторная работа № 18**
**Тема: Настройка ACL-списков**

**Цель работы: получить практические навыки по работе с программой Packet Tracer: выполнить настройку расширенных списков контроля доступа.**

Таблица адресации

| Устройство | Интерфейс | IP-адрес | Маска подсети | Шлюз по умолчанию |
|---|---|---|---|---|
| R1 | G0/0 | 172.22.34.65 | 255.255.255.224 | — |
| | G0/1 | 172.22.34.97 | 255.255.255.240 | — |
| | G0/2 | 172.22.34.1 | 255.255.255.192 | — |
| Server | NIC | 172.22.34 | 62 255.255.255 | 192 172.22.34.1 |
| PC1 | NIC | 172.22.34.66 | 255.255.255.224 | 172.22.34.65 |
| PC2 | NIC | 172.22.34.98 | 255.255.255.240 | 172.22.34.97 |
| | | | | |

**Задачи**

**Часть 1. Настройка, применение и проверка расширенного нумерованного списка контроля**

доступа

**Часть 2. Настройка, применение и проверка расширенного именованного списка контроля**

**доступа**

Общие сведения/сценарий

Двум сотрудникам предприятия требуется доступ к сервисам, предоставляемым этим сервером. Узлу

PC1 требуется доступ только по FTP, а узлу PC2 — только доступ в Интернет. Оба компьютера могут

получать отчеты на ping-запросы к серверу, но не друг к другу.

Инструкции

**Часть 1. Настройка, применение и проверка расширенного нумерованного ACL-списка**

**Шаг 1.** Настройте ACL-список на разрешение FTP и ICMP с PC1 LAN.

a. В режиме глобальной конфигурации на маршрутизаторе R1 введите следующую команду, чтобы

определить первый действительный номер для расширенного списка контроля доступа. Откройте окно конфигурации

R1(config)# access-list ?

<1-99> IP standard access list

<100-199> IP extended access list

b. Добавьте 100 к команде, а затем поставьте вопросительный знак.

R1(config)# access-list 100 ?

deny Specify packets to reject

permit Specify packets to forward

remark Access list entry comment

c. Чтобы разрешить трафик FTP, введите команду permit с вопросительным знаком.

```
R1(config)# access-list 100 permit ?
 ahp Authentication Header Protocol
 eigrp Cisco's EIGRP routing protocol
 esp Encapsulation Security Payload
 gre Cisco's GRE tunneling
 icmp Internet Control Message Protocol
 ip Any Internet Protocol
 ospf OSPF routing protocol
 tcp Transmission Control Protocol
 udp User Datagram Protocol
```

d. При настройке и применении этот ACL должен разрешать FTP и ICMP. Протокол ICMP входит в этот список, а протокол FTP — нет. Это связано с тем, что FTP является протоколом уровня приложений, который использует TCP на транспортном уровне. Введите TCP, чтобы уточнить подсказку списка контроля доступа.

```
R1(config)# access-list 100 permit tcp ?
 A.B.C.D Source address
 any Any source host
 host A single source host
```

e. Адрес источника может представлять одно устройство, например PC1, используя ключевое слово host , а затем IP-адрес PC1. Использование ключевого слова any разрешает любой хост в любой сети. Фильтрацию также можно выполнить по сетевому адресу. В этом случае это любой хост, который имеет адрес, принадлежащий сети 172.22.34.64/27. Введите сетевой адрес со знаком вопроса в конце.

```
R1(config)# access-list 100 permit tcp 172.22.34.64 ?
 A.B.C.D Source wildcard bits
```

f. Рассчитайте шаблонную маску, определяющую двоичную противоположность /27 маски подсети.

11111111.11111111.11111111.11100000 = 255.255.255.224
00000000.00000000.00000000.00011111 = 0.0.0.31

g. Введите сетевой адрес, а после него — знак вопроса.

```
R1(config)# access-list 100 permit tcp 172.22.34.64 0.0.0.31 ?
 A.B.C.D Destination address
 any Any destination host
 eq Match only packets on a given port number
 gt Match only packets with a greater port number
 host A single destination host
 lt Match only packets with a lower port number
 neq Match only packets not on a given port number
 range Match only packets in the range of port numbers
```

h. Настройте адрес места назначения. В этом сценарии мы фильтруем трафик для единственного места назначения — сервера. Введите ключевое слово host, а после него — IP-адрес сервера.

```
R1(config)# access-list 100 permit tcp 172.22.34.64 0.0.0.31 host
```

172.22.34.62 ?
 dscp Match packets with given dscp value
eq Match only packets on a given port number
 established established
 gt Match only packets with a greater port number
 lt Match only packets with a lower port number
 neq Match only packets not on a given port number
 precedence Match packets with given precedence value
 range Match only packets in the range of port numbers
 <cr>

i. Обратите внимание на параметр <cr> (возврат каретки). Другими словами, вы можете нажать клавишу ВВОД, и согласно правилу будет разрешен весь трафик TCP. Однако мы хотим разрешить только трафик FTP. Поэтому введите ключевое слово eq, после которого поставьте вопросительный знак, чтобы отобразить доступные параметры. Затем введите ftp и нажмите клавишу Enter.

R1(config)# access-list 100 permit tcp 172.22.34.64 0.0.0.31 host
172.22.34.62 eq ?
 <0-65535> Port number
 ftp File Transfer Protocol (21)
 pop3 Post Office Protocol v3 (110)
 smtp Simple Mail Transport Protocol (25)
 telnet Telnet (23)
 www World Wide Web (HTTP, 80)
R1(config)# access-list 100 permit tcp 172.22.34.64 0.0.0.31 host
172.22.34.62 eq ftp

j. Создайте вторую запись списка контроля доступа, разрешающую передачу трафика ICMP (pingзапрос и др.) от PC1 на Server. Обратите внимание, что номер списка контроля доступа остается прежним и нет необходимости указывать конкретный тип трафика ICMP.

R1(config)# access-list 100 permit icmp 172.22.34.64 0.0.0.31 host
172.22.34.62

k. Остальной трафик запрещен по умолчанию.

l. Выполните команду show access-list и убедитесь, что список доступа 100 содержит правильные инструкции. Обратите внимание, что инструкция deny any не отображается в конце списка доступа. Выполнение списка доступа по умолчанию заключается в том, что если пакет не соответствует инструкции в списке доступа, он не разрешен через интерфейс.

R1#show access-lists
Extended IP access list 100
 10 permit tcp 172.22.34.64 0.0.0.31 host 172.22.34.62 eq ftp
 20 permit icmp 172.22.34.64 0.0.0.31 host 172.22.34.62

**Шаг 2. Примените этот список контроля доступа на соответствующем интерфейсе, чтобы фильтровать трафик.**

С точки зрения маршрутизатора R1, трафик, к которому применяется список ACL 100, является входящим из сети, подключенной к интерфейсу Gigabit Ethernet 0/0. Войдите в режим интерфейсной настройки и примените этот список контроля доступа.

Примечание. В реальной операционной сети не рекомендуется применять непроверенный список
доступа к активному интерфейсу.
R1(config)# interface gigabitEthernet 0/0
R1(config-if)# ip access-group 100 in
**Шаг 3. Проверьте работу списка контроля доступа.**
a. Отправьте ping-запрос с PC1 на Server. Если ответов на ping-запросы нет, проверьте IP-адреса
перед тем, как продолжить.
b. Отправьте FTP-трафик от PC1 на Server. Имя пользователя и пароль — cisco.
PC> ftp 172.22.34.62
c. Выход из службы FTP.
ftp> quit
Закройте окно настройки.
d. Пощлите эхо-запрос от PC1 к PC2. Хост назначения должен быть недоступен, поскольку ACL явно
не разрешает трафик.
Часть 2. Настройка, применение и проверка расширенного именованного ACL-списка
Шаг 1. Настройте список контроля доступа на разрешение доступа по протоколу HTTP и ICMP с PC2 LAN..
a. Именованные списки контроля доступа начинаются с ключевого слова ip. В режиме глобальной
настройки маршрутизатора R1 введите следующую команду, после которой поставьте вопросительный знак.
Откройте окно конфигурации
R1(config)# ip access-list ?
 extended Extended Access List
 standard Standard Access List
b. Можно настроить именованные стандартные и расширенные ACL-списки. Посредством этого
списка доступа фильтруются как IP-адреса источника, так и IP-адреса узла-назначения; таким
образом, список должен быть расширенным. Введите HTTP_ONLY в качестве имени. (Для определения рейтинга Packet Tracer имя чувствительно к регистру, а инструкции списка доступа должны быть в правильном порядке.)
R1(config)# ip access-list extended HTTP_ONLY
c. Командная строка изменится. Теперь активирован режим настройки именованного расширенного
ACL-списка. Всем устройствам в локальной сети хоста PC2 требуется доступ по TCP. Введите
сетевой адрес со знаком вопроса в конце.
R1(config-ext-nacl)# permit tcp 172.22.34.96 ?
 A.B.C.D Source wildcard bits
d. Другой способ расчета шаблонной маски заключается в вычитании маски подсети из 255.255.255.255.
 255.255.255.255
- 255.255.255.240
---
= 0. 0. 0. 15
R1(config-ext-nacl)# permit tcp 172.22.34.96 0.0.0.15

e. Допишите правило, определив адрес сервера как в части 1 и настроив фильтрацию трафика www.
R1(config-ext-nacl)# permit tcp 172.22.34.96 0.0.0.15 host 172.22.34.62 eq www
f. Создайте вторую запись списка контроля доступа, разрешающую передачу трафика ICMP (pingзапрос и др.) от PC2 на Server. Примечание. Приглашение остается прежним, и нет
необходимости указывать конкретный тип трафика ICMP.
R1(config-ext-nacl)# permit icmp 172.22.34.96 0.0.0.15 host 172.22.34.62
g. Остальной трафик запрещен по умолчанию. Выход из расширенного именованного режима
конфигурации ACL.
h. Выполните команду show access-list и убедитесь, что список доступа HTTP_ONLY содержит
правильные инструкции.
R1# show access-lists
Extended IP access list 100
10 permit tcp 172.22.34.64 0.0.0.31 host 172.22.34.62 eq ftp
20 permit icmp 172.22.34.64 0.0.0.31 host 172.22.34.62
Extended IP access list HTTP_ONLY
10 permit tcp 172.22.34.96 0.0.0.15 host 172.22.34.62 eq www
20 permit icmp 172.22.34.96 0.0.0.15 host 172.22.34.62
Шаг 2. Примените этот список контроля доступа на соответствующем интерфейсе, чтобы фильтровать трафик.
С точки зрения маршрутизатора R1, трафик, к которому применяется ACL-список HTTP_ONLY,
является входящим из сети, подключенной к интерфейсу Gigabit Ethernet 0/1. Войдите в режим
интерфейсной настройки и примените этот список контроля доступа.
В реальной операционной сети не рекомендуется применять непроверенный список доступа к
активному интерфейсу. Этого следует избегать, если это возможно.
R1(config)# interface gigabitEthernet 0/1
R1(config-if)# ip access-group HTTP_ONLY in
Шаг 3. Проверьте работу списка контроля доступа.
a. Отправьте ping-запрос с PC2 на Server. Если ответы на ping-запросы не приходят, проверьте IPадреса.
b. С PC2 откройте веб-браузер и введите IP-адрес Сервера. Должна быть отображена веб-страница
Сервера.
c. Отправьте FTP-трафик от PC2 на Server. Подключение не должно быть успешным. Если нет,
устраняйте инструкции списка доступа и конфигурации групп доступа на интерфейсах.
**Сделайте вывод по работе, выполните отчет.**

## Лабораторная работа № 19
## Тема: Изучение протоколов DHCP.

**Цель работы: получить практические навыки по работе с программой Packet Tracer: Выполнить настройку протокола DHCPv4**

Таблица адресации

| Устройство | Интерфейс | IPv4-адрес | Маска подсети | Шлюз по умолчанию |
|---|---|---|---|---|
| R1 | G0/0 | 192.168.10.1 | 255.255.255.0 | — |

| | | | | |
|---|---|---|---|---|
| R1 | S0/0/0 | 10.1.1.1 | 255.255.255.252 | — |
| R2 | G0/0 | 192.168.20.1 | 255.255.255.0 | — |
| R2 | G0/1 | Назначенный DHCP | Назначенный DHCP | — |
| R2 | S0/0/0 | 255.255.255.252 | 10.1.1.2 | — |
| R2 | S0/0/1 | 10.2.2.2 | 255.255.255.252 | — |
| R3 | G0/0 | 192.168.30.1 | 255.255.255.0 | — |
| R3 | S0/0/1 | 10.2.2.1 | 255.255.255.0 | — |
| PC1 | NIC | Назначенный DHCP | Назначенный DHCP | Назначенный DHCP |
| PC2 | NIC | Назначенный DHCP | Назначенный DHCP | Назначенный DHCP |
| DNS Server | NIC | 192.168.20.254 | 255.255.255. | 0 192.168.20.1 |
| | | | | |

**Сценарий**

Выделенный сервер DHCP хорошо масштабируется и им относительно легко управлять, однако использование подобного сервера в каждой точке сети может оказаться слишком затратным. Вместе с тем маршрутизатор Cisco можно настроить для обеспечения DHCP-служб без необходимости в выделенном сервере. Будучи сетевым специалистом вашей компании, вам была назначена задача настройки маршрутизатора Cisco в качестве DHCP-сервера. Также необходимо настроить пограничный маршрутизатор в качестве DHCP-клиента таким образом, чтобы он получал IP-адрес от сети Интернет-провайдера.

**Часть 1. Настройка маршрутизатора в роли DHCP-сервера**

**Шаг 1. Исключите зарезервированные IPv4-адреса из пула DHCP.**

Адреса, статически назначенные устройствам в сетях, которые будут использовать DHCP, должны
быть исключены из пулов DHCP. Это позволяет избежать ошибок, связанных с дублирующимися IPадресами. В этом случае IP-адреса интерфейсов LAN R1 и R3 должны быть исключены из пула DHCP.

Кроме того, девять других адресов исключаются для статического назначения другим устройствам,
таким как серверы и интерфейсы управления устройствами.

a. Настройте маршрутизатор R2 таким образом, чтобы исключить первые 10 адресов из локальных
сетей маршрутизатора R1.

Откройте окно конфигурации

R2(config)# ip dhcp excluded-address 192.168.10.1 192.168.10.10

b. Настройте маршрутизатор R2 таким образом, чтобы исключить первые 10 адресов из локальных
сетей маршрутизатора R3.

**Шаг 2. На маршрутизаторе R2 создайте пул DHCP для локальной сети маршрутизатора R1.**

a. Создайте пул DHCP под названием R1-LAN (с учетом регистра).

R2(config)# ip dhcp pool R1-LAN

b. Настройте пул DHCP с учетом сетевого адреса, шлюза по умолчанию и IP-адреса сервера DNS.

R2(dhcp-config)# network 192.168.10.0 255.255.255.0

R2(dhcp-config)# default-router 192.168.10.1

R2(dhcp-config)# dns-server 192.168.20.254

**Шаг 3. На маршрутизаторе R2 создайте пул DHCP для локальной сети маршрутизатора R3.**

a. Создайте пул DHCP под названием R3-LAN (с чувствительным регистром).

b. Настройте пул DHCP с учетом сетевого адреса, шлюза по умолчанию и IP-адреса сервера DNS.

См. таблицу адресации.

Закройте окно настройки.

**Часть 2. Настройка DHCP-ретрансляции**

**Шаг 1. Настройте маршрутизаторы R1 и R3 в качестве агентов-ретрансляторов.**

Чтобы клиенты DHCP получали адрес от сервера в другом сегменте локальной сети, интерфейс, к
которому подключены клиенты, должен содержать вспомогательный адрес, указывающий на DHCPсервер. В этом случае узлы локальных сетей, подключенных к R1 и R3, получат доступ к DHCPсерверу, настроенному на R2. IP-адреса последовательных интерфейсов R2, подключенных к R1 и R3,
используются в качестве вспомогательных адресов. Трафик DHCP от узлов локальных сетей R1 и R3
будет перенаправляться на эти адреса и обрабатываться DHCP-сервером, настроенным на R2.

a. Настройте helper address для интерфейса локальной сети на R1.

Откройте окно конфигурации

R1(config)# interface g0/0

R1(config-if)# ip helper-address 10.1.1.2

b. Настройте helper address для интерфейса локальной сети на R3.

Шаг 2. Настройте узлы для получения информации об IP-адресации от DHCP.

a. Настройте узлы PC1 и PC2 для получения IP-адресов от DHCP-сервера.







b. Убедитесь, что узлы получили адреса из нужных пулов DHCP.

Закройте окно настройки.

Часть 3. Настройка маршрутизатора в качестве DHCP-клиента

Так же, как ПК может получать адрес IPv4 от сервера, интерфейс маршрутизатора имеет возможность
делать то же самое. Маршрутизатор R2 должен быть настроен на получение адресации от поставщика
услуг Интернета.

a. Настройте интерфейс Gigabit Ethernet 0/1 на маршрутизаторе R2 для получения информации об
IP-адресации через DHCP и включения интерфейса.

Откройте окно конфигурации

R2(config)# interface g0/1

R2(config-if)# ip address dhcp

R2(config-if)# no shutdown

Примечание. Используйте функцию Fast Forward Time Packet Tracer для ускорения процесса.

b. Используйте команду show ip interface brief, чтобы убедиться, что маршрутизатор R2 получил IPадрес от DHCP-сервера.

**Часть 4. Проверка DHCP и связности**

**Шаг 1. Проверьте ассоциации MAC- и IP-адресов в DHCP.**

R2# show ip dhcp binding
IP address Client-ID/ Lease expiration Type
Hardware address
192.168.10.11 0002.4AA5.1470 -- Automatic
192.168.30.11 0004.9A97.2535 -- Automatic
Закройте окно настройки.

**Шаг 2. Проверьте конфигурации**.

Убедитесь в том, что PC1 и PC2 теперь могут отправлять эхо-запросы друг другу и другим устройствам.

**Сделайте вывод по работе, выполните отчет.**

## Лабораторная работа № 20
## Тема: Изучение работы с NAT и PAT

**Цель работы: получить практические навыки по работе с программой Packet Tracer: выполнить настройку NAT для IPv4 (версия для инструкторов)**

**Топология:**

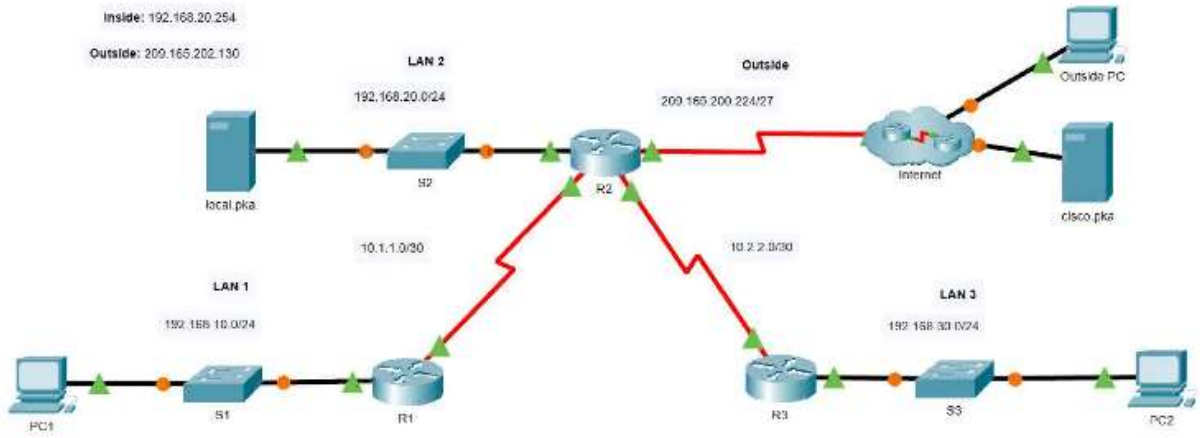



**Таблица адресации**

| Устройство | Интерфейс | IP-адрес |
|---|---|---|
| R1 | S0/0/0 | 10.1.1.1/30 |
| | F0/0 | 192.168.10.1/24 |
| R2 | S0/0/0 | 10.1.1.2/30 |
| | S0/0/1 | 10.2.2.1/30 |
| | S0/1/0 | 209.165.200.225/27 |
| | F0/0/0 | 192.168.20.1/24 |
| R3 | S0/0/1 | 10.2.2.2/30 |
| | F0/0 | 192.168.30.1/24 |
| PC1 | Сетевой адаптер | 192.168.10.10/24 |
| PC2 | Сетевой адаптер | 192.168.30.10/24 |
| local.pka | Сетевой адаптер | 192.168.20.254/24 |

| Устройство | Интерфейс | IP-адрес |
|---|---|---|
| Внешний компьютер | Сетевой адаптер | 209.165.201.14/28 |
| cisco.pka | Сетевой адаптер | 209.165.201.30/28 |

PAT-это преобразователь адреса из трех внутренних локальных сетей в один внешний адрес. Кроме того, вы настроите статический NAT для преобразования внутреннего адреса сервера во внешний адрес.
В этом упражнении вы будете настраивать только маршрутизатор R2.
Используйте именованный ACL, чтобы разрешить преобразование адресов из LAN1, LAN2 и LAN3. Укажите локальные сети в этом порядке.
Используйте имя **R2NAT**. Используемое вами имя должно точно соответствовать этому имени.
Создайте пул NAT с именем **R2POOL**. Пул должен использовать **первый** адрес из адресного пространства **209.165.202.128/30**. Используемое вами имя пула должно точно соответствовать этому имени. Все преобразованные адреса должны использовать этот адрес в качестве внешнего адреса.
Настройте NAT с помощью созданного вами пула ACL и NAT.
Настройте статический NAT для сопоставления внутреннего адреса локального сервера.pka со **вторым** адресом из адресного пространства **209.165.202.128 / 30**.
Настройте интерфейсы, которые будут участвовать в NAT.
Конфигурации ответов
**Маршрутизатор R2**
включить
настройку
интерфейса терминала FastEthernet0 / 0
ip nat внутри
интерфейса Serial0 /0 / 0
 ip nat внутри
интерфейса Serial0 / 0 / 1
 ip nat внутри
интерфейса Serial0 / 1 / 0
 ip nat вне
пула ip nat R2POOL 209.165.202.129 209.165.202.129 маска сети 255.255.255.252
ip nat внутри списка источников R2NAT пул R2POOL перегрузка
ip nat внутри источника статический
192.168.20.254 209.165.202.130 стандартный список доступа к ip R2NAT
 разрешение 192.168.10.0 0.0.0.255
 разрешение 192.168.20.0 0.0.0.255
 разрешение 192.168.30.0 0.0.0.255
конец

## Список литературы

**1. Цифровые основы [Электронный ресурс] – Режим доступа https://netacad.sadlab.su/**
**2. Электронное учебное пособие cisco [Электронный ресурс] – Режим доступа https://cisco.nntc.nnov.ru/**
**3. Электронное учебное пособие cisco [Электронный ресурс] – Режим доступа http://ssa1.kbgtk07.ru/**
**4. Cisco Packet Tracer [Электронный ресурс] – Режим доступа: http://dvboyarkin.ru/wp-content/uploads/2015/05/1.Metodichka_Cisco_Packet_Tracer.pdf**