Министерство науки и высшего образования Российской Федерации

Томский государственный университет
систем управления и радиоэлектроники

Ф. Н. Захаров, В. С. Беликов

СЕТЕВЫЕ ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ
ЧАСТЬ 1

Лабораторный практикум
для обучающихся по техническим направлениям

Томск
2023

УДК 621.39
ББК 32.88-01
З–38

Рецензенты:
Акулиничев Ю.П., профессор кафедры радиотехнических систем, д-р техн. наук, профессор

Захаров, Фёдор Николаевич, Беликов, Валерий Сергеевич
З–38 Сетевые информационные технологии. Часть 1 : лабораторный практикум для обучающихся по техническим направлениям / Захаров Ф. Н., Беликов В. С. – Томск: Томск. гос. ун-т систем упр. и радиоэлектроники, 2023 – 69 с

Лабораторный практикум составлен с учетом требований федерального государственного образовательного стандарта высшего образования (ФГОС ВО).

Лабораторный практикум позволяет студентам закрепить знания в области сетевых технологий, сетевой модели OSI, базовых протоколов стека TCP/IP и освоить базовую настройку сетевых устройств локальной сети. Практикум предназначен для обучающихся по техническим направлениям, изучающих сетевые технологии.

Одобрено на заседании кафедры РТС, протокол № 5 от 01.12.2022

УДК 621.39
ББК 32.88-01

1 ВВЕДЕНИЕ

Лабораторный практикум содержит методические указания к выполнению девяти лабораторных работ по основам сетевых технологий. Лабораторный практикум позволяет студентам закрепить знания в области сетевых технологий, сетевой модели OSI, базовых протоколов стека TCP/IP и освоить базовую настройку сетевых устройств локальной сети. Практикум предназначен для обучающихся по техническим направлениям, изучающих сетевые технологии.

Цель лабораторных работ – получить представление о принципах работы локальных сетей и освоить базовые навыки настройки сетевого оборудования.

В лабораторном практикуме приведены следующие работы:

1. Изучение справки и навигации Packet Tracer
2. Основы работы в Cisco Packet Tracer и базовая настройка коммутатора
3. Изучение моделей TCP/IP и OSI
4. Подключение проводной и беспроводной локальных сетей
5. Использование программы Wireshark для просмотра сетевого трафика
6. Настройка локальной сети на основе коммутаторов
7. Анализ работы ARP протокола
8. Настройка маршрутизатора
9. Работа с IP-адресами

Лабораторные работы выполняются в программе сетевого моделирования Cisco Packet Tracer (работы 1-4 и 6-8), программе просмотра сетевого трафика Wireshark (работа 5) и калькуляторе Windows (работа 9).

Программное решение Cisco Packet Tracer позволяет имитировать работу различных сетевых устройств: маршрутизаторов, коммутаторов, точек беспроводного доступа, персональных компьютеров, сетевых принтеров, IP-телефонов и т. д. Работа с интерактивным симулятором дает весьма правдоподобное ощущение настройки реальной сети, состоящей из десятков или даже сотен устройств. Настройки, в свою очередь, зависят от характера устройств: одни можно настроить с помощью команд операционной системы Cisco IOS, другие – за счет графического веб-интерфейса, третьи – через командную строку операционной системы или графические меню.

Благодаря такому свойству Cisco Packet Tracer, как режим визуализации, пользователь может отследить перемещение данных по сети, появление и изменение параметров IP-пакетов при прохождении данных через сетевые устройства, скорость и пути перемещения IP-пакетов. Анализ событий, происходящих в сети, позволяет понять механизм ее работы и обнаружить неисправности. Cisco Packet Tracer может быть использован не только как симулятор, но и как сетевое приложение для симулирования виртуальной сети через реальную сеть, в том числе Интернет. Пользователи разных компьютеров, независимо от их местоположения, могут работать над одной сетевой топологией, производя ее настройку или устраняя проблемы. Эта функция многопользовательского режима Cisco Packet Tracer широко применяется для организации командной работы, а также для проведения игр и соревнований между удаленными участниками.

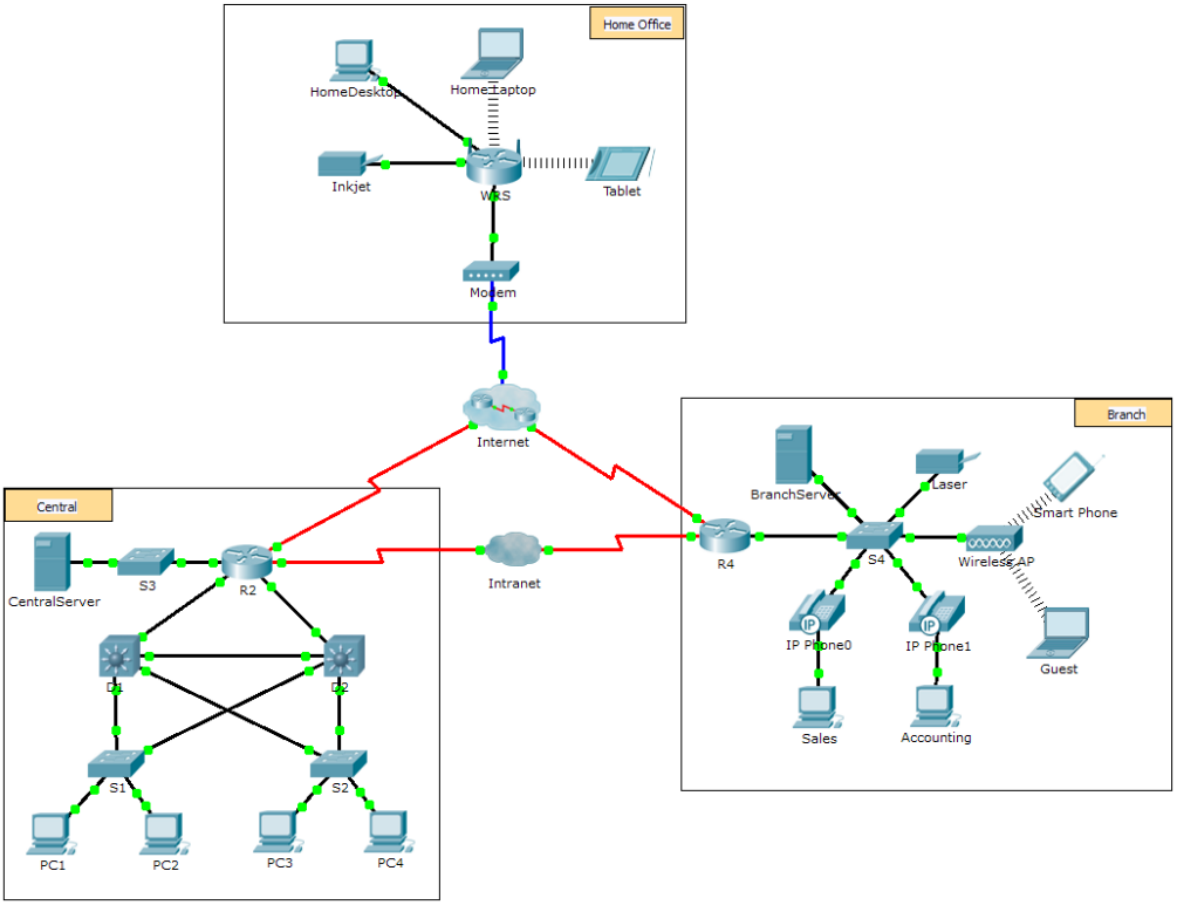
Помимо этого, с помощью Cisco Packet Tracer пользователь может симулировать построение не только логической, но и физической модели сети и, следовательно, получать навыки проектирования. Схему сети можно наложить на чертеж реально существующего здания или даже города и спроектировать всю его кабельную проводку, разместить устройства в тех или иных зданиях и помещениях с учетом физических ограничений, таких как длина и тип прокладываемого кабеля или радиус зоны покрытия беспроводной сети.

Wireshark – это широко распространённый инструмент для захвата и анализа сетевого трафика, который активно используется как для образовательных целей, так и для устранения неполадок на компьютере или в сети. Wireshark работает практически со всеми протоколами модели OSI, обладает понятным для обычного пользователя интерфейсом и удобной системой фильтрации данных. Помимо всего этого, программа является кроссплатформенной и поддерживает следующие операционные системы: Windows, Linux, Mac OS X, Solaris, FreeBSD, NetBSD, OpenBSD.

ЛАБОРАТОРНАЯ РАБОТА №1
ИЗУЧЕНИЕ СПРАВКИ И НАВИГАЦИИ PACKET TRACER

1 ВВЕДЕНИЕ

1.1 Топология сети



1.2 Задачи

Обзор программы Packet Tracer.

1.3 Общие сведения

Packet Tracer — простая, универсальная программа для домашнего использования, которая поможет вам в освоении учебного курса. С помощью Packet Tracer можно экспериментировать с сетевым поведением, создавать сетевые модели и проводить анализ типа «что, если».

В этой работе вы подробно ознакомитесь с принципом работы относительно сложной сети с помощью некоторых функций Packet Tracer. При этом вы узнаете, как пользоваться справкой и учебными руководствами. Вы также научитесь переключаться между различными режимами и рабочими областями. Чтобы увидеть сеть в полном масштабе, возможно, потребуется изменить размер окна Packet Tracer. При необходимости с помощью инструментов масштабирования можно настроить размер окна Packet Tracer.

2 ИЗУЧЕНИЕ ПРОГРАММЫ PACKET TRACER

2.1 Изучение справки и интерфейса

2.1.1 Получите доступ к разделам справки Packet Tracer, учебным видеороликам и интерактивным материалам

Доступ к разделам справки программы Packet Tracer можно получить двумя способами.

- Щелкнуть знак вопроса в правом верхнем углу меню панели инструментов.
- Открыть меню Help (Справка) и выбрать команду Contents (Содержимое).

Чтобы открыть учебные видеоролики Packet Tracer, выберите меню **Help** (Справка) > **Tutorials** (Учебные пособия). В этих видеоматериалах наглядно представлена информация из разделов **Help** (Справка), а также продемонстрированы различные возможности программы Packet Tracer. Чтобы получить некоторое представление об интерфейсе программы Packet Tracer и режиме симуляции можно посмотреть следующие видеоролики:

- видеоролик **Interface Overview** (Обзор интерфейса) в разделе **Getting Started** (Начало работы) учебных пособий.
- видеоролик **Simulation Environment** (Среда симуляции) в разделе **Realtime** and **Simulation Modes** (Режимы реального времени и симуляции) **учебных пособий**.

Найдите учебное пособие Configuring Devices Using the Desktop Tab (Настройка устройств с помощью вкладки Desktop). Посмотрите первую часть учебного пособия и ответьте на следующий вопрос: «Какие данные можно настроить в окне IP Configuration (Настройка IP-адресов)?».

2.1.2 Выполните переключение между режимами реального времени и симуляции

Найдите слово **Realtime** (Реальное время) в правом нижнем углу интерфейса Packet Tracer. В режиме реального времени сеть всегда действует как реальная независимо от того, работаете ли вы с ней или нет. Настройки применяются в реальном времени, и сеть реагирует на них в режиме, близком к реальному времени.

Перейдите на вкладку сразу за вкладкой **Realtime** (Реальное время), чтобы переключиться в режим **Simulation** (Симуляция). В режиме симуляции сеть отображается с более низкой скоростью, позволяя наблюдать за путями передачи данных и подробно исследовать пакеты данных.

Откройте панель моделирования и нажмите кнопку **Auto Capture/Play** (Автоматический захват/воспроизведение). Теперь вы должны видеть пакеты данных, представленные в виде конвертов разного цвета, которые движутся между устройствами.

Нажмите кнопку **Auto Capture/Play** (Автоматический захват/воспроизведение) еще раз, чтобы приостановить симуляцию.

Нажмите кнопку **Capture/Forward** (Захват/вперед), чтобы включить пошаговое моделирование. Нажмите кнопку еще несколько раз, чтобы увидеть процесс в действии.

В топологии сети слева щелкните один из конвертов на промежуточном устройстве и изучите его содержимое. По мере изучения курса вы познакомитесь с большей частью

содержимого этих конвертов. На данный момент попробуйте ответить на следующие вопросы.

1) На вкладке OSI Model (Модель OSI) сколько уровней In Layers (Входящие уровни) и Out Layers (Исходящие уровни) содержат информацию?
2) Какие заголовки у основных разделов на вкладках Inbound PDU Details (Сведения о входящей PDU) и Outbound PDU Details (Сведения об исходящей PDU)?
3) Несколько раз перейдите между вкладками Inbound PDU Details (Сведения о входящей PDU) и Outbound PDU Details (Сведения об исходящей PDU). Изменились ли данные? Если да, то как?

Нажмите кнопку-переключатель, расположенную над режимом **Simulation** (Симуляция) в правом нижнем углу, чтобы вернуться в режим **Realtime** (Реальное время).

2.1.3 Выполните переключение между логическим и физическим представлениями

Найдите слово **Logical** (Логическая) в левом верхнем углу интерфейса Packet Tracer. В настоящее время вы находитесь в рабочей области Logical (Логическая); ее вы будете использовать чаще всего для построения, настройки, изучения сетей и устранения неполадок в них.

Примечание. Несмотря на то, что в рабочую область Logical (Логическая) можно добавить географическую карту в качестве фонового изображения, как правило, эта карта никак не связана с фактическим физическим расположением устройств.

Перейдите на вкладку под областью **Logical** (Логическая), чтобы переключиться на рабочую область **Physical** (Физическая). Рабочая область Physical (Физическая) содержит физическое отображение логической топологии сети. Она позволяет оценить масштаб и расположение элементов (например, как сеть может выглядеть в реальной среде).

В курсе вы будете периодически использовать эту рабочую область. На данный момент вам просто необходимо знать, что она существует. Дополнительные сведения о физической рабочей области см. в файлах справки и учебных видеороликах.

Нажмите кнопку-переключатель под областью **Physical** (Физическая) в правом верхнем углу, чтобы вернуться в рабочую область **Logical** (Логическая).

2.2 Изучение сетевых устройств

2.2.1 Определите общие компоненты сети, представленные в Packet Tracer

Панель инструментов со значками в левом нижнем углу содержит сетевые компоненты различных категорий. Эти категории соответствуют промежуточным устройствам, оконечным устройствам и средствам подключения. Категория Connections (Подключения) (со значком молнии) представляет средства подключения, поддерживаемые программой Packet Tracer. Доступна также категория End Devices (Оконечные устройства) и две категории, связанные с Packet Tracer: Custom Made Devices (Устройства, изготовленные на заказ) и Multiuser Connection (Многопользовательское подключение).

1) Перечислите категории промежуточных устройств.
2) Не входя в облако Интернет или Интранет, перечислите количество значков в топологии, представляющих оконечные устройства (к ним идёт только один кабель или соединение).

3) Если не учитывать два облака, сколько значков в топологии представляют промежуточные устройства (к ним идут несколько соединений)?
4) Сколько оконечных устройств не являются настольными компьютерами?
5) Сколько типов средств подключения используются в этой топологии сети?

2.2.2 Объясните назначение устройств

В программе Packet Tracer только устройство Server-PT может выступать в роли сервера. Настольные и портативные компьютеры не могут быть серверами.

1) Объясните суть модели «клиент-сервер» на основе полученных знаний.
2) Назовите минимум две функции промежуточных устройств.
3) Назовите минимум два критерия для выбора типа средства сетевого подключения.

2.2.3 Сравните и сопоставьте локальные и глобальные сети

1) Объясните различия между локальной и глобальной сетью. Приведите примеры каждой из сетей.
2) Сколько глобальных сетей представлено в сети программы Packet Tracer?
3) Сколько представлено локальных сетей?
4) Интернет в этой сети Packet Tracer значительно упрощен и не отражает структуру и форму реального Интернета. Дайте краткое описание сети Интернет.
5) Перечислите несколько распространенных способов подключения домашних пользователей к Интернету.
6) Перечислите несколько распространенных методов подключения предприятий к Интернету в вашем регионе.

3 ЗАДАНИЕ НА РАБОТУ

3.1. Изучите материал и выполните задания раздела 2.

3.2. Добавьте оконечное устройство в топологию и подключите его к одной из локальных сетей, используя соответствующее средство подключения.

Попытайтесь ответить на вопросы:

1) Что еще требуется этому устройству для передачи данных другим конечным пользователям?
2) Как можно убедиться в правильности подключения устройства?

3.3. Добавьте промежуточное устройство в одну из сетей и подключите его к одной из локальных или глобальных сетей, используя соответствующее средство подключения.

Попытайтесь ответить на вопрос:

1) Что еще требуется этому устройству для работы в качестве промежуточного устройства для других устройств в сети?

3.4. Создайте небольшую локальную сеть и подключите его к существующей сети. Объясните ваше решение.

3.5. Напишите отчет.

Требования к отчету

Отчёт оформляется в соответствии с образовательным стандартом ТУСУР и содержит следующие элементы:

1) титульный лист;

2) цель работы;

3) скриншоты выполненных пунктов 3.2-3.4, комментарии к каждому скриншоту и ответы на вопросы из этих пунктов

4) выводы.

4 КОНТРОЛЬНЫЕ ВОПРОСЫ

1. Что такое сеть?

2. Перечислите компоненты сети.

3. Чем локальная сеть (LAN) отличается от глобальной (WAN)?

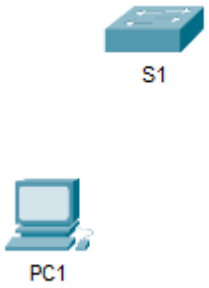
4. Перечислите и опишите элементы сети, с которыми вы работали при выполнении лабораторной работы.

ЛАБОРАТОРНАЯ РАБОТА №2
ОСНОВЫ РАБОТЫ В CISCO PACKET TRACER И БАЗОВАЯ НАСТРОЙКА КОММУТАТОРА

ЧАСТЬ 1. НАВИГАЦИЯ ПО IOS

1.1 Топология

Откройте **новый** документ Packet Tracer, выберете для работы коммутатор и ПК.



1.2 Задачи

1. Создание основных подключений, доступ к интерфейсу командной строки (CLI) и изучение справки
2. Изучение режимов EXEC
3. Настройка часов

1.3 Общие сведения

В этом упражнении вы сможете на практике отработать навыки, необходимые для навигации по операционной системе Cisco IOS, включая различные пользовательские режимы доступа, всевозможные режимы конфигурации, а также наиболее распространенные команды, используемые регулярно. Кроме того, вы поработаете с контекстной справкой при настройке команды **clock**.

1.4 Создание основных подключений, доступ к интерфейсу командной строки (CLI) и изучение справки

В этой части упражнения вы подключите ПК к коммутатору через консольное соединение и изучите различные командные режимы и функции справки.

1.4.1 Подключите PC1 к S1 с помощью консольного кабеля

Щелкните значок **Connections** (Подключения) (в виде молнии) в левом нижнем углу окна Packet Tracer.

Выберите светло-голубой консольный кабель, щелкнув по нему. Указатель мыши примет вид разъема со свисающим концом кабеля.

Щелкните **PC1**. В окне будет показан вариант для подключения RS-232.

Перетащите другой конец консольного подключения к коммутатору S1 и щелкните коммутатор, чтобы открыть список подключений.

Выберите порт **Console** (Консольный), чтобы завершить подключение.

1.4.2 Установите сеанс диалога с коммутатором S1

Щелкните **PC1** и откройте вкладку **Desktop** (Рабочий стол).

Щелкните значок приложения **Terminal** (Терминал). Проверьте правильность параметров конфигурации портов, заданных по умолчанию.

Нажмите **OK**.

В появившемся окне может отображаться несколько сообщений. В окне должно появиться сообщение Press RETURN to get started! (Нажмите ВОЗВРАТ, чтобы начать работу). Нажмите клавишу ввода.

1.4.3 Изучите справку по IOS

1) В IOS доступна справка по командам в зависимости от уровня работы. В данный момент отображается приглашение **User EXEC** (Пользовательский режим EXEC), и устройство ожидает ввода команды. Самый простой способ вызова справки — ввести вопросительный знак (?) в командной строке, чтобы получить список доступных команд.

```
S1> ?
```

В командной строке введите **t** с вопросительным знаком в конце (**?**).

```
S1> t?
```

Посмотрите, какие отображаются команды.

2) В командной строке введите **te** с вопросительным знаком в конце (**?**).

```
S1> te?
```

Посмотрите, какие отображаются команды.

Справка такого вида называется контекстной. Чем подробнее вводятся команды, тем больше сведений может предоставить справка.

1.5 Изучение режимов EXEC

В этой части упражнения вы переключитесь в привилегированный режим EXEC и выполните дополнительные команды.

1.5.1 Войдите в привилегированный режим EXEC

1) В командной строке введите вопросительный знак (**?**).

```
S1> ?
```

Посмотрите, какие из показанных данных описывают команду **enable**.

2) Введите **en** и нажмите клавишу **TAB**.

```
S1> en<Tab>
```

Посмотрите, что отображается после нажатия клавиши **TAB**.

Это называется завершением команды (или завершение нажатием клавиши TAB). Введя часть команды, можно нажать клавишу **TAB** и завершить частичный ввод этой команды. Если введенных символов достаточно для уникального определения команды (например, как в случае с командой **enable**), оставшаяся часть будет введена автоматически.

3) Введите команду **enable** и нажмите клавишу ввода.

4) Введите в командной строке вопросительный знак (**?**).

```
S1# ?
```

В пользовательском режиме EXEC только одна команда начинается с буквы «c». (**Совет**. Можно ввести «c?», чтобы отобразить только команды, начинающиеся с буквы «c».)

1.5.2 Войдите в режим глобальной конфигурации

1) В привилегированном режиме EXEC одна из команд, начинающихся с буквы «c», — **configure**. Введите либо команду полностью, либо столько символов, сколько будет нужно для уникального определения команды. Нажмите клавишу <**Tab**>, чтобы выполнить команду, и нажмите клавишу ввода.

```
S1# configure
```

Какое появилось сообщение?

2) Нажмите клавишу ввода, чтобы принять параметр по умолчанию, заключенный в квадратные скобки, — **[terminal]**.

Обратите внимание на то, как изменилась командная строка.

3) Такой режим называется режимом глобальной конфигурации. Он будет более подробно рассмотрен в последующих упражнениях и лабораторных работах. А теперь вернитесь в привилегированный режим EXEC, введя команду **end** или **exit** либо нажав клавиши **Ctrl+Z**.

```
S1(config)# exit
S1#
```

1.6 Настройка часов

1.6.1 Используйте команду clock

1) Используйте команду **clock**, чтобы подробнее изучить справку и синтаксис команды. Введите **show clock** в привилегированном режиме EXEC.

```
S1# show clock
```

2) Используйте контекстную справку и команду **clock**, чтобы установить текущее время на коммутаторе. Введите команду **clock** и нажмите клавишу ввода.

```
S1# clock<ENTER>
```

3) IOS вернет сообщение «% Incomplete command». Это означает, что для команды **clock** требуются дополнительные параметры. В справке можно получить дополнительные сведения, если ввести после команды пробел и вопросительный знак (?).

```
S1# clock ?
```

4) Установите время с помощью команды **clock set**. Продолжайте выполнять команду поэтапно.

```
S1# clock set ?
```

Посмотрите, какие отобразятся сведения, если ввести только команду **clock set**, не запрашивая справку с помощью вопросительного знака.

5) Взяв за основу сведения, запрошенные при помощи команды **clock set ?**, введите время 15:00 в 24-часовом формате (15:00:00). Проверьте, нужны ли дополнительные параметры.

```
S1# clock set 15:00:00 ?
```

Система возвращает запрос на получение дополнительных сведений.

<1-31> Day of the month

MONTH Month of the year

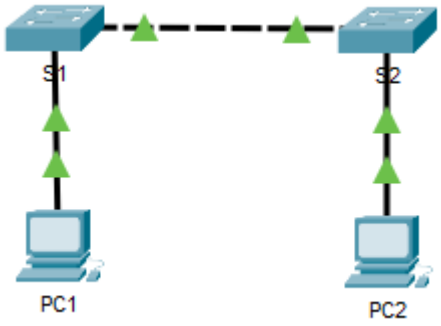
6) Попробуйте установить дату 31 января 2035 г., используя запрошенный формат. Для этого может потребоваться запросить дополнительную информацию с помощью контекстной справки. По окончании выполните команду **show clock**, чтобы отобразить настройку часов. В результате на экране должны отобразиться следующие данные.

```
S1# show clock
*15:0:4.869 UTC Tue Jan 31 2035
```

ЧАСТЬ 2. НАСТРОЙКА НАЧАЛЬНЫХ ПАРАМЕТРОВ КОММУТАТОРА

2.1 Топология

Создайте сеть, согласно топологии ниже



2.2 Задачи

1. Проверка конфигурации коммутатора по умолчанию
2. Настройка основных параметров коммутатора
3. Настройка баннера MOTD (сообщения дня)
4. Сохранение файлов конфигурации в NVRAM
5. Настройка коммутатора S2

2.3 Общие сведения

В этом упражнении вы осуществите базовую настройку коммутатора. Затем вам будет необходимо обеспечить безопасность доступа к интерфейсу командной строки (CLI) и портам консоли с помощью зашифрованных и текстовых паролей. Вы также научитесь настраивать сообщения для пользователей, выполняющих вход в систему коммутатора. Эти баннеры также предупреждают пользователей о том, что несанкционированный доступ запрещен.

2.4 Проверка конфигурации коммутатора по умолчанию

1) Введите команду **show running-config**.

```
Switch# show running-config
```

2) Ответьте для себя на следующие вопросы.

1) Сколько у коммутатора интерфейсов FastEthernet?
2) Сколько у коммутатора интерфейсов Gigabit Ethernet?
3) Каков диапазон значений, отображаемых в линиях vty?
4) Какая команда отображает текущее содержимое энергонезависимого ОЗУ (NVRAM)?
5) Почему коммутатор отвечает сообщением startup-config is not present?

2.5 Настройка основных параметров коммутатора

2.5.1 Присвойте коммутатору имя

Для настройки параметров коммутатора, возможно, потребуется переключаться между режимами настройки. Обратите внимание, как изменяется командная строка при переходе между режимами командной строки коммутатора.

```
Switch# configure terminal
Switch(config)# hostname S1
S1(config)# exit
S1#
```

2.5.2 Обеспечьте безопасный доступ к консоли

Для безопасного доступа к консоли перейдите в режим config-line и установите для консоли пароль **123** (Внимание! В работе используются простые пароли, но при настройке реального оборудования необходимо использовать длинные пароли).

```
S1# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)# line console 0
S1(config-line)# password 123
S1(config-line)# login
S1(config-line)# exit
S1(config)# exit
%SYS-5-CONFIG_I: Configured from console by console
S1#
```

2.5.3 Убедитесь, что доступ к консоли защищен

Выйдите из привилегированного режима, чтобы убедиться, что для консольного порта установлен пароль.

```
S1# exit
Switch con0 is now available
Press RETURN to get started.

User Access Verification
Password:
S1>
```

Примечание. Если коммутатор не выводит запрос на ввод пароля, значит, вы не настроили параметр **login** в шаге 2. Нужно перезагрузить коммутатор и заново настроить парольный доступ.

2.5.4 Защитите доступ к привилегированному режиму

Установите для **enable** пароль **456**. Этот пароль ограничивает доступ к привилегированному режиму.

```
S1> enable
S1# configure terminal
S1(config)# enable password 456
S1(config)# exit
%SYS-5-CONFIG_I: Configured from console by console
S1#
```

2.5.5 Убедитесь, что доступ к привилегированному режиму защищен

1) Введите команду **exit** еще раз, чтобы выйти из коммутатора.

2) Нажмите **<Enter>**, после чего вам будет предложено ввести пароль.

```
User Access Verification
Password:
```

3) Первый пароль — это пароль для доступа к устройству через консольное подключение, который был задан для **line con 0**. Введите этот пароль, чтобы вернуться в пользовательский режим EXEC.

4) Введите команду для доступа к привилегированному режиму.

5) Введите второй пароль, который был задан для ограничения доступа к привилегированному режиму EXEC.

6) Проверьте конфигурацию, изучив содержимое файла running-configuration:

```
S1# show running-config
```

Обратите внимание, что пароли для консоли и привилегированного режима отображаются в виде обычного текста. Это может быть небезопасно, так как пароль может увидеть любой находящийся рядом человек.

2.5.6 Настройте зашифрованный пароль для защиты доступа к привилегированному режиму

Открытый пароль **enable password** нужно заменить на новый зашифрованный пароль с помощью команды **enable secret**. Установите для enable secret пароль **789**.

```
S1# config t
S1(config)# enable secret 789
S1(config)# exit
S1#
```

Примечание. Пароль **enable secret** имеет приоритет перед паролем **enable password**. Если для коммутатора заданы оба пароля, для перехода в привилегированный режим EXEC нужно ввести пароль **enable secret**. Поэтому, при выполнении работ по курсу команду "**enable password** password» использовать не рекомендуется. Вместо неё нужно использовать команду «**enable secret** password».

2.5.7 Убедитесь, что в файл конфигурации добавлен пароль enable secret

1) Введите команду **show running-config** еще раз, чтобы проверить новый пароль **enable secret**.

Примечание. Команду **show running-config** можно сократить до

```
S1# show run
```

2) Посмотрите, что отображается при выводе пароля **enable secret**.

2.5.8 Зашифруйте пароли enable и console

Как было видно на предыдущем шаге, пароль **enable secret** зашифрован, а пароли **enable** password и **console** хранятся в виде обычного текста. Сейчас мы зашифруем эти открытые пароли с помощью команды **service password-encryption**.

```
S1# config t
S1(config)# service password-encryption
S1(config)# exit
```

2.6 Настройка баннера MOTD (сообщения дня)

В набор команд Cisco IOS входит команда, позволяющая настроить сообщение, которое будут видеть все, кто входит в систему на коммутаторе. Это сообщение называется сообщением дня или баннером MOTD (message of the day). Текст баннера нужно заключить в двойные кавычки или использовать разделитель, отличный от любого символа в строке MOTD.

```
S1# config t
S1(config)# banner motd "This is a secure system. Authorized Access Only!"
S1(config)# exit
%SYS-5-CONFIG_I: Configured from console by console
S1#
```

2.7 Сохранение файлов конфигурации в NVRAM

2.7.1 Проверьте правильность конфигурации с помощью команды show run

2.7.2 Сохраните файл конфигурации

Вы завершили основную настройку коммутатора. Теперь выполните резервное копирование файла конфигурации в NVRAM и убедитесь, что внесенные изменения не были потеряны при перезагрузке системы или отключении питания (команды **write** или **copy running-config startup-config**).

```
S1# write
Destination filename [startup-config]?[Enter]
Building configuration...
[OK]
```

2.7.3 Изучите файл загрузочной конфигурации

1) Какая команда отображает содержимое NVRAM?
2) Все ли внесенные изменения были записаны в файл?

2.8 Настройка коммутатора S2

Вы завершили настройку коммутатора S1. Теперь настройте коммутатор S2. Если вы не можете вспомнить команды, вернитесь к предыдущим пунктам.

Настройте для коммутатора S2 следующие параметры.

1) Имя устройства: **S2**.
2) Защитите доступ к консоли паролем **321**.
3) Задайте пароль enable password **654** и пароль enable secret **987**.
4) Введите в сообщении для пользователей, выполняющих вход в систему на коммутаторе свою фамилию, имя, отчество, факультет и номер группы.
5) Зашифруйте все открытые пароли.
6) Проверьте правильность конфигурации.
7) Сохраните файл конфигурации, чтобы предотвратить его потерю в случае отключения питания коммутатора.

ЧАСТЬ 3. НАСТРОЙКА УДАЛЕННОГО ДОСТУПА КОММУТАТОРА

3.1 Задачи

Используя настроенные в части 2 коммутаторы, настройте удаленный доступ к этим коммутаторам.

3.2 Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети
S1	VLAN 1	192.168.XX.253	255.255.255.0
S2	VLAN 1	192.168.XX.254	255.255.255.0
PC1	FastEthernet0	192.168.XX.1	255.255.255.0
PC2	FastEthernet0	192.168.XX.2	255.255.255.0
Примечание: XX – последние две цифры зачетки студента.			

3.3 Настройка ПК

Настройте IP-адрес для PC1 и PC2 согласно таблице адресации.

3.3.1 Настройте IP-адреса для обоих ПК

1) Щелкните PC1 и откройте вкладку **Desktop** (Рабочий стол).

2) Выберите **IP Configuration** (Настройка IP-адресов). В таблице адресации выше можно увидеть, что PC1 назначен IP-адрес 192.168.XX.1 и маска подсети 255.255.255.0. Введите эти данные для PC1 в окне **IP Configuration** (Настройка IP-адресов).

3) Повторите пункты 1) и 2) для компьютера PC2.

3.3.2 Проверьте подключение к коммутаторам

1) Щелкните PC1. Закройте окно **IP Configuration** (Настройка IP-адресов), если оно открыто. На вкладке **Desktop** (Рабочий стол) нажмите **Command Prompt** (Командная строка).

2) Введите команду **ping** с IP-адресом коммутатора S1 и нажмите клавишу ввода.
Packet Tracer → PC → Command Line 1.0

```
PC> ping 192.168.1.253
```

Был ли эхо-запрос обработан успешно?

3.3 Настройка интерфейса управления коммутатором

Настройте IP-адреса для коммутаторов S1 и S2.

3.3.1 Настройте IP-адрес для коммутатора S1.

Коммутаторы можно использовать в режиме «plug & play». Это значит, что они могут начать работать и без предварительной настройки. Коммутаторы пересылают данные между портами, опираясь на MAC-адреса. Настраивать IP-адреса нужно для возможности удалённо (из другой сети) настраивать коммутатор. Для этого на коммутаторе существуют виртуальные интерфейсы VLAN. Таких интерфейсов поддерживается до 1024. В рамках данного курса будет использоваться только первый интерфейс VLAN 1.

Чтобы настроить удалённый доступ по защищенному протоколу SSH, необходимо выполнить следующее:

1) задать имя устройства (измените ранее настроенные имена коммутаторов S1 и S2 на **S1_ФИО и S2_ФИО** (ФИО – инициалы студента латиницей), соответственно),
2) задать доменное имя,
3) сгенерировать ключ шифрования,
4) создать учётную запись администратора с паролем,
5) установить пароль для доступа к привилегированному режиму,
6) настроить IP-адрес интерфейса VLAN 1,
7) настроить доступ к виртуальному терминалу по протоколу SSH.

Доменное имя настраивается следующим образом (в работе используется доменное имя **test.cisco**):

```
S1(config)# ip domain-name test.cisco
```

Ключ шифрования генерируется с помощью команды:

```
S1(config)# crypto key generate rsa
```

После чего система запрашивает длину ключа. Рекомендованное значение **1024.**

Учетная запись администратора Admin и пароль ФИОXX (ФИО – инициалы студента латиницей, XX – последние две цифры зачетки студента):

```
S1(config)# username Admin secret ФИОXX
```

Чтобы настроить IP-адрес на коммутаторе S1, используйте следующие команды.

```
S1(config)# interface vlan 1
S1(config-if)# ip address 192.168.XX.253 255.255.255.0
S1(config-if)# no shutdown
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed
state to up
S1(config-if)#
S1(config-if)# exit
S1#
```

Настройка виртуального терминала, чтобы разрешить удаленный доступ по протоколу SSH:

```
S1# configure terminal
S1(config)# line vty 0 15
S1(config-line)# login local
S1(config)# transport input ssh
```

3.3.2 Настройте IP-адрес для коммутатора S2

Используя данные из таблицы адресации, настройте удаленный доступ для S2.

3.3.3 Проверьте настройки IP-адресов на коммутаторах S1 и S2

Команда **show ip interface brief** выводит сведения об IP-адресе, а также о состоянии всех портов и интерфейсов коммутатора. Для этого можно также использовать команду **show running-config**.

3.3.4 Сохраните конфигурации для S1 и S2 в NVRAM

Какая команда сохраняет файл конфигурации из RAM в NVRAM?

3.3.5 Проверьте подключение к сети

Подключение к сети можно проверить с помощью команды **ping**. Очень важно, чтобы подключения работали во всей сети. В случае сбоя необходимо устранить неполадку. Проверьте связь коммутаторов S1 и S2 с компьютерами PC1 и PC2.

1) Щелкните PC1 и откройте вкладку **Desktop** (Рабочий стол).

2) Нажмите **Command Prompt** (Командная строка).

3) С помощью команды ping проверьте доступность IP-адреса компьютера PC2.

4) С помощью команды ping проверьте доступность IP-адреса коммутатора S1.

5) С помощью команды ping проверьте доступность IP-адреса коммутатора S2.

Примечание. Команду **ping** можно использовать в интерфейсе командной строки коммутатора и на PC2.

Все эхо-запросы должны быть обработаны успешно. Если результат первой проверки – 80 %, повторите попытку. Теперь результат должен быть 100 %. Позже вы узнаете, почему первая проверка иногда завершается неудачно. Если проверить связь с устройствами не удается, проверьте конфигурацию на наличие ошибок.

3.3.6 Проверьте удаленный доступ

Зайдите на **PC1**, откройте вкладку Desktop и запустите программу для удалённого доступа к сетевому оборудованию «**Telnet / SSH Client**». В появившемся окне выберете протокол SSH, укажите IP-адрес коммутатора S2, а в поле Username имя учетной записи Admin. Нажмите Connect. Если всё настроено верно, то клиент запросит пароль для удаленного доступа, после чего вы получите удалённый доступ к коммутатору S2.

Аналогичным образом проверьте удаленный доступ с PC2 к коммутатору S1.

ЧАСТЬ 4. ЗАДАНИЕ НА РАБОТУ

4.1. Изучите материал и выполните задания частей 1-3.

4.2. Напишите отчет. В отчёт включите скриншоты выполненных пунктов работы.

Требования к отчету

Отчёт оформляется в соответствии с образовательным стандартом ТУСУР и содержит следующие элементы:

1) титульный лист;

2) цель работы;

3) таблица адресации и исходные требования из окна «PT Activity»;

4) скриншоты топологии сети, скриншоты выполненных пунктов **4.1-4.2**, комментарии к каждому скриншоту;

5) выводы.

5 КОНТРОЛЬНЫЕ ВОПРОСЫ

1. К какому компоненту сетевой ОС может быть отнесен драйвер?

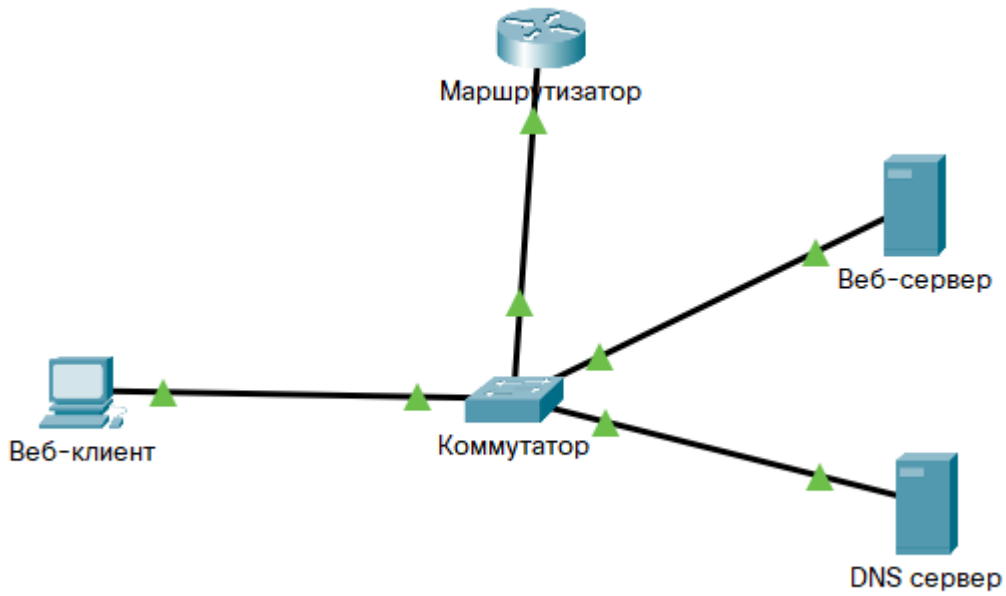
2. Для чего нужна настройка удаленного доступа к коммутатору?

3. Для чего нужна команда «write» и что произойдет, если её не выполнить?

ЛАБОРАТОРНАЯ РАБОТА №3
ИЗУЧЕНИЕ МОДЕЛЕЙ TCP/IP И OSI

1 ВВЕДЕНИЕ

1.1 Топология сети



1.2 Задачи

1. Изучение HTTP-трафика.

2. Отображение элементов семейства протоколов TCP/IP

1.3 Общие сведения

Данное упражнение по симуляции – первый шаг на пути к пониманию принципов работы стека проколов TCP/IP и его взаимосвязи с моделью OSI. Режим симуляции позволяет просматривать содержимое пересылаемых по сети данных на каждом из уровней.

При передаче данных по сети они разбиваются на более мелкие фрагменты и идентифицируются таким образом, чтобы их можно было воссоединить по прибытию в пункт назначения. Каждый фрагмент получает собственное имя (единица данных протокола – PDU) и ассоциируется с конкретным уровнем моделей TCP/IP и OSI. Режим симуляции программы Packet Tracer позволяет просматривать все уровни и относящиеся к ним PDU. Ниже описана последовательность шагов пользователя для запроса веб-страницы с веб-сервера с помощью установленного на клиентском ПК веб-браузера.

Хотя большая часть показанной на экране информации будет подробнее рассмотрена далее, это даст вам возможность ознакомиться с возможностями программы Packet Tracer, а также наглядно рассмотреть процесс инкапсуляции.

2. ИЗУЧЕНИЕ HTTP-ТРАФИКА

2.1 Перейдите из режима реального времени в режим симуляции

В правом нижнем углу интерфейса Packet Tracer (PT) находятся вкладки для переключения между режимами **Realtime** (режим реального времени) и **Simulation** (режим симуляции). PT всегда запускается в режиме реального времени, в котором сетевые протоколы работают с реалистичными значениями времени. Однако широкие возможности Packet Tracer позволяют пользователю «остановить время», переключившись в режим симуляции. В режиме симуляции пакеты отображаются как анимированные конверты, временем управляют события, и пользователи могут пошагово переходить от одного сетевого события к другому.

1) Щелкните значок режима **Simulation** для переключения из режима **реального времени** в режим **симуляции**.

2) Выберите в списке **Event List Filters** (Фильтры списка событий) пункт **HTTP**.

HTTP в этот момент уже может быть единственным видимым событием. Нажмите кнопку **Edit Filters** (Изменить фильтры) для отображения доступных видимых событий. Установите или снимите флажок **Show All/None** (Показать все/ничего) и обратите внимание на то, как изменится состояние установленных и снятых флажков.

Щелкайте флажок **Show All/None**, пока все флажки не будут сняты, а затем выберите **HTTP**. Щелкните любое место за пределами поля **Edit Filters**, чтобы скрыть его. В разделе видимых событий теперь отображается только HTTP.

2.2 Сгенерируйте веб-трафик (HTTP).

На данный момент панель симуляции пуста. В верхней части панели симуляции видны наименования шести столбцов списка событий. По мере генерации и продвижения трафика в списке будут появляться события. Столбец **Info** (Информация) содержит информацию о конкретном событии.

Примечание. Веб-сервер и веб-клиент показаны на левой панели. Размер панели можно изменить, если навести указатель на полосу прокрутки и, когда он примет вид двунаправленной стрелки, перетащить его влево или вправо.

1) Щелкните **Web Client** на крайней левой панели.

2) Щелкните вкладку **Desktop** (Рабочий стол), затем щелкните значок **Web Browser**, чтобы открыть веб-браузер.

3) В поле URL введите адрес **www.work.test** и нажмите кнопку **Go**.

Поскольку время в режиме симуляции привязано к событиям, для отображения событий в сети необходимо использовать кнопку **Capture/Forward** (Захват/вперед).

4) Нажмите кнопку **Capture/Forward** четыре раза. В списке событий должны быть четыре события.

Посмотрите на страницу веб-клиента в веб-браузере. Что-нибудь изменилось?

2.3 Изучите содержимое HTTP-пакета.

1) Щелкните первый цветной квадрат в столбце **Info** (Информация) списка событий **Event List**. Вам может понадобиться развернуть **панель симуляции** или использовать полосу прокрутки непосредственно под списком событий **Event List**.

Откроется окно **PDU Information at Device: Web Client** (Информация о PDU на устройстве: веб-клиент). В этом окне есть только две вкладки: **OSI Model** (Модель OSI) и **Outbound PDU Details** (Сведения об исходящей PDU), поскольку это только начало передачи. По мере изучения новых событий станут видны три вкладки, включая новую вкладку **Inbound PDU Details** (Сведения о входящей PDU). Когда событие является последним в потоке трафика, отображаются только вкладки **OSI Model** и **Inbound PDU Details**.

2) Убедитесь в том, что выбрана вкладка **OSI Model**. Убедитесь, что в столбце **Out Layers** (Исходящие уровни) выделено поле **Layer 7** (Уровень 7).

Какой текст отображается рядом с меткой **Layer 7**?

Какая информация перечислена в пронумерованных шагах непосредственно под полями **In Layers** (Входящие уровни) и **Out Layers** (Исходящие уровни)?

3) Нажмите кнопку **Next Layer** (Следующий уровень). Должен быть выделен уровень 4. Какое значение имеет параметр **Dst Port** (Порт назначения)?

4) Нажмите кнопку **Next Layer** (Следующий уровень). Должен быть выделен уровень 3. Какое значение имеет параметр **Dest. IP** (IP-адрес назначения)?

5) Нажмите кнопку **Next Layer** (Следующий уровень). Какая информация отображается на этом уровне?

6) Щелкните вкладку **Outbound PDU Details** (Сведения об исходящей PDU).

Сведения на вкладке **PDU Details** (Сведения о PDU) отражают уровни модели TCP/IP.

Примечание. Сведения в разделе **Ethernet II** представляют собой еще более подробные данные, чем показанные в разделе уровня 2 на вкладке **OSI Model**. Вкладка **Outbound PDU Details** содержит более описательные и подробные сведения. Значения **DEST MAC** (MAC-адрес назначения) и **SRC MAC** (MAC-адрес источника) в разделе **Ethernet II** на вкладке **PDU Details** отображаются на вкладке **OSI Model** в разделе Layer 2, но не указаны в качестве таковых.

Если сравнить сведения в разделе **IP** вкладки **PDU Details** со сведениями на вкладке **OSI Model**, какая информация является для них общей? К какому уровню она относится?

Если сравнить сведения в разделе **TCP** вкладки **PDU Details** со сведениями на вкладке **OSI Model**, какая информация является для них общей и к какому уровню она относится?

Какой **Host** (узел) указан в разделе **HTTP** вкладки **PDU Details**? С каким уровнем будут связаны эти сведения на вкладке **OSI Model**?

7) Щелкните следующий цветной квадрат в столбце **Info** списка **Event List**. Активен только уровень 1 (не отображается серым цветом). Устройство извлекает кадр из буфера и помещает его в сеть.

8) Перейдите к следующему полю HTTP **Info** в списке событий **Event List** и щелкните цветной квадрат. В этом окне есть два столбца: **In Layers** и **Out Layers**. Обратите внимание на направление стрелки непосредственно под столбцом **In Layers**. Она смотрит вверх, показывая направление перемещения данных. Пролистайте эти уровни, обращая внимание на просмотренные ранее элементы. В верхней части столбца стрелка указывает вправо. Это означает, что сервер теперь отправляет данные обратно клиенту.

Сравните данные в столбце **In Layers** с данными в столбце **Out Layers** и скажите, в чем заключается основное отличие между ними.

9) Щелкните вкладку **Outbound PDU Details** (Сведения об исходящей PDU). Прокрутите вниз до раздела **HTTP**.

Какова первая строка в показанном HTTP-сообщении?

10) Щелкните последний цветной квадрат в столбце **Info**. Сколько вкладок отображается с этим событием и почему?

3. ОТОБРАЖЕНИЕ ЭЛЕМЕНТОВ СЕМЕЙСТВА ПРОТОКОЛОВ TCP/IP

3.1 Просмотрите дополнительные события

1) Закройте все окна со сведениями о PDU.

2) В разделе Event List Filters > Visible Events (Фильтры списка событий > Видимые события) нажмите кнопку **Show All** (Показать все).

Какие дополнительные типы событий показаны?

Эти дополнительные записи играют различные роли в семействе протоколов TCP/IP. Если в списке указан ARP (протокол разрешения адресов), то этот протокол осуществляет поиск MAC-адресов. Протокол DNS отвечает за преобразование имен (например, **www.google.com**) в IP-адреса. Дополнительные события TCP связаны с установлением соединений, согласованием параметров связи и разъединением сеансов связи между устройствами. Эти протоколы упоминались ранее и будут рассмотрены более подробно в ходе изучения курса. В настоящее время Packet Tracer позволяет захватывать более 35 протоколов (типов событий).

3) Щелкните первое событие DNS в столбце **Info**. Просмотрите вкладки **OSI Model** и **PDU Detail** и обратите внимание на процесс инкапсуляции. На вкладке **OSI Model** с выделенным полем **Layer 7** непосредственно под столбцами **In Layers** и **Out Layers** отображается описание того, что происходит. ("1. The DNS client sends a DNS query to the DNS server." [DNS-клиент отправляет DNS-запрос на DNS-сервер]) Это очень полезная информация, которая помогает понять, что происходит во время процесса связи.

4) Щелкните вкладку **Outbound PDU Details** (Сведения об исходящей PDU). Какие сведения показаны в поле **NAME**: в разделе DNS QUERY?

5) Щелкните последний цветной квадрат DNS **Info** в списке событий. Какое устройство отображено?

Какое значение показано рядом с полем **ADDRESS**: в разделе DNS ANSWER на вкладке **Inbound PDU Details**?

6) Найдите первое событие **HTTP** в списке и щелкните цветной квадрат события **TCP** сразу после этого события. Выделите **Layer 4** на вкладке**OSI Model**. Какие сведения отображаются под пунктами 4 и 5 в пронумерованном списке непосредственно под столбцами **In Layers** и **Out Layers**?

TCP, наряду с другими функциями, управляет подключением и отключением канала связи. Данное конкретное событие указывает на то, что канал связи был установлен (ESTABLISHED).

7) Щелкните последнее событие TCP. Выделите Layer 4 на вкладке **OSI Model**. Проверьте действия, перечисленные непосредственно под столбцами **In Layers** и **Out Layers**. Расскажите, для чего предназначено событие, используя информацию, предоставленную в последнем пункте списка (это должен быть пункт 4).

4. ЗАДАНИЕ НА РАБОТУ

В этом упражнении по симуляции рассмотрен пример сеанса веб-связи между клиентом и сервером в локальной сети (LAN). Клиент делает запросы к определенным службам, функционирующим на сервере. Сервер должен быть настроен на прослушивание определенных портов для получения запросов клиентов. (Совет. Для получения информации о порте см. Layer 4 на вкладке **OSI Model**.)

1) Очистите панель симуляции, нажав на кнопку **Reset Simulation**. Установите фильтр на протоколы HTTP и DNS.

2) Откройте в браузере на Веб-клиенте сайт **www.work.test**.

3) Запустите симуляцию. У вас должно захватиться 7 пакетов протокола DNS и 7 пакетов протокола HTTP, как показано на рисунке ниже.

Event List

Vis.	Time(sec)	Last Device	At Device	Type
	0.000	--	Веб-клиент	DNS
	0.004	--	Веб-клиент	DNS
	0.005	Веб-клиент	Коммутат...	DNS
	0.006	Коммутатор	DNS серв...	DNS
	0.007	DNS сервер	Коммутат...	DNS
	0.008	Коммутатор	Веб-клиент	DNS
	0.016	--	Веб-клиент	HTTP
	0.017	--	Веб-клиент	HTTP
	0.018	Веб-клиент	Коммутат...	HTTP
	0.019	Коммутатор	Веб-серв...	HTTP
	0.020	Веб-сервер	Коммутат...	HTTP
	0.021	Коммутатор	Веб-клиент	HTTP

4) Используя полученные данные, заполните следующие таблицы.

4.1) Для первого DNS пакета, выходящего с Веб-клиента

Параметр	**Значение**
Столбец Out Layers	
Транспортный уровень (Layer 4), порт источника (Src Port)	
Транспортный уровень (Layer 4), порт назначения (Dst Port)	
Сетевой уровень (Layer 3), IP-адрес источника (Src. IP)*	
Сетевой уровень (Layer 3), IP-адрес назначения (Dst. IP)*	
Вкладка Outbound PDU Details	
IP-адрес источника (SRC IP) в пакете IP*	
IP-адрес назначения (DST IP) в пакете IP*	
Порт источника (SOURSE PORT) в сегменте UDP	
Порт назначения (DESTINATION PORT) в сегменте UDP	
Значение поля «NAME» DNS запроса (DNS Query)	
* По IP-адресам дополнительно определите и запишите в таблицу соответствующие им устройства	

4.2) Для DNS пакета, выходящего с DNS сервера

Параметр	**Значение**
Вкладка Inbound PDU Details	
IP-адрес источника (SRC IP) в пакете IP*	
IP-адрес назначения (DST IP) в пакете IP*	
Порт источника (SOURSE PORT) в сегменте UDP	
Порт назначения (DESTINATION PORT) в сегменте UDP	
Значение поля «NAME» DNS запроса (DNS Query)	
Значение поля «IP» DNS ответа (DNS Answer)	
* По IP-адресам дополнительно определите и запишите в таблицу соответствующие им устройства	

4.3) Для первого HTTP пакета, выходящего с Веб-клиента

Параметр	**Значение**
Столбец Out Layers	
Транспортный уровень (Layer 4), порт источника (Src Port)	
Транспортный уровень (Layer 4), порт назначения (Dst Port)	
Сетевой уровень (Layer 3), IP-адрес источника (Src. IP)*	
Сетевой уровень (Layer 3), IP-адрес назначения (Dst. IP)*	
Вкладка Outbound PDU Details	
IP-адрес источника (SRC IP) в пакете IP*	
IP-адрес назначения (DST IP) в пакете IP*	
Порт источника (SOURSE PORT) в сегменте TCP	
Порт назначения (DESTINATION PORT) в сегменте TCP	
* По IP-адресам дополнительно определите и запишите в таблицу соответствующие им устройства	

4.4) Для HTTP пакета, выходящего с Веб-сервера

Параметр	**Значение**
Вкладка Inbound PDU Details	
IP-адрес источника (SRC IP) в пакете IP*	
IP-адрес назначения (DST IP) в пакете IP*	
Порт источника (SOURSE PORT) в сегменте TCP	
Порт назначения (DESTINATION PORT) в сегменте TCP	
* По IP-адресам дополнительно определите и запишите в таблицу соответствующие им устройства	

4.5) По полученным данным опишите процесс работы протоколов DNS и HTTP и ответьте на вопросы:

Какой порт прослушивает **веб-сервер** для получения веб-запросов?

Какой порт прослушивает **DNS-сервер** для получения DNS-запросов?

5) Очистите панель симуляции. Установите фильтр на протокол ICMP.

6) Откройте на Веб-клиенте командную строку (Command Promt) и выполните ping запрос на маршрутизатор (IP адрес 10.0.0.1)

7) Запустите симуляцию. У вас должно захватиться не менее 6 пакетов протокола ICMP.

8) Используя полученные данные, заполните следующие таблицы.

8.1) Для ICMP пакета, выходящего с Веб-клиента и поступающего на коммутатор

Параметр	**Значение**
Вкладка Inbound PDU Details	
MAC адрес назначения (DEST ADDR) в кадре Ethernet	
MAC адрес источника (SRC ADDR) в кадре Ethernet	
IP-адрес источника (SRC IP) в пакете IP*	
IP-адрес назначения (DST IP) в пакете IP*	
* По IP-адресам дополнительно определите и запишите в таблицу соответствующие им устройства	

8.2) Для ICMP пакета, выходящего с маршрутизатора и поступающего на коммутатор

Параметр	**Значение**
Вкладка Inbound PDU Details	
MAC адрес назначения (DEST ADDR) в кадре Ethernet	
MAC адрес источника (SRC ADDR) в кадре Ethernet	
IP-адрес источника (SRC IP) в пакете IP*	
IP-адрес назначения (DST IP) в пакете IP*	
* По IP-адресам дополнительно определите и запишите в таблицу соответствующие им устройства	

9) Сделайте выводы по полученным результатам и напишите отчет.

Требования к отчету

Отчёт оформляется в соответствии с образовательным стандартом ТУСУР и содержит следующие элементы:

1) титульный лист;

2) цель работы;

3) скриншоты топологии сети, заполненные таблицы;

4) выводы.

5 КОНТРОЛЬНЫЕ ВОПРОСЫ

1. В чем отличие логической топологии сети от физической?

2. Что стандартизует модель OSI?

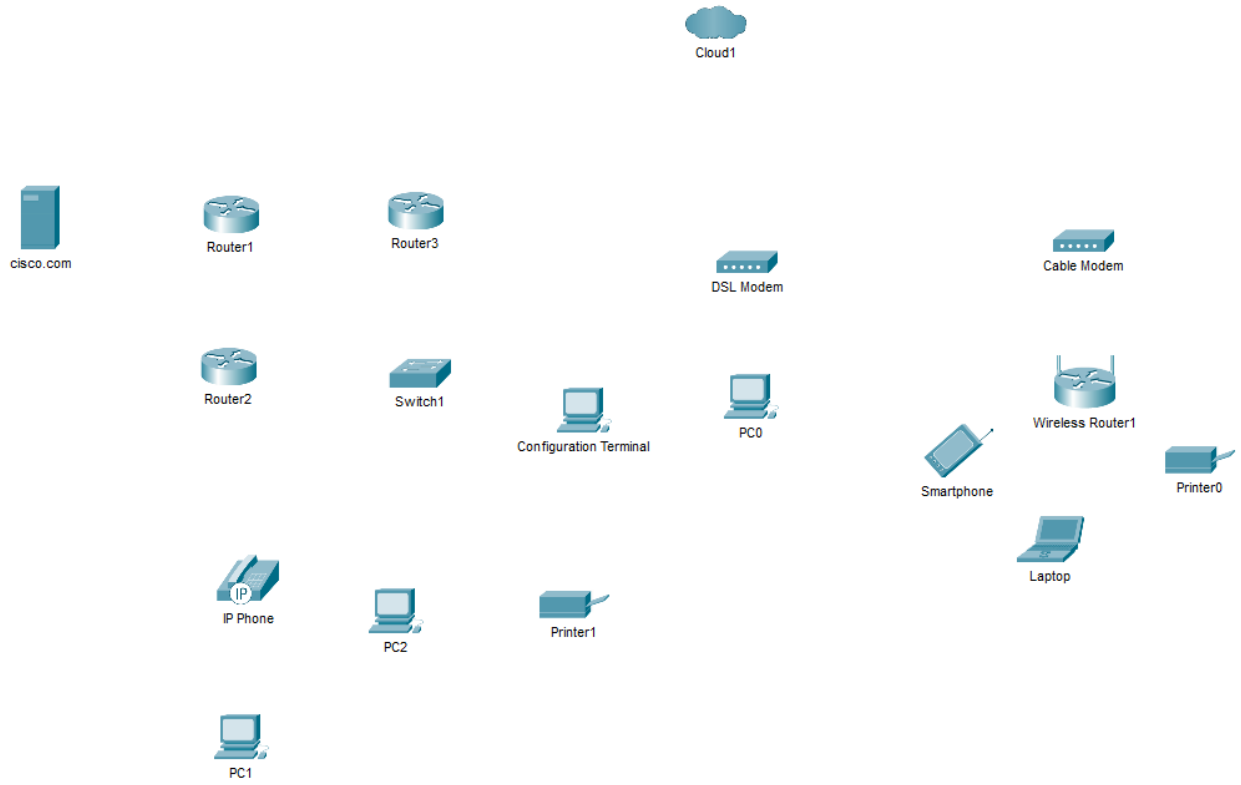
3. Что стандартизует стек OSI?

4. Дайте краткое описание функций каждого уровня и приведите примеры стандартных протоколов для каждого уровня модели OSI.

ЛАБОРАТОРНАЯ РАБОТА №4
ПОДКЛЮЧЕНИЕ ПРОВОДНОЙ И БЕСПРОВОДНОЙ ЛОКАЛЬНЫХ СЕТЕЙ

1 ВВЕДЕНИЕ

1.1 Топология



1.2 Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети	Подключается к	
				устройство	порт
Облачная среда	FastEthernet2	10.0.2.2	255.255.255.0	Router3	FastEthernet1/0
	Coaxial5	—	—	Кабельный модем	Port0
	Modem7	—	—	DSL модем	Port0
Кабельный модем	Port0	—	—	Облачная среда	Coax5
	Port1	—	—	WirelessRouter	Internet
DSL модем	Port0	—	—	Облачная среда	Modem7
	Port1	—	—	PC0	FastEthernet0
Router1	GigEthernet0/0	8.8.8.1	255.255.255.0	Cisco.com	FastEthernet0
	GigEthernet0/1	10.0.0.1	255.255.255.0	Router2	GigEthernet0/0
	Serial0/0/0	10.0.1.1	255.255.255.0	Router3	Serial0/0/0

Продолжение таблицы адресации

Router2	GigEthernet0/0	10.0.0.2	255.255.255.0	Router1	GigEthernet0/1
	GigEthernet0/1	192.168.XX.1	255.255.255.0	Switch	GigEthernet0/1
Router3	Serial0/0/0	10.0.1.2	255.255.255.0	Router1	Serial0/0/0
	FastEthernet1/0	10.0.2.1	255.255.255.0	Облачная среда	FastEthernet2
WirelessRouter	Internet	192.168.2.2	255.255.255.0	Кабельный модем	Port1
	Wireless	192.168.0.0	255.255.255.0	Smartphone, Laptoop, Printer0	Wireless
Switch	FastEthernet0/1	—	—	IP Phone	Switch
	FastEthernet0/2	—	—	PC2	FastEthernet0
	FastEthernet0/3	—	—	Printer1	FastEthernet0
	GigEthernet0/1	—	—	Router2	GigEthernet0/1
	VLAN1	172.16.0.2	255.255.255.0		—
	Консоль	—	—	Configuration Terminal	RS232
Cisco.com	FastEthernet0	8.8.8.8	255.255.255.0	Router1	GigEthernet0/0
PC0	FastEthernet0	192.168.200.10	255.255.255.0	DSL модем	Port1
PC1	FastEthernet0	192.168.XX.11	255.255.255.0	IP Phone	PC
PC2	FastEthernet0/2	192.168.XX.10	255.255.255.0	Switch	FastEthernet0/2
Configuration Terminal	RS232	—	—	Switch	Консоль
Laptoop	Wireless	DHCP	DHCP	WirelessRouter	Wireless
Smartphone	Wireless	DHCP	DHCP	WirelessRouter	Wireless
Printer0	Wireless	DHCO	DHCP	WirelessRouter	Wireless
Printer1	FastEthernet0	192.168.XX.254	255.255.255.0	Switch	FastEthernet0/3
IP Phone	Switch	—	—	Switch	FastEthernet0/1
	PC	—	—	PC1	FastEthernet0
Примечание: XX – последние две цифры зачетки студента.					

1.3 Задачи

1. Подключение сетевых устройств в соответствии с таблицей адресации.

2. Начальная настройка коммутатора.

1.4 Общие сведения

При работе в программе Packet Tracer (в рамках лабораторной работы или в реальных условиях) вы должны уметь выбирать необходимый кабель и надлежащим образом подключать устройства. В ходе данного упражнения будут рассмотрены: конфигурирование устройств в программе Packet Tracer, выбор кабеля в зависимости от конфигурации, а также подключение устройств. Работа выполняется в файле «Лабораторная работа 4.pkt».

2 ПОДКЛЮЧЕНИЕ СЕТЕВЫХ УСТРОЙСТВ

2.1 Подключение к облаку Cloud

1) В левом нижнем углу щелкните значок в виде оранжевой молнии, чтобы открыть список доступных **подключений**.

2) Выберите правильный кабель для подключения оптического порта **FastEthernet1/0 Router3** к порту **FastEthernet2 Cloud**. После подключения правильного кабеля индикатор канала на кабеле загорится зеленым цветом.

3) Выберите правильный кабель для подключения порта **Coaxial5 Cloud** к порту **Port0 Cable Modem (Кабельный модем)**. После подключения правильного кабеля индикатор канала на кабеле загорится зеленым цветом.

4) Выберите правильный кабель для подключения порта **Modem7 Cloud** к порту **Port0 DSL Modem** (телефонная линия). После подключения правильного кабеля индикатор канала на кабеле загорится зеленым цветом.

2.2 Подключение к маршрутизатору Router1

1) Выберите правильный кабель для подключения порта **Serial0/0/0 Router1** к порту **Serial0/0/0 Router3**. Используйте один из доступных последовательных (**Serial**) кабелей. После подключения правильного кабеля индикатор канала на кабеле загорится зеленым цветом.

2) Выберите правильный кабель для подключения порта **GigEthernet0/1 Router1** к порту **GigEthernet0/0 Router2**. Маршрутизаторы используют одинаковые контакты для отправки (1-й и 2-й) и получения (3-й и 6-й) данных. У кабеля, который нужно выбрать, эти пары меняются местами. Хотя многие современные сетевые платы могут автоматически определить, какие пары используются для приема и передачи, на маршрутизаторах Cisco нет сетевых плат с этой функцией автоопределения. После подключения правильного кабеля индикатор канала на кабеле загорится зеленым цветом.

3) Выберете медный прямой кабель для подключения порта **GigEthernet0/0 Router1** к порту **FastEthernet0** сервера **Cisco.com**. После подключения правильного кабеля индикатор канала на кабеле загорится зеленым цветом.

2.3 Подключение Configuration Terminal

Выберите правильный кабель для подключения порта **Console** коммутатора **Switch** к порту **RS232 Configuration Terminal**. Этот кабель не обеспечивает сетевой доступ к **Configuration Terminal**, но позволяет настроить **Switch** через терминал.

2.3 Подключение оставшихся устройств

1) Подключите оставшиеся устройства (кроме Laptoop, Smartphone и Printer0) согласно таблице адресации. Для подключения используйте медный прямой кабель.

2) На устройствах Laptoop, Smartphone и Printer0 включите модуль беспроводной связи и автоматическую настройку IP-адреса по протоколу DHCP.

3) IP-телефон необходимо подключить к сети питания (вкладка Physical –> Power adapter; сетевой адаптер необходимо подключить к соответствующему разъему на телефоне).

3 НАСТРОЙКА УСТРОЙСТВ

3.1 Начальная настройка коммутатора

Используя **Configuration Terminal**, выполните начальную настройку коммутатора:

1. Задайте коммутатору имя **Sw_ФИО** (ФИО – инициалы студента латиницей).
2. Используйте пароль **classXX** для всех линий (XX – последние две цифры зачетки студента).
3. Используйте скрытый (secret) пароль **ciscoXX** (XX – последние две цифры зачетки студента).
4. Зашифруйте все незашифрованные пароли.
5. Настройте удаленный доступ.
6. Включите в баннер MOTD вашу фамилию.
7. Сохраните настройки.

3.2 Настройка адресации маршрутизатора Router2

Порт **GigEthernet0/1** маршрутизатора **Router2** по умолчанию выключен и не имеет IP-адреса. Для настройки на нем IP-адреса в режиме глобальной конфигурации используйте следующие команды:

```
Router (config)#interface gig0/1
Router (config-if)#ip address 192.168.XX.1 255.255.255.0
Router (config-if)#no shutdown
Router (config-if)#exit
```

3.3 Настройка адресации устройств

1) Настройте адресацию для всех устройств в соответствии с таблицей адресации. Для устройств, подключенных к коммутатору, необходимо дополнительно задать **шлюз по умолчанию (Default Gateway)** 192.168.XX.1 и **DNS сервер** 8.8.8.8.

2) Убедитесь в наличии соединения между устройствами.

3) Подключение к серверу:

1. Откройте командную строку на PC1 или PC2 и выполните команду ping для сервера cisco.com.
2. Откройте веб-браузер на PC1 или PC2 и введите адрес cisco.com.

4 ЗАДАНИЕ НА РАБОТУ

4.1. Выполните задания предыдущих разделов

4.2. Напишите отчет, содержащий скриншоты каждого выполненного задания с Вашими пояснениями.

5 КОНТРОЛЬНЫЕ ВОПРОСЫ

1. Каким образом можно проверить наличие связи между устройствами?

2. Чем прямой кабель Ethernet отличается от кроссового?

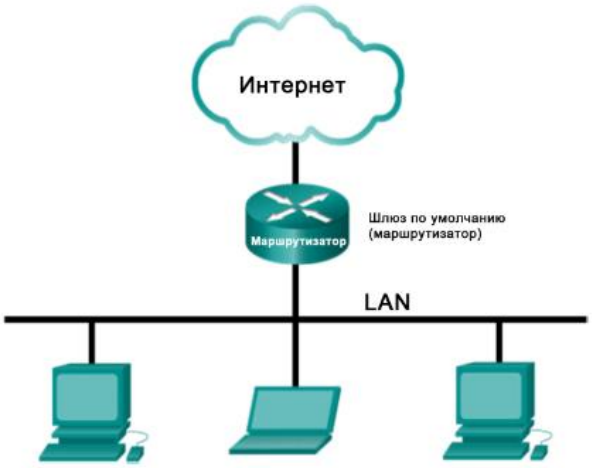
3. Для чего нужен кроссовый кабель Ethernet?

4. Какая топология используется в беспроводных сетях Wi-Fi?

ЛАБОРАТОРНАЯ РАБОТА №5
ИСПОЛЬЗОВАНИЕ ПРОГРАММЫ WIRESHARK ДЛЯ ПРОСМОТРА СЕТЕВОГО ТРАФИКА

1 ВВЕДЕНИЕ

1.1 Топология



1.2 Задачи

1. Сбор и анализ данных протокола ICMP в программе Wireshark при передаче данных в локальной сети.

2. Сбор и анализ данных протокола ICMP в программе Wireshark при передаче данных в удаленную сеть.

1.3 Общие сведения

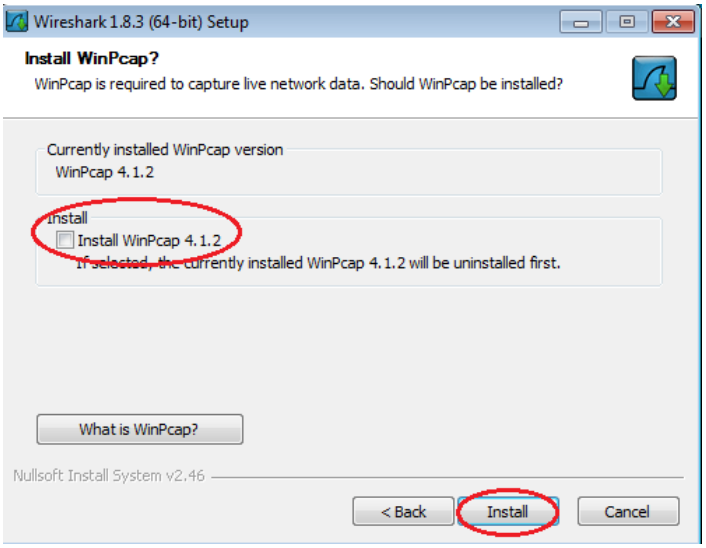
Wireshark – это программа для анализа протоколов (анализатор пакетов), которая используется для поиска и устранения неполадок в сети, анализа, разработки программного обеспечения и протоколов, а также обучения. По мере движения потоков данных по сети анализатор «захватывает» каждую единицу данных протокола (PDU), после чего расшифровывает или анализирует ее содержание согласно соответствующему документу RFC или другим спецификациям.

Wireshark – полезный инструмент для всех, кто работает с сетями. Его можно использовать для анализа данных, а также для поиска и устранения неполадок при выполнении большинства лабораторных работ в рамках курсов CCNA. В ходе лабораторной работы вы научитесь пользоваться программой Wireshark для захвата IP-адресов пакетов данных ICMP и MAC-адресов Ethernet-кадров.

1.4 Установка программы

Программу Wireshark можно загрузить с сайта www.wireshark.org.

Для сбора сетевых данных на ваш ПК необходимо установить программу WinPcap. Данная программа автоматически установится при установке Wireshark, если будет установлен флажок **Install WinPcap x.x.x** (Установить версию WinPcap с номером x.x.x).



2 СБОР И АНАЛИЗ ДАННЫХ ПРОТОКОЛА ICMP В ПРОГРАММЕ WIRESHARK ПРИ ПЕРЕДАЧЕ ДАННЫХ В ЛОКАЛЬНОЙ СЕТИ

2.1 Определение адреса интерфейсов вашего ПК.

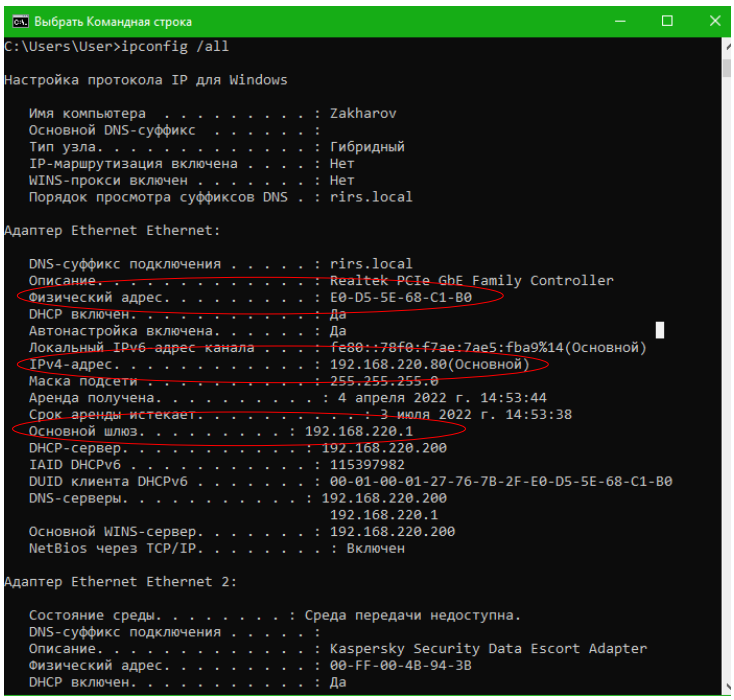
В этой части лабораторной работы вы должны отправить эхо-запрос с помощью команды ping на другой ПК в локальной сети и перехватить ICMP-запросы и отклики в программе Wireshark. Кроме того, вам нужно найти необходимую информацию в собранных кадрах. Этот анализ поможет понять, как заголовки пакетов позволяют доставлять данные адресатам.

Вам необходимо узнать IP-адрес компьютера и физический адрес сетевой платы, который называется MAC-адресом.

1) Откройте окно командной строки, введите команду **ipconfig /all** и нажмите клавишу ввода.

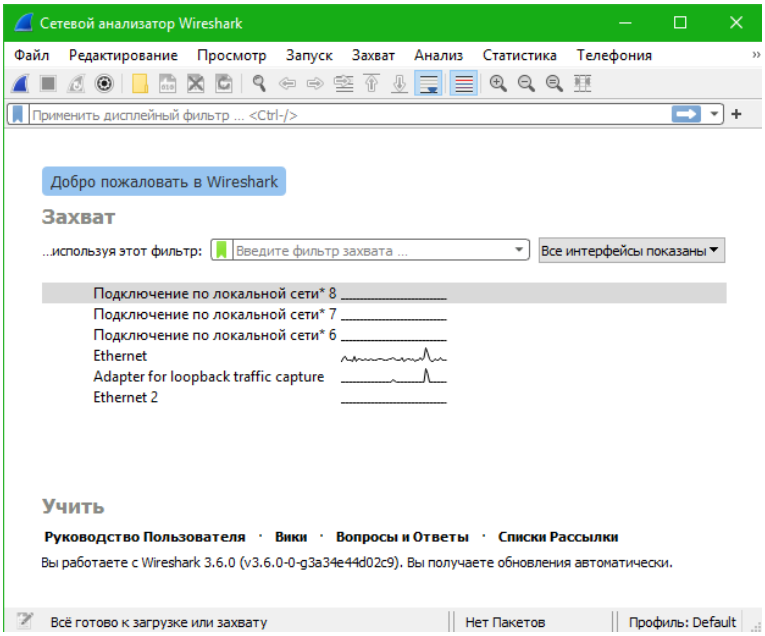
2) Запишите IP-адрес и MAC-адрес (физический адрес) интерфейса ПК, а так же IP адрес шлюза по умолчанию (основной шлюз).

3) Обменяйтесь IP-адресами ПК с другими учащимися, но пока что не сообщайте им свой MAC-адрес (ПК должны находиться в одной локальной сети).

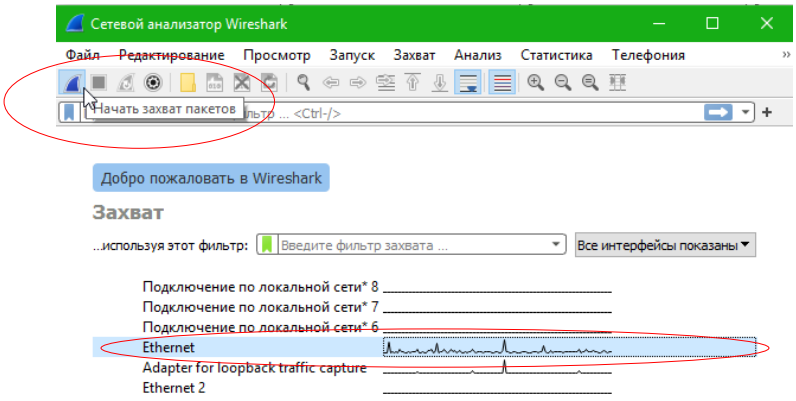


2.2 Запуск программы Wireshark и сбор данных

1) После запуска программы откроется список доступных на ПК интерфейсов (**Interface List**)

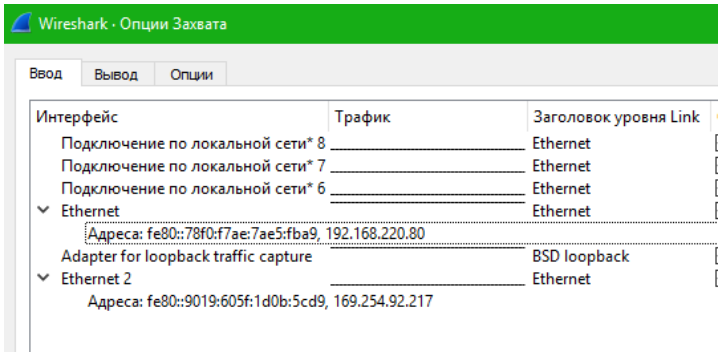


2) Выберите нужный интерфейс и нажмите кнопку «Начать захват пакетов».

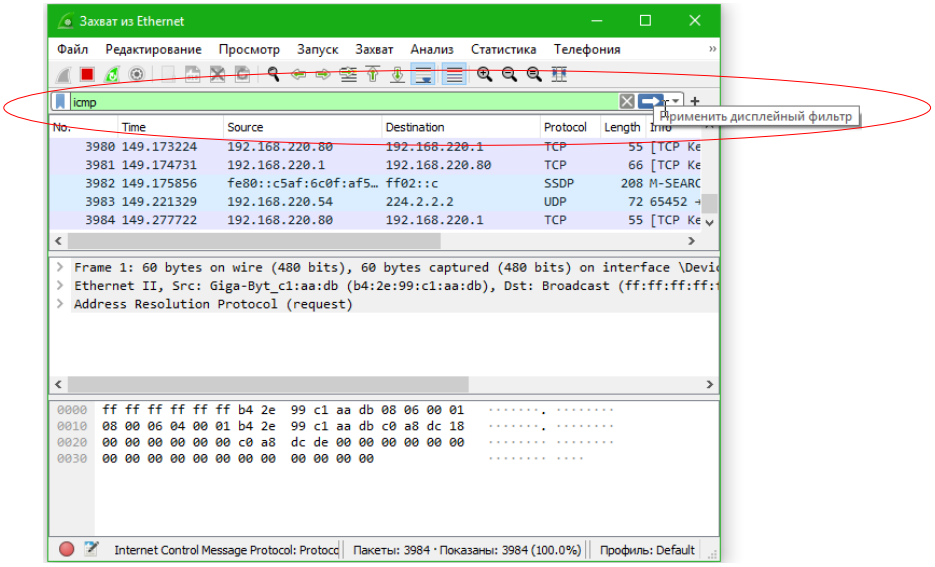


В верхней части окна программы Wireshark начнет прокручиваться информация. Строки данных выделяются различными цветами в зависимости от протокола.

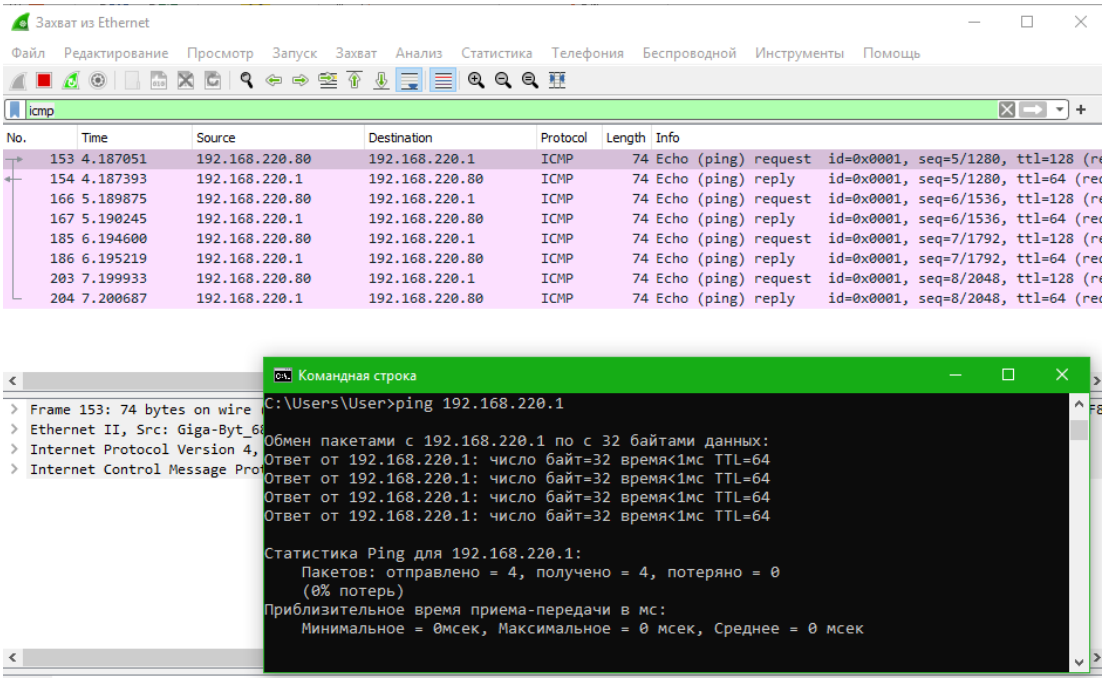
Примечание. Если вы не знаете, какой выбрать интерфейс, посмотрите название сети, которое отобразилось в командной строке после ввода команды ipconfig /all и для которой вы определяли IP и MAC адреса. Проверить правильность выбора можно в окне «Опции захвата», где указаны IP и MAC адреса каждого интерфейса ПК.



3) Информация может прокручиваться очень быстро, это зависит от интенсивности взаимодействия ПК с локальной сетью. Чтобы облегчить просмотр и работу с данными, собранными программой Wireshark, можно применить фильтр. В этой лабораторной работе нас интересуют только единицы данных протокола (PDU) ICMP (эхо-запрос с помощью команды ping). Чтобы вывести на экран только единицы данных протокола ICMP (эхо-запрос с помощью команды ping), в поле фильтра в верхней части окна программы Wireshark введите **icmp** и нажмите клавишу ввода или кнопку **Apply** (Применить фильтр).



4) После этого все данные в верхнем окне исчезнут, однако захват трафика в интерфейсе продолжится (если данные не исчезли, нажмите кнопку «Перезапустить текущий захват»). Откройте окно командной строки, которое вы открывали ранее, и отправьте эхо-запрос с помощью команды ping на IP-адрес, полученный от другого учащегося. Обратите внимание на то, что в верхней части окна программы Wireshark снова появятся данные.



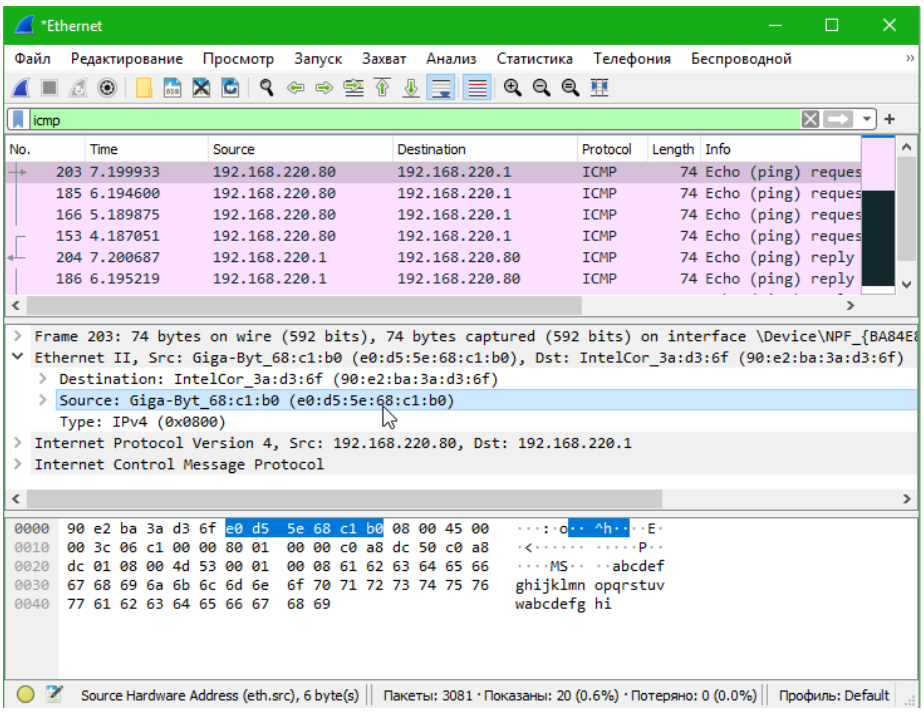
5) Остановите захват данных, нажав на значок «Остановить захват пакетов».

2.3 Анализ полученных данных

1) Программа Wireshark отображает данные в трех разделах: 1) в верхнем разделе отображается список полученных кадров PDU со сводной информацией об IP-пакетах; 2) в среднем разделе приводится информация о PDU для кадра, выбранного в верхней части экрана, а также разделение перехваченного кадра PDU по уровням протоколов; 3) в нижнем разделе показываются необработанные данные каждого уровня. Необработанные данные отображаются как в шестнадцатеричном, так и в десятичном форматах.

2) Выберите кадры PDU первого запроса ICMP в верхнем разделе окна программы Wireshark. Обратите внимание на то, что в столбце Source (Источник) указывается IP-адрес вашего компьютера, а в столбце «Destination» (Назначение) – IP-адрес ПК другого участника, на который вы отправили эхо-запрос с помощью команды ping.

3) Не меняя выбор кадра PDU в верхнем разделе окна, перейдите в средний раздел. Нажмите на символ «>» слева от строки «Ethernet II», чтобы увидеть MAC-адреса источника и назначения. Сравните эти адреса вашим адресом и адресом второго участника.



4) Посмотрите другие элементы кадра Ethernet и пакета Internet Protocol версии 4 и перечислите эти поля. Найдите поле Данные. Определите размер этого поля.

5) Полученные данные занесите в таблицу

Параметр	**Значение**
Размер кадра в битах и байтах	
MAC адрес назначения (Destination)	
MAC адрес источника (Source)	
IP адрес источника (Src)	
IP адрес назначения (Dst)	
Размер поля «Данные» IP пакета	
Версия IP протокола	

6) Отправьте эхо-запрос на шлюз по умолчанию. Заполните аналогичную таблицу.

3 СБОР И АНАЛИЗ ДАННЫХ ПРОТОКОЛА ICMP В ПРОГРАММЕ WIRESHARK ПРИ ПЕРЕДАЧЕ ДАННЫХ В УДАЛЕННУЮ СЕТЬ

В этой части вы должны будете отправить эхо-запросы с помощью команды ping на удаленные узлы (расположенные за пределами локальной сети) и изучить данные, сформированные этими запросами. Затем вам нужно будет определить различия между этими данными и данными, которые вы изучали в разделе 2.

3.1 Запуск захвата данных в интерфейсе

1) Нажмите на кнопку «Начать захват пакетов». Появится окно с предложением сохранить полученные ранее данные перед началом нового захвата. Сохранять эти данные необязательно. Нажмите «Продолжить без сохранения».

2) Активировав захват данных, отправьте эхо-запрос с помощью команды ping на следующие три URL-адреса веб-сайтов:

1) www.tusur.ru (если сайт не отвечает, то отправьте запрос на сайт www.yandex.ru)

2) www.cisco.com

3) www.google.com

Примечание. При отправке эхо-запросов с помощью команды ping на указанные URL-адреса обратите внимание на то, что служба доменных имен (DNS) преобразует адрес URL в IP-адрес. Запишите IP-адреса, полученные для каждого URL-адреса.

3) Остановите захват данных, нажав на кнопку «Остановить захват».

3.2 Анализ полученных данных

1) Нажмите на кнопку «Начать захват пакетов». Появится окно с предложением сохранить полученные ранее данные перед началом нового захвата. Сохранять эти данные необязательно. Нажмите «Продолжить без сохранения».

2) Просмотрите собранные данные в программе Wireshark и изучите IP- и MAC-адреса трех веб-сайтов, на которые вы отправили эхо-запросы. Заполните таблицу.

Веб-сайт	**IP-адрес назначения**	**MAC-адрес назначения**
www.tusur.ru		
www.cisco.com		
www.google.com		

3) Измените фильтр протоколов в верхней части окна программы Wireshark на dns. Определите IP-адрес и MAC-адрес DNS-сервера. Посмотрите, для каких сайтов отправляются DNS-запросы. Заполните таблицу.

Веб-сайт	**IP-адрес DNS-сервера**	**MAC-адрес DNS-сервера**
www.tusur.ru		
www.cisco.com		
www.google.com		

4) Измените фильтр протоколов в верхней части окна программы Wireshark на arp. Очистите ARP таблицу ПК (команда **arp -d** в командной строке). Отправьте эхо-запросы на устройства, указанные в таблице и для каждого ARP-запроса определите IP-адрес и MAC-адрес назначения.

Веб-сайт	**IP-адрес назначения**	**MAC-адрес назначения**
Соседний ПК		
Шлюз по умолчанию		
www.google.com		

Примечание. Подробнее протокол ARP будет рассматриваться в лабораторной работе № 7.

4 ЗАДАНИЕ НА РАБОТУ

4.1. Выполните задания предыдущих разделов

4.2. Напишите отчет, содержащий скриншоты каждого выполненного задания с Вашими пояснениями.

5 КОНТРОЛЬНЫЕ ВОПРОСЫ

1. Для чего нужен широковещательный MAC адрес?

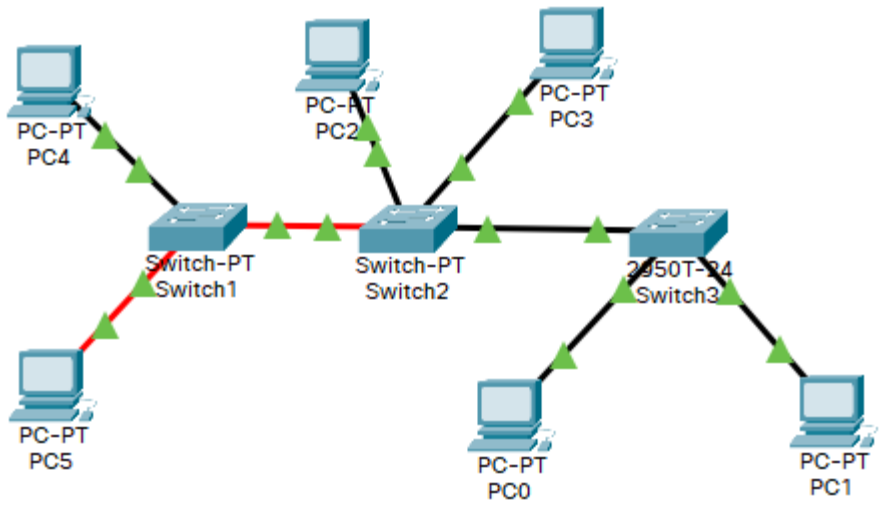
2. Почему при отправке эхо-запросов MAC-адреса назначения в исходящих кадрах не изменяются?

3. Для чего нужна служба доменных имен (DNS)?

ЛАБОРАТОРНАЯ РАБОТА №6
НАСТРОЙКА ЛОКАЛЬНОЙ СЕТИ НА ОСНОВЕ КОММУТАТОРОВ

1 ВВЕДЕНИЕ

1.1 Топология



1.2 Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети	Подключается к		Тип кабеля
				устройство	порт	
Switch1	GigEthernet	—	—	Switch2	GigEthernet	Оптический
	FastEthernet	—	—	PC	FastEthernet	UTP
	GigEthernet	—	—	PC	GigEthernet	Оптический
	VLAN1	172.16.XX.1	255.255.255.0	—	—	—
Switch2	GigEthernet	—	—	Switch1	GigEthernet	Оптический
	GigEthernet	—	—	Switch3	GigEthernet	UTP
	FastEthernet	—	—	PC	FastEthernet	UTP
	FastEthernet	—	—	PC	FastEthernet	UTP
	VLAN1	172.16.XX.2	255.255.255.0	—	—	—
Switch3	GigEthernet	—	—	Switch2	GigEthernet	UTP
	FastEthernet	—	—	PC	FastEthernet	UTP
	FastEthernet	—	—	PC	FastEthernet	UTP
	VLAN1	172.16.XX.3	255.255.255.0	—	—	—

Примечание:

1. ПК присвоить IP-адреса начиная с 172.16.XX.101 и не более 172.16.XX.120. Маска подсети 255.255.255.0
2. XX – последние две цифры зачетки студента.

1.3 Задачи

1. Собрать локальную сеть на основе коммутаторов согласно топологии.

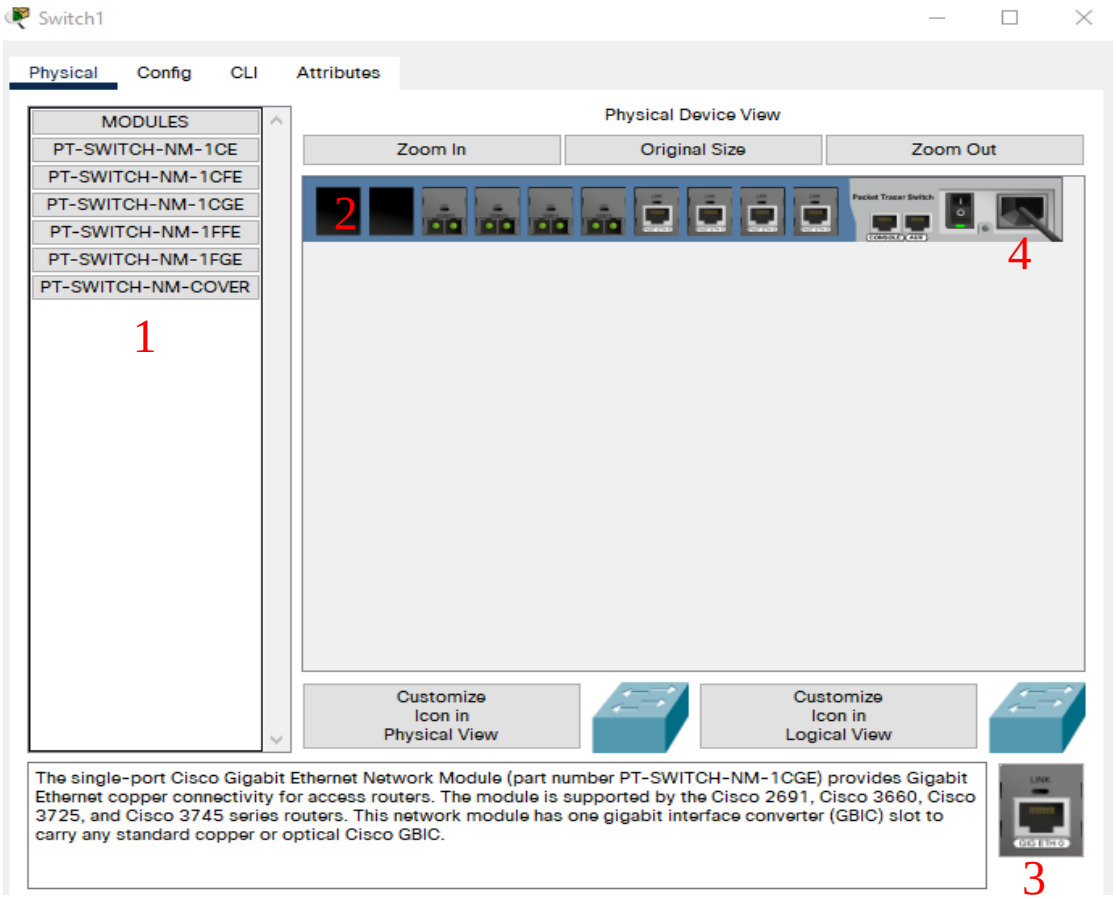
2. Выполнить базовую настройку коммутаторов и настроить удалённый доступ к ним с любого ПК.

2 ЗАДАНИЕ

2.1 Сбор локальной сети

1) Выбрать три коммутатора такие, что у первого и второго должны быть оптические интерфейсы, поддерживающие стандарт Gigabit Ethernet, а у второго и третьего интерфейсы, поддерживающие подключение по стандарту Gigabit Ethernet по кабелю типа UTP.

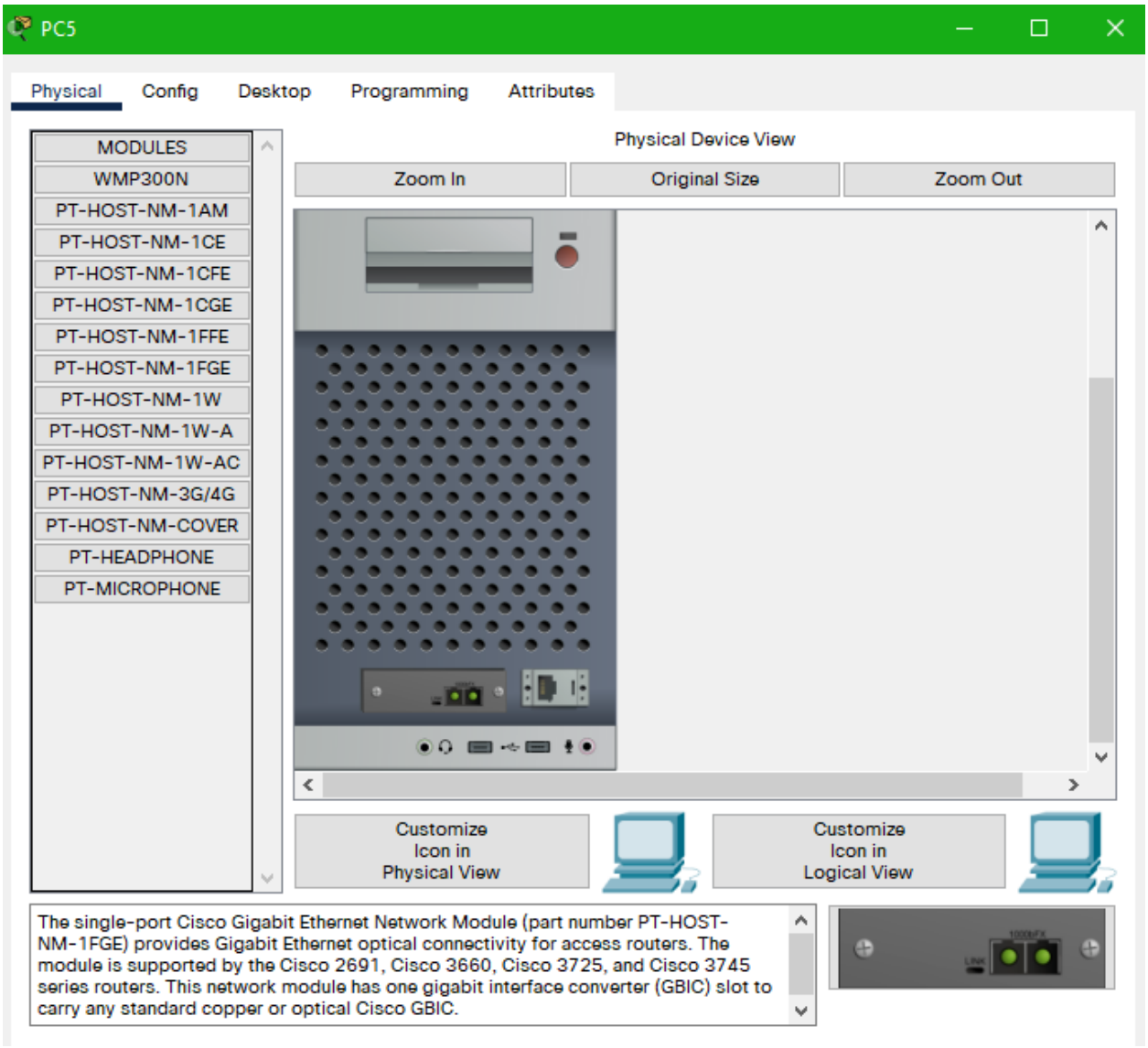
Если у коммутатора отсутствуют данные интерфейсы, то их можно добавить во вкладке Physical. Слева (цифра 1 на рисунке ниже) на вкладке находится список модулей, которыми можно укомплектовать устройство. В центральной части (Physical Device View) представлен внешний вид устройства и места, куда можно установить дополнительные модули (пустоты в виде чёрных прямоугольников – цифра 2). Вам нужно выбрать необходимый модуль (оптический Gigabit Ethernet или Gigabit Ethernet для витой пары) и перетащить его (цифра 3) на одно из свободных мест устройства. Так же можно удалить модули, перетащив их с устройства в правый нижний угол вкладки (цифра 3). Добавление и удаление устройств осуществляется при выключенном питании (цифра 4).



2) Соединить коммутаторы между собой соответствующими кабелями

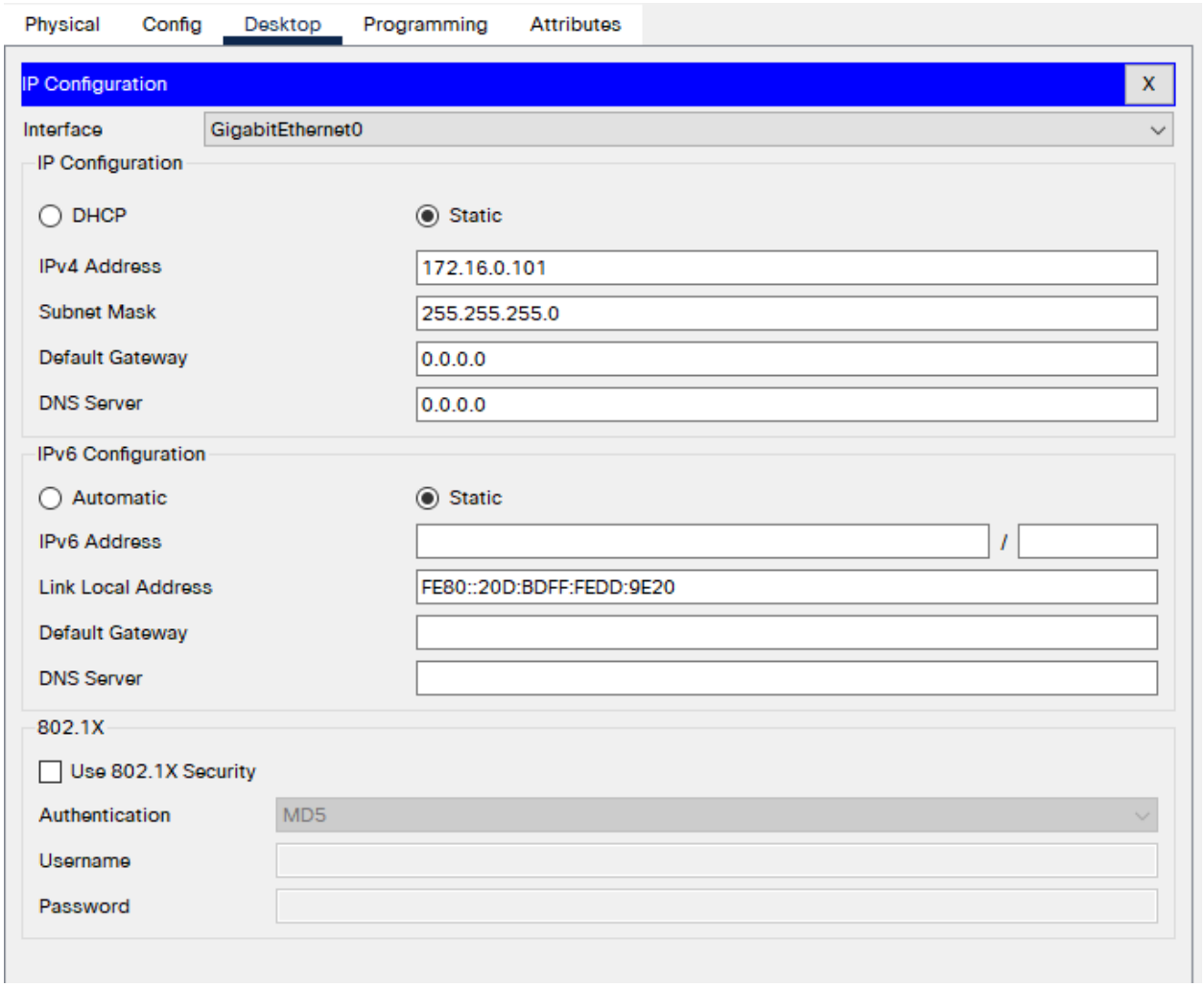
3) Выбрать произвольное количество ПК (не менее шести) и подключить их к коммутаторам. Один из ПК должен быть подключен к коммутатору с использованием

оптического кабеля. Для этого в ПК нужно вместо разъема Ethernet установить оптический разъем (см. рисунок ниже).



2.2 Настройка IP-адресов ПК

Каждому ПК назначить свой индивидуальный IP-адрес. Назначение IP-адресов необходимо выполнять в модуле IP Configuration на вкладке Desktop. IP-адреса для ПК должны начинаться с адреса 172.16.XX.101: первый ПК - 172.16.XX.101, второй ПК 172.16.XX.102 и т.д. Маска подсети для всех ПК 255.255.255.0.



2.3 Настройка коммутаторов

Для каждого коммутатора выполните следующее:

1. Задайте коммутатору имя **Sw_No_ФИО** (No – порядковый номер коммутатора, ФИО – инициалы студента латиницей).
2. Используйте пароль **classXX** для всех линий (XX – последние две цифры зачетки студента).
3. Используйте скрытый (secret) пароль **ciscoXX** (XX – последние две цифры зачетки студента).
4. Зашифруйте все незашифрованные пароли.
5. Настройте удаленный доступ по протоколу SSH и IP-адресу, указанному в таблице адресации.
6. Включите в баннер MOTD вашу фамилию и порядковый номер коммутатора.
7. Сохраните настройки.

2.4 Проверка удаленного доступа

1) С любого ПК выполните эхо-запросы на все остальные ПК и на виртуальные интерфейсы (VLAN 1) всех коммутаторов.

2) Выполните удалённый доступ к каждому коммутатору с любых двух ПК.

3) Напишите отчет, содержащий скриншоты успешно выполненных эхо-запросов.

5 КОНТРОЛЬНЫЕ ВОПРОСЫ

1. Какие функции выполняет коммутатор?

2. Для чего на коммутаторе нужен виртуальный интерфейс VLAN1 и почему он называется виртуальным?

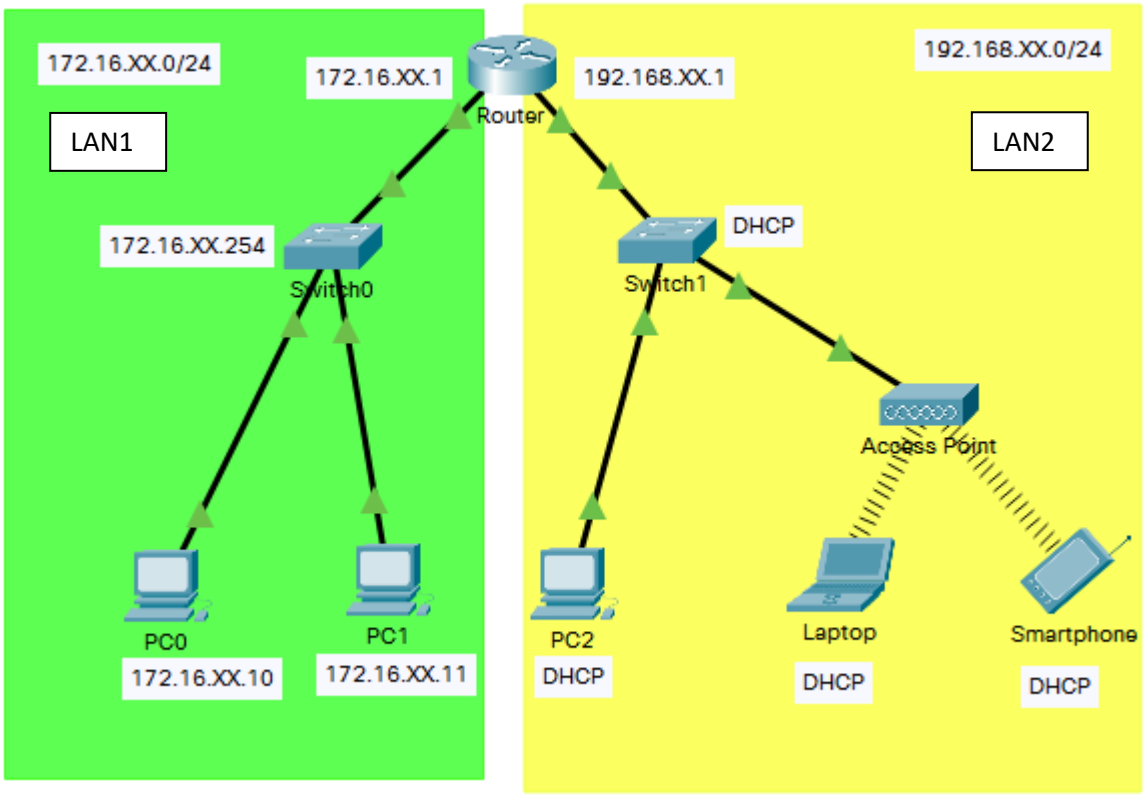
3. Что произойдёт, если на ПК не настроить IP-адрес?

4. Что произойдет, если на ПК указать IP-адрес соседнего ПК?

ЛАБОРАТОРНАЯ РАБОТА №7
АНАЛИЗ РАБОТЫ ARP ПРОТОКОЛА

1 ВВЕДЕНИЕ

1.1 Топология



1.2 Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети
Router	GigEthernet0/0	172.16.XX.1	255.255.255.0
	GigEthernet0/1	192.168.XX.1	255.255.255.0
Switch0	VLAN1	172.16.XX.254	255.255.255.0
Switch1	VLAN1	DHCP	DHCP
PC0	FastEthernet	172.16.XX.10	255.255.255.0
PC1	FastEthernet	172.16.XX.11	255.255.255.0
PC2	FastEthernet	DHCP	DHCP
Laptoop	Wireless	DHCP	DHCP
Smartphone	Wireless	DHCP	DHCP
Примечание: XX – последние две цифры зачетки студента.			

1.3 Задачи

1. Подключение и настройка сетевых устройств в соответствии с таблицей адресации.

2. Изучение ARP-запроса и ARP-ответа.

3. Изучение таблицы ARP сетевых устройств.

1.4 Общие сведения

Протокол ARP расшифровывается, как Address Resolution Protocol – протокол разрешения адресов. ARP – протокол разрешения адресов, который позволяет по IP-адресу определить MAC-адрес компьютера в локальной сети. ARP работает в режиме запрос-ответ. Запрос отправляется на широковещательный адрес и его получают все компьютеры в сети, а отвечает только тот компьютер, который узнал свой IP-адрес и в ответ он вкладывает искомый MAC-адрес. Результаты ARP запросов для повышения производительности записываются в ARP-таблицу.

2 ПОДКЛЮЧЕНИЕ И НАСТРОЙКА СЕТЕВЫХ УСТРОЙСТВ

2.1 Настройка коммутаторов

1) Выполните базовую настройку коммутатора **Switch0**, включая настройку удаленного доступа.

2) Выполните базовую настройку коммутатора **Switch1**, включая настройку удаленного доступа таким образом, чтобы IP-адрес виртуального интерфейса **VLAN1** назначался по протоколу **DHCP**, а не задавался вручную. Для этого при настройке IP-адреса виртуального интерфейса нужно выполнить следующую команду:

```
Switch(config-if)#ip address dhcp
```

2.2 Настройка портов маршрутизатора

1) Порт **GigEthernet0/0** маршрутизатора **Router** по умолчанию выключен и не имеет IP-адреса. Для настройки на нем IP-адреса в режиме глобальной конфигурации используйте следующие команды:

```
Router (config)#interface gig0/0
Router (config-if)#ip address 172.16.XX.1 255.255.255.0
Router (config-if)#no shutdown
Router (config-if)#exit
```

2) Аналогичным образом настройте порт **GigEthernet0/1** с учётом таблицы адресации.

2.3 Настройка DHCP сервера на маршрутизаторе

DHCP сервер можно реализовать на отдельном сервере или на маршрутизаторе. В небольших сетях нет необходимости устанавливать отдельный сервер, поэтому часто DHCP сервер реализуют на маршрутизаторе.

DHCP сервер — это специальная функция на маршрутизаторе, которая в автоматическом режиме назначает IP адреса для каждого подключающегося к сети устройства. Наличие работающего DHCP сервера на маршрутизаторе избавляет от необходимости вручную прописывать эти адреса для каждого устройства.

3) Для настройки DHCP сервера необходимо выполнить следующие команды:

```
Router#configure terminal                          Переход в режим глобальной конфигурации.
Router(config)#ip dhcp pool имя пула               Задаем имя пула адресов (произвольное)
Router(dhcp-config)#network 192.168.XX.0           Задаем IP-адрес сети и маску
255.255.255.0
Router(dhcp-config)#default-router                 Задаем IP-адрес шлюза по умолчанию
192.168.XX.1
Router(dhcp-config)#dns-server 192.168.XX.1        Задаем IP-адрес DNS-сервера
Router(dhcp-config)#exit
```

Далее необходимо указать адреса, которые нельзя выдавать сетевым устройствам. К этим адресам относятся адрес шлюза по умолчанию (порта маршрутизатора), зарезервированные адреса для некоторых сетевых устройств, например серверов, принтеров и т.п. В нашем случае исключим первые 10 IP-адресов:

```
Router(config)#ip dhcp excluded-address 192.168.0.1 192.168.0.10
```

Данной командой указывается первый и последний зарезервированные адреса. Т.е. маршрутизатор не будет выдавать сетевым устройствам адреса начиная с 192.168.0.1 и заканчивая 192.168.0.10.

2.4 Настройка адресации устройств

1) Настройте адресацию для оконечных устройств в соответствии с таблицей адресации. Для устройств, подключенных к коммутатору Switch1 и беспроводной точке доступа (Access Point) необходимо указать, что сетевые настройки получить по протоколу DHCP.

2) Убедитесь в наличии соединения между PC0 и обоими коммутаторами.

3 АНАЛИЗ ARP-ЗАПРОСА И ARP ТАБЛИЦЫ

3.1 Анализ сообщений ARP

1) На PC0 откройте командную строку и выполните команду **arp -d**, чтобы очистить таблицу ARP.

2) Перейдите в режим **Simulation** (Моделирование) и установите фильтр только на ARP сообщения (кнопка **Edit Filters**).

3) Создайте ARP-запросы, отправив эхо-запрос с PC0 на PC1. Будет создано две единицы данных протокола PDU. Команда **ping** не может отправить ICMP-пакет, не зная MAC-адрес назначения. Поэтому компьютер отправляет широковещательный кадр ARP, чтобы найти MAC-адрес назначения. В режиме Моделирования пошагово проследите за перемещением сообщения ARP от PC0 и обратно. На каждом шаге откройте сообщение и на вкладках **Inbound PDU Details** и **Outbound PDU Details** посмотрите содержимое ARP сообщения и заполните таблицу ниже:

	Кадр Ethernet		ARP сообщение			
Тип адреса	DEST ADDR (адрес получателя в кадре Ethernet)	SRC ADDR (адрес отправителя в кадре Ethernet)	Source MAC (MAC адрес источника)	Source IP (IP адрес источника)	Target MAC (MAC адрес получателя)	Target IP (IP адрес получателя)
Исходящее сообщение от PC0						
Значение:						
Принятое PC0 сообщение от PC1						
Значение:						

4) Отправьте эхо-запрос с PC0 на PC2 и заполните таблицу ниже:

	Кадр Ethernet		ARP сообщение			
Тип адреса	DEST ADDR (адрес получателя в кадре Ethernet)	SRC ADDR (адрес отправителя в кадре Ethernet)	Source MAC (MAC адрес источника)	Source IP (IP адрес источника)	Target MAC (MAC адрес получателя)	Target IP (IP адрес получателя)
Исходящее сообщение от PC0						
Значение:						
Исходящее сообщение от Маршрутизатора для PC0 (LAN1)						
Значение:						
Исходящее сообщение от Маршрутизатора в LAN2						
Значение:						
Принятое маршрутизатором сообщение от PC2						
Значение:						

Ответьте на вопросы:

1. Почему в ARP запросе от PC0 указан IP-адрес шлюза по умолчанию, а не PC2?
2. Почему Маршрутизатор тоже отправляет ARP-запрос?
3. Какие устройства в локальной сети 2 (LAN 2) получают ARP запрос от маршрутизатора?

3.2 Анализ ARP таблицы

1) Перейдите в режим Реального времени (**Realtime**) и выполните с PC0 эхо-запросы на все сетевые устройства, включая коммутаторы.

2) На PC0 откройте командную строку и выполните команду **arp -a**, чтобы посмотреть таблицу ARP. Сохраните эту таблицу в отчёт.

3) Посмотрите ARP таблицу на PC2 и ноутбуке. Сохраните эти таблицы в отчёт.

4) Посмотрите ARP таблицу на маршрутизаторе. Для этого выполните команду:

```
Router#show arp
```

По полученной таблице заполните следующую таблицу:

IP-адрес из ARP таблицы	MAC-адрес из ARP таблицы	Название сетевого устройства	MAC-адрес устройства*
172.16.0.10	0001.63C3.D14D	PC0	
…			
* Примечание: 1. Определить MAC адреса на ПК можно с помощью команды **ipconfig /all** в командной строке. 2. Определить MAC адреса коммутатора и маршрутизатора можно с помощью команды **show interfaces** в привилегированном режиме			

4 АНАЛИЗ ТАБЛИЦЫ MAC-АДРЕСОВ КОММУТАТОРА

1) Посмотрите таблицы MAC-адресов обоих коммутаторов. Для этого выполните команду **show mac-address-table** на каждом коммутаторе.

2) Определите, к какому поту коммутатора подключено какое устройство.

3) Ответьте на вопрос, почему у Switch1 два MAC-адреса связаны с одним портом?

5 ЗАДАНИЕ НА РАБОТУ

5.1. Выполните задания предыдущих разделов

5.2. Напишите отчет, содержащий скриншоты каждого выполненного задания с Вашими пояснениями.

6 КОНТРОЛЬНЫЕ ВОПРОСЫ

1. Для чего нужен ARP протокол?

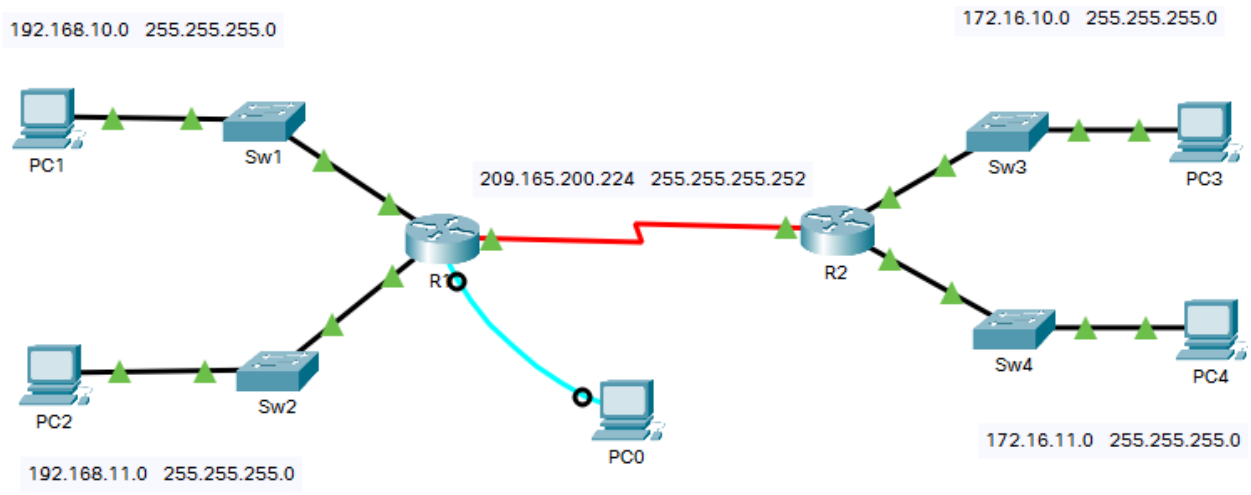
2. Для чего нужен DHCP сервер?

3. Какая информация содержится в поле «Данные» ARP-ответа?

ЛАБОРАТОРНАЯ РАБОТА №8
НАСТРОЙКА МАРШРУТИЗАТОРА

1 ВВЕДЕНИЕ

1.1 Топология



1.2 Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети	Шлюз по умолчанию
Router1	GigEthernet0/0	192.168.10.1	255.255.255.0	–
	GigEthernet0/1	192.168.11.1	255.255.255.0	–
	Serial0/0/0	209.165.200.225	255.255.255.252	–
Router2	GigEthernet0/0	172.16.10.1	255.255.255.0	–
	GigEthernet0/1	172.16.11.1	255.255.255.0	–
	Serial0/0/0	209.165.200.226	255.255.255.252	–
PC1	FastEthernet	192.168.10.100	255.255.255.0	192.168.10.1
PC2	FastEthernet	192.168.11.101	255.255.255.0	192.168.11.1
PC3	FastEthernet	172.16.10.100	255.255.255.0	172.16.10.1
PC4	FastEthernet	172.16.11.101	255.255.255.0	172.16.11.1

1.3 Задачи

1. Первоначальная настройка маршрутизатора.
2. Подключение маршрутизаторов к локальным сетям.
3. Настройка IP-адресов сетевых устройств.

2 НАСТРОЙКА НАЧАЛЬНЫХ ПАРАМЕТРОВ МАРШРУТИЗАТОРА

2.1 Проверка конфигурации маршрутизатора по умолчанию

1) Установите консольное подключение компьютера PC0 к маршрутизатору R1.

2) Войдите в привилегированный режим и проверьте текущую конфигурацию с помощью команды

```
Router# show running-config
```

Ответьте на следующие вопросы.

1. Как называется узел маршрутизатора?
2. Сколько у маршрутизатора интерфейсов Fast Ethernet?
3. Сколько у маршрутизатора интерфейсов Gigabit Ethernet?
4. Сколько у маршрутизатора последовательных интерфейсов?
5. Каков диапазон значений, отображаемых в vty-линиях?

Выведите на экран текущее содержимое памяти NVRAM с помощью команды

```
Router# show startup-config
```

Почему маршрутизатор отвечает сообщением `startup-config is not present` (startup-config отсутствует)?

2.2 Настройка и проверка начальной конфигурации маршрутизатора R1

1) Настройте начальные параметры на маршрутизаторе R1:

1. Задайте имя маршрутизатора **R1_ФИО** (ФИО – инициалы студента латиницей).
2. Используйте следующие пароли:
   - консольный режим: **class**;
   - привилегированный режим EXEC, зашифрованный: **cisco**;
3. Зашифруйте все открытые пароли
4. Включите в баннер MOTD вашу фамилию.

При настройке используются те же команды, что и для коммутатора

2) Проверьте начальные параметры на маршрутизаторе R1 с помощью команды

```
Router# show running-config
```

3) Сохраните файл конфигурации в NVRAM с помощью команды

```
Router# write
```

4) Сохраните файл загрузочной конфигурации во флэш-память. В качестве резервного копирования файл загрузочной конфигурации можно сохранить во флэш-память. По умолчанию маршрутизатор загружает загрузочную конфигурацию из NVRAM. Но если память NVRAM будет повреждена, загрузочную конфигурацию можно будет восстановить, скопировав её из флэш-памяти.

Выполните следующие действия, чтобы сохранить загрузочную конфигурацию во флэш-память:

– Проверьте содержимое флэш-памяти, выполнив команду **show flash**:

```
R1# show flash
```

1. Сколько файлов хранится во флэш-памяти в данный момент?
2. Какой из этих файлов, по вашему мнению, является образом IOS?
3. Почему вы считаете, что этот файл — образ IOS?

– Сохраните файл загрузочной конфигурации во флэш-память, выполнив следующие команды:

```
R1# copy startup-config flash
Destination filename [startup-config]
```

Маршрутизатор предложит сохранить файл во флэш-память с названием в квадратных скобках. В названии файла введите ваши инициалы латиницей и нажмите клавишу **ENTER**.

– С помощью команды **show flash** убедитесь, что файл загрузочной конфигурации сохранен во флэш-памяти.

2.3 Настройка и проверка начальной конфигурации маршрутизатора R2

Выполните аналогичные действия для маршрутизатора R2 (Имя маршрутизатора задайте **R2_ФИО**).

3 ПОДКЛЮЧЕНИЕ МАРШРУТИЗАТОРА К ЛОКАЛЬНОЙ СЕТИ (LAN)

3.1 Просмотр сведений о маршрутизаторе

Отобразите сведения об интерфейсах на маршрутизаторе R1.

1) Для просмотра информации о последовательном интерфейсе Serial 0/0/0 введите команду

```
R1> show interface serial0/0/0
```

1. Какой IP-адрес настроен на маршрутизаторе R1?
2. Какую пропускную способность имеет интерфейс Serial 0/0/0?

2) Для просмотра информации о, интерфейсе GigabitEthernet 0/0 введите команду

```
R1> show interface GigabitEthernet0/0
```

1. Какой IP-адрес настроен на маршрутизаторе R1?
2. Какой MAC-адрес имеет интерфейс GigabitEthernet 0/0?
3. Какую пропускную способность имеет интерфейс GigabitEthernet 0/0?

3) Для просмотра информации обо всех интерфейсах введите команду

```
R1> show ip interface brief
```

1. Сколько последовательных интерфейсов на маршрутизаторах R1 и R2?
2. Сколько интерфейсов Ethernet на маршрутизаторах R1 и R2?

3.2 Анализ таблицы маршрутизации на маршрутизаторе R1.

1) Отобразите таблицу маршрутизации маршрутизатора R1 используя команду

```
Router# show ip route
```

1. Сколько в таблице подключенных маршрутов (имеют код «C»)?
2. Есть ли маршрут по умолчанию?
3. Какие маршруты ведут к удаленным сетям?

2) Отобразите таблицу маршрутизации маршрутизатора R2 и ответьте на те же вопросы.

3.3 Настройка интерфейсов маршрутизатора

1) Настройте IP-адреса компьютеров и соответствующие им шлюзы по умолчанию (**Default gateway**) согласно таблице адресации.

Чтобы устройство могло обмениваться данными в пределах нескольких сетей, ему должен быть присвоен IP-адрес, маска подсети и шлюз по умолчанию. Шлюз по умолчанию используется в том случае, когда узлу необходимо отправить пакет устройству, находящемуся в другой сети. Адресом шлюза по умолчанию обычно является адрес интерфейса маршрутизатора, подключенного к локальной сети, к которой подключен узел.

2) Настройте интерфейс GigabitEthernet 0/0 на маршрутизаторе R1.

Введите указанные ниже команды для задания адреса и активирования интерфейса GigabitEthernet 0/0 на маршрутизаторе **R1**.

```
R1(config)# interface gigabitethernet 0/0
R1(config-if)# ip address 192.168.10.1 255.255.255.0
R1(config-if)# no shutdown
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0,
changed state to up
```

Рекомендуется указать описание для каждого интерфейса с помощью команды **description**, что поможет при документировании сведений о сети. Настройте описание интерфейса, указав, к какому устройству он подключен.

```
R1(config-if)# description LAN connection  to Sw1
```

Маршрутизатор **R1** должен теперь иметь возможность отправить эхо-запрос на компьютер **PC1**.

```
R1(config-if)# end
%SYS-5-CONFIG_I: Configured from console by console
R1# ping 192.168.10.10

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.10, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/2/8 ms
```

3) Аналогичным образом настройте остальные интерфейсы **Gigabit Ethernet** и последовательные интерфейсы **Serial** на маршрутизаторах **R1** и **R2** согласно таблице адресации.

4) Проверьте конфигурации интерфейсов с помощью соответствующих команд:

Выполните команду **show ip interface brief** на маршрутизаторах **R1** и **R2**, чтобы быстро убедиться в том, что интерфейсы имеют правильные IP-адреса и находятся в активном состоянии.

5) Выполните команду **show ip route** на маршрутизаторах **R1** и **R2**, чтобы просмотреть текущие таблицы маршрутизации, и ответьте на следующие вопросы.

1. Сколько в таблице подключенных маршрутов (имеют код «C»)?
2. Есть ли маршрут по умолчанию?
3. Какие маршруты ведут к удаленным сетям?

6) Проверьте сквозное подключение через сеть.

Теперь вы должны иметь возможность отправить эхо-запросы на любой ПК с любого ПК в сети. Кроме того, вы должны иметь возможность отправлять эхо-запросы на активные интерфейсы маршрутизаторов. Например, указанные ниже тесты должны быть успешно выполнены.

- В командной строке на компьютере PC1 отправьте эхо-запрос компьютеру PC4.
- В командной строке на маршрутизаторе R2 отправьте эхо-запрос компьютеру PC2.

7) Сделайте резервную копию конфигураций в NVRAM.

4 ЗАДАНИЕ НА РАБОТУ

4.1. Выполните задания предыдущих разделов

4.2. Напишите отчет, содержащий скриншоты каждого выполненного задания с Вашими пояснениями.

5 КОНТРОЛЬНЫЕ ВОПРОСЫ

1. Какие функции выполняет маршрутизатор?

2. Почему каждый порт маршрутизатора должен иметь свой IP-адрес?

3. Что такое шлюз по умолчанию? Для чего он нужен?

ЛАБОРАТОРНАЯ РАБОТА №9
РАБОТА С IP-АДРЕСАМИ

1 ВВЕДЕНИЕ

1.1 Задачи

1. Использование калькулятора Windows при работе с сетевыми адресами.

2. Преобразование IP-адресов в двоичный формат.

3. Определение IP-адресов.

2 ИСПОЛЬЗОВАНИЕ КАЛЬКУЛЯТОРА WINDOWS В РАБОТЕ С СЕТЕВЫМИ АДРЕСАМИ

2.1 Общие сведения

При работе с компьютерами и сетевыми устройствами сетевые инженеры используют двоичные, десятичные и шестнадцатеричные числа. В операционную систему компании Microsoft входит встроенный калькулятор. Версия калькулятора в ОС Windows 7 включает обычный режим, который можно использовать для выполнения простейших арифметических задач, например сложения, вычитания, умножения и деления, а также расширенные возможности для программных, научных и статистических расчетов.

В данной части лабораторной работы вы будете переводить числа в двоичную, десятичную и шестнадцатеричную системы счисления и обратно в режиме «Программист» калькулятора Windows и определять количество узлов, к которым нужно обратиться, исходя из количества доступных узловых бит.

2.2 Перевод чисел из одной системы счисления в другую

Запустите калькулятор Windows в режиме «Программист». В режиме «Программист» доступны несколько систем счисления: Hex (шестнадцатеричная с основанием 16), Dec (десятичная с основанием 10), Oct (восьмеричная с основанием 8) и Bin (двоичная с основанием 2).

Мы привыкли использовать десятичную систему счисления с цифрами от 0 до 9. Она применяется в повседневной жизни для всех подсчетов и финансовых операций. Компьютеры и прочие электронные устройства для хранения и передачи данных, а также числовых вычислений, используют двоичную систему, состоящую только из нулей и единиц. Все компьютерные расчеты выполняются в двоичной (цифровой) форме, независимо от того, в каком виде они отображаются.

Недостаток этой системы в том, что двоичный эквивалент большого десятичного числа может быть очень длинным. Это усложняет чтение и написание чисел. Один из способов решения этой проблемы — организация двоичных чисел в группы по четыре шестнадцатеричных числа. Шестнадцатеричные числа имеют основание 16, а для представления двоичных или десятичных эквивалентов используют комбинацию цифр от 0 до 9 и букв от A до F. Шестнадцатеричные символы используются при записи или отображении IPv6- и MAC-адресов.

Восьмеричная система счисления мало чем отличается от шестнадцатеричной. Восьмеричные числа представляют собой двоичные числа в группах по три цифры. В этой системе счисления используются цифры от 0 до 7. С помощью восьмеричных чисел

удобно представлять большие двоичные числа в меньших группах, однако эта система счисления не очень распространенная.

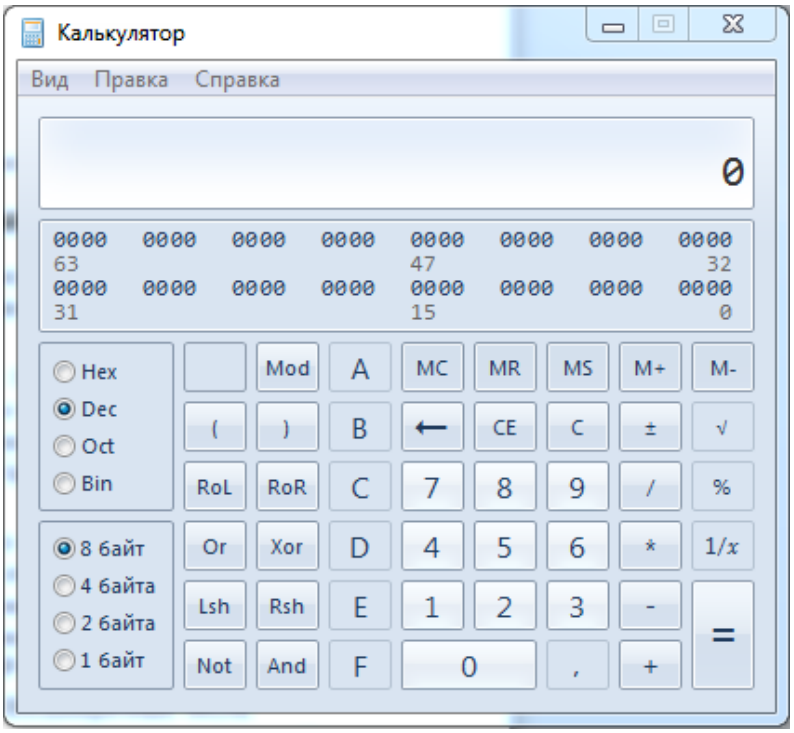


Рисунок 1 – Калькулятор Windows

Числа переводятся из одной системы счисления в другую путем выбора нужной системы счисления. Введите в десятичной системе счисления число любое число. Нажмите на переключатель **Bin**. Число отобразится в двоичной системе счисления. Снова нажмите на переключатель **Dec**. Число будет переведено обратно в десятичную систему. Выполните аналогичные операции для других систем счисления.

Используя калькулятор, заполните таблицу.

Десятичные	**Двоичные**	**Шестнадцатеричные**
86		
175		
204		
	0001 0011	
	0100 1101	
	0010 1010	
		38
		93
		E4

Обратите внимание на взаимосвязь между двоичными и шестнадцатеричными числами.

2.3 Преобразование IP-адресов узлов и масок подсети в двоичный формат

Адреса и маски подсети IPv4 представлены в десятичном формате с точкой-разделителем (четыре октета): соответственно 192.168.1.10 и 255.255.255.0. Это сделано для удобочитаемости адресов. Каждый из десятичных октетов адреса может быть переведен в 8 двоичных октетов. Октет – это всегда 8 двоичных бит.

1) Воспользуйтесь калькулятором Windows для перевода IP-адресов 192.168.1.10 в двоичную систему и занесите полученные двоичные числа в следующую таблицу:

Десятичные	Двоичные
192	
168	
1	
10	

2) Маски подсети, например, 255.255.255.0, также представлены в десятичном формате с точкой- разделителем. Маска подсети всегда будет состоять из четырех 8-битных октетов, каждый из которых представлен в виде десятичного числа. С помощью калькулятора Windows переведите 8 возможных десятичных значений октета маски подсети в двоичные числа и занесите полученные двоичные числа в следующую таблицу:

Десятичные	Двоичные
0	
128	
192	
224	
240	
248	
252	
254	
255	

2.4 Определение количества узлов в сети с помощью степеней числа два

1) При наличии IP-адреса и маски подсети можно определить сетевую часть, а также количество доступных в сети узлов. Для вычисления количества узлов в сети необходимо определить сетевую и узловую части адреса. На примере адреса 192.168.1.10 с маской подсети 255.255.248.0 определим количество узлов в сети. Для этого переведите IP-адрес и маску в двоичный формат:

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

Поскольку первый 21 бит в маске подсети — это последовательные единицы, первый 21 бит в IP-адресе в двоичном формате таков: 11000000101010000000. Это сетевая часть адреса. Остальные 11 бит в IP-адресе сети должны быть равными 0.

2) Запишите сетевую часть адреса в десятичном и двоичном формате.

3) Поскольку сетевая часть и широковещательный адрес используют два адреса из возможного диапазона адресов сети, количество узлов, доступных в локальной сети, равно числу 2 в степени количества доступных битов в узловой части минус 2:

Количество доступных узлов = 2 (количество битов в узловой части) - 2

В данном примере в сети доступно 2046 узлов (2^{11} - 2).

4) Используя калькулятор посчитайте для каждой маски подсети количество доступных узлов и занесите это значение в следующую таблицу:

Маска подсети	Маска подсети в двоичном формате	Количество доступных битов в узловой части	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		

3 ПРЕОБРАЗОВАНИЕ IP-АДРЕСОВ В ДВОИЧНЫЙ ФОРМАТ

3.1 Общие сведения

Каждый IP-адрес состоит из двух частей — сетевой и узловой. Сетевая часть адреса одинакова для всех устройств, которые находятся в одной и той же сети. Узловая часть определяет конкретный узел в пределах соответствующей сети. Маска подсети используется для определения сетевой части IP- адреса. Устройства в одной сети могут обмениваться данными напрямую; для взаимодействия между устройствами из разных сетей требуется промежуточное устройство уровня 3, например маршрутизатор.

Чтобы понять принцип работы устройств в сети, нам необходимо увидеть адреса в том виде, в котором с ними работают устройства — в двоичном представлении. Для этого необходимо перевести IP-адрес и его маску подсети из десятичного представления с точками в двоичное значение. После этого можно определить сетевой адрес с помощью побитовой операции И.

В этой лабораторной работе описывается порядок определения сетевой и узловой частей IP-адресов. Для этого нужно перевести адреса и маски подсети из десятичного представления с точками в двоичный формат, а затем применить побитовую операцию И. После этого вы воспользуетесь полученной информацией для определения адресов в сети.

3.2 Использование побитовой операции И для определения сетевых адресов

1) Сначала вам необходимо перевести десятичный IP-адрес и маску подсети в их двоичный эквивалент. При использовании операции И десятичное значение в каждой битовой позиции 32-битного IP-адреса узла сравнивается с соответствующей позицией в 32-битной маске подсети. При наличии двух нулей или 0 и 1 результатом операции И будет 0. При наличии двух единиц результатом будет 1, как показано в приведенном примере

Описание	Десятичные	Двоичные
IP-адрес	192.168.10.131	11000000.10101000.00001010.10000011
Маска подсети	255.255.255.192	11111111.11111111.11111111.11000000
Сетевой адрес	192.168.10.128	11000000.10101000.00001010.10000000

2) Выполните операцию И, чтобы определить сетевой адрес для каждой пары IP-адреса – маска подсети:

Описание	Десятичные	Двоичные
IP-адрес	192.168.XX.10	
Маска подсети	255.255.255.0	
Сетевой адрес		

Описание	Десятичные	Двоичные
IP-адрес	172.16.145.XX	
Маска подсети	255.255.0.0	
Сетевой адрес		

Описание	Десятичные	Двоичные
IP-адрес	192.168.XX.XX	
Маска подсети	255.255.255.128	
Сетевой адрес		

Описание	Десятичные	Двоичные
IP-адрес	172.XX.188.15	
Маска подсети	255.255.240.0	
Сетевой адрес		

Описание	Десятичные	Двоичные
IP-адрес	10.172.XX.8	
Маска подсети	255.224.0.0	
Сетевой адрес		

XX – последние две цифры зачетки студента.

3.3 Применение расчетов сетевых адресов

1) Определите, находятся ли IP-адреса в одной и той же сети

Вы настраиваете два ПК для своей сети. Компьютеру PC-A присвоен IP-адрес 192.168.1.XX, а компьютеру PC-B — IP-адрес 192.168.1.33. Маска подсети обоих компьютеров — 255.255.255.240.

1. Какой сетевой адрес у PC-A?
2. Какой сетевой адрес у PC-B?
3. Смогут ли эти ПК взаимодействовать друг с другом напрямую?
4. Какой наибольший адрес, присвоенный компьютеру PC-B, позволит ему находиться в одной сети с PC-A?

Вы настраиваете два ПК для своей сети. Компьютеру PC-A присвоен IP-адрес 10.0.0.XX, а компьютеру PC-B — IP-адрес 10.1.14.68. Маска подсети обоих компьютеров — 255.254.0.0.

1. Какой сетевой адрес у PC-A?
2. Какой сетевой адрес у PC-B?
3. Смогут ли эти ПК взаимодействовать друг с другом напрямую?
4. Какой наименьший адрес, присвоенный компьютеру PC-B, позволит ему находиться в одной сети с PC-A?

2) Установите адрес шлюза по умолчанию

В вашей компании действует политика использования первого IP-адреса в сети в качестве адреса шлюза по умолчанию. Узел в локальной сети (LAN) имеет IP-адрес 172.16.140.XX и маску подсети 255.255.192.0.

1. Какой у этой сети сетевой адрес?
2. Какой адрес имеет шлюз по умолчанию для этого узла?

4 ОПРЕДЕЛЕНИЕ IP-АДРЕСОВ

4.1 Проанализируйте приведенную ниже таблицу и определите сетевую и узловую части указанных IP-адресов

Первые две строки содержат примеры заполнения таблицы.

Сокращения, используемые в таблице:

С = все 8 бит для октета содержатся в сетевой части адреса

с = бит в сетевой части адреса

У = все 8 бит для октета содержатся в узловой части адреса

у = бит в узловой части адреса

IP-адрес/префикс	Сеть/узел С,с = сеть, У,у = узел	Маска подсети	Сетевой адрес
192.168.10.10/24	С.С.С.У	255.255.255.0	192.168.10.0
10.101.99.17/23	С.С.ссссссу.У	255.255.254.0	10.101.98.0
209.165.XX.227/27			
172.31.XX.252/24			
10.1.XX.200/26			
172.16.117.XX /20			
10.XX.XX.101/25			
209.165.202.140/27			
192.168.XX.45/28			

4.2 Проанализируйте приведенную ниже таблицу и укажите диапазон адресов узлов и широковещательных адресов в виде пары маски подсети и префикса.

В первой строке приведен пример заполнения таблицы.

IP-адрес/префикс	Адрес первого узла	Адрес последнего узла	Широковещательный адрес
192.168.10.10/24	192.168.10.1	192.168.10.254	192.168.10.255
10.101.99.17/23			
209.165.XX.227/27			
172.31.XX.252/24			
10.1.XX.200/26			
172.16.117.XX /20			
10.XX.XX.101/25			
209.165.202.140/27			
192.168.XX.45/28			

4.3 Проанализируйте приведенную ниже таблицу и определите тип адреса (адрес сети, узла, многоадресной или широковещательной рассылки).

В первой строке приведен пример заполнения таблицы.

IP-адрес	Маска подсети	Тип адреса
10.1.1.1	255.255.255.252	узел
192.168.XX.63	255.255.255.192	
239.192.XX.100	255.252.0.0	
172.25.XX.52	255.255.255.0	
XX.255.0.0	255.0.0.0	
172.16.XX.48	255.255.255.240	
209.165.202.159	255.255.255.224	
172.16.0.255	255.255.0.0	
224.10.XX.11	255.255.255.0	

4.4 Проанализируйте приведенную ниже таблицу и определите тип адреса: публичный или частный.

IP-адрес/префикс	Публичный или частный
209.165.201.XX /27	
192.168.255.253/24	
10.100.XX.103/16	
172.30.XX.100/28	
192.31.7.XX /24	
172.20.XX.150/22	
128.107.10.XX /16	
192.135.250.XX /24	
64.104.0.XX /16	

5 ЗАДАНИЕ НА РАБОТУ

5.1. Выполните задания предыдущих разделов

5.2. Напишите отчет, содержащий скриншоты каждого выполненного задания с Вашими пояснениями.

6 КОНТРОЛЬНЫЕ ВОПРОСЫ

1. Как отличить широковещательный IP-адрес от локального?

2. Что такое префикс в IP-адресе?

3. Чем публичный IP-адрес отличается от частного?

СПИСОК РЕКОМЕНДУЕМОЙ ЛИТЕРАТУРЫ

1. Одом У. Официальное руководство по подготовке к сертификационным экзаменам Cisco CCENT/CCNA ICND1 100-101: Пер. с англ. М.: ООО Вильямс, 2015. 912 с.

2. Пайпер Б. Администрирование сетей Cisco: освоение за месяц / пер. с англ. М. ДМК Пресс, 2018. 316 с.

3. Одом У. Официальное руководство по подготовке к сертификационным экзаменам Cisco CCNA ICND2 200-101: маршрутизация и коммутация: Пер. с англ. М.: ООО Вильямс, 2015. 736 с.

4. Илюхин Б. В. Сетевые информационные технологии: Учебное пособие. Томск, ТУСУР, 2012. 183 с.

ЗАКЛЮЧЕНИЕ

Лабораторный практикум позволяет студентам получить представление о принципах работы локальных сетей и освоить базовые навыки настройки сетевого оборудования. По результатам выполнения работ студенты должны знать и понимать функции каждого уровня модели OSI, уметь настраивать локальную сеть и выполнять базовую настройку коммутаторов и маршрутизаторов. Кроме того, студенты должны знать принципы адресации в сети, назначение MAC и IP-адресов, маски подсети, шлюза по умолчанию.

Оглавление