Отчёт по лабораторной работе 1

Знакомство с Cisco Packet Tracer

Седохин Даниил Алексеевич

Содержание

Список иллюстраций

Список таблиц

1 Цель работы

Установка инструмента моделирования конфигурации сети Cisco Packet Tracer, знакомство с его интерфейсом.

2 Задание

1. Установить на домашнем устройстве Cisco Packet Tracer.
2. Постройте простейшую сеть в Cisco Packet Tracer, проведите простейшую настройку оборудования.

3 Выполнение лабораторной работы

Начиная с версии 7 для работы Packet Tracer требуется наличие учётной записи в Network Academy: https://www.netacad.com/ или https:// skillsforall.com/. При запуске Packet Tracer на компьютере без доступа к сети учётная запись не проверяется.

Установите в вашей операционной системе Cisco Packet Tracer Для ОС типа Windows требуется блокировать для Packet Tracer доступ в Интернет:

Откройте «Панель управления».

Откройте пункт «Брандмауэр» Защитника Windows или просто Брандмауэр Windows.

В открывшемся окне нажмите «Дополнительные параметры». Откроется окно брандмауэра в режиме повышенной безопасности.

Выберите «Правило для исходящего подключения», а потом — «Создать правило».

Выберите «Для программы» и нажмите «Далее».

Укажите путь к исполняемому файлу программы, которой нужно запретить доступ в Интернет. В данном случае путь к установленному у вас в ОС Packet Tracer.

В следующем окне оставьте отмеченным пункт «Блокировать подключение».

В следующем окне отметьте, для каких сетей выполнять блокировку. Если для любых, то оставьте отмеченными все пункты.

Укажите понятное для вас имя правила и нажмите «Готово».

Запустите Packet Tracer. При корректной настройке после запуска не должна требоваться аутентификация. (рис. 3.1).

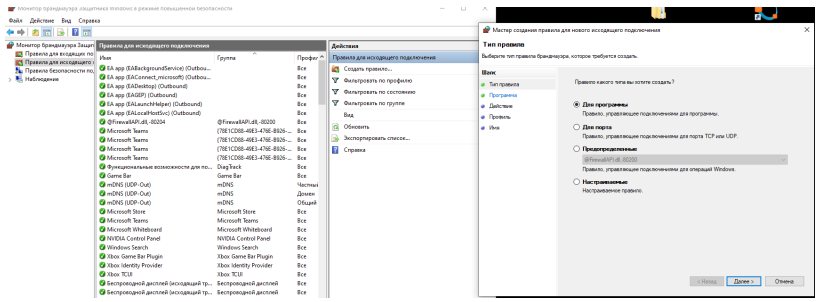

Рисунок 3.1: Установка Packet Tracer и блокировка для него доступа в Интернет

Создайте новый проект (например, lab_PT-01.pkt).

В рабочем пространстве разместите концентратор (Hub-PT) и четыре оконечных устройства PC. Соедините оконечные устройства с концентратором прямым кабелем (рис. 3.2).

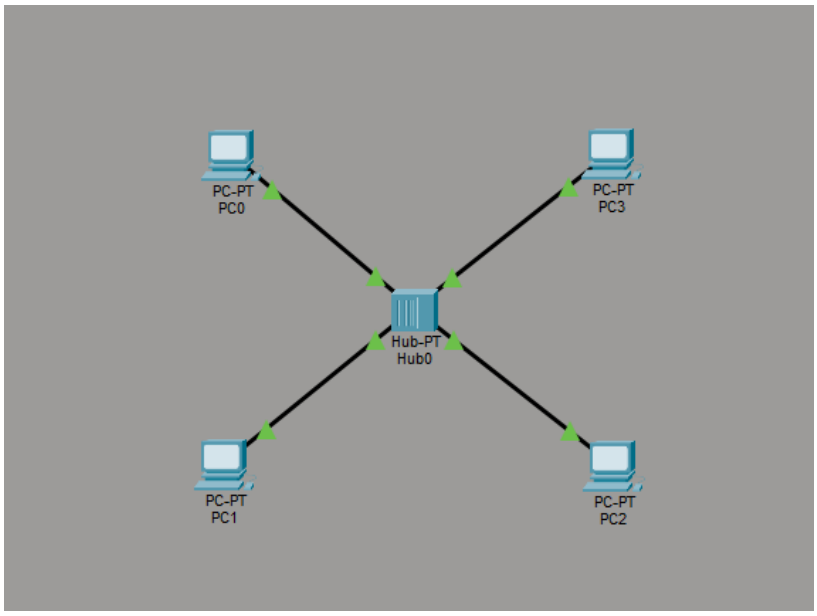

Рисунок 3.2: Создание нового проекта и воспроизведение топологии сети

Щёлкнув последовательно на каждом оконечном устройстве, задайте статические IP-адреса 192.168.1.11, 192.168.1.12, 192.168.1.13, 192.168.1.14 с маской подсети 255.255.255.0 (рис. 3.3).

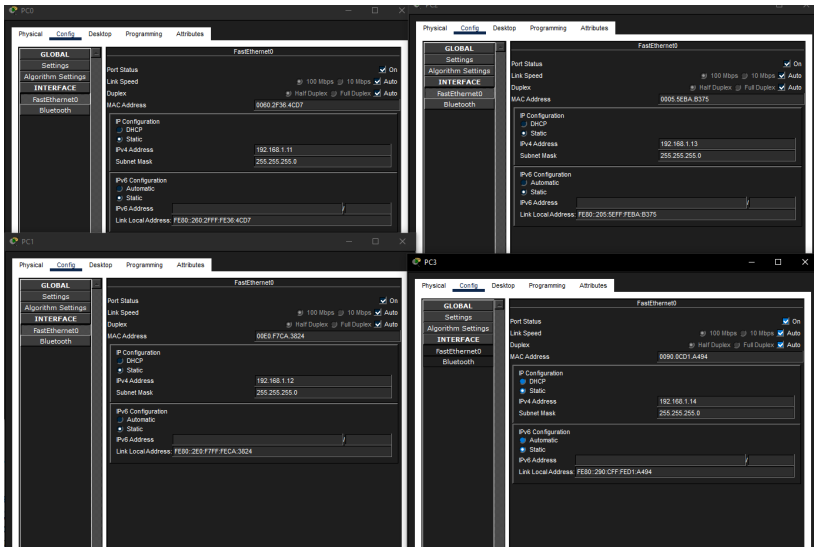

Рисунок 3.3: Задаем ip адреса и маски подсети

В основном окне проекта перейдите из режима реального времени (Realtime) в режим моделирования (Simulation). Выберите на панели инструментов мышкой «Add Simple PDU (P)» и щёлкните сначала на PC0, затем на PC2.

В рабочей области должны будут появится два конверта, обозначающих пакеты, в списке событий на панели моделирования должны будут появиться два события, относящихся к пакетам ARP и ICMP соответственно На панели моделирования нажмите кнопку «Play» и проследите за движением пакетов ARP и ICMP от устройства PC0 до устройства PC2 и обратно. (рис. 3.4).

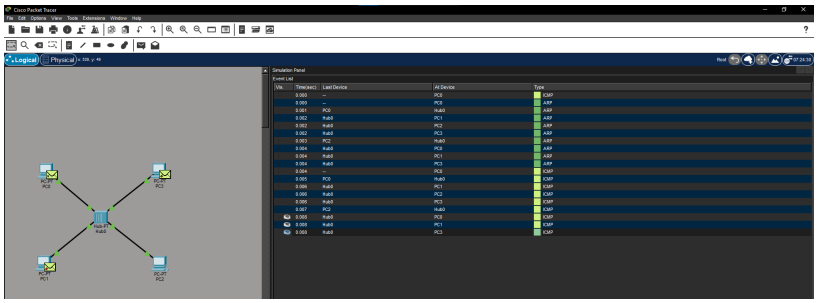

Рисунок 3.4: Просмотр путей движения пакетов ARP и ICMP от PC0 до PC2 и обратно

Щёлкнув на строке события, откройте окно информации о PDU и изучите, что происходит на уровне модели OSI при перемещении пакета (рис. 3.5).

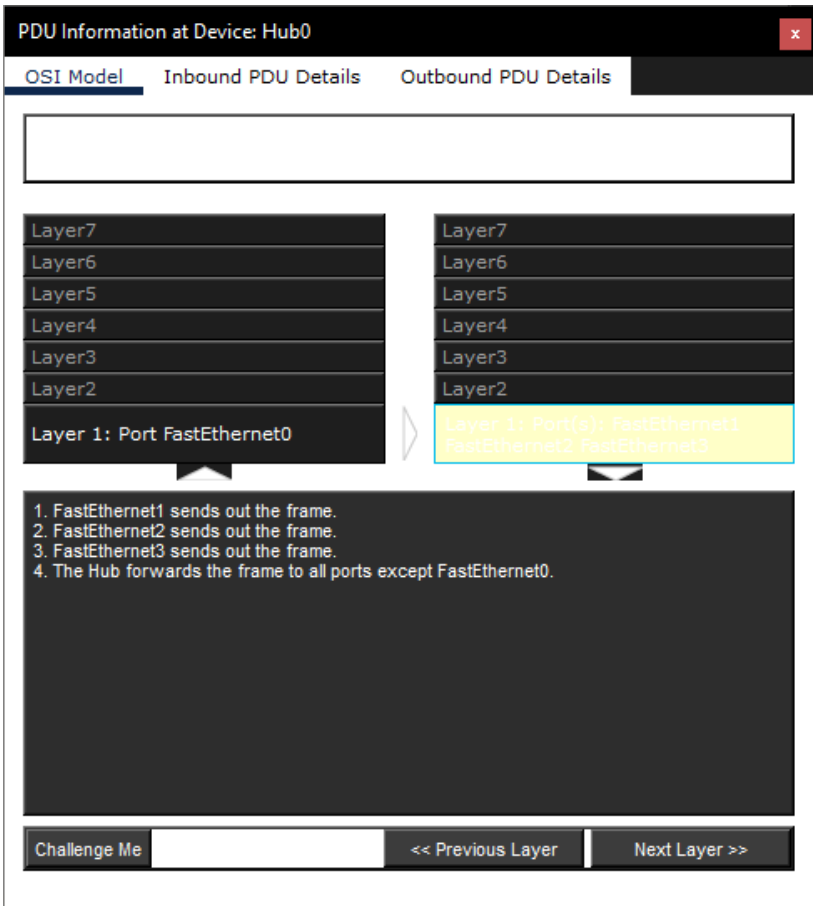

Рисунок 3.5: Просмотр модели OSI при перемещении пакета

Откройте вкладку с информацией о PDU Исследуйте структуру пакета ICMP. (рис. 3.6).

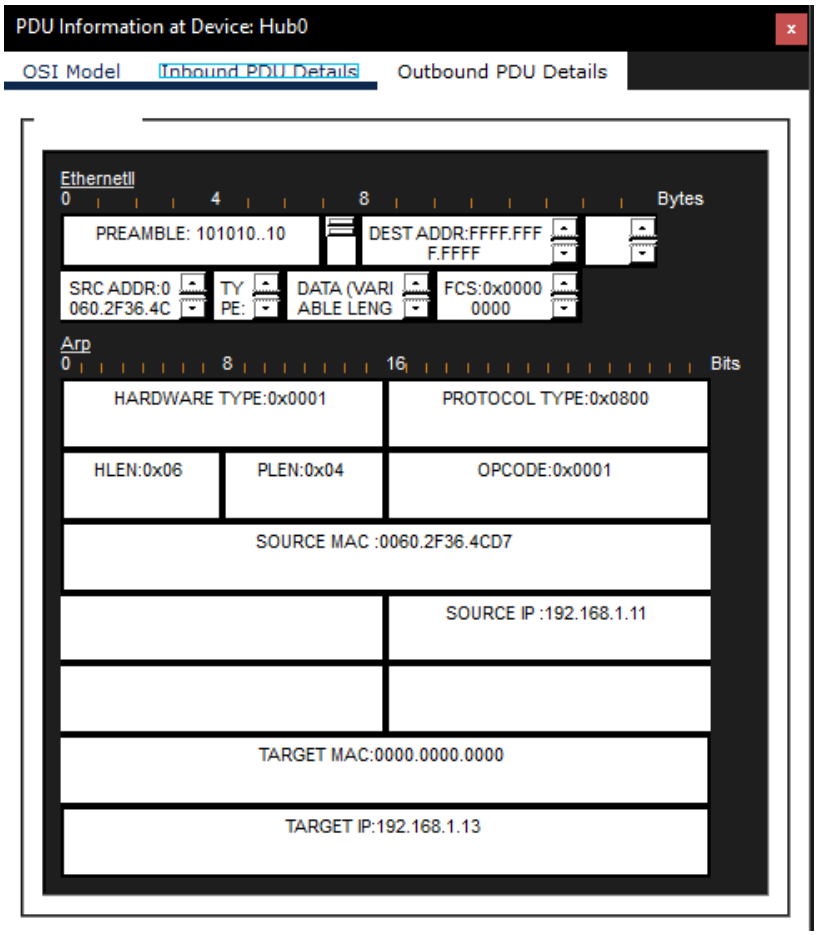

Рисунок 3.6: Просмотр структуры пакета ICMP

Очистите список событий, удалив сценарий моделирования. Выберите на панели инструментов мышкой «Add Simple PDU (P)» и щёлкните сначала на PC0, затем на PC2. Снова выберите на панели инструментов мышкой «Add Simple PDU (P)» и щёлкните сначала на PC2, затем на PC0. На панели моделирования нажмите кнопку «Play» и проследите за возникновением коллизии (рис. 3.7).

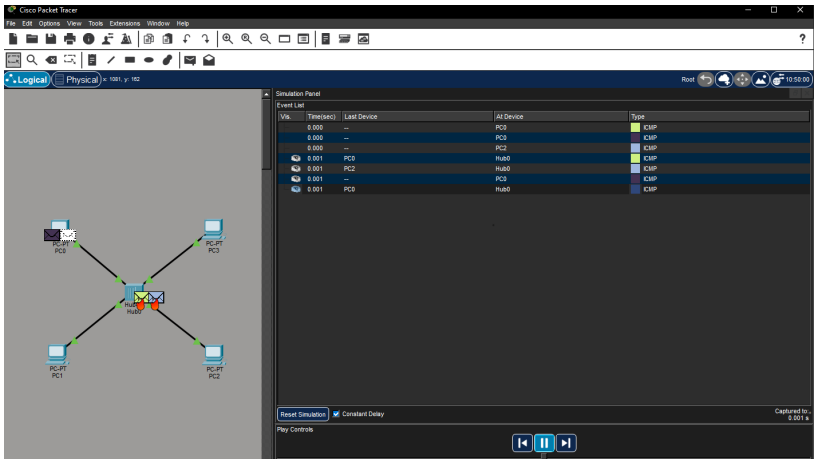

Рисунок 3.7: Моделирование ситуации с возникновением коллизии

В списке событий посмотрите информацию о PDU. Кадр Ethernet (L2)

DEST ADDR: 0060.2F36.4CD7 — MAC-адрес получателя (компьютер с IP 192.168.1.11).

SRC ADDR: 0005.5EBA.... — MAC-адрес отправителя (компьютер с IP 192.168.1.13).

Это уже не широковещательный кадр, а адресный (unicast).

2. Пакет IP (L3)

SRC IP: 192.168.1.13 — отправитель.

DST IP: 192.168.1.11 — получатель.

PRO: 0x01 — протокол ICMP.

TTL: 255 — время жизни пакета.

3. Сообщение ICMP (L4)

TYPE: 0x08 — Echo Request (ping-запрос).

CODE: 0x00 — стандартный код.

SEQ NUMBER: 1 — первый пакет в серии.

Вывод: Это ping-запрос от компьютера 192.168.1.13 к компьютеру 192.168.1.11. MAC-адреса уже известны (ARP-запрос ранее отработал), поэтому пакет идёт сразу получателю. (рис. 3.8).

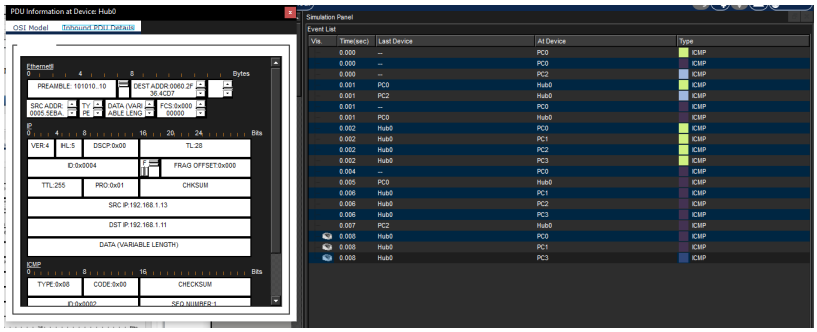

Рисунок 3.8: Просмотр информации о PDU

Перейдите в режим реального времени (Realtime). В рабочем пространстве разместите коммутатор (например Cisco 2950-24) и 4 оконечных устройства PC. Соедините оконечные устройства с коммутатором прямым кабелем. Щёлкнув последовательно на каждом оконечном устройстве, задайте 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. 3.9).

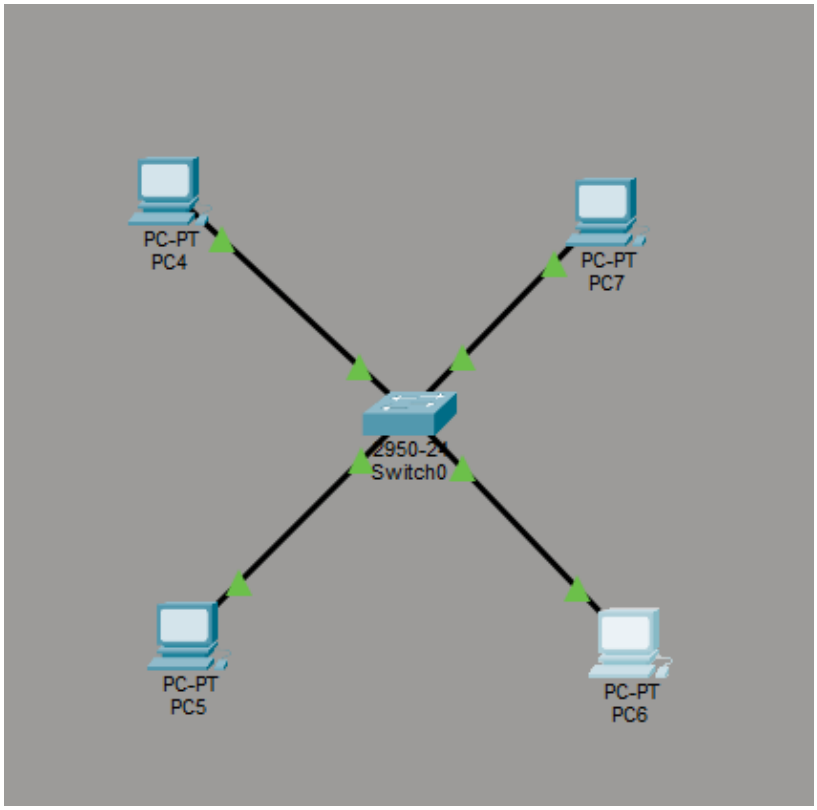

Рисунок 3.9: Воспроизведение новой топологии сети с коммутатором

В основном окне проекта перейдите из режима реального времени (Realtime) в режим моделирования (Simulation). Выберите на панели инструментов мышкой «Add Simple PDU (P)» и щёлкните сначала на PC4, затем на PC6.

В рабочей области должны будут появится два конверта, обозначающих пакеты, в списке событий на панели моделирования должны будут появиться два события, относящихся к пакетам ARP и ICMP соответственно. На панели моделирования нажмите кнопку «Play» и проследите за движением пакетов ARP и ICMP от устройства PC4 до устройства PC6 и обратно. Устройство 192.168.1.21 пингует устройство 192.168.1.24.

Это уже второй пакет (Seq=2).

MAC-адреса известны (нет ARP-запроса).

Пакет идёт через коммутатор (Switch0), который просто передаст его на нужный порт по таблице MAC-адресов. (рис. 3.10).

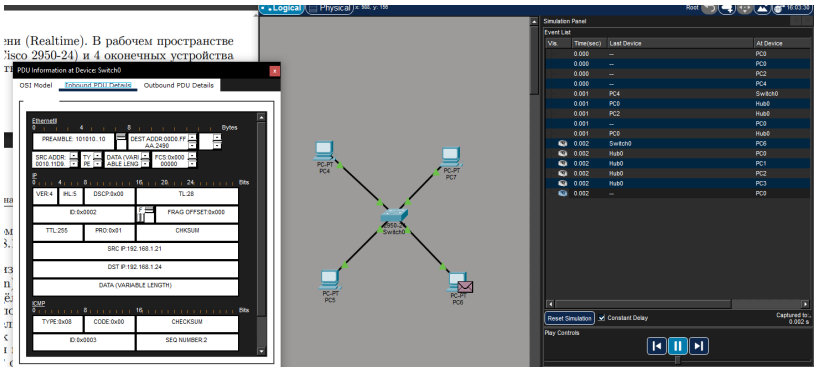

Рисунок 3.10: Просмотр пути пакетов ARP и ICMP от PC4 до PC6

Очистите список событий, удалив сценарий моделирования. Выберите на панели инструментов мышкой «Add Simple PDU (P)» и щёлкните сначала на PC4, затем на PC6. Снова выберите на панели инструментов мышкой «Add Simple PDU (P)» и щёлкните сначала на PC6, затем на PC4. На панели моделирования нажмите кнопку «Play» и проследите за движением пакетов. (рис. 3.11).

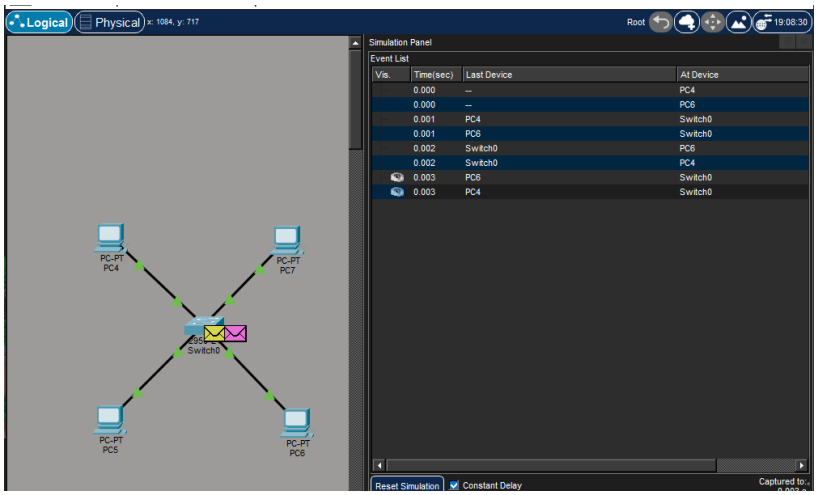

Рисунок 3.11: Моделирование ситуации с возможной коллизией, но с коммутатором

Перейдите в режим реального времени (Realtime). В рабочем пространстве соедините кроссовым кабелем концентратор и коммутатор. Перейдите в режим моделирования (Simulation). Очистите список событий, удалив сценарий моделирования. Выберите на панели инструментов мышкой «Add Simple PDU (P)» и щёлкните сначала на PC0, затем на PC4. Снова выберите на панели инструментов мышкой «Add Simple PDU (P)» и щёлкните сначала на PC4, затем на PC0. На панели моделирования нажмите кнопку «Play» и проследите за движением пакетов. Коллизия возникает из-за работы концентраторов:

Несколько устройств (PC1, PC3, PC5 и др.) начали передачу одновременно (на метке времени 0.000).

Концентратор — это «тупое» устройство. Он не умеет управлять очередностью, а просто тупо повторяет сигнал сразу во все порты.

Когда два сигнала сталкиваются в среде передачи (на хабе), возникает коллизия. Данные искажаются, и никто никого не слышит.

Почему потом пакеты всё же доходят:

После коллизии срабатывает механизм CSMA/CD (Carrier Sense Multiple Access with Collision Detection).

Устройства «замолкают», ждут случайный промежуток времени и пытаются

отправить данные заново.

Если повезёт, и в новый момент времени канал окажется свободен (передаёт кто-то один), пакет успешно добирается до адресата. (рис. 3.12).

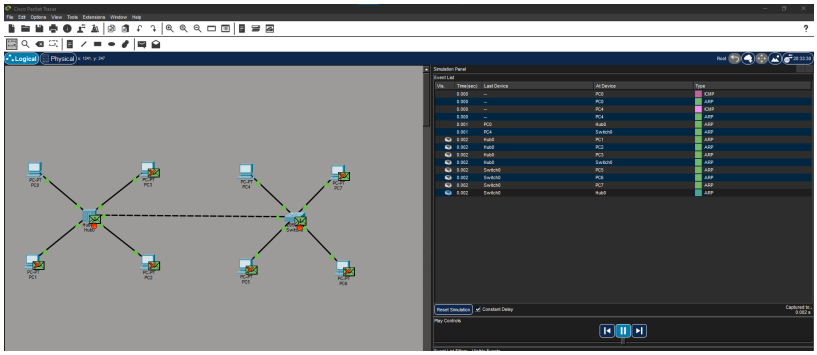

Рисунок 3.12: Видоизменение топологии сети и повторный сценарий с возникновением коллизии

Очистите список событий, удалив сценарий моделирования. На панели моделирования нажмите «Play» и в списке событий получите пакеты STP Исследуйте структуру STP. 1. Тип кадра Ethernet: Ethernet 802.3 (не Ethernet II). Вместо поля Type — поле LEN (длина данных).

2. Структура MAC-адресов:

DST MAC: 0180.C200.0000 — групповой (multicast) адрес для STP.

SRC MAC: не полностью виден, но начинается с 000C.CF61... — первые 3 байта — идентификатор производителя (OUI), вторые 3 — уникальный номер устройства. (рис. 3.13).

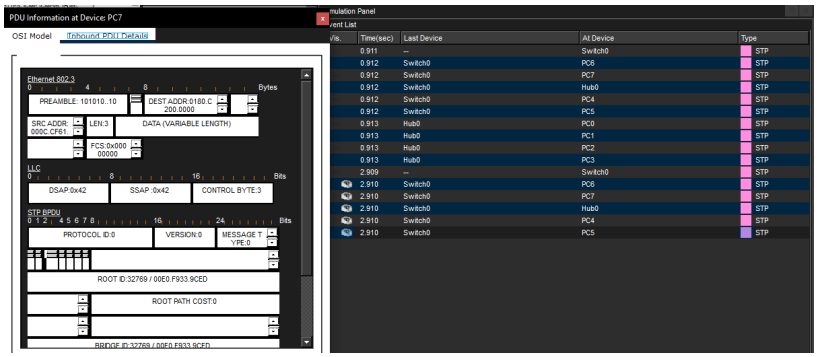

Рисунок 3.13: Просмотр структуры пакетов STP

Перейдите в режим реального времени (Realtime). В рабочем пространстве добавьте маршрутизатор (например, Cisco 2811). Соедините прямым кабелем коммутатор и маршрутизатор. Щёлкните на маршрутизаторе и на вкладке его конфигурации пропишите статический IP-адрес 192.168.1.254 с маской 255.255.255.0, активируйте порт, поставив галочку «On» напротив «Port Status» (рис. 3.14).

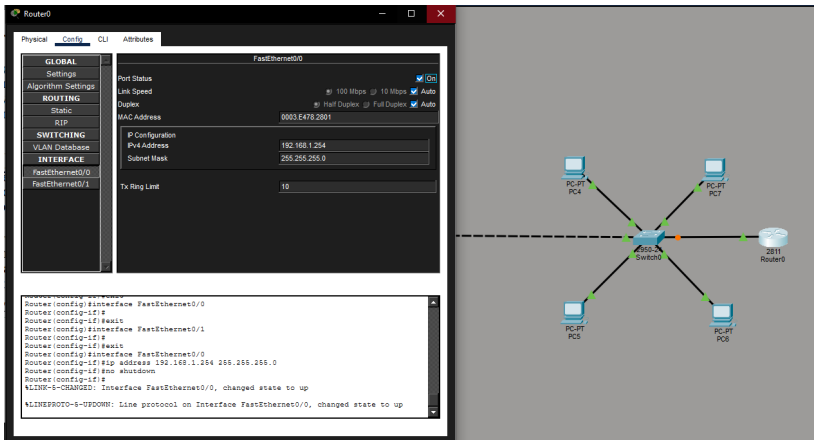

Рисунок 3.14: Добавление маршрутизатора и его настройка

Перейдите в режим моделирования (Simulation). Очистите список событий, удалив сценарий моделирования. Выберите на панели инструментов мышкой «Add Simple PDU (P)» и щёлкните сначала на PC3, затем на маршрутизаторе. На панели моделирования нажмите кнопку «Play» и проследите за движением пакетов ARP, ICMP, STP и CDP (рис. 3.15).

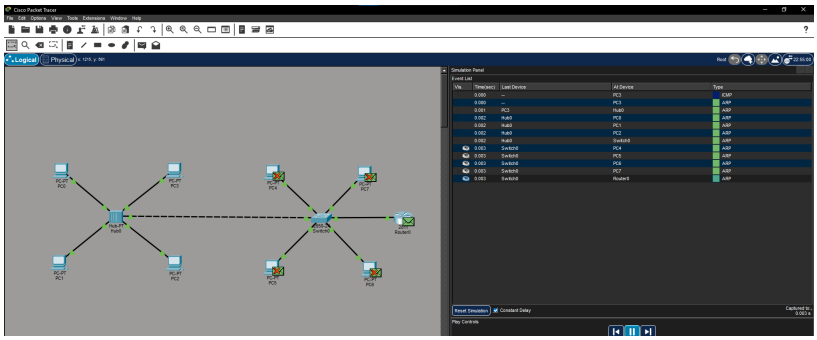

Рисунок 3.15: Просмотр пути движения пакетов ARP, ICMP, STP и CDP

Исследуйте структуру пакета CDP, опишите структуру кадра Ethernet. Какой тип имеет кадр Ethernet? Опишите структуру MAC-адресов. 1. Тип кадра Ethernet: Ethernet 802.3 (так как используется LLC, а не поле Type).

2. Структура MAC-адресов:

DST MAC: 0180.C200.0000 — групповой (multicast) адрес Cisco для CDP (все устройства Cisco слушают этот адрес).

SRC MAC: Не полностью виден, но это уникальный MAC-адрес отправителя (первые 3 байта — OUI производителя, последние 3 — серийный номер устройства).

3. Внутри кадра:

LLC (Logical Link Control):

DSAP: 0xAA

SSAP: 0xAA

CONTROL: 0x03 — указывает на использование SNAP (Subnetwork Access Protocol).

SNAP:

OUI: 0x00000C (Cisco)

PID: 0x2000 (CDP).

CDP (Cisco Discovery Protocol): служебный протокол Cisco для сбора информации о соседних устройствах. (рис. 3.16).

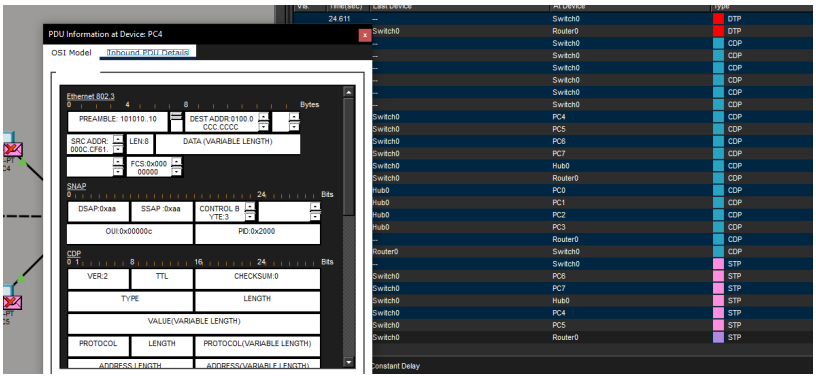

Рисунок 3.16: Просмотр структуры пакетов CDP

4 Контрольные вопросы

1. Концентратор, коммутатор, маршрутизатор, шлюз

Концентратор — устройство физического уровня, которое повторяет сигнал, полученный на один порт, на все остальные порты (не анализируя данные). Используется крайне редко (устарел), только для очень маленьких сетей или в лабораторных целях.

Коммутатор — устройство канального уровня, которое передает данные напрямую только тому устройству, которому они предназначены (на основе MAC-адресов). Используется внутри локальной сети для соединения компьютеров и других устройств.

Маршрутизатор — устройство сетевого уровня, которое соединяет разные сети (например, LAN и Интернет) и выбирает путь для данных на основе IP-адресов. Используется для выхода в интернет и объединения сетей.

Шлюз (Gateway) — это устройство или программа для соединения сетей с разными протоколами (например, для выхода из локальной сети в интернет). Обычно под шлюзом понимают адрес маршрутизатора, через который устройства выходят в другие сети.

2. IP-адрес, сетевая маска, broadcast-адрес

IP-адрес — это уникальный числовой идентификатор устройства (хоста) в сети (например, 192.168.1.5).

Сетевая маска — это число, которое «отсекает» от IP-адреса часть, отвечающую за номер самой сети, от части, отвечающей за номер узла (например, 255.255.255.0 говорит, что первые три цифры — это сеть, а последняя — устройство).

Broadcast-адрес — это специальный адрес, который используется для отправки данных сразу всем устройствам в данной сети (например, 192.168.1.255).

3. Как можно проверить доступность узла сети? С помощью команды ping (в командной строке: ping). Она отправляет специальные запросы узлу и ждет ответа, показывая, доходит ли связь и с какой скоростью.

5 Выводы

Я установил инструмент моделирования конфигурации сети Cisco Packet Tracer, ознакомился с его интерфейсом