

Лабораторная работа №4. Проектирование сети малого предприятия и крупной корпоративной сети в Cisco Packet Tracer.

Цель работы: изучить режим реального времени, основные операции с устройствами. Спроектировать корпоративную сеть в Cisco Packet Tracer.

Теоретические сведения:

Данный программный продукт разработан компанией Cisco и рекомендован использоваться при изучении телекоммуникационных сетей и сетевого оборудования. На основе программного продукта Packet Tracer есть возможность создавать сетевые топологии из широкого множества маршрутизаторов и коммутаторов компании Cisco, рабочих станций и сетевых соединений типа Ethernet, Serial, ISDN, Frame Relay. Функции симулятора могут быть пригодны как для обучения, так и для работы, настройки сети еще на этапе планирования.

Packet Tracer включает следующие особенности:

- Рабочее пространство для создания сети любого размера и сложности
- Моделирование в режиме реального времени
- Моделирование в режиме симуляции
- Графический интерфейс для взаимодействия с пользователем при настройке сетевых устройств
- Изображение сетевого оборудования с поддержкой добавления, удаления, перемещения различных компонентов

Данный симулятор позволяет студентам проектировать свои собственные сети, создавая и отправляя различные пакеты данных, сохранять и комментировать свою работу. Предоставляется возможность изучать и использовать такие сетевые устройства, как коммутаторы, маршрутизаторы, рабочие станции, определять типы связей между ними и соединять их. Отличительной особенностью данного симулятора является наличие в нем режима симуляции. В данном режиме все пакеты, пересылаемые внутри сети, отображаются графически. Эта возможность позволяет студентам наглядно продемонстрировать, по какому интерфейсу в данный момент перемещается пакет, какой протокол используется и т. д. Работая в симуляторе в другом режиме, режиме реального времени, нельзя проследить за перемещением пакетов, сразу отображается конечный результат выполненных действий. Packet Tracer является удобным средством моделирования сетей передачи данных. Работа с симулятором дает весьма правдоподобное ощущение настройки реальной сети, состоящей из различных устройств. Настройку сетевого оборудования можно проводить как с помощью команд операционной системы Cisco IOS, так и посредством графического интерфейса. Благодаря режиму симуляции можно проследить перемещение данных по сети, появление и изменение параметров пакетов при прохождении данных через сетевые устройства, скорость и пути перемещения пакетов. Анализ событий, происходящих в сети, позволяет понять механизм ее работы и обнаружить неисправности.

В рамках лабораторного практикума изучаются построение топологии сети, проверка ее работоспособности посредством ICMP-сообщений, протокол разрешения адреса, прикладные протоколы электронной почты, вопросы содержимого пакетов заданного протокола. Работы выполняются с помощью симулятора Cisco Packet Tracer,

необходимое программное обеспечение установлено на компьютеры в лаборатории. Все лабораторные работы содержат необходимые теоретические сведения, общую часть работы, обязательную для выполнения, и индивидуальные задания.

В содержании лабораторных работ при настройке сетевых устройств есть упоминание о службе DNS. В первых двух работах служба DNS непосредственно не участвует, а значит, присваивать IP-адрес DNS-серверу необязательно.

Выполнение работы:

1. Построение топологии сети

В конце вводной лабораторной работы мы создали следующую топологию сети, состоящую из конечных узлов (PC), коммутаторов и маршрутизатора (рис. 4.1):

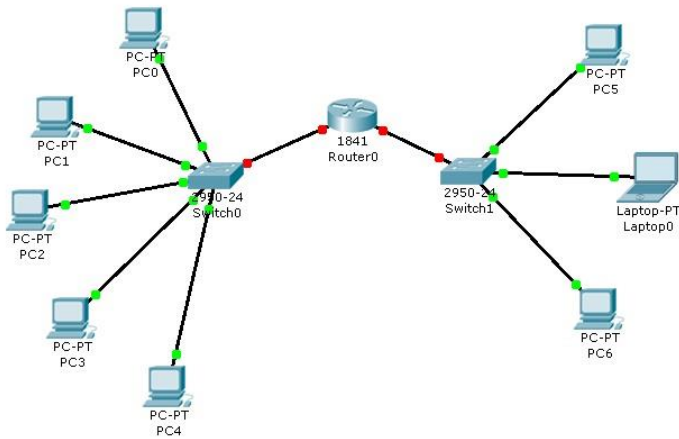


Рис. 4.1 Тестовая топология сети

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

2. 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. 4.2):

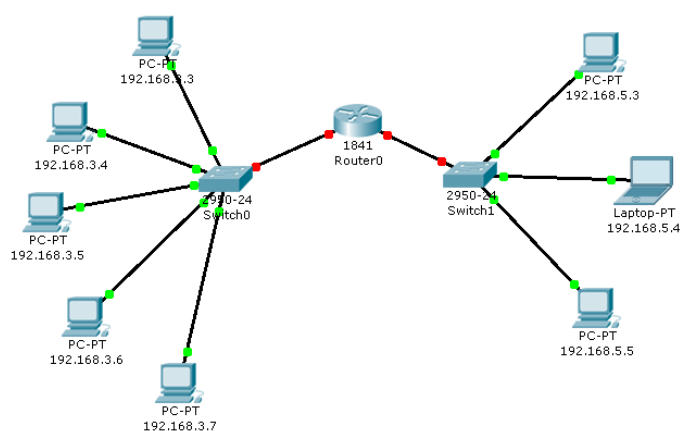


Рис. 4.2 Вид рабочей области

3. 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. 4.3).

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

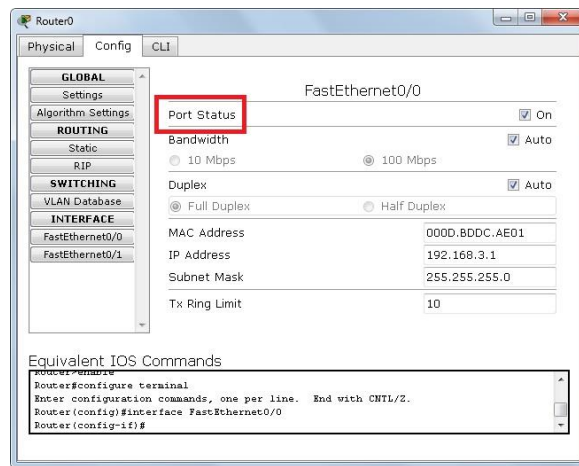


Рис. 4.3 Настройка интерфейса маршрутизатора

4) Закрываем окно, смотрим на всю топологию сети. Зеленые индикаторы состояния на линии связи между Router0 и Switch0 сигнализируют, что интерфейс подключен правильно (рис. 4.4).

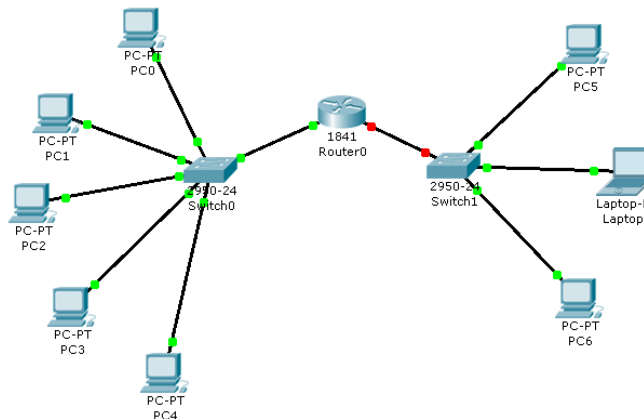


Рис. 4.4 Вид рабочей области

Аналогично производим настройку интерфейса FastEthernet0/1 (рис. 4.5).

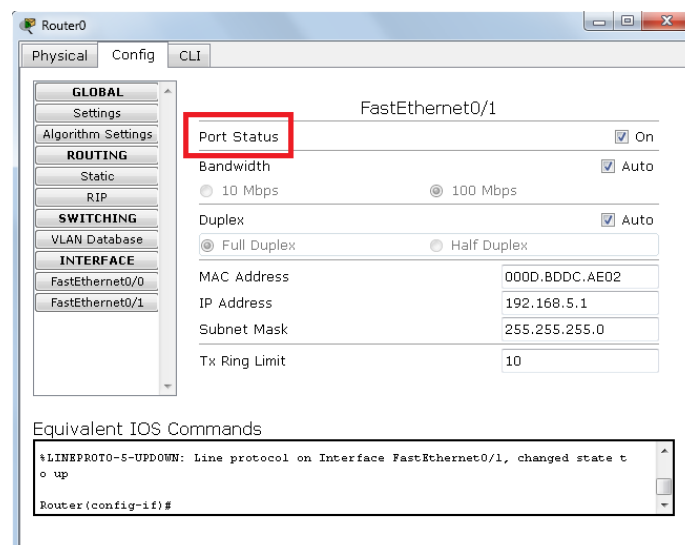




Рис. 4.5 Настройка интерфейса маршрутизатора

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.

4. 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. 

Откроется окно событий, в котором вы увидите список событий, управляющие кнопки, заданные фильтры (рис. 4.6). 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

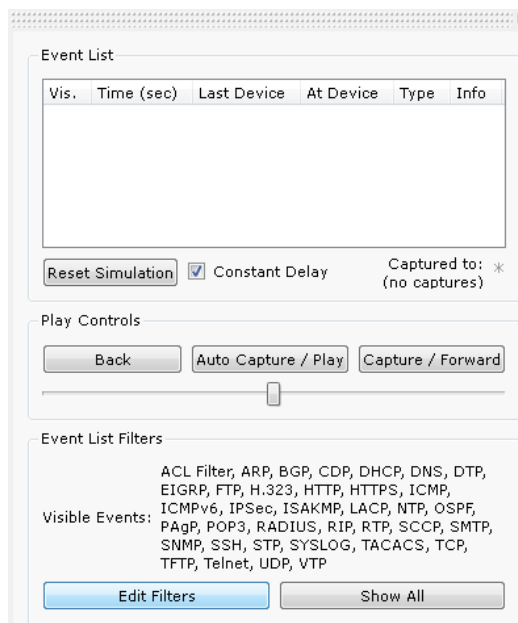


Рис. 4.6 Окно событий режима симуляции

В данной лабораторной работе нас интересуют пакеты двух типов ARP и ICMP. Следовательно, нужно поставить фильтр только на сообщения заданного типа (рис. 4.7):

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

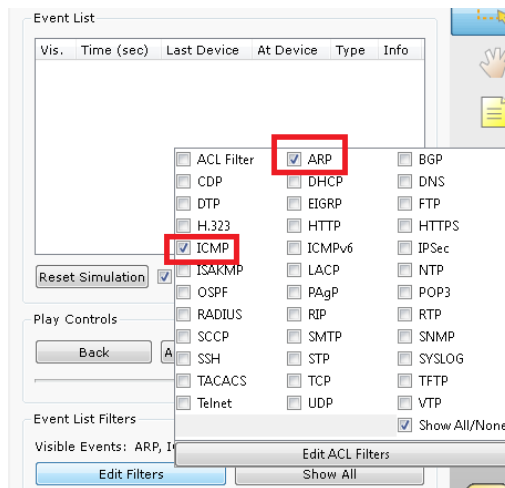


Рис. 4.7 Добавление фильтров на протоколы ARP и ICMP

4) Убедимся, что заданные протоколы для фильтрации назначены (рис. 4.8)

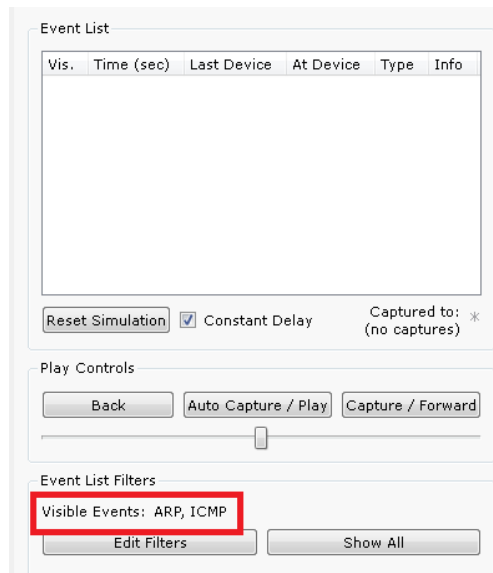


Рис. 4.8 Окно событий режима симуляции

5. Проверка работы сети в режиме симуляции

Отправим тестовый ping-запрос с конечного узла с 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. 4.9)

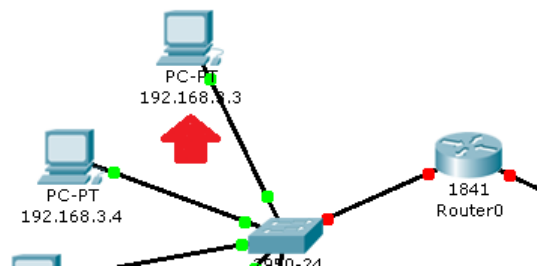


Рис. 4.9 Выбор узла 192.168.3.3

- 2) Выбираем вкладку Desktop, в которой содержатся симуляторы некоторых программ, доступных на компьютере.
- 3) Выбираем “Command Prompt”, программу, имитирующую командную строку компьютера.
- 4) С помощью утилиты ping отправляем ping-запрос (рис. 4.10). (Не забудьте нажать Enter).

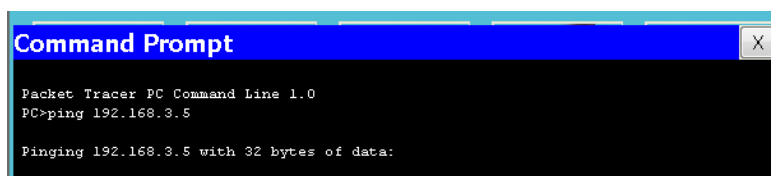


Рис. 4.10 Командная строка узла 192.168.3.3

На устройстве-источнике формируются два пакета протокола ARP и ICMP (рис. 4.11). ARP-запрос возникает всегда, когда хост пытается связаться с другим хостом.

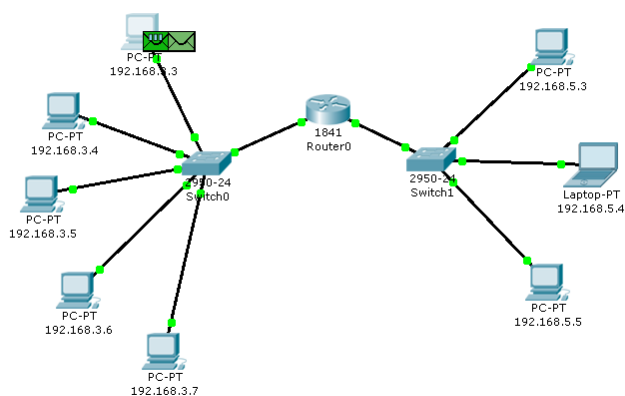


Рис. 4.11 Вид рабочей области

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. 4.12).

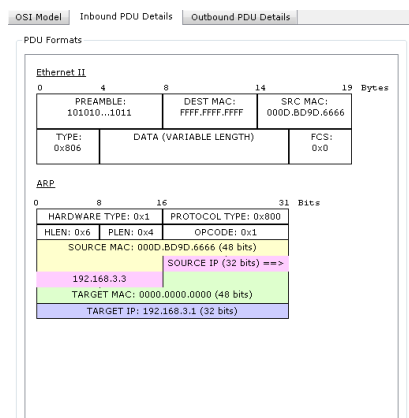


Рис. 4.12 Формат пакета ARP-запроса

Узел 192.168.3.3 построил запрос и посылает его широковещательным сообщением всем хостам подсети. Помимо IP-адреса назначения, запрос содержит IP-адрес и MAC-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. 4.13).

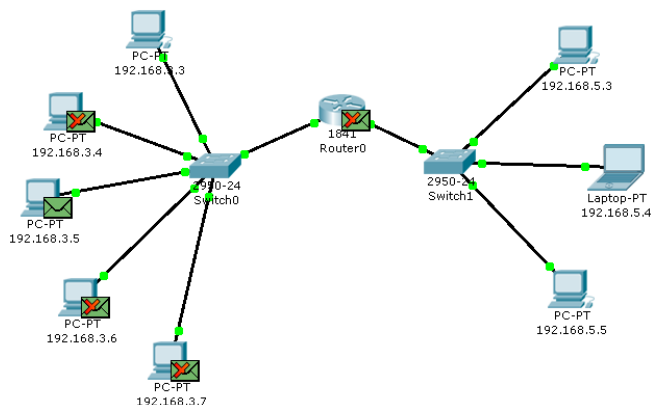


Рис. 4.13 Вид рабочей области

Посмотрите содержимое пакета ARP-ответа, пришедшего на хост 192.168.3.3 (рис. 4.14).

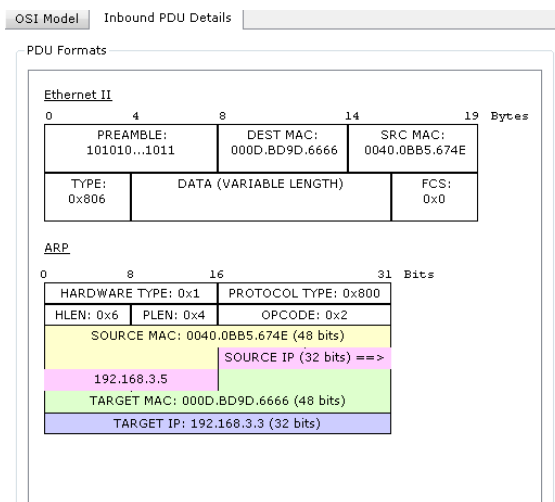


Рис. 4.14 Формат пакета ARP-ответа

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

Далее отправляется ICMP-сообщение ping-запроса. Посмотрите содержимое пакета, сделав клик по пакету (конверту) (рис. 4.15).

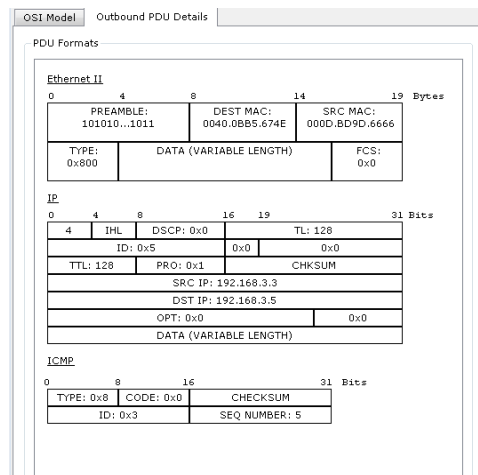


Рис. 4.15 Формат пакета ICMP-эхо-запроса

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. 4.16).

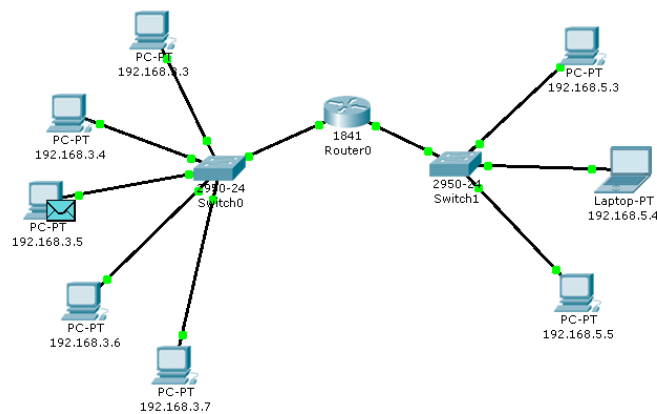


Рис. 4.16 Вид рабочей области

Посмотрите содержимое пакета ring-ответа, пришедшего на хост 192.168.3.3 (рис. 4.17).

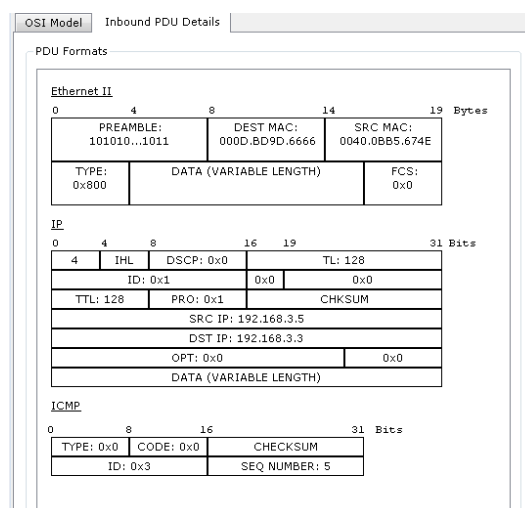


Рис. 4.17 Формат пакета ICMP-эхо-ответа

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. 4.18).

```
PC>ping 192.168.3.5

Pinging 192.168.3.5 with 32 bytes of data:

Reply from 192.168.3.5: bytes=32 time=8ms TTL=128
Reply from 192.168.3.5: bytes=32 time=4ms TTL=128
Reply from 192.168.3.5: bytes=32 time=4ms TTL=128
Reply from 192.168.3.5: bytes=32 time=4ms TTL=128

Ping statistics for 192.168.3.5:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 4ms, Maximum = 8ms, Average = 5ms
```

Рис. 4.18 Вывод программы ping

В окне событий так же указаны маршруты запроса ARP и ICMP: через какие устройства прошли пакеты (рис. 4.19).

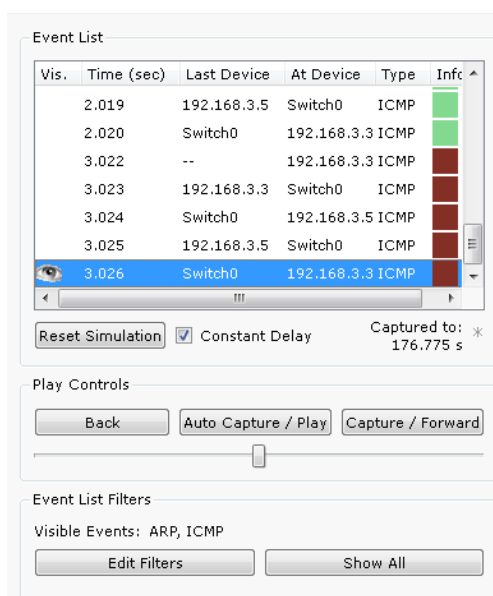


Рис. 4.19 Окно событий режима симуляции

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.

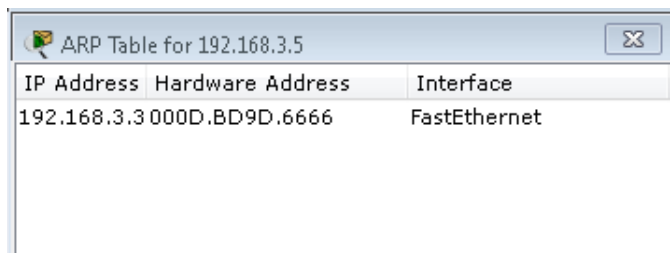
Содержимое ARP-таблицы узла 192.168.3.3 (рис. 4.20):

```
PC>arp -a

Internet Address      Physical Address      Type
192.168.3.1          000d.bddc.ae01       dynamic
192.168.3.5          0040.0bb5.674e       dynamic
```

Рис. 4.20 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. 4.21).



IP Address	Hardware Address	Interface
192.168.3.3	000D.BD9D.6666	FastEthernet

Рис. 4.21 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”.

6. Посылка ping-запроса во внешнюю сеть

Отправим тестовый ping-запрос с конечного узла с 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 отправки ARP-запроса внутри локальной сети. Протокол ARP в этом случае определял непосредственно MAC-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 MAC-адреса маршрутизатора. Таким образом, пакет будет передан маршрутизатору для дальнейшей ретрансляции. Открываем “Command Prompt”, имитирующую командную строку, на компьютере 192.168.3.4 и посылаем на хост 192.168.5.5. ping-запрос (рис. 4.22).

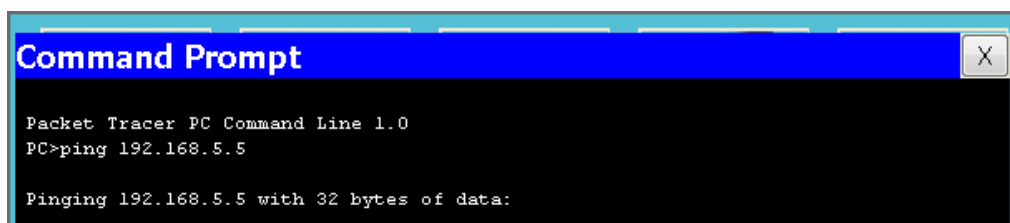


Рис. 4.22 Командная строка узла 192.168.3.4

В этом случае инициируется ARP-запрос маршрутизатору, который пересылает пакеты в сеть назначения. На узле-источнике формируются два пакета протокола ARP и ICMP (рис. 4.23).

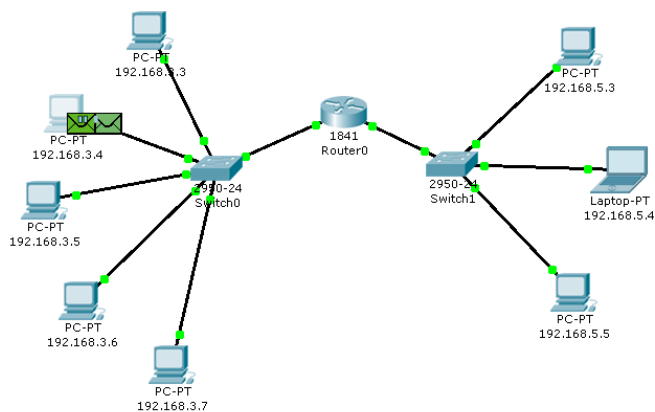


Рис. 4.23 Вид рабочей области

Формат пакета ARP-запроса содержит те же сведения, что и для разрешения локального адреса устройства, и рассылается широковещательно всем узлам подсети (рис. 4.24).

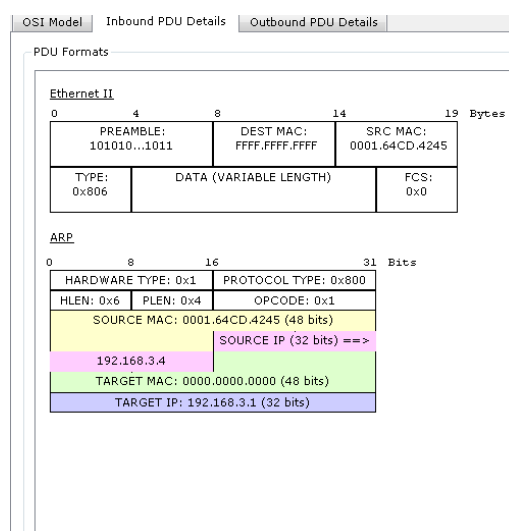


Рис. 4.24 Формат пакета ARP-запроса

Все узлы игнорируют пакет, кроме маршрутизатора, которому этот пакет предназначался (рис. 4.25).

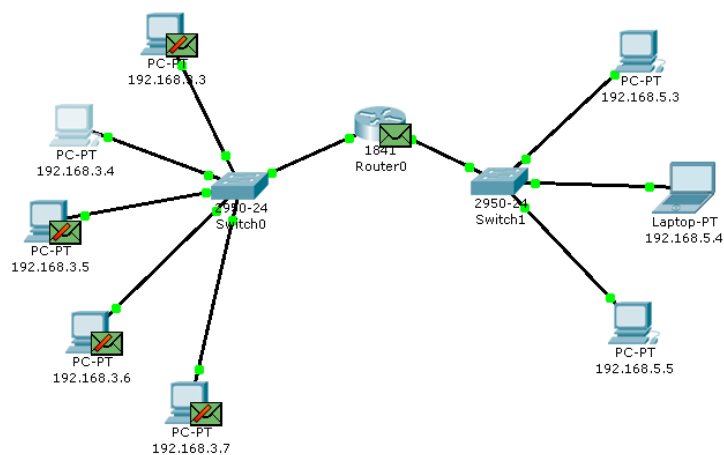


Рис. 4.25 Вид рабочей области

Маршрутизатор формирует ARP-ответ, указывая свой физический адрес, и отправляет его узлу 192.168.3.4 (рис. 4.26).

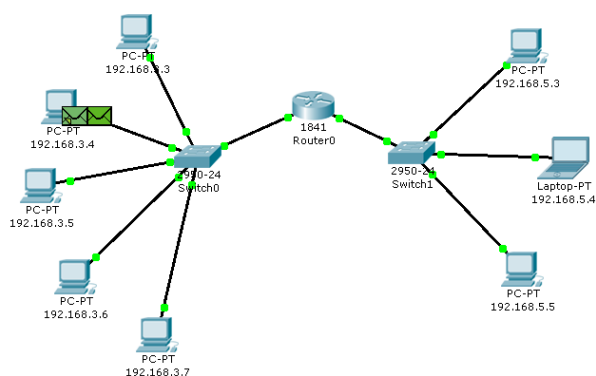


Рис. 4.27 Вид рабочей области

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. 4.28).

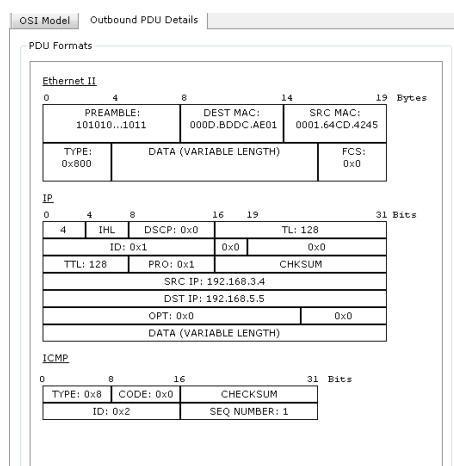


Рис. 4.28 Формат пакета ICMP-эхо-запроса

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 MAC-адрес получателя, если такового нет в ARP-таблице маршрутизатора. Таким образом, снова решается задача разрешения локального адреса (рис. 4.29).

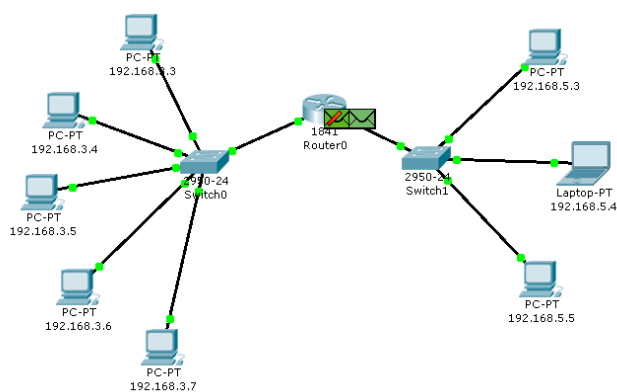


Рис. 4.29 Вид рабочей области

Маршрутизатор вынужден сперва узнать физический адрес получателя, прежде чем он сможет отправить ring-запрос по назначению, поэтому пакет с ring-запросом, пришедший на маршрутизатор, отклонен. Новый ARP-запрос отправляется широковещательным сообщением от маршрутизатора, содержит его IP-адрес и MAC-адрес (рис. 4.30). IP-адрес назначения – узел 192.168.5.5.

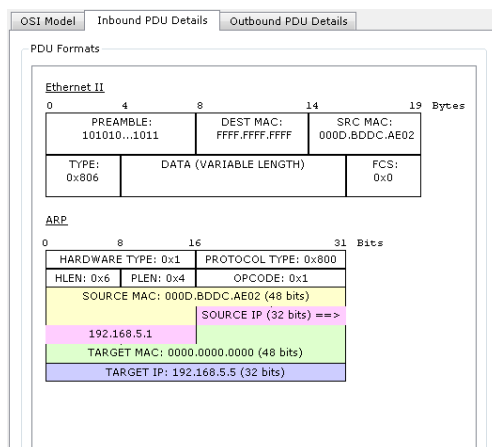


Рис. 4.30 Формат пакета ARP-запроса

Узлы подсети, которым пакет не предназначен, его игнорируют (рис. 4.31).

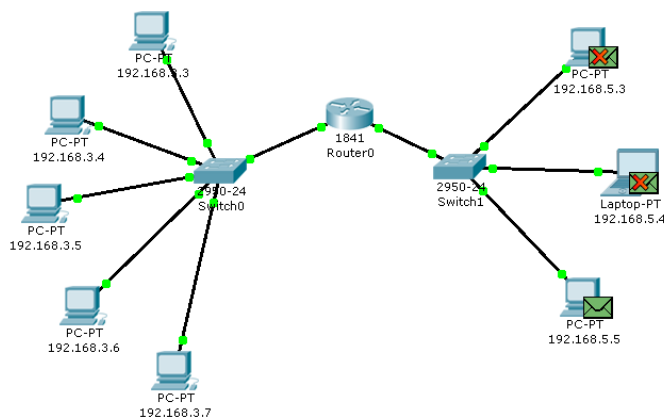


Рис. 4.31 Вид рабочей области

Узел 192.168.5.5. формирует ARP-ответ и отправляет его обратно маршрутизатору (рис. 4.32), указав свой MAC-адрес, о чем свидетельствует содержимое пакета (рис. 4.32).

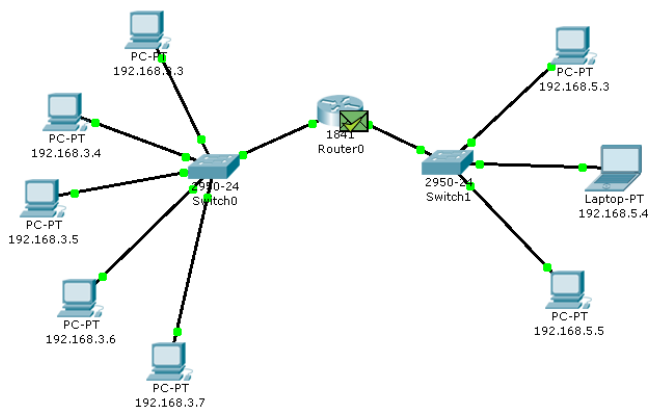


Рис. 4.32 Вид рабочей области

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

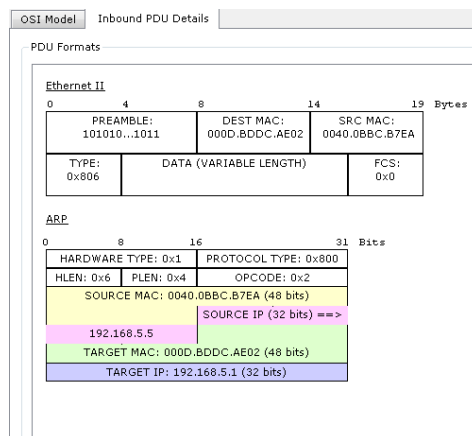


Рис. 4.32 Формат пакета ARP-ответа

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. 4.33). Проследите маршрут пакета самостоятельно.

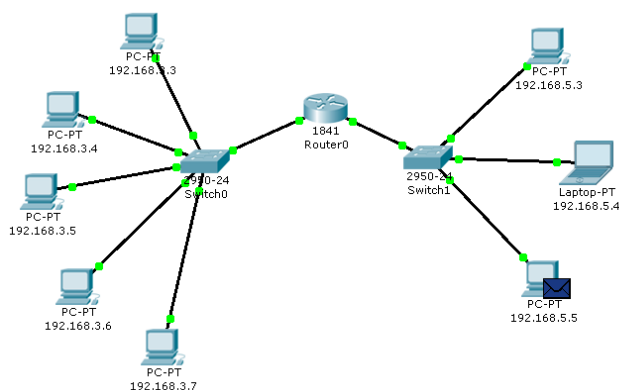


Рис. 4.33 Вид рабочей области

Узел формирует ping-ответ, который отправляется обратно узлу 192.168.3.4 (рис. 4.34).

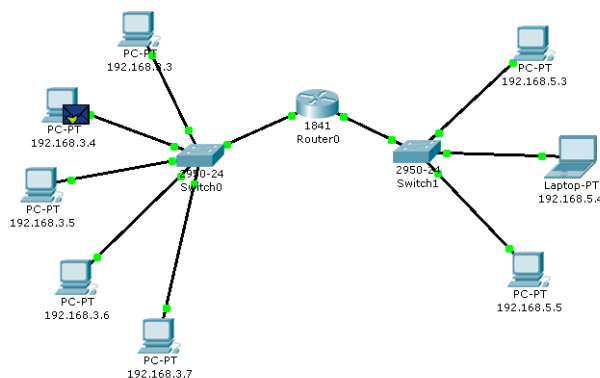


Рис. 4.34 Вид рабочей области

Посмотрите содержимое пакета ping-ответа, пришедшего на хост 192.168.3.4 (рис. 4.35).

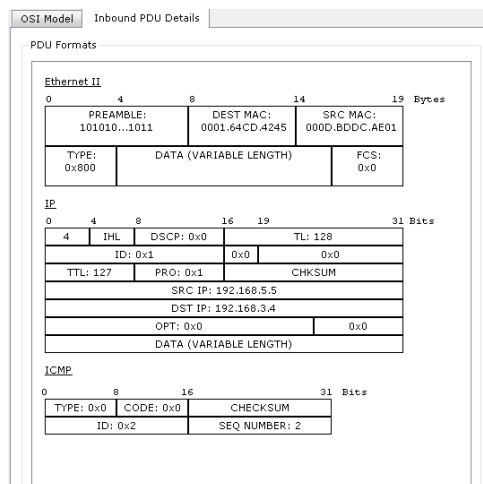


Рис. 4.35 Формат пакета ICMP-эхо-ответа

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. 4.36).

```

Command Prompt

Packet Tracer PC Command Line 1.0
PC>ping 192.168.5.5

Pinging 192.168.5.5 with 32 bytes of data:

Request timed out.
Reply from 192.168.5.5: bytes=32 time=8ms TTL=127
Reply from 192.168.5.5: bytes=32 time=8ms TTL=127
Reply from 192.168.5.5: bytes=32 time=8ms TTL=127

Ping statistics for 192.168.5.5:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 8ms, Maximum = 8ms, Average = 8ms
  
```

Рис. 4.36 Вывод программы ping

Маршрут пакета можно посмотреть с помощью команды tracert. Выполним эту команду, например, в командной строке компьютера 192.168.3.5 (рис. 4.37):

```

PC>tracert 192.168.5.4

Tracing route to 192.168.5.4 over a maximum of 30 hops:

  1  4 ms      4 ms      4 ms      192.168.3.1
  2  8 ms      8 ms      8 ms      192.168.5.4

Trace complete.
  
```

Рис. 4.37 Вывод программы tracert

На пути пакета до хоста 192.168.5.4 один промежуточный маршрутизатор.

7. 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. 4.38).

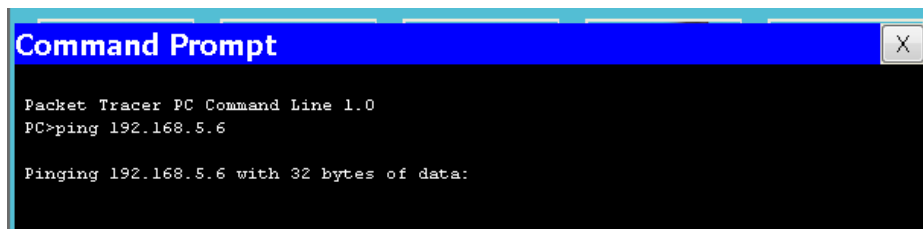


Рис. 4.38 Командная строка узла 192.168.3.7

ARP-таблица на узле-источнике не содержит соответствующей записи о MAC-адресе узла 192.168.5.6, поэтому формируется ARP-запрос (рис. 4.39).

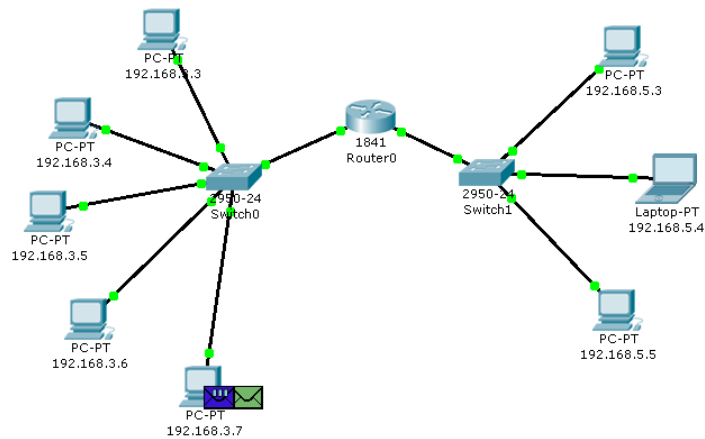


Рис. 4.39 Вид рабочей области

Все узлы игнорируют пакет, кроме маршрутизатора, которому этот пакет предназначен (рис. 4.40).

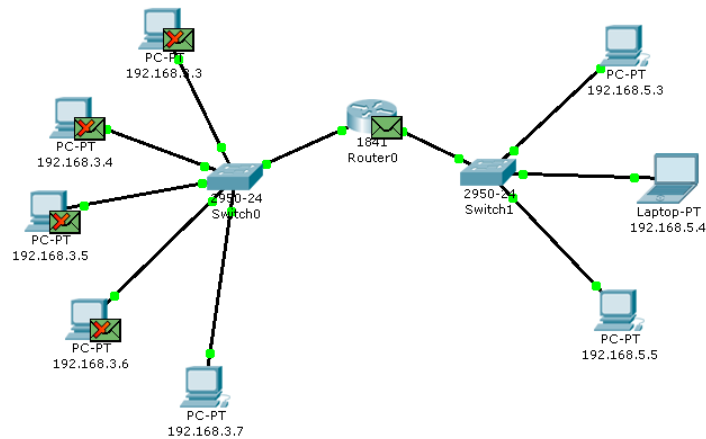


Рис. 4.40 Вид рабочей области

Узел 192.168.3.7 получает ARP-ответ с MAC-адресом маршрутизатора. Теперь, зная его аппаратный адрес, хост отправляет ping-запрос на узел 192.168.5.6 (рис. 4.41).

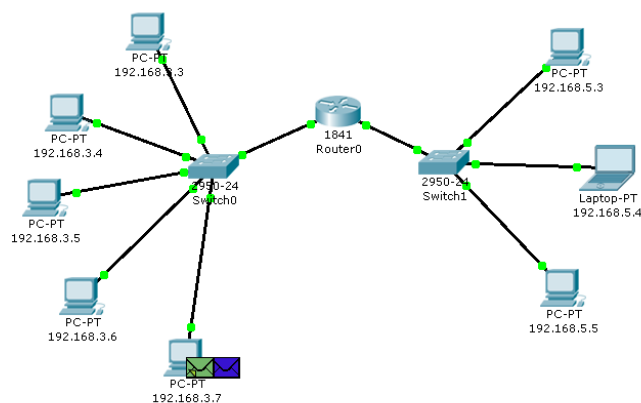


Рис. 4.41 Вид рабочей области

Маршрутизатор пришедший пакет уничтожает, т.к. не может его перенаправить на указанный адрес, потому что соответствующего MAC-адреса он «не знает». В связи с этим маршрутизатор формирует ARP-запрос по адресу 192.168.5.6 (рис. 4.42).

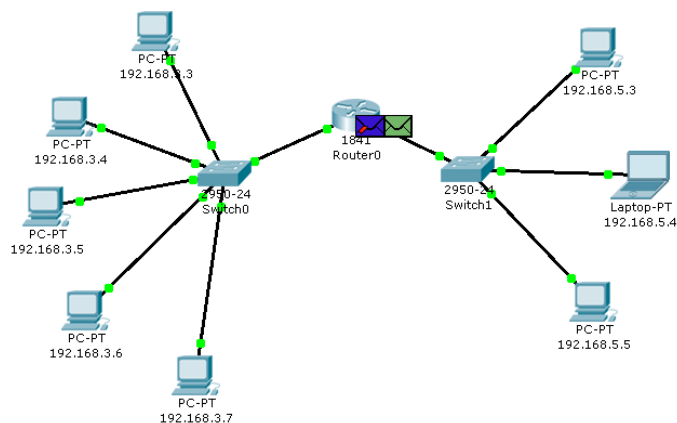


Рис. 4.42 Вид рабочей области

Все узлы подсети игнорируют пакет, потому что IP-адрес в запросе не соответствует их собственным (рис. 4.43). Маршрутизатор никакого ответа ни от кого не получает.

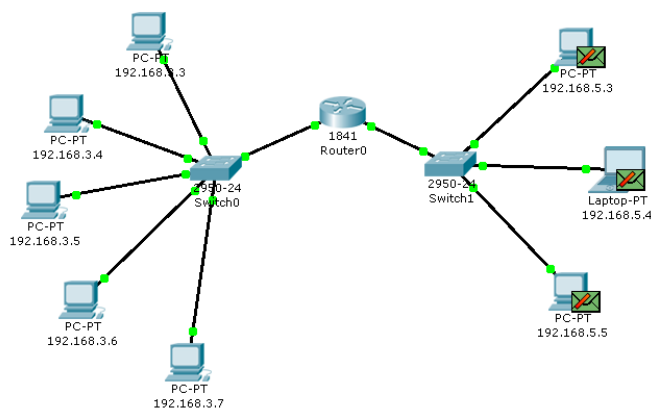
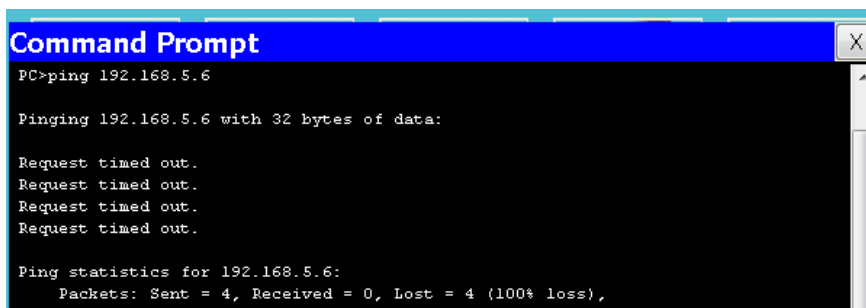


Рис. 4.43 Вид рабочей области

Процедура прохождения пакетов повторяется в течение всего сценария симуляции:

маршрутизатор по-прежнему «не знает» MAC-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. 4.44).



```
Command Prompt
PC>ping 192.168.5.6

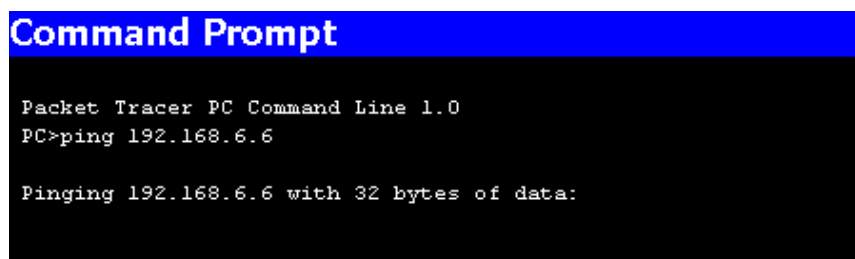
Pinging 192.168.5.6 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.5.6:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Рис. 4.44 Вывод программы ping

Попробуем отправить ping-запрос, содержащий IP-адрес узла, в сеть, на которую нет маршрута. Откроем программу “Command Prompt” на узле 192.168.3.6 и попробуем отправить ping-запрос на несуществующий хост с IP-адресом 192.168.6.6 (рис. 4.45).



```
Command Prompt
Packet Tracer PC Command Line 1.0
PC>ping 192.168.6.6

Pinging 192.168.6.6 with 32 bytes of data:
```

Рис. 4.45 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. 4.46).

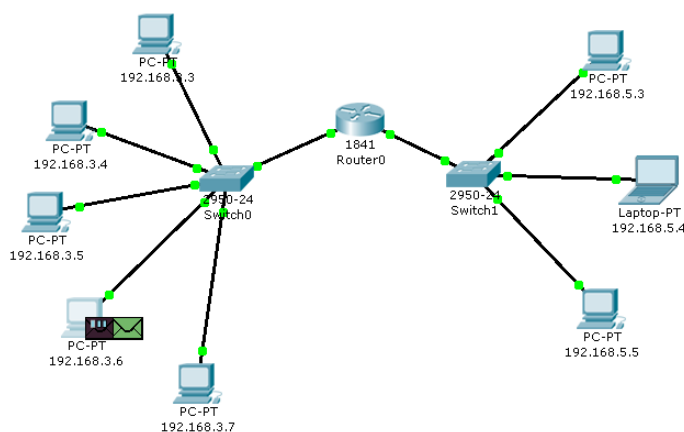


Рис. 4.46 Вид рабочей области

Все узлы игнорируют пакет, кроме маршрутизатора, которому этот пакет предназначался

(рис. 4.47).

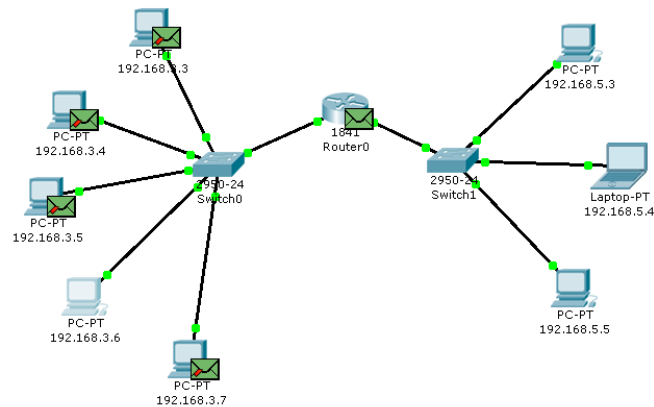


Рис. 4.47 Вид рабочей области

Узел 192.168.3.6 получает ARP-ответ с MAC-адресом маршрутизатора. Теперь, зная его аппаратный адрес, хост отправляет ping-запрос (рис. 4.48).

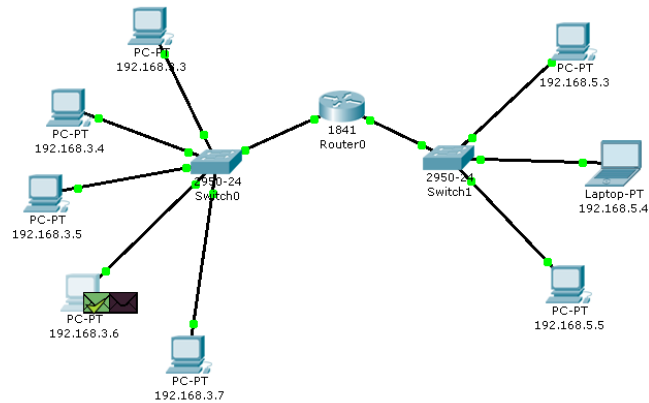


Рис. 4.48 Вид рабочей области

Когда ping-запрос попадает на маршрутизатор, тот не может его перенаправить 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. 4.49).

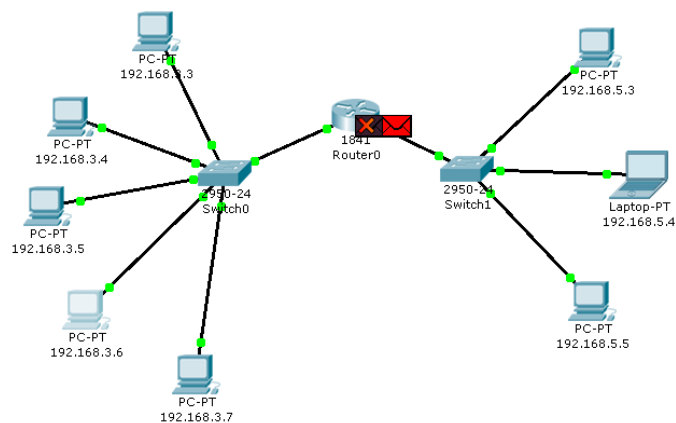


Рис. 4.49 Вид рабочей области

Посмотрим содержимое пакета, сформированного маршрутизатором (рис. 4.50).

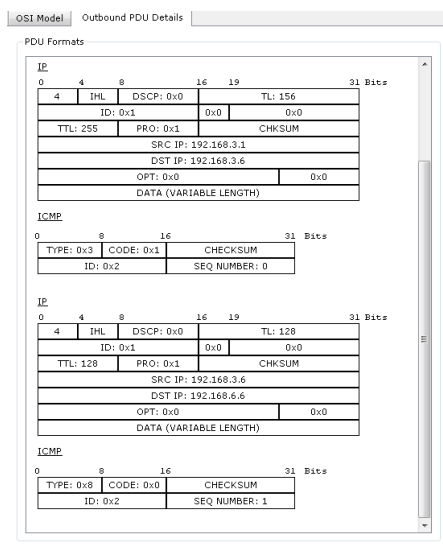


Рис. 4.50 Формат пакета ICMP «хост недостижим»

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. 4.51).

```

Command Prompt

Packet Tracer PC Command Line 1.0
PC>ping 192.168.6.6

Pinging 192.168.6.6 with 32 bytes of data:

Reply from 192.168.3.1: Destination host unreachable.
Reply from 192.168.3.1: Destination host unreachable.
Reply from 192.168.3.1: Destination host unreachable.
Reply from 192.168.3.1: Destination host unreachable.

Ping statistics for 192.168.6.6:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
  
```

Рис. 4.51 Вывод программы ping

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

Индивидуальное задание.

1. На примере построения топологии сети, самостоятельно спроектировать сеть малого предприятия или крупной корпоративной сети в Cisco Packet Tracer;
2. Дать полное описание каждого выбранного элемента, количества, их взаимосвязь и процесса работы (в виде табличных данных);
3. Настройка конечных узлов;
4. Настройка маршрутизатора;
5. Проверка работы сети в режиме симуляции;
6. Посылка ping-запроса внутри сети;

7. Посылка ping-запроса во внешнюю сеть;
8. Посылка ping-запроса на несуществующий IP-адрес узла.

Требования к лабораторной работе:

1. Изучить материал согласно указанной темы работы;
2. Составить подробный отчет с каждым проделанным шагом (скриншоты Cisco Packet Tracer) и описать их;
3. Структура отчета. Титульный лист, цель работы, теоретическая часть, практическая часть, вывод;
4. Защита отчета.

Контрольные вопросы:

1. Топологии сети и ее виды;
2. Описать настройку маршрутизатора в Cisco Packet Tracer;
3. Конечный узел сети – это ... ;
4. Что показывает ping?