КАЗАНСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ
ИНСТИТУТ ФИЗИКИ
Кафедра радиофизики

П.А. КОРЧАГИН

ЗАДАНИЯ ДЛЯ ЛАБОРАТОРНЫХ РАБОТ ПО ДИСЦИПЛИНЕ «ОСНОВЫ СЕТЕВЫХ ТЕХНОЛОГИЙ»

Учебно-методическое пособие

КАЗАНЬ
2023

УДК 004.45(075.8)
ББК 32.973.202я73 К70

Печатается по рекомендации учебно-методической комиссии Института физики Казанского (Приволжского) федерального университета (протокол N 06 от 6.02.2023 г.)

Автор-составитель
старший преподаватель **П.А. Корчагин**

Рецензент
кандидат физико-математических наук, доцент **Е.Ю. Зыков**

Корчагин П.А.

К70 Задания для лабораторных работ по дисциплине «Основы сетевых технологий»: учебно-методическое пособие / П.А. Корчагин. – Казань: Издательство Казанского университета, 2023. – 47 с.

Учебно-методическое пособие предназначено для студентов направления подготовки «Информационная безопасность» и «Информационные процессы и коммуникационные (киберфизические) системы».

В пособии изложены задания и справочный материал для выполнения лабораторных работ. Оно может быть использовано при освоении дисциплин «Радиотелекоммуникационные системы», «Информационные технологии», «Сети и системы передачи данных» и «Безопасность вычислительных сетей».

УДК 004.45(075.8)
ББК 32.973.202я73

Оглавление

Лабораторная работа № 1

Основные понятия сетевых технологий

1. Провести обзор прикладного программного обеспечения для визуализации топологии локальной сети.

2. Провести анализ топологии и построить схему сети в виде рисунка. Образец представлен на рис. 1.1.

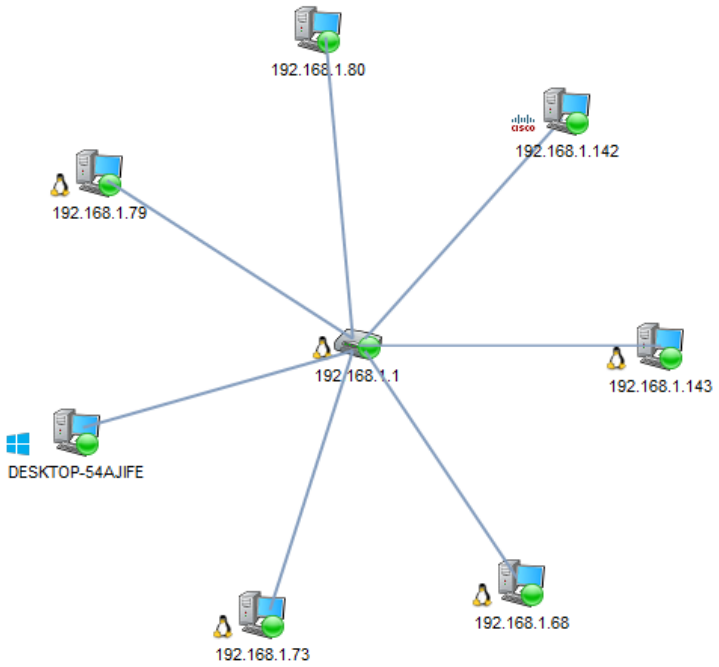

Рис. 1.1. Топология «Звезда»

3. На рисунке 1.2 показан план офисного помещения. Требуется объединить в локальную сеть все сетевые устройства, находящиеся в помещении, выбрать топологию сети и необходимое оборудование. Информацию об оборудовании занесите в табл. 1.1.

Таблица 1.1

Список необходимого оборудования

№	Наименование	Количество	Стоимость

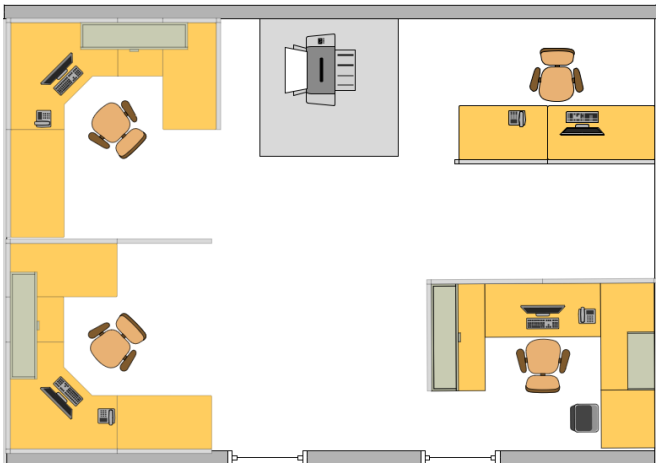

Рис. 1.2. План офисного помещения

4. Установить программу-анализатор трафика Wireshark.

5. Ознакомиться с интерфейсом программы-анализатора трафика Wireshark.

6. Подготовить обзор основных возможностей программы-анализатора трафика Wireshark.

7. Ответьте на вопросы, приведенные ниже:

1) сеть, объединяющая компьютеры разных городов, регионов, государств, относится к классу …….;

2) ……. – это устройство, которое позволяет подключаться к сети и взаимодействовать с другими устройствами;

3) сетевая модель OSI имеет семь уровней: …….;

4) блок данных канального уровня называется:

– сегмент;

– пакет;

– кадр;

– фрейм.

5) за выбор наилучшего маршрута до сети назначения отвечает ……. уровень модели OSI;

6) ……. – это процесс, при котором к данным добавляется заголовок определенного уровня перед отправкой в сеть.

7) блок данных сетевого уровня называется:

– сегмент;

– пакет;

– кадр;

– фрейм.

8. Подготовить отчет по пунктам 1, 2, 3, 6, 7 в формате docx.

Лабораторная работа № 2

Кабельные системы локальных вычислительных сетей

1. На рисунке 2.1 показан план офисных помещений. В каждом кабинете – по шесть рабочих станций. Требуется объединить в локальную сеть все сетевые устройства. В смежном помещении монтажные работы проводить запрещается. С точки зрения безопасности сетевое оборудование располагать в холле нежелательно. Предложить вариант кабельной подсистемы и расположения сетевого оборудования.

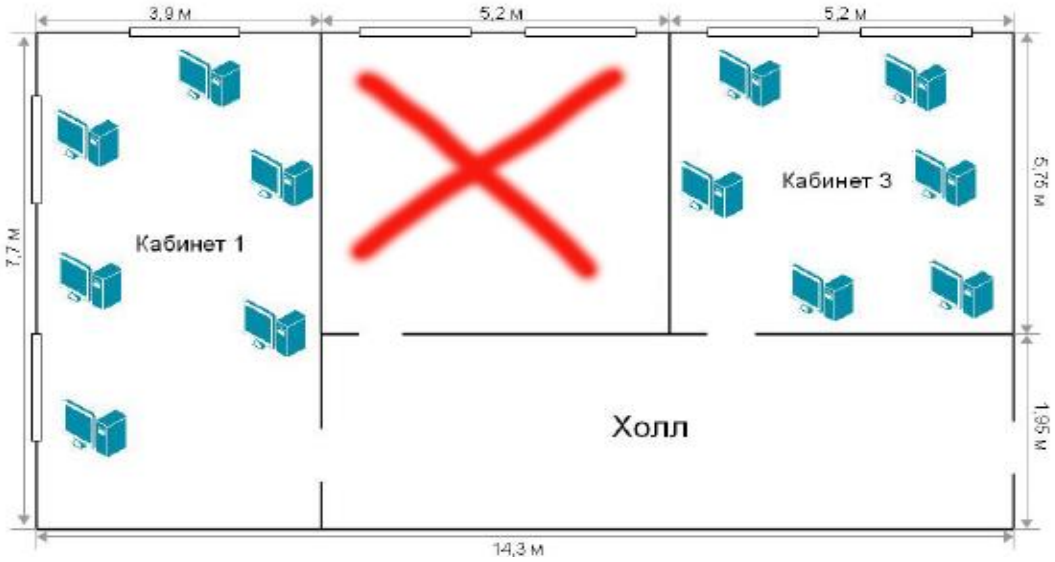

Рис. 2.1. План офисных помещений

2. На рисунке 2.2. показан план офисных помещений, расположенных в отдельных зданиях. Выполнить задание, аналогичное заданию в п. 1.

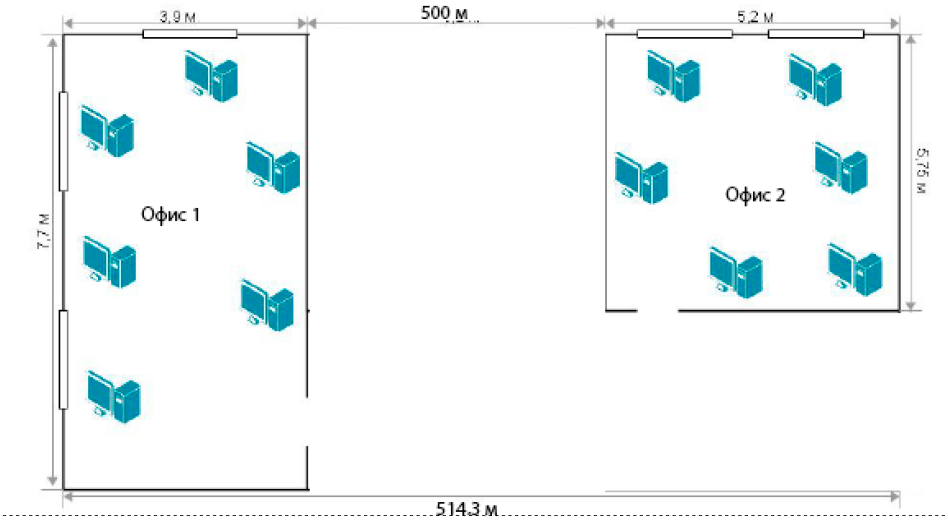

Рис. 2.2. План офисных помещений в отдельных зданиях

3. Подготовить обзор инструментов и приборов для монтажа и диагностики волоконно-оптического кабеля.

4. Подготовить обзор основных возможностей Cisco Packet Tracer и eNSP.

5. Ответьте на вопросы, приведенные ниже:

1) модель TCP/IP включает ……. уровней;

2) к достоинствам модели TCP/IP можно отнести: …….;

3) какие кабели запрещены при прокладке в вентиляционных шахтах?

4) перечислите кабельные среды передачи данных: …….;

5) протокол ……., из модели TCP/IP TCP, обеспечивает передачу данных с гарантией доставки;

6) к основным характеристикам канала связи относятся: …….;

7) в зависимости от направления, по которому можно передавать данные, каналы связи бывают: …….

6. Подготовить отчет по результатам выполнения заданий.

Лабораторная работа № 3

Настройка среды моделирования. Построение простейшей локальной сети

1. Загрузите необходимое программное обеспечение: WinPcap 4.1.3, Wireshark 3.6.2, VirtualBox 5.2.44 и eNSP.

2. Произведите установку загруженного программного обеспечения в следующей последовательности: WinPcap 4.1.3, Wireshark 3.6.2, VirtualBox 5.2.44 и eNSP.

3. Запустите симулятор eNSP.

4. Выберите создание новой топологии (New Topo). Пользователю будет представлена панель холста, на которой можно установить сетевую топологию для практических занятий и анализа поведения сети. В этом примере должна быть создана простая сеть «точка-точка».

5. Выберите раздел End Device –> PC, чтобы показать список конечных устройств, которые могут быть применены. Выберите значок PC, перетащите его на панель холста, отпустите значок, чтобы разместить его на холсте. Аналогичным образом разместите вторую рабочую станцию (рис. 3.1). Устройства на панели холста представляют собой имитируемые конечные системы, которые могут использоваться для эмуляции реальных операций.

Рис. 3.1. Простейшая локальная сеть

6. Выберите значок соединений (рис. 3.2), чтобы показать список сред, которые могут быть применены в топологии. Выберите Auto из списка. После нажатия на значок курсор будет представлять соединитель для отображения текущей роли курсора в качестве соединителя.

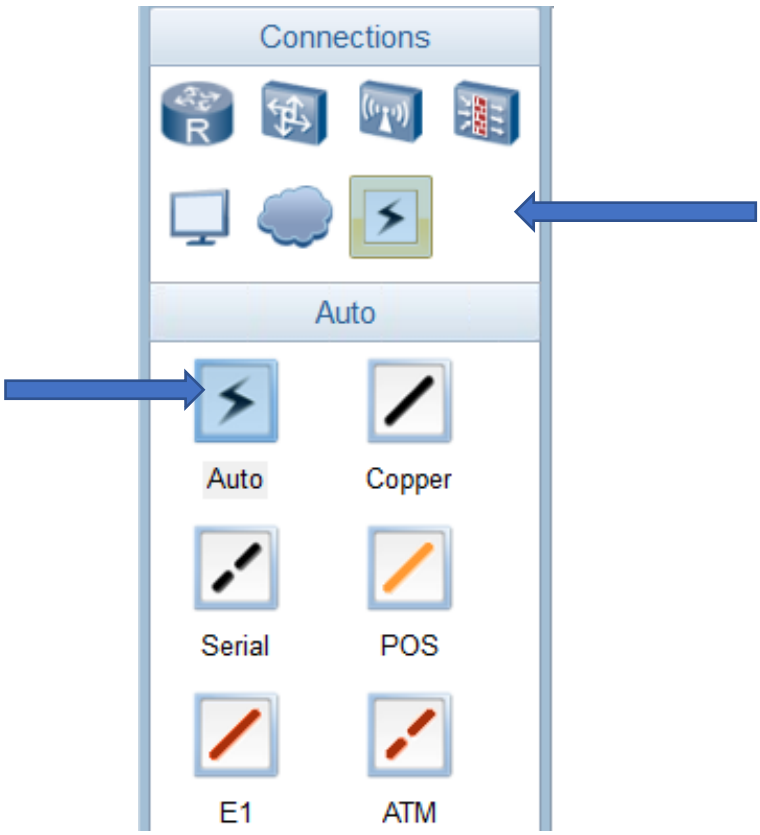

Рис. 3.2. Создание физической среды

7. Последовательно щелкните мышкой на рабочих станциях PC1 и PC2. Создание сети «точка-точка» показывает соединение с двумя красными точками на среде, представляющими текущее состояние интерфейсов, к которым среда подключается в качестве отключенной (рис. 3.3).

Рис. 3.3. Сеть «точка-точка»

8. Настройте статический IP-адрес на рабочих станциях PC1 и PC2. Выберите рабочую станцию PC1 и используйте правую кнопку мыши для отображения меню свойств. Настройте параметры согласно рис. 3.4.

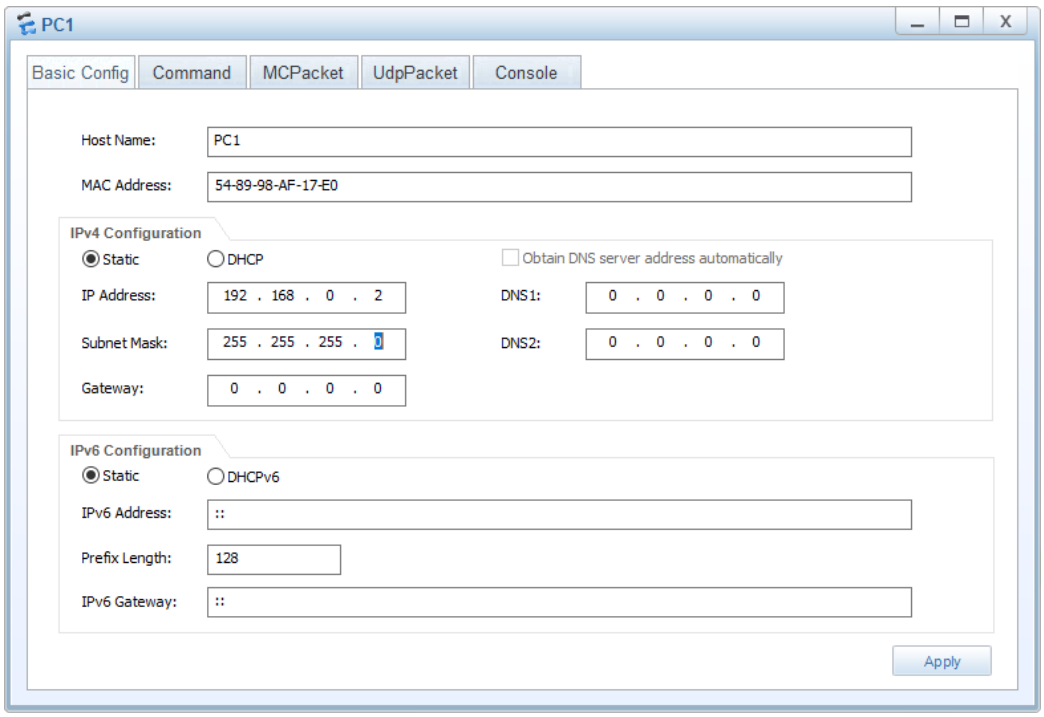

Рис. 3.4. Настройка параметров рабочей станции PC1

9. Повторите п. 8 для рабочей станции PC2, указав host name: PC2 и IP address: 192.168.0.3.

10. Активируйте устройства с использованием кнопки Start Device (рис. 3.5).

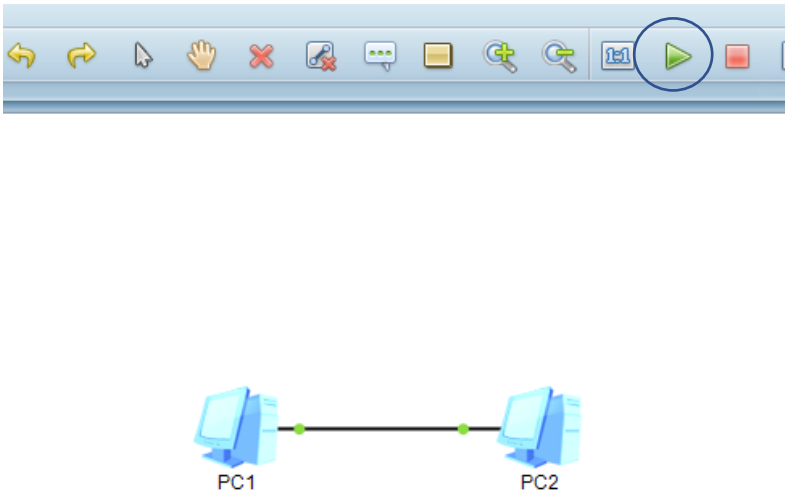

Рис. 3.5. Активация устройств

11. Выполнение захвата пакетов на интерфейсе. Выберите PC1 и щелкните правой кнопкой мыши для отображения меню настроек. Выделите опцию захвата данных (Capture Data), чтобы отобразить список интерфейсов, которые

принадлежат устройству и доступны для наблюдения с помощью инструмента захвата пакетов. Выберите интерфейс из списка, состояние которого необходимо отслеживать. Выбор интерфейса приведет к активации инструмента захвата пакетов Wireshark для выбранного интерфейса.

12. Откройте командное окно на рабочей станции PC1: либо дважды щелкните по значку клиента и выберите вкладку Command, либо с помощью правой кнопки мыши войдите в меню свойств и в настройках выберите вкладку Command.

13. Введите команду: ping 192.168.0.3 (рис. 3.6). Утилита ping работает по протоколу ICMP.

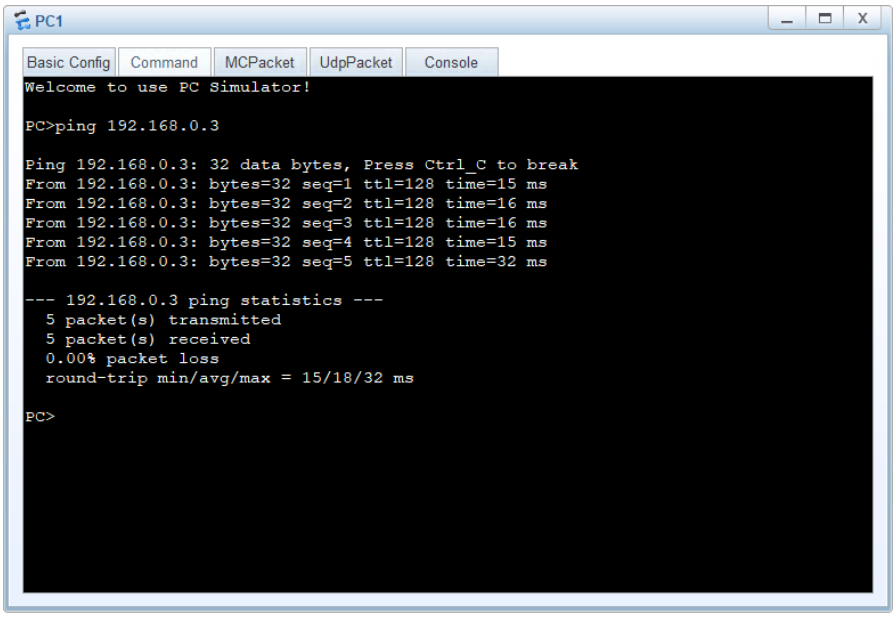

Рис. 3.6. Генерирование трафика на интерфейсе

14. Пронаблюдайте захват трафика. Чему теперь равен MAC-адрес отправителя пакета и получателя пакета?

15. Найдите MAC-адрес отправителя в захваченных данных и определите через онлайн-сервис производителя оборудования.

16. Проведите фильтрацию захваченного трафика по протоколам ICMP и ARP.

17. Разработать скрипт для вывода MAC-адресов сетевых интерфейсов локального компьютера. По полученным данным определить производителей

сетевых адаптеров. Таблицу соответствия можно взять с ресурса https://gitlab.com/wireshark/wireshark/-/raw/master/manuf или воспользоваться сервисом https://tools.alexell.ru/mac-inf.

Для реализации скрипта рекомендуется использовать модуль **psutil** (python system and process utilities), который является кросс-платформенной библиотекой для получения информации о запущенных процессах и использования системы (процессор, память, диски, сеть) в Python.

Справка: ***метод net_if_addrs()*** *– возвращает адреса, связанные с каждой сетевой картой, установленной в системе, в виде словаря, ключи которого – имена сетевых карт, а значение – список именованных кортежей для каждого адреса, назначенного сетевой карте.*

Пример использования: вывод имени сетевой карты и ее IP-адреса.

```
import psutil
for k, v in psutil.net_if_addrs().items():
    for item in v:
        address = item[1]
        if '.' in address and len(address) <= 15:
            print(k)
            print(address)
```

```
VirtualBox Host-Only Network
192.168.56.1
Ethernet
192.168.1.76
Ethernet 2
169.254.131.37
VMware Network Adapter VMnet1
192.168.182.1
VMware Network Adapter VMnet8
192.168.206.1
Loopback Pseudo-Interface 1
127.0.0.1
```

18. Подготовить отчет по лабораторной работе в формате docx.

Лабораторная работа № 4

Создание локальной сети с использованием коммутатора и маршрутизатора. Начальная конфигурация устройств

1. Создайте топологию согласно рис. 4.1. Используйте коммутатор S3700.

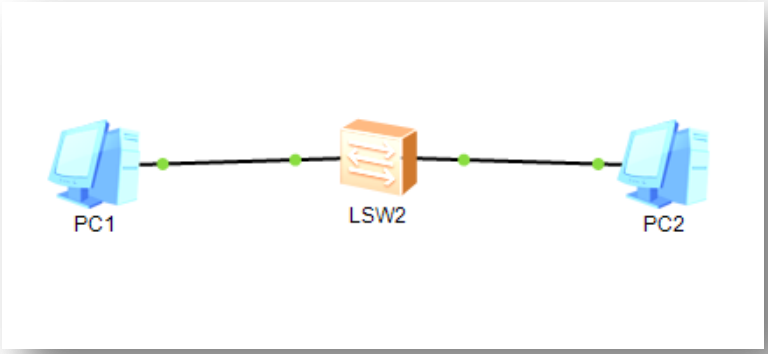

Рис. 4.1. Сеть с использованием коммутатора S3700

2. Через динамическое меню Settings –> View просмотрите внешний вид коммутатора.

3. Произведите запуск устройств.

4. Настройте статические IP-адреса для рабочих станций: PC1 – 192.168.1.2, PC2 – 192.168.1.3. Задайте маску подсети 255.255.255.0 (рис. 4.2).

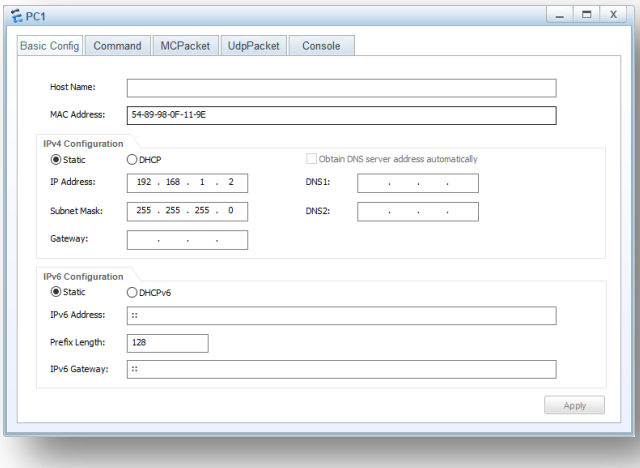

Рис. 4.2. Настройка IP-адреса

5. Используя команду ping, протестируйте связь между рабочими станциями PC1 и PC2 (рис. 4.3).

```
PC>ping 192.168.1.3

Ping 192.168.1.3: 32 data bytes, Press Ctrl_C to break
From 192.168.1.3: bytes=32 seq=1 ttl=128 time=47 ms
From 192.168.1.3: bytes=32 seq=2 ttl=128 time=31 ms
From 192.168.1.3: bytes=32 seq=3 ttl=128 time=63 ms
From 192.168.1.3: bytes=32 seq=4 ttl=128 time=62 ms
From 192.168.1.3: bytes=32 seq=5 ttl=128 time=47 ms

--- 192.168.1.3 ping statistics ---
  5 packet(s) transmitted
  5 packet(s) received
  0.00% packet loss
  round-trip min/avg/max = 31/50/63 ms
```

Рис. 4.3. Результат работы команды ping

6. На коммутаторе запустите команду **display version**, чтобы просмотреть версию программного обеспечения и информацию об оборудовании системы. Для этого используйте динамическое меню и команду CLI (рис. 4.4).

```
<Huawei>display version
Huawei Versatile Routing Platform Software
VRP (R) software, Version 5.110 (S3700 V200R001C00)
Copyright (c) 2000-2011 HUAWEI TECH CO., LTD

Quidway S3700-26C-HI Routing Switch uptime is 0 week, 0 day, 0 hour, 36 minute
<Huawei>
```

Рис. 4.4. Результат работы команды display version

В выходных данных команды отображается версия операционной системы VRP, модель устройства и время запуска.

7. Измените параметры системного времени и даты с использованием команды **clock datetime** 12:00:00 2022-03-11. Установите точное время и текущую дату. Выполните команду **display clock**, чтобы убедиться, что новое системное время вступило.

8. Выполните команду **system**, чтобы получить доступ к системному представлению и присвоению имени коммутатору SW1 при помощи команды **sysname**.

9. Выйдите из системы при помощи команды **quit**.

10. Выполните команду **dir** в пользовательском представлении, чтобы отобразить список файлов в текущем каталоге (рис. 4.5).

```
<SW1>dir
Directory of flash:/

  Idx  Attr     Size(Byte)  Date        Time        FileName
    0  drw-              -  Aug 06 2015 21:26:42   src
    1  drw-              -  May 17 2022 20:58:50   compatible

32,004 KB total (31,972 KB free)
```

Рис. 4.5. Список файлов в текущем каталоге

11. Сохраните текущую конфигурацию, используя команду **save**.

12. Выполните следующую команду, чтобы просмотреть информацию о текущей конфигурации: **display current-configuration**.

13. Для перезапуска устройства используется команда **reboot**. Перезапустите устройство.

14. Добавьте к сети маршрутизатор AR1200 и подключите его к коммутатору через сетевой интерфейс GigabitEthernet 0/0/1.

15. Через динамическое меню Settings –> View просмотрите внешний вид маршрутизатора (рис. 4.6).

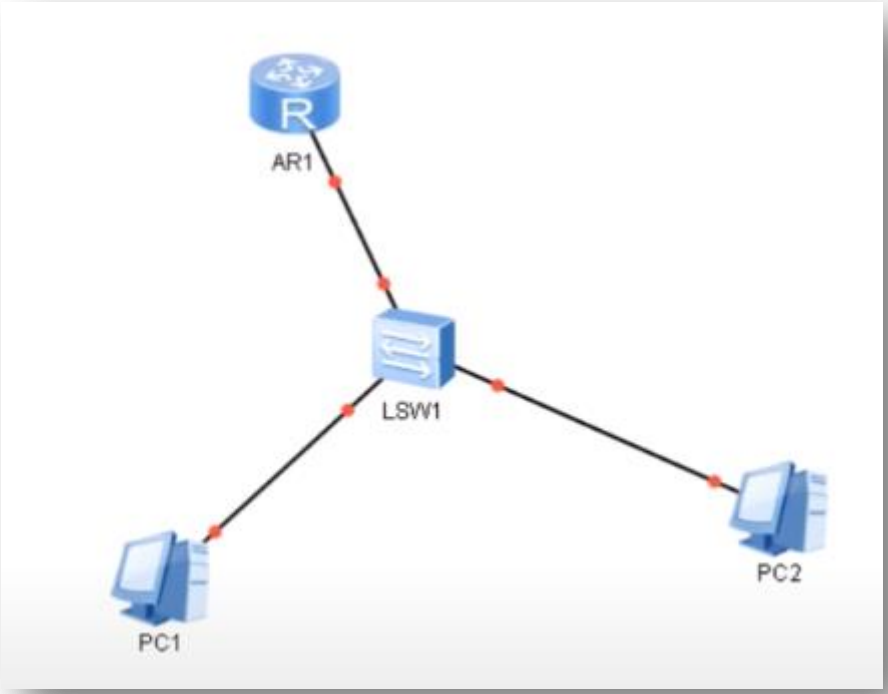

Рис. 4.6. Учебная сеть

16. Выполните п. 6, 7, 8 (имя устройства – R1), 11, 12 на маршрутизаторе.

17. Войдите в режим системных настроек (команда **system**) и настройте сетевой интерфейс GigabitEthernet 0/0/1, используя команду **interface GigabitEthernet 0/0/1.** Пропишите IP-адрес, используя команду **ip address 192.168.10.1 24** (рис. 4.7).

```
[Huawei-GigabitEthernet0/0/1]ip address 192.168.10.1 24
```

Рис. 4.7. Настройка IP-адреса

18. Завершите конфигурирование интерфейса командой **quit**.

19. Включаем функцию DHCP на маршрутизаторе командой **dhcp enable**.

20. Создаем пул адресов с помощью команды **ip poll NET1.**

21. Укажите диапазон IP-адресов, которые могут быть динамически распределены: **network 192.168.10.0 mask 255.255.255.0.**

22. Задайте шлюз: **gateway-list 192.168.10.1.**

23. Задайте DNS: **dns-list 8.8.8.8.**

24. Установите срок для аренды IP-адреса на 10 дней и 12 часов (команда **lease day 10 hour 12 minute 0**).

25. Укажите IP-адрес (192.168.10.2), который нельзя автоматически назначить из пула (команда **excluded-ip-address 192.168.10.2**).

26. Выйдите из режима конфигурирования пула с помощью команды **quit**.

27. Войдите в режим настройки интерфейса, используя команду **interface GigabitEthernet 0/0/1**, и задайте режим DHCP командой **dhcp select global**.

28. Выйдите из настройки интерфейса (команда **quit**).

29. В настройках рабочей станции укажите динамическое получение адреса (рис. 4.8).

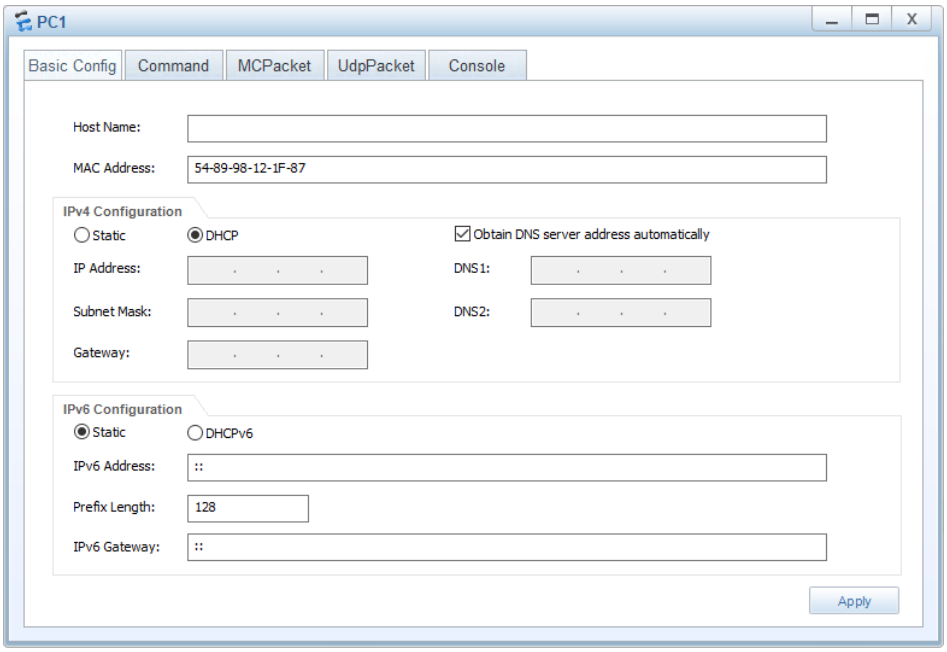

Рис. 4.8. Настройка задания IP-адреса на рабочей станции

30. На рабочей станции просмотрите настройку конфигурации протокола TP/IP, используя команду **ipconfig** (рис. 4.9).

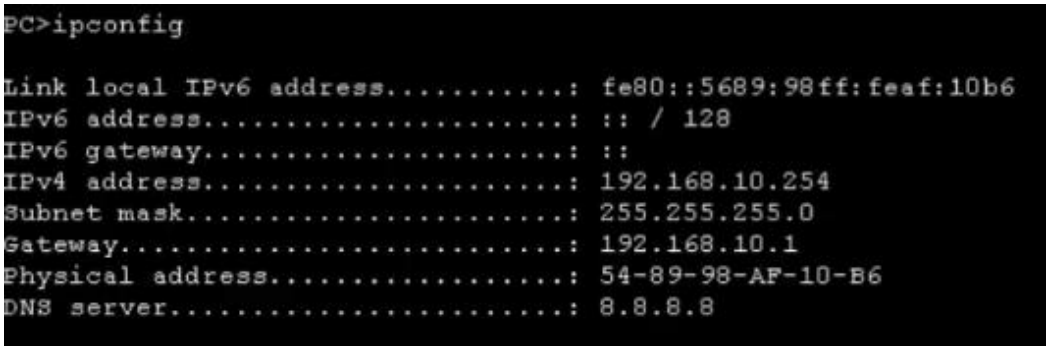

Рис. 4.9. Настройка конфигурации протокола TP/IP

31. Определите IP-адрес второй рабочей станции.

32. Пропингуйте шлюз (192.168.10.1) и рабочие станции (рис. 4.10).

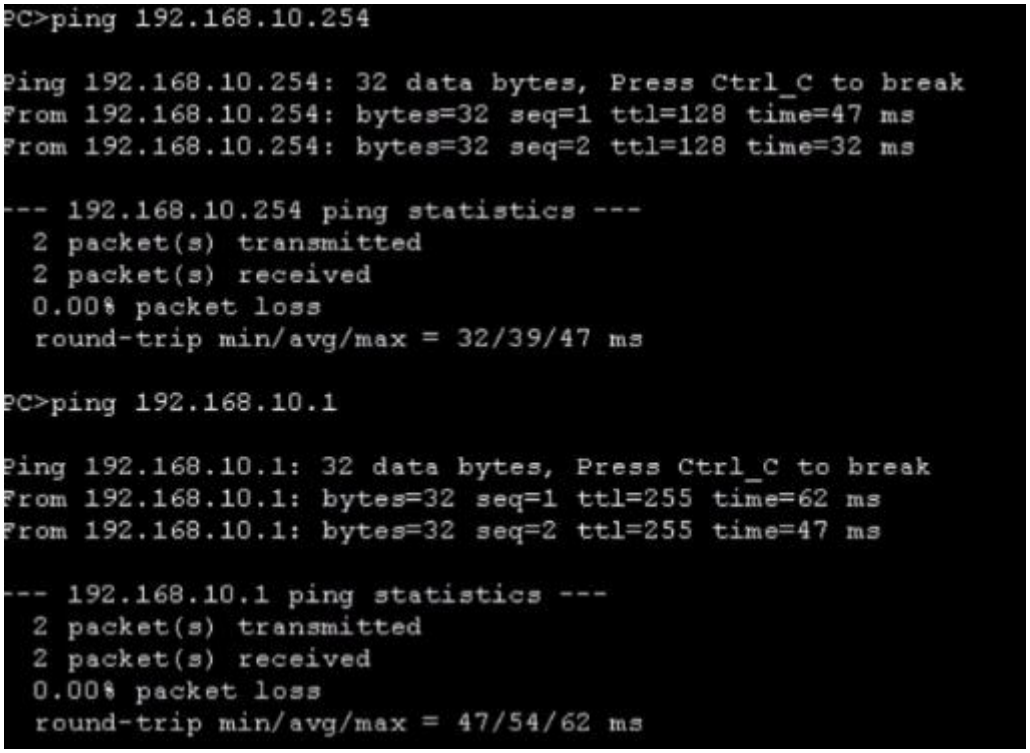

Рис. 4.10. Результат выполнения команды ping

33. Разработать скрипт для перевода числа из шестнадцатеричной системы в двоичную и десятичную системы счисления.

34. Подготовить отчет по лабораторной работе. В отчете должны присутствовать скриншоты выполнения всех команд из пунктов лабораторной работы.

Лабораторная работа № 5

Работа с коммутаторами. Изучение команд оборудования Huawei

1. Создайте топологию согласно рис. 5.1. Используйте два концентратора.

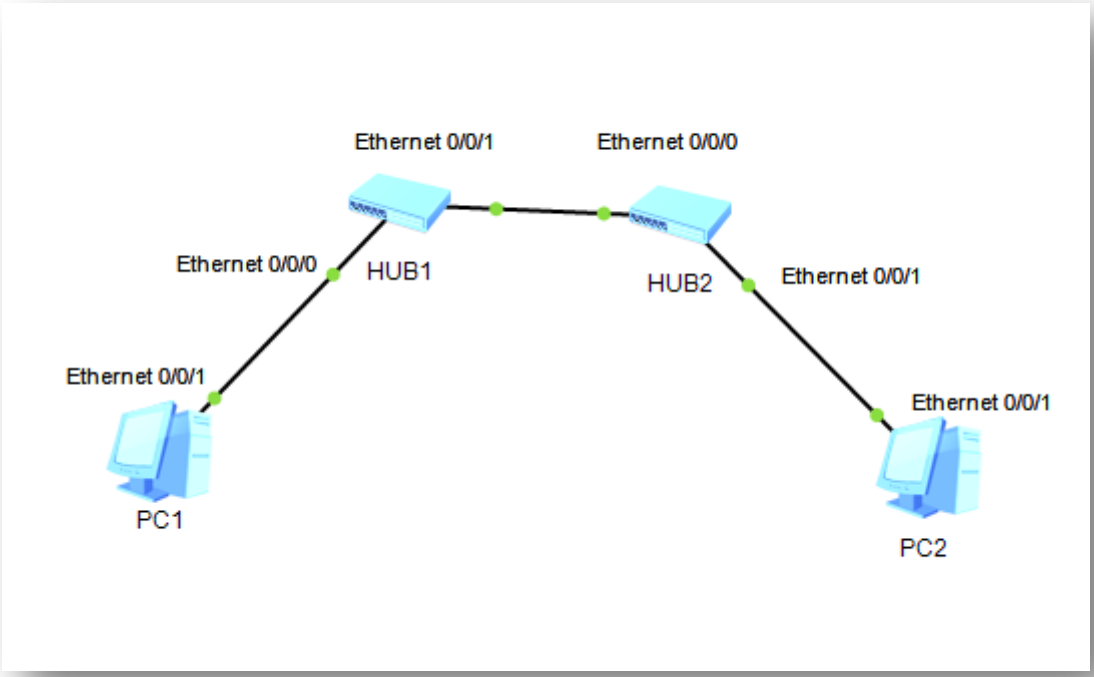

Рис. 5.1. Сеть с использованием концентраторов

2. Настройте статические IP-адреса для рабочих станций: PC1 – 192.168.10.2, PC2 – 192.168.10.3. Задайте маску подсети 255.255.255.0.

3. Произведите запуск устройств.

4. Настройте захват пакетов с интерфейсов Ethernet 0/0/1 рабочих станций.

5. Используя команду ping, протестируйте соединения между рабочими станциями.

6. Пронаблюдайте захват пакетов (рис. 5.2).

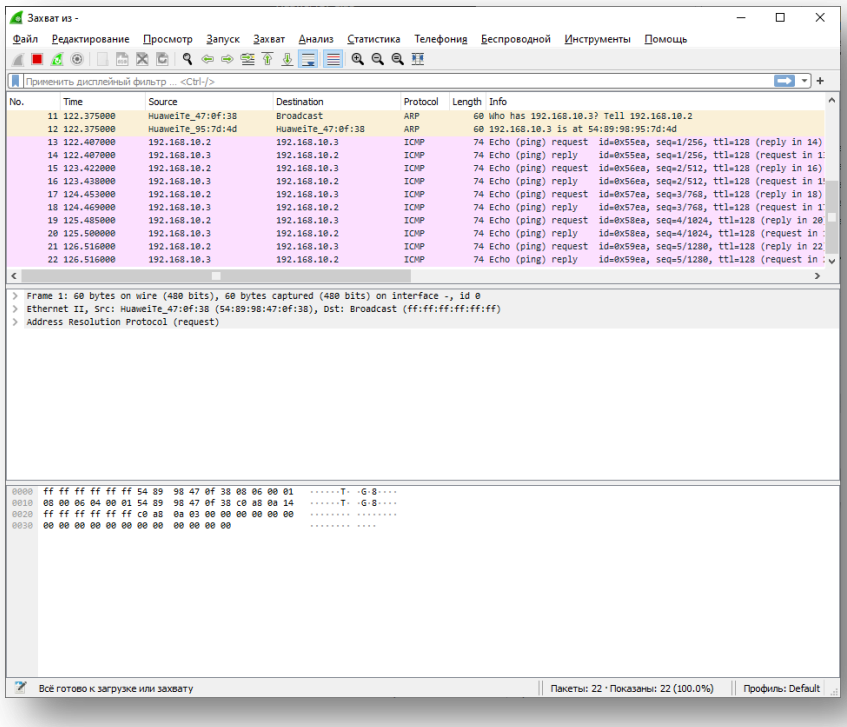

Рис. 5.2. Захват пакетов с интерфейса Ethernet 0/0/1 PC1

7. Подключите к схеме, как показано на рис. 5.3, еще один концентратор для образования кольца.

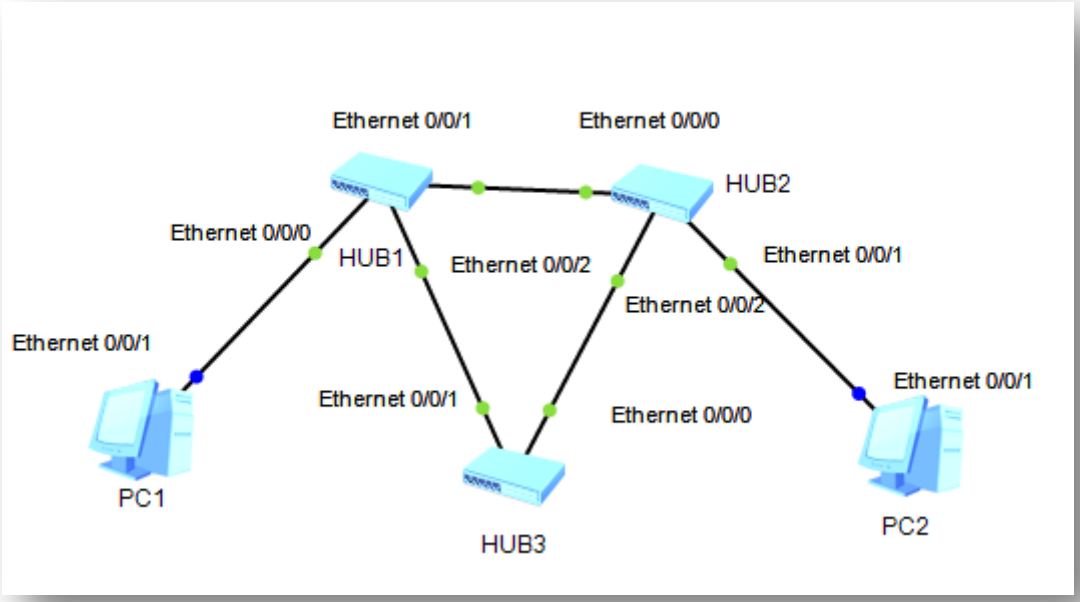

Рис. 5.3. Топология с кольцом

8. Используя команду ping, протестируйте связь между рабочими станциями PC1 и PC2. Поясните полученный результат (рис. 5.4).

```
PC>ping 192.168.10.3

Ping 192.168.10.3: 32 data bytes, Press Ctrl_C to break
Request timeout!
Request timeout!
Request timeout!
Request timeout!
Request timeout!

--- 192.168.10.3 ping statistics ---
  5 packet(s) transmitted
  0 packet(s) received
  100.00% packet loss
```

Рис. 5.4. Результат тестирования

9. Внесите изменения в топологию сети, заменив концентраторы на коммутаторы S3700 (рис. 5.5).

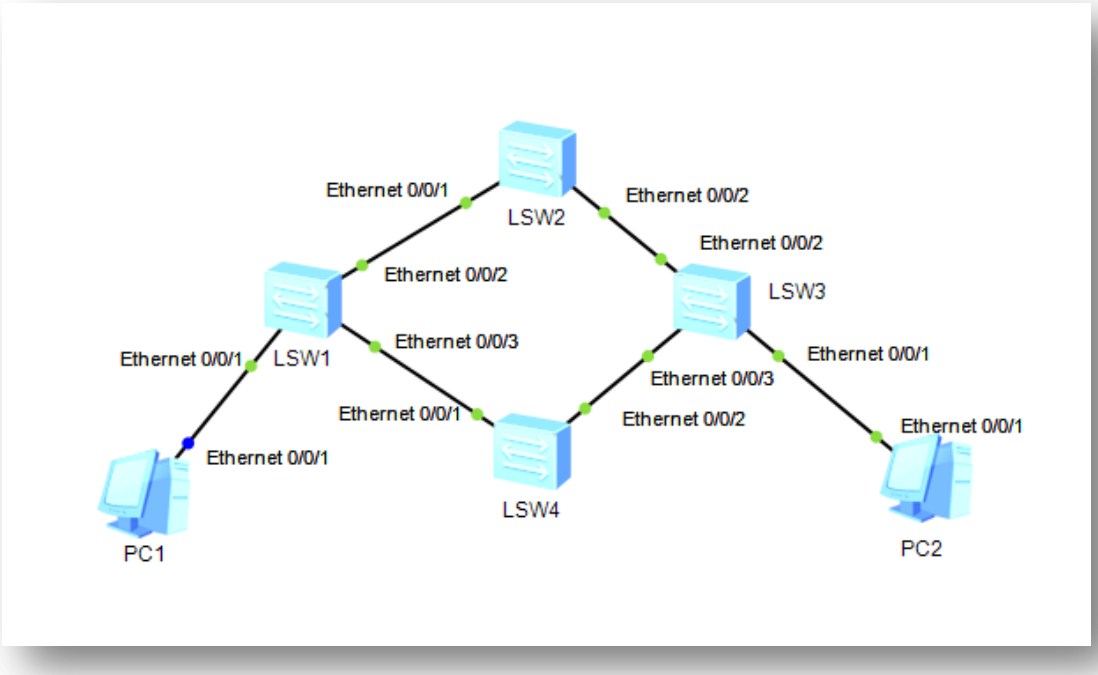

Рис. 5.5. Сеть на основе коммутаторов S3700

10. Запустите устройства и протестируйте связь между рабочими станциями PC1 и PC2. Поясните полученный результат.

11. Определите MAC-адреса коммутаторов. Для этого выполните команду **display bridge mac-add** на каждом коммутаторе. Полученные данные занесите в табл. 5.1.

Таблица 5.1

Имя коммутатора	MAC-адрес	Примечание
LSW1	.....	
LSW2	.....	
LSW3	.....	
LSW4	.....	

12. Проанализируйте данные табл. 5.1 и определите имя корневого коммутатора.

13. Проверьте через программу-анализатор трафика Wireshark правильность определения корневого коммутатора (рис. 5.6).

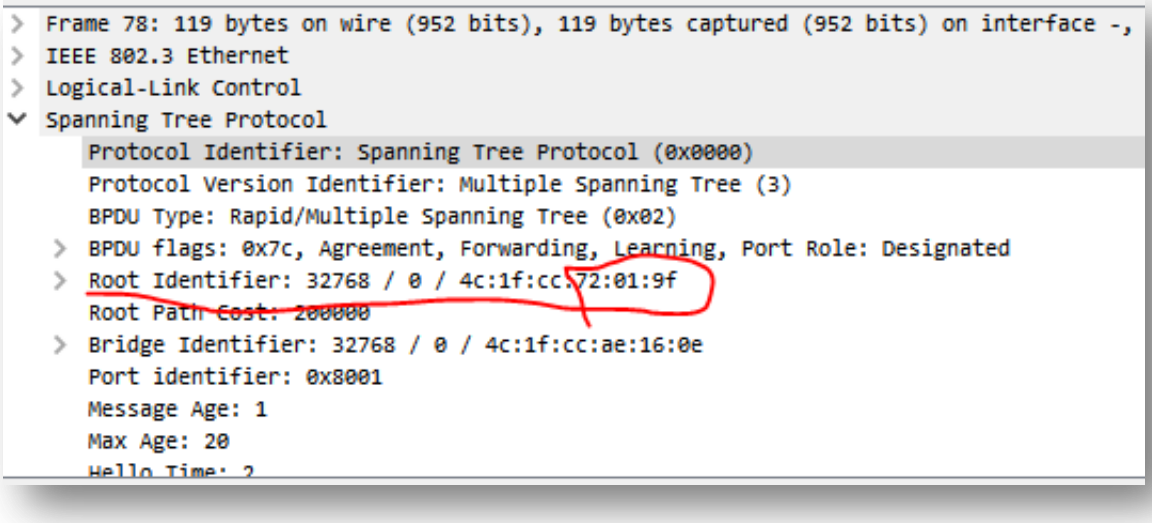

Рис. 5.6. MAC-адрес корневого коммутатора

14. Проверьте через команду **display stp** правильность определения корневого коммутатора (рис. 5.7).

```
<Huawei>display stp
-------[CIST Global Info][Mode MSTP]-------
CIST Bridge          :32768.4c1f-ccae-160e
Config Times         :Hello 2s MaxAge 20s FwDly 15s MaxHop 20
Active Times         :Hello 2s MaxAge 20s FwDly 15s MaxHop 20
CIST Root/ERPC       :32768.4c1f-cc72-019f / 200000
CIST RegRoot/IRPC    :32768.4c1f-ccae-160e / 0
CIST RootPortId      :128.2
BPDU-Protection      :Disabled
TC or TCN received   :9
TC count per hello   :0
STP Converge Mode    :Normal
Time since last TC   :0 days 0h:47m:33s
Number of TC         :8
Last TC occurred     :Ethernet0/0/2
----[Port1(Ethernet0/0/1)][FORWARDING]----
```

Рис. 5.7. Информация о коммутаторе

15. Настройте захват пакетов с интерфейсов корневого коммутатора (рис. 5.8).

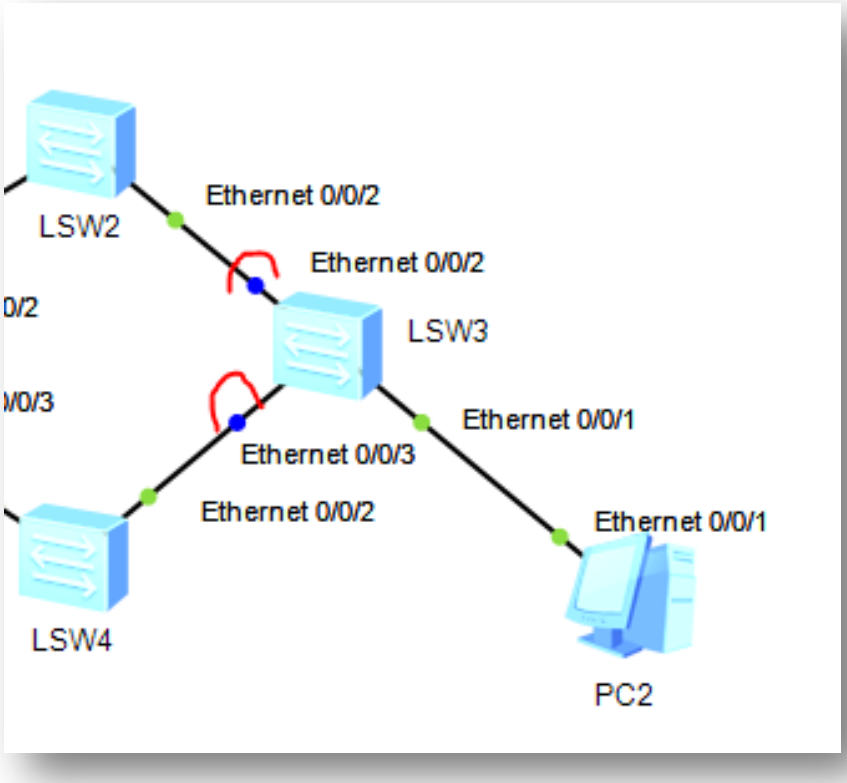

Рис. 5.8. Захват пакетов с интерфейсов коммутатора

16. Определите, какое соединение с корневым коммутатором отключено.

17. Проведите расчет кратчайшего пути и определите, какое соединение должно быть отключено согласно правилам STP.

18. Произведите разрыв рабочего соединения с корневым коммутатором.

19. Используя команду ping, протестируйте связь между рабочими станциями PC1 и PC2. Поясните полученный результат.

20. Отключите все устройства.

21. Восстановите подключение к корневому коммутатору.

22. Замените отключенное соединение на соединение с интерфейсом GE 0/0/1.

23. Запустите устройства.

24. Определите через Wireshark, какое соединение с корневым коммутатором отключено. Поясните результат.

25. Перейдите в режим администрирования на коммутаторе LSW2 при помощи команды **system-view**.

26. Просмотрите таблицу коммутации на коммутаторе LSW2. Для просмотра используйте команду **display mac-address**.

27. Завершите работу в административном режиме командой **quit**.

28. Подготовьте отчет по лабораторной работе. В отчете должны присутствовать скриншоты выполнения всех команд из пунктов лабораторной работы.

Лабораторная работа № 6

6.1. Диагностика WiFi сетей и анализ загруженности каналов

Для выполнения работы потребуется компьютер с WiFi-адаптером и наличие нескольких работающих точек доступа в зоне действия адаптера.

1. Скачайте и установите программу inSSIDer.

2. Изучите документацию к программе inSSIDer и подготовьте описание основных возможностей и интерфейса программы.

3. Определите количество сетей, работающих в диапазоне 2,4 и 5 ГГц.

4. Постройте диаграмму распределения сетей по каналам. Для выполнения задания удобно использовать сортировку по каналам или фильтр (рис. 6.1).

Примеры фильтров:

1, 5 – каналы первый, пятый и их комбинации с другими каналами;

1–5 – каналы с первого по пятый включительно.

Рис. 6.1. Использование фильтра беспроводных сетей по каналам

5. На основе информации из п. 4 определите наименее занятые каналы.

6. Отсортируйте беспроводные сети в порядке возрастания максимально возможной скорости работы сетевого оборудования (Max Rate) и определите минимальное значение.

SIGNAL	CHANNEL	SECURITY	MAC ADDRESS	MAX RATE ▲	802.11
-78	4	WPA2-Personal	50:D4:F7:CC:A9:CB	54	unknown
-72	12	WPA2-Personal	4C:5E:0C:B7:05:B3	130	n
-95	11	WPA2-Personal	9C:9D:7E:8B:EA:C6	144	n
-90	10	WPA2-Personal	AA:28:5D:67:85:C8	150	n
-95	8	WPA2-Personal	DE:07:B6:D3:CA:84	216	n
-95	1+5	WPA2-Personal	D8:0D:17:F1:1D:F7	270	n
-95	11+7	WPA2-Personal	12:50:72:E1:2C:D2	300	n
-78	4+8	WPA2-Personal	DC:E3:05:DF:7B:24	300	n
-95	3+7	WPA2-Personal	04:71:53:FC:F8:2C	300	n
-95	3+7	WPA2-Personal	06:71:53:EC:F8:2C	300	n
-87	11+7	WPA2-Personal	DC:E3:05:45:E7:82	300	n
-95	1+5	WPA2-Personal	DC:E3:05:45:69:EF	300	n

Рис. 6.2. Максимальные скорости работы сетевого оборудования

7. Определите по рис. 6.3, на какие каналы настроен WiFi-роутер сети TP-Link_B692.

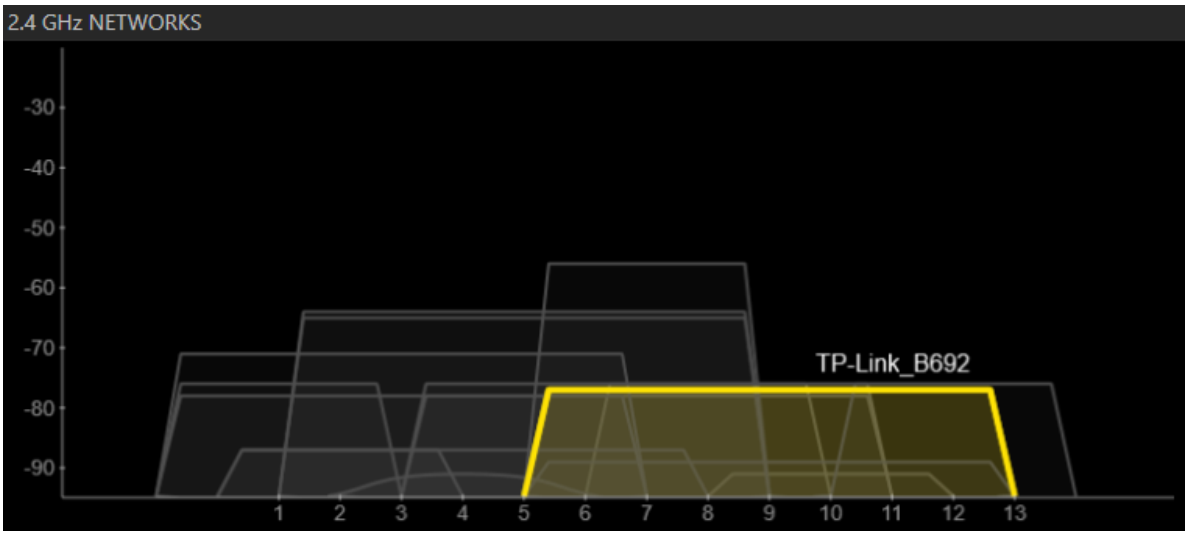

Рис. 6.3. Использование диапазона WiFi 2,4 ГГц

6.2. Протокол IP. Диагностические утилиты

1. Задача первая: адрес сети равен 111.81.192.0, адрес узла – 111.81.208.26. Чему равно наименьшее возможное значение третьего слева байта маски? Ответ запишите в виде десятичного числа.

2. Задача вторая: определите, какое количество подсетей можно получить при использовании маски, если в вашем распоряжении имеется сеть 138.214.0.0, а размеры требуемых подсетей равны 126 узлам в подсети. Какое значение при этом должна иметь маска?

3. Перейдите в командную строку Windows (cmd).

4. Проверьте конфигурацию TCP/IP физического интерфейса с помощью утилиты ipconfig (рис. 6.4). Результат занесите в табл. 6.1.

Таблица 6.1

Конфигурация TCP/IP

1	IP-адрес	
2	Маска подсети	
3	Основной шлюз	
4	Используется ли DHCP (адрес DHCP-сервера)	
5	Описание адаптера	
6	Физический адрес сетевого адаптера	
7	Адрес DNS-сервера	

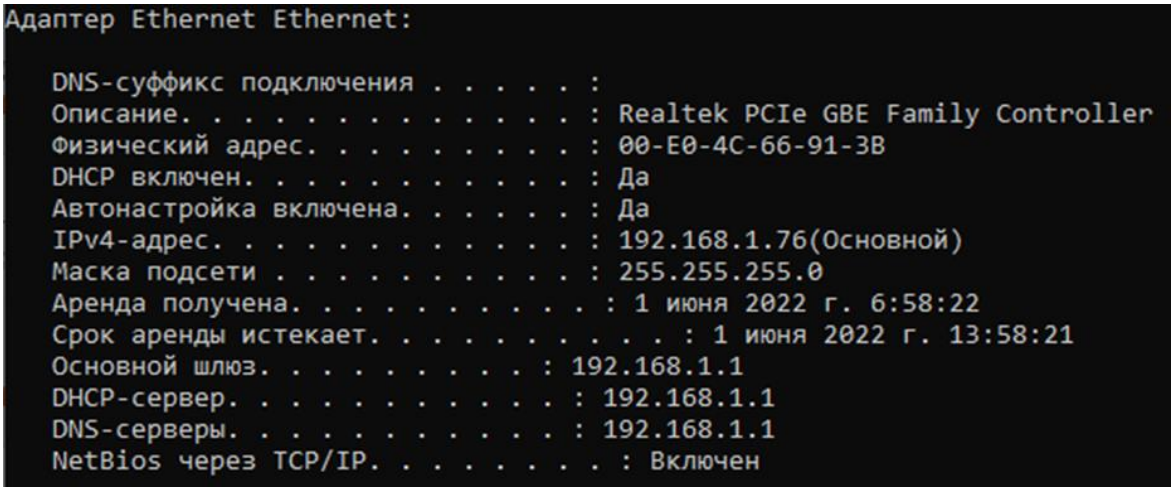

Рис. 6.4. Результат работы команды ipconfig /all

5. С помощью команды ping проверьте перечисленные ниже адреса и для каждого из них отметьте время отклика:

127.0.0.1, 127.0.0.127, 185.125.56.223, 5.255.355.60.

6. С помощью команды tracert проверьте для перечисленных ниже адресов, через какие промежуточные узлы идет сигнал:

185.125.56.223, 5.255.355.60.

7. С помощью утилиты arp просмотрите ARP-таблицу локального компьютера.

8. Воспользуйтесь командой route print -4 для вывода таблицы маршрутизации. На основе полученных данных для IPv4 определите:

– маршрут по умолчанию;

– местную петлю;

– маршрутизацию локального хоста.

Справка:

– сетевой адрес – это IP-адрес, адрес сети или адрес 0.0.0.0, используемый для шлюза по умолчанию;

– маска сети (Netmask) – маска сети. Каждому IP-адресу соответствует своя стандартная маска;

– адрес шлюза (Gateway) – IP-адрес шлюза, через который будет выполняться отправка пакета для достижения конечной точки;

– интерфейс (Interface) - IP-адрес сетевого интерфейса, через который выполняется доставка пакета к конечной точке маршрута;

– метрика (Metric) – значение метрики (1-9999). Метрика представляет собой числовое значение, позволяющее оптимизировать доставку пакета получателю, если конечная точка маршрута может быть достижима по нескольким разным маршрутам. Чем меньше значение метрики, тем выше приоритет маршрута.

9. Внесите новый маршрут 8.8.8.8 с маской 255.255.255.255, с адресом стандартного шлюза и метрикой 100. Пример команды: route add 8.8.8.8 mask 255.255.255.255 192.168.1.1 metric 100.

10. Выведите таблицу маршрутизации. Поясните изменение метрики нового маршрута.

11. Удалите добавленный маршрут командой route delete 8.8.8.8.

12. Настройте перехват пакетов физического интерфейса через Wireshark.

13. Установите фильтр IP, выделите пакет и выберите заголовок (рис. 6.5).

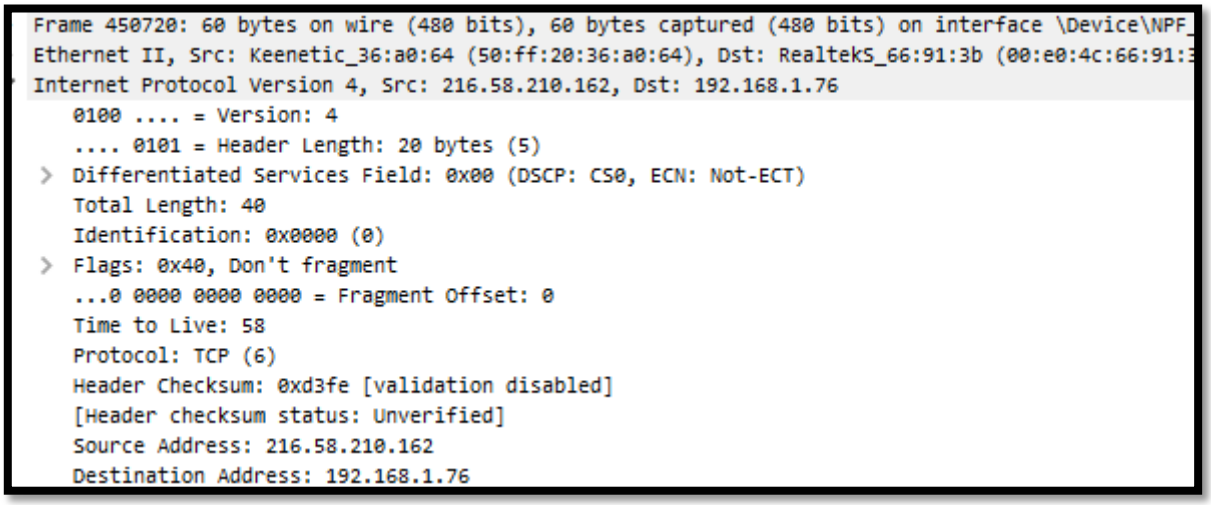

Рис. 6.5. Заголовок IP

14. Просмотрите и проанализируйте информацию в полях заголовка IP-пакета и определите:

– адрес получателя;

– длину заголовка;

– фрагментирован пакет или нет;

– время жизни пакета;

– код протокола следующего уровня;

– контрольную сумму заголовка.

Лабораторная работа № 7

Управляющие протоколы сетевого уровня

Для выполнения работы потребуется компьютер с доступом в Internet.

1. Запустите анализатор сети Wireshark и настройте захват пакетов с физического интерфейса.

2. Установите фильтр пакетов bootp.

3. Перейдите в командную строку Windows.

4. Используя команду ipconfig /all, определите время получения аренды IP-адреса и срок аренды.

5. Освободите арендованный адрес. Для этого введите команду ipconfig /release Ethernet (Ethernet – имя сети).

6. Получите новый IP-адрес. Для этого введите команду ipconfig /renew Ethernet (рис. 7.1).

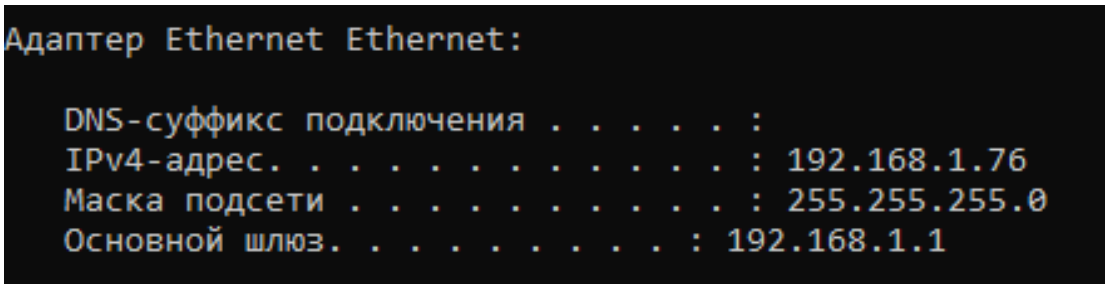

Рис. 7.1. Результат получения нового IP-адреса

7. Найдите пакеты DORA в Wireshark.

8. Заполните адресами отправителя и получателя табл. 7.1.

Таблица 7.1

Адресация пакетов DORA

Наименование	Адрес получателя	Адрес отправителя
Discover		
Offer		
Request		
ACK		

9. Просмотрите содержимое пакета offer. Определите, какой IP-адрес и какой маршрутизатор по умолчанию предложил DHCP-сервер, время аренды адреса (рис. 7.2).

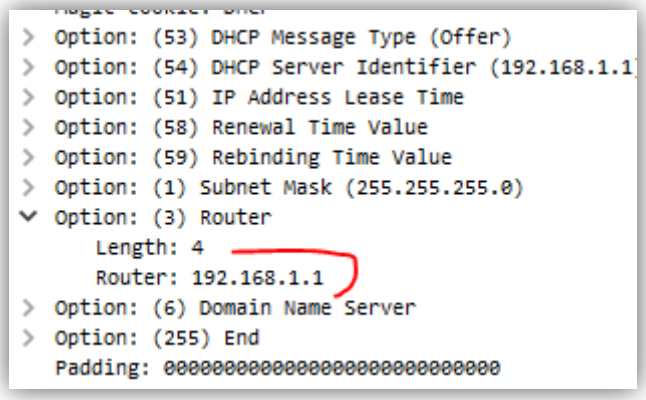

Рис. 7.2. Маршрутизатор по умолчанию

10. Просмотрите содержимое пакета Request и определите, какой адрес запрашивает компьютер (Option 50).

11. Просмотрите, какие дополнительные опции предлагает DHCP-сервер.

12. Просмотрите содержимое пакета ACK.

13. Отобразите таблицу соответствия IP- и MAC-адресов, для этого в командную строку введите команду arp -a.

14. Внесите в отчет все динамические записи ARP-таблицы.

15. Удалите одну динамическую запись. Пример команды для удаления записи: arp -d 172.20.4.12.

16. Установите фильтр пакетов arp.

17. Определите пакеты ARP-запроса и ARP-ответа.

18. Просмотрите заголовок канального уровня пакета ARP.

19. Проанализируйте поля данных протокола ARP. Дайте расшифровку полученной информации (рис. 7.3).

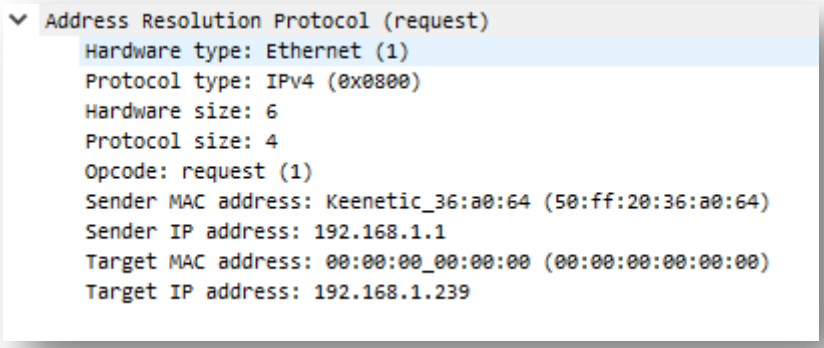

Рис. 7.3. Поля данных протокола ARP

20. Установите фильтр пакетов icmp.

21. Произведите проверку доступности 8.8.8.8 с помощью команды ping 8.8.8.8 (рис. 7.4).

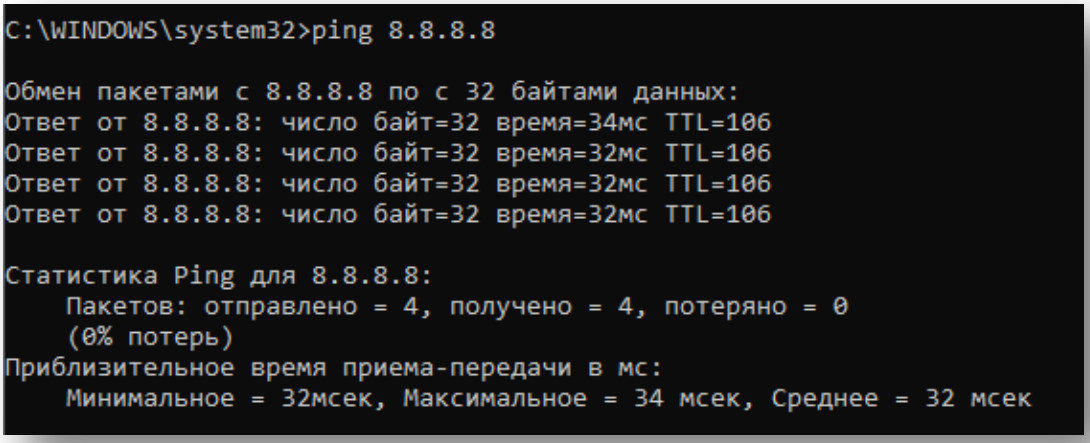

Рис. 7.4. Результат работы команды ping

22. Определите количество Echo-ответов в Wireshark. Проверьте их соответствие выводу команды ping.

23. Просмотрите основные поля заголовка протокола ICMP (рис. 7.5).

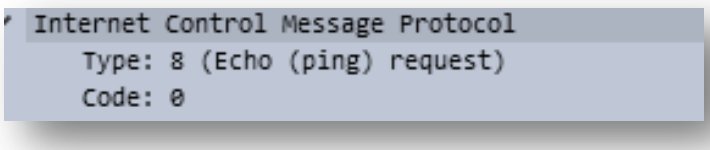

Рис. 7.5. Основные поля заголовка протокола ICMP

24. Определите, какие данные были переданы в Echo-ответе.

25. Введите команду ping -I 1 8.8.8.8. Команда позволит установить время жизни пакета – 1.

26. Поясните результат работы команды ping.

27. Определите код сообщения протокола ICMP, соответствующего выполнению команды из п. 25.

28. По результатам выполнения работы необходимо подготовить отчет.

Лабораторная работа № 8

Протоколы транспортного уровня TCP и UDP

Для выполнения работы потребуется компьютер с доступом в Internet.

1. Найдите и ознакомьтесь с описанием протоколов TCP и UDP в соответствующих RFC.

2. Запустите анализатор сети Wireshark и настройте захват пакетов с физического интерфейса.

3. Установите фильтр пакетов dns и перейдите в браузере на сайт www.huawei.ru.

4. Определите номер порта назначения в заголовке протокола UDP-пакета на запрос разрешения доменного имени huawei.ru (рис. 8.1).

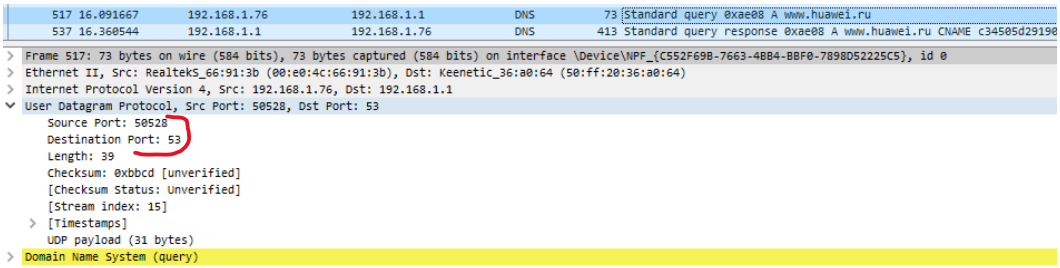

Рис. 8.1. Заголовок протокола UDP

5. Установите фильтр пакетов dhcp.

6. Освободите арендованный адрес. Для этого введите команду ipconfig /release Ethernet (Ethernet – имя сети).

7. Получите новый IP-адрес. Для этого введите команду ipconfig /renew Ethernet.

8. В заголовке протокола UDP найдите информацию о номере порта клиента и порта сервера DHCP.

9. Установите фильтр пакетов http.

10. В заголовке протокола TCP найдите информацию о номере порта клиента и порта Web-сервера.

11. Занесите информацию о полученных в данной работе закрепленных портах в табл. 8.1.

Таблица 8.1

Закрепленные порты

Номер порта	Сервис	Примечание

Справка по утилите netstat

Утилита netstat предназначена для получения сведений о состоянии сетевых соединений и слушаемых на данном компьютере портах TCP и UDP, а также для отображения статистических данных по сетевым интерфейсам и протоколам.

Формат командной строки: netstat [-a] [-b] [-e] [-f] [-n] [-o] [-p протокол] [-r] [-s] [-t] [интервал].

Параметры командной строки: -a – отображение всех подключений и ожидающих портов, -b – отображение исполняемого файла, участвующего в создании каждого подключения или ожидающего порта.

Иногда известные исполняемые файлы содержат множественные независимые компоненты. Тогда отображается последовательность компонентов, участвующих в создании подключения, либо ожидающий порт. В этом случае имя исполняемого файла находится снизу в скобках [ ], сверху – компонент, который им вызывается, и так до тех пор, пока не достигается TCP/IP. Заметьте, что такой подход может занять много времени и требует достаточных разрешений.

-e – отображение статистики Ethernet. Может применяться вместе с параметром -s;

-f – отображение полного имени домена (FQDN) для внешних адресов;

-n – отображение адресов и номеров портов в числовом формате;

-o – отображение кода (ID) процесса каждого подключения;

-p-протокол – отображение подключений для протокола, задаваемых этим параметром. Допустимые значения: TCP, UDP, TCPv6 или UDPv6. Используется вместе с параметром -s для отображения статистики по протоколам. Допустимые значения: IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP или UDPv6;

-r – отображение содержимого таблицы маршрутов;

-s – отображение статистики протокола. По умолчанию статистика отображается для протоколов IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP и UDPv6. Параметр -p позволяет указать подмножество выводимых данных;

-t – отображение текущего подключения в состоянии переноса нагрузки с процессора на сетевой адаптер при передаче данных ("offload");

-v – подробный вывод информации, если это возможно;

– интервал – повторный вывод статистических данных через указанный интервал в секундах. Для прекращения вывода данных нажмите клавиши CTRL+C. Если параметр не задан, сведения о текущей конфигурации выводятся один раз.

12. Получите информацию обо всех установленных соединениях и открытых для прослушивания портах. Для этого воспользуйтесь командой netstat -a (рис. 8.2).

```
Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    phantom:epmap          phantom:0              LISTENING
  TCP    phantom:microsoft-ds   phantom:0              LISTENING
  TCP    phantom:1026           phantom:0              LISTENING
  TCP    phantom:7144           phantom:0              LISTENING
  TCP    phantom:7145           phantom:0              LISTENING
  TCP    phantom:1029           phantom:0              LISTENING
  TCP    phantom:netbios-ssn    phantom:0              LISTENING
  TCP    phantom:2168           linux:microsoft-ds     ESTABLISHED
  UDP    phantom:microsoft-ds   *:*
  UDP    phantom:isakmp         *:*
  UDP    phantom:1025           *:*
  UDP    phantom:1044           *:*
```

Рис. 8.2. Список установленных TCP/UDP-соединений
и открытых для прослушивания портов

13. Просмотрите список активных соединений с указанием процесса. Для этого воспользуйтесь командой netstat -n -b (рис. 8.3).

Для выполнения операции необходимо запустить командную строку с правами администратора.

```
Active Connections

  Proto  Local Address          Foreign Address        State           PID
  TCP    192.168.1.2:2168       192.168.1.6:445        ESTABLISHED     4
  [System]
```

Рис. 8.3. Список активных соединений с указанием процесса

14. Получите статистику по протоколам. Для этого воспользуйтесь командой netstat -e -s (рис. 8.4).

```
Interface Statistics

                           Received            Sent

Bytes                      30095310       142750144
Unicast packets               81452           39921
Non-unicast packets           11700             136
Discards                          0               0
Errors                            0               0
Unknown protocols               784

IPv4 Statistics

  Packets Received                    = 85277
  Received Header Errors              = 0
  Received Address Errors             = 0
  Datagrams Forwarded                 = 0
  Unknown Protocols Received          = 0
  Received Packets Discarded          = 0
```

Рис. 8.4. Статистика по протоколам

15. Установите в Wireshark фильтр пакетов tcp.

16. Найдите среди пакетов три сегмента, отвечающие за процесс, называемый термином «трехстороннее рукопожатие» (three-way handshake) (рис. 8.5).

```
Length Info
    66 64409 → 51833 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
    66 51833 → 64409 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=8
    54 64409 → 51833 [ACK] Seq=1 Ack=1 Win=1051136 Len=0
```

Рис. 8.5. «Трехстороннее рукопожатие»

17. Проанализируйте флаги трех пакетов. Поясните изменения значений флагов у пакетов.

18. Определите номер байта TCP (Sequense Number) в последовательности для каждого пакета. Предварительно отключите опцию «Настройки протокола –> TCP –> Analyze TCP sequence numbers».

19. Найдите пакеты, ответственные за разрыв соединения и проанализируйте флаги этих пакетов. Поясните изменения значений флагов у пакетов.

20. Процесс установления и разрыва соединения между клиентом и сервером можно посмотреть в разделе «Статистика –> График потока», установив опцию «Тип потока –> TCP Flows».

21. По результатам выполнения работы необходимо подготовить отчет.

Лабораторная работа № 9

9.1. Инкапсуляция протоколов. Использование сокетов

Для выполнения работы потребуется компьютер с доступом в Internet.

1. Запустите анализатор сети Wireshark и настройте захват пакетов с физического интерфейса.

2. Установите фильтр пакетов http и определите, к каким сетевым уровням относятся сообщения пакета http.

3. Установите фильтр пакетов arp и определите, к каким сетевым уровням относятся сообщения пакета arp.

4. Установите фильтр пакетов bootp и определите, к каким сетевым уровням относятся сообщения пакета dhcp.

5. Разработать клиент-серверное приложение с использованием сокетов. Функционал: по запросу клиента сервер должен выдавать псевдослучайное уникальное число из диапазона динамических портов.

6. Провести тестирование приложения. Зафиксировать полученные от сервера данные.

9.2. Настройка брандмауэра Windows с использованием программы Netsh

Netsh – это служебная программа на базе командной строки, которая позволяет показывать или изменять конфигурацию сети активного компьютера. Команды Netsh можно выполнять путем ввода в командной строке Netsh, также их можно использовать в пакетных файлах или скриптах. Удаленные компьютеры и локальный компьютер можно настроить с помощью команд Netsh.

1. Запустите командное окно от имени администратора.

2. Введите команду netsh (введите /?).

3. Просмотрите список контекстов.

4. Введите команду bye.

5. Просмотрите текущую конфигурацию брандмауэра. Для этого введите команду: netsh advfirewall firewall show rule name=all.

6. Введите команду: netsh advfirewall firewall show rule name=eNSP.

7. Проанализируйте правила для приложения eNSP (рис. 9.1).

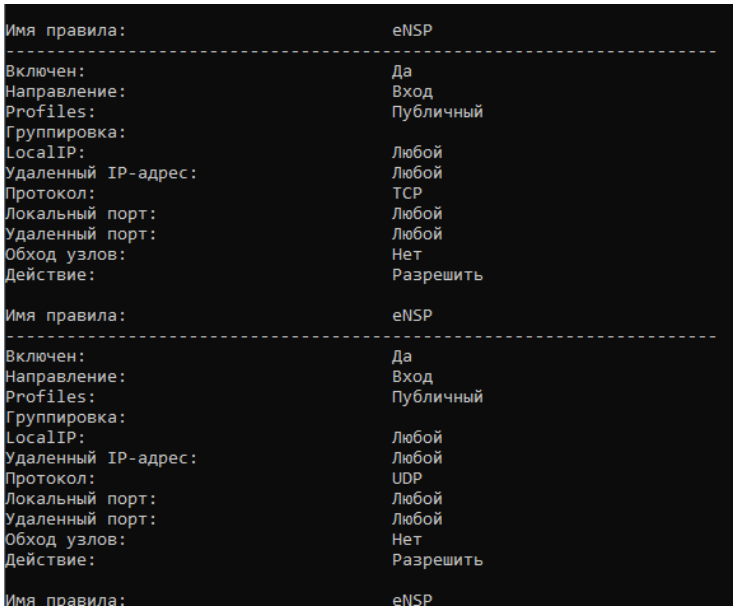

Рис. 9.1. Правила для приложения eNSP

8. Временно отключите брандмауэр. Для этого введите команду: netsh advfirewall set allprofiles state off.

9. Включите брандмауэр. Для этого введите команду: netsh advfirewall set allprofiles state on.

10. Сохраните настройки брандмауэра в файл. Для этого введите команду: netsh advfirewall export “C:\temp\WFconfiguration.wfw”.

11. Убедитесь, что файл с настройками создан (рис. 9.2).

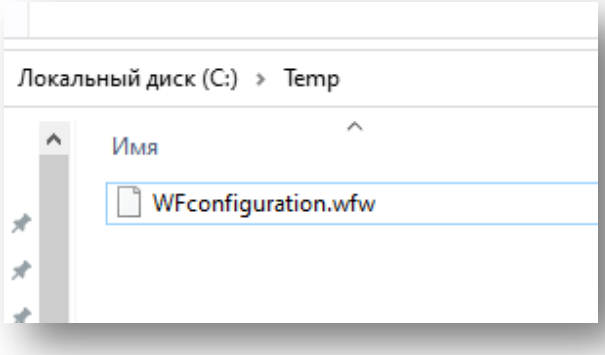

Рис. 9.2. Файл с настройками брандмауэра

12. Восстановите настройки брандмауэра по умолчанию. Для этого введите команду: netsh advfirewall reset.

13. Введите команду: netsh advfirewall firewall show rule name=eNSP.

14. Поясните результат п. 13.

15. Откройте брандмауэр для программы eNSP. Для этого введите команду: netsh advfirewall firewall add rule name=“eNSP” dir=in action=allow program=“C:\Program Files\Huawei\eNSP\eNSP_Client.exe” enable=yes.

16. Введите команду: netsh advfirewall firewall show rule name=eNSP.

17. Создайте правило открытия порта 80. Для этого введите команду: netsh advfirewall firewall add rule name=“Open Port 80” dir=in action=allow protocol=TCP localport=80.

18. Для просмотра информации введите команду: netsh advfirewall firewall show rule name=“Open Port 80”.

19. Удалите правило для порта 80. Для этого введите команду: netsh advfirewall firewall delete rule name=“Open Port 80” protocol= TCP localport=80.

20. Удалите правило для программы eNSP. Для этого введите команду: netsh advfirewall firewall delete rule name=“брандмауэр” program=“C:\Program Files\Huawei\eNSP\eNSP_Client.exe” (рис. 9.3).

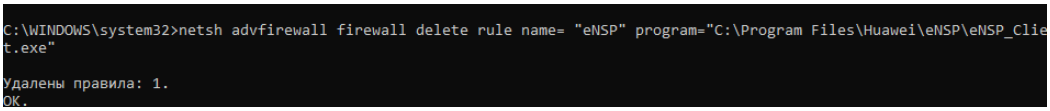

Рис. 9.3. Результат удаления правила “eNSP”

21. Восстановите настройки из файла. Для этого введите команду: netsh advfirewall import “C:\temp\WFconfiguration.wfw”.

22. Убедитесь, что настройки восстановлены.

23. По результатам выполнения работы необходимо подготовить отчет.

Лабораторная работа № 10

Прикладной уровень. Протоколы DNS и HTTP

Для выполнения работы потребуется компьютер с доступом в Internet.

1. Запустите командное окно.

2. Определите IP-адрес сервера kpfu.ru. Для этого введите команду: nslookup kpfu.ru.

3. Запустите браузер.

4. Введите в адресную строку браузера полученный IP-адрес.

5. Запустите анализатор сети Wireshark и настройте захват пакетов с физического интерфейса.

6. Установите фильтр пакетов http.

7. Определите, какие IP-адреса соответствуют серверу www.yandex.ru. Воспользуйтесь утилитой nslookup.

8. Перейдите в Wireshark, просмотрите пакет с DNS-запросом, определите:

– порт получателя в протоколе UDP;

– номер транзакции;

– значения флага запроса на работу DNS-сервера в рекурсивном режиме;

– тип записи в запросе.

9. Просмотрите пакет с DNS-ответом и определите:

– индикатор транзакции;

– наличие или отсутствие ошибок;

– IP-адреса, переданные сервером DNS;

– время сохранения информации в кэш.

10. Просмотрите пакет со вторым DNS-запросом и определите:

– индикатор транзакции;

– тип запрашиваемой записи.

11. Просмотрите пакет со вторым DNS-ответом и определите IPv6 сервера www.yandex.ru.

12. Определите адреса серверов, обслуживающих корневой домен. Для этого введите команду: nslookup -type=ns.

13. Произведите запрос на один из серверов, обслуживающих корневой домен. Для этого введите команду: nslookup www.yandex.ru 199.9.14.201 (рис. 10.1).

Рис. 10.1. Список серверов, обслуживающих зону RU

14. Поясните полученный в п. 13 результат.

15. Перейдите в Wireshark, просмотрите пакет с DNS-ответом на запрос доменного имени www.yandex.ru у сервера с IP-адресом 199.9.14.201 и определите:

– значения флага запроса на работу DNS-сервера в рекурсивном режиме;

– значения IP-адресов серверов, обслуживающих зону RU.

16. Произведите запрос на один из серверов, обслуживающих доменную зону RU. Для этого введите команду: nslookup www.yandex.ru 193.232.156.17.

17. Перейдите в Wireshark, просмотрите пакет с DNS-ответом на запрос доменного имени www.yandex.ru у сервера с IP-адресом 193.232.156.17 и определите:

– значения флага запроса на работу DNS-сервера в рекурсивном режиме;

– количество и IP-адреса серверов, ответственных за доменную зону yandex.ru.

18. Произведите запрос на один из серверов, обслуживающих доменную зону yandex.ru. Для этого введите команду: nslookup www.yandex.ru 213.180.193.1.

19. Чем отличается результат работы команды в п. 18 от п. 7?

Справка: hosts – текстовый файл, содержащий базу данных доменных имен и используемый при их трансляции в сетевые адреса узлов. Файл hosts появился во времена зарождения Интернета (ARPANET). Запрос к этому файлу имеет приоритет перед обращением к DNS-серверам. В отличие от системы DNS, содержимое файла задается администратором компьютера. Путь к папке, где лежит файл hosts, зависит от операционной системы, которая установлена на вашем компьютере:

– Windows XP, 2003, Vista, 7, 8, 10 – c:\windows\system32\drivers\etc\hosts (рис. 10.2);

– Linux, Ubuntu, Unix, BSD – /etc/hosts;

– MacOS – /private/etc/hosts.

Для внесения изменений в файл требуются права администратора.

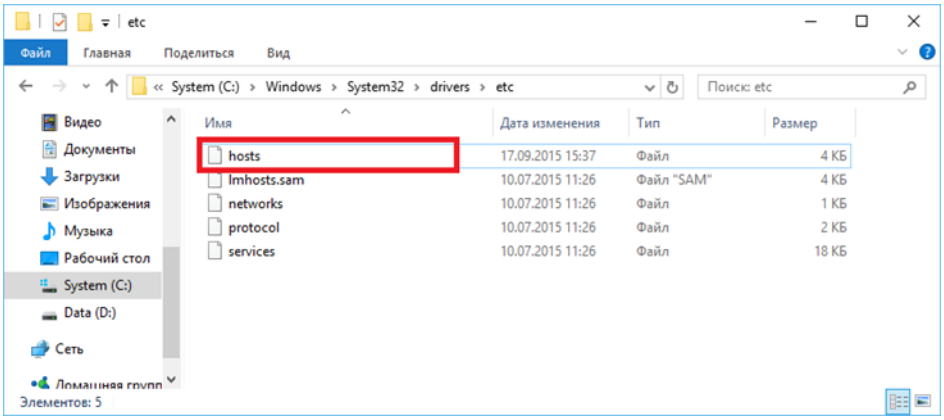

Рис. 10.2. Расположение файла hosts в ОС Windows

20. Откройте файл hosts от имени администратора на своем ПК.

21. Укажите IP-адрес 127.0.0.1 и через пробел – адрес vc.com. Сохраните изменения.

22. Запустите браузер и попробуйте перейти на страницу vc.com.

23. Внесите запись в файл hosts: IP-адрес сервера kpfu.ru.

24. Сохраните результат и проверьте его доступность через браузер сервера kpfu.ru (рис. 10.3).

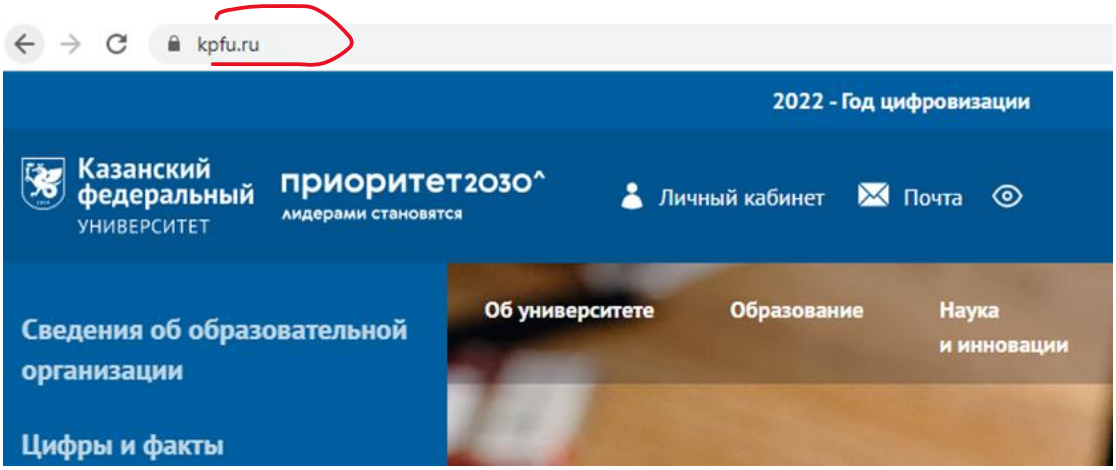

Рис. 10.3. Страничка при обращении к серверу kpfu.ru.

25. Удалите все внесенные в файл hosts записи. Сохраните изменения.

26. Запустите клиент терминала PuTTY.

27. Произведите установку параметров согласно рис. 10.4.

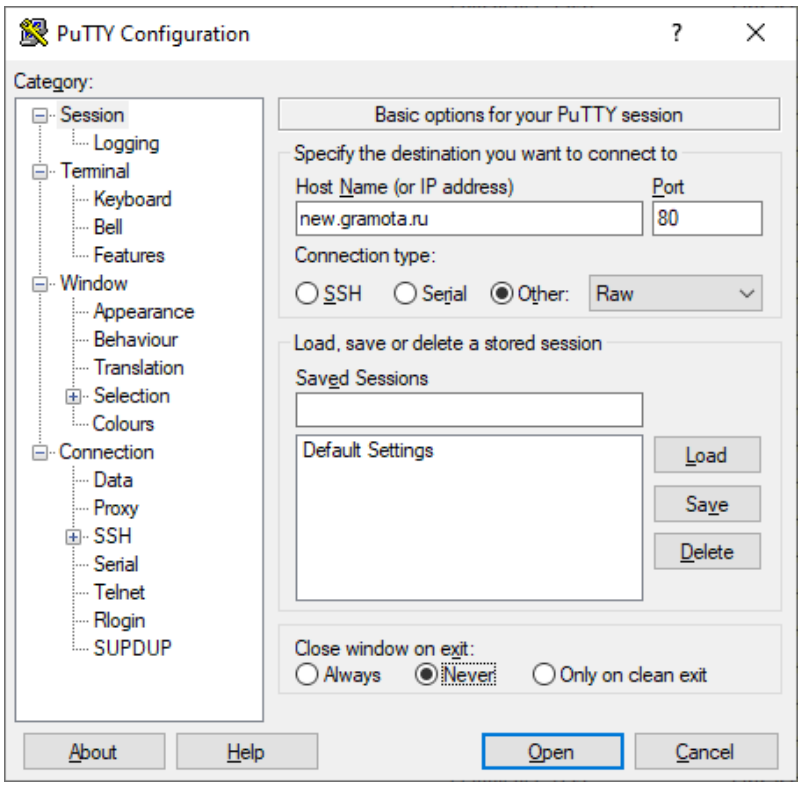

Рис. 10.4. Установка параметров для работы с сервером new.gramota.ru

28. Введите запрос HTTP в окно терминала: GET / HTTP/1.1 (host: new.gramota.ru).

29. Проанализируйте ответ от сервера и определите:

– реализацию сервера;

– дату последнего изменения.

30. Введите запрос HTTP в окно терминала: GET /321 HTTP/1.1 (host: new.gramota.ru).

31. Поясните причину возникновения ответа с кодом 404.

32. Установите параметры для www.cisco.ru по аналогии с п. 27.

33. Введите запрос HTTP в окно терминала: GET /321 HTTP/1.1 (host: www.cisco.ru).

34. Поясните причину возникновения ответа с кодом 301.

35. По результатам выполнения работы необходимо подготовить отчет.