Laboratory work report №1 administration of local subsystems

Cisco Packet Tracer

Выполнил: Леснухин Даниил Дмитриевич,
НПИбд-02-22, 1132221553

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

Packet Tracer — интегрированная обучающая среда моделирования и визуализации сети устройств и протоколов, выпускаемый фирмой Cisco Systems. Спомощьюданного симулятора можно строить модели сетей передачи данных, изучать настройки и принципы функционирования сетевого оборудования производителя, проводить диагностику работоспособности моделируемой сети.

1.Установите в вашей операционной системе Cisco Packet Tracer. 2.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. (рис. [-@fig:001], рис. [-@fig:002], рис. [-@fig:003])

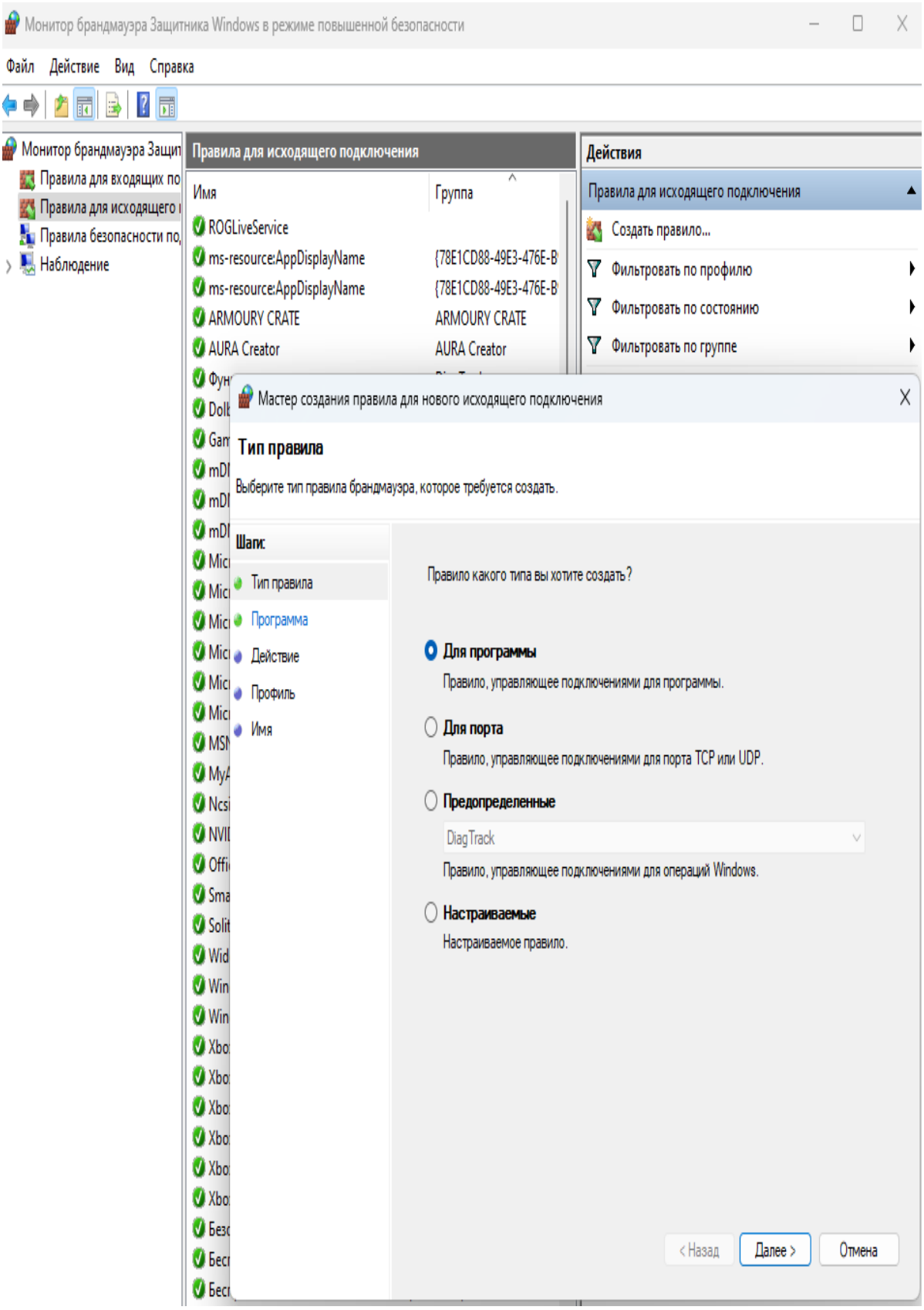


Рис. 1: Настройка брандмауэра

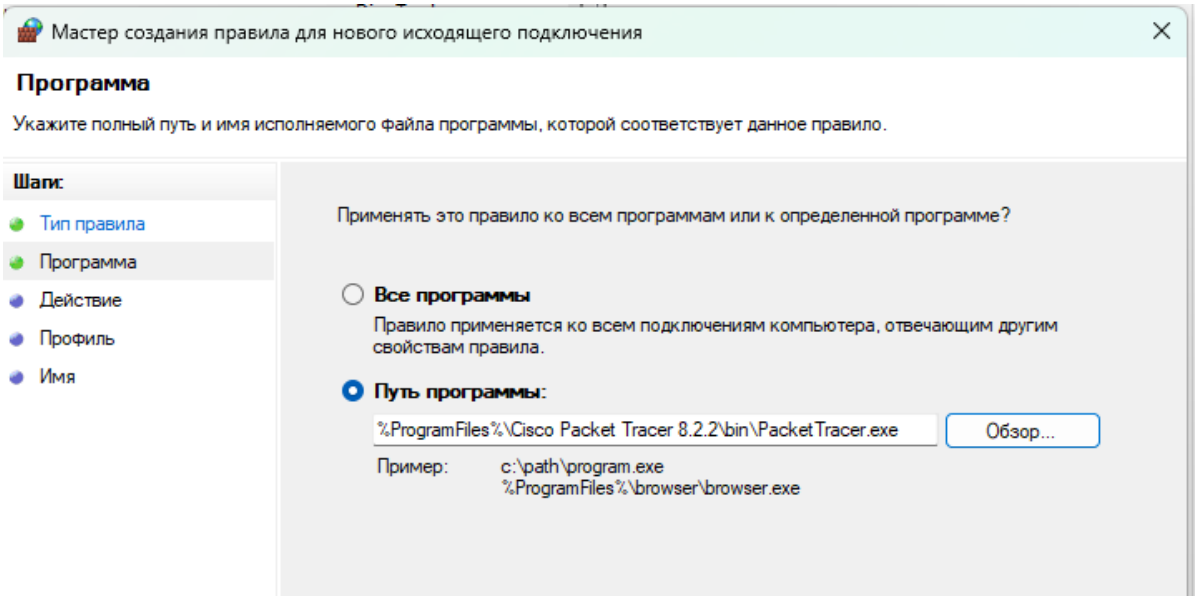


Рис. 2: Создание нового правила для подкл.чения

Рис. 3: Блокировка подключения

После правильной настройки брандмауэра программа не будет запрашивать авторизацию (рис. [-@fig:004])

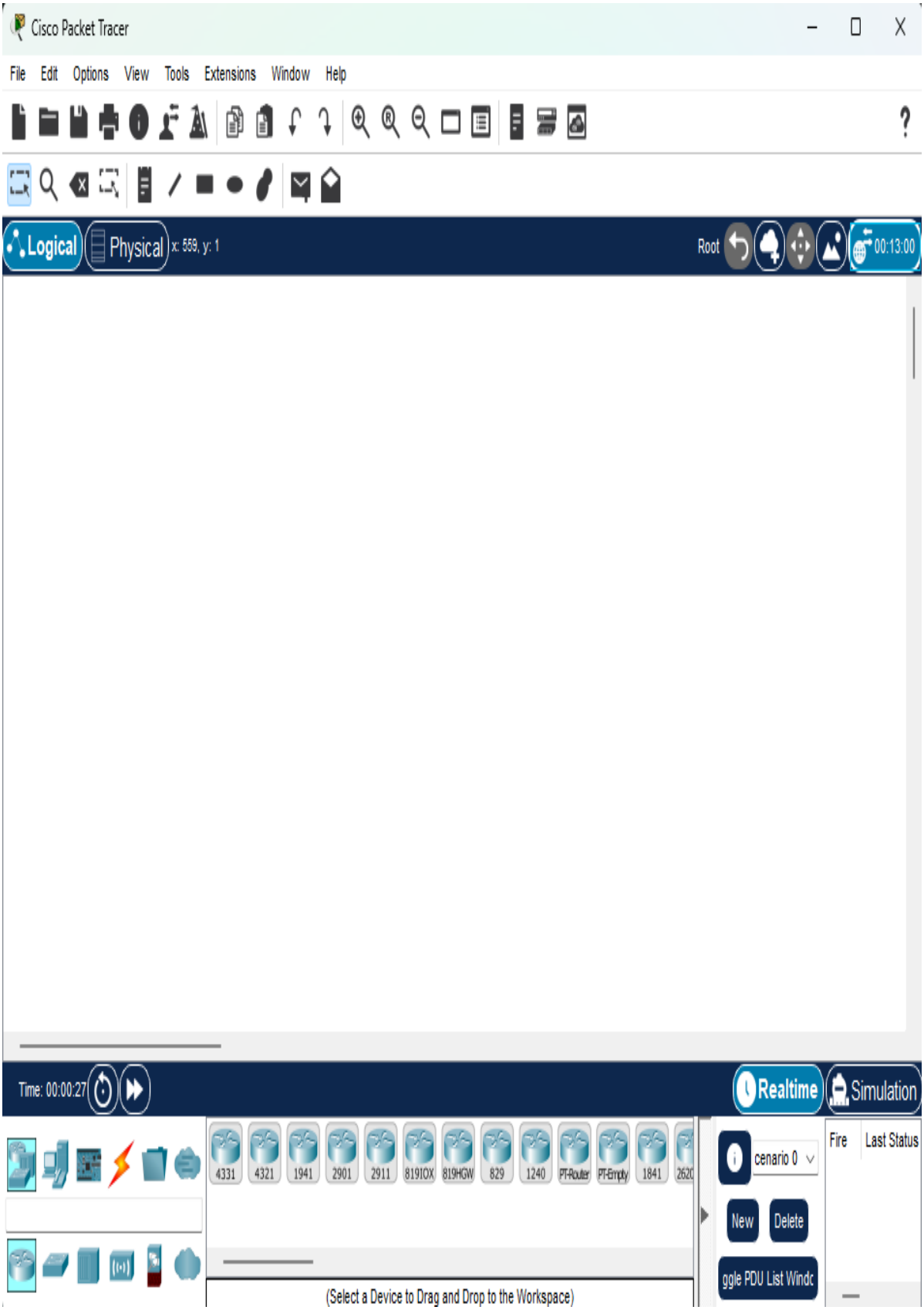


Рис. 4: Рабочее пространство Packet Tracer

В рабочем пространстве разместим концентратор (Hub-Pt) и четыре оконченных устройства PC. Соединим их прямым кабелем (рис. [-@fig:005]). После этого последовательном зададим статические ip-адреса (рис. [-@fig:006]).

192.168.1.11

192.168.1.12

192.168.1.13

192.168.1.14

с маской подсети 255.255.255.0

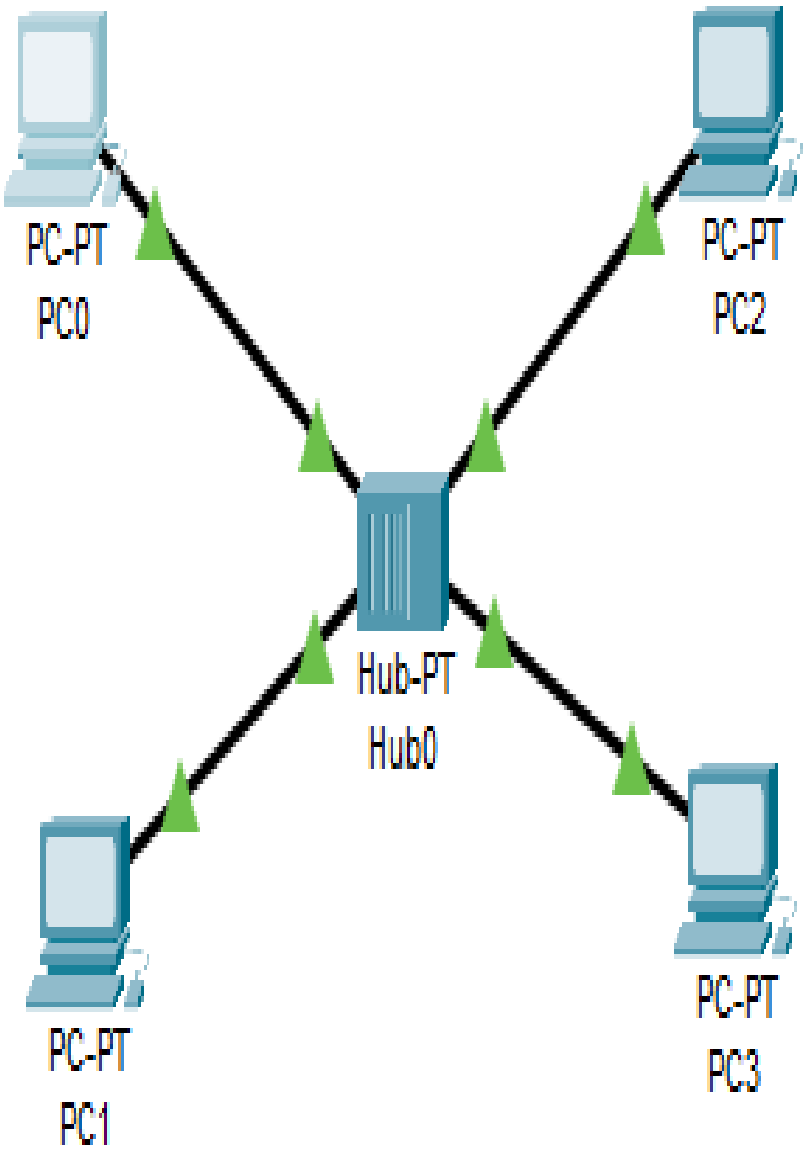


Рис. 5: Рабочий проект с концентратором и окоченными устройствами

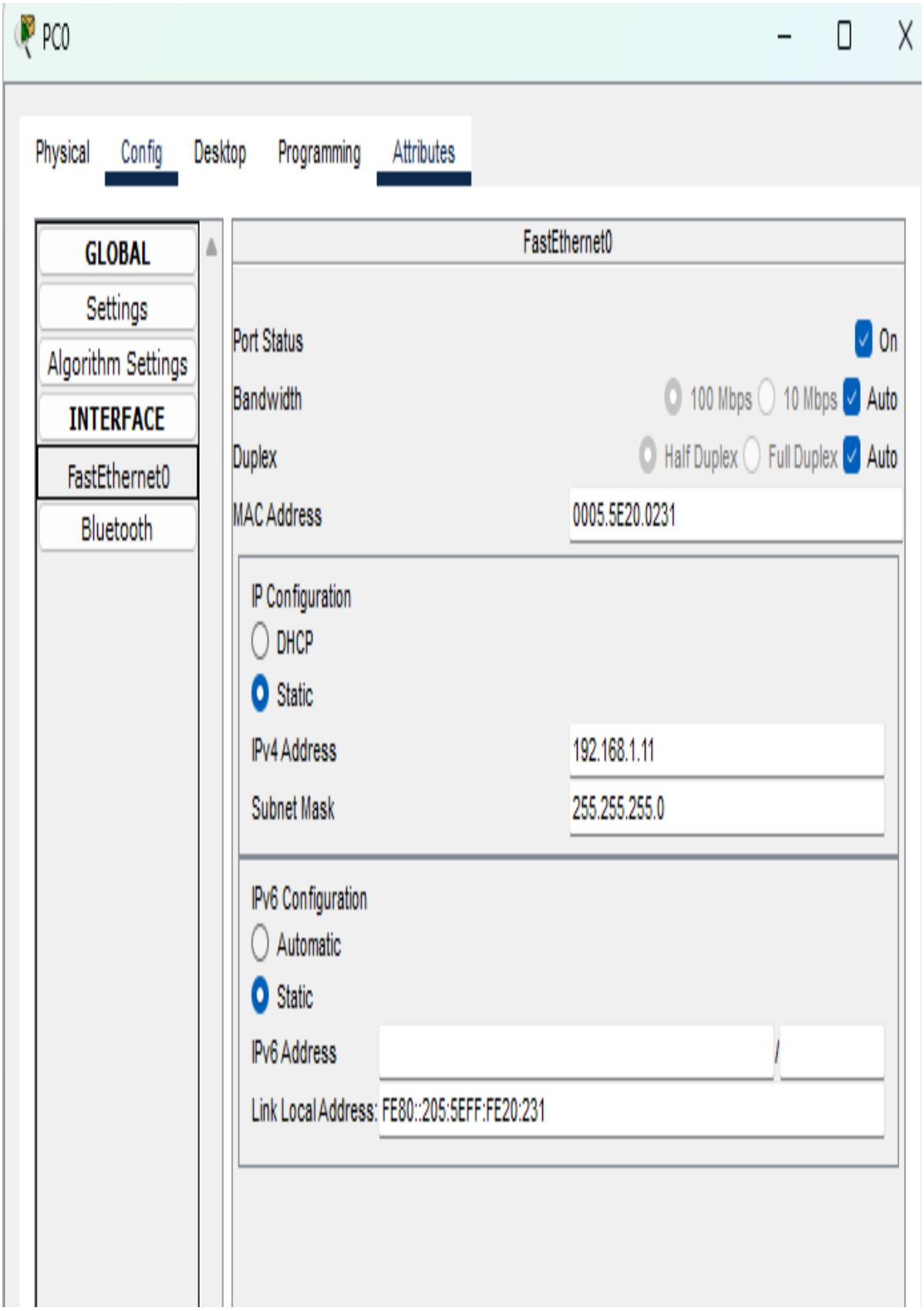


Рис. 6: Задаем статический ip-адрес

Далее мы переходим из режима реального времени (Realtime) в режим моделирования (Simulation). Выберем на панели инструментов мышкой «Add Simple PDU (P)» и щелкним сначала на PC0, затем на PC2.(рис. [-@fig:007]) В рабочей области появились два конверта, обозначающих пакеты, в списке событий на панели моделирования появились два события, относящихся к пакетам ARP и ICMP соответственно. Далее нажмем кнопку “PLAY”. (рис. [-@fig:008]).

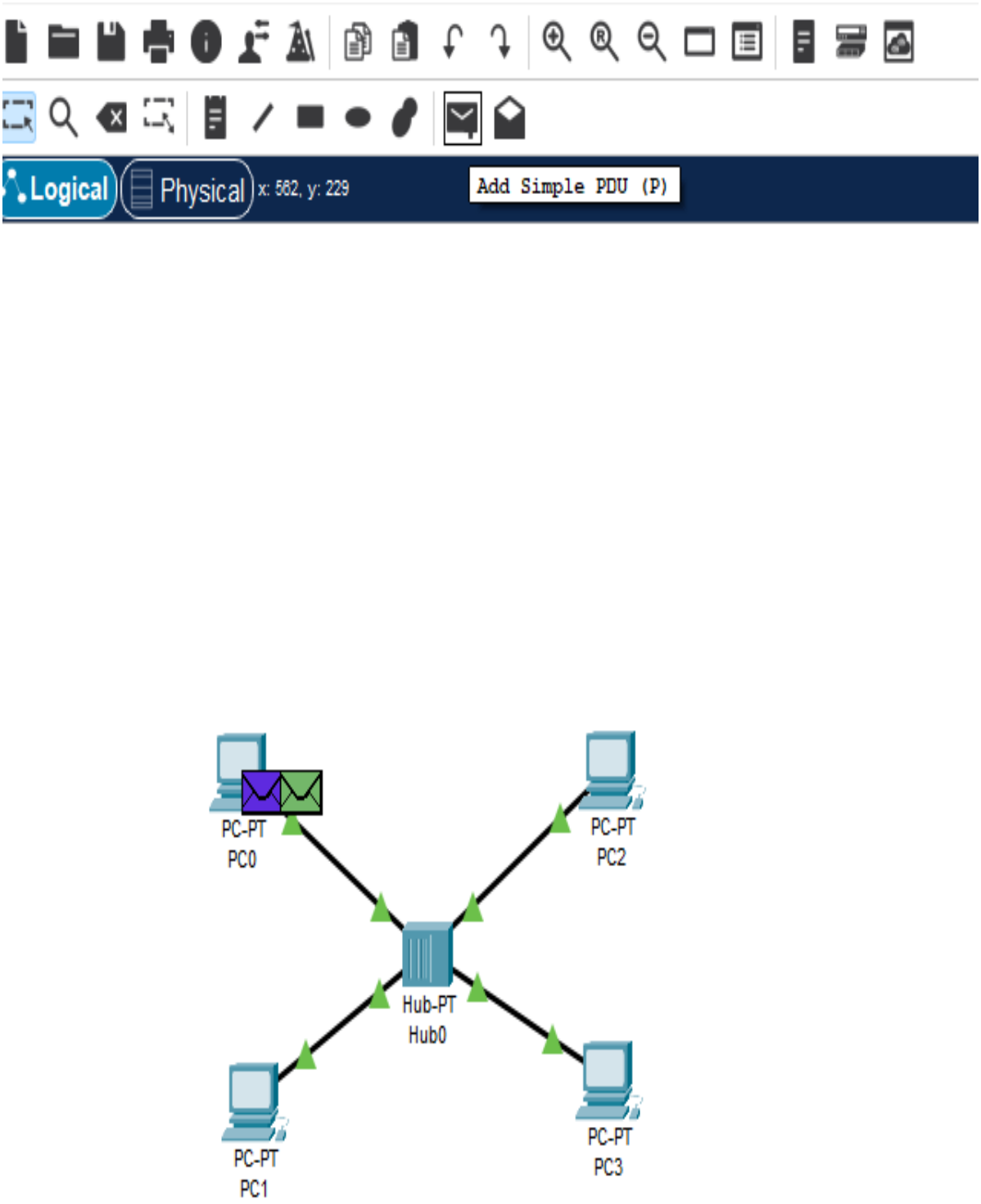
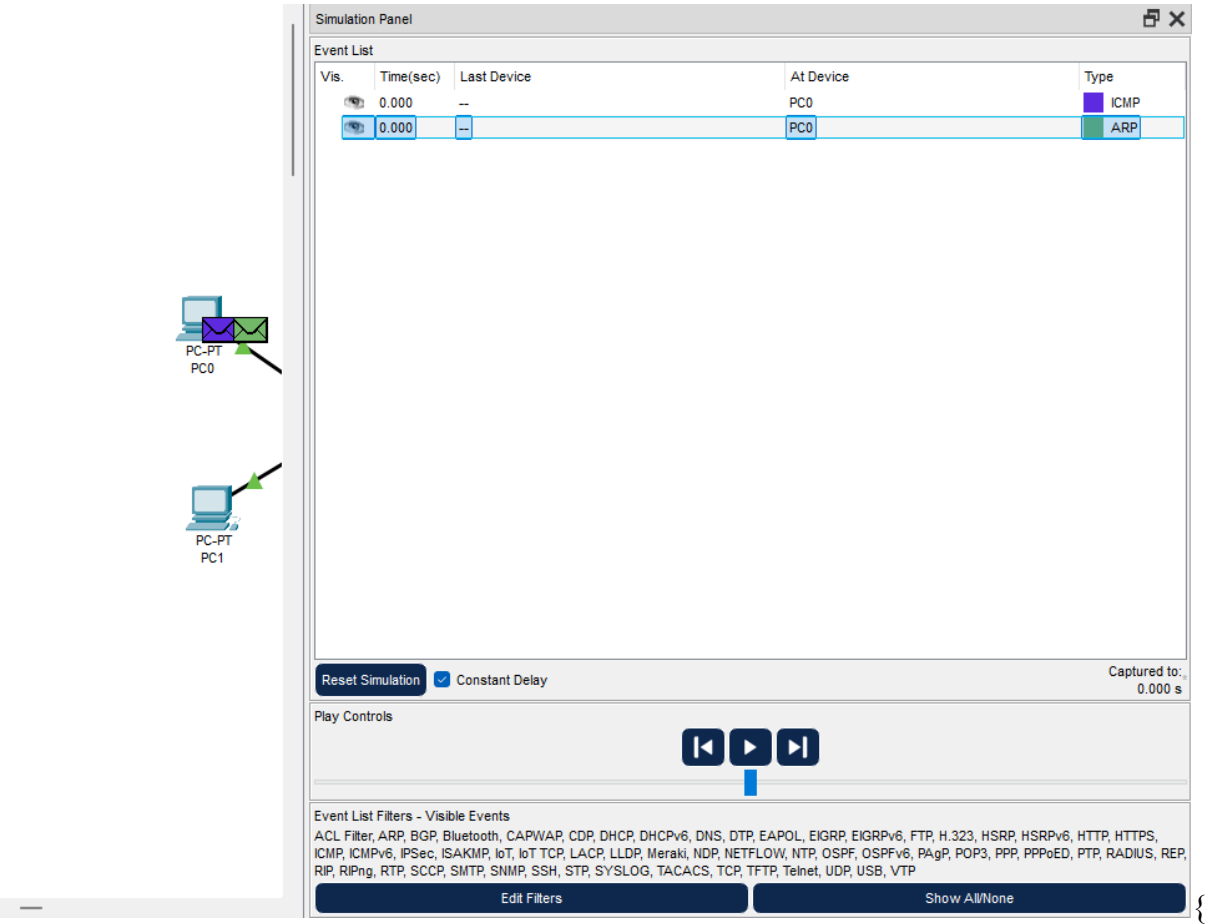


Рис. 7: Отправляем пакеты



{#fig:008 width = 100% height = 100%}

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. [-@fig:009])

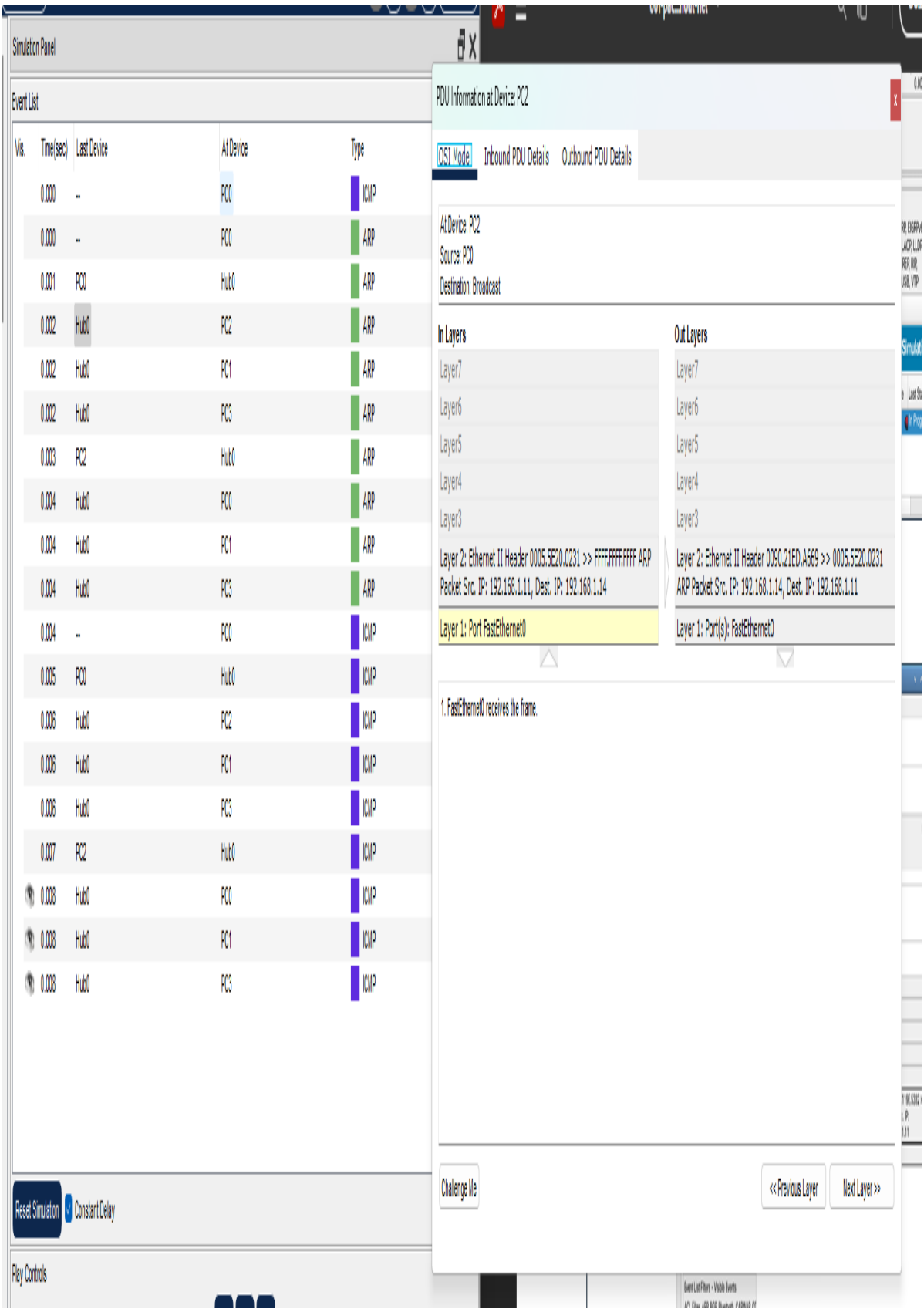


Рис. 8: Challenge me - ответы на вопросы

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.11 [-@fig:010]) Кадр: EthernetII

Преамбула: PREAMBLE

Контрольная сумма: FCS

Адрес MAC: DEST ADDR

Источник: SRC ADDR

Тип вложения: TYPE

Длина: DATA

ICMP – находится на сетевом уровне

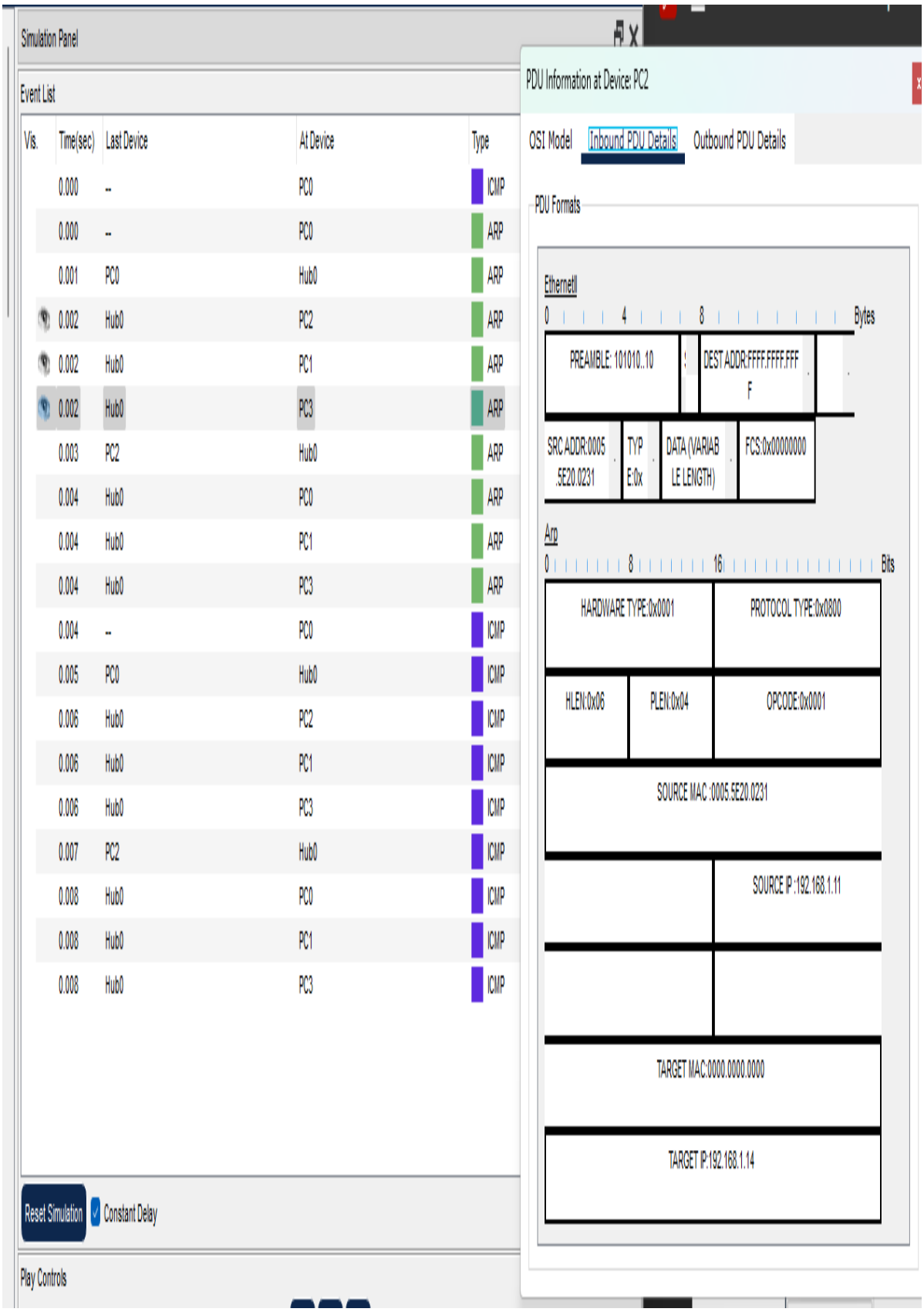


Рис. 9: Исследование структуры пакета ICMP

Далее мы очищаем рабочее пространство, удаляю сценарии. (рис. [-@fig011])

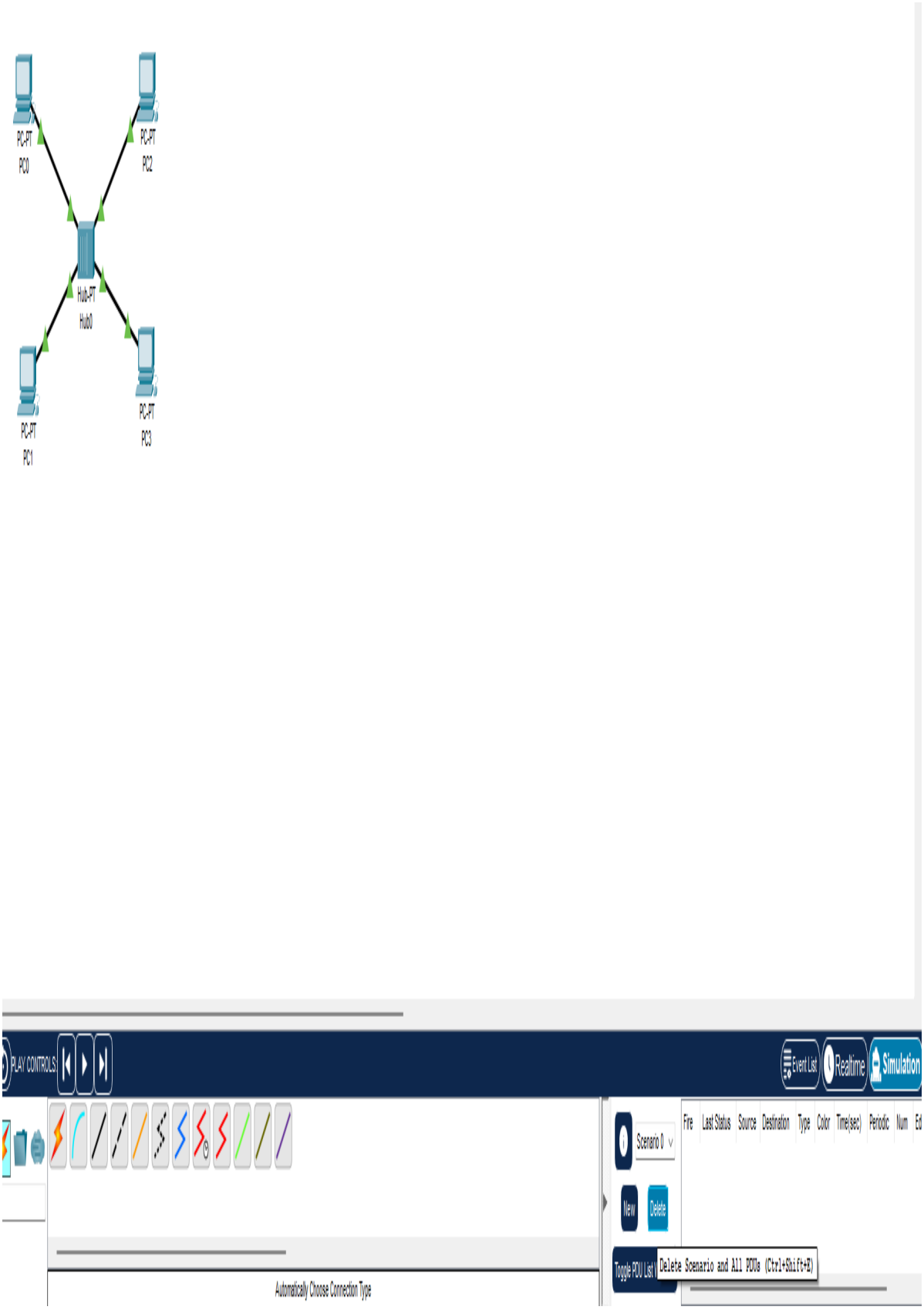


Рис. 10: Удаление сценария

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 повторяем действия в обратном порядке. (рис. [-@fig:012]). В списке соытий посмотрим информацию о PDU (рис. [-@fig:013])

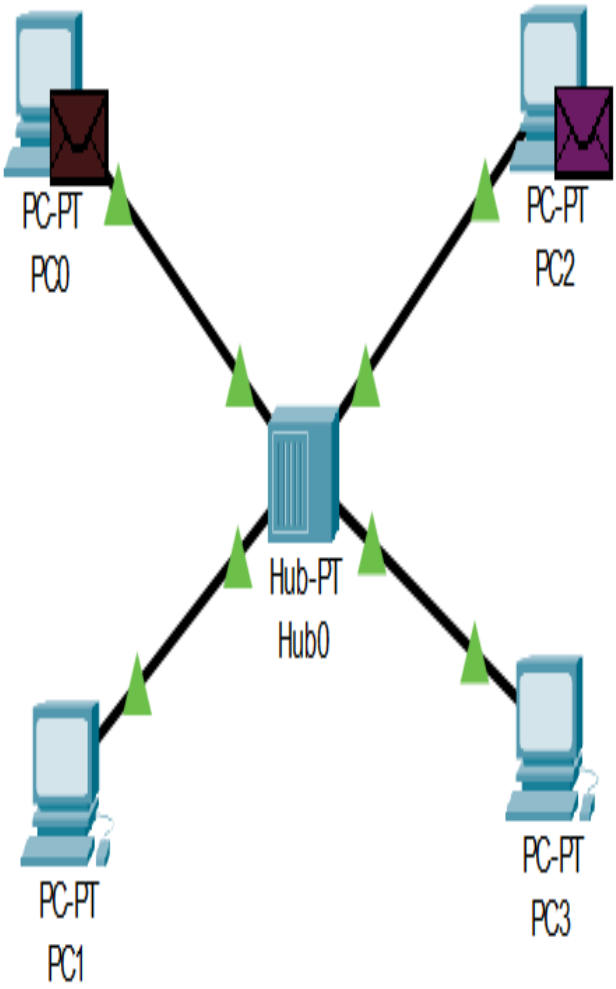
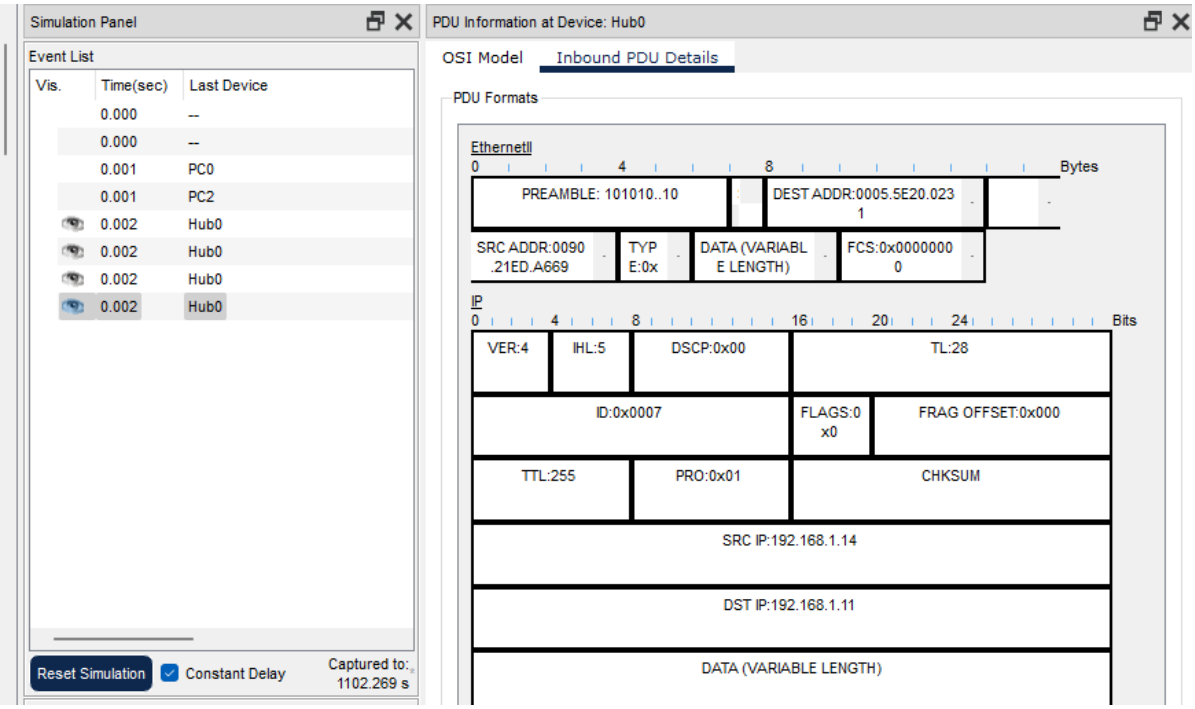


Рис. 11: PC0->PC2. PC2->PC0



{#fig:013 width=100% height=100%}

В рабочем пространстве разместим коммутатор (Cisco 2950-24) и 4 оконечных устройства PC

Соединим оконечные устройства с коммутатором прямым кабелем. 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. [-@fig:014])

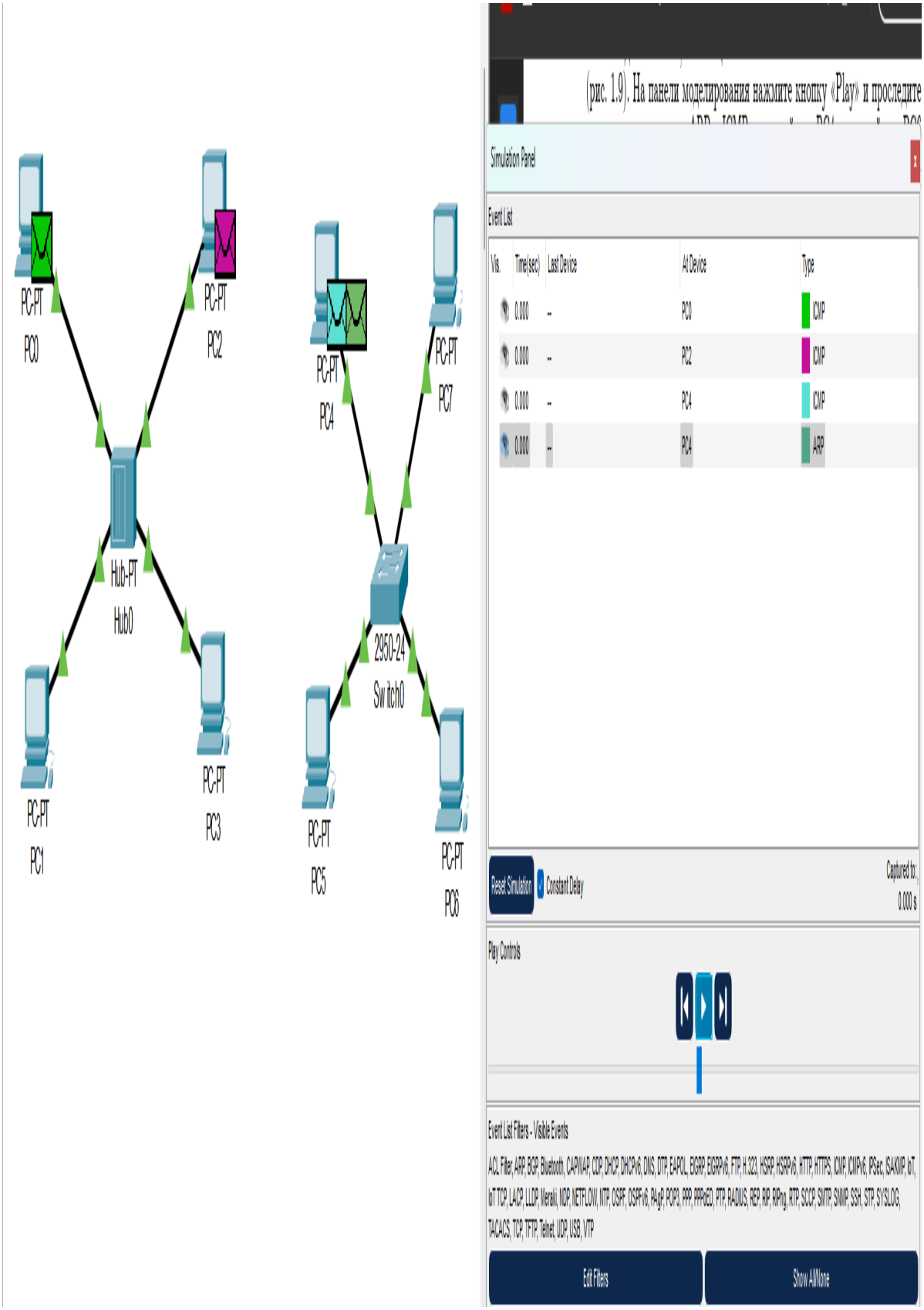


Рис. 12: Коммутатор и 4 оконченных устройства

Перейдём в режим реального времени (Realtime). В рабочем пространстве соединим кроссовым кабелем концентратор и коммутатор (рис. [-@fig:015]) Выберем на панели инструментов мышкой «Add Кулябов Simple PDU (P)» и щёлкнем сначала на PC0, затем на PC4 и повторить действия в обратном порядке.

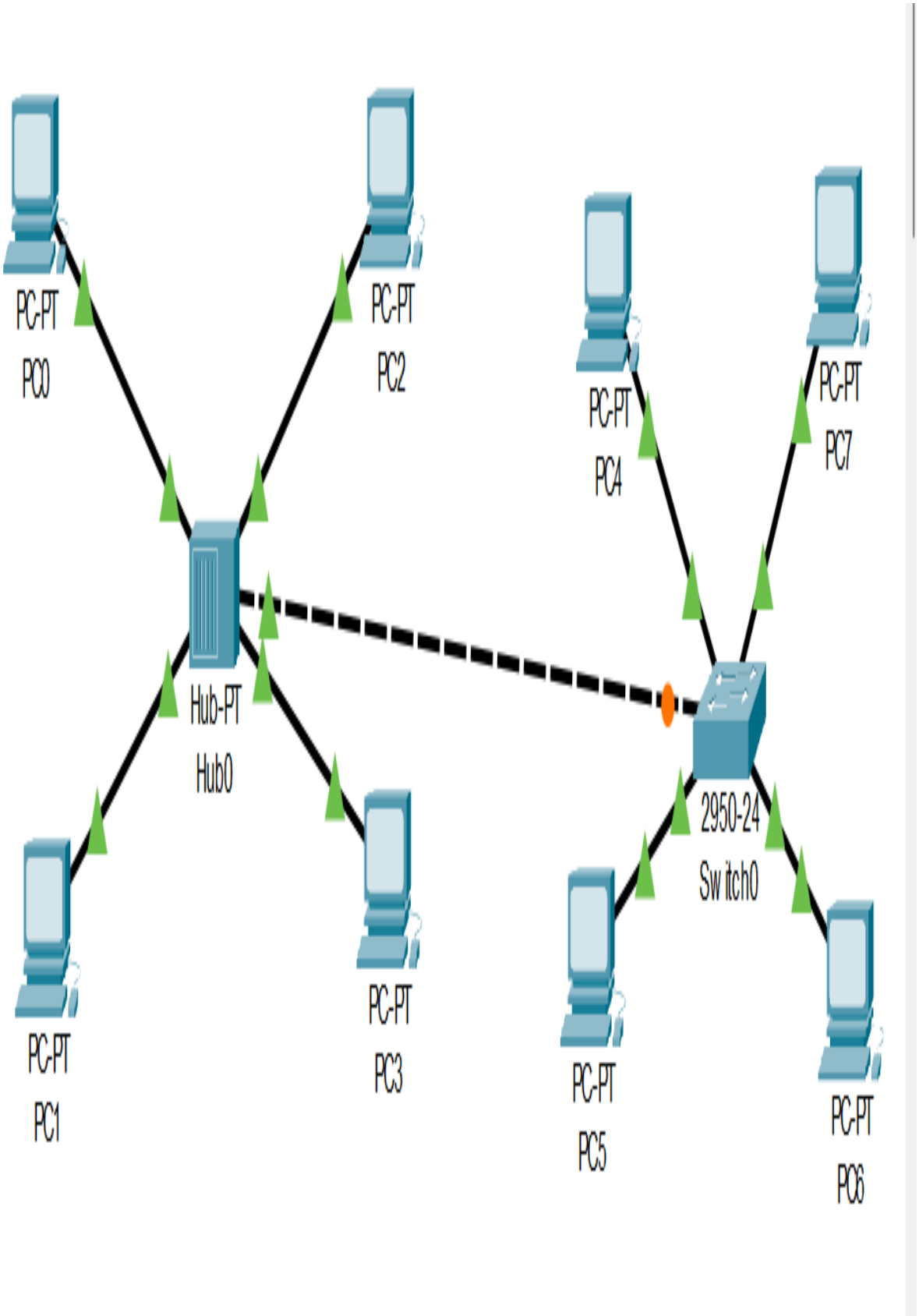


Рис. 13: Соединение крссовым кабелем концентратора и коммутатора

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. [-@fig:016])

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

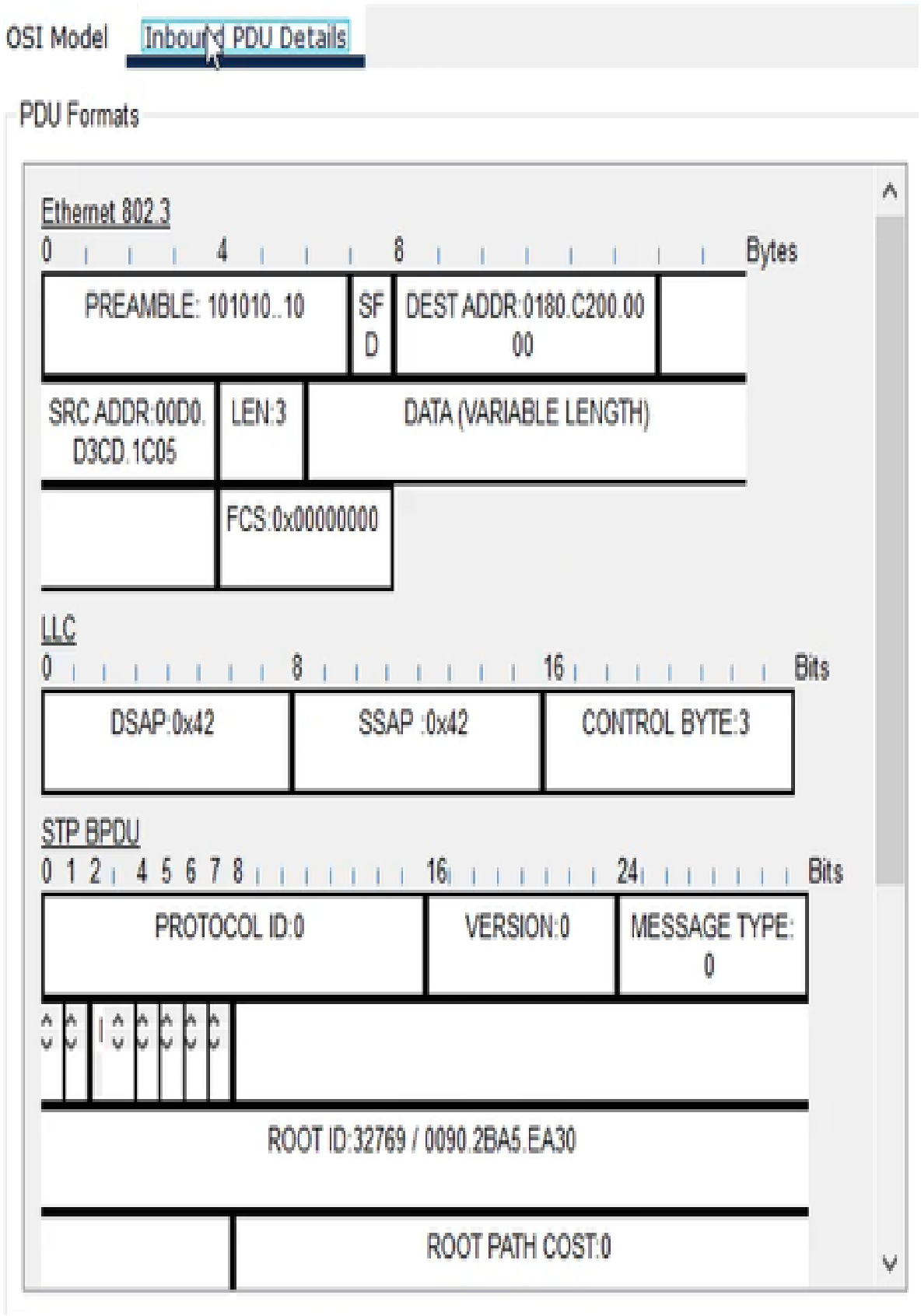


Рис. 14: Исследование структуры STP

Перейдём в режим реального времени (Realtime). В рабочем пространстве добавим маршрутизатор (Cisco 2811). Соединим прямым кабелем коммутатор и маршрутизатор 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. [-@fig:017])

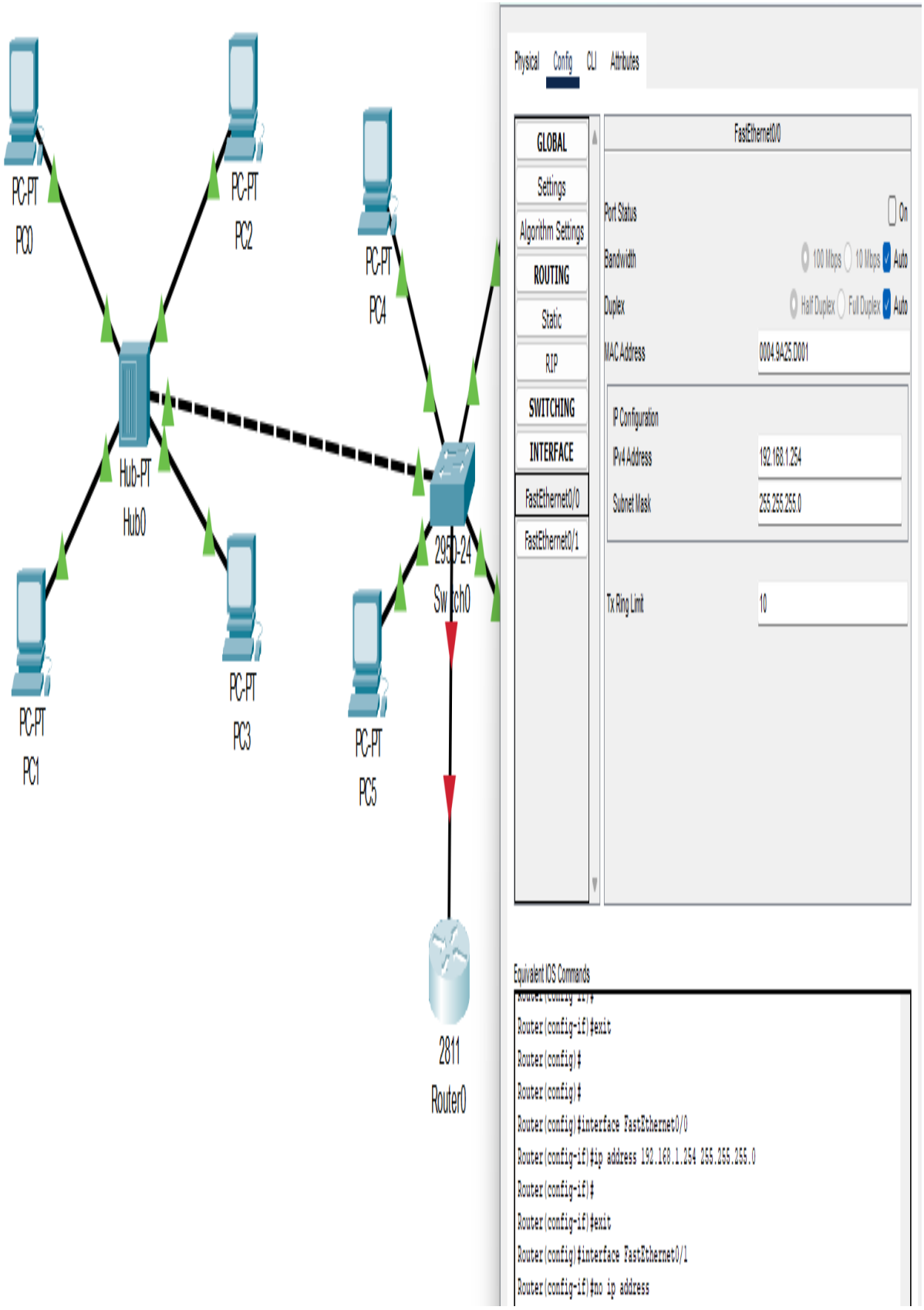
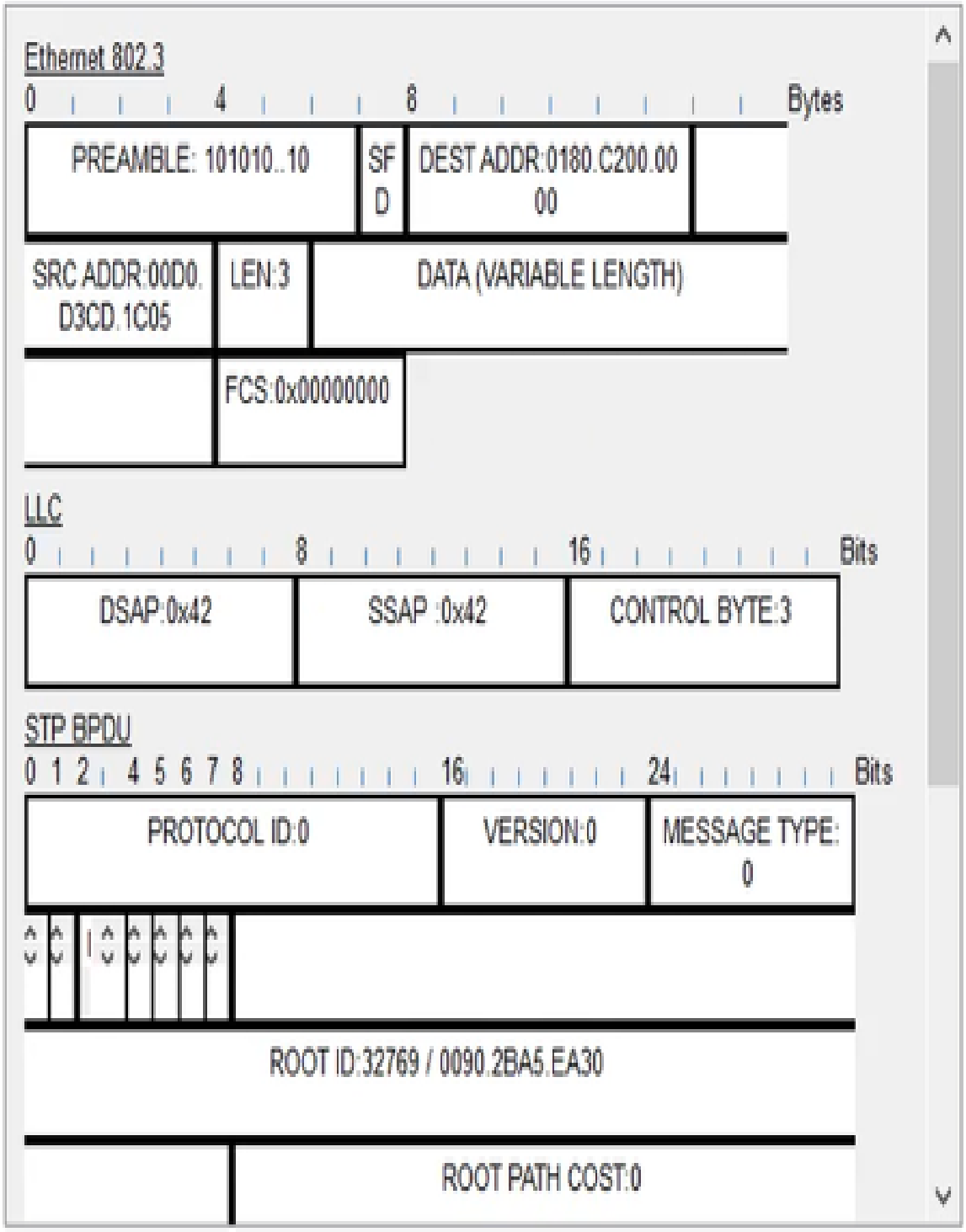


Рис. 15: Добавление маршрутизатора cisco2811

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. [-@fig:018])

OSI Model | Inbound PDU Details

PDU Formats



Самостоятельная работа

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

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 с 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 инструмен-

ты, 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 для управления сетями, которые предоставляют информацию о 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.