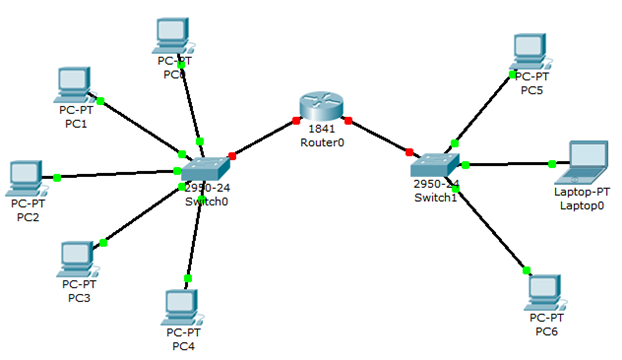
*8. Построение топологии сети, состоящей из двух подсетей*

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):



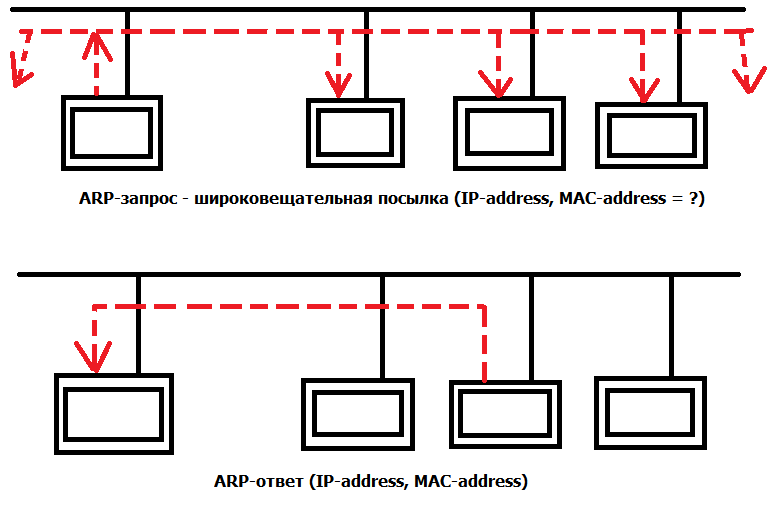
*Рис. 4.24. Топология сети для лабораторной работы №2*

Для построения 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.

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.*

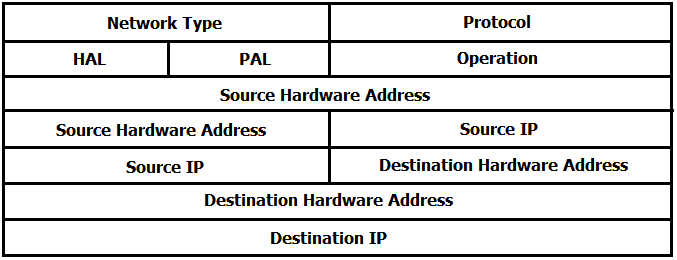
В ARP-таблице могут содержаться как статические, так и динамические за­писи. Динамические записи добавляются и удаляются автоматически, статиче­ские заносятся вручную.

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

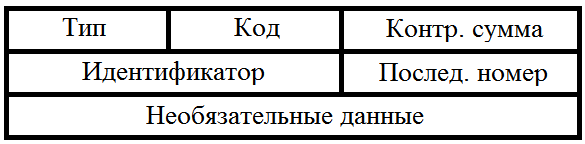
· HAL - длина канального адреса

· 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.

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

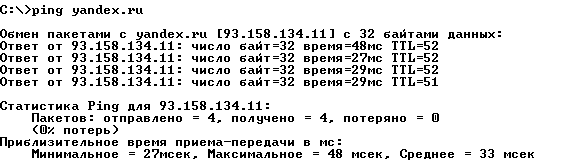
· Последовательный номер – номер пакета в потоке

[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*

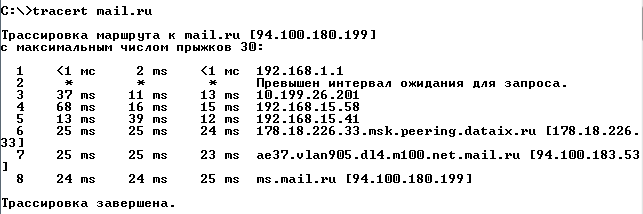
Программа tracert позволяет посмотреть маршрут, по которому двигаются IP-дейтаграммы от одного хоста к другому.

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.

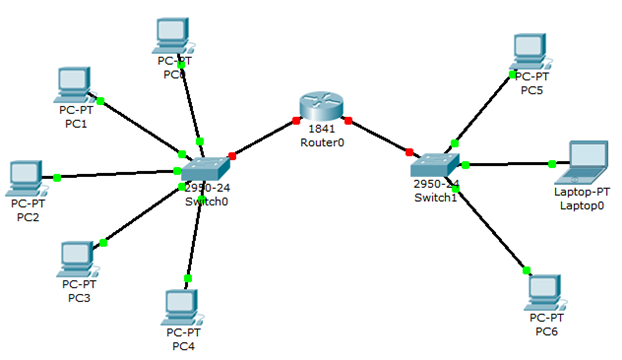
Для каждого значения TTL отправляется 3 дейтаграммы. Для каждого возвращенного ICMP-сообщения рассчитывается и печатается время возврата.

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

**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. 4.32):



*Рис. 4.32. 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

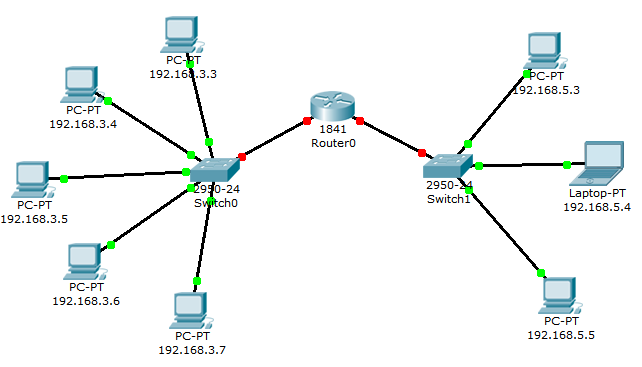
|  |  |  |
| --- | --- | --- |
| Хост | IP-адрес | Маска подсети |
| PC0 | 192.168.3.3 | 255.255.255.0 |
| PC1 | 192.168.3.4 | 255.255.255.0 |
| PC2 | 192.168.3.5 | 255.255.255.0 |
| PC3 | 192.168.3.6 | 255.255.255.0 |
| PC4 | 192.168.3.7 | 255.255.255.0 |

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. 4.33):



*Рис. 4.33. 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:

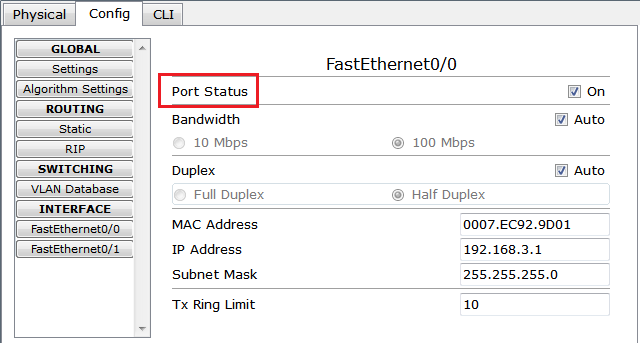
1) Один клик по устройству (маршрутизатору);

2) Выбираем вкладку “Config”;

3) Находим интерфейс FastEthernet0/0, задаем нужный IP-адрес и маску подсети (рис. 4.34).

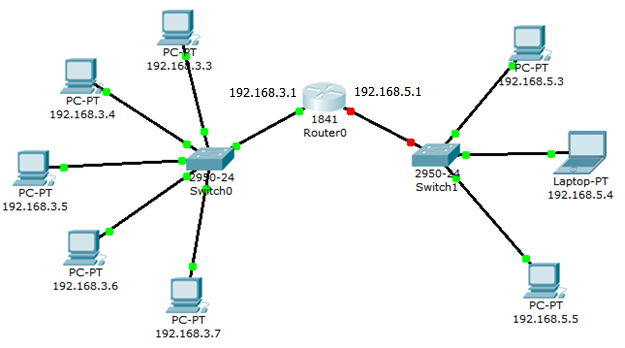
# Важно: интерфейс маршрутизатора, по умолчанию, отключен; необходимо его включить, кликнув мышкой рядом с “On”.

[Предыдущая](https://studopedia.info/3-103685.html)[1](https://studopedia.info/3-103679.html)[2](https://studopedia.info/3-103680.html)[3](https://studopedia.info/3-103681.html)[4](https://studopedia.info/3-103682.html)[5](https://studopedia.info/3-103683.html)[6](https://studopedia.info/3-103684.html)[7](https://studopedia.info/3-103685.html)**8**[9](https://studopedia.info/3-103687.html)[10](https://studopedia.info/3-103688.html)[11](https://studopedia.info/3-103689.html)[12](https://studopedia.info/3-103690.html)[13](https://studopedia.info/3-103691.html)[Следующая](https://studopedia.info/3-103687.html)



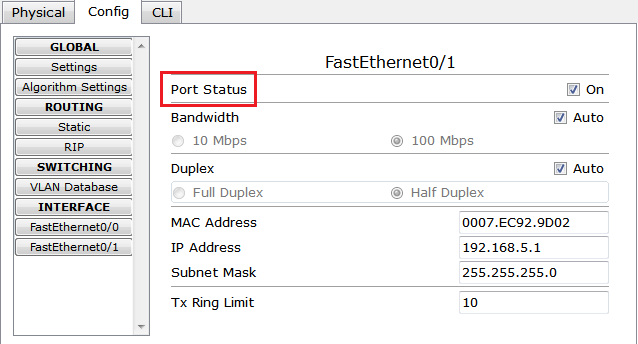
*Рис. 4.34. Настройка интерфейса маршрутизатора*

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



*Рис. 4.35. Вид рабочей области*

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



*Рис. 4.36. Настройка интерфейса маршрутизатора*

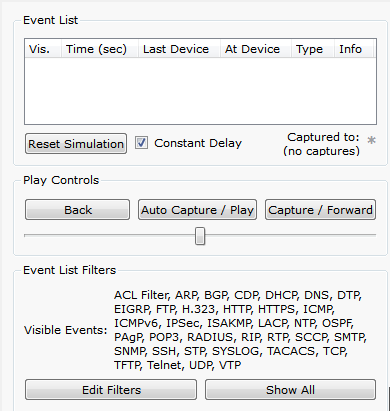
Сделать надписи к интерфейсам маршрутизатора, можно с помощью инструмента Place Note на панели Common Tools http://konspekta.net/studopediainfo/baza3/1517812499821.files/image063.png . Необходимо кликнуть на инструмент, затем сделать клик в нужном месте на рабочей области.

*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. 4.37). По умолчанию, фильтруются, т.е. будут отображаться, пакеты всех возможных протоколов, необходимо поправить и ограничить этот список до исследуемых протоколов.



*Рис. 4.37. Окно событий режима симуляции*

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

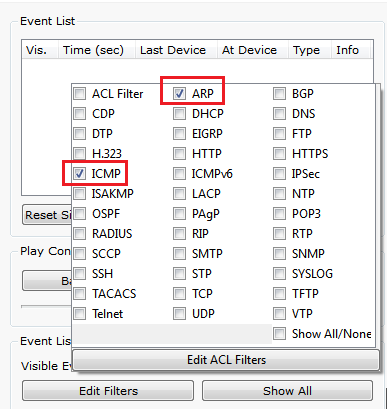
В данной лабораторной работе нас интересуют пакету двух типов ARP и ICMP.

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”

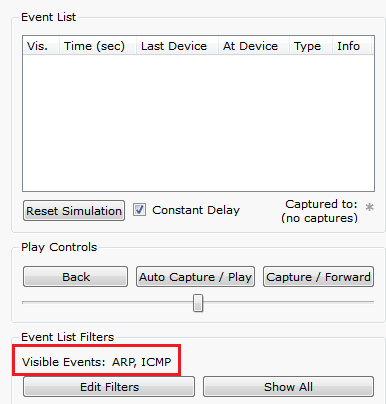
3) Выбираем ARP и ICMP



*Рис. 4.38. Добавление фильтров на протоколы ARP и ICMP*

4) Убедимся, что заданные протоколы для фильтрации назначены

(рис. 4.39)

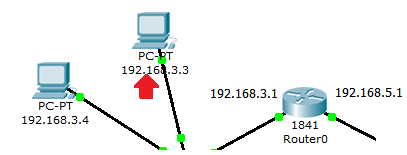


*Рис. 4.39. Окно событий режима симуляции*

*5. 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.

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

**

*Рис. 4.40. Выбор узла 192.168.3.3*

2) Выбираем вкладку *Desktop*, в которой содержатся симуляторы некоторых программ, доступных на компьютере (см. рис. 3.4).

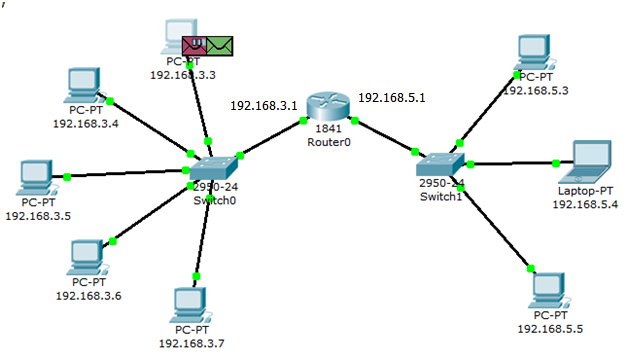
3) Выбираем “Command Prompt”, программу, имитирующую командную строку компьютера.

4) С помощью утилиты ping отправляем ping-запрос (рис. 4.41). (Не забудьте нажать Enter).

http://konspekta.net/studopediainfo/baza3/1517812499821.files/image069.png

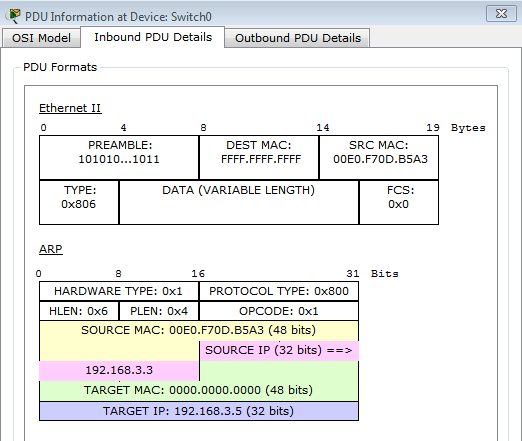
*Рис. 4.41. Командная строка узла 192.168.3.3*

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*

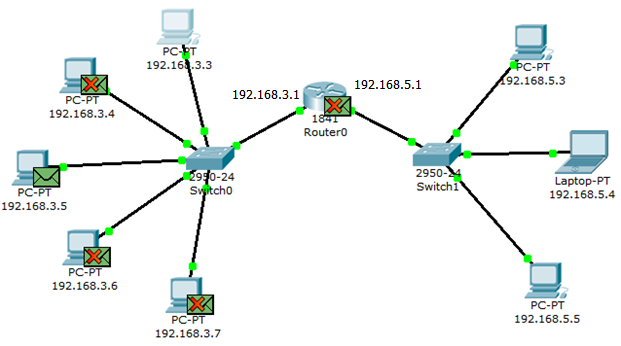
Нажимаем на кнопку “Auto Capture/play” или “Capture/Forward”, последняя позволит вам управлять движением пакетов от устройства к устройству самим. Видим, что первым отправляется пакет протокола ARP, так как ARP-таблица хоста 192.168.3.3 пуста, и он еще «не знает», кому отправлять ping-запрос. Сделайте 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*

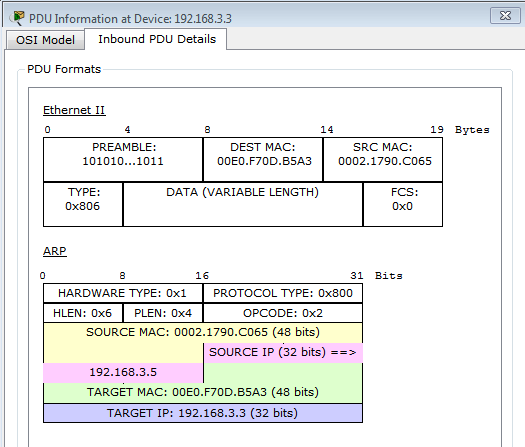
Узел 192.168.3.3 построил запрос и посылает его широковещательным сообщением всем хостам подсети. Помимо IP-адреса назначения, запрос содержит IP-адрес и МАС-адрес отправителя, чтобы приемная сторона могла ответить.

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*

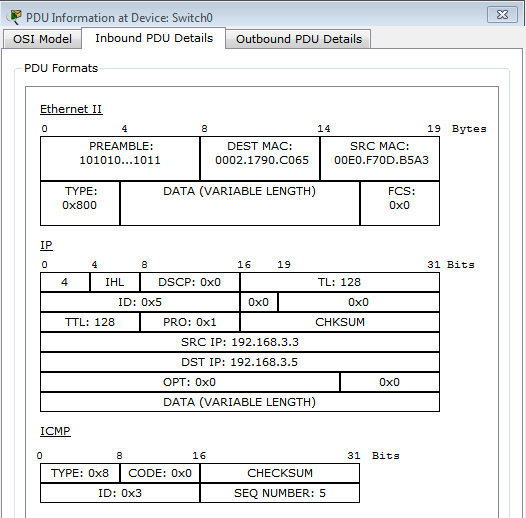
Посмотрите содержимое пакета ARP-ответа, пришедшего на хост 192.168.3.3 (рис. 4.45).



*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”.

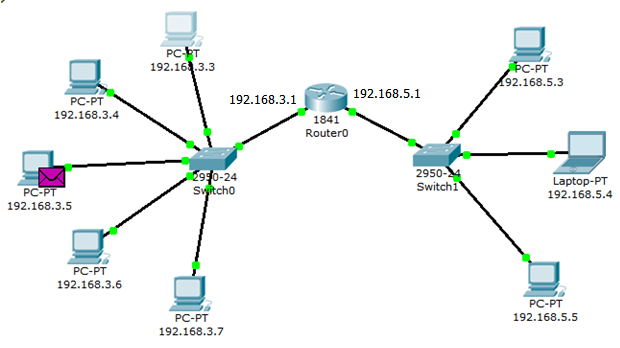
Далее отправляется ICMP-сообщение ping-запроса. Посмотрите содержимое пакета, сделав клик по пакету (конверту) (рис. 4.46).



*Рис. 4.46. Формат пакета ICMP-эхо-запроса*

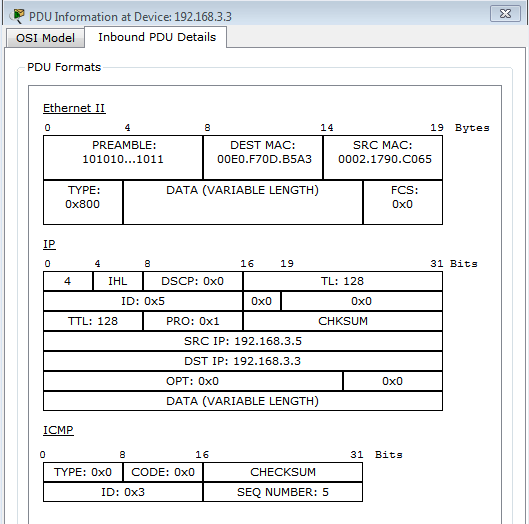
Физические адреса узлов известны. IP-адрес источника – 192.168.3.3. IP-адрес назначения – 192.168.3.5. Тип ICMP-сообщения – 8 (эхо-запрос).

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



*Рис. 4.47. Вид рабочей области*

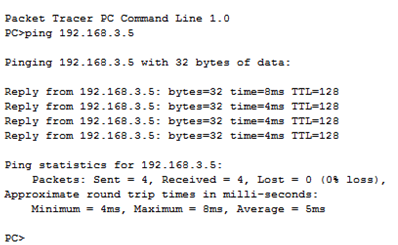
Посмотрите содержимое пакета ping-ответа, пришедшего на хост 192.168.3.3 (рис. 4.48).



*Рис. 4.48. Формат пакета ICMP-эхо-ответа*

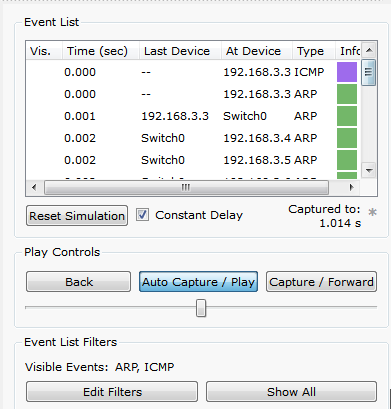
IP-адрес источника – 192.168.3.5. IP-адрес назначения – 192.168.3.3. Тип ICMP-сообщения – 0 (эхо-ответ).

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

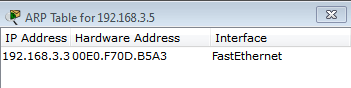
“arp –a” в командной строке.

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

http://konspekta.net/studopediainfo/baza3/1517812499821.files/image079.png

*Рис. 4.51. ARP-таблица узла 192.168.3.3 в командной строке*

Можно воспользоваться другим способом: нажать на кнопку «Inspect» http://konspekta.net/studopediainfo/baza3/1517812499821.files/image080.png , нажать на выбранное устройство, выбрать «ARP table» и просмотреть записи ARP-таблицы узла (рис. 4.52).



*Рис. 4.52. ARP-таблица узла 192.168.3.3, 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 c IP-адресом 192.168.3.4 на хост с IP-адресом 192.168.5.5.

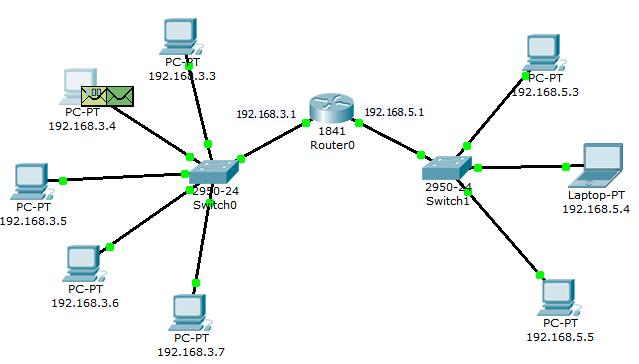
В пункте 5 лабораторной работы был рассмотрен случай посылки ARP-запроса внутри локальной сети. Протокол ARP в этом случае определял непосредственно МАС-адрес узла-приемника запроса. Теперь рассмотрим ситуацию, когда узел-источник и узел-приемник находятся в разных сетях. Протокол ARP работает в пределах 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).

http://konspekta.net/studopediainfo/baza3/1517812499821.files/image082.png

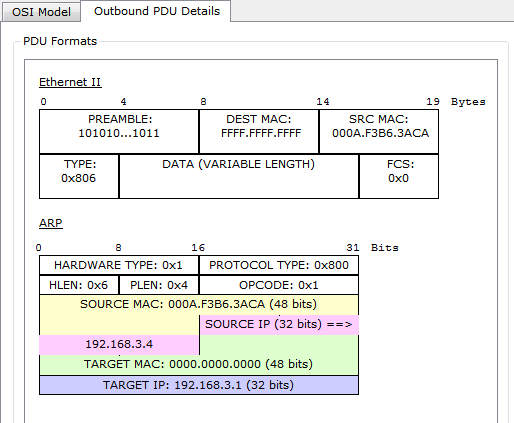
*Рис. 4.53. Командная строка узла 192.168.3.4*

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).



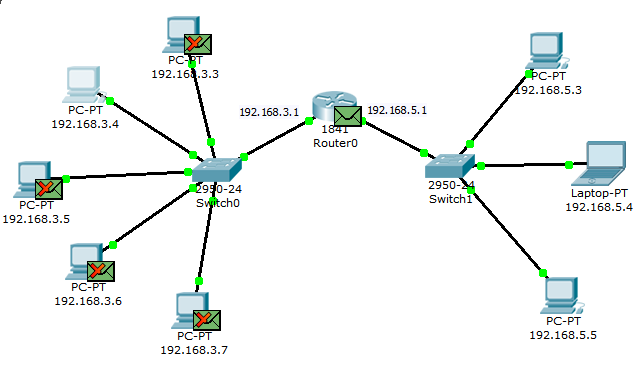
*Рис. 4.54. Вид рабочей области*

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



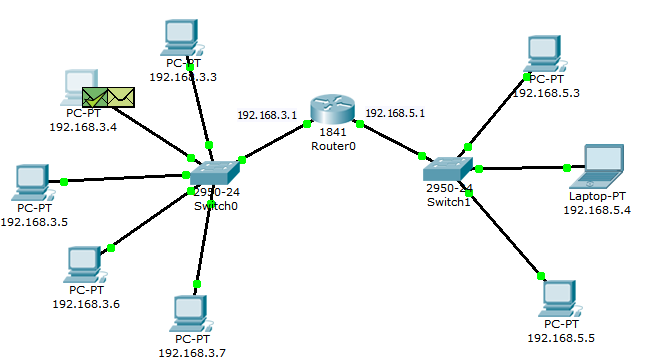
*Рис. 4.55. Формат пакета ARP-запроса*

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



*Рис. 4.56. Вид рабочей области*

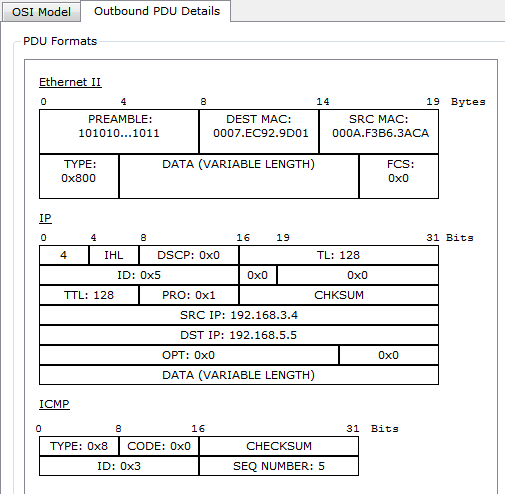
Маршрутизатор формирует ARP-ответ, указывая свой физический адрес, и отправляет его узлу 192.168.3.4 (рис. 4.57).



*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.

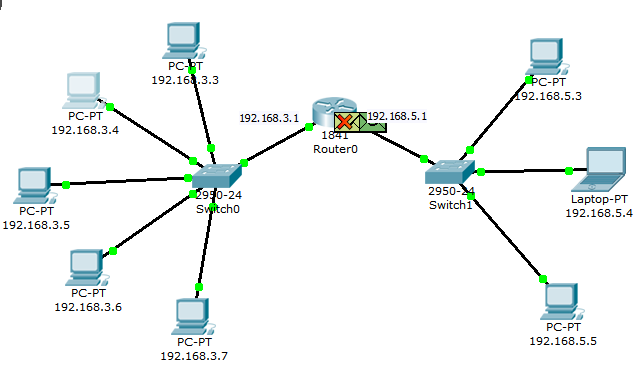
Посмотрите содержимое пакета, сделав клик по пакету (конверту) (рис. 4.58).



*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).

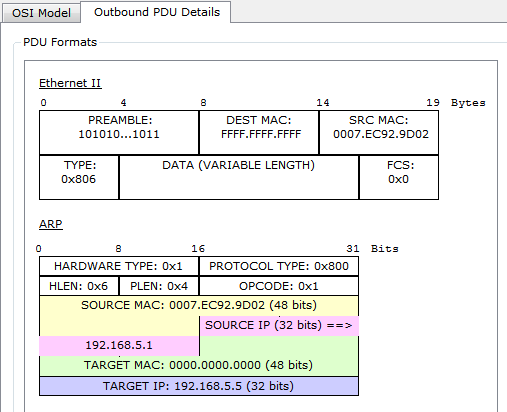
Когда запрос приходит в сеть назначения, то маршрутизатор определяет МАС-адрес получателя, если такового нет в ARP-таблице маршрутизатора. Таким образом, снова решается задача разрешения локального адреса (рис. 4.59).



*Рис. 4.59. Вид рабочей области*

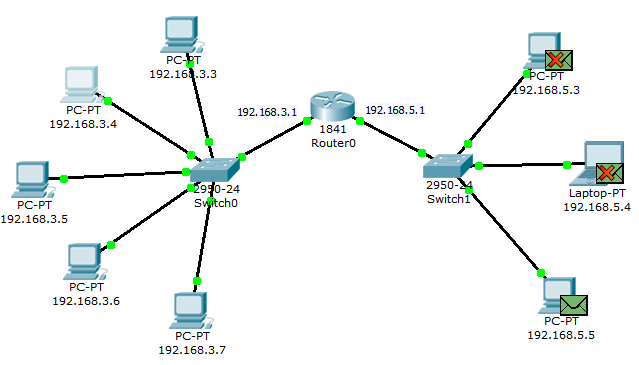
Маршрутизатор вынужден сперва узнать физический адрес получателя, прежде чем он сможет отправить ping-запрос по назначению, поэтому пакет с ping-запросом, пришедший на маршрутизатор, отклонен.

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.



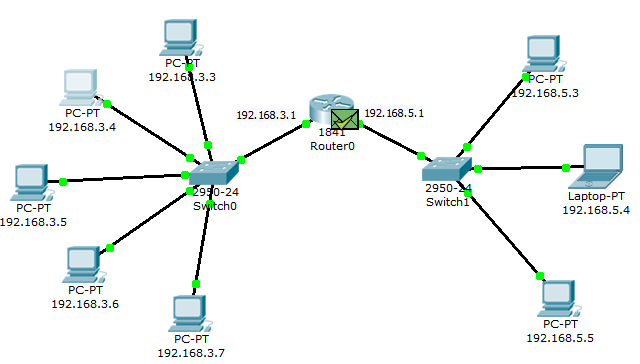
*Рис. 4.60. Формат пакета ARP-запроса*

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

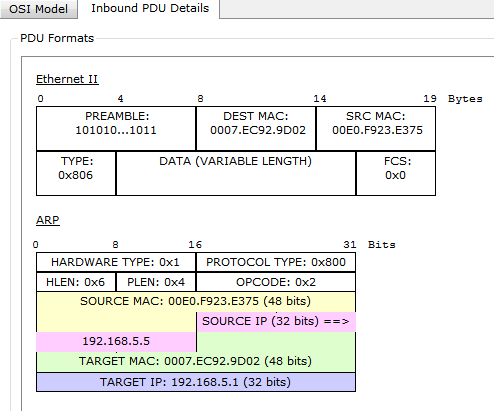


*Рис. 4.61. Вид рабочей области*

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).



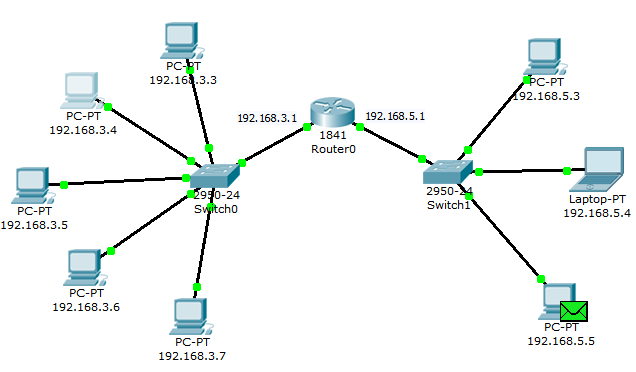
*Рис. 4.62. Вид рабочей области*



*Рис. 4.63. Формат пакета ARP-ответа*

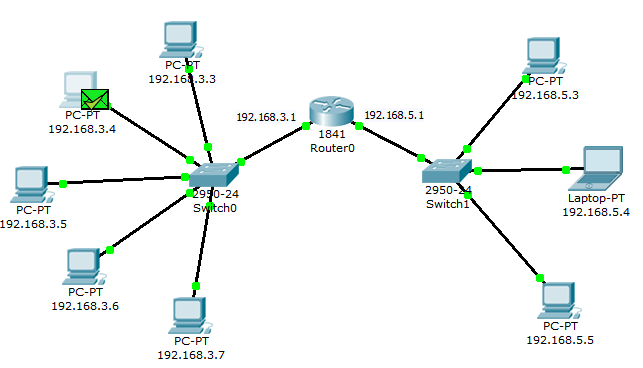
После того, как маршрутизатор определил МАС-адрес получателя входящего ping-запроса, он посылает ICMP-ответ маршрутизатору хоста отправителя. (В данном случае это тот же маршрутизатор Router0).

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.



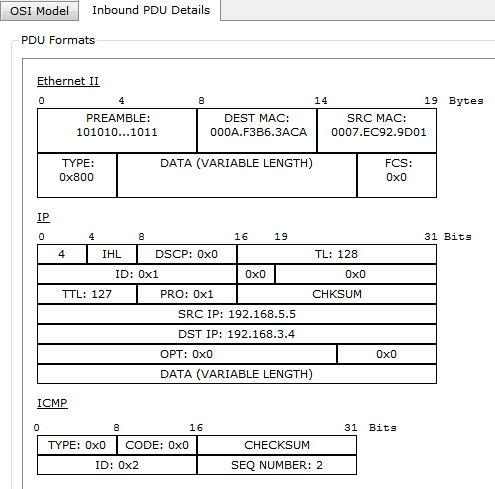
*Рис. 4.64. Вид рабочей области*

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



*Рис. 4.65. Вид рабочей области*

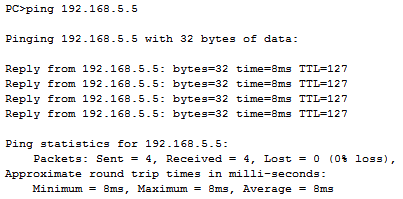
Посмотрите содержимое пакета ping-ответа, пришедшего на хост 192.168.3.4 (рис. 4.66).



*Рис. 4.66. Формат пакета ICMP-эхо-ответа*

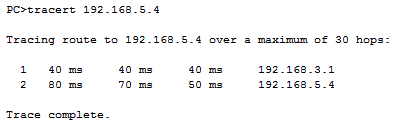
IP-адрес источника – 192.168.5.5. IP-адрес назначения – 192.168.3.4. Тип ICMP-сообщения – 0 (эхо-ответ).

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.

*7. Посылка ping-запроса на несуществующий хост*

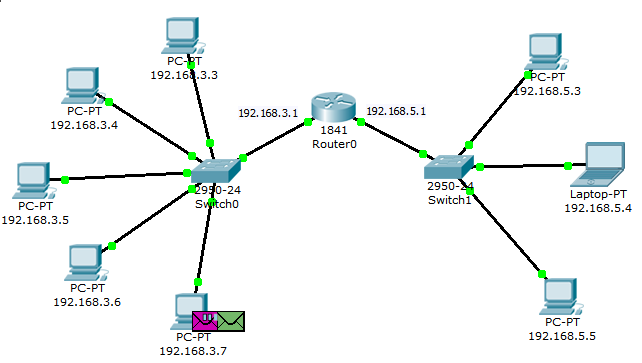
Отправим ping-запрос на несуществующий адрес в сеть 192.168.5.0/24.

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. 4.69).

http://konspekta.net/studopediainfo/baza3/1517812499821.files/image098.png

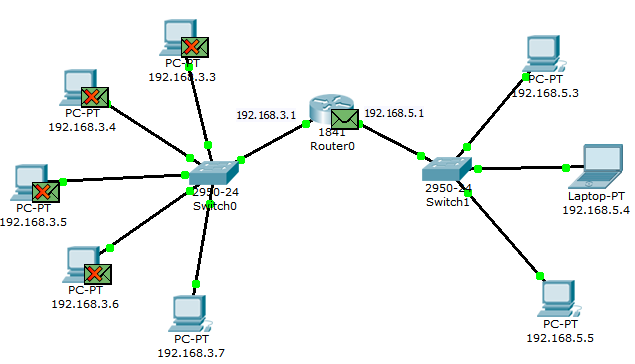
*Рис. 4.69. Командная строка узла 192.168.3.7*

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



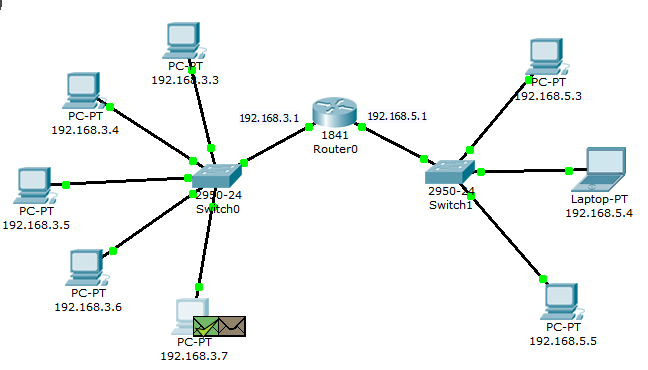
*Рис. 4.70. Вид рабочей области*

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



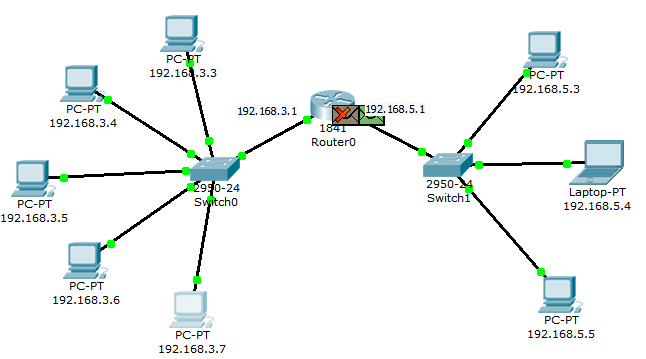
*Рис. 4.71. Вид рабочей области*

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).

**

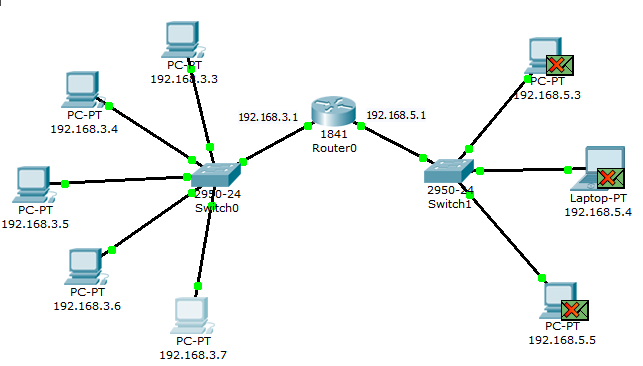
*Рис. 4.72. Вид рабочей области*

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.

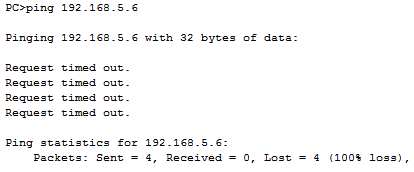


*Рис. 4.74. Вид рабочей области*

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*

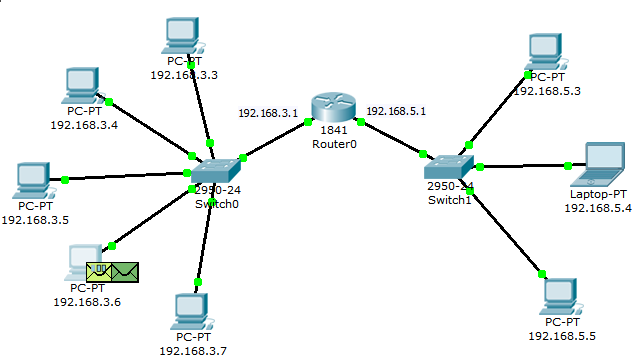
Попробуем отправить ping-запрос, содержащий IP-адрес узла, в сеть, на которую нет маршрута.

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).

http://konspekta.net/studopediainfo/baza3/1517812499821.files/image105.png

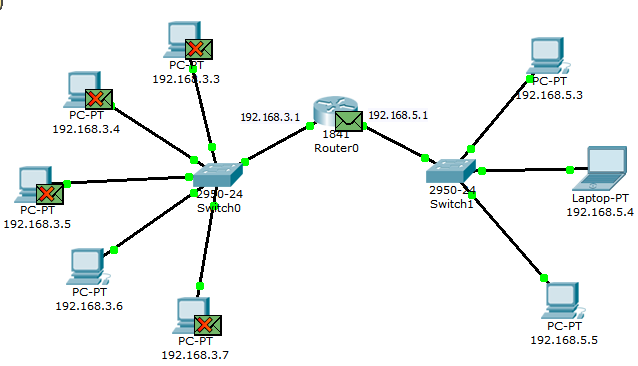
*Рис. 4.76. Командная строка узла 192.168.3.6*

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).



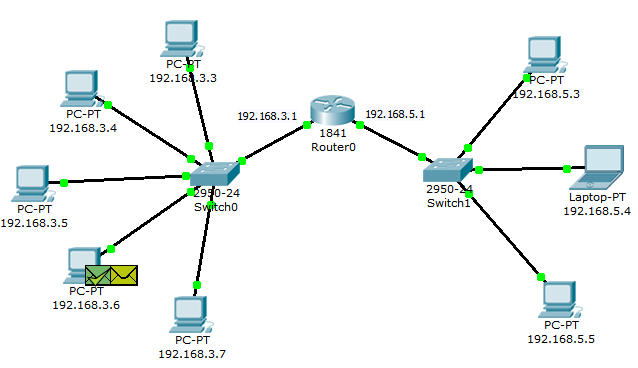
*Рис. 4.77. Вид рабочей области*

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



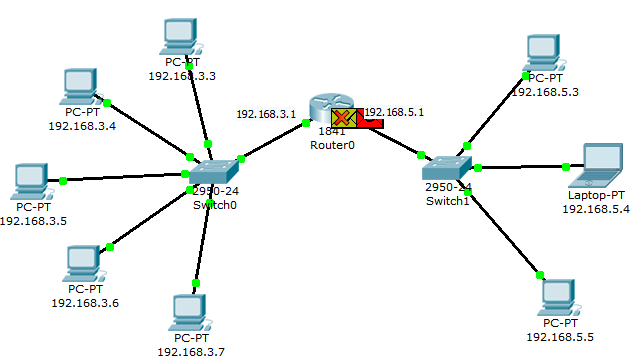
*Рис. 4.78. Вид рабочей области*

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



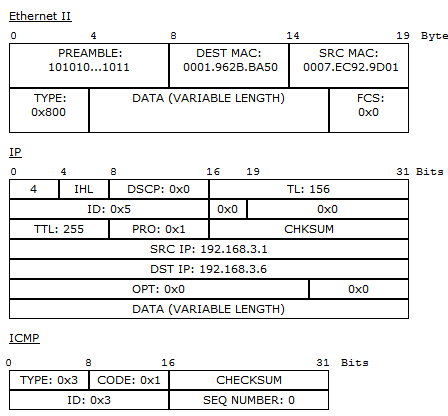
*Рис. 4.79. Вид рабочей области*

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*

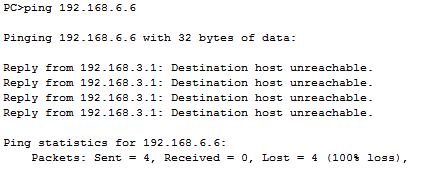
Посмотрим содержимое пакета, сформированного маршрутизатором (рис. 4.81).



*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.

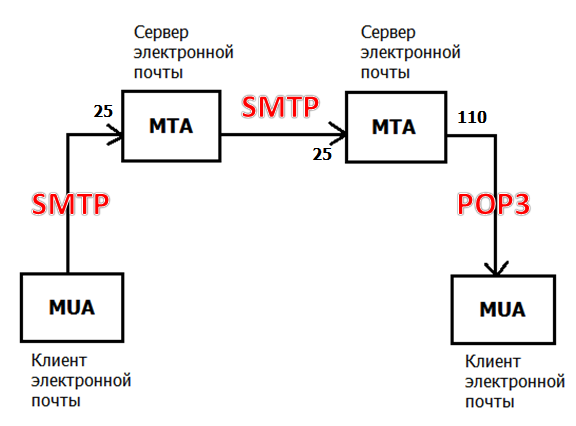
Результат ping-запроса в командной строке узла 192.168.3.6: «хост назначения недостижим» (рис. 4.82).



*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».

Схема взаимодействия с прикладными почтовыми протоколами представлена на рис. 4.83.



*Рис. 4.83. Схема взаимодействия с прикладными почтовыми протоколами*

Mail Transfer Agent (MTA) – агент передачи почты, являющийся основным компонентом системы передачи почты, представляет данный компьютер для сетевой системы электронной почты. Обычно пользователи не работают непосредственно с MTA, а используют Mail User Agent (MUA) – клиент электронной почты.

Для передачи сообщений по TCP-соединению большинство почтовых агентов пользуются протоколом Simple Mail Transfer Protocol (SMTP).

SMTP принят в качестве стандартного метода передачи электронной почты

в сети Internet. Действующий стандарт протокола описан в RFC 2821. В качестве транспортного протокола SMTP использует TCP, соединение устанавливается через порт с номером 25. Для обслуживания этого соединения используется специальная программа, которая именуется почтовым сервером. Для формирования сообщения и установления соединения используется почтовая программа пользователя. После установления соединения обмен информацией происходит посредством команд. Для пользователя эти команды не доступны, если при работе он использует клиент электронной почты [5].

Главной целью протокола SMTP является надежная и эффективная доставка электронных почтовых сообщений. Для реализации протокола требуется только надежный канал связи. Средой для SMTP может служить отдельная локальная сеть, система сетей или же всемирная сеть Internet.

Эта передача обычно осуществляется непосредственно с хоста отправителя на хост получателя, когда оба хоста используют один транспортный сервис. Если же хосты не подключены к общей транспортной системе, передача осуществляется с использованием одного или нескольких промежуточных серверов SMTP. Сегодня в Internet обычной практикой является представление исходного сообщения промежуточному серверу, который выполняет некоторые дополнительные функции. Промежуточный сервер в таких случаях действует как шлюз в другие среды передачи и выбирается обычно с использованием MX-записей DNS (служба доменных имен).

Протокол SMTP базируется на следующей модели коммуникаций: в ответ на запрос пользователя почтовая программа-отправитель сообщения устанавливает двустороннюю связь с программой-приемником (почтовым сервером). Получателем может быть оконечный или промежуточный адресат. Если необходимо, почтовый сервер может установить соединение с другим сервером и передать сообщение дальше.

Для того чтобы получить сообщение из своего почтового ящика, почтовая программа пользователя соединяется с сервером уже не по протоколу SMTP, а по специальному почтовому протоколу получения сообщений. Такой протокол позволяет работать с почтовым ящиком: забирать сообщения, удалять сообщения, сортировать их и выполнять другие операции. Самым популярным в настоящее время протоколом такого рода является протокол Post Office Protocol v.3 (POP3).

Многие концепции, принципы и понятия протокола POP3 выглядят и функционируют подобно SMTP: взаимодействие происходит посредством команд. Сервер POP3 находится между агентом пользователя и почтовыми ящиками.

Он предусматривает соединение с почтовым сервером на основе транспортного протокола TCP через порт 110. Спецификация РОР3 определена в документе RFC 1939. PОРЗ разработан с учетом специфики доставки почты на персональные компьютеры и имеет соответствующие операции для этого [6].

Конструкция протокола РОР3 обеспечивает возможность пользователю обратиться к своему почтовому серверу и изъять накопившуюся для него почту. Пользователь может получить доступ к РОР3-серверу из любой точки доступа к Internet. При этом он должен запустить специальный почтовый агент, работающий по протоколу РОР3, и настроить его для работы со своим почтовым сервером. Сообщения доставляются клиенту по протоколу POP3, а посылаются при помощи SMTP. То есть на компьютере пользователя существуют два отдельных агента-интерфейса к почтовой системе – доставки (POP3) и отправки (SMTP).