Тема 6 **«Использование сетевых компьютерных технологий в служебной деятельности»**

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 6.2

Учебные вопросы:

1. Изучение пользовательского интерфейса и возможностей специализированного программного обеспечения для моделирования компьютерных сетей.
2. Создание и администрирование локальной вычислительной сети

ВОПРОСЫ ДЛЯ АКТУАЛИЗАЦИИ ЗНАНИЙ:

1. Локальная вычислительная сеть – это?
2. Что такое сетевой мост?
3. Коммутаторы локальных сетей?
4. Протокол TCP?
5. Какие устройства можно подключить к магистрали виртуальной локальной сети VLAN?

КРАТКИЕ ТЕОРЕТИЧЕСКИЕ СВЕДЕНИЯ ПО ПЕРВОМУ ВОПРОСУ:

Cisco Packet Tracer – это программа которая является эмулятором сети передачи данных. Программа позволяет разрабатывать виртуальную модель сети, которая имеет максимальную схожесть с реальной. С помощью Packet Tracer можно построить свою сеть и проверить ее на работоспособность. В арсенале оборудования имеются:

- Маршрутизаторы: 1800, 2600, 2800
- Коммутаторы: 2950, 2960, 3650
- Серверы: DHCP, HTTP, TFTP, FTP
- Рабочие станции
- Различные кабели и модули
- Устройства Wifi

КРАТКИЕ ТЕОРЕТИЧЕСКИЕ СВЕДЕНИЯ ПО ВТОРОМУ ВОПРОСУ:

При создании локальной вычислительной сети компьютеры можно соединить между собой, чтобы передавать информацию другим компьютерам, подключенным в локальную сеть. При помощи локальной сети также можно подключаться к компьютеру–шлюзу – компьютеру, который подключен к сети Интернет и выступает раздающим его на остальные ПК.

Рассмотрим способ создания локальной сети, состоящей из двух и более компьютеров. Для этого необходимо дополнительное оборудование – свитч или роутер (используется для раздачи интернет канала всем или некоторым ПК). Каждая современная материнская плата обычно оборудуется встроенной сетевой картой, которая используется для подключения по локальной сети.

Количество компьютеров определяется количеством выходов на свитче. Такое подключение при определенной настройке операционной системы, позволяет соединить все компьютеры в единую локальную сеть, при этом, если какой-то компьютер будет выключенным от сети, остальные компьютеры будут продолжать свое существование в ней.

Для подключения каждого персонального компьютера к свитчу требуется специальный сетевой кабель («витая пара»). После разводки и подключения всех проводов от компьютера к свитчу, следует приступить к завершающему этапу – настройке операционной системы.

Первое поле IP-адрес указывает системе виртуальный сетевой адрес компьютера: 192.168.1.* – где * является любым целым числом от 1 до 255. Следующее поле, необходимое к заполнению Маска подсети – в данном случае она едина для всех компьютеров настоящей локальной сети: 255.255.255.0

После того, как IP–адреса и маски подсети заданы, необходимо присвоить каждому компьютеру уникальное имя и единую рабочую группу. В поле ввода имени компьютера задается уникальное желаемое имя, например, PK1 или OFFICE1. Все изменения сохранятся и каждый компьютер необходимо перезагрузить. Локальная сеть настроена, необходимо ее проверить.

Наиболее быстрым способом проверки работоспособности локальной сети является системная команда PING, которая посылает сетевой запрос на заданный IP–адрес компьютера, получает ответ и выводит отчет на экран.

ЗАДАНИЕ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ:

На рабочем столе – создайте папку: **Тема 6_Фамилия_№ группы.**

В созданной папке создайте документ MS Word с именем: **Тема 6_Фамилия.**

1 Методические указания к занятию

Основной целью занятия является изучение построения компьютерных сетей и сетевых протоколов, приобретение навыков работы в режиме реального времени и симуляции PacketTracer. На занятии 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 CiscoPacketTracer, необходимое программное обеспечение. Все предложенные задания дифференцированы по уровням сложности, содержат необходимые теоретические сведения, общую часть работы, обязательную для выполнения, и индивидуальные задания с учетом индивидуальных способностей обучающихся

Знакомство со средой CiscoPacketTracer

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

Выполнение работы:

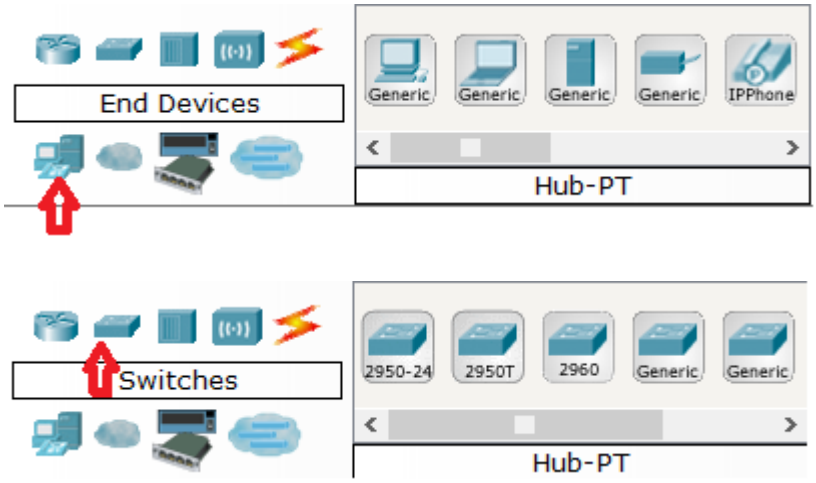
Запускаем среду CiscoPacketTracer. При запуске программы открывается главное окно симулятора.

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 работе мы используем простые сетевые устройства: концентратор, коммутатор, конечные устройства (компьютеры).

NetworkComponentBox содержит все представленное оборудование, с помощью которого можно построить сеть. С помощью одного клика по каждой группе устройств и соединений можно отобразить различные их варианты, отличающиеся между собой (рис. 1).



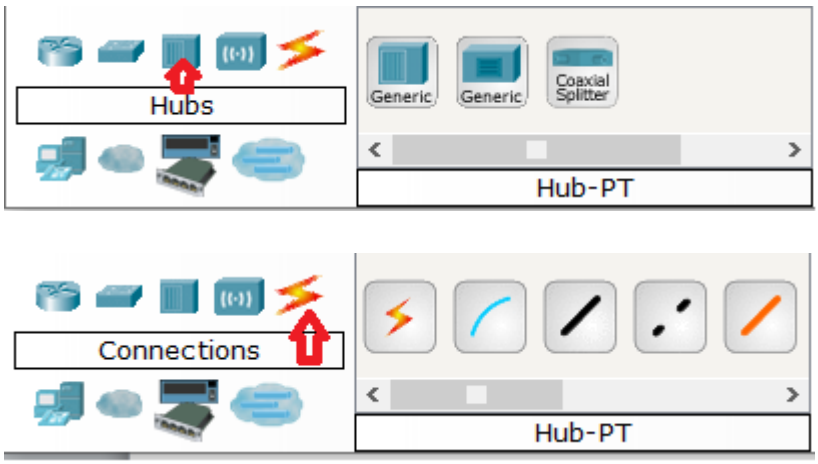


Рис. 1 Виды устройств и соединений

2. Построение топологии, добавление узлов

Один клик по конечным устройствам (рис. 2).

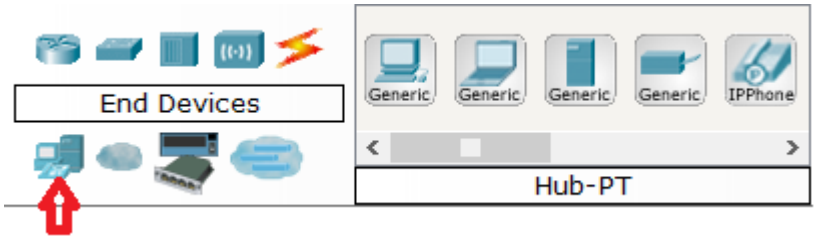


Рис. 2 Виды конечных устройств

Один клик по выбранному устройству, для нашей работы это PC (рис. 3).

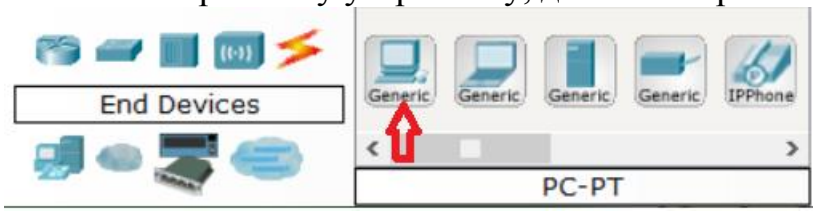


Рис. 3 Выбор конечного устройства

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).

Рис. Вид рабочей области

3. 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. 5).

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

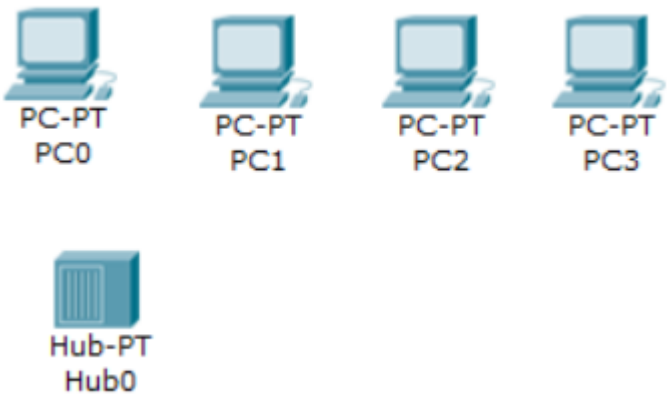


Рис. 5 Вид рабочей области

Подключим PC0 к Hub0, выбрав сначала тип подключения. Для этого случая подойдет медный кабель с прямым подключением (рис. 6).

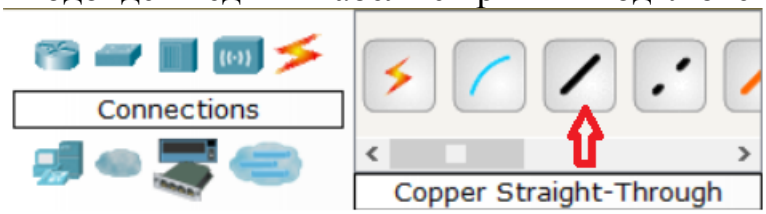


Рис. 6 Выбор соединения с прямым подключением

Для подключения PC0 к Hub0 выполните следующие действия (рис. 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.

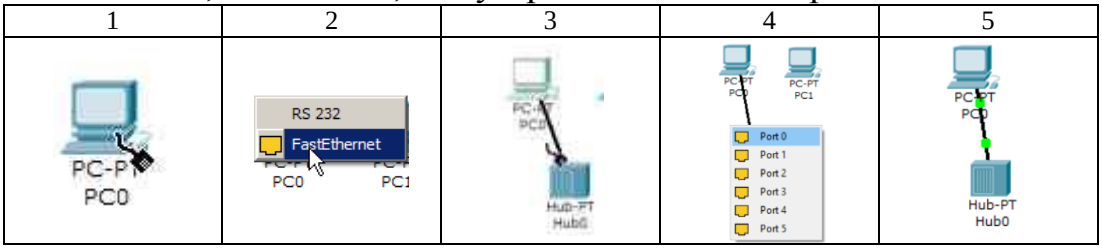


Рис. 7 Подключение PC0 к Hub0

Повторите описанные выше действия для подключения PC1 к Hub0, выбрав на концентраторе порт 1 (рис.8). Фактически номер порта значения не имеет, однако удобнее занимать порты последовательно.

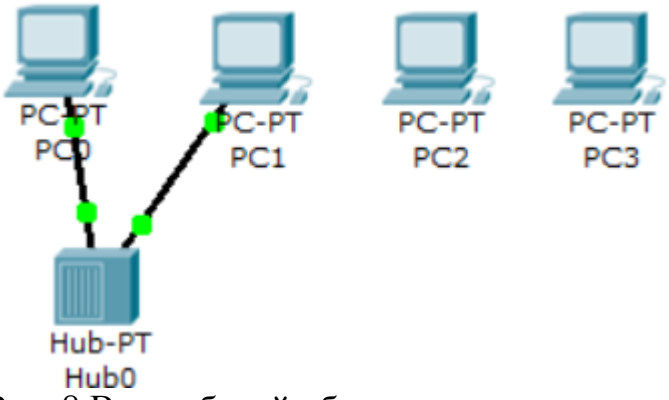
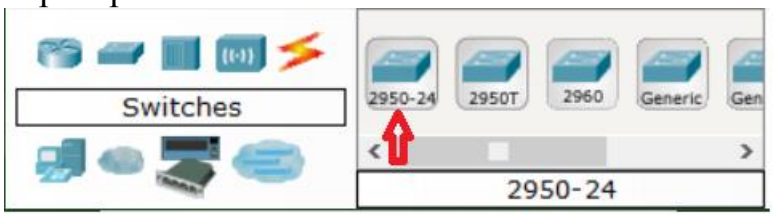


Рис. 8 Вид рабочей области

Далее размещаем на рабочей области симулятора коммутатор, например, модель 2950-24 (рис. 9).

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.



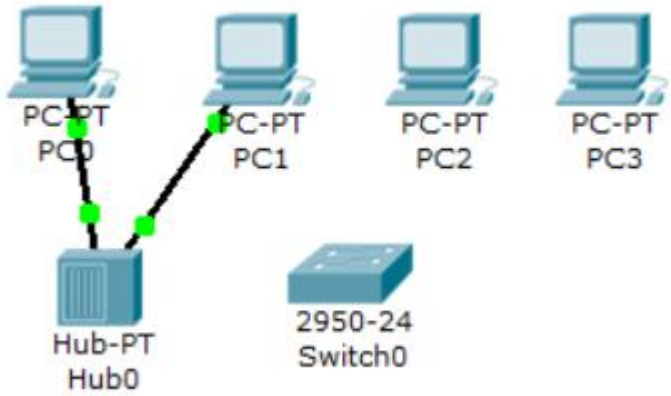


Рис. 9 Вид рабочей области

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

Для подключения выполните следующие действия (рис. 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.

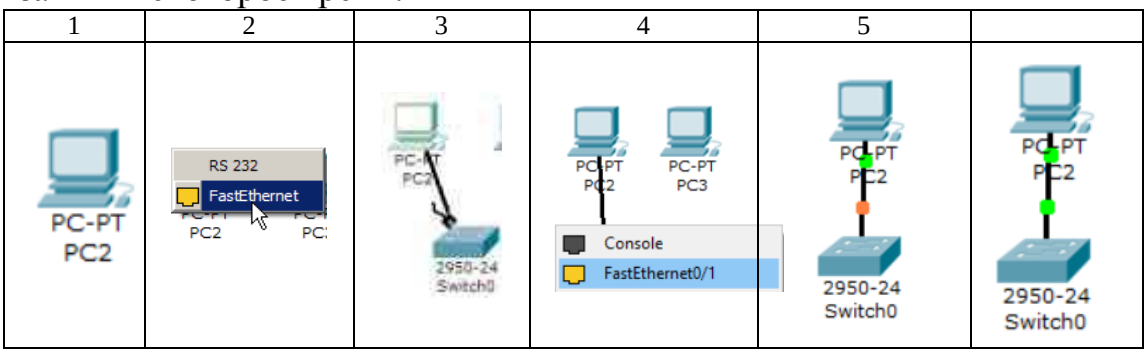


Рис. 10 Подключение PC2 к Switch0

Повторите описанные выше действия для подключения PC3 к Switch0, выбрав один из его интерфейсов FastEthernet0/2 (рис. 11).

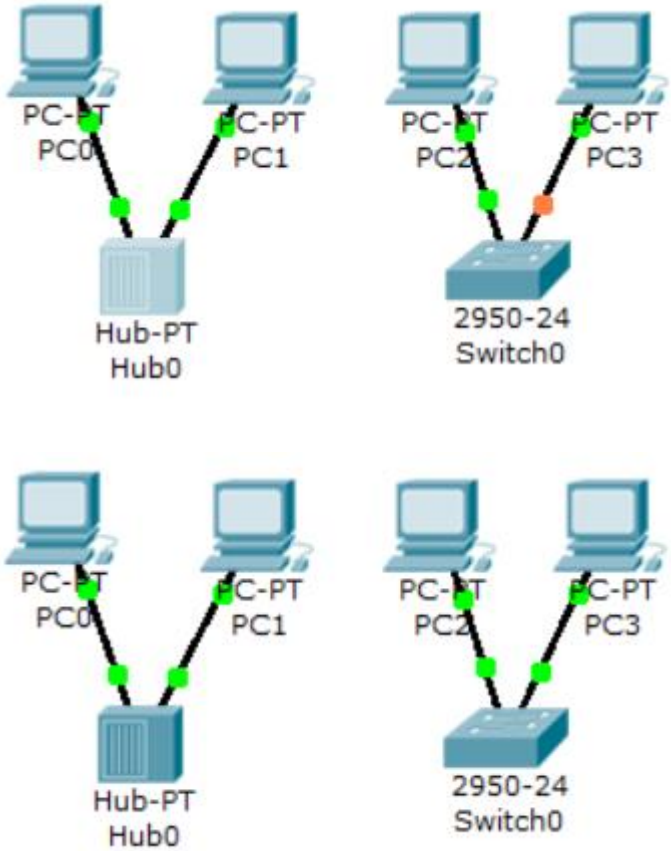


Рис. 11 Вид рабочей области (вверху оба устройства не готовы к работе)

Если навести курсор на один из индикаторов, можно посмотреть, какой интерфейс задействован при данном подключении (рис. 12).

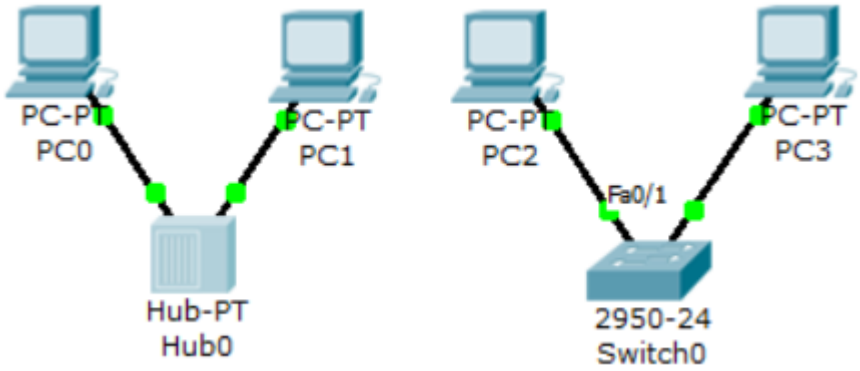


Рис. 12 Вид рабочей области

4. 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. 13).

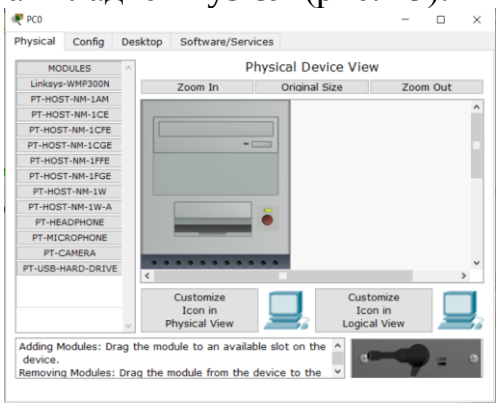


Рис. 13 Вкладка Physical конечного устройства (компьютера)

Физический вид устройства мы менять не будем, поэтому сразу переходим к настройке в вкладке Config (рис. 14).

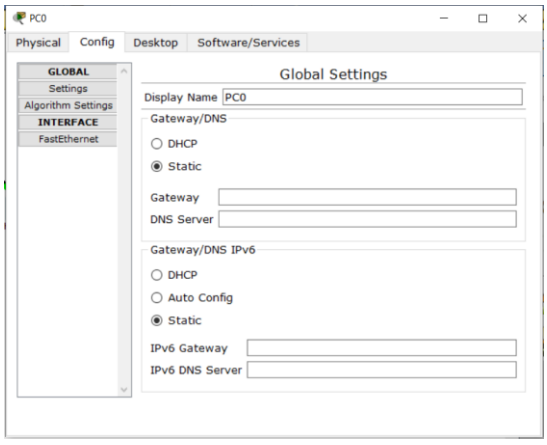


Рис. 14 Вкладка Config конечного устройства (компьютера)

Кликните мышью на интерфейсе FastEthernet (рис. 15). Укажите IP-

адрес компьютера 192.168.1.1. Нажмите на поле для ввода маски подсети, она определится автоматически 255.255.255.0.

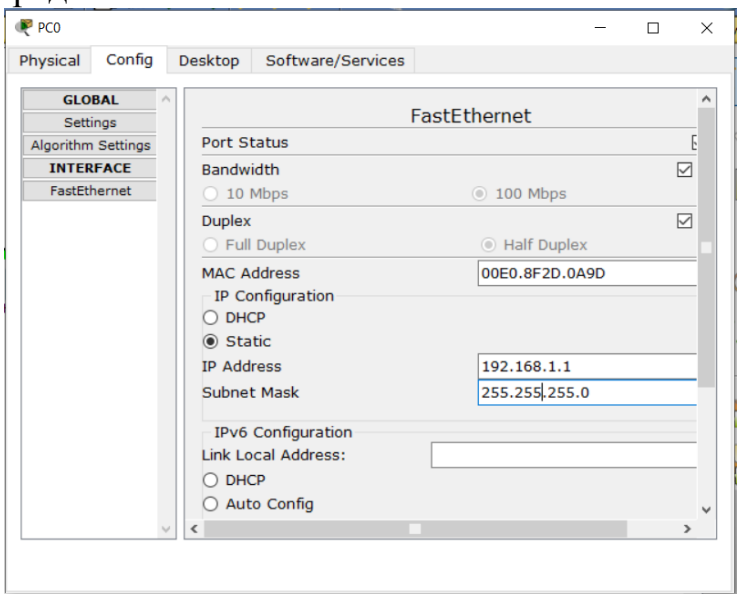


Рис. 15 Настройки интерфейса конечного устройства

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 1 (в таблице для примера указан ПЭВМ №10).

Таблица 1

Хост	IP-адрес	Маска подсети
PC0	192.168.1.№ПЭВМ	255.255.255.0
PC1	192.168.1. №ПЭВМ+1	255.255.255.0
PC2	192.168.1. №ПЭВМ +2	255.255.255.0
PC3	192.168.1. №ПЭВМ +3	255.255.255.0

Можно проверить введенную вами информацию на узлах (рис. 17). Для этого наведите курсор на интересующее вас устройство.

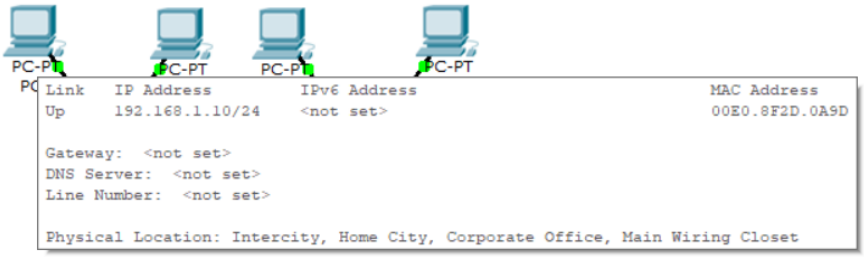


Рис. 17 Проверка настроек конечного устройства (компьютера)

Если при построении сети какие-либо устройства или связи оказались лишними, их можно удалить при помощи инструмента Delete на боковой панели симулятора (CommonToolsBar). Для удаления нужно щелкнуть один

раз на инструмент Delete, затем на элемент сети.

5. Соединение концентратора и коммутатора

Для подключения такого типа устройств, как коммутатора и концентратора, используется перекрестный кабель (рис. 18).

Рис. 18. Выбор соединения

Для подключения Hub0 к Switch0 выполните следующие действия:

1) Щелкните один раз на Hub0, выберите порт 2 (рис. 19).

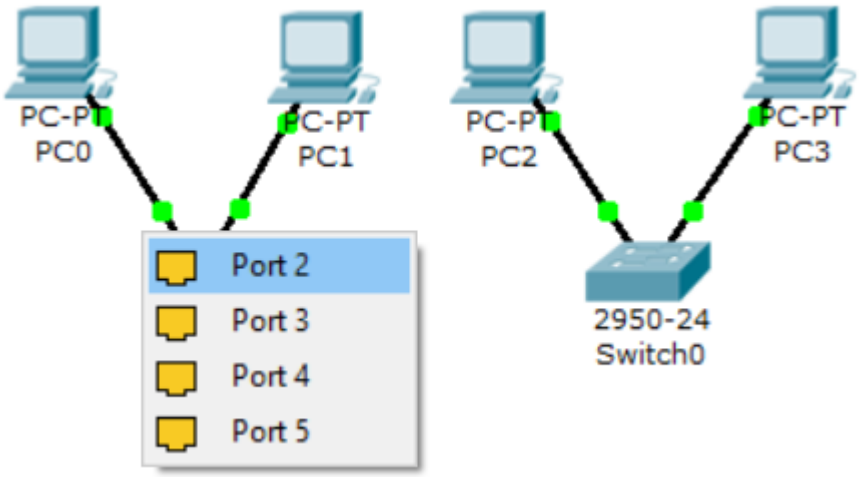


Рис. 19 Вид рабочей области

2) Переместите курсор на Switch0, щелкните на нем мышью и выберите интерфейс FastEthernet0/3 (рис. 20).

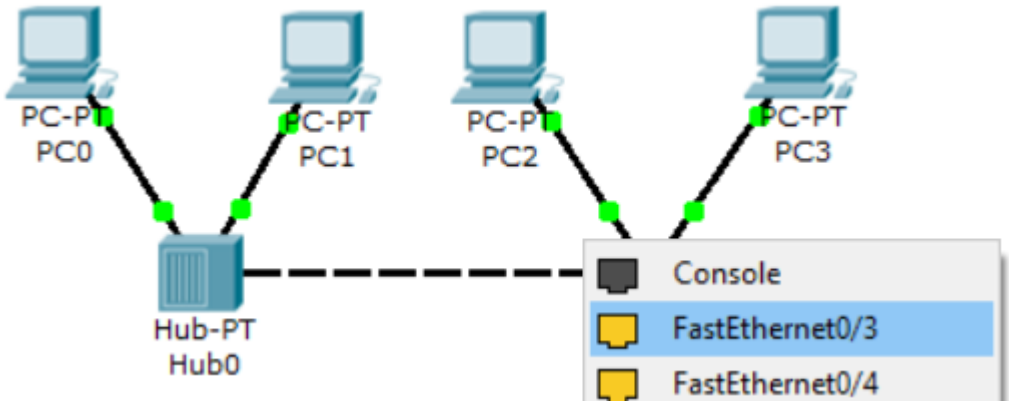


Рис. 20. Вид рабочей области

3) Когда оба устройства будут готовы к работе, индикаторы состояния станут зелеными (рис. 21).

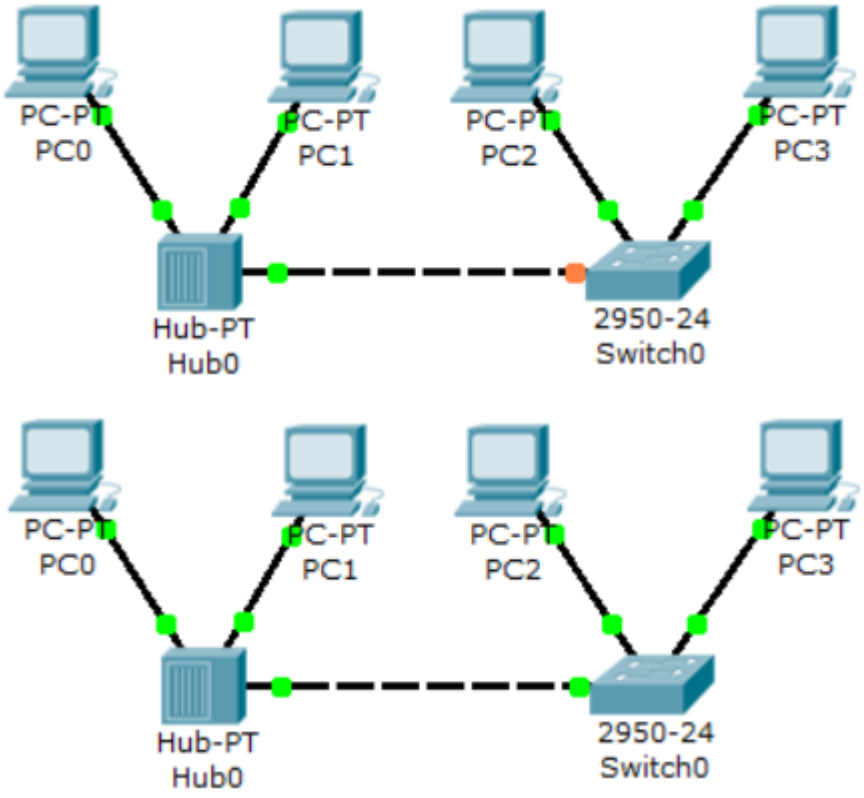


Рис. 21. Вид рабочей области (вверху оба устройства не готовы к работе)

С помощью кнопки на клавиатуре <Prt Sc> сохраните копию экрана в буфер обмена.

Перейдите в документ Word. Вставьте под первым пунктом слова: **1. Топология сети** *и вставьте в документ картинку из программы.*

В дальнейшем будем обозначать + ***(*КОПИЯ ЭКРАНА*)***

6. Выполним проверку в режиме реального времени

Убедитесь, что вы находитесь в режиме реального времени.

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

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. 22).

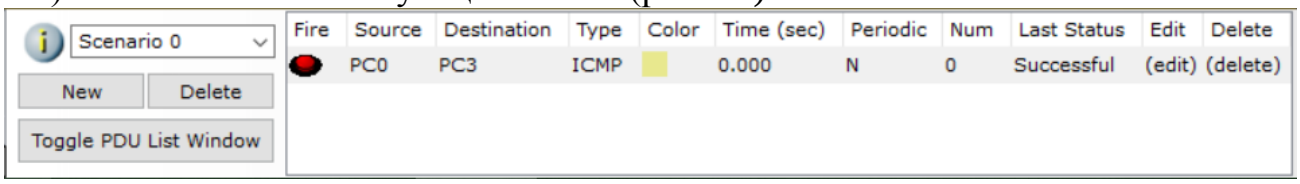


Рис. 22 Окно управления пакетами

2. Проверка соединения + *(*КОПИЯ ЭКРАНА*)*

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?

3. Проверка соединения + *(*КОПИЯ ЭКРАНА*)*

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

Нажмите на кнопку Delete на панели User Created Packet Window (рис. 23).

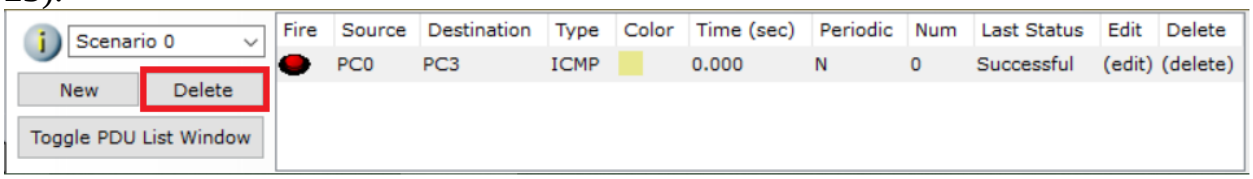


Рис. 23 Окно управления пакетами

Все записи сценария удалятся.

7. Сохранение созданной топологии

Выберите в MenuBar вкладку File, далее Saveas. Выберите папку на рабочем столе **…\Тема 6..** и сохраните под именем: **сеть6.1_Фамилия.pkt**. (Все файлы симулятора CiscoPacketTracer имеют расширение .pkt.)

Построение топологии сети, состоящей из двух подсетей, изучение ПРОТОКОЛЫ ARP И ICMP (ПРОГРАММЫ PING И TRACERT)

Цель работы: изучить режим симуляции CiscoPacketTracer, протоколы ARP и ICMP на примере программ ping и tracert.

Программа работы:

1. Построение топологии сети, настройка конечных узлов;
2. Настройка маршрутизатора;
3. Проверка работы сети в режиме симуляции;
4. Посылка ping-запроса внутри сети;
5. Посылка ping-запроса во внешнюю сеть;
6. Посылка ping-запроса на несуществующий IP-адрес узла;
7. Выполнение индивидуального задания.

Выполнение работы:

1. Построение топологии сети

Создайте следующую топологию сети, состоящую из конечных узлов

(PC), коммутаторов и маршрутизатора (рис. 32):

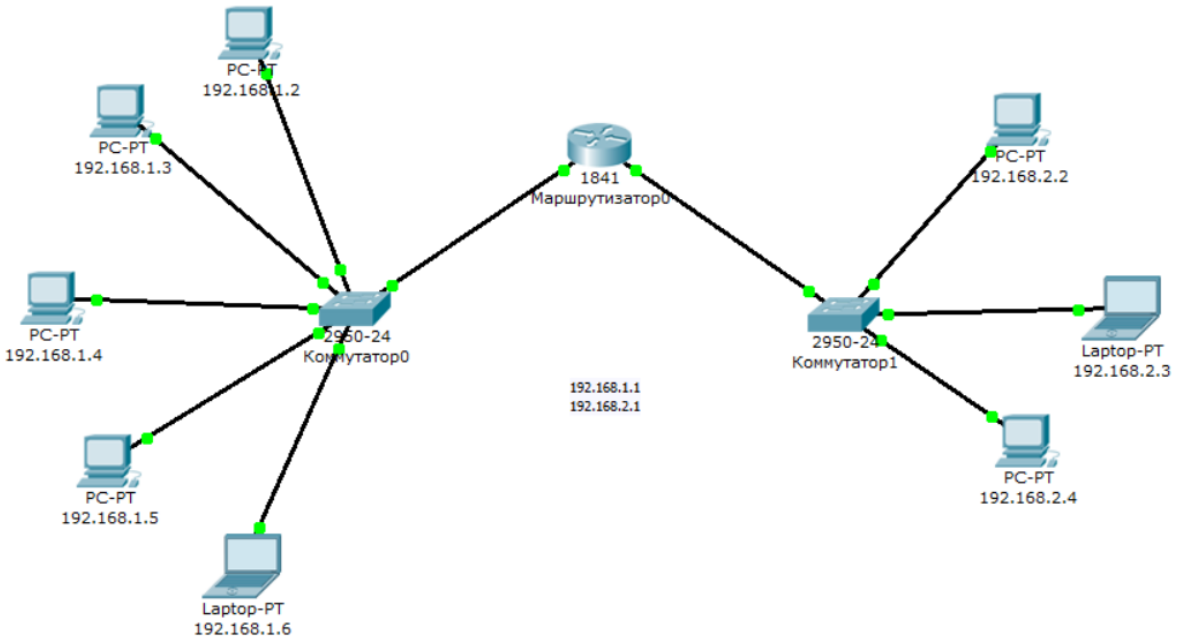


Рис. 32 Тестовая топология сети

При добавлении маршрутизатора выберите модель 1841, т.к. она имеет два интерфейса.

При соединении устройств между собой воспользуйтесь медным кабелем с прямым подключением.

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 2). IP-адрес шлюза для всех узлов – 192.168.№ПЭВМ.1. IP-адрес DNS-сервера указывать необязательно, т.к. в данной работе он использоваться не будет.

Таблица 2

Хост	IP-адрес	Маска подсети
PC0	192.168.№ПЭВМ.№ПЭВМ+1	255.255.255.0
PC1	192.168.№ПЭВМ.№ПЭВМ+2	255.255.255.0
PC2	192.168.№ПЭВМ.№ПЭВМ+3	255.255.255.0
PC3	192.168.№ПЭВМ.№ПЭВМ+4	255.255.255.0
Laptop6	192.168.№ПЭВМ.№ПЭВМ+5	255.255.255.0

На устройствах PC5, Laptop0, PC6 установим заданные IP-адреса и маску подсети (таблица 3). IP-адрес шлюза для всех узлов – 192.168.№ПЭВМ+2.1 IP-адрес DNS-сервера указывать необязательно.

Таблица 3

Хост	IP-адрес	Маска подсети
PC5	192.168.№ПЭВМ+2.№ПЭВМ+1	255.255.255.0
Laptop0	192.168.№ПЭВМ+2.№ПЭВМ+2	255.255.255.0
PC6	192.168. №ПЭВМ+2.№ПЭВМ+3	255.255.255.0

Каждый узел переименуем его же IP-адресом, получится следующее

(рис. 33):

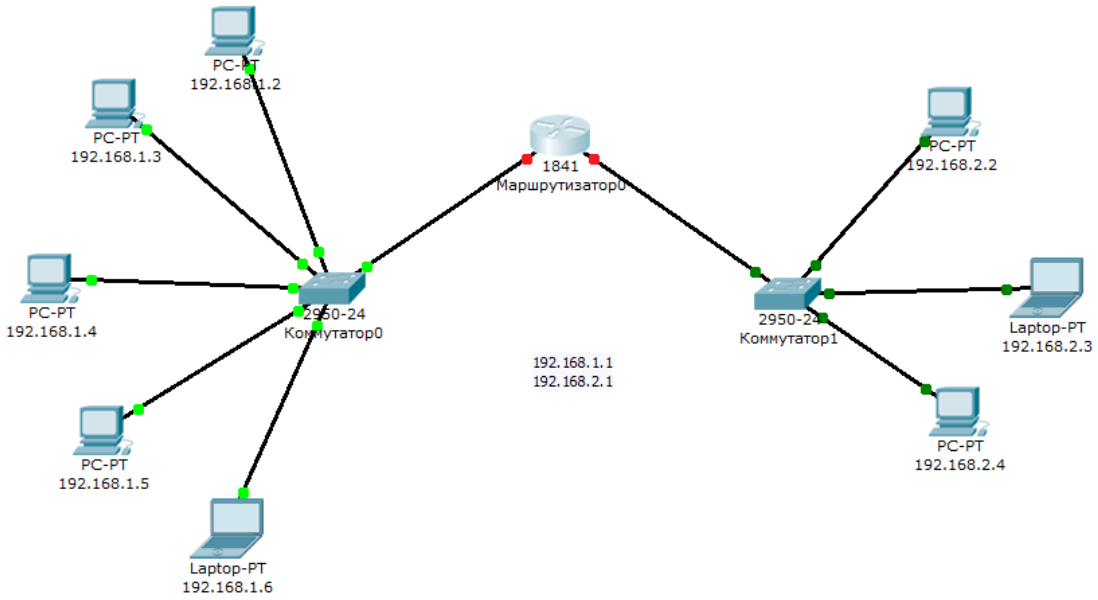


Рис. 33 Вид рабочей области

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. 34).

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

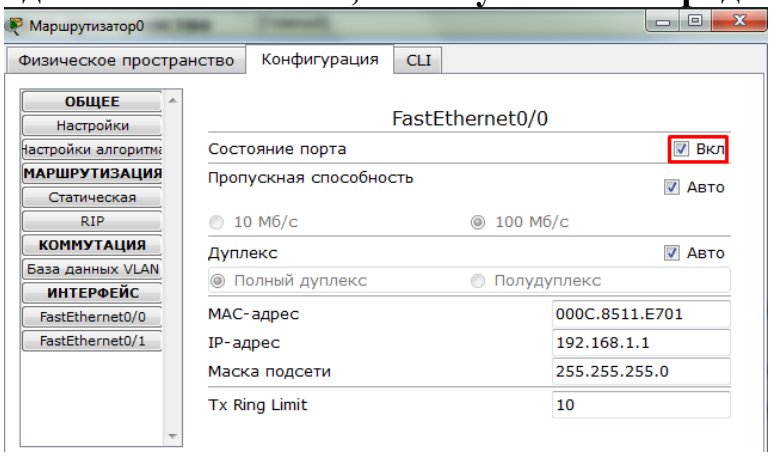


Рис. 34 Настройка интерфейса маршрутизатора

4) Закрываем окно, смотрим на всю топологию сети. Зеленые индикаторы состояния на линии связи между Router0 и Switch0 сигнализируют, что интерфейс подключен правильно (рис. 35).

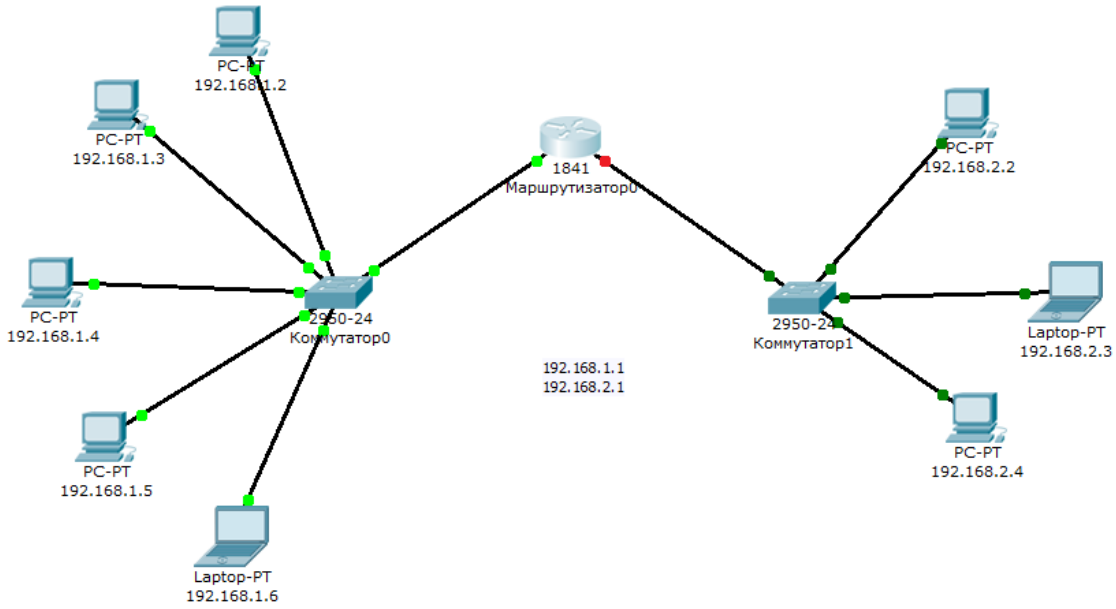


Рис. 35 Вид рабочей области

Аналогично производим настройку интерфейса FastEthernet0/1 (рис. 36).

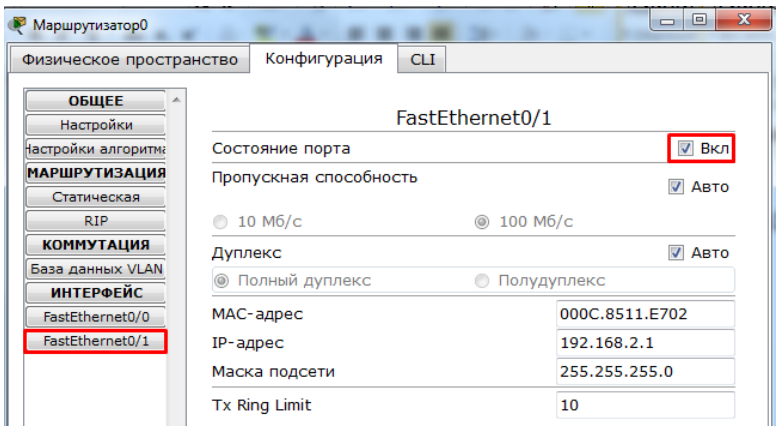


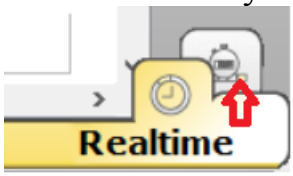
Рис. 36 Настройка интерфейса маршрутизатора

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

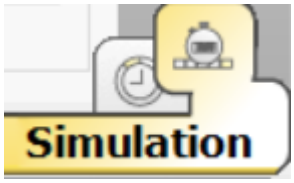
В документе WORD на новом листе – вставьте: **Задание 6.2,** с новой строки **1. Топология сети +** ***(*КОПИЯ ЭКРАНА*)***

4. Режим симуляции Cisco Packet Tracer

Для этого кликните на иконку симуляции в правом нижнем углу рабочей области симулятора.



Убедитесь, что вы находитесь в режиме симуляции.



Откроется окно событий, в котором вы увидите список событий, управляющие кнопки, заданные фильтры (рис. 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
- AutoCapture/Play – автоматический захват пакетов от источника до приемника и обратно
- Capture/Forward – захват пакетов только от одного устройства до другого

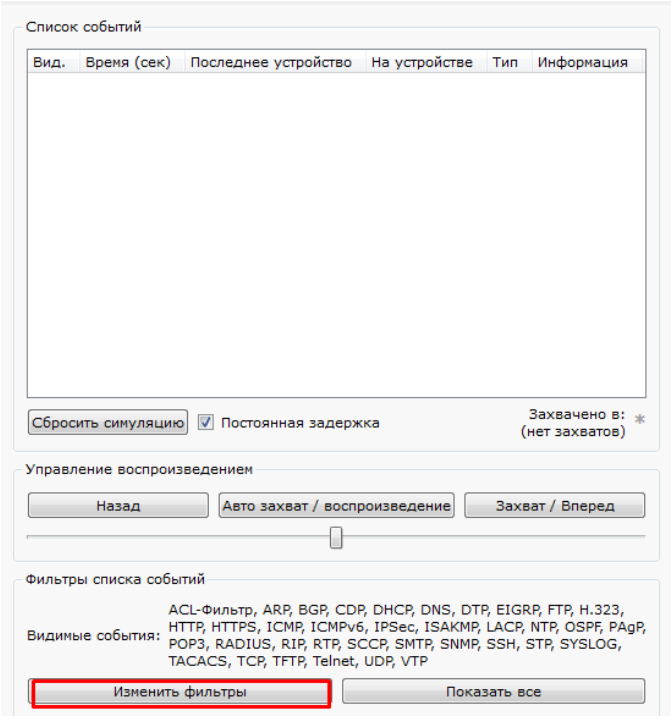


Рис. 37 Окно событий режима симуляции

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

ARP — протокол в компьютерных сетях, предназначенный для определения MAC-адреса другого компьютера по известному IP-адресу.

Протокол Internet Control Message Protocol (ICMP) – это набор коммуникационных правил, которые устройства используют для распространения информации об ошибках передачи данных в сети. При обмене сообщениями между отправителем и получателем могут возникнуть непредвиденные ошибки.

Следовательно, нужно поставить фильтр только на сообщения заданного типа (рис. 38):

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

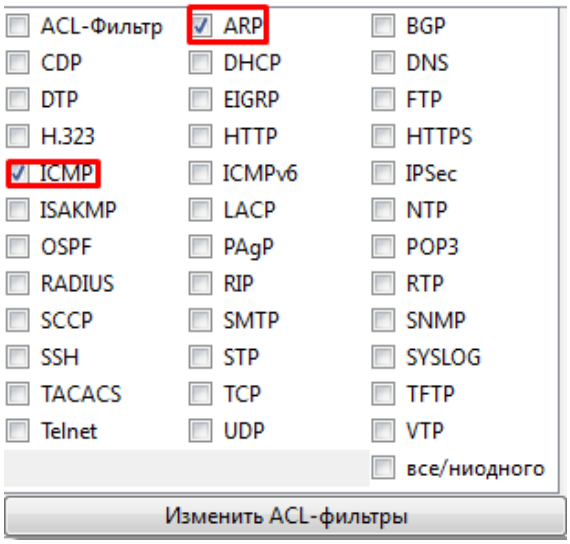


Рис. 38 Добавление фильтров на протоколы ARP и ICMP

4) Убедимся, что заданные протоколы для фильтрации назначены (рис. 39)

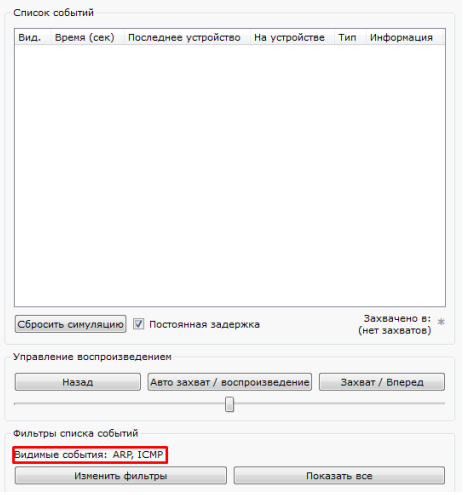


Рис. 39 Окно событий режима симуляции

2. Протоколы + *(*КОПИЯ ЭКРАНА*)*

5. Проверка работы сети в режиме симуляции

Отправим тестовый ping-запрос с конечного узла с IP-адресом 192.168.1.2 на хост с IP-адресом 192.168.1.5.

Важно: оба узла находятся в пределах одного сегмента сети

1) Один клик по выбранному устройству (рис. 40)

Рис. 40 Выбор узла 192.168.1.2

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

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

4) С помощью утилиты ping отправляем ping-запрос (рис. 41). (Не забудьте нажать Enter).

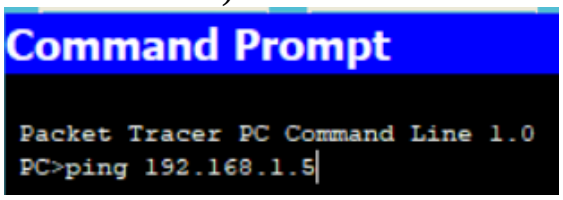


Рис. 41 Командная строка узла 192.168.1.2

3. Ping + *(*КОПИЯ ЭКРАНА*)*

На устройстве-источнике формируются два пакета протокола ARP и ICMP (рис. 42). ARP-запрос возникает всегда, когда хост пытается связаться с другим хостом.

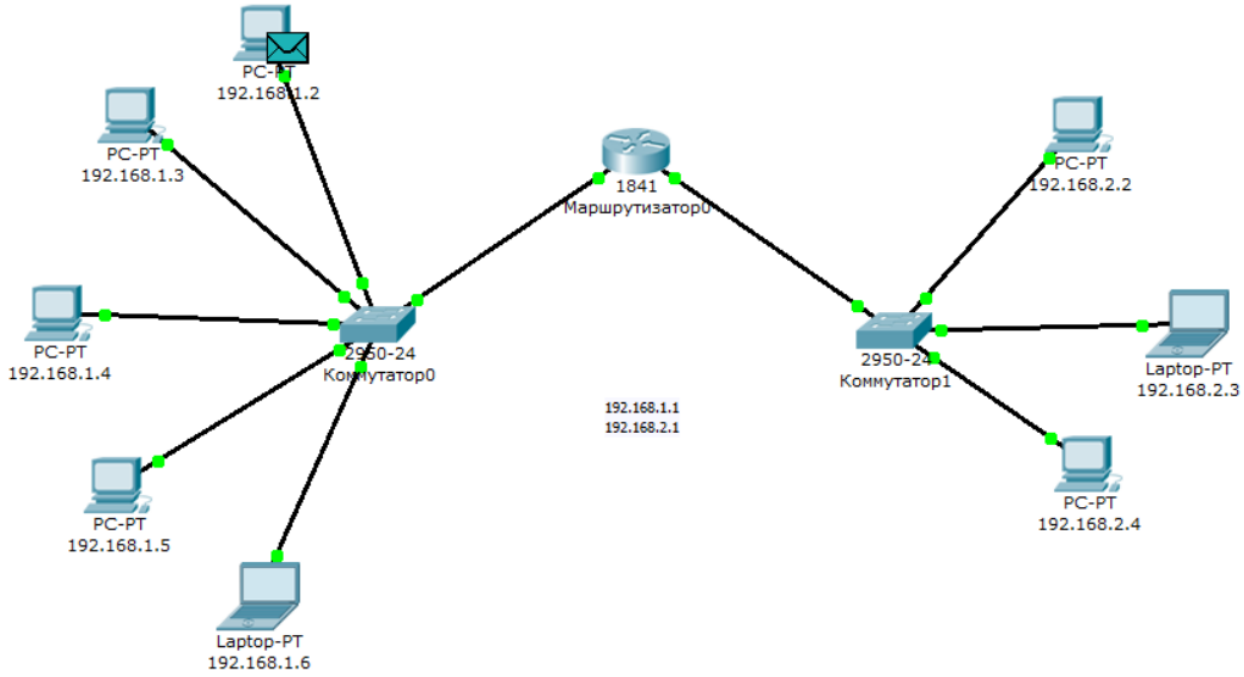


Рис. 42 Вид рабочей области

4. Протоколы + *(*КОПИЯ ЭКРАНА*)*

Нажимаем на кнопку “AutoCapture/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 192.168.1.2 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 “InboundPDUDetails”, которая содержит структуру пакета (рис. 43).

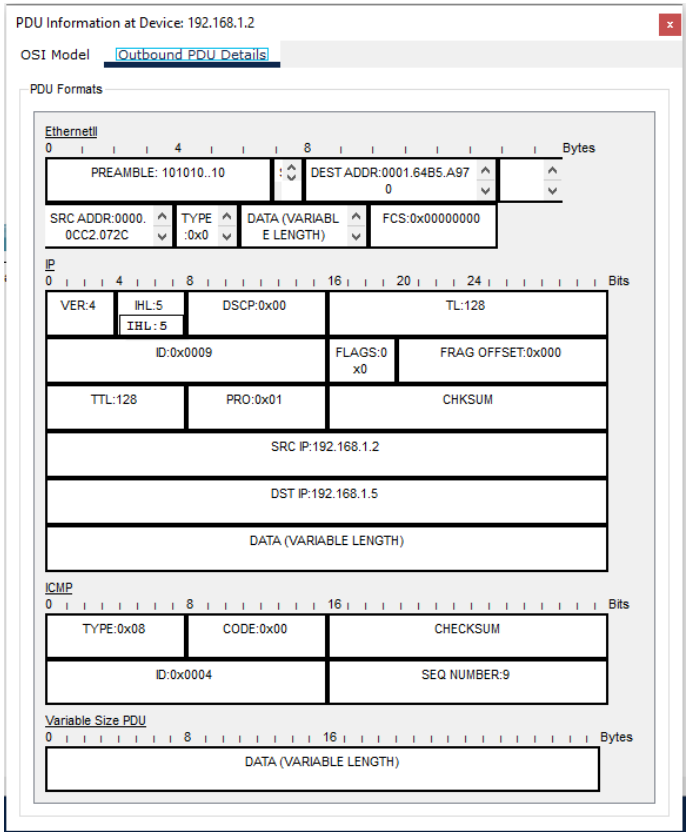
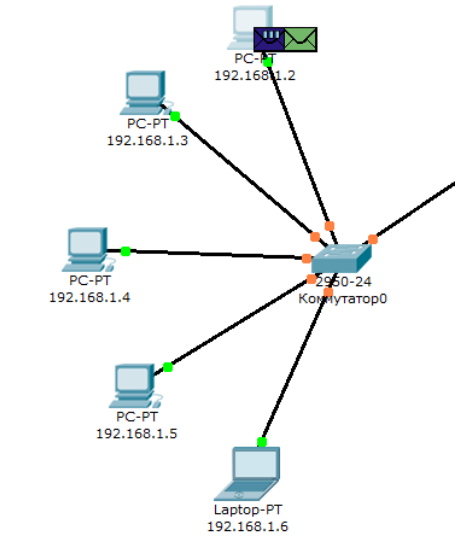


Рис. 43 Формат пакета ARP-запроса

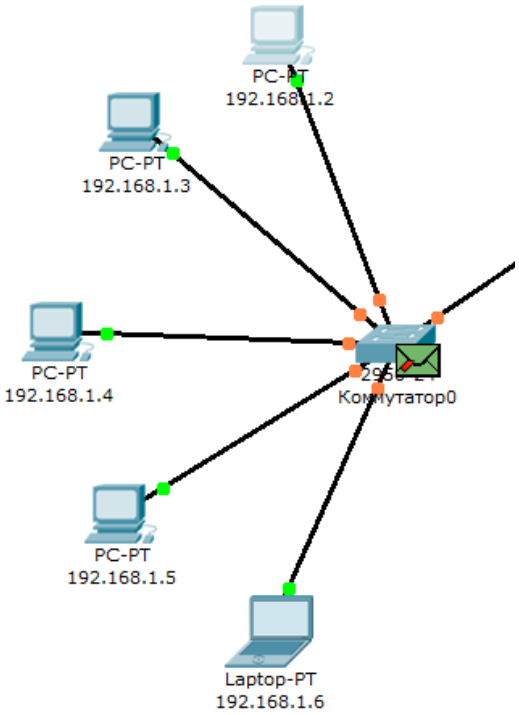
5. Протоколы + *(*КОПИЯ ЭКРАНА*)*

Узел 192.168.1.2 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.

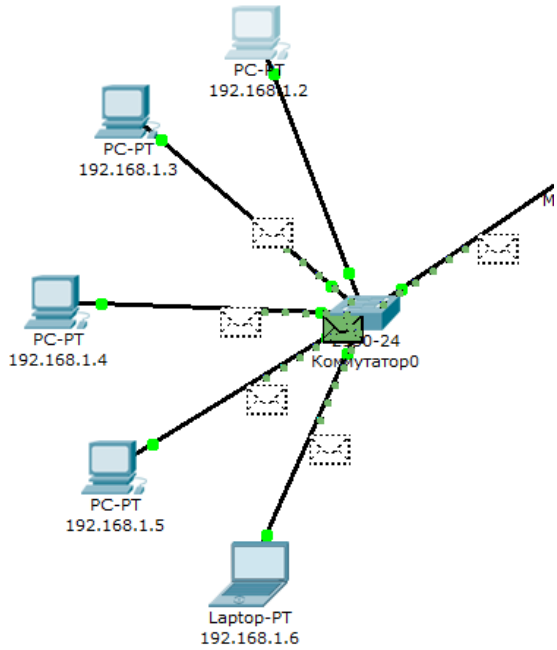
При просмотре прохождения пакетов убедитесь, что на ARP-запрос ответит только хост 192.168.1.5. Каждый хост в подсети получает запрос и проверяет на соответствие свой IP-адрес. Если он не совпадает с указанным адресом в запросе, то запрос игнорируется (рис. 44).



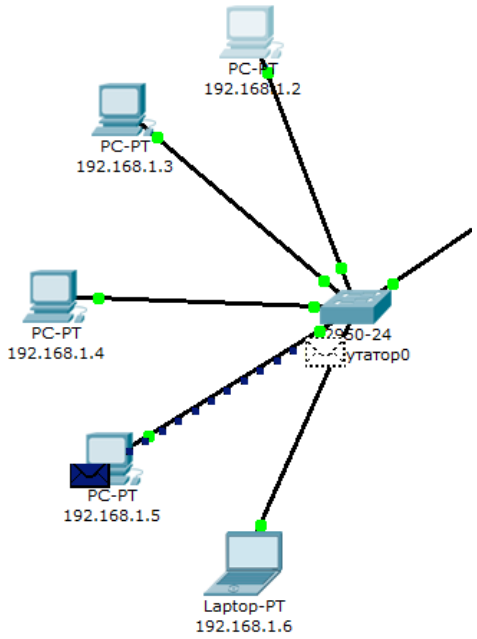
С адреса 192.168.1.2 запрос идет на коммутатор



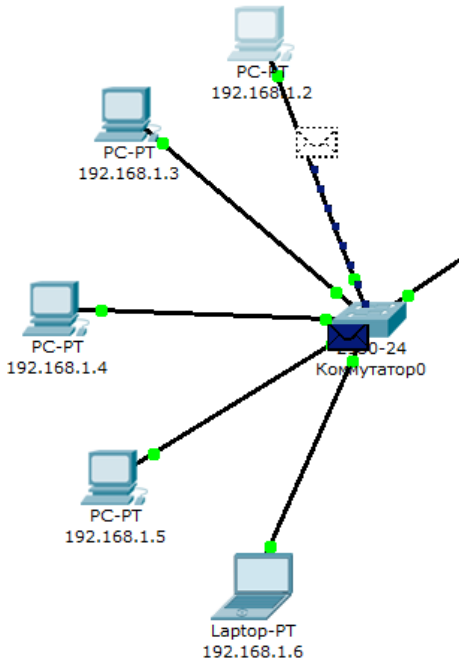
Запрос пришел на коммутатор



Далее коммутатор рассылает дальше по всем ip-адресам



ip-адрес запроса совпадает с ip-адресом 192.168.1.5



И только с ip-адреса 192.168.1.5 возвращается ответ

Рис. 44 Вид рабочей области (последовательное получение пакетов и ответ)

6. Протоколы + *(*КОПИЯ ЭКРАНА*)*

Посмотрите содержимое пакета ARP-ответа, пришедшего на хост 192.168.1.2 (рис. 45).

Рис. 45 Формат пакета ARP-ответа

7. Протоколы + *(*КОПИЯ ЭКРАНА*)*

Узел 192.168.1.5. 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. 46).

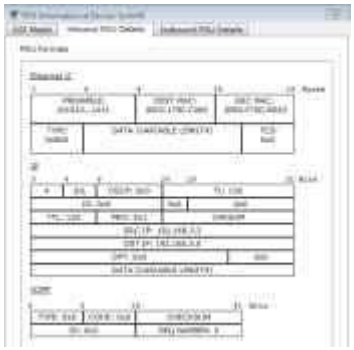


Рис. 46 Формат пакета ICMP-эхо-запроса

8. Протоколы + *(*КОПИЯ ЭКРАНА*)*

Физические адреса узлов известны. IP-адрес источника – 192.168.1.2. IP-адрес назначения – 192.168.1.5. Тип ICMP-сообщения – 8 (эхо-запрос).

Запрос производится на хост 192.168.1.5 через коммутатор (рис. 47).

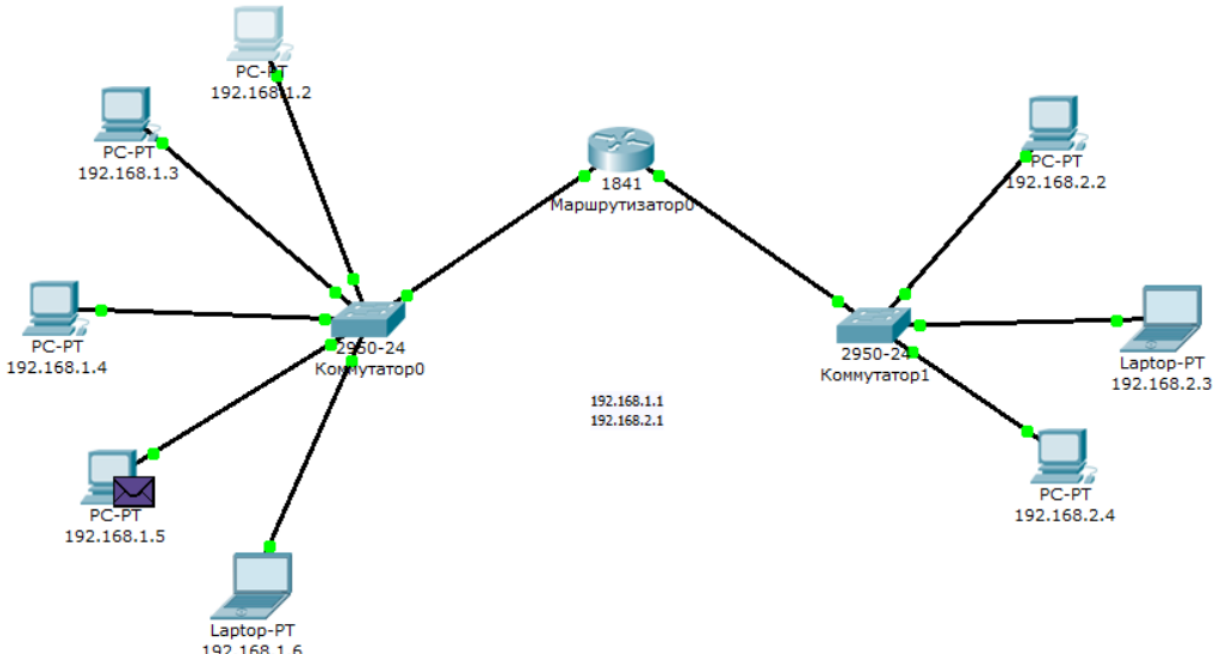


Рис. 47 Вид рабочей области

Посмотрите содержимое пакета ping-ответа, пришедшего на хост 192.168.1.2 (рис. 48).

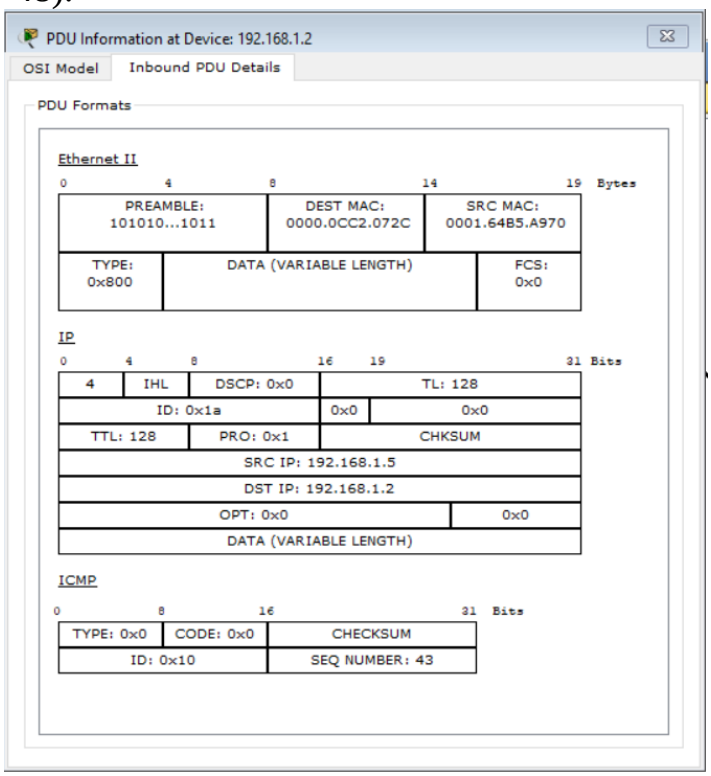


Рис. 48 Формат пакета ICMP-эхо-ответа

9. Протоколы + *(*КОПИЯ ЭКРАНА*)*

IP-адрес источника – 192.168.1.5. IP-адрес назначения – 192.168.1.2. Тип ICMP-сообщения – 0 (эхо-ответ).

Посмотрите ping-ответ в командной строке хоста 192.168.1.2 (рис. 49).

```
PC>ping 192.168.1.5

Pinging 192.168.1.5 with 32 bytes of data:

Reply from 192.168.1.5: bytes=32 time=62ms TTL=128
Reply from 192.168.1.5: bytes=32 time=63ms TTL=128
Reply from 192.168.1.5: bytes=32 time=62ms TTL=128
Reply from 192.168.1.5: bytes=32 time=63ms TTL=128

Ping statistics for 192.168.1.5:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 62ms, Maximum = 63ms, Average = 62ms
```

Рис. 49 Вывод программы ping

10. *Ping + (*КОПИЯ ЭКРАНА*)*

В окне событий так же указаны маршруты запроса ARP и ICMP: через какие устройства прошли пакеты (рис. 50).

Рис. 50 Окно событий режима симуляции

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

Теперь ARP-таблицы хостов 192.168.1.2 и 192.168.1.5 не пусты, в них содержится одна запись. Чтобы просмотреть содержимое ARP-таблицы, нужно выполнить команду

“arp –a” в командной строке.

Содержимое ARP-таблицы узла 192.168.1.2 (рис. 51):

```
PC>arp -a
  Internet Address      Physical Address      Type
  192.168.1.1           000c.8511.e701        dynamic
  192.168.1.5           0001.64b5.a970        dynamic
```

Рис. 51 ARP-таблица узла 192.168.1.2 в командной строке

11. *ARP + (*КОПИЯ ЭКРАНА*)*

Можно воспользоваться другим способом: нажать на кнопку «Inspect»  , нажать на выбранное устройство, выбрать «ARPtable» и просмотреть записи ARP-таблицы узла (рис. 52).

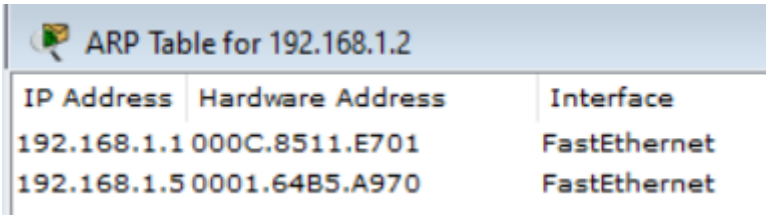


Рис. 52 ARP-таблица узла 192.168.1.2, показанная с помощью инструмента «Inspect»

12. ***ARP + (*КОПИЯ ЭКРАНА*)***

Если снова задать ping-запрос на хост 192.168.1.5, 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».

8. Сохранение созданной топологии

Выберите в MenuBar вкладку File, далее Saveas. Выберите папку на рабочем столе**…\Тема 6..**\ и сохраните под именем: **сеть6_Фамилия.pkt**. (Все файлы симулятора CiscoPacketTracer имеют расширение .pkt.)

Оформите первый лист созданного документа по образцу файла **Титульный лист.doc**: *Тема №6 «Локальные вычислительные сети»*