Лабораторная работа №1

Знакомство с Cisco Packet Tracer

Ромицына Анастасия Романовна

Содержание

Список иллюстраций

Список таблиц

1 Цель работы

Установить инструмент моделирования конфигурации сети Cisco Packet Tracer и познакомиться с его интерфейсом.

2 Выполнение лабораторной работы

Создадим новый проект с названием lab_PT-01.pkt (рис. 2.1).

Рис. 2.1: Создание нового проекта.

В рабочем пространстве разместим концентратор (Hub-PT) и четыре оконечных устройства PC Соединим оконечные устройства с концентратором прямым кабелем последовательно на каждом оконечном устройстве, зададим статические IP-адреса (рис. 2.2). 192.168.1.11 192.168.1.12 192.168.1.13 192.168.1.14 с маской подсети 255.255.255.0

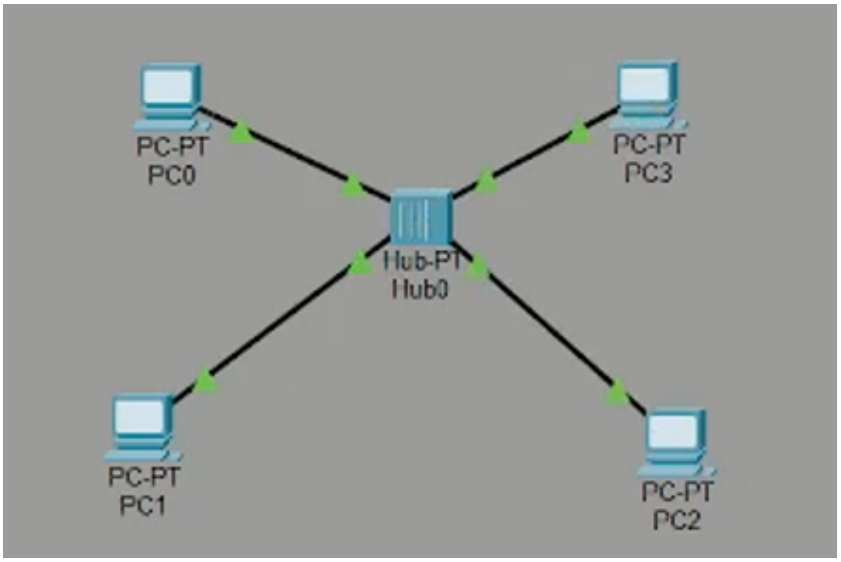

Рис. 2.2: Размещение концентратора и четырёх оконечных устройств.

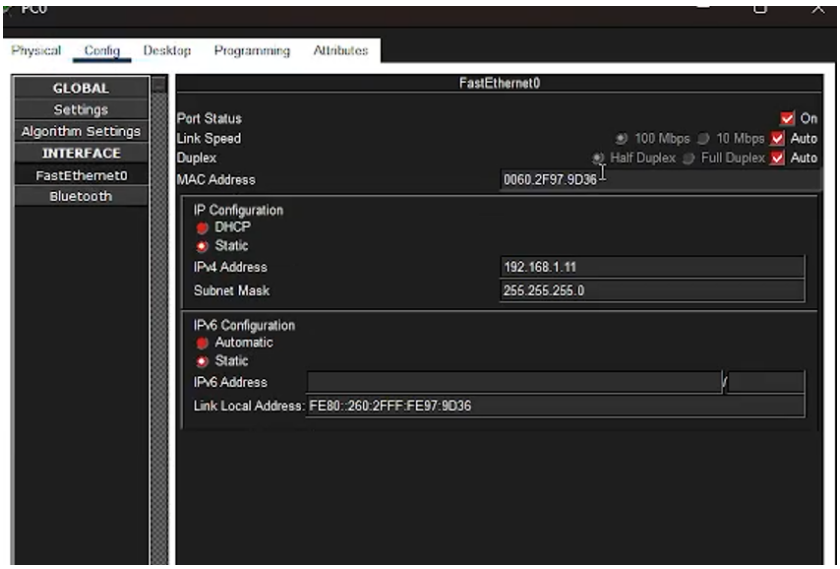

Рис. 2.3: Присвоение статического IP-адреса и маски подсети.

В основном окне проекта перейдём из режима реального времени (Realtime) в режим моделирования (Simulation) (Рис. 2.4). Выберем на панели инструментов мышкой «Add Simple PDU (P)» (Рис. 2.5) и щёлкним сначала на PC0, затем на PC2. В рабочей области появились два конверта, обозначающих пакеты, (Рис. 2.6) в списке событий на панели моделирования появились два события, относящихся к пакетам ARP и ICMP соответственно (Рис. 2.7). На панели моделирования нажмём кнопку «Play» и проследим за движением пакетов ARP и ICMP от устройства PC0 до устройства PC2 и обратно (Рис. 2.8):

Рис. 2.4: Переход из режима реального времени в режим моделирования.

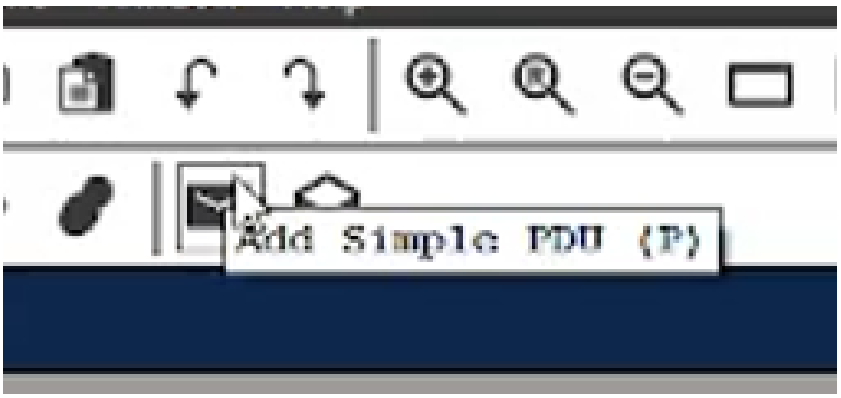

Рис. 2.5: «Add Simple PDU (P)».

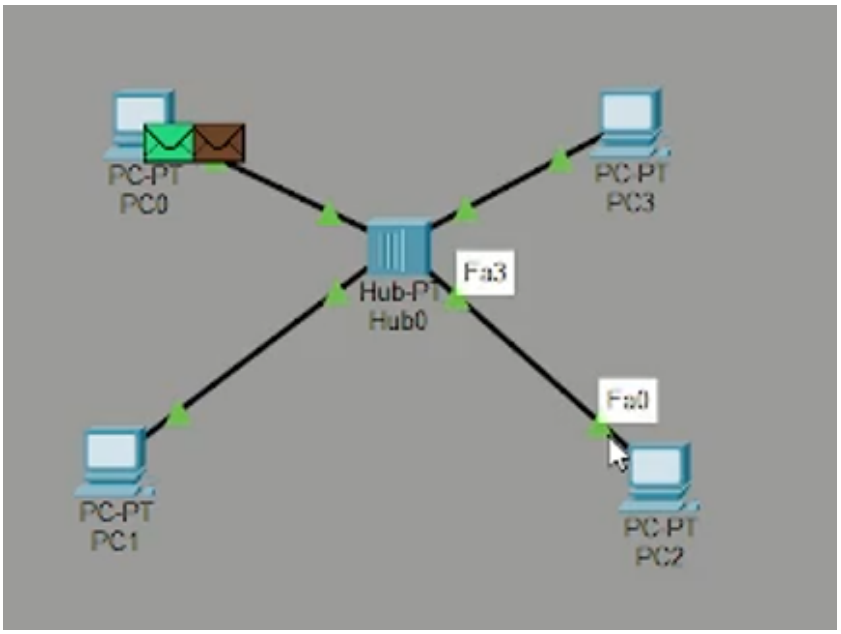

Рис. 2.6: Появление в рабочей области двух конвертов, обозначающих пакеты.

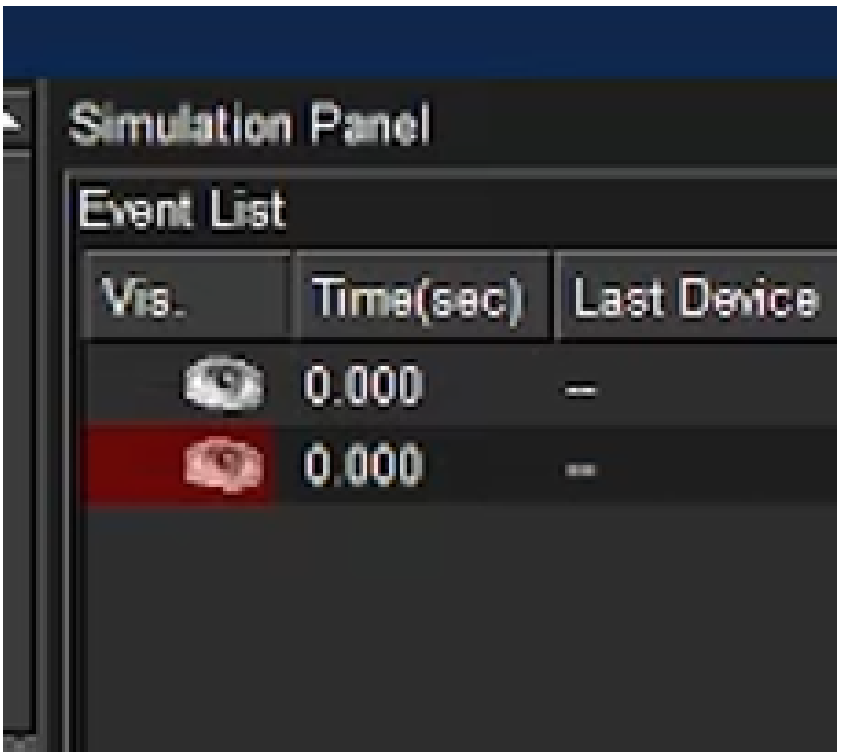

Рис. 2.7: Появление двух событий на панели моделирования, относящихся к пакетам ARP и ICMP.

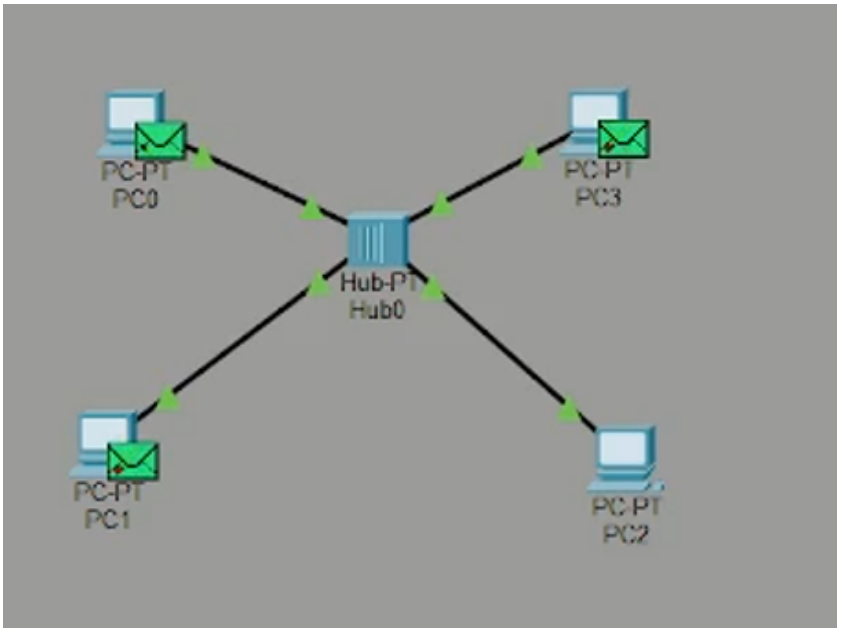

Рис. 2.8: Нажатие на панели моделирования кнопки «Play» и отслеживание движений пакетов ARP и ICMP.

Щёлкнув на строке события, откроем окно информации о PDU и изучим, что происходит на уровне модели OSI при перемещении пакета. Используя кнопку «Проверь себя» (Challenge Me) на вкладке OSI Model, ответим на вопросы (Рис. 2.9): (рис. 2.9).

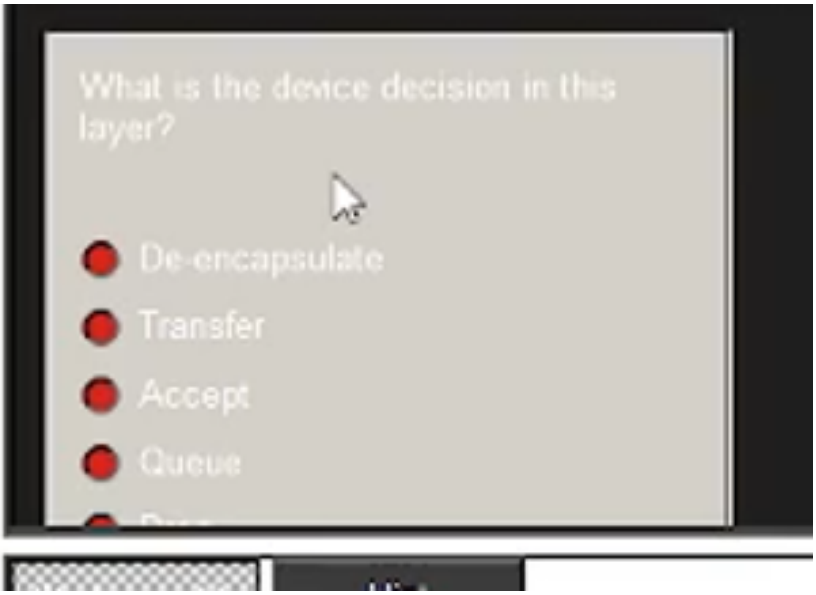

Рис. 2.9: Challenge me – ответы на вопросы.

Откроем вкладку с информацией о PDU. Исследуем структуру пакета ICMP. Опишем структуру кадра Ethernet. Какие изменения происходят в кадре Ethernet при передвижении пакета? Какой тип имеет кадр Ethernet? Опишем структуру MAC-адресов (Рис. 2.10). Кадр: EthernetII Преамбула: PREAMBLE Контрольная сумма: FCS Адрес MAC: DEST ADDR Источник: SRC ADDR Тип вложения: TYPE Длина: DATA ICMP – находится на сетевом уровне(рис. 2.10).

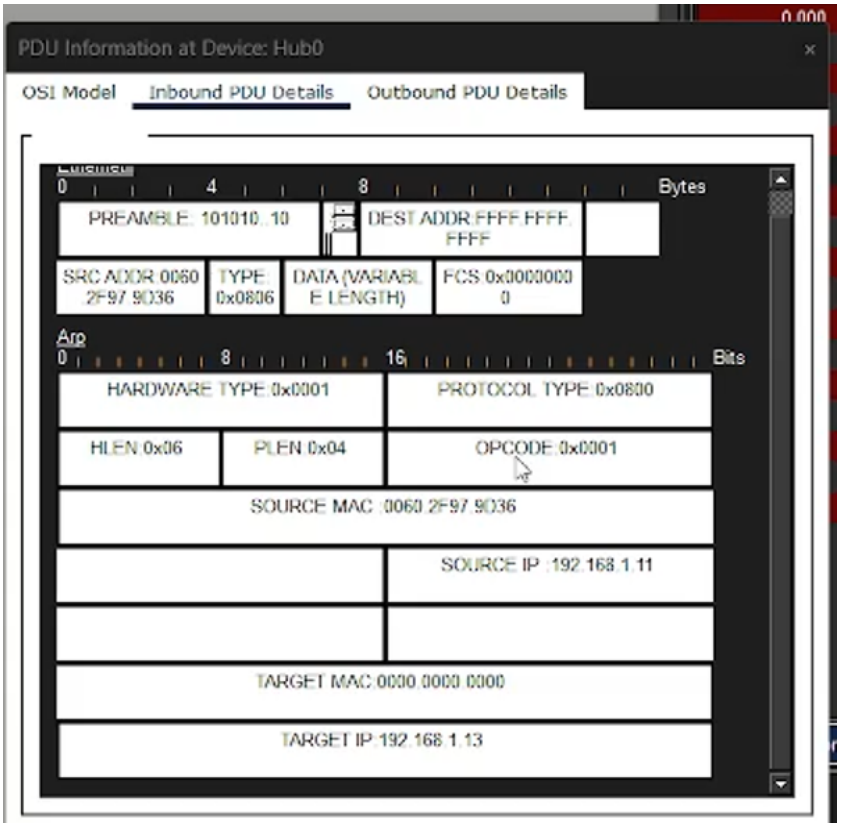

Рис. 2.10: Исследование структуры пакета ICMP.

Очистим список событий, удалив сценарий моделирования (Рис. 2.11). Выберем на панели инструментов мышкой «Add Simple PDU (P)» и щёлкнем сначала на PC0 затем на PC2 Снова выберем на панели инструментов мышкой «Add Simple PDU (P)» и щёлкнем сначала на PC2 затем на PC0 (Рис. 2.12). На панели моделирования нажмём кнопку «Play» и проследим за возникновением коллизии. В списке событий просмотрим информацию о PDU (рис. 2.13):

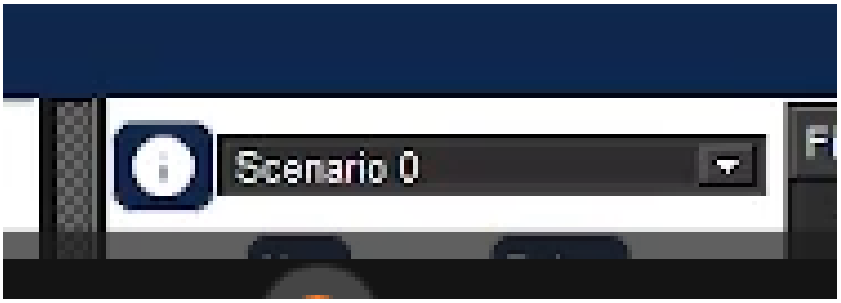

Рис. 2.11: Очистка списка событий, удалив сценарий моделирования.

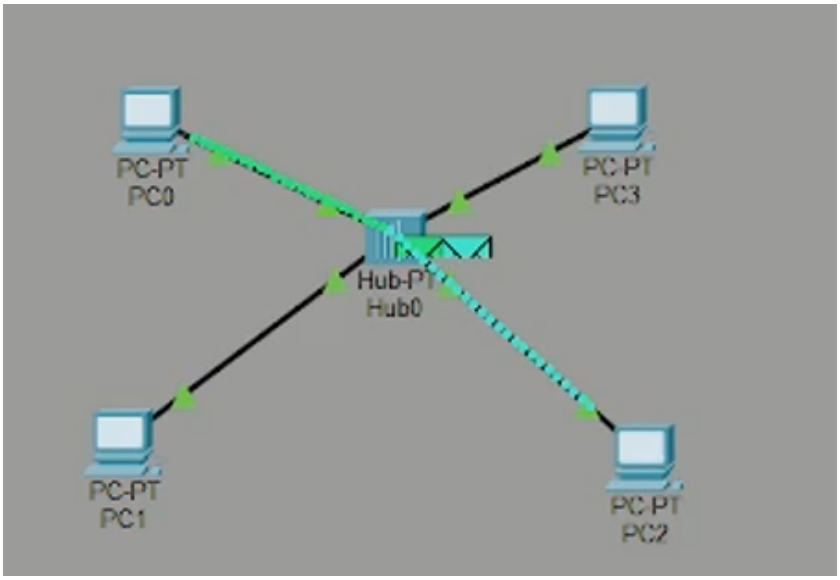

Рис. 2.12: PC0 -> PC2 PC2 -> PC0

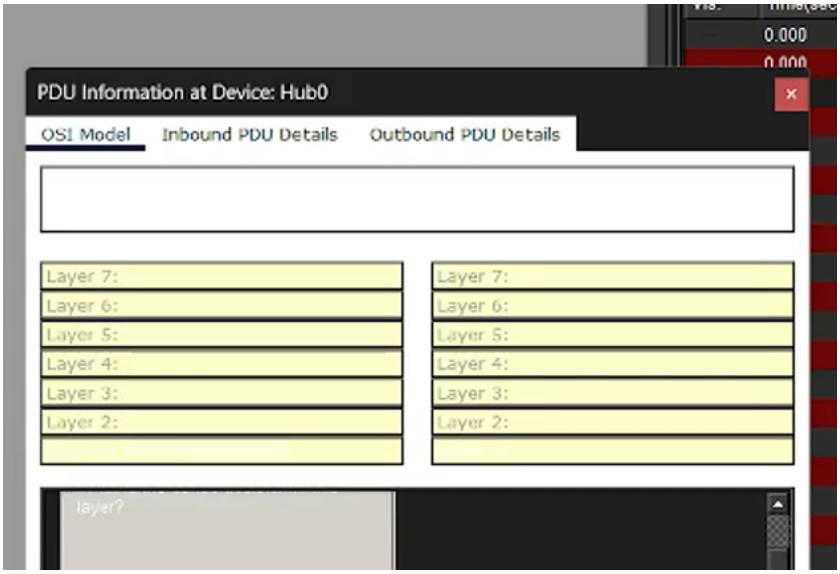

Рис. 2.13: Просмотр в списке событий информации о PDU.

Перейдём в режим реального времени (Realtime). В рабочем пространстве разместим коммутатор (Cisco 2950-24) и 4 оконечных устройства PC Соединим оконечные устройства с коммутатором прямым кабелем (Рис. 2.14). Щёлкнув последовательно на каждом оконечном устройстве, зададим статические IP-адреса 192.168.1.21, 192.168.1.22, 192.168.1.23, 192.168.1.24 с маской подсети

255.255.255.0 (Рис. 2.15).

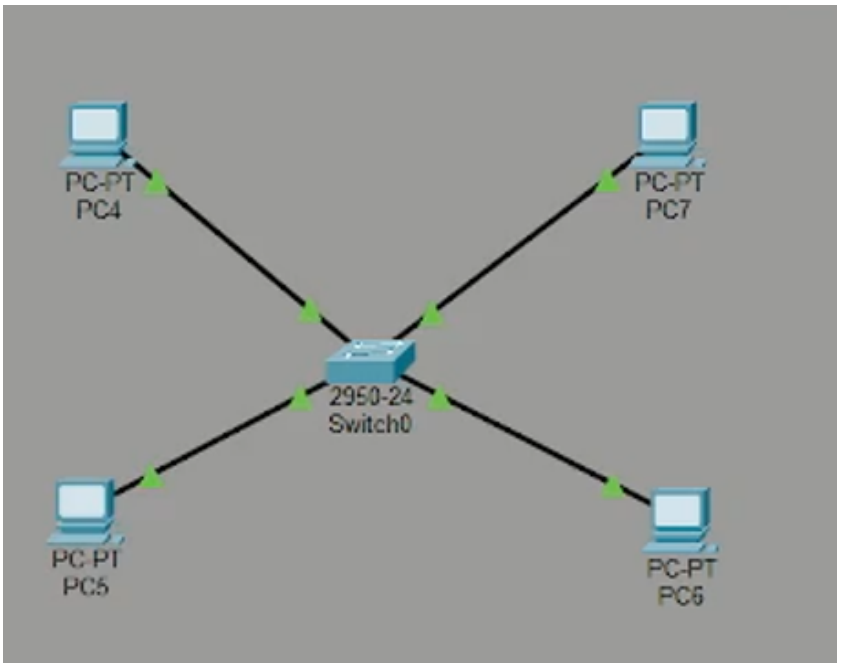

Рис. 2.14: Размещение в рабочем пространстве коммутатора и 4 оконечных устройства PC. Соединение оконечных устройств с коммутатором прямым кабелем.

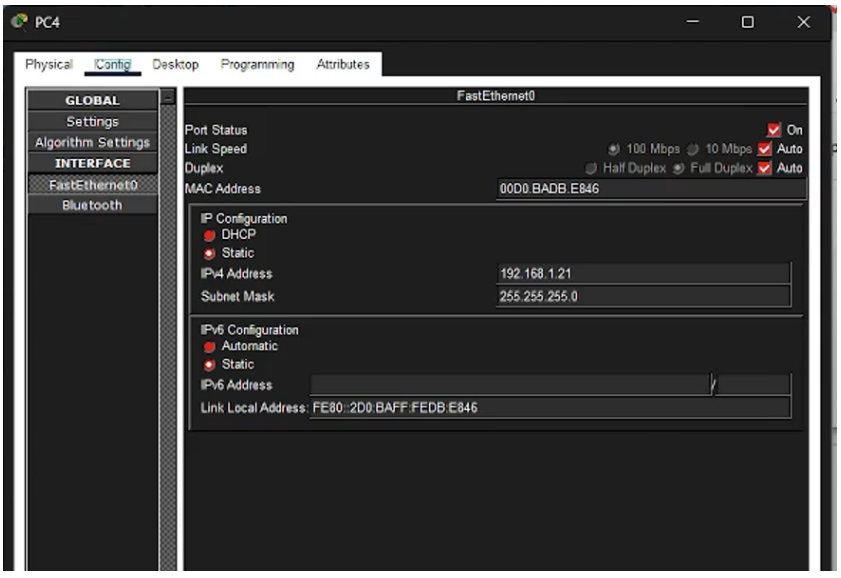

Рис. 2.15: Присвоение статического IP-адреса и маски подсети.

В основном окне проекта перейдём из режима реального времени (Realtime)

в режим моделирования (Simulation). Выберем на панели инструментов мышкой «Add Simple PDU (P)» и щёлкнем сначала на PC4, затем на PC6 . В рабочей области появились два конверта, обозначающих пакеты (Рис. 2.16), в списке событий на панели моделирования появились два события, относящихся к пакетам ARP и ICMP соответственно (Рис. 2.17). На панели моделирования нажмём кнопку «Play» и проследим за движением пакетов ARP и ICMP от устройства PC4 до устройства PC6 и обратно (отличие заключается в том, что у нас происходит запоминание нужного компьютера, то есть нет рассылки всем, после первой такой отправки).

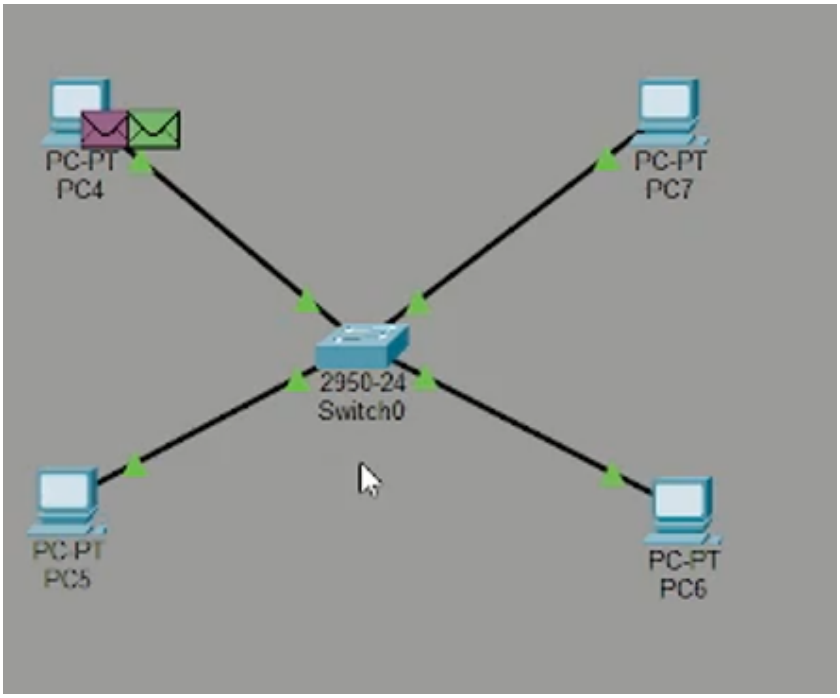

Рис. 2.16: Появление в рабочей области двух конвертов, обозначающих пакеты.

Рис. 2.17: Появление в списке событий на панели моделирования двух событий, относящихся к пакетам ARP и ICMP.

Очистим список событий, удалив сценарий моделирования. Выберем на панели инструментов мышкой «Add Simple PDU (P)» и щёлкнем сначала на PC4- ,

затем на PC6 Снова выберем на панели инструментов мышкой «Add Simple PDU (P)» и щёлкнем сначала на PC6, затем на PC4 (Рис. 2.18). На панели моделирования нажмём кнопку «Play» и проследим за движением пакетов.

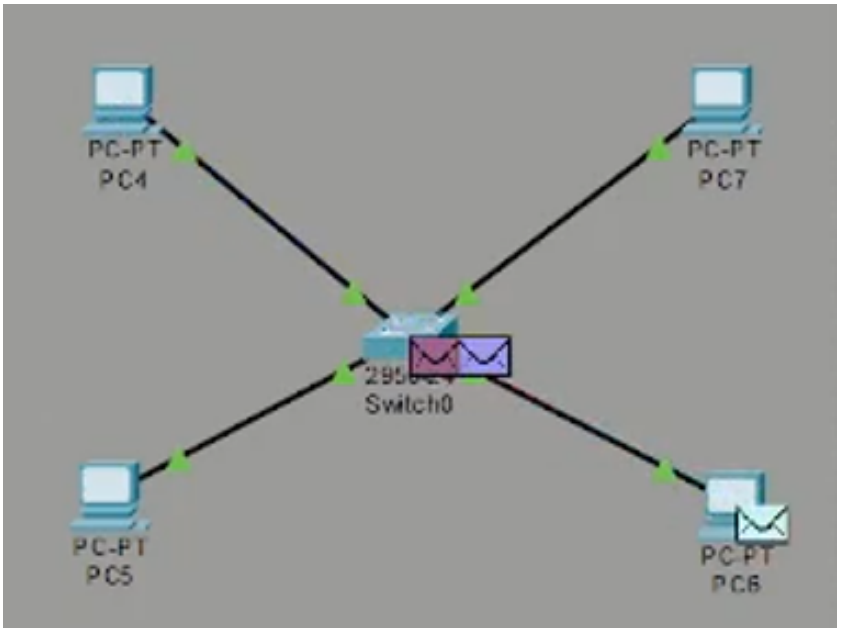

Рис. 2.18: PC4 -> PC6. PC6 -> PC4.

Перейдём в режим реального времени (Realtime). В рабочем пространстве соединим кроссовым кабелем концентратор и коммутатор (Рис. 2.19). Перейдём в режим моделирования (Simulation). Очистим список событий, удалив сценарий моделирования. Выберем на панели инструментов мышкой «Add Кулябов Simple PDU (P)» и щёлкнем сначала на PC0-ismakhorin, затем на PC4-ismakhorin. Снова выберем на панели инструментов мышкой «Add Simple PDU (P)» и щёлкнем сначала на PC4-ismakhorin, затем на PC0-ismakhorin. На панели моделирования нажмём кнопку «Play» и проследим за движением пакетов (Рис. 2.20):

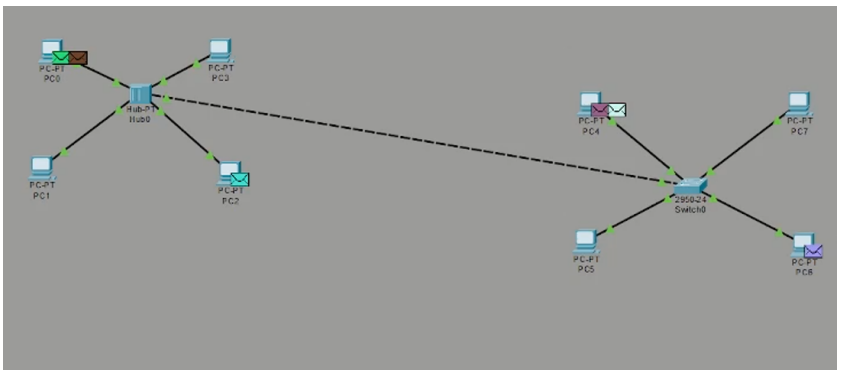

Рис. 2.19: Соединение в рабочем пространстве кроссовым кабелем концентратора и коммутатора.

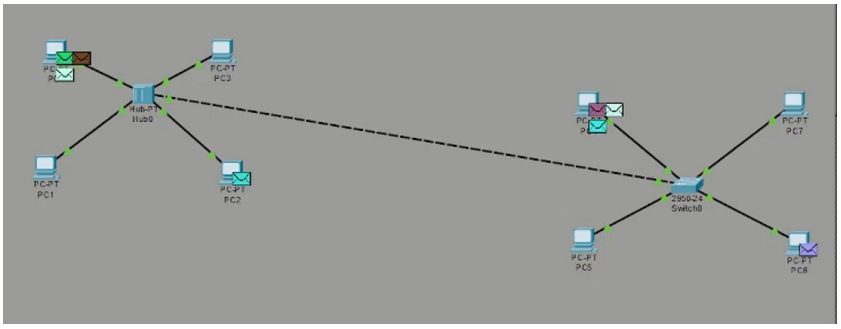

Рис. 2.20: PC0 -> PC4. PC4 -> PC0.

Очистим список событий, удалив сценарий моделирования. На панели моделирования нажмём «Play» и в списке событий получим пакеты STP. Исследуем структуру STP. Опишем структуру кадра Ethernet в этих пакетах (Рис. 2.21): Работает поверх Ethernet 802.3/LLC Преамбула: PREAMBLE Контрольная сумма: FCS Адрес назначения: DEST ADDR Адрес источник: SRC ADDR Тип вложения: TYPE Длина: DATA STP– находится на канальном уровне

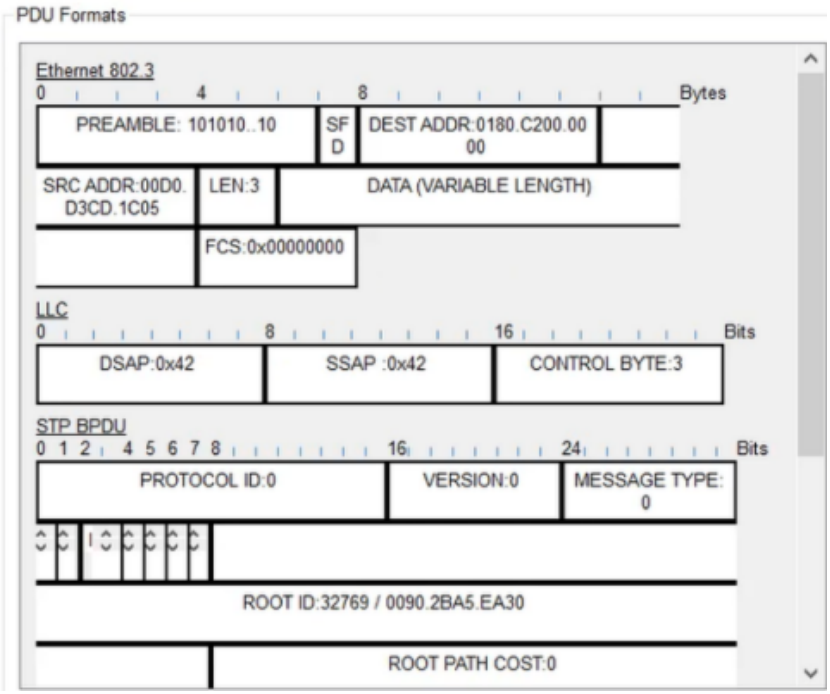

Рис. 2.21: Исследование структуры STP.

Перейдём в режим реального времени (Realtime). В рабочем пространстве добавим маршрутизатор (Cisco 2811). Соединим прямым кабелем коммутатор и маршрутизатор (Рис. 2.22). Щёлкнем на маршрутизаторе и на вкладке его конфигурации пропишем статический IP-адрес 192.168.1.254 с маской 255.255.255.0, активируем порт, поставив галочку «On» напротив «Port Status»(Рис. 2.23):

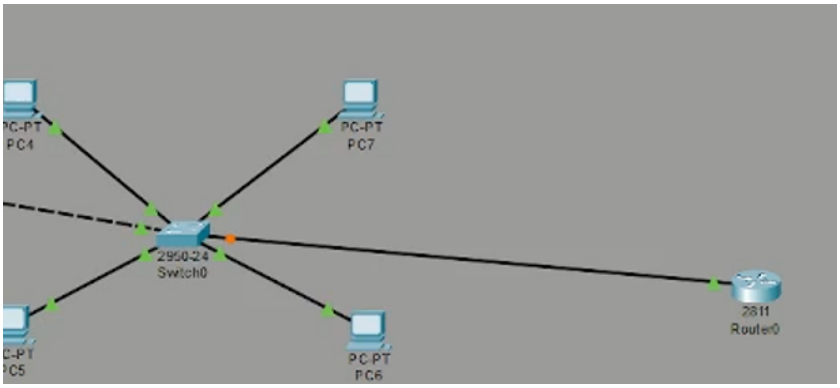

Рис. 2.22: Добавление в рабочем пространстве маршрутизатора Cisco 2811 и соединение прямым кабелем коммутатора и маршрутизатора.

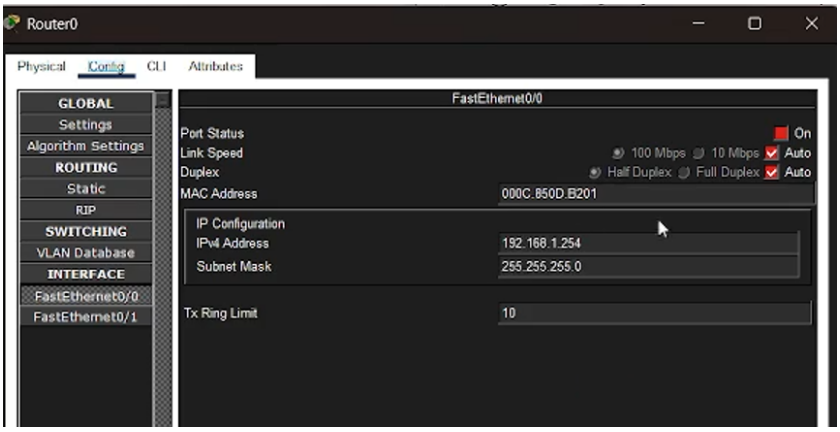

Рис. 2.23: Присвоение статического IP-адреса 192.168.1.254 с маской 255.255.255.0, активация порта.

Перейдём в режим моделирования (Simulation). Очистим список событий, удалив сценарий моделирования. Выберем на панели инструментов мышкой «Add Simple PDU (P)» и щёлкнем сначала на PC3-ismakhorin, затем на маршрутизатор (Рис. 2.24). На панели моделирования нажмём кнопку «Play» и проследим за движением пакетов ARP, ICMP, STP и CDP. Исследуем структуру пакета CDP, опишем структуру кадра Ethernet. Какой тип имеет кадр Ethernet? (Рис. 2.25).

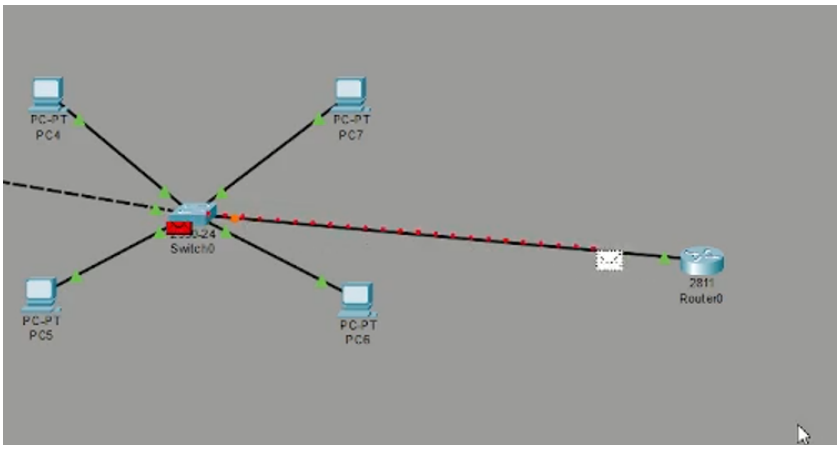

Рис. 2.24: PC3 -> маршрутизатор.

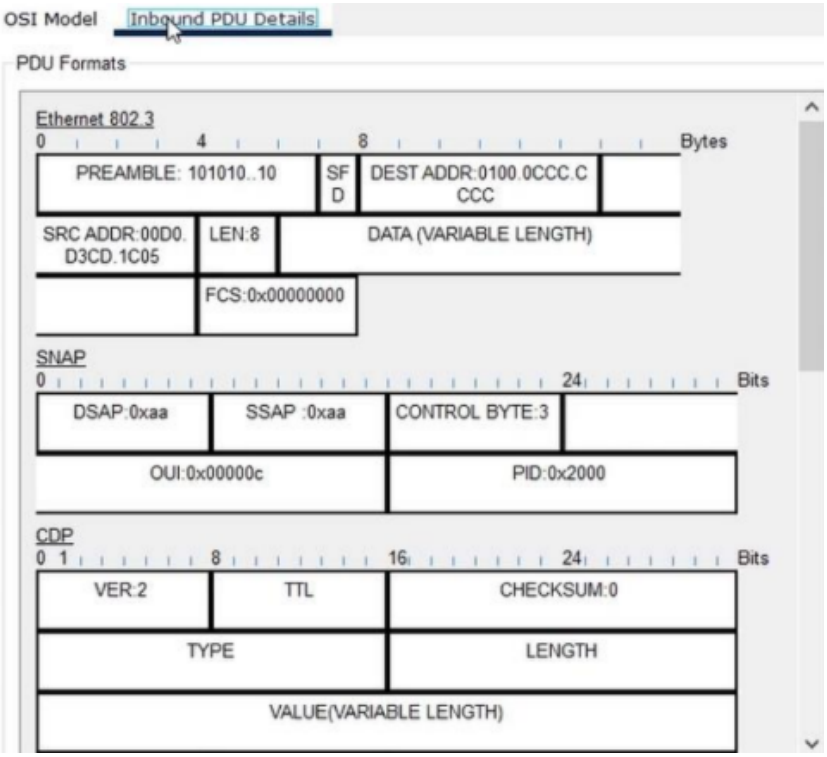

Рис. 2.25: Исследование структуры пакета CDP.

3 Выводы

В ходе выполнения лабораторной работы мы научились устанавливать инструмент моделирования конфигурации сети Cisco Packet Tracer без учётной записи и познакомились с его интерфейсом.

4 Ответы на контрольные вопросы:

1. Дайте определение следующим понятиям: концентратор, коммутатор, маршрутизатор, шлюз (gateway). В каких случаях следует использовать тот или иной тип сетевого оборудования? Концентратор (Hub): концентратор является устройством, которое принимает данные с одного устройства сети и передает их всем остальным устройствам в сети. Он работает на физическом уровне модели OSI (Open Systems Interconnection), просто усиливая сигнал и передавая его по всем портам. Концентратор не имеет интеллекта для анализа данных или управления трафиком. Обычно используется в небольших сетях или для расширения количества портов в сети. Коммутатор (Switch): коммутатор также работает на канальном уровне OSI и способен анализировать адреса MAC (Media Access Control) устройств, подключенных к нему. В отличие от концентратора, коммутатор передает данные только тому устройству, для которого они предназначены, что делает его более эффективным по сравнению с концентратором. Коммутаторы обычно используются в сетях с высокой пропускной способностью, где требуется эффективное управление трафиком и безопасностью. Маршрутизатор (Router): маршрутизатор работает на сетевом уровне OSI и способен анализировать IP-адреса устройств в сети. Он принимает решения о передаче данных между различными сетями на основе IP-адресации и информации о маршрутах. Маршрутизаторы используются для соединения различных сетей (например, локальной сети и Интернета) и обеспечения маршрутизации данных между ними.

Шлюз (Gateway): шлюз - это устройство, которое соединяет различные сети с разными протоколами, форматами данных или архитектурой. В контексте сетей Шлюз часто используется как точка доступа к другой сети, например, для доступа к Интернету из локальной сети. Шлюз выполняет преобразование данных и управляет коммуникацией между разными сетями. В зависимости от конкретного применения, шлюз может быть представлен как программное или аппаратное оборудование. Выбор типа сетевого оборудования зависит от конкретных потребностей сети: Для простых сетей малого размера без особых требований к управлению трафиком можно использовать концентраторы. Для сетей среднего и большого размера, где требуется управление трафиком и безопасность, рекомендуется использовать коммутаторы. Для подключения сетей различных типов и обеспечения маршрутизации данных между ними необходимы маршрутизаторы. Шлюзы используются там, где требуется соединение сетей с разными протоколами или доступ к внешним сетям, таким как Интернет. 2 Дайте определение следующим понятиям: ip-адрес, сетевая маска, broadcast адрес. IP-адрес (Internet Protocol Address): IP-адрес - это числовая метка присвоенная каждому устройству в компьютерной сети,использующей протокол Интернета (IP). Он используется для идентификации и адресации устройств в сети, позволяя маршрутизаторам правильно направлять пакеты данных к их назначению. IP-адрес состоит из 32 бит (для IPv4) или 128 бит (для IPv6) и представляется в виде четырех чисел, разделенных точками (для IPv4) или в виде группы шестнадцатеричных чисел, разделенных двоеточиями (для IPv6). Сетевая маска (Network Mask): сетевая маска используется для определения, какая часть IP-адреса относится к сети, а какая - к узлу в этой сети. Она представляет собой набор битов, который определяет количество битов, зарезервированных для идентификации сети, в IP-адресе. Обычно сетевая маска записывается вместе с IP-адресом, используя формат, подобный

“192.168.1.0/24”, где /24 указывает на количество битов, отведенных для сети. Broadcast-адрес: Broadcast-адрес - это специальный адрес в сети, который используется для отправки данных всем устройствам в этой сети. Когда устройство отправляет пакет данных на broadcast-адрес, все устройства в этой сети получают этот пакет. Broadcast-адрес для IPv4 обычно имеет значение, в котором все биты хоста установлены в 1, например, для сети 192.168.1.0 с сетевой маской /24 broadcast-адрес будет 192.168.1.255. Для IPv6 broadcast-адреса не существует, вместо этого используется multicast для доставки данных на несколько устройств. 3 Как можно проверить доступность узла сети? Ping (ICMP Echo Request): Ping - это самый распространенный способ проверки доступности узла. Это делается отправкой ICMP (Internet Control Message Protocol) Echo Request пакета на IP-адрес узла и ожиданием ответа. Если узел доступен, он отправит обратно ICMP Echo Reply пакет. Traceroute (или traceroute6 для IPv6): Этот инструмент используется для определения маршрута, который пакеты данных пройдут от отправителя до получателя. Он посылает серию пакетов увеличивающимся TTL (Time-to-Live) и анализирует ответы для определения промежуточных узлов. Это позволяет выявить места, где возникают проблемы в маршрутизации. Проверка порта (Port Scan): Если вам нужно не только убедиться, что узел отвечает на пинг, но и проверить, работает ли на нем конкретное сетевое приложение, вы можете выполнить сканирование портов. Существуют различные инструменты, такие как Nmap, которые позволяют сканировать порты на удаленном узле и определить, какие порты открыты и доступны для подключения. Использование специализированных сетевых инструментов: Существует множество специализированных инструментов управления сетями, которые предоставляют информацию доступности узлов, их статусе и производительности. Это могут быть мониторинговые системы, такие как Zabbix, Nagios, Prometheus, или программное обеспечение от

производителей сетевого оборудования. Использование интерфейсов управления сетевым оборудованием: Многие сетевые устройства предоставляют интерфейсы управления или CLI (Command Line Interface), через которые можно проверить доступность узлов в сети, например, используя команды ping или traceroute на маршрутизаторе. Выбор метода зависит от конкретных требований и характеристик вашей сетевой инфраструктуры.

Список литературы