Отчёт по лабораторной работе № 1

Знакомство с Cisco Packet Tracer

Поляков Глеб Сергеевич

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

1. Установите в вашей операционной системе Cisco Packet Tracer.
2. Для ОС типа Linux требуется установить firejail (https://firejail.wordpress.com/), который ограничивает среду выполнения ненадёжных приложений с помощью пространств имён Linux и seccomp-bpf. Запуск Packet Tracer с отключённой сетью осуществляется посредством следующей команды: firejail –net=none –noprofile packettracer
3. 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.

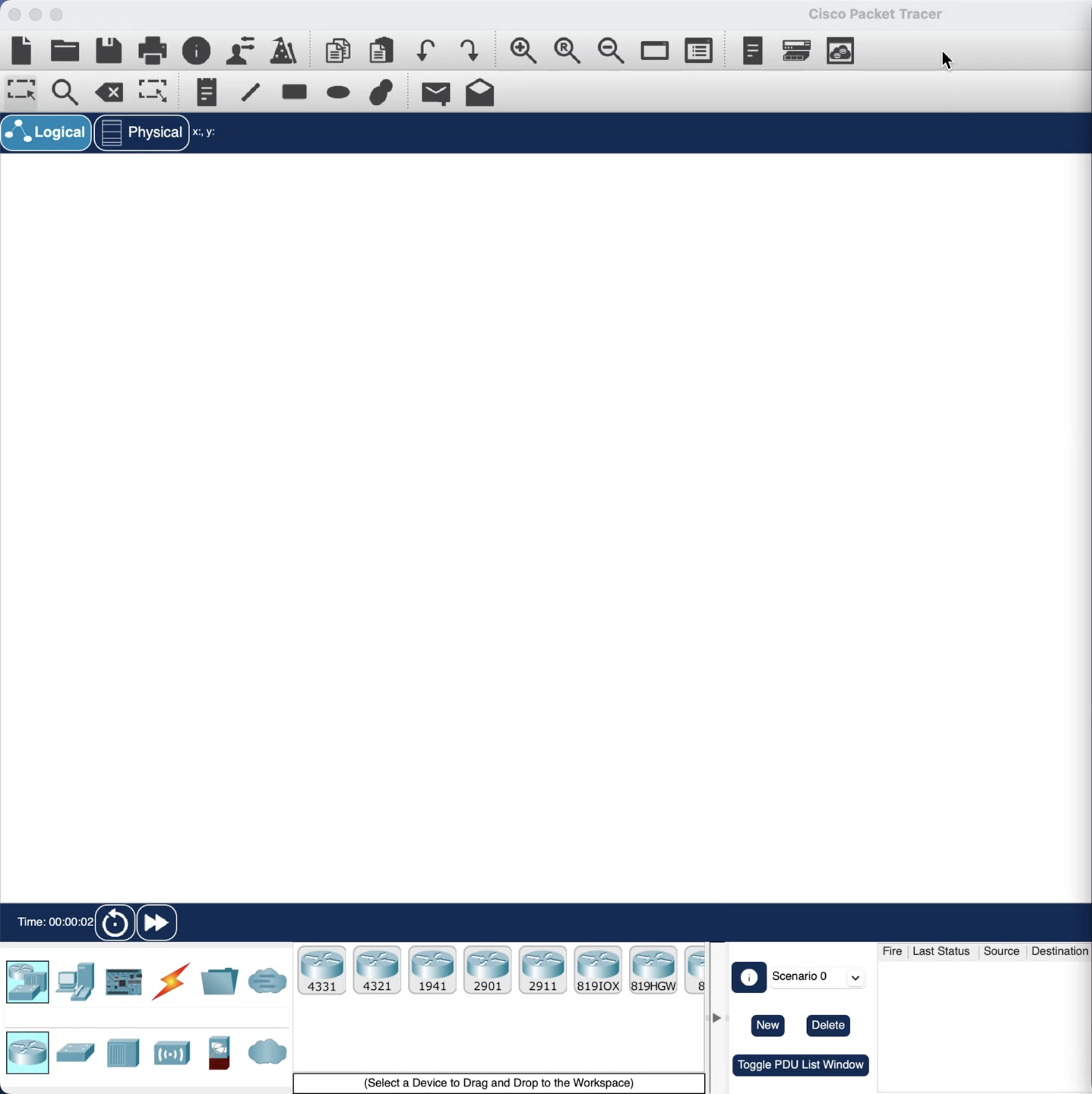
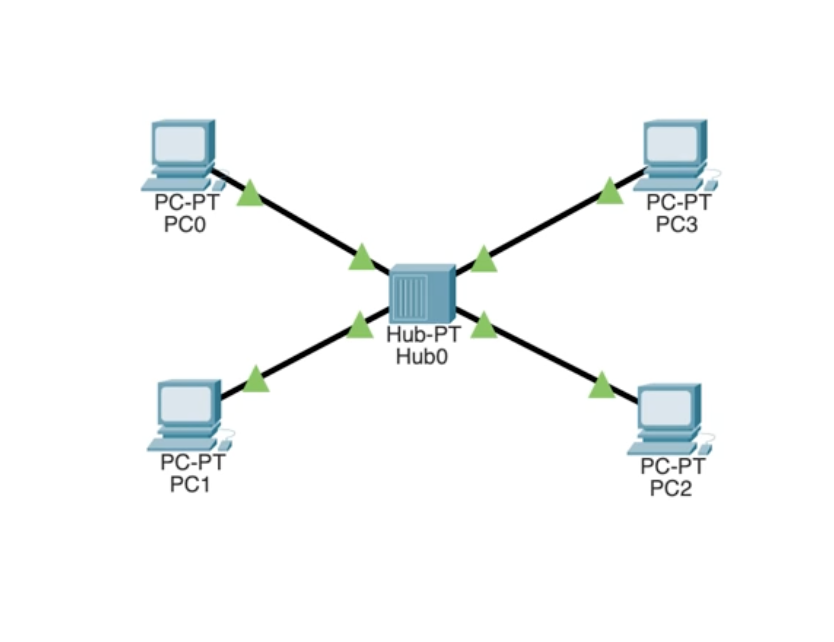
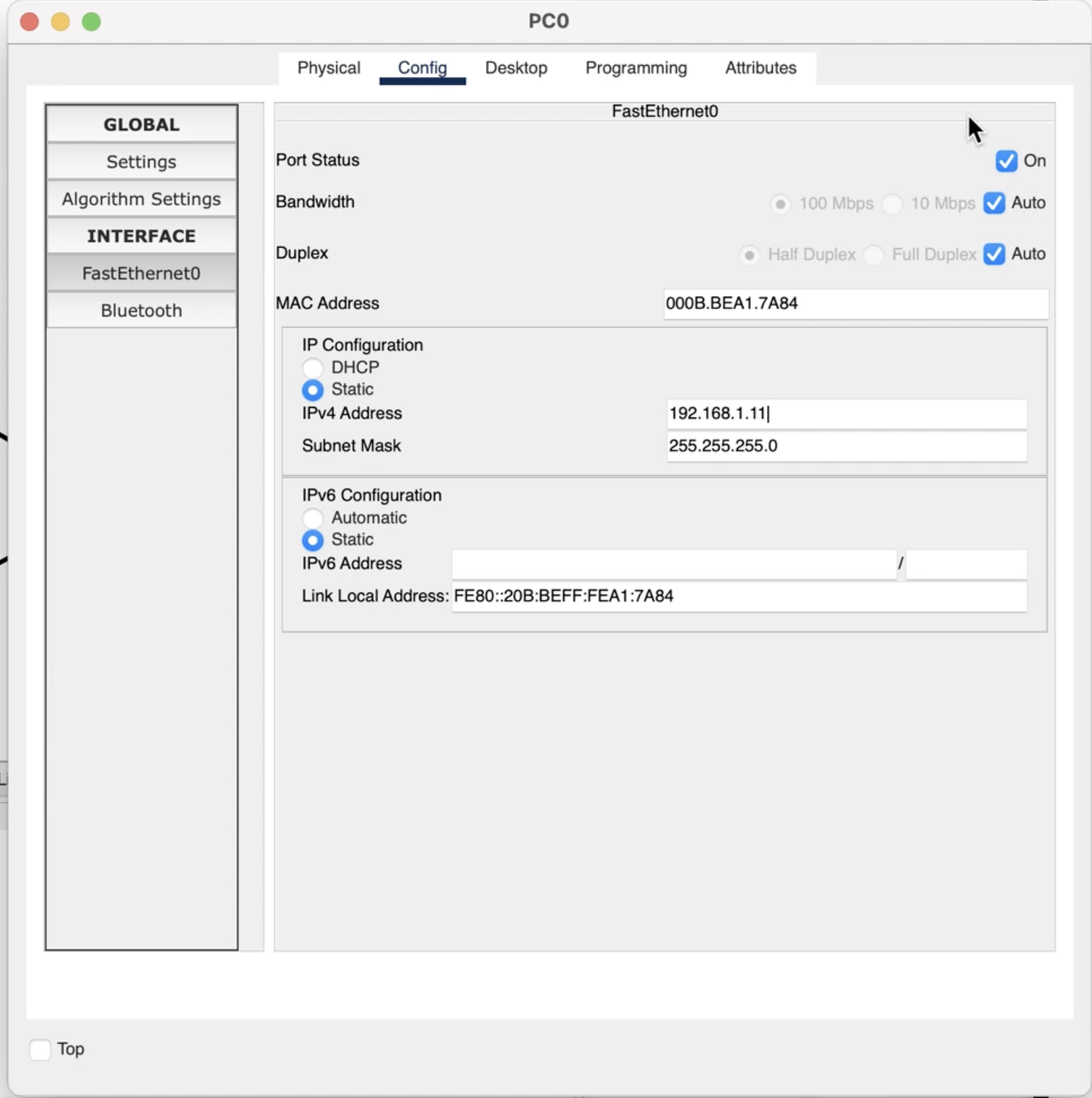
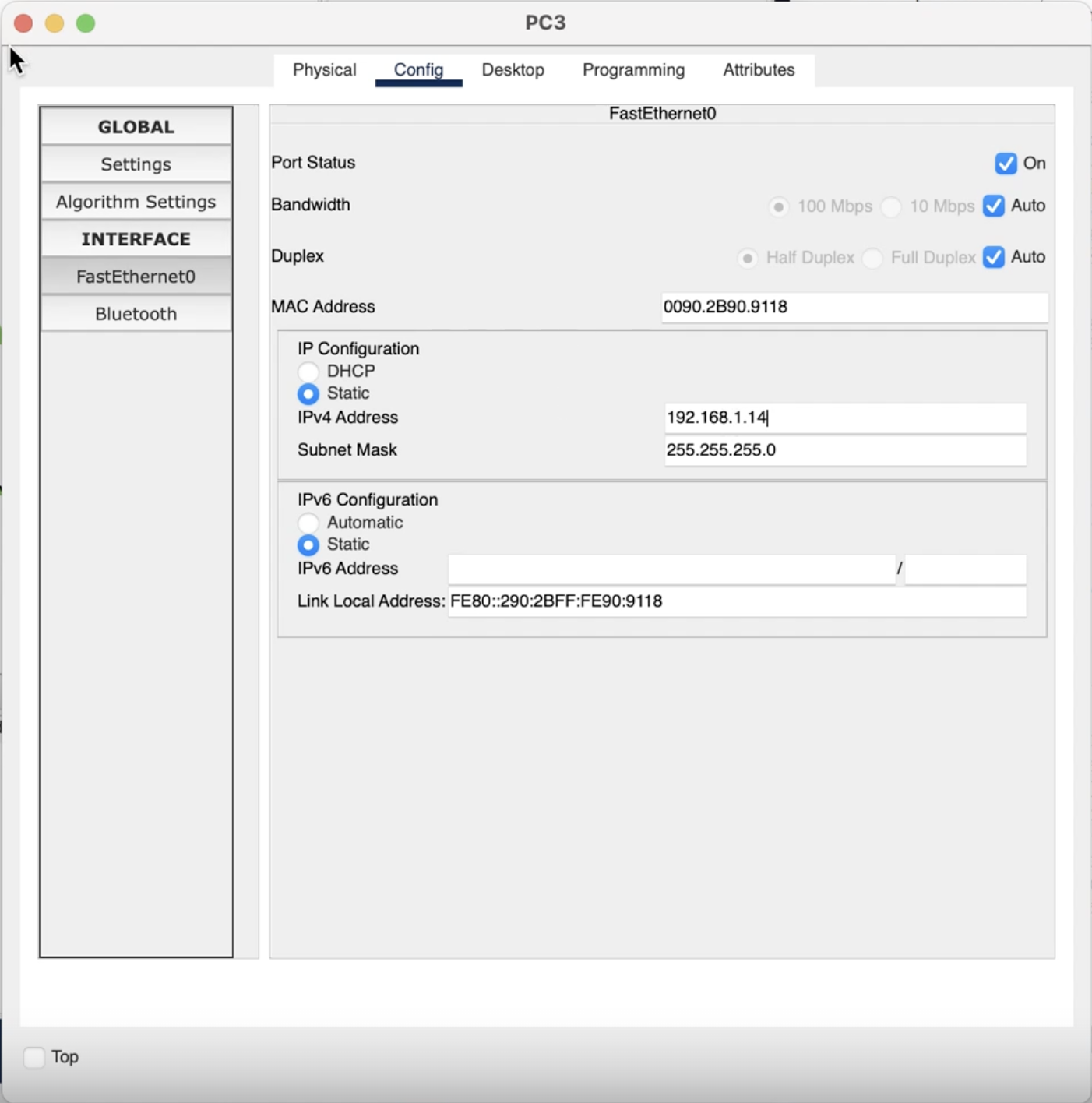
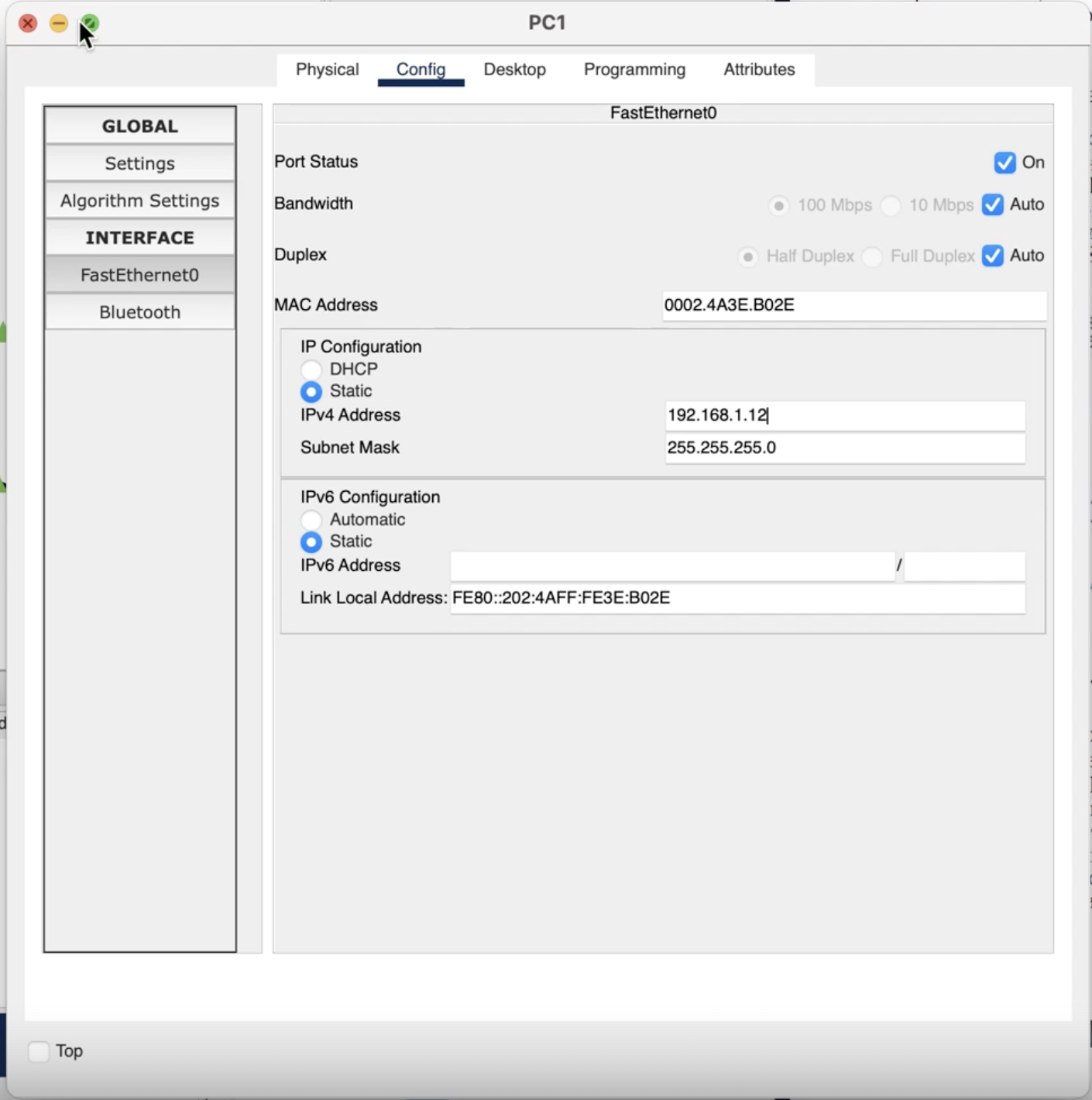
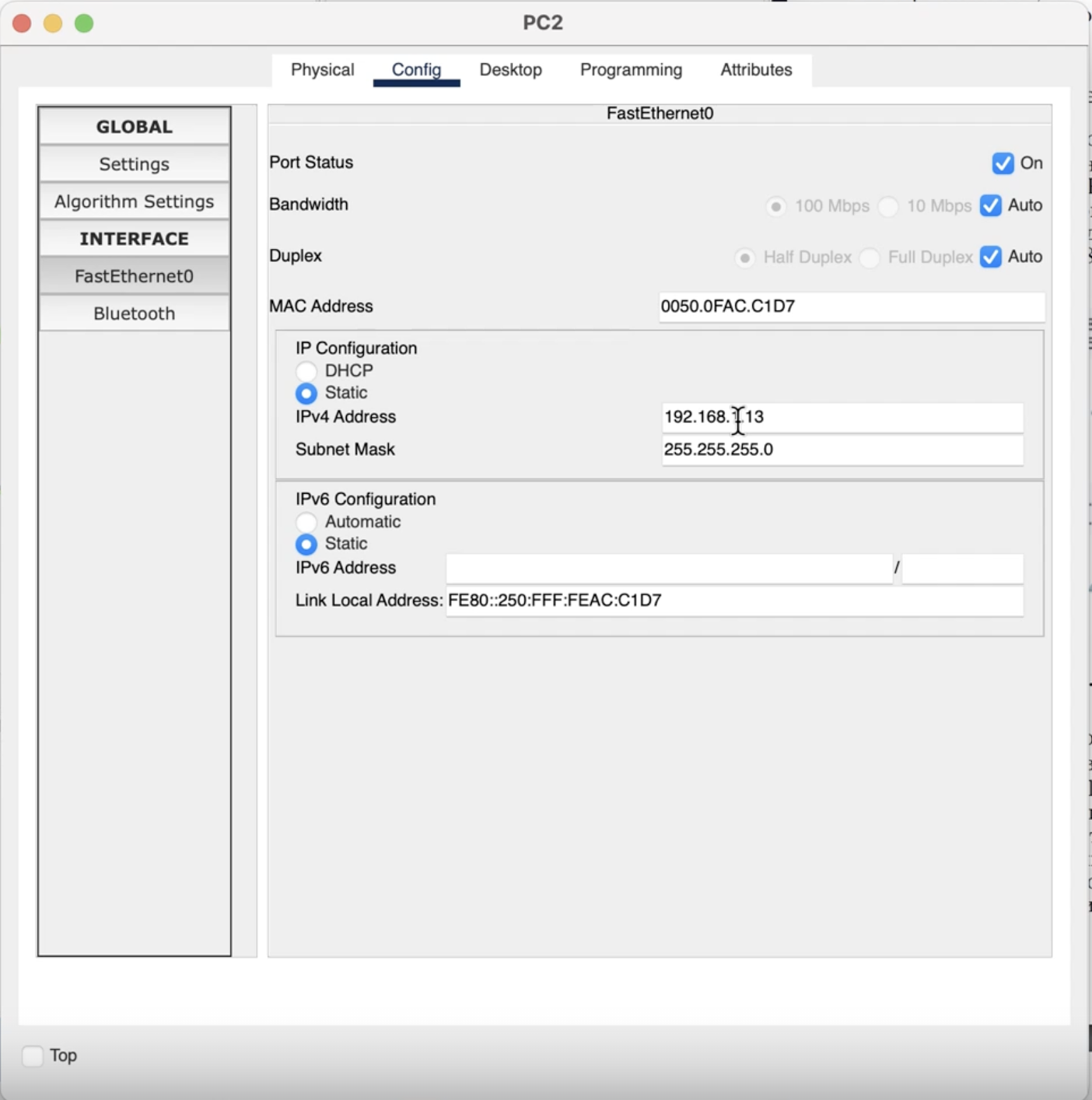
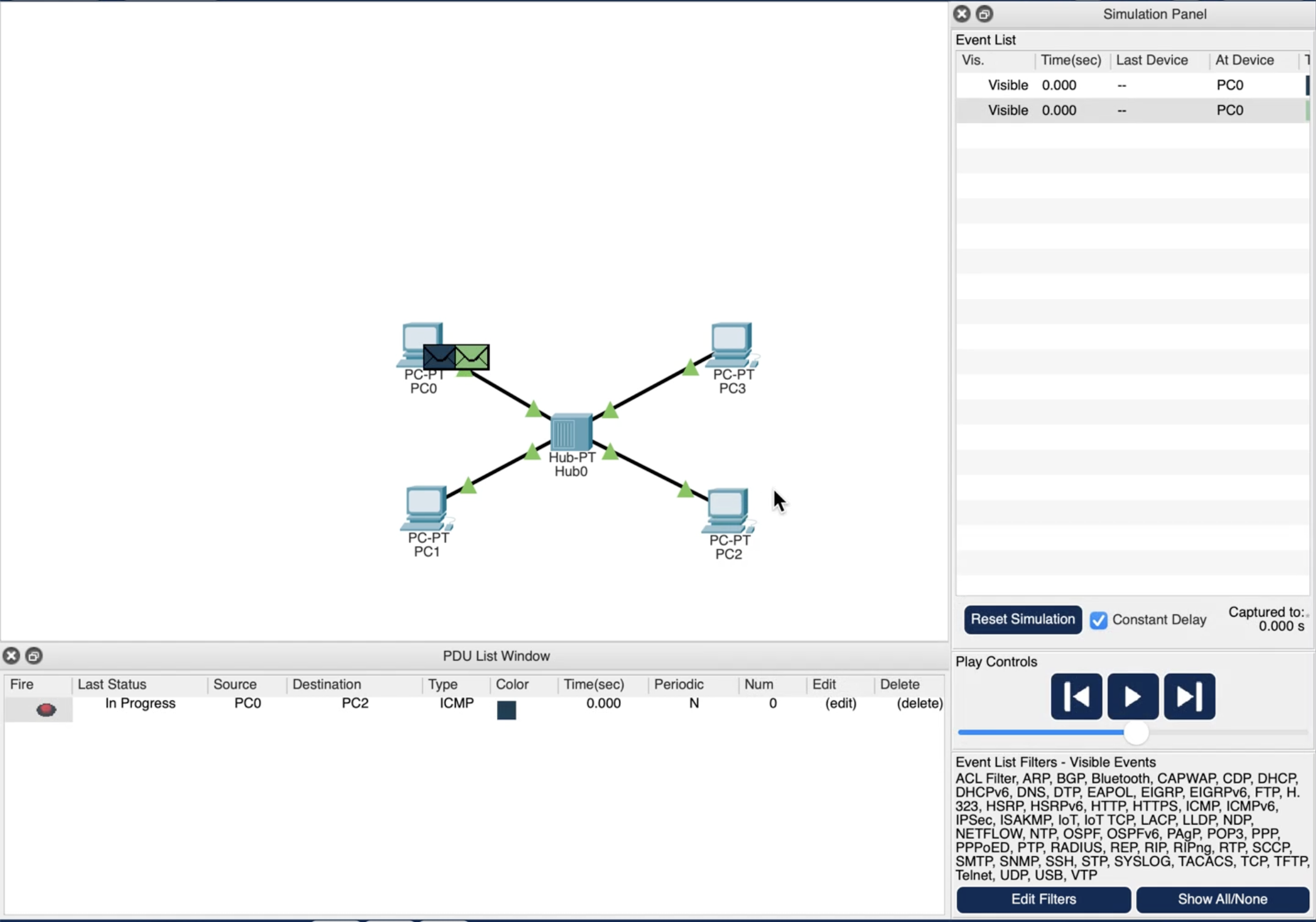
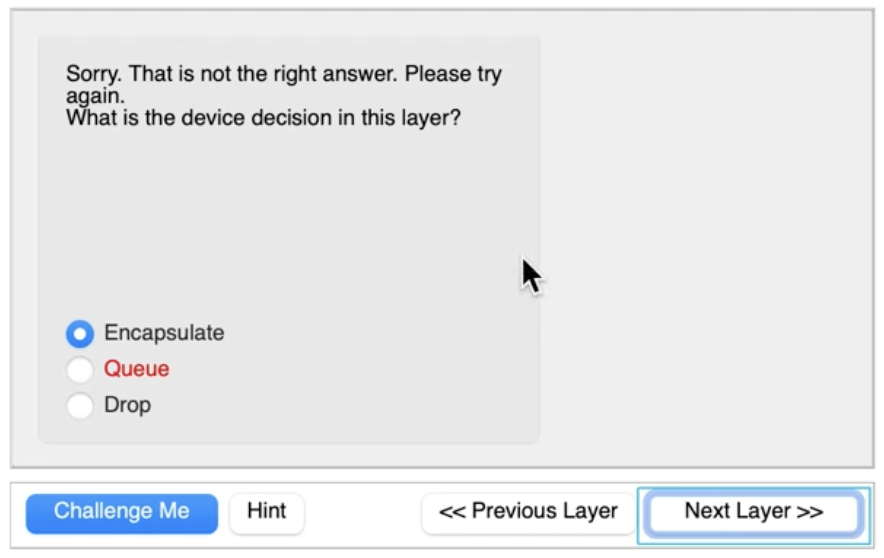
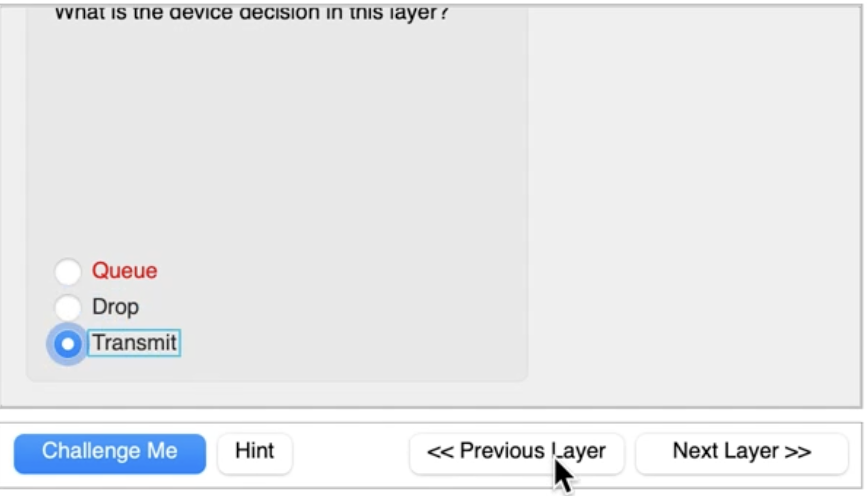
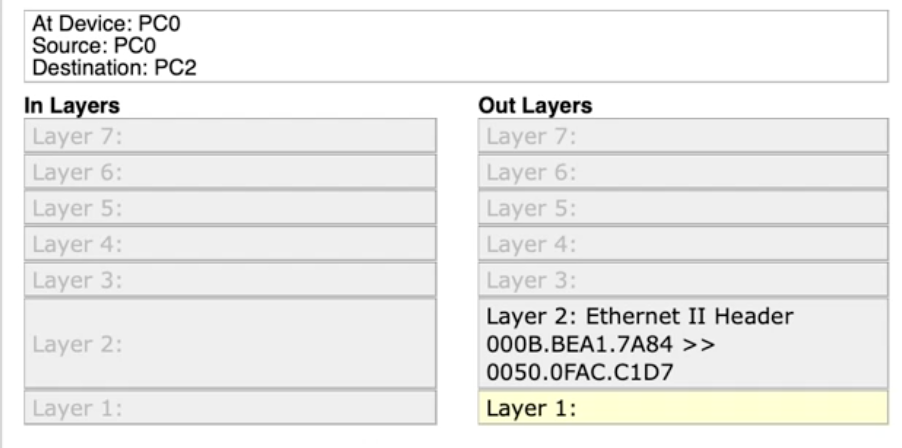
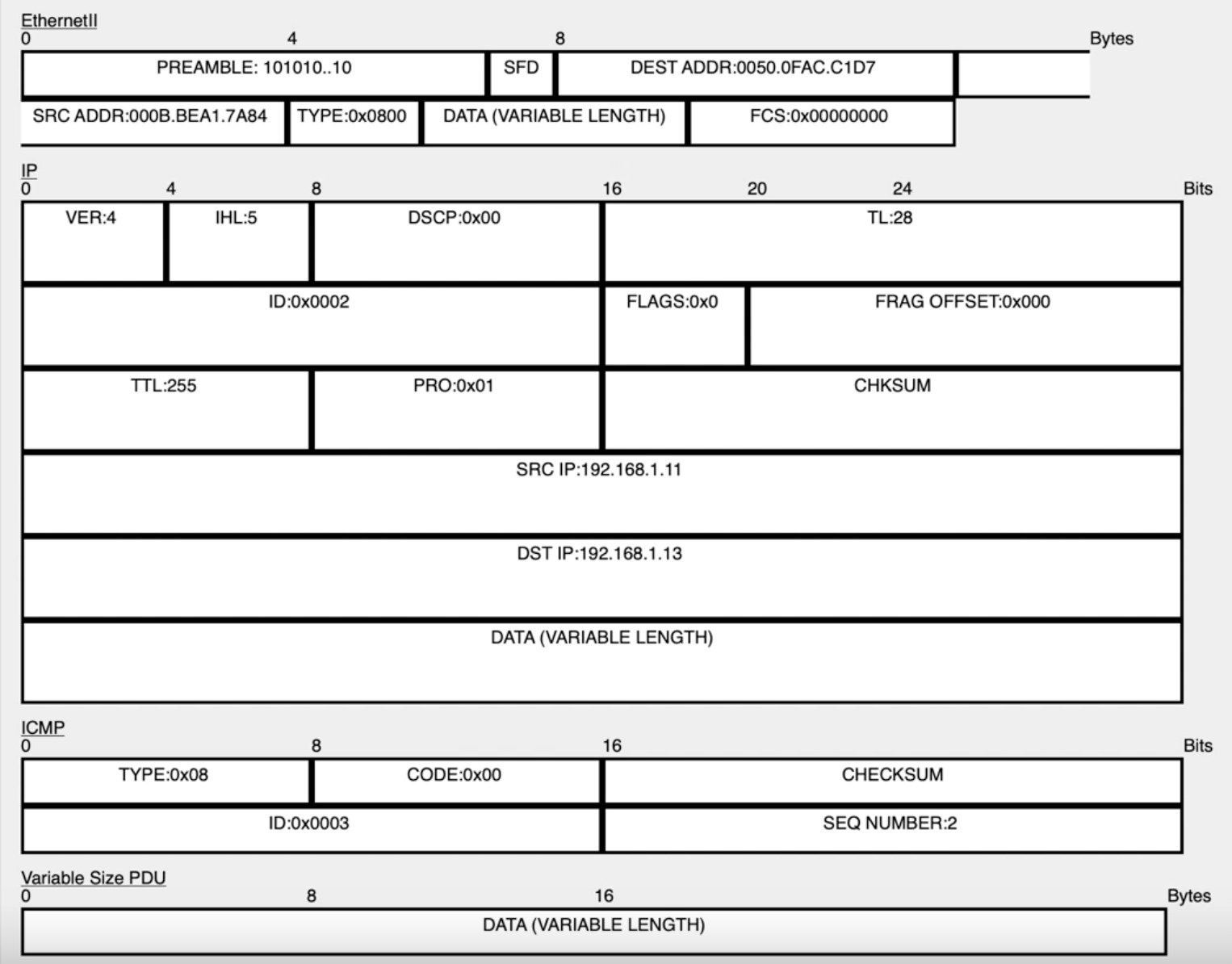
###1.3.2. Знакомство с интерфейсом Packet Tracer

Основное окно программы содержит рабочее пространство (1) с переключением на логическую (Logical) или физическую (Physical) область проекта (2); наверху расположено меню (3), панели инструментов (4)–(5), внизу — меню выбора объекта (7) и его типа (8), а также переключатель режимов работы в реальном времени (Realtime) и в режиме моделирования (Simulation) (6), окно с информацией по пакету данных (9), возникающему в сети во время моделирования.

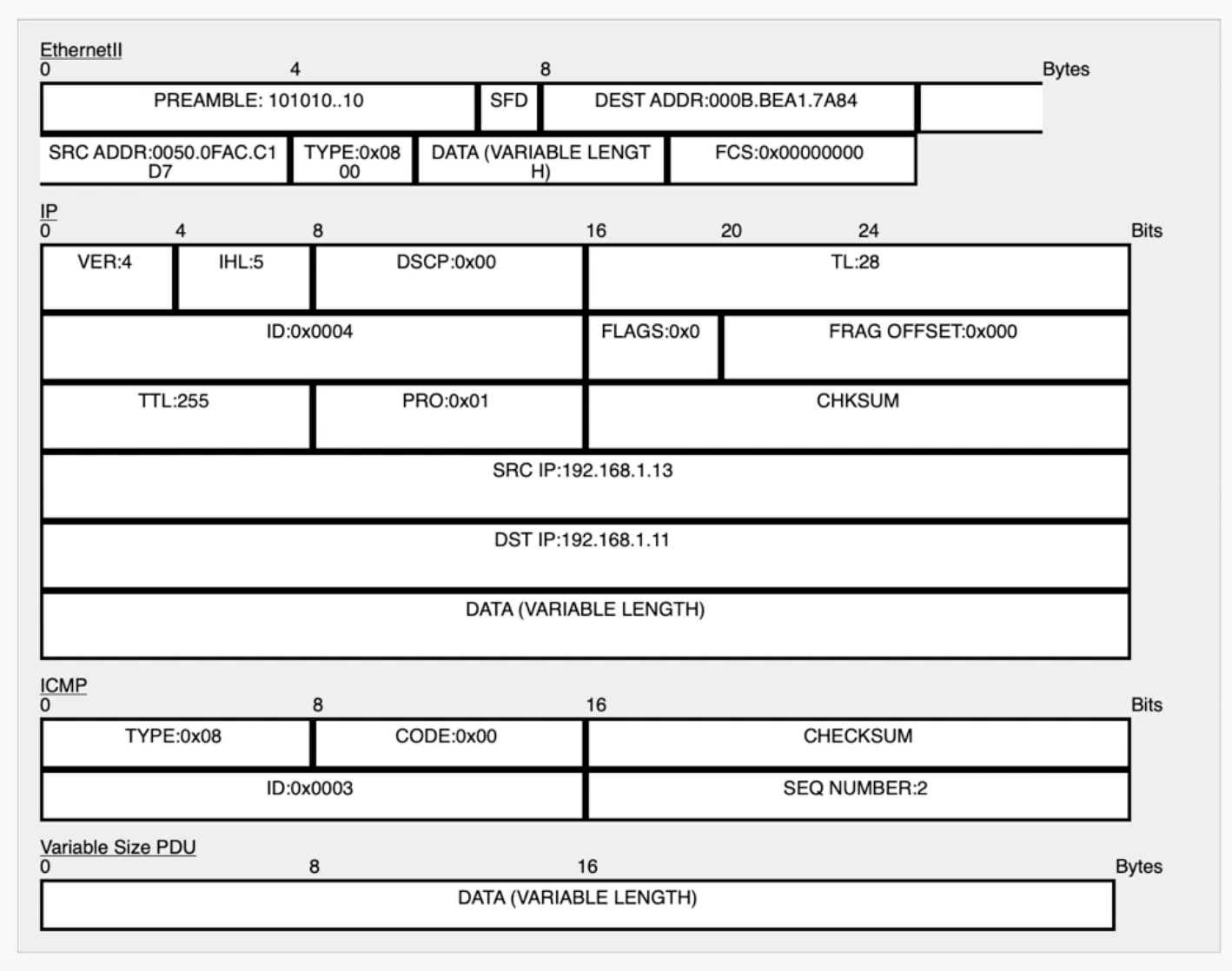
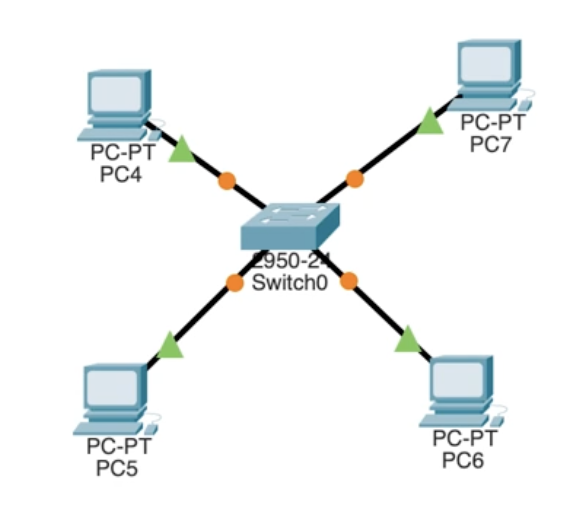
Меню и панель инструментов позволяют создать, открыть, сохранить или распечатать проект, скопировать и вставить элемент, масштабировать рабочее пространство проекта. Также здесь расположены пиктограммы инструментов для работы с проектом и его объектами: инструменты выделения одного или нескольких объектов проекта, добавления и удаления объектов, добавления текстового комментария к элементу проекта и др.

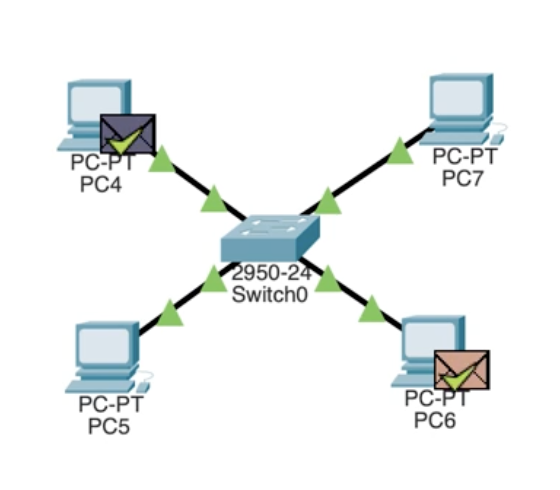
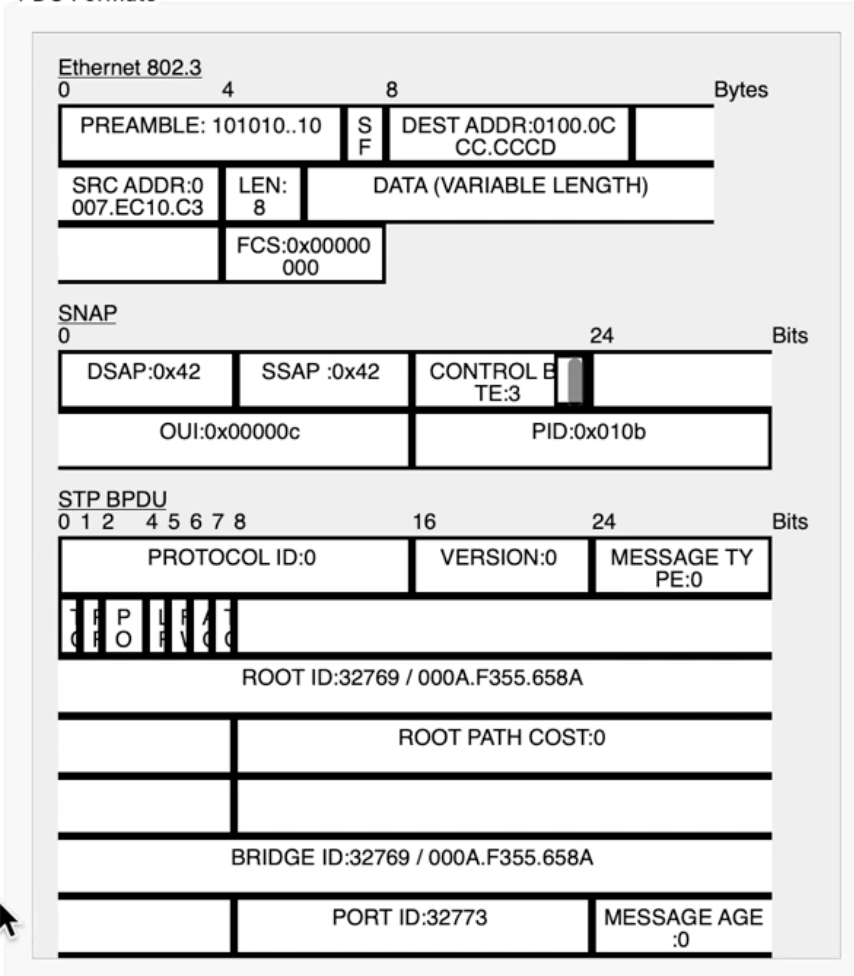
Переключение из режима работы в реальном времени в режим моделирования применяется, если нужно более детально изучить, например, движение передаваемых от устройства к устройству данных, форматы конкретных пакетов.

###1.3.3. Построение простейшей сети

1. Создал новый проект (например, lab\_PT-01.pkt). 
2. В рабочем пространстве разместил концентратор (Hub-PT) и четыре оконечных устройства PC. Соединил оконечные устройства с концентратором прямым кабелем (рис. 1.3). Щёлкнув последовательно на каждом оконечном устройстве, задал 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. 1.4).     
3. В основном окне проекта перешёл из режима реального времени (Realtime) в режим моделирования (Simulation). Выбрал на панели инструментов мышкой «Add Simple PDU (P)» и щёлкнул сначала на PC0, затем на PC2. В рабочей области появились два конверта, обозначающих пакеты, в списке событий на панели моделирования появились два события, относящихся к пакетам ARP и ICMP соответственно (рис. 1.5). На панели моделирования нажал кнопку «Play» и проследил за движением пакетов ARP и ICMP от устройства PC0 до устройства PC2 и обратно. 
4. Щёлкнув на строке события, открыл окно информации о PDU и изучил, что происходило на уровне модели OSI при перемещении пакета (рис. 1.6). Используя кнопку «Проверь себя» (Challenge Me) на вкладке OSI Model, ответил на вопросы.  
5. Открыл вкладку с информацией о PDU (рис. 1.7). Исследовал структуру пакета ICMP. Описал структуру кадра Ethernet. Определил, какие изменения произошли в кадре Ethernet при передвижении пакета. Определил тип кадра Ethernet. Описал структуру MAC-адресов.   Структура кадра Ethernet

* Кадр Ethernet состоит из следующих полей:  
    
   \* Preamble (Прелюдия) – 7 байтовый пролог (101010…10), синхронизирующий приёмник.  
   \* SFD (Start Frame Delimiter) – 1 байт, указывающий начало кадра.  
   \* MAC-адрес отправителя – 6 байтов, в данном случае 00:0B:BE:A1:7A:84.  
   \* MAC-адрес получателя – 6 байтов, в данном случае 00:50:0F:AC:C1:D7.  
   \* EtherType – 2 байта, указывающие тип полезных данных (0x0800, что означает IPv4).  
   \* Данные – переменной длины, содержат IP-пакет.  
   \* FCS (Frame Check Sequence) – 4 байта контрольной суммы.  
    
   Изменения в кадре Ethernet при передвижении пакета  
    
   При прохождении пакета через маршрутизаторы или другие сетевые устройства MAC-адреса источника и назначения изменяются. Внутри одной сети MAC-адрес источника — это адрес отправителя, а MAC-адрес назначения — адрес ближайшего узла (например, маршрутизатора или конечного получателя). Однако IP-адреса остаются неизменными.  
    
   Определение типа кадра Ethernet  
    
   В данном случае поле Type содержит 0x0800, что указывает на протокол IPv4.  
    
   Структура MAC-адресов  
    
   MAC-адрес состоит из 6 байтов (48 бит) и записывается в шестнадцатеричном формате (00:0B:BE:A1:7A:84). Первые 3 байта (OUI) идентифицируют производителя устройства, а оставшиеся 3 байта — уникальный идентификатор.

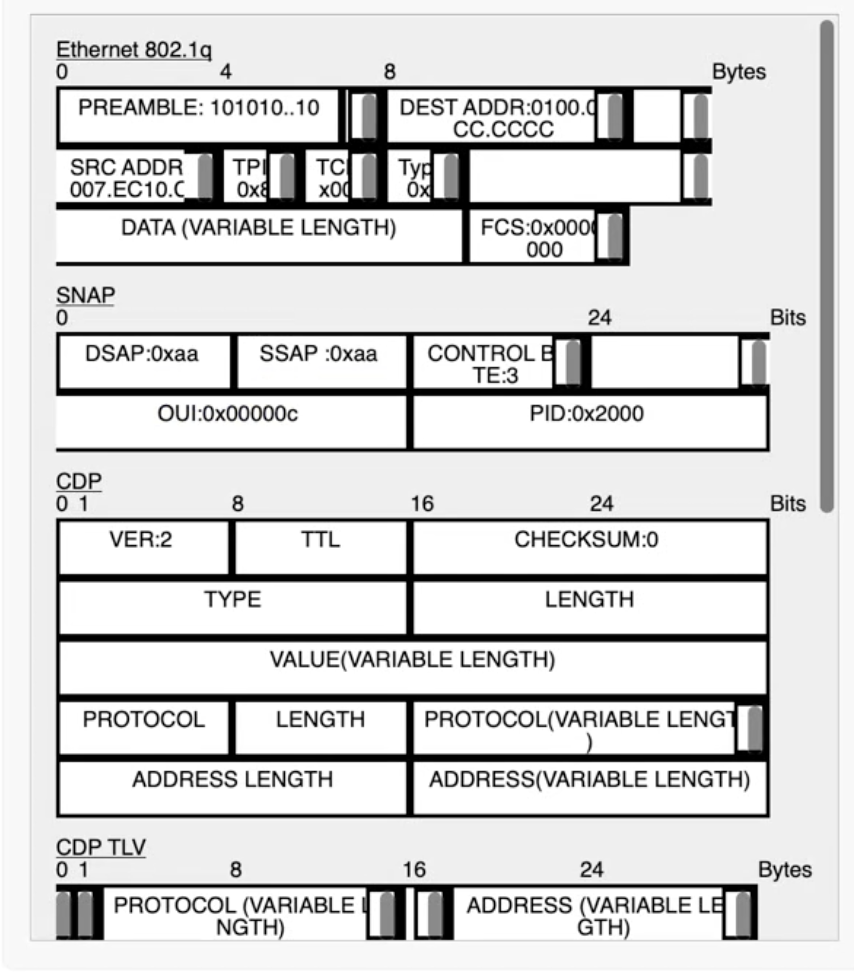
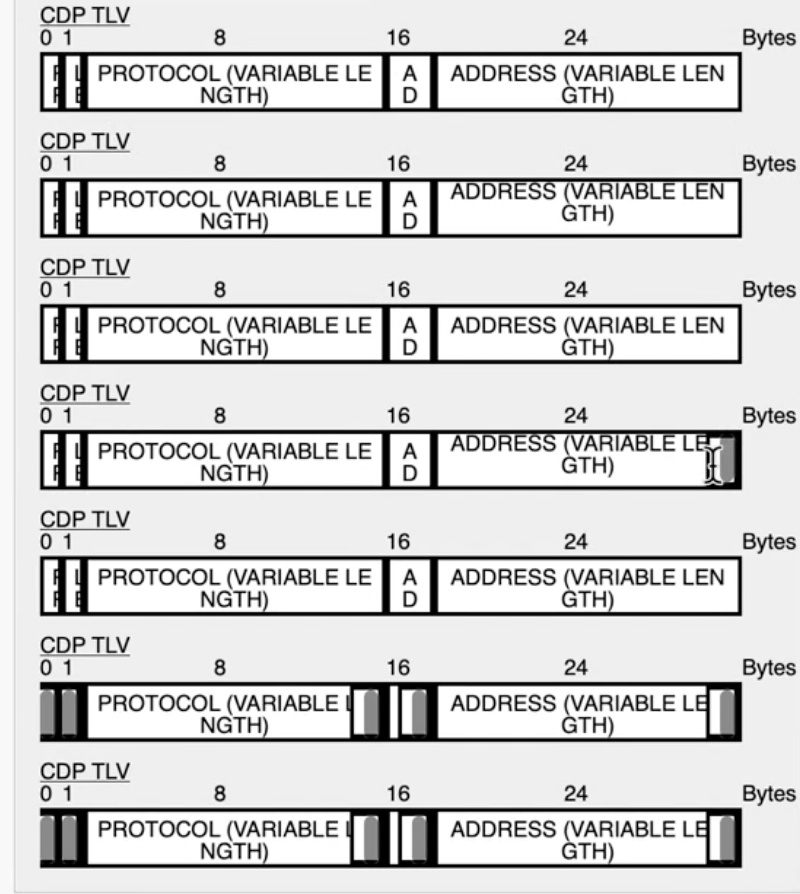
1. Очистил список событий, удалив сценарий моделирования. Выбрал на панели инструментов мышкой «Add Simple PDU (P)» и щёлкнул сначала на PC0, затем на PC2. Снова выбрал на панели инструментов мышкой «Add Simple PDU (P)» и щёлкнул сначала на PC2, затем на PC0. На панели моделирования нажал кнопку «Play» и проследил за возникновением коллизии (рис. 1.8). В списке событий посмотрел информацию о PDU. В отчёте пояснил, как отображалась в заголовках пакетов информация о коллизии и почему возникла коллизия:  
   1. CSMA/CD (Carrier Sense Multiple Access with Collision Detection)
      * В проводных сетях Ethernet (до 1 Гбит/с) используется механизм CSMA/CD.
      * Если станция передаёт кадр и обнаруживает сигнал другой передачи в сети, это означает коллизию.
      * В случае коллизии все узлы прекращают передачу и отправляют JAM-сигнал (специальный битовый паттерн).
      * После этого каждый узел ждёт случайное время (алгоритм экспоненциальной задержки) и повторяет попытку передачи.
   2. Поле FCS (Frame Check Sequence) в заголовке Ethernet
      * Коллизии могут привести к повреждению данных, что обнаруживается по полю FCS (Frame Check Sequence).
      * Если контрольная сумма не совпадает с рассчитанным значением, пакет отбрасывается.
   3. Отсутствие подтверждения доставки на уровне Ethernet
      * Если передача была прервана из-за коллизии, устройство не получит подтверждение и предпримет повторную передачу.
2. Перешёл в режим реального времени (Realtime). В рабочем пространстве разместил коммутатор (например, Cisco 2950-24) и 4 оконечных устройства PC. Соединил оконечные устройства с коммутатором прямым кабелем. Щёлкнув последовательно на каждом оконечном устройстве, задал 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. 
3. В основном окне проекта перешёл из режима реального времени (Realtime) в режим моделирования (Simulation). Выбрал на панели инструментов мышкой «Add Simple PDU (P)» и щёлкнул сначала на PC4, затем на PC6. В рабочей области появились два конверта, обозначающих пакеты, в списке событий на панели моделирования появились два события, относящихся к пакетам ARP и ICMP соответственно (рис. 1.9). На панели моделирования нажал кнопку «Play» и проследил за движением пакетов ARP и ICMP от устройства PC4 до устройства PC6 и обратно. В отчёте пояснил, есть ли различия и в чём они заключались в событиях протокола ARP в сценарии с концентратором:

*  
  1. Коммутатор направляет ARP-запрос только на нужные порты
     + Если MAC-адрес известен, запрос отправляется только на соответствующий порт.
     + Если MAC-адрес неизвестен, запрос всё равно передаётся только в рамках VLAN, а не на все порты.
  2. ARP-ответ передаётся только отправителю
     + В отличие от концентратора, коммутатор направляет ответ только узлу, отправившему запрос.
  3. Меньше коллизий и меньше трафика
     + В коммутируемой сети используется полный дуплекс, что исключает коллизии.
     + Уменьшается количество широковещательного трафика, что улучшает производительность сети.

1. Исследовал структуру пакета ICMP. Описал структуру кадра Ethernet. Определил, какие изменения произошли в кадре Ethernet при передвижении пакета. Определил тип кадра Ethernet. Описал структуру MAC-адресов.
2. Очистил список событий, удалив сценарий моделирования. Выбрал на панели инструментов мышкой «Add Simple PDU (P)» и щёлкнул сначала на PC4, затем на PC6. Снова выбрал на панели инструментов мышкой «Add Simple PDU (P)» и щёлкнул сначала на PC6, затем на PC4. На панели моделирования нажал кнопку «Play» и проследил за движением пакетов. В отчёте пояснил, почему не возникала коллизия.
3. Перешёл в режим реального времени (Realtime). В рабочем пространстве соединил кроссовым кабелем концентратор и коммутатор. Перешёл в режим моделирования (Simulation). Очистил список событий, удалив сценарий моделирования. Выбрал на панели инструментов мышкой «Add Simple PDU (P)» и щёлкнул сначала на PC0, затем на PC4. Снова выбрал на панели инструментов мышкой «Add Simple PDU (P)» и щёлкнул сначала на PC4, затем на PC0. На панели моделирования нажал кнопку «Play» и проследил за движением пакетов. В отчёте пояснил, почему сначала возникала коллизия (рис. 1.10), а затем пакеты успешно достигали пункта назначения.

* Почему сначала возникает коллизия:
  + Коллизия в полудуплексном режиме: Концентратор передаёт полученный сигнал на все порты одновременно, не разделяя домены коллизий. Когда ПК отправляют пакеты почти одновременно (например, PC0 и PC4), их сигналы сталкиваются на общем сегменте. Это классическая ситуация в среде с использованием технологии CSMA/CD, где одновременная передача приводит к коллизии.
  + Отсутствие интеллектуальной коммутации: В отличие от коммутатора, концентратор не умеет направлять кадры только к нужному получателю, а просто ретранслирует сигнал на все порты, что увеличивает вероятность столкновений при одновременной передаче данных.
* Почему после коллизии пакеты доходят до адресата:
  + Механизм обнаружения коллизии (CSMA/CD): После возникновения коллизии все участвующие узлы обнаруживают её, отправляют сигнал о коллизии (jam signal) и прекращают передачу. Затем используется алгоритм экспоненциального случайного ожидания, благодаря которому устройства повторно инициируют передачу пакетов в разные моменты времени.
  + Устранение коллизии: При повторных попытках, благодаря случайной задержке, устройства начинают передавать пакеты последовательно, избегая повторной коллизии. Таким образом, пакеты успешно доставляются до пункта назначения.

В итоге, первоначальная коллизия — следствие одновременной передачи в условиях общего (коллизионного) сегмента сети с концентратором, а дальнейшая успешная доставка пакетов обеспечивается корректной работой алгоритма CSMA/CD, который управляет повторными попытками передачи после обнаружения коллизии.

1. Очистил список событий, удалив сценарий моделирования. На панели моделирования нажал «Play» и в списке событий получил пакеты STP (рис. 1.11). Исследовал структуру STP. Описал структуру кадра Ethernet в этих пакетах. Определил тип кадра Ethernet. Описал структуру MAC-адресов.
2. Перешёл в режим реального времени (Realtime). В рабочем пространстве добавил маршрутизатор (например, Cisco 2811). Соединил прямым кабелем коммутатор и маршрутизатор (рис. 1.12). Щёлкнул на маршрутизаторе и на вкладке его конфигурации прописал статический IP-адрес 192.168.1.254 с маской 255.255.255.0, активировал порт, поставив галочку «On» напротив «Port Status» (рис. 1.13).
3. Перешёл в режим моделирования (Simulation). Очистил список событий, удалив сценарий моделирования. Выбрал на панели инструментов мышкой «Add Simple PDU (P)» и щёлкнул сначала на PC3, затем на маршрутизаторе. На панели моделирования нажал кнопку «Play» и проследил за движением пакетов ARP, ICMP, STP и CDP. Исследовал структуру пакета CDP, описал структуру кадра Ethernet. Определил тип кадра Ethernet. Описал структуру MAC-адресов.   Ниже приведён подробный анализ выполненных действий и описание изученных структур:
   1. Сценарий моделирования После перехода в режим моделирования (Simulation) пользователь очистил список событий, удалив предыдущий сценарий. Затем с помощью инструмента «Add Simple PDU (P)» был инициирован обмен сообщениями – сначала был выбран ПК (PC3), затем маршрутизатор. При запуске симуляции («Play») можно было проследить прохождение различных типов пакетов, таких как ARP, ICMP, STP и CDP.
   2. Исследование пакета CDP CDP (Cisco Discovery Protocol) – это проприетарный протокол Cisco, используемый для обнаружения соседних устройств. Его особенности:
      * Инкапсуляция: Пакет CDP инкапсулируется в Ethernet-кадр, но не как классический Ethernet II кадр, а с использованием заголовка LLC (Logical Link Control).
      * Заголовок LLC: В LLC-подзаголовке устанавливаются следующие поля:
      * DSAP (Destination Service Access Point): обычно 0xAA
      * SSAP (Source Service Access Point): также 0xAA
      * Контрольное поле: обычно имеет значение 0x03
      * Заголовок SNAP: После LLC следует заголовок SNAP, который содержит:
      * OUI (Organizationally Unique Identifier): для Cisco обычно 00-00-0C
      * Поле PID (Protocol Identifier): для CDP – значение 0x2000
      * TLV-блоки: Основная полезная нагрузка представлена набором TLV (Type-Length-Value) блоков, где содержатся такие данные, как идентификатор устройства (Device-ID), идентификатор порта (Port-ID), возможности устройства, версия программного обеспечения, платформа и другие параметры.
   3. Структура Ethernet-кадра Стандартный Ethernet-кадр состоит из нескольких основных полей:
      * Преамбула и SFD:
      * Преамбула (7 байт) и Start Frame Delimiter (SFD, 1 байт) используются для синхронизации приема.
      * Адресация:
      * MAC-адрес получателя (6 байт)
      * MAC-адрес отправителя (6 байт)
      * Поле EtherType/Length:
      * В Ethernet II кадрах это 2 байта, которые указывают тип протокола (например, 0x0800 для IP).
      * В случае LLC/SNAP инкапсуляции, как у CDP, значение EtherType может не использоваться напрямую – вместо этого информация о протоколе передается через поля LLC (DSAP, SSAP) и SNAP.
      * Поле данных (Payload):
      * Содержит полезную нагрузку, длиной от 46 до 1500 байт.
      * Контрольная последовательность (FCS):
      * 4 байта, используемые для контроля целостности кадра.
   4. Определение типа Ethernet-кадра В рассматриваемом случае пакет CDP передаётся не как обычный Ethernet II кадр, а как 802.2 LLC кадр с последующей индикацией протокола через SNAP.
      * Значения DSAP и SSAP (0xAA) в LLC заголовке указывают на использование протоколов, определяемых посредством SNAP.
      * SNAP-заголовок, в свою очередь, содержит поле, в котором протокол CDP идентифицируется значением 0x2000. Таким образом, тип кадра определяется как кадр с LLC/SNAP инкапсуляцией (а не как стандартный Ethernet II кадр).
   5. Структура MAC-адресов MAC-адрес – уникальный идентификатор, присваиваемый каждому сетевому интерфейсу, имеет следующие особенности:
      * Длина: 48 бит (6 байт).
      * Формат представления: Обычно записывается как шесть групп по две шестнадцатеричные цифры, разделённых двоеточиями или тире (например, 00:1A:2B:3C:4D:5E).
      * Структура:
      * OUI (Organizationally Unique Identifier): первые 3 байта, которые идентифицируют производителя (например, Cisco имеет свой OUI, часто начинающийся с 00-00-0C).
      * Идентификатор устройства: оставшиеся 3 байта, уникальные для конкретного устройства.

# 4 Выводы

Установил инструмент моделирования конфигурации сети Cisco Packet Tracer, ознакомился с его интерфейсом.

#1.5. Контрольные вопросы

1. Определения сетевого оборудования и их применение

* Определения сетевого оборудования и их применение {#tbl:std-dir}

| Устройство | Определение | Когда использовать |
| --- | --- | --- |
| Концентратор (Hub) | Устройство, передающее все входящие пакеты на все порты без обработки. Работает на уровне 1 (физический уровень) модели OSI. | Используется в простых сетях с небольшим количеством устройств, но из-за высокой нагрузки и коллизий в сети почти не применяется. |
| Коммутатор (Switch) | Интеллектуальное устройство, передающее пакеты только целевому MAC-адресу. Работает на уровне 2 (канальный уровень) OSI. | Используется для соединения компьютеров в локальной сети (LAN) для увеличения скорости и уменьшения коллизий. |
| Маршрутизатор (Router) | Устройство, соединяющее разные сети и определяющее маршруты пакетов по IP-адресам. Работает на уровне 3 (сетевой уровень) OSI. | Используется для связи локальных сетей между собой и подключения к интернету. |
| Шлюз (Gateway) | Устройство или программный компонент, преобразующий протоколы между разными сетями. Может работать на любом уровне OSI. | Используется для связи между разными типами сетей (например, между IPv4 и IPv6 или LAN и VPN). |

1. Определения сетевых терминов
   * IP-адрес – уникальный числовой идентификатор устройства в сети, например, 192.168.1.1 (IPv4) или 2001:db8::1 (IPv6).
   * Сетевая маска (Subnet Mask) – определяет, какая часть IP-адреса относится к сети, а какая к устройству. Например, 255.255.255.0 означает, что первые три октета – это сеть, а последний – хост.
   * Broadcast-адрес – специальный адрес для отправки данных всем устройствам в сети. Например, для 192.168.1.0/24 широковещательный адрес – 192.168.1.255.
2. Проверка доступности узла в сети
   1. Ping – отправка ICMP-запроса:
   * ping 192.168.1.1
   * Проверяет, отвечает ли устройство на запросы.
   1. Traceroute (tracert в Windows) – отслеживание маршрута до узла:
   * traceroute 8.8.8.8 # Linux/macOS  
     tracert 8.8.8.8 # Windows
   * Показывает, через какие узлы проходит трафик.
   1. NSLookup/Dig – проверка DNS:
   * nslookup google.com # Windows  
     dig google.com # Linux/macOS
   * Проверяет, правильно ли работает доменное имя.
   1. Telnet – проверка доступности порта:
   * telnet 192.168.1.1 80
   * Полезно для проверки доступности веб-серверов.
   1. Netcat (nc) – аналог telnet, но с расширенными возможностями:
   * nc -zv 192.168.1.1 22
   * Проверяет открытые порты.

# Список литературы