Лабораторная работа № 1. Знакомство с Cisco Packet Tracer

1.1. Цель работы

Установка инструмента моделирования конфигурации сети Cisco Packet Tracer [3], знакомство с его интерфейсом.

1.2. Задание

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

1.3. Последовательность выполнения работы

1.3.1. Запуск Cisco Packet Tracer без использования сетевого соединения

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

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.

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

Рабочее пространство Packet Tracer представлено на рис. 1.1.

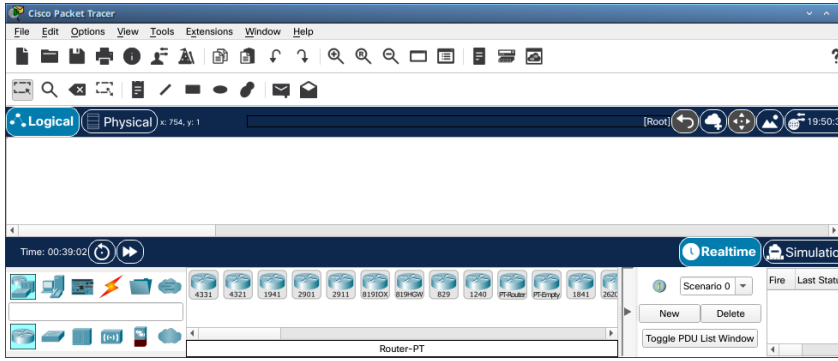

Рис. 1.1. Рабочее пространство Packet Tracer

На рис. 1.2 представлена структура интерфейса Packet Tracer.

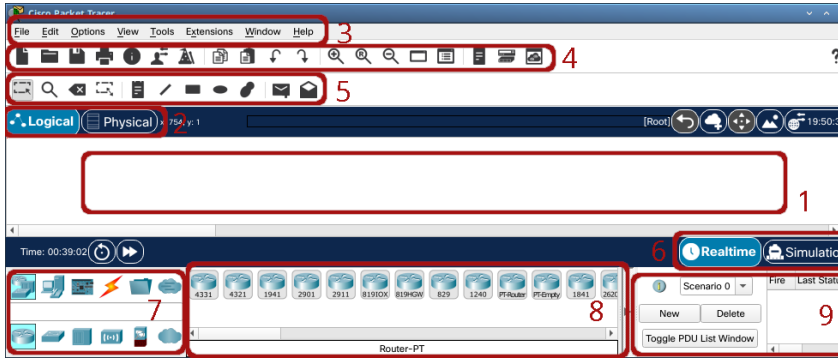

Рис. 1.2. Структура интерфейса Packet Tracer

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. Создайте новый проект (например, `lab_PT-01.pkt`).
2. В рабочем пространстве разместите концентратор (Hub-PT) и четыре оконечных устройства PC. Соедините оконечные устройства с концентратором прямым кабелем (рис. 1.3). 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. 1.4).

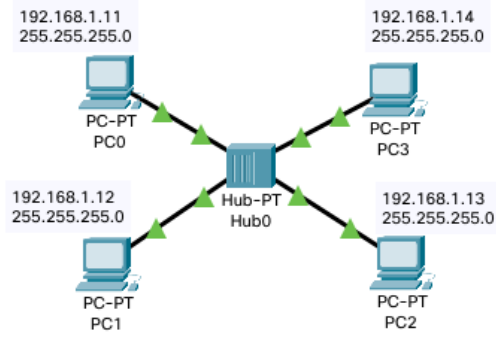

Рис. 1.3. Модель простой сети с концентратором

3. 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 (рис. 1.5). На панели моделирования нажмите кнопку «Play» и проследите за движением пакетов ARP и ICMP от устройства PC0 до устройства PC2 и обратно.

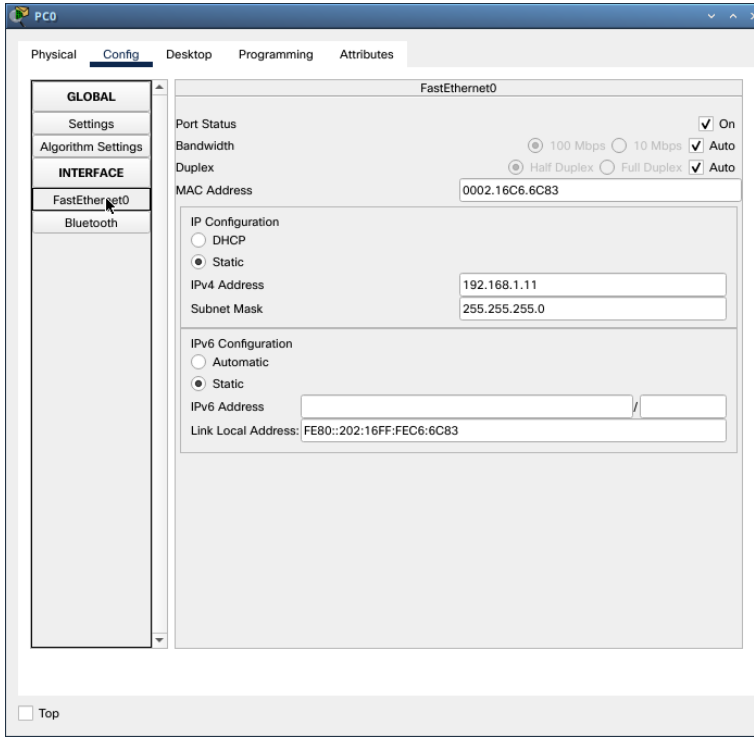

Рис. 1.4. Настройка статического IP-адреса на оконечном устройстве

4. Щёлкнув на строке события, откройте окно информации о PDU и изучите, что происходит на уровне модели OSI при перемещении пакета (рис. 1.6). Используя кнопку «Проверь себя» (Challenge Me) на вкладке OSI Model, ответьте на вопросы.
5. Откройте вкладку с информацией о PDU (рис. 1.7). Исследуйте структуру пакета ICMP. Опишите структуру кадра Ethernet. Какие изменения происходят в кадре Ethernet при передвижении пакета? Какой тип имеет кадр Ethernet? Опишите структуру MAC-адресов.
6. 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. 1.8). В списке событий посмотрите информацию о PDU. В отчёте поясните, как отображается в заголовках пакетов информация о коллизии и почему возникла коллизия.

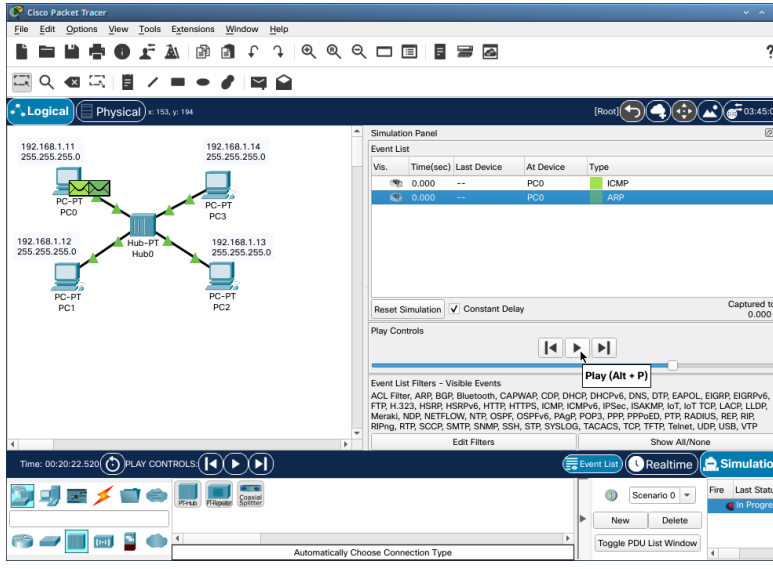

Рис. 1.5. События в режиме моделирования Packet Tracer

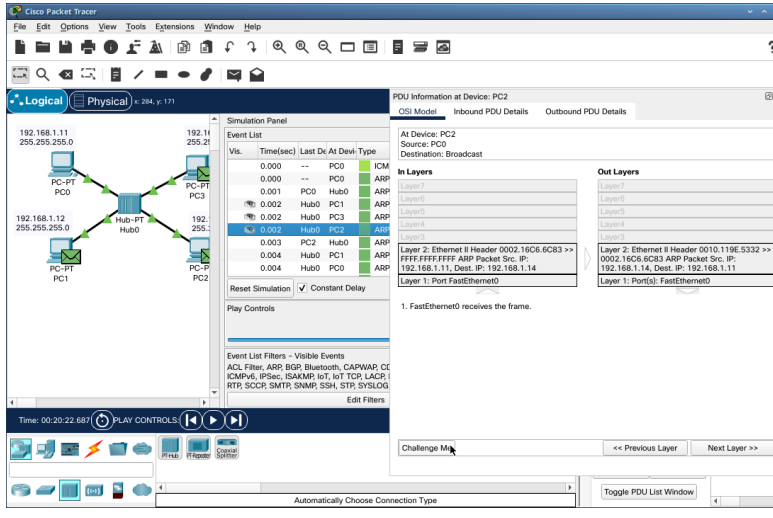

Рис. 1.6. Информация о PDU: уровень OSI

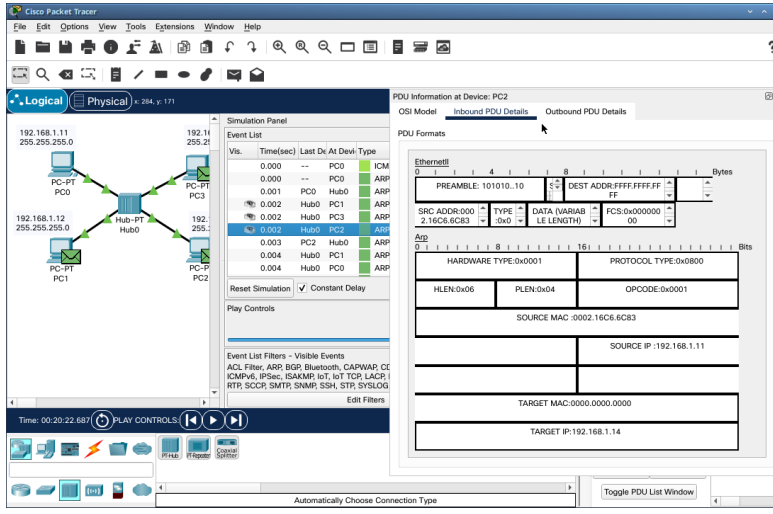

Рис. 1.7. Информация о PDU: форматы пакетов

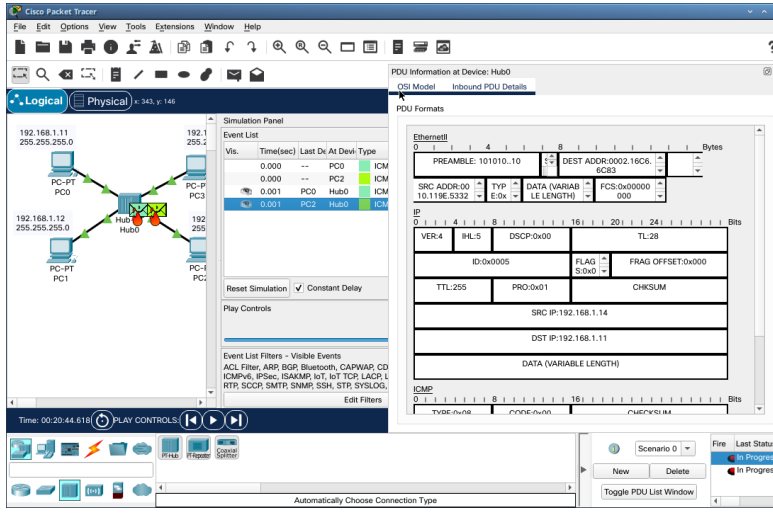

Рис. 1.8. Сценарий с возникновением коллизии

7. 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.

8. 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 (рис. 1.9). На панели моделирования нажмите кнопку «Play» и проследите за движением пакетов ARP и ICMP от устройства PC4 до устройства PC6 и обратно. В отчёте поясните, есть ли различия и в чём они заключаются в событиях протокола ARP в сценарии с концентратором.

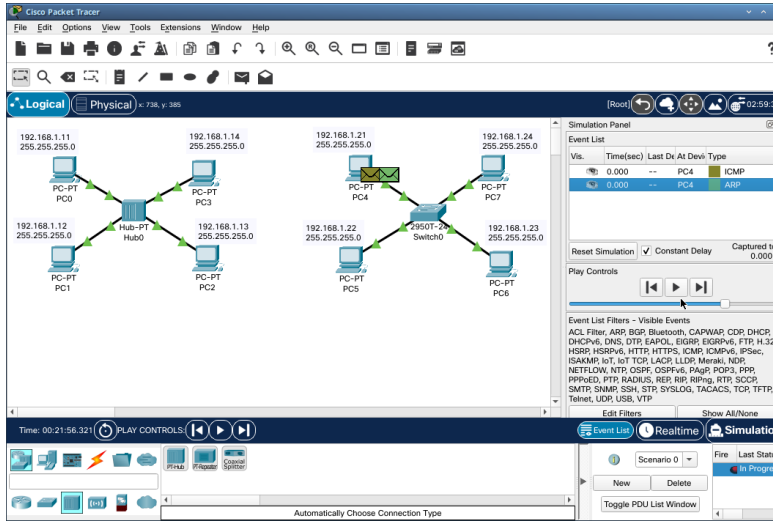

Рис. 1.9. Модель простой сети с коммутатором

9. Исследуйте структуру пакета ICMP. Опишите структуру кадра Ethernet. Какие изменения происходят в кадре Ethernet при передвижении пакета? Какой тип имеет кадр Ethernet? Опишите структуру MAC-адресов.
10. 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. В отчёте поясните, почему не возникает коллизия.
11. 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. В отчёте поясните, почему сначала возникает коллизия (рис. 1.10), а затем пакеты успешно достигают пункта назначения.

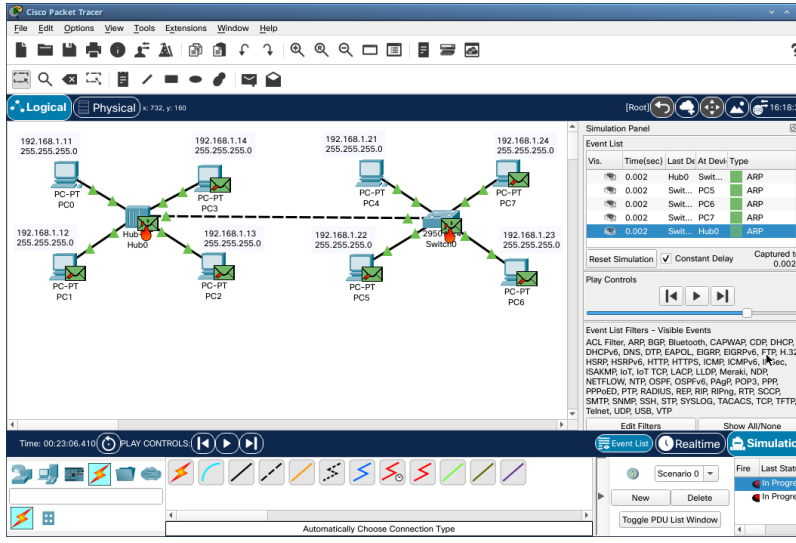

Рис. 1.10. Сценарий с возникновением коллизии

12. Очистите список событий, удалив сценарий моделирования. На панели моделирования нажмите «Play» и в списке событий получите пакеты STP (рис. 1.11). Исследуйте структуру STP. Опишите структуру кадра Ethernet в этих пакетах. Какой тип имеет кадр Ethernet? Опишите структуру MAC-адресов.
13. Перейдите в режим реального времени (Realtime). В рабочем пространстве добавьте маршрутизатор (например, Cisco 2811). Соедините прямым кабелем коммутатор и маршрутизатор (рис. 1.12). 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. 1.13).
14. 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. Исследуйте структуру пакета CDP, опишите структуру кадра Ethernet. Какой тип имеет кадр Ethernet? Опишите структуру MAC-адресов.

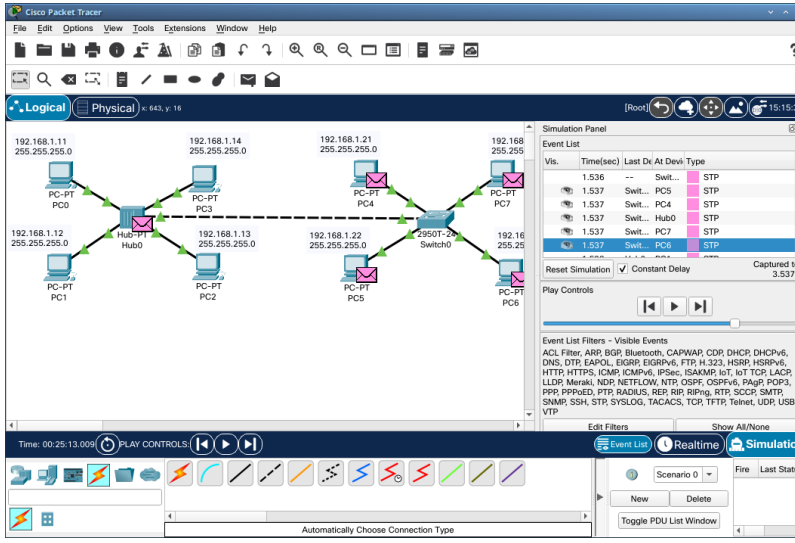

Рис. 1.11. Сценарий с протоколом STP

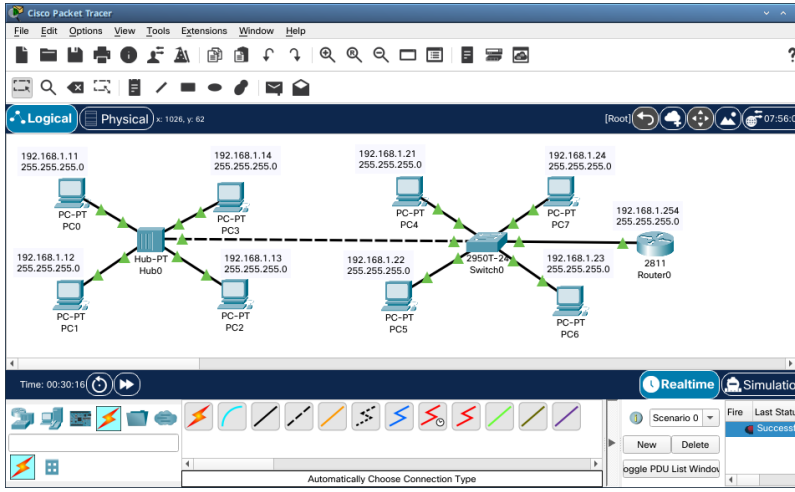

Рис. 1.12. Модель простой сети с маршрутизатором

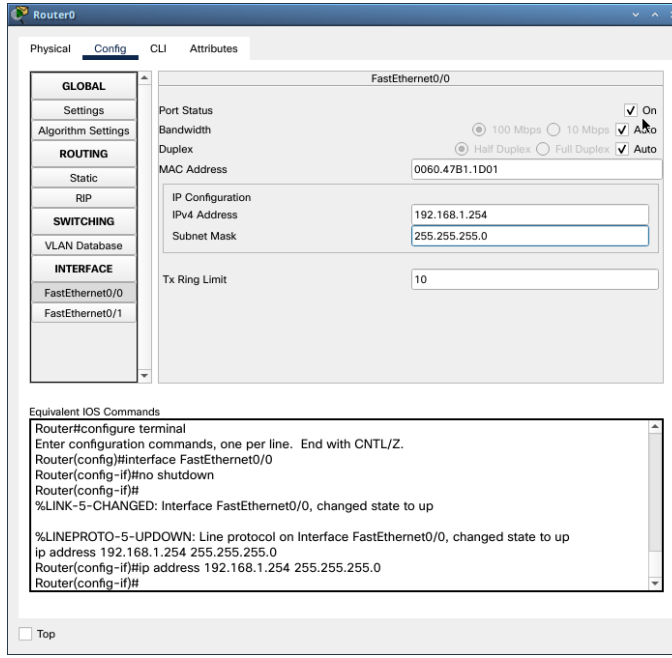

Рис. 1.13. Активация порта на маршрутизаторе

1.4. Содержание отчёта

1. Титульный лист с указанием номера лабораторной работы и ФИО студента.
2. Формулировка задания работы.
3. Описание результатов выполнения задания:
   - скриншоты (снимки экрана), фиксирующие выполнение лабораторной работы;
   - резюме содержания часового курса академии Cisco;
   - описание основных панелей и меню интерфейса Packet Tracer.
4. Выводы, согласованные с заданием работы.
5. Ответы на контрольные вопросы.

1.5. Контрольные вопросы

1. Дайте определение следующим понятиям: концентратор, коммутатор, маршрутизатор, шлюз (gateway). В каких случаях следует использовать тот или иной тип сетевого оборудования?
2. Дайте определение следующим понятиям: ip-адрес, сетевая маска, broadcast-адрес.
3. Как можно проверить доступность узла сети?

При ответах на вопросы рекомендуется ознакомиться с информацией из источников [3; 4; 14; 18; 20—24].

Литература по теме

1. 802.1D-2004 - IEEE Standard for Local and Metropolitan Area Networks. Media Access Control (MAC) Bridges : тех. отч. / IEEE. — 2004. — С. 1—277. — DOI: 10.1109/IEEESTD.2004.94569. — URL: http://ieeexplore.ieee.org/servlet/opac?punumber=9155.
2. 802.1Q - Virtual LANs. — URL: http://www.ieee802.org/1/pages/802.1Q.html.
3. *A J.* Packet Tracer Network Simulator. — Packt Publishing, 2014. — ISBN 9781782170426. — URL: https://books.google.com/books?id=eVOcAgAAQBAJ&dq=cisco+packet+tracer&hl=es&source=gbs_navlinks_s.
4. *Cotton M., Vegoda L.* Special Use IPv4 Addresses : RFC / RFC Editor. — 01.2010. — С. 1—11. — № 5735. — DOI: 10.17487/rfc5735. — URL: https://www.rfc-editor.org/info/rfc5735.
5. *Droms R.* Dynamic Host Configuration Protocol : RFC / RFC Editor. — 03.1997. — С. 1—45. — № 2136. — DOI: 10.17487/rfc2131. — URL: https://www.ietf.org/rfc/rfc2131.txt%20https://www.rfc-editor.org/info/rfc2131.
6. *McPherson D., Dykes B.* VLAN Aggregation for Efficient IP Address Allocation, RFC 3069. — 2001. — URL: http://www.ietf.org/rfc/rfc3069.txt.
7. *Moy J.* OSPF Version 2 : RFC / RFC Editor. — 1998. — С. 244. — DOI: 10.17487/rfc2328. — URL: https://www.rfc-editor.org/info/rfc2328.
8. NAT Order of Operation. — URL: https://www.cisco.com/c/en/us/support/docs/ip/network-address-translation-nat/6209-5.html.
9. NAT: вопросы и ответы / Сайт поддержки продуктов и технологий компании Cisco. — URL: https://www.cisco.com/cisco/web/support/RU/9/92/92029_nat-faq.html.
10. *Neumann J. C.* Cisco Routers for the Small Business A Practical Guide for IT Professionals. — Apress, 2009.
11. *Odom S., Nottingham H.* Cisco Switching: Black Book. — The Coriolis Group, 2001. — ISBN 9781576107065. — URL: http://books.google.sk/books?id=GYsLAAAACAAJ.
12. *Tetz E.* Cisco Networking All-in-One For Dummies. — Indianapolis, Indiana : John Wiley & Sons, Inc., 2011. — (For Dummies). — URL: http://www.dummies.com/store/product/Cisco-Networking-All-in-One-For-Dummies.productCd-0470945583.html.
13. ГОСТ Р ИСО/МЭК 7498-1-99. — «ВОС. Базовая эталонная модель. Часть 1. Базовая модель». — ОКС: 35.100.70. — Действует с 01.01.2000. — URL: http://protect.gost.ru/v.aspx?control=7&id=132355.
14. *Кларк К., Гамильтон К.* Принципы коммутации в локальных сетях Cisco. — М. : Вильямс, 2003. — (Cisco Press Core Series). — ISBN 5-8459-0464-1.

15. *Королькова А. В.*, *Кулябов Д. С.* Архитектура и принципы построения современных сетей и систем телекоммуникаций. — М. : Издательство РУДН, 2009.

16. *Королькова А. В.*, *Кулябов Д. С.* Прикладные протоколы Интернет и www. Курс лекций. — М. : РУДН, 2012. — ISBN 9785209049500.

17. *Королькова А. В.*, *Кулябов Д. С.* Прикладные протоколы Интернет и www. Лабораторные работы. — М. : РУДН, 2012. — ISBN 9785209049357.

18. *Королькова А. В.*, *Кулябов Д. С.* Сетевые технологии. Лабораторные работы. — М. : РУДН, 2014. — ISBN 785209056065.

19. *Куроуз Д. Ф.*, *Росс К. В.* Компьютерные сети. Нисходящий подход. — 6-е изд. — М. : Издательство «Э», 2016. — (Мировой компьютерный бестселлер).

20. *Одом У.* Официальное руководство Cisco по подготовке к сертификационным экзаменам CCENT/CCNA ICND1 100-101. — М. : Вильямс, 2017. — (Cisco Press Core Series). — ISBN 978-5-8459-1906-9.

21. *Одом У.* Официальное руководство Cisco по подготовке к сертификационным экзаменам CCNA ICND2 200-101. Маршрутизация и коммутация. — М. : Вильямс, 2016. — (Cisco Press Core Series).

22. *Олифер В. Г.*, *Олифер Н. А.* Компьютерные сети. Принципы, технологии, протоколы. — 5-е изд. — Питер : Питер, 2017. — (Учебник для вузов). — ISBN 978-5-496-01967-5.

23. Сети и системы передачи информации: телекоммуникационные сети / К. Е. Самуйлов [и др.]. — М. : Изд-во Юрайт, 2016. — ISBN 978-5-9916-7198-9.

24. *Таненбаум Э.*, *Уэзеролл Д.* Компьютерные сети. — 5 изд. — Питер : Питер, 2016. — (Классика Computer Science). — ISBN 978-5-496-00831-0.

25. *Хилл Б.* Полный справочник по Cisco. — М. : Вильямс, 2009. — ISBN 978-5-8459-1309-8.

26. Цикл статей «Сети для самых маленьких». — URL: `http://linkmeup.ru/blog/11.html`.

27. Часто задаваемые вопросы технологии NAT / Сайт поддержки продуктов и технологий компании Cisco. — URL: `https://www.cisco.com/c/ru_ru/support/docs/ip/network-address-translation-nat/26704-nat-faq-00.html`.