**Министерство науки и высшего образования Российской Федерации**

**федеральное государственное автономное образовательное учреждение высшего образования**

**“НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО”**

|  |  |
| --- | --- |
| **Факультет** | **Программной Инженерии и Компьютерной Техники** |
| **Направление подготовки (специальность)** |  |
| **Дисциплина** | **Компьютерные сети** |

Лабораторная работа 1

ЗАДАНИЕ

Оглавление

[Лабораторная работа №1. Знакомство со средой Cisco Packet Tracer 2](#_Toc190072786)

[**1. Введение в работу** 2](#_Toc190072787)

[**2. Теория. Протоколы ARP и ICMP (программы ping и tracert)** 13](#_Toc190072788)

[**3. Выполнение работы. Пошаговое описание.** 19](#_Toc190072789)

[**Индивидуальное задание** 50](#_Toc190072790)

# Лабораторная работа №1. Знакомство со средой Cisco Packet Tracer

**Цель работы:** познакомиться с интерфейсом симулятора, изучить режим реального времени, основные операции c устройствами.

**Программа работы:**

1. Создание топологии сети;
2. Добавление конечных узлов;
3. Подключение к конечным узлам сетевых устройств;
4. Настройка IP-адресов и масок сети на узлах;
5. Проверка работы сети в режиме реального времени,
6. Разбор простых протоколов низких уровней.

## **1. Введение в работу**

Запускаем среду Cisco Packet Tracer. При запуске программы открывается главное окно симулятора (см. рис. 3.5).

1. Построение топологии сети

Создаем новую топологию сети, выбираем необходимые устройства и соединения.

Топология сети может быть сконфигурирована из различных устройств и связей. В данной лабораторной работе мы используем простые сетевые устройства: концентратор, коммутатор, конечные устройства (компьютеры).

Network Component Box содержит все представленное оборудование, с помощью которого можно построить сеть (см. рис.3.6). С помощью одного клика по каждой группе устройств и соединений можно отобразить различные их варианты, отличающиеся между собой (рис. 4.1).

Рис. 4.1 Виды устройств и соединений

1. Построение топологии, добавление узлов

Один клик по конечным устройствам (рис. 4.2).



Рис. 4.2 Виды конечных устройств

Один клик по выбранному устройству, для нашей работы это PC (рис. 4.3).



Рис. 4.3 Выбор конечного устройства

Переместите курсор на рабочую область симулятора. Курсор должен превратиться в знак “+”. Щелкните мышью в любом месте на области и выбранное вами устройство скопируется. Проделайте эту процедуру еще три раза, на рабочей области у вас будет 4 PC (рис. 4.4).



Рис. 4.4. Вид рабочей области

1. Подключение к узлам концентратора и коммутатора

Выберите группу устройств концентраторы (Hubs), из этой группы выберите первую модель (Hub-PT). Разместите концентратор между PC0 и PC1 (рис. 4.5).

Задача концентратора довольно проста: он повторяет пакет, принятый на одном порту на всех остальных портах.



Рис. 4.5 Вид рабочей области

Подключим PC0 к Hub0, выбрав сначала тип подключения. Для этого случая подойдет медный кабель с прямым подключением (рис. 4.6).



Рис. 4.6 Выбор соединения с прямым подключением

Для подключения PC0 к Hub0 выполните следующие действия (рис. 4.7):

1. Один раз щелкните мышью на PC0
2. Выберите тип интерфейса FastEthernet
3. Переместите курсор на Hub0
4. Нажмите на Hub0 один раз и выберите порт 0
5. Обратите внимание на зеленые индикаторы двух устройств на соединении, что значит, оба устройства готовы к работе.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 1 | 2 | 3 | 4 | 5 |
|  |  |  |  |  |

Рис. 4.7 Подключение PC0 к Hub0

Повторите описанные выше действия для подключения PC1 к Hub0, выбрав на концентраторе порт 1 (рис.4.8). Фактически номер порта значения не имеет, однако удобнее занимать порты последовательно.



Рис. 4.8 Вид рабочей области

Далее размещаем на рабочей области симулятора коммутатор, например, модель 2950-24 (рис. 4.9). Описание семейства коммутаторов серии 2950 можно найти на сайте компании Cisco Systems. [Электронный ресурс]. URL:

<http://www.cisco.com/web/RU/products/hw/switches/ps628/ps627/index.html>.

Коммутаторы - это устройства, работающие на канальном уровне модели OSI и предназначенные для объединения нескольких узлов в пределах одного или нескольких сегментах сети. Коммутатор передает пакеты на основании внутренней таблицы - таблицы коммутации, следовательно, трафик идёт только на тот порт, которому он предназначается, а не повторяется на всех портах, в отличие от концентратора.



Рис. 4.9 Вид рабочей области

Подключим PC2 к Switch0, выбрав тип соединения медный кабель с прямым подключением.

Для подключения выполните следующие действия (рис. 4.10):

1. Щелкните мышью один раз на PC2
2. Выберите тип интерфейса FastEthernet
3. Переместите курсор на Switch0
4. Нажмите один раз на Switch0 и выберите FastEthernet0/1
5. Обратите внимание, что для правильной работы сети оба подключенных устройства должны быть готовы, о чем свидетельствуют зеленые индикаторы. В отличие от подключения к концентратору, это может занять некоторое время.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 1 | 2 | 3 | 4 | 5 |  |
|  |  |  |  |  |  |

Рис. 4.10 Подключение PC2 к Switch0

Повторите описанные выше действия для подключения PC3 к Switch0, выбрав один из его интерфейсов FastEthernet0/2 (рис. 4.11).

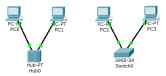


Рис. 4.11 Вид рабочей области

Если навести курсор на один из индикаторов, можно посмотреть, какой интерфейс задействован при данном подключении (рис. 4.12).



Рис. 4.12 Вид рабочей области

1. Настройка IP-адреса и маски подсети на хостах

Прежде чем мы сможем общаться между хостами по сети, нам нужно настроить IP-адреса и маски подсети на устройствах.

Щелкните мышью один раз на PC0. Откроется окно свойств конечного узла на вкладке Physical (рис. 4.13).



Рис. 4.13 Вкладка Physical конечного устройства (компьютера)

Физический вид устройства мы менять не будем, поэтому сразу переходим к настройке в вкладке Config (рис. 4.14).

Именно здесь вы можете изменить название PC0 (например, ввести IP-адрес этого компьютера, чтобы не подглядывать его каждый раз в настройках). Кроме того, здесь вы можете указать IP-адрес шлюза, также известный как шлюз по умолчанию, и IP-адрес DNS-сервера. Мы обсудим это позже, но это будет IP-адрес локального маршрутизатора. Если вы хотите, вы можете ввести IP-адрес шлюза 192.168.1.1 и IP-адрес DNS-сервера 192.168.1.100, хотя он не будет использоваться в этой лабораторной работе.



Рис. 4.14 Вкладка Config конечного устройства (компьютера)

Кликните мышью на интерфейсе FastEthernet (рис. 4.15). Укажите IP-адрес компьютера 192.168.1.10. Нажмите на поле для ввода маски подсети, она определится автоматически 255.255.255.0.



Рис. 4.15 Настройки интерфейса конечного устройства

Информация автоматически сохраняется после ввода.

Закройте окно настройки PC0 и повторите указанные выше действия для остальных узлов сети, используя информацию о IP-адресах и маски подсети, представленную в таблице 4.1

Таблица 4.1

|  |  |  |
| --- | --- | --- |
| Хост | IP-адрес | Маска подсети |
| PC0 | 192.168.1.10 | 255.255.255.0 |
| PC1 | 192.168.1.11 | 255.255.255.0 |
| PC2 | 192.168.1.12 | 255.255.255.0 |
| PC3 | 192.168.1.13 | 255.255.255.0 |

После настройки узлов рабочая область симулятора будет выглядеть следующим образом (рис. 4.16):

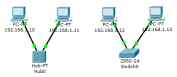


Рис. 4.16 Вид рабочей области

Можно проверить введенную вами информацию на узлах (рис. 4.17). Для этого наведите курсор на интересующее вас устройство.



Рис. 4.17 Проверка настроек конечного устройства (компьютера)

Если при построении сети какие-либо устройства или связи оказались лишними, их можно удалить при помощи инструмента Delete на боковой панели симулятора (Common Tools Bar). Для удаления нужно щелкнуть один раз на инструмент Delete, затем на элемент сети.

1. Соединение концентратора и коммутатора

Для подключения такого типа устройств, как коммутатора и концентратора, используется перекрестный кабель (рис. 4.18).



Рис. 4.18. Выбор соединения

Для подключения Hub0 к Switch0 выполните следующие действия:

1. Щелкните один раз на Hub0, выберите порт 2 (рис. 4.19).

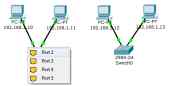


Рис. 4.19 Вид рабочей области

1. Переместите курсор на Switch0, щелкните на нем мышью и выберите интерфейс FastEthernet0/3 (рис. 4.20).

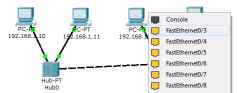


Рис. 4.20. Вид рабочей области

1. Когда оба устройства будут готовы к работе, индикаторы состояния станут зелеными (рис. 4.21).

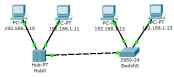


Рис. 4.21. Вид рабочей области

1. Выполним проверку в режиме реального времени

Убедитесь, что вы находитесь в режиме реального времени.



Сформируем простой пакет ping-запроса для проверки работы сети, воспользовавшись Add Simple PDU. Нажмите один раз на Add Simple PDU.



Теперь нужно выбрать два узла: источник и приемник ping-запроса. Наведите курсор на PC0 (192.168.1.10) и щелкните на нем мышью (источник ping-запроса), затем переместите курсор на PC3 (192.168.1.13) (приемник ping-запроса) и кликните на нем.

Так как все интерфейсы и связи сети настроены правильно (о чем говорят зеленые индикаторы состояния), то ping-запрос должен пройти успешно. В окне управления пакетами User Created Packet Window (см. рис. 3.6) появится соответствующая запись (рис. 4.22).



Рис. 4.22 Окно управления пакетами

Важно: измените IP-адрес 192.168.1.13 узла PC3 на IP-адрес 192.168.2.13, с той же маской подсети 255.255.255.0. Выполните ping-запрос от PC0 к PC3. Какой получился результат? Каковы причины?

Чтобы очистить список выполненных операций моделирования, необходимо удалить соответствующий сценарий симуляции.

Нажмите на кнопку Delete на панели User Created Packet Window (рис. 4.23).



Рис. 4.23 Окно управления пакетами

Все записи сценария удалятся.

1. Сохранение созданной топологии

Выберите в Menu Bar вкладку File, далее Save as. Выберите соответствующую директорию. Все файлы симулятора Cisco Packet Tracer имеют расширение .pkt.

1. Построение топологии сети, состоящей из двух подсетей

В результате первой работы мы изучили основные операции с устройствами. Для подготовки к выполнению следующей лабораторной работы у нас есть соответствующие знания и навыки для построения топологии сети следующего вида (рис. 4.24):

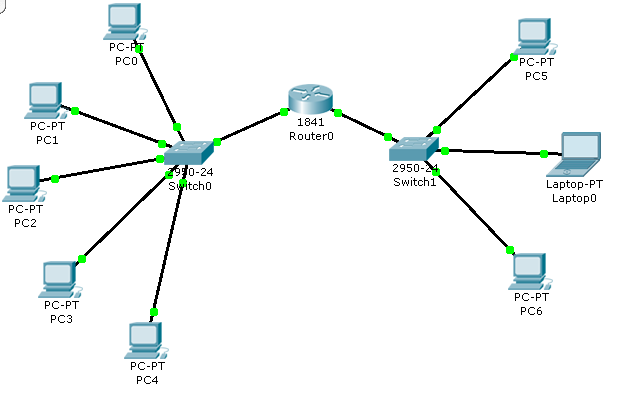


Рис. 4.24. Топология сети для лабораторной работы №2

такой топологии нужно добавить в рабочую область симулятора конечные узлы, два коммутатора и маршрутизатор. При добавлении маршрутизатора выберите модель 1841, т.к. она имеет два интерфейса. Описание маршрутизаторов серии 1841 можно найти на сайте компании Cisco Systems. [Электронный ресурс]. URL: <http://www.cisco.com/en/US/products/ps5875/index.html>. При соединении устройств между собой воспользуйтесь медным кабелем с прямым подключением.

## **2. Теория. Протоколы ARP и ICMP (программы ping и tracert)**

**Протокол ARP**

Для определения физического адреса по IP-адресу используется протокол разрешения адреса Address Resolution Protocol (ARP). Протокол ARP работает различным образом в зависимости от того, какой протокол канального уровня работает в данной сети с возможностью широковещательного доступа одновременно ко всем узлам сети. [1]

Протокол ARP позволяет динамически определить МАС-адрес по IP-адресу. МАС-адрес – это уникальный серийный номер, присваиваемый каждому сетевому устройству для идентификации его в сети, так же называется физическим или аппаратным адресом. Протокол локальной сети, поддерживаемый в лабораторной работе – Ethernet. В Ethernet сетях, использующих стек TCP/IP, сетевой интерфейс имеет физический адрес длиной в 48 бит. Кадры, которыми обмениваются на канальном уровне, должны содержать аппаратный адрес сетевого интерфейса. Однако TCP/IP использует собственную схему адресации: 32-битные IP-адреса. Значение IP-адреса приемника недостаточно, чтобы отправить дейтаграмму этому хосту. Драйвер Ethernet должен знать МАС-адрес интерфейса назначения, чтобы послать туда данные. В задачу ARP входит обеспечение динамического соответствия между 32-битными IP-адресами и 48-битными МАС-адресами, используемыми различными сетевыми технологиями. Протокол ARP работает в пределах одной подсети и автоматически запускается, когда возникает необходимость преобразования IP-адреса в аппаратный адрес. [2]

Работа протокола ARP поясняется на рис. 4.25.

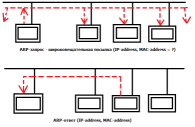


Рис. 4.25 ARP-запрос и ARP-ответ

Узел, которому нужно выполнить отображение IP-адреса на локальный адрес, формирует ARP-запрос, вкладывает его в кадр протокола канального уровня, указывая в нем известный IP-адрес, и рассылает запрос широковещательно. Все узлы локальной сети получают ARP запрос и сравнивают указанный там IP-адрес с собственным. В случае их совпадения узел формирует ARP-ответ, в котором указывает свой IP-адрес и свой локальный адрес и отправляет его уже направленно, так как в ARP запросе отправитель указывает свой локальный адрес.

Для того чтобы уменьшить количество посылаемых запросов ARP, каждое устройство в сети, использующее протокол ARP, должно иметь специальную буферную память. В ней хранятся пары адресов (IP-адрес, физический адрес) устройств в сети. Всякий раз, когда устройство получает ARP-ответ, оно сохраняет в буферной памяти соответствующую пару. Если адрес есть в списке пар, то нет необходимости посылать ARP-запрос. Эта буферная память называется ARP-таблицей.

В ARP-таблице могут содержаться как статические, так и динамические записи. Динамические записи добавляются и удаляются автоматически, статические заносятся вручную.

Так как большинство устройств в сети поддерживает динамическое разрешение адресов, то администратору, как правило, нет необходимости вручную указывать записи протокола ARP в таблице адресов.

Каждая запись в ARP-таблице имеет свое время жизни. Политики очистки ARP-таблицы продиктованы используемой операционной системой. При добавлении записи для нее активируется таймер.

Сообщения протокола ARP при передаче по сети инкапсулируются в поле данных кадра. Они не содержат IP-заголовка. В отличие от сообщений большинства протоколов, сообщения ARP не имеют фиксированного формата заголовка. Это объясняется тем, что протокол был разработан таким образом, чтобы он был применим для разрешения адресов в различных сетях. [3]

ARP-запросы и ответы используют один и тот же формат пакета. Так как локальные адреса могут в различных типах сетей иметь различную длину, то формат пакета протокола ARP зависит от типа сети. На рис. 4.26 показана структура пакета запросов и ответов. [4]



Рис. 4.26 Формат пакета ARP

* Network Type – тип канального протокола

Для Ethernet – 1.

* Protocol - протокол сетевого уровня
* HAL - длина канального адреса
* PAL - длина сетевого адреса
* Operation - тип операции (1 – запрос, 2 – ответ)

Узел, отправляющий ARP-запрос, заполняет в пакете все поля, кроме поля искомого локального адреса. Значение этого поля заполняется узлом, опознавшим свой IP-адрес.

**Протокол ICMP**

Протокол ICMP предназначен для передачи управляющих и диагностических сообщений. С его помощью передаются сообщения об ошибках, а также о возникновении ситуаций, требующих повышенного внимания. Протокол относится к сетевому уровню модели TCP/IP. Сообщения ICMP генерируются и обрабатываются протоколами сетевого (IP) и более высоких уровней (TCP или UDP). При появлении некоторых ICMP-сообщений генерируются сообщения об ошибках, которые передаются пользовательским процессам. ICMP-сообщения передаются внутри IP-дейтаграмм (рис. 4.27). [2]



Рис. 4.27 Инкапсуляция ICMP-сообщений в IP-дейтаграммы

Формат ICMP-сообщения показан на рис. 4.28. Заголовок ICMP включает 8 байт, но только первые 4 байта одинаковы для всех сообщений, остальные поля заголовка и тела сообщения определяются типом сообщения.



Рис. 4.28 Формат ICMP-сообщения

Поле контрольной суммы охватывает ICMP-сообщение целиком.

Тип сообщения определяется значением поля “Тип” заголовка. Некоторые типы ICMP-сообщений имеют внутреннюю детализацию (код), при этом конкретный вид сообщения определяется как типом, так и кодом сообщения. Подробнее с видами типов и кодов ICMP-сообщений можно ознакомиться в спецификации протокола ICMP RFC 792. [Электронный ресурс]. URL: <http://tools.ietf.org/html/rfc792>.

**Программа ping**

Программа ping была разработана для проверки доступности удаленного узла. Программа посылает ICMP-эхо-запрос на узел и ожидает возврата ICMP-эхо-отклика. Программа рing является обычно первым диагностическим средством, с помощью которого начинается идентификация какой-либо проблемы в сетях. Помимо доступности, с помощью ping можно оценить время возврата пакета от узла, что дает представление о том, "насколько далеко" находится узел. Кроме этого, Ping имеет опции записи маршрута и временной метки. Сообщения эхо-запроса и эхо-отклика имеют один формат (рис 4.29). [2]



Рис. 4.29 Формат пакета ICMP-сообщения

* Тип – тип пакета

8 – запрос эха

0 – ответ на запрос эха

* Код – расшифровка назначения пакета внутри типа (в данном случае 0)
* Контрольная сумма вычисляется для всего пакета
* Идентификатор – номер потока сообщений
* Последовательный номер – номер пакета в потоке [3]

Так же, как в случае других ICMP-запросов, в эхо-отклике должны содержаться поля идентификатора и номера последовательности. Кроме того, любые дополнительные данные, посланные компьютером, должны быть отражены эхом.

В поле идентификатора ICMP сообщения устанавливается идентификатор процесса, отправляющего запрос. Это позволяет программе ping идентифицировать вернувшийся ответ, если на одном и том же хосте в одно и то же время запущено несколько программ ping.

Номер последовательности начинается с 0 и инкрементируется каждый раз, когда посылается следующий эхо-запрос. Вывод программы показан на рис. 4.30. Первая строка вывода содержит IP-адрес хоста назначения, даже если было указано имя. Поэтому программа рing часто используется для определения IP-адреса удаленного узла. [2]

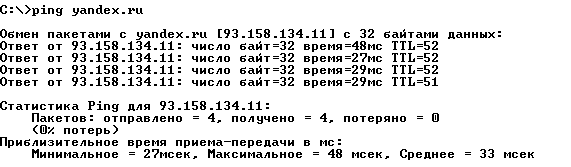


Рис. 4.30 Вывод программы ping

**Программа tracert**

Программа tracert позволяет посмотреть маршрут, по которому двигаются IP-дейтаграммы от одного хоста к другому.

Программа tracert не требует никаких специальных серверных приложений. В ее работе используются стандартные функции протоколов ICMP и IP. Для понимания работы программы следует вспомнить порядок обработки поля TTL в заголовке IP-дейтаграммы.

Каждый маршрутизатор, обрабатывающий дейтаграмму, уменьшает значение поля TTL в ее заголовке на единицу. При получении дейтаграммы с TTL равным 1, маршрутизатор уничтожает ее и посылает хосту, который ее отправил, ICMP-сообщение "время истекло". При этом дейтаграмма, содержащая это ICMP-сообщение, имеет в качестве адреса источника IP-адрес маршрутизатора.

Это и используется в программе tracert. На хост назначения отправляется IP-дейтаграмма, в которой поле TTL, установлено в единицу. Первый маршрутизатор на пути дейтаграммы, уничтожает ее (так как TTL равно 1) и отправляет ICMP-сообщение об истечении времени. Таким образом, определяется первый маршрутизатор в маршруте. Затем tracert отправляет дейтаграмму с полем TTL равным 2, что позволяет получить IP-адрес второго маршрутизатора. Аналогичные действия продолжаются до тех пор, пока дейтаграмма не достигнет хоста назначения. При получении ответа от этого узла процесс трассировки считается завершённым.

Пример вывода программы показан на рис. 4.31.



Рис. 4.31 Вывод программы tracert

Первая строка, без номера содержит имя и IP адрес пункта назначения и указывает на то, что величина TTL не может быть больше 30.

Следующие строки вывода начинаются с распечатки значения TTL (1, 2, 3 и т.д.) и содержат имя (IP-адрес) хоста или маршрутизатора и время возврата ICMP-сообщения.

Для каждого значения TTL отправляется 3 дейтаграммы. Для каждого возвращенного ICMP-сообщения рассчитывается и печатается время возврата.

Если ответ на дейтаграмму не получен в течение пяти секунд, печатается звездочка, после чего отправляется следующая дейтаграмма. [2]

## **3. Выполнение работы. Пошаговое описание.**

1. Построение топологии сети

В конце вводной лабораторной работы мы создали следующую топологию сети, состоящую из конечных узлов (PC), коммутаторов и маршрутизатора (рис. 4.32):

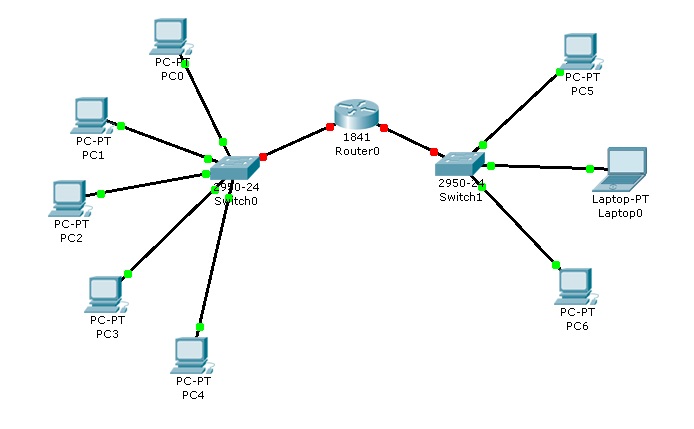


Рис. 4.32 Тестовая топология сети

Маршрутизатор Router0 имеет два интерфейса и соединяет две подсети. Произведем настройку конечных узлов.

1. Настройка конечных узлов

На устройствах PC0-PC4 установим заданные IP-адреса и маску подсети (таблица 4.2). IP-адрес шлюза для всех узлов – 192.168.3.1. IP-адрес DNS-сервера указывать необязательно, т.к. в данной работе он использоваться не будет.

Таблица 4.2

|  |  |  |
| --- | --- | --- |
| Хост | IP-адрес | Маска подсети |
| PC0 | 192.168.3.3 | 255.255.255.0 |
| PC1 | 192.168.3.4 | 255.255.255.0 |
| PC2 | 192.168.3.5 | 255.255.255.0 |
| PC3 | 192.168.3.6 | 255.255.255.0 |
| PC4 | 192.168.3.7 | 255.255.255.0 |

На устройствах PC5, Laptop0, PC6 установим заданные IP-адреса и маску подсети (таблица 4.3). IP-адрес шлюза для всех узлов – 192.168.5.1. IP-адрес DNS-сервера указывать необязательно.

Таблица 4.3

|  |  |  |
| --- | --- | --- |
| Хост | IP-адрес | Маска подсети |
| PC5 | 192.168.5.3 | 255.255.255.0 |
| Laptop0 | 192.168.5.4 | 255.255.255.0 |
| PC6 | 192.168.5.5 | 255.255.255.0 |

Каждый узел переименуем его же IP-адресом, получится следующее (рис. 4.33):

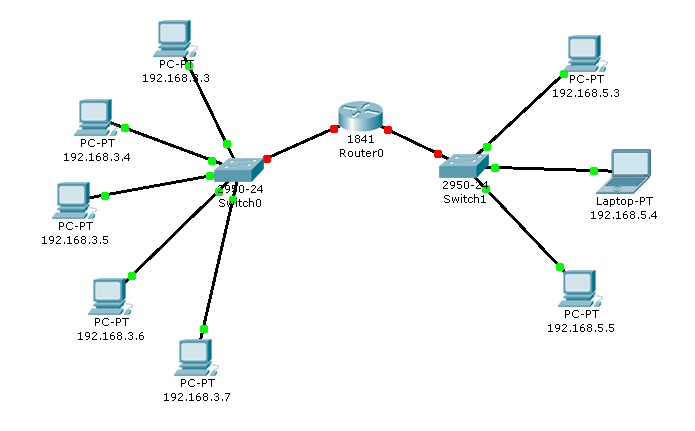


Рис. 4.33 Вид рабочей области

1. Настройка маршрутизатора

При настройке конечных узлов уже упоминалось о том, что маршрутизатор в данной топологии сети имеет два интерфейса. Произведем настройку интерфейса FastEthernet0/0:

1. Один клик по устройству (маршрутизатору);
2. Выбираем вкладку “Config”;
3. Находим интерфейс FastEthernet0/0, задаем нужный IP-адрес и маску подсети (рис. 4.34).

**Важно: интерфейс маршрутизатора, по умолчанию, отключен; необходимо его включить, кликнув мышкой рядом с “On”.**

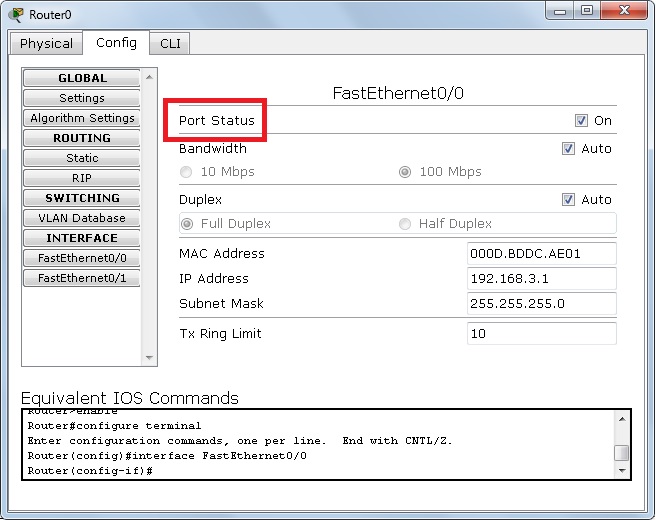


Рис. 4.34 Настройка интерфейса маршрутизатора

1. Закрываем окно, смотрим на всю топологию сети. Зеленые индикаторы состояния на линии связи между Router0 и Switch0 сигнализируют, что интерфейс подключен правильно (рис. 4.35).

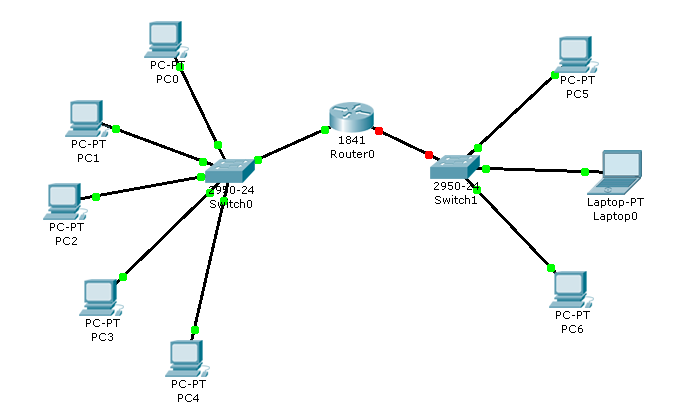


Рис. 4.35 Вид рабочей области

Аналогично производим настройку интерфейса FastEthernet0/1 (рис. 4.36).

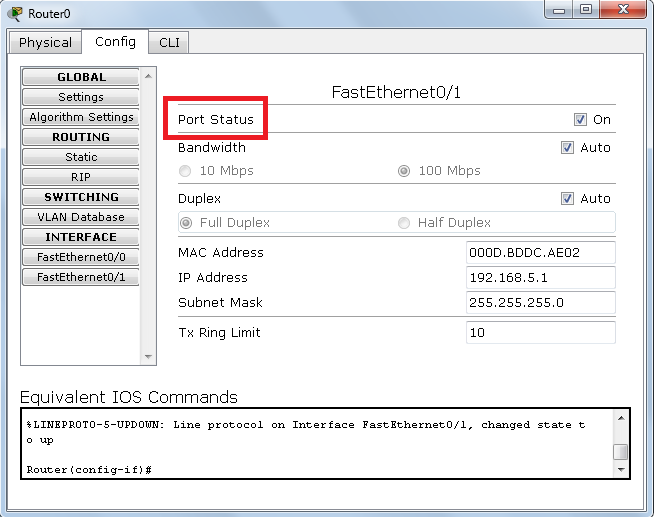


Рис. 4.36 Настройка интерфейса маршрутизатора

Сделать надписи к интерфейсам маршрутизатора, можно с помощью инструмента Place Note на панели Common Tools . Необходимо кликнуть на инструмент, затем сделать клик в нужном месте на рабочей области.

1. Режим симуляции Cisco Packet Tracer

Убедитесь, что вы находитесь в режиме симуляции. Для этого кликните на иконку симуляции в правом нижнем углу рабочей области симулятора. Описание: 8.png

Откроется окно событий, в котором вы увидите список событий, управляющие кнопки, заданные фильтры (рис. 4.37). По умолчанию, фильтруются, т.е. будут отображаться, пакеты всех возможных протоколов, необходимо поправить и ограничить этот список до исследуемых протоколов.

Управляющие кнопки:

* Back – назад
* Auto Capture/Play – автоматический захват пакетов от источника до приемника и обратно
* Capture/Forward – захват пакетов только от одного устройства до другого

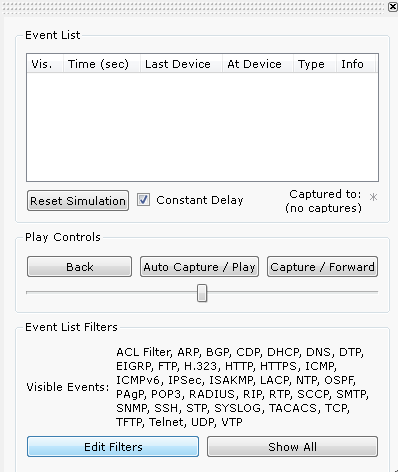


Рис. 4.37 Окно событий режима симуляции

В данной лабораторной работе нас интересуют пакету двух типов ARP и ICMP.

Следовательно, нужно поставить фильтр только на сообщения заданного типа (рис. 4.38):

1. Нажимаем на кнопку “Edit Filters”
2. Снимаем метку с “Show All/None”
3. Выбираем ARP и ICMP

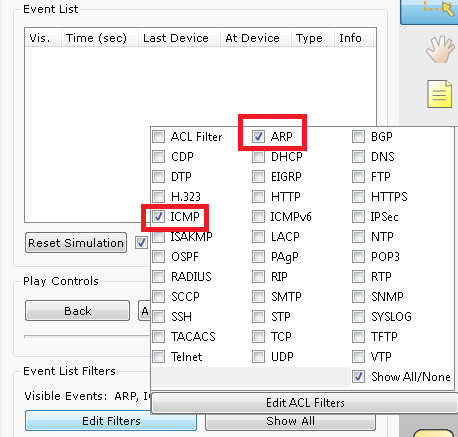


Рис. 4.38 Добавление фильтров на протоколы ARP и ICMP

1. Убедимся, что заданные протоколы для фильтрации назначены (рис. 4.39)

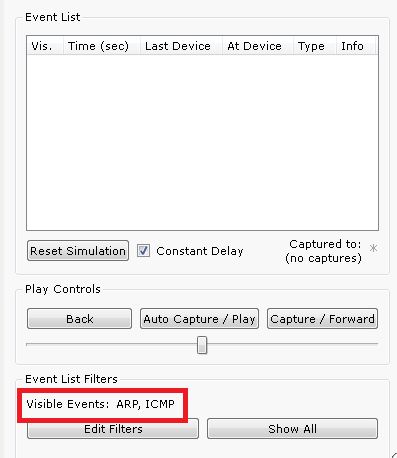


Рис. 4.39 Окно событий режима симуляции

1. Проверка работы сети в режиме симуляции

Отправим тестовый ping-запрос с конечного узла c IP-адресом 192.168.3.3 на хост с IP-адресом 192.168.3.5.

**Важно: оба узла находятся в пределах одного сегмента сети**

1. Один клик по выбранному устройству (рис. 4.40)

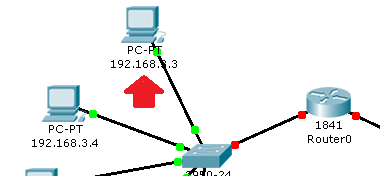


Рис. 4.40 Выбор узла 192.168.3.3

1. Выбираем вкладку Desktop, в которой содержатся симуляторы некоторых программ, доступных на компьютере (см. рис. 3.4).
2. Выбираем “Command Prompt”, программу, имитирующую командную строку компьютера.
3. С помощью утилиты ping отправляем ping-запрос (рис. 4.41). (Не забудьте нажать Enter).

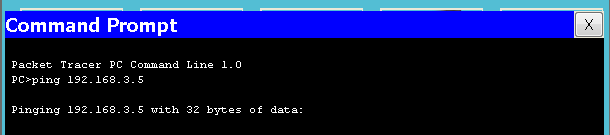


Рис. 4.41 Командная строка узла 192.168.3.3

На устройстве-источнике формируются два пакета протокола ARP и ICMP (рис. 4.42). ARP-запрос возникает всегда, когда хост пытается связаться с другим хостом.

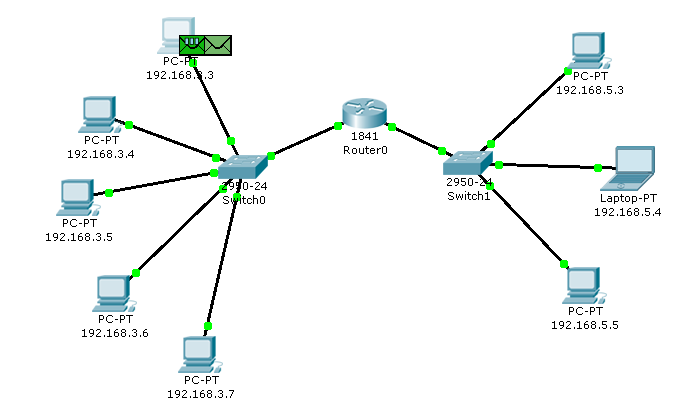


Рис. 4.42 Вид рабочей области

Нажимаем на кнопку “Auto Capture/play” или “Capture/Forward”, последняя позволит вам управлять движением пакетов от устройства к устройству самим. Видим, что первым отправляется пакет протокола ARP, так как ARP-таблица хоста 192.168.3.3 пуста, и он еще «не знает», кому отправлять ping-запрос. Сделайте один клик по самому пакету (конверту), ознакомьтесь, какие уровни модели OSI задействованы. Перейдите к вкладке “Inbound PDU Details”, которая содержит структуру пакета (рис. 4.43).

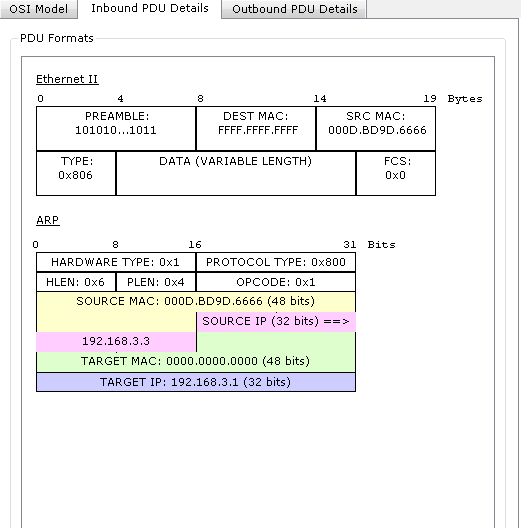


Рис. 4.43 Формат пакета ARP-запроса

Узел 192.168.3.3 построил запрос и посылает его широковещательным сообщением всем хостам подсети. Помимо IP-адреса назначения, запрос содержит IP-адрес и МАС-адрес отправителя, чтобы приемная сторона могла ответить.

При просмотре прохождения пакетов убедитесь, что на ARP-запрос ответит только хост 192.168.3.5. Каждый хост в подсети получает запрос и проверяет на соответствие свой IP-адрес. Если он не совпадает с указанным адресом в запросе, то запрос игнорируется (рис. 4.44).

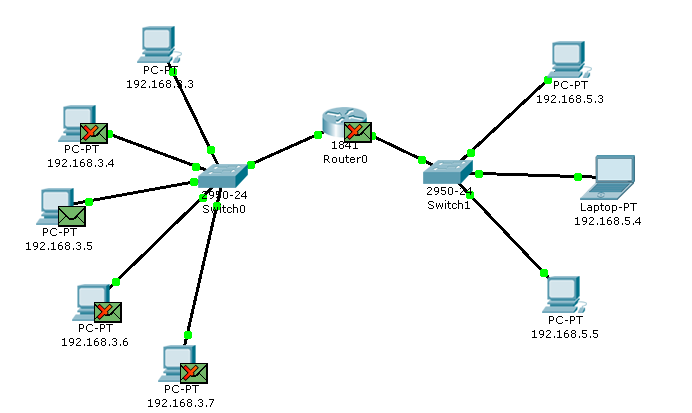


Рис. 4.44 Вид рабочей области

Посмотрите содержимое пакета ARP-ответа, пришедшего на хост 192.168.3.3 (рис. 4.45).

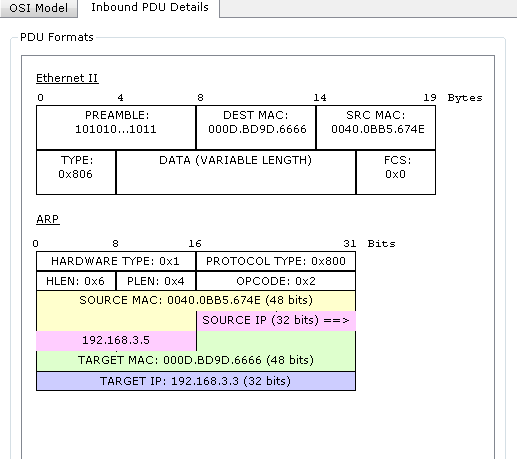


Рис. 4.45 Формат пакета ARP-ответа

Узел 192.168.3.5. послал ARP-ответ непосредственно отправителю, используя его МАС-адрес, с указанием собственного МАС-адреса в поле “Target МАС”.

Далее отправляется ICMP-сообщение ping-запроса. Посмотрите содержимое пакета, сделав клик по пакету (конверту) (рис. 4.46).

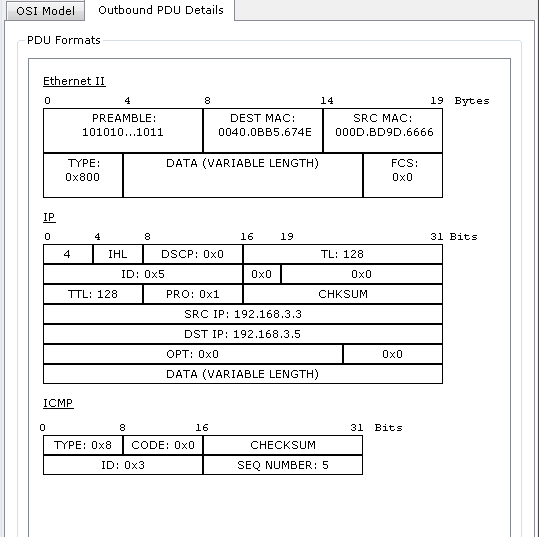


Рис. 4.46 Формат пакета ICMP-эхо-запроса

Физические адреса узлов известны. IP-адрес источника – 192.168.3.3. IP-адрес назначения – 192.168.3.5. Тип ICMP-сообщения – 8 (эхо-запрос).

Запрос производится на хост 192.168.3.5 через коммутатор (рис. 4.47).

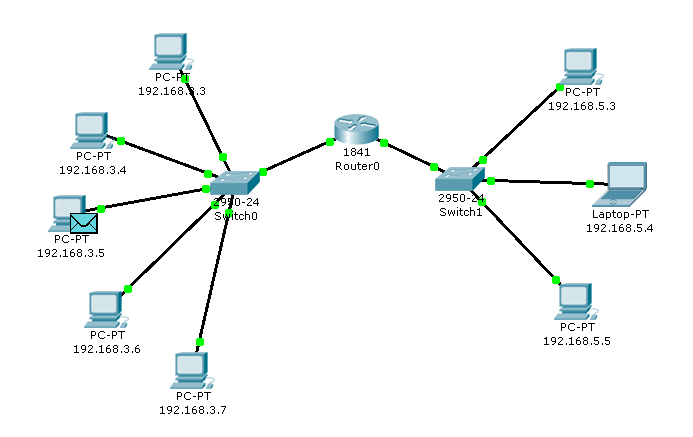


Рис. 4.47 Вид рабочей области

Посмотрите содержимое пакета ping-ответа, пришедшего на хост 192.168.3.3 (рис. 4.48).

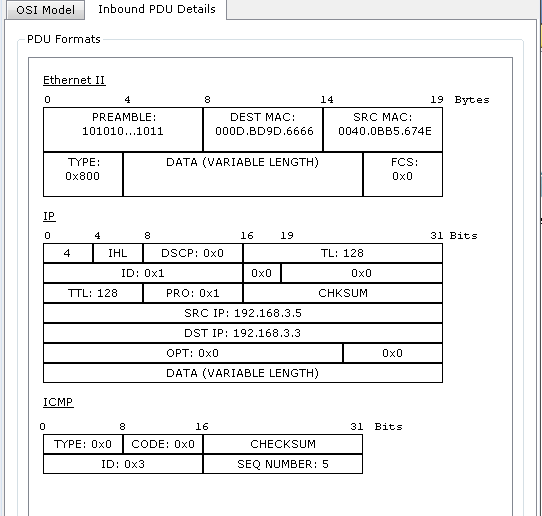


Рис. 4.48 Формат пакета ICMP-эхо-ответа

IP-адрес источника – 192.168.3.5. IP-адрес назначения – 192.168.3.3. Тип ICMP-сообщения – 0 (эхо-ответ).

Посмотрите ping-ответ в командной строке хоста 192.168.3.3 (рис. 4.49).

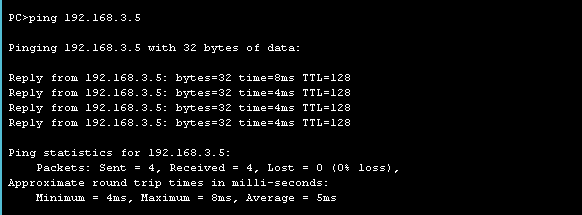


Рис. 4.49 Вывод программы ping

В окне событий так же указаны маршруты запроса ARP и ICMP: через какие устройства прошли пакеты (рис. 4.50).

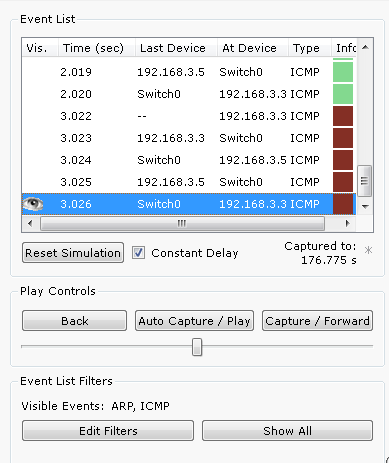


Рис. 4.50 Окно событий режима симуляции

Удалить сценарий симуляции можно с помощью кнопки “Reset Simulation” или воспользоваться кнопкой “Delete” в области User Created Packet Window.

Теперь ARP-таблицы хостов 192.168.3.3 и 192.168.3.5 не пусты, в них содержится одна запись. Чтобы просмотреть содержимое ARP-таблицы, нужно выполнить команду

“arp –a” в командной строке.

Содержимое ARP-таблицы узла 192.168.3.3 (рис. 4.51):

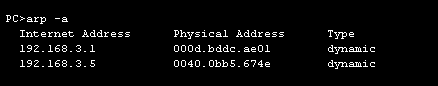


Рис. 4.51 ARP-таблица узла 192.168.3.3 в командной строке

Можно воспользоваться другим способом: нажать на кнопку «Inspect» , нажать на выбранное устройство, выбрать «ARP table» и просмотреть записи ARP-таблицы узла (рис. 4.52).

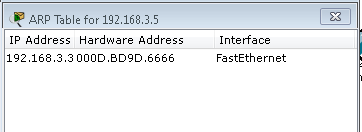


Рис. 4.52 ARP-таблица узла 192.168.3.5, показанная с помощью инструмента «Inspect»

Если снова задать ping-запрос на хост 192.168.3.5, то сразу будет сформирован только один пакет ICMP-сообщения, т.к. в ARP-таблице компьютера-источника уже хранится соответствующий локальный адрес.

Попробуйте отправить ping-запрос снова.

Чтобы удалить все записи ARP-таблицы, следует воспользоваться командой “arp –d”.

1. Посылка ping-запроса во внешнюю сеть

Отправим тестовый ping-запрос с конечного узла c IP-адресом 192.168.3.4 на хост с IP-адресом 192.168.5.5.

**Важно: один узел пытается передать пакет другому узлу, находящемуся с ним в разных сетях.**

В пункте 5 лабораторной работы был рассмотрен случай посылки ARP-запроса внутри локальной сети. Протокол ARP в этом случае определял непосредственно МАС-адрес узла-приемника запроса. Теперь рассмотрим ситуацию, когда узел-источник и узел-приемник находятся в разных сетях. Протокол ARP работает в пределах сегмента сети, поэтому в данном случае он будет использоваться для определения МАС-адреса маршрутизатора. Таким образом, пакет будет передан маршрутизатору для дальнейшей ретрансляции.

Открываем “Command Promt”, имитирующую командную строку, на компьютере 192.168.3.4 и посылаем на хост 192.168.5.5. ping-запрос (рис. 4.53).

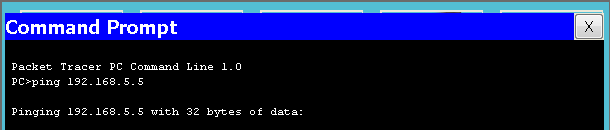


Рис. 4.53 Командная строка узла 192.168.3.4

В этом случае инициируется ARP-запрос маршрутизатору, который пересылает пакеты в сеть назначения. На узле-источнике формируются два пакета протокола ARP и ICMP (рис. 4.54).

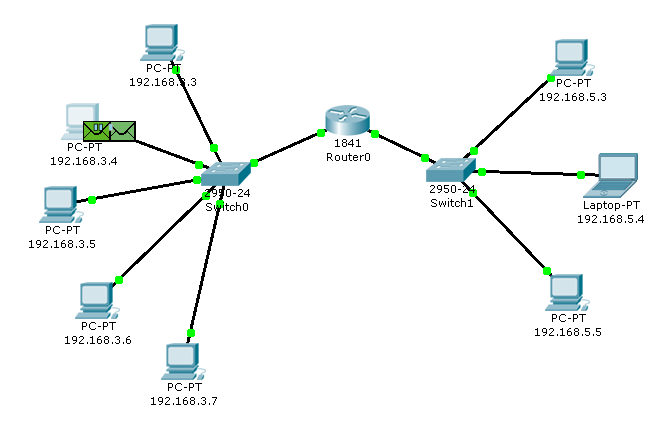


Рис. 4.54 Вид рабочей области

Формат пакета ARP-запроса содержит те же сведения, что и для разрешения локального адреса устройства, и рассылается широковещательно всем узлам подсети (рис. 4.55).

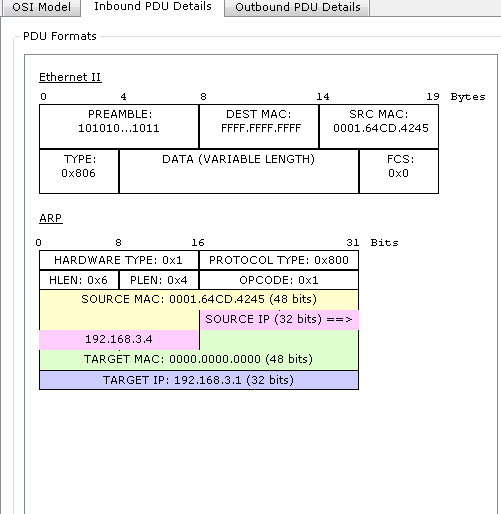


Рис. 4.55 Формат пакета ARP-запроса

Все узлы игнорируют пакет, кроме маршрутизатора, которому этот пакет предназначался (рис. 4.56).

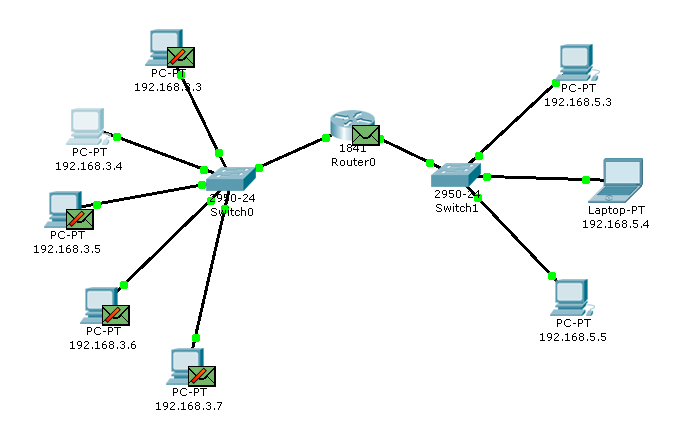


Рис. 4.56 Вид рабочей области

Маршрутизатор формирует ARP-ответ, указывая свой физический адрес, и отправляет его узлу 192.168.3.4 (рис. 4.57).

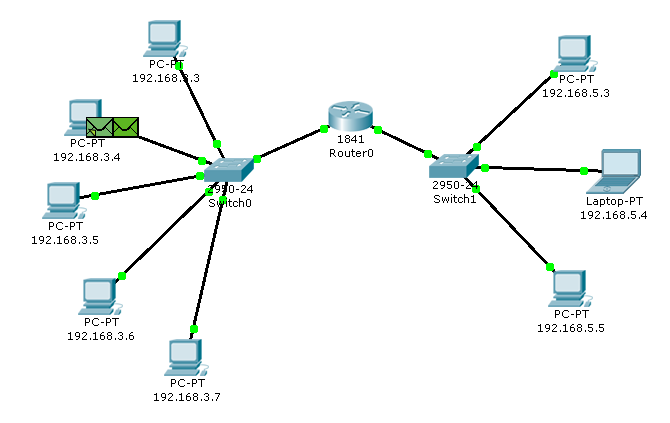


Рис. 4.57 Вид рабочей области

После получения ARP-ответа хост 192.168.3.4 посылает ICMP-сообщение ping-запроса через маршрутизатор в сеть назначения.

Посмотрите содержимое пакета, сделав клик по пакету (конверту) (рис. 4.58).

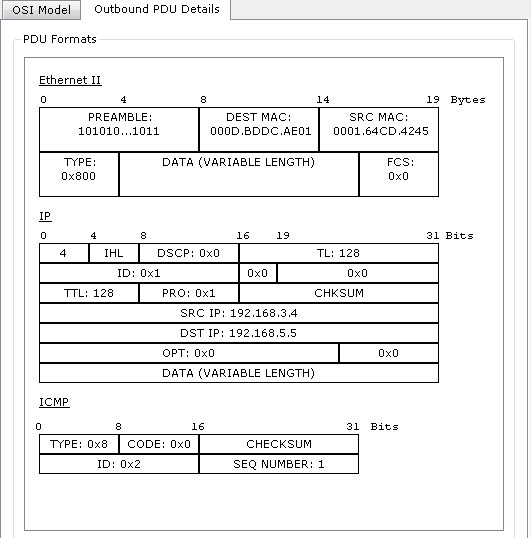


Рис. 4.58 Формат пакета ICMP-эхо-запроса

IP-адрес источника – 192.168.3.4. IP-адрес назначения – 192.168.5.5. Тип ICMP-сообщения – 8 (эхо-запрос).

Когда запрос приходит в сеть назначения, то маршрутизатор определяет МАС-адрес получателя, если такового нет в ARP-таблице маршрутизатора. Таким образом, снова решается задача разрешения локального адреса (рис. 4.59).

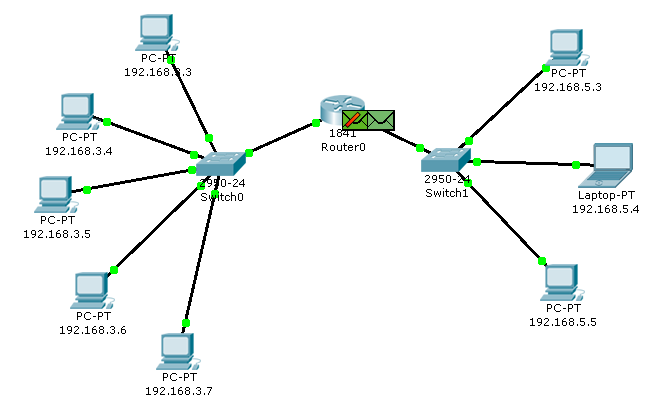


Рис. 4.59 Вид рабочей области

Маршрутизатор вынужден сперва узнать физический адрес получателя, прежде чем он сможет отправить ping-запрос по назначению, поэтому пакет с ping-запросом, пришедший на маршрутизатор, отклонен.

Новый ARP-запрос отправляется широковещательным сообщением от маршрутизатора, содержит его IP-адрес и МАС-адрес (рис. 4.60). IP-адрес назначения – узел 192.168.5.5.

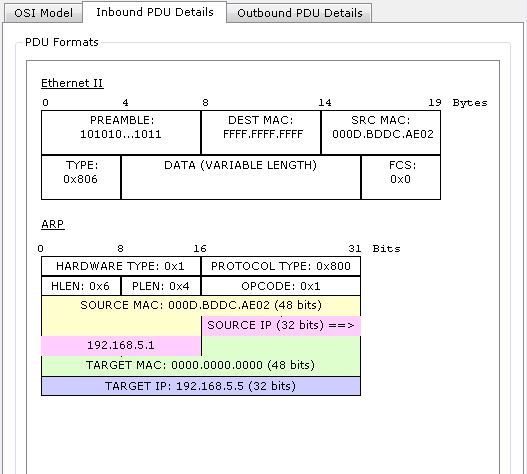


Рис. 4.60 Формат пакета ARP-запроса

Узлы подсети, которым пакет не предназначен, его игнорируют (рис. 4.61).

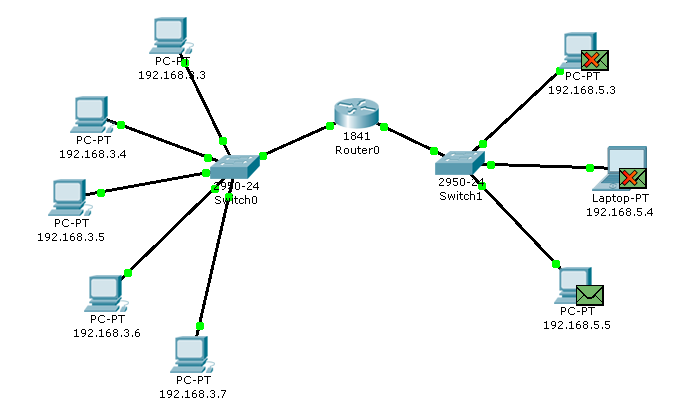


Рис. 4.61 Вид рабочей области

Узел 192.168.5.5. формирует ARP-ответ и отправляет его обратно маршрутизатору (рис. 4.62), указав свой МАС-адрес, о чем свидетельствует содержимое пакета (рис. 4.63).

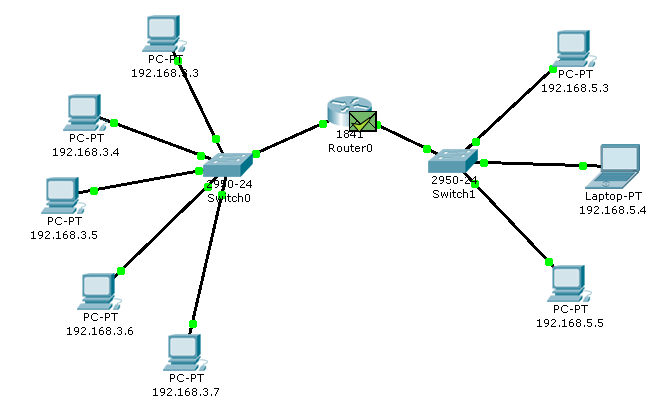


Рис. 4.62 Вид рабочей области

После того, как маршрутизатор определил МАС-адрес получателя входящего ping-запроса, он посылает ICMP-ответ маршрутизатору хоста отправителя. (В данном случае это тот же маршрутизатор Router0).

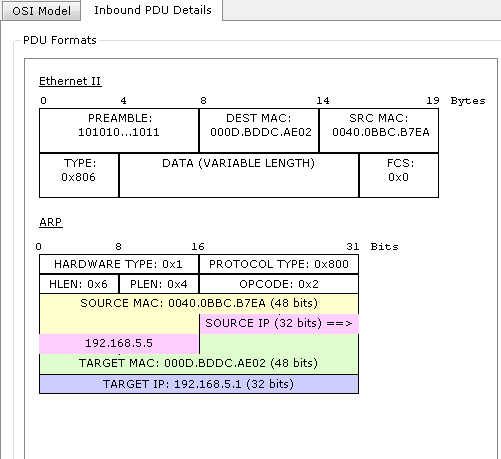


Рис. 4.63 Формат пакета ARP-ответа

Узел 192.168.3.4. снова пытается отправить ping-запрос во внешнюю сеть узлу 192.168.5.5. Его маршрут должен лежать через коммутатор Switch0, маршрутизатор Router0, коммутатор Switch1 и достигнуть узла назначения (рис. 4.64). Проследите маршрут пакета самостоятельно.

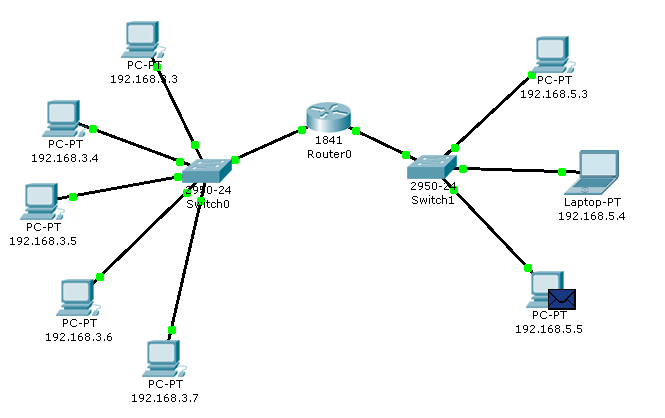


Рис. 4.64 Вид рабочей области

Узел формирует ping-ответ, который отправляется обратно узлу 192.168.3.4 (рис. 4.65).

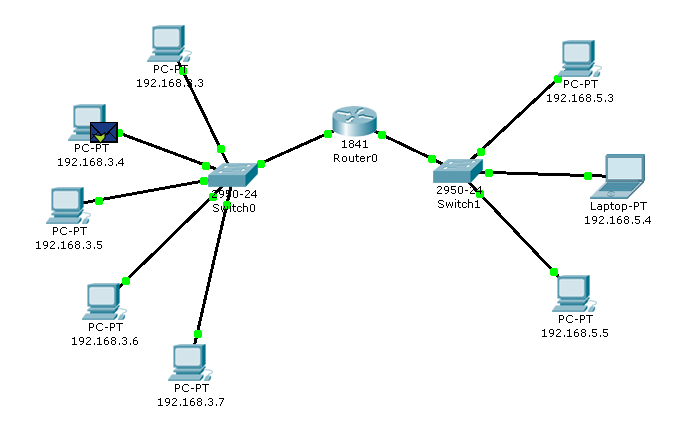


Рис. 4.65 Вид рабочей области

Посмотрите содержимое пакета ping-ответа, пришедшего на хост 192.168.3.4 (рис. 4.66).

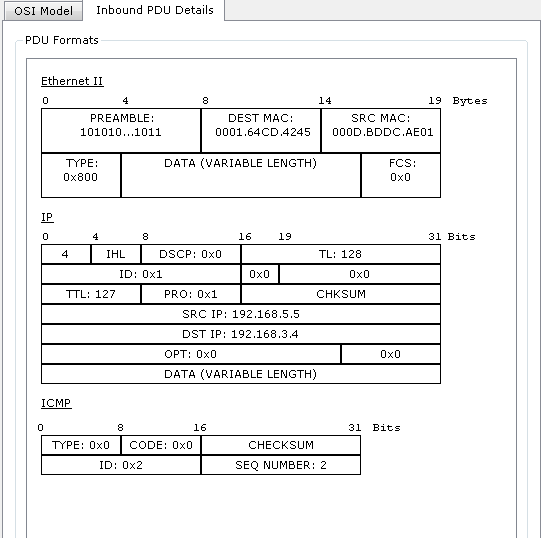


Рис. 4.66 Формат пакета ICMP-эхо-ответа

IP-адрес источника – 192.168.5.5. IP-адрес назначения – 192.168.3.4. Тип ICMP-сообщения – 0 (эхо-ответ).

Посмотрите ping-ответ в командной строке хоста 192.168.3.4 (рис. 4.67).

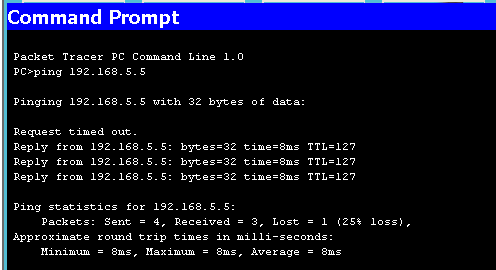


Рис. 4.67 Вывод программы ping

Маршрут пакета можно посмотреть с помощью команды tracert. Выполним эту команду, например, в командной строке компьютера 192.168.3.5 (рис. 4.68):

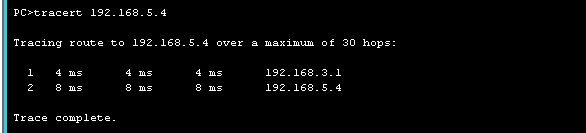


Рис. 4.68 Вывод программы tracert

На пути пакета до хоста 192.168.5.4 один промежуточный маршрутизатор.

1. Посылка ping-запроса на несуществующий хост

Отправим ping-запрос на несуществующий адрес в сеть 192.168.5.0/24.

Откроем программу “Command Promt” на узле 192.168.3.7 и попробуем отправить ping-запрос на несуществующий хост с IP-адресом 192.168.5.6 (рис. 4.69).

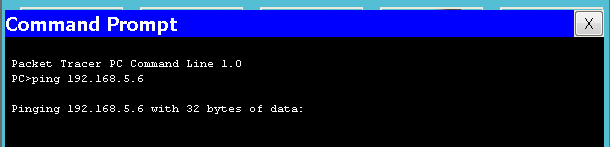


Рис. 4.69 Командная строка узла 192.168.3.7

ARP-таблица на узле-источнике не содержит соответствующей записи о МАС-адресе узла 192.168.5.6, поэтому формируется ARP-запрос (рис. 4.70).

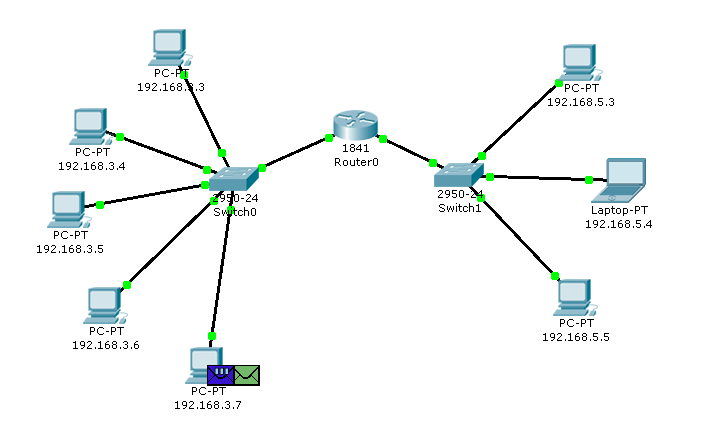


Рис. 4.70 Вид рабочей области

Все узлы игнорируют пакет, кроме маршрутизатора, которому этот пакет предназначался (рис. 4.71).

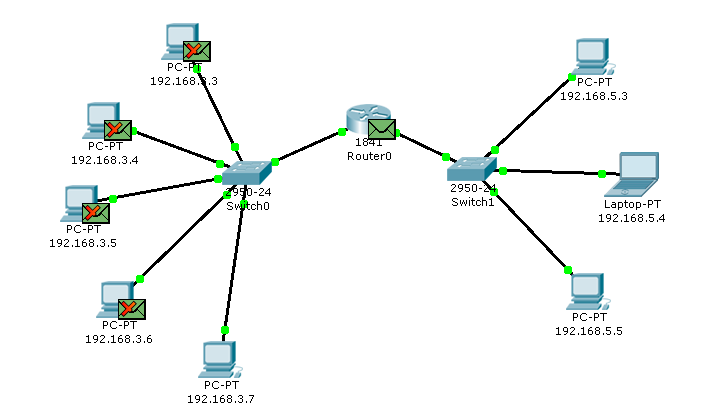


Рис. 4.71 Вид рабочей области

Узел 192.168.3.7 получает ARP-ответ с МАС-адресом маршрутизатора. Теперь, зная его аппаратный адрес, хост отправляет ping-запрос на узел 192.168.5.6 (рис. 4.72).

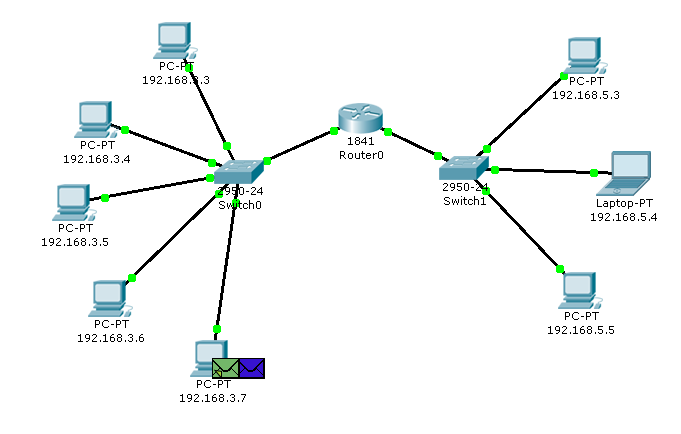


Рис. 4.72 Вид рабочей области

Маршрутизатор пришедший пакет уничтожает, т.к. не может его перенаправить на указанный адрес, потому что соответствующего МАС-адреса он «не знает». В связи с этим маршрутизатор формирует ARP-запрос по адресу 192.168.5.6 (рис. 4.73).

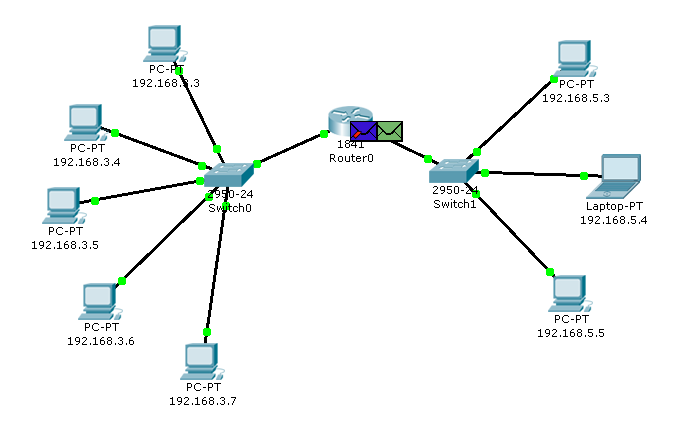
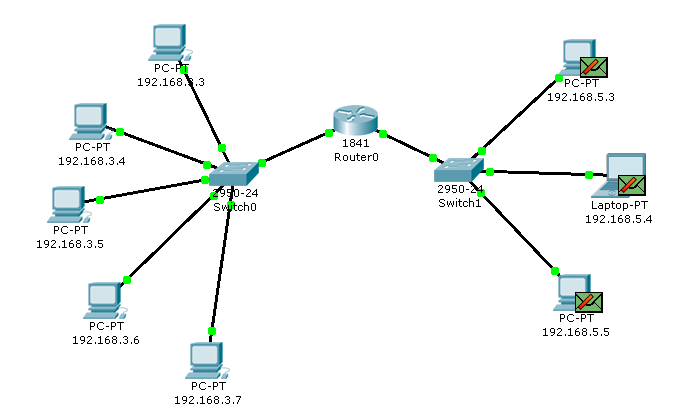


Рис. 4.73 Вид рабочей области

Все узлы подсети игнорируют пакет, потому что IP-адрес в запросе не соответствует их собственным (рис. 4.74). Маршрутизатор ни какого ответа ни от кого не получает.

программный лабоРис. 4.74 Вид рабочей области

Процедура прохождения пакетов повторяется в течение всего сценария симуляции: маршрутизатор по-прежнему «не знает» МАС-адрес указанного в ping-запросе IP-адреса 192.168.5.6 и продолжает рассылать ARP-запросы. Ни один из узлов подсети на эти запросы не реагирует. Не получив ответа, маршрутизатор и сам «молчит», никак не уведомляя об ошибке хост-источник ping-запроса.

Примечание: на самом деле в данном случае маршрутизатору следует отправить ICMP-сообщение «хост недостижим»: сообщение типа 3 с кодом 1. Однако проведенный эксперимент с теорией разошелся.

Посмотрим ответ на ping-запрос в командной строке узла-источника 192.168.3.7: «превышено время ожидания» (рис. 4.75).

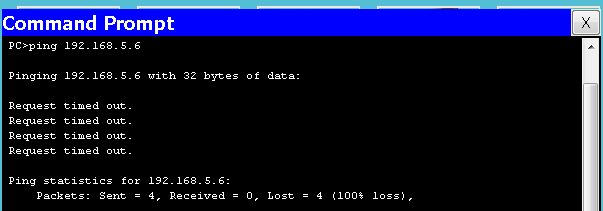


Рис. 4.75 Вывод программы ping

Попробуем отправить ping-запрос, содержащий IP-адрес узла, в сеть, на которую нет маршрута.

Откроем программу “Command Promt” на узле 192.168.3.6 и попробуем отправить ping-запрос на несуществующий хост с IP-адресом 192.168.6.6 (рис. 4.76).

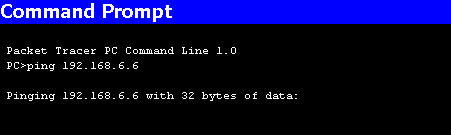


Рис. 4.76 Командная строка узла 192.168.3.6

Так как ARP-таблица узла-источника соответствующей записи не имеет, формируется ARP-запрос на заданный узел с IP-адресом 192.168.6.6 (рис. 4.77).

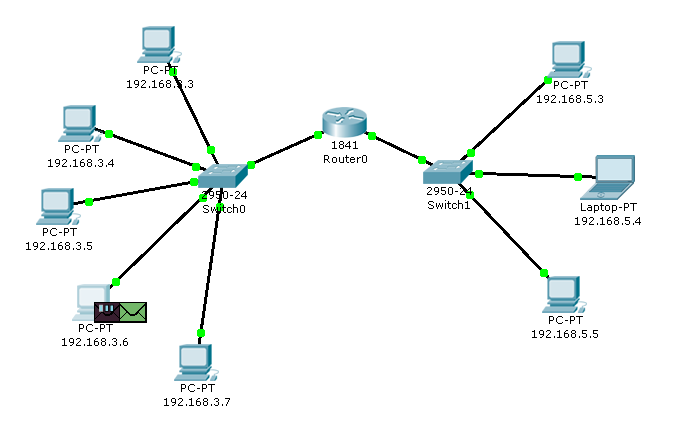


Рис. 4.77 Вид рабочей области

Все узлы игнорируют пакет, кроме маршрутизатора, которому этот пакет предназначался (рис. 4.78).

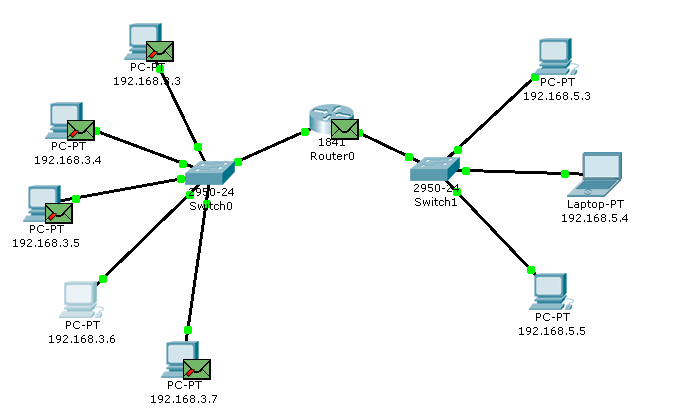


Рис. 4.78 Вид рабочей области

Узел 192.168.3.6 получает ARP-ответ с МАС-адресом маршрутизатора. Теперь, зная его аппаратный адрес, хост отправляет ping-запрос (рис. 4.79).

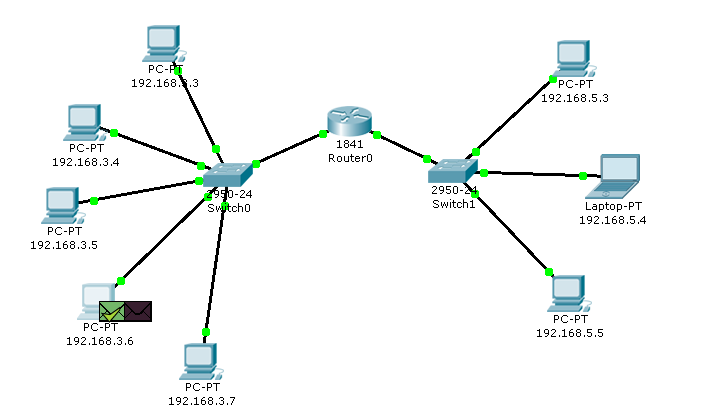


Рис. 4.79 Вид рабочей области

Когда ping-запрос попадает на маршрутизатор, тот не может его перенаправить не на какой из своих интерфейсов, т.к. IP-адреса его интерфейсов не совпадают с тем адресом, который указан в ping-запросе. Соответственно, этот пакет уничтожается и формируется новое ICMP-сообщение (рис. 4.80).

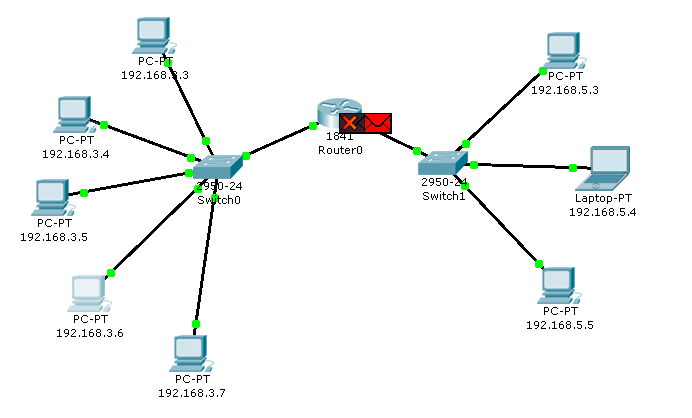


Рис. 4.80 Вид рабочей области

Посмотрим содержимое пакета, сформированного маршрутизатором (рис. 4.81).

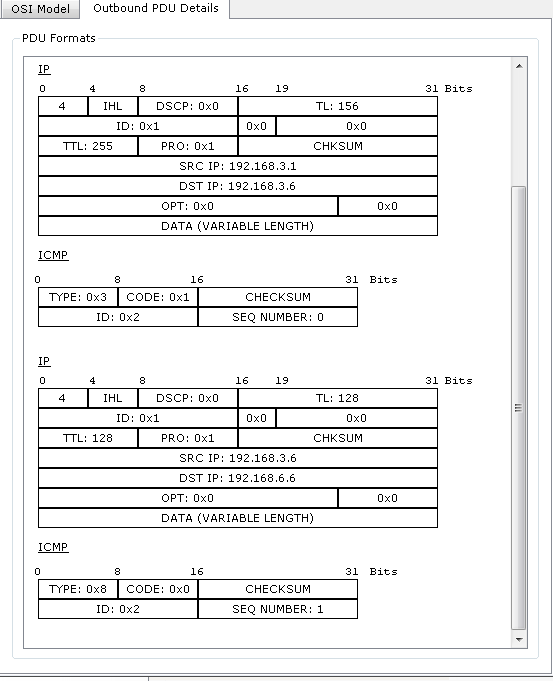


Рис. 4.81 Формат пакета ICMP «хост недостижим»

IP-адрес источника – 192.168.3.1. IP-адрес назначения – 192.168.3.6. Тип ICMP-сообщения – 3 с кодом 1, что означает «хост недостижим». Этот пакет приходит на узел 192.168.3.6.

Результат ping-запроса в командной строке узла 192.168.3.6: «хост назначения недостижим» (рис. 4.82).

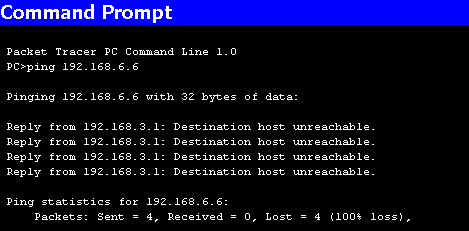


Рис. 4.82 Вывод программы ping

Таким образом, маршрутизатор «ответил» на ping-запрос, для которого у него не было соответствующего маршрута, новым ICMP-сообщением «хост недостижим».

Примечание: корректно ли отреагировал маршрутизатор в данной ситуации, отправив на хост-источник ping-запроса ICMP-сообщение «хост недостижим»? Чтобы ответить на этот вопрос, необходимо обратиться к спецификации протокола ICMP RFC 792 и ознакомится с другими типами ICMP-сообщений. [Электронный ресурс]. URL: <http://tools.ietf.org/html/rfc792>.

## **Индивидуальное задание**

1. **Формирование IP-адреса**

В рамках практической работы каждому студенту необходимо самостоятельно сформировать IP-адрес для своих компьютеров. Адрес должен соответствовать следующим правилам:

1. Первый байт всегда **192 для первой подсети** и **191 для второй подсети**.
2. Второй байт – это первые три цифры вашего студенческого ID.
3. Третий байт – это вторые три цифры вашего студенческого ID.
4. Четвертый байт – это номер вашего компьютера в локальной сети (произвольно выбирается студентом в пределах допустимого диапазона).

Пример:

Допустим, у студента ID 654321, а компьютер имеет номер 15. Тогда IP-адрес будет: 192.654.321.15

1. **Практическое задание**

В рамках практической работы необходимо выполнить **два варианта ping-запроса**:

1. **Внутри сети** – отправить ICMP-запрос на IP-адрес другого компьютера внутри локальной подсети.
2. **Во внешнюю сеть** – отправить ICMP-запрос во вторую подсеть.

**Нужно провести пошаговую симуляцию и уметь объяснить каждый шаг (движение) пакета.**

Дополнительно с помощью **команды tracert** необходимо определить маршрут пакета, отправленного во внешнюю сеть.