**ОБЩИЕ УКАЗАНИЯ**

Лабораторная работа по дисциплине *«Архитектура компьютерных систем*» направлена на углубление теоретических знаний и получение практических навыков работы с компьютерными сетями. Для того, чтобы участвовать в лабораторных работах, студенты должны пройти теоретическую часть курса. Их заранее обучают технике охраны труда в компьютерных лабораториях, подписывая учебный лист. Знание теоретического материала имеет важное значение. Студенты должны быть знакомы с теоретическим материалом, относящимся к соответствующей теме, и понимать, как ведется лаборатория. Присутствие преподавателя или ассистента является обязательным на всей территории лаборатории. Они окажут помощь и сориентацию во время работы. Лабораторное оборудование, включая компьютеры и любое специфическое оборудование (например, микропроцессорный эмулятор), должно использоваться в соответствии с соответствующими инструкциями. Каждому ученику дается задание в индивидуальном порядке. По окончании лабораторной работы студент сообщает профессору или ассистенту код программы и полученные результаты.

К базовым элементам для отчетности относятся: наименование и цель работы, код программы, результаты выполнения программы. Крайним сроком сдачи лабораторной работы является дата выполнения следующей работы. Все лабораторные работы в текущем цикле будут выполняться в среде моделирования Cisco **Packet Tracer 6.0.1 студенческой** версии.

**ВВЕДЕНИЕ В CISCO PACKET TRACER 6.0.1**

Cisco Packet Tracer — это инструмент моделирования и визуализации сети, который позволяет пользователям настраивать различное телекоммуникационное оборудование Cisco, включая коммутаторы, маршрутизаторы, IP-телефоны, шлюзы, серверы и сетевые дисплеи. Его простой в использовании интерфейс позволяет легко создавать и настраивать сеть независимо от знания сетевых технологий или оборудования Cisco. Программное обеспечение используется для проектирования сетей, обучения, подготовки к сертификационным экзаменам CCNA/CCNP, а также получения практических навыков обучения сетевых администраторов и устранения неполадок в устройствах Cisco.

Несмотря на то, что Cisco Packet Tracer не доступен для бесплатного скачивания (доступен только членам Сетевой академии Cisco), в сети можно легко найти дистрибутив. Для лабораторных работ мы продолжим использовать Cisco Pscket Tracer версии 6.0.2 для студентов. При использовании Cisco Packet Tracer необходимо указать, что вы хотите использовать гостевой доступ. Кроме того, существуют бесплатные версии Cisco Packet Tracer для Android и iOS.

Cisco Packet Tracer — это универсальное приложение, используемое в различных областях, включая обучение сетевым технологиям, сертификацию Cisco, разработку приложений, проектирование сетей, дистанционное обучение, тестирование устройств и протоколов, моделирование сетевой безопасности, обучение работе в чрезвычайных ситуациях и подготовку к карьере. Он предоставляет безопасную среду для изучения и отработки концепций сетей, позволяя ИТ-специалистам тестировать и проверять настройки, разрабатывать приложения и сервисы в моделируемой сетевой среде, а также проектировать и планировать компьютерные сети. Это также помогает в обеспечении готовности к чрезвычайным ситуациям и восстановлении после стихийных бедствий в телекоммуникациях и сетях. В целом, Cisco Packet Tracer является ценным инструментом для профессионалов в различных областях.

Cisco Packet Tracer — это программное обеспечение, которое предлагает множество преимуществ в обучении и развитии компьютерных сетей. Он предоставляет виртуальную лабораторную среду для настройки и тестирования сетей без физического оборудования, снижая затраты и облегчая доступ к ресурсам. Он также обеспечивает интерактивное обучение, позволяя учащимся создавать, изменять и экспериментировать с сетевыми топологиями в безопасной среде. Программное обеспечение доступно бесплатно, что позволяет образовательным учреждениям развивать навыки работы в сети. Он обеспечивает реалистичное моделирование поведения сетевых устройств, экономит время на настройку, поддерживает различные устройства, развивает практические навыки, облегчает совместную работу, позволяет экспериментировать с передовыми протоколами, а также позволяет осуществлять мониторинг и устранение неполадок.

Виртуальная лабораторная среда Cisco Packet Tracer позволяет пользователям создавать, настраивать и экспериментировать с компьютерными сетями. Он предлагает несколько функций, в том числе создание сетевых топологий, позволяющих конфигурировать и тестировать сетевые устройства и протоколы, обеспечивать эмпирическое обучение и демонстрацию устройств Cisco. Виртуальная среда также облегчает тестирование сетевых протоколов, включая TCP/IP, OSPF, EIGRP и VLAN. Он также предоставляет симуляции безопасности и обучение по управлению инцидентами безопасности. Packet Tracer полезен для учебных заведений и преподавателей, обеспечивая интерактивный и безопасный способ обучения компьютерным сетям. Он также обеспечивает гибкость и экономию времени без физического оборудования.

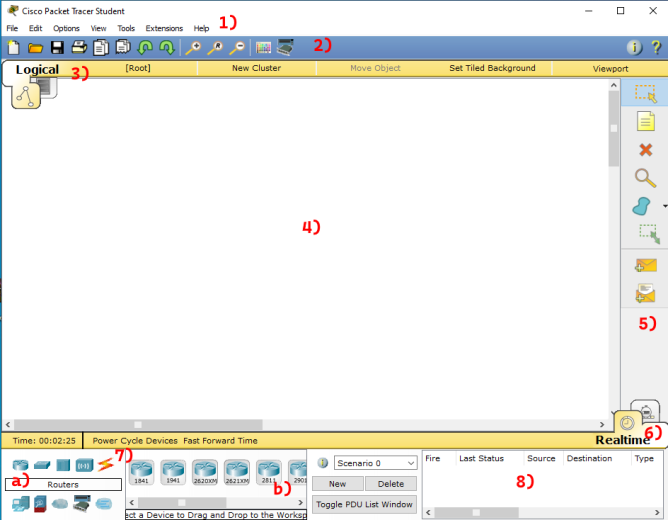
**Лабораторная работа No1  
ПРОЕКТИРОВАНИЕ ПОДСЕТЕЙ НА БАЗЕ КОММУТАТОРА**

1. **Цель работы**: понять концепцию проектирования подсетей, провести практические занятия по проектированию и настройке подсетей и развить практические навыки использования сетевого оборудования.
2. **Общие теоретические понятия**

Главное рабочее окно в Cisco Packet Tracer — это центральный интерфейс, в котором выполняется проектирование, настройка и моделирование сети. Это окно открывается автоматически при запуске программы и служит отправной точкой для всех последующих операций.

После запуска Cisco Packet Tracer пользователь будет постоянно взаимодействовать с главным рабочим окном для создания, настройки и анализа различных элементов сети. Это окно предоставляет доступ к широкому спектру инструментов и ресурсов, необходимых для моделирования сложных сетей и конкретных сценариев.

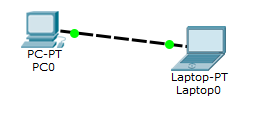
1. ***Главное рабочее окно Трассировщик пакетов***
2. **Вкладки логической/физической рабочей области**. Логические/физические рабочие области используются для переключения между логическими и физическими рабочими областями.
3. **Рабочая область.** Рабочая область - это основная рабочая область в Packet Tracer, где создается необходимая топология (конфигурация сети) и отображается симуляция процесса сетевого взаимодействия.
4. **Панель общих инструментов.** Общая панель инструментов - предоставляет возможность выбора инструментов для работы с сетевыми диаграммами, таких как выбор и изменение местоположения устройств, выделение и изменение положения устройств, размещение меток и примечаний, удаление, изменение размера и выбор простого (Simple PDU) или сложного (Complex PDU) пользовательского блока данных.



***Рисунок 1.1. Главное рабочее окно***

1. **Вкладки реального времени/симуляции.** Переключатель выбора режима — обеспечивает переключение между режимами работы в реальном времени и симуляцией. Этот коммутатор также предоставляет возможность управления синхронизацией и захватом пакетов в сети.
2. **Блок сетевых компонентов.** Блок "Сетевые компоненты" содержит сетевое оборудование и конечные точки, доступные в программе "Трассировка пакетов". Он разделен на два направления:
   1. **Окно выбора типа устройства.** Флажок «Тип устройства» содержит основные категории устройств (маршрутизаторы, коммутаторы, концентраторы, беспроводные устройства, сетевые кабели, конечные точки и прочее);
   2. **Окно выбора для конкретного устройства.** Окно выбора для конкретного устройства. После выбора категории здесь становятся доступны различные модели устройств.
3. **Созданный пользователем пакетный ящик.** Созданный пользователем пакетный ящик предназначен для того, чтобы пользователи могли создавать подробные тесты топологии сети и отображать их результаты.
4. ***Создание простой схемы сети***

В окне "Выбор сетевого компонента" в категории "Конечные устройства" выберите "Генетический ПК" и "Универсальный ноутбук". Оба устройства подключаются к рабочей области Packet Tracer. Затем нажмите «Соединения», а затем выберите «Медный кроссовер». Сначала нажмите на изображение ПК и выберите интерфейс FastEthernet устройства из открывшегося списка. Далее кликаем по изображению ноутбука и выбираем интерфейс FastEthernet. При правильном подключении индикаторы состояния устройства должны гореть зеленым цветом, что говорит о том, что интерфейсы устройства включены.



***Рисунок 1.2. Простая топология подсети***

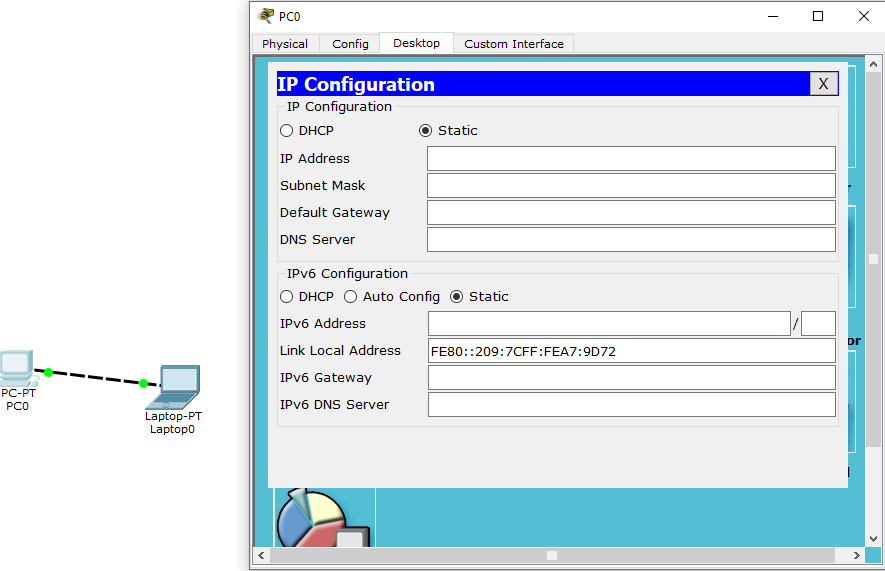
Чтобы настроить устройство, например ПК, нажмите на его изображение, а затем выберите вкладку «Рабочий стол» (рис. 1.3.). Выберите инструмент настройки IP-адреса и введите IP-адрес и маску подсети устройства.



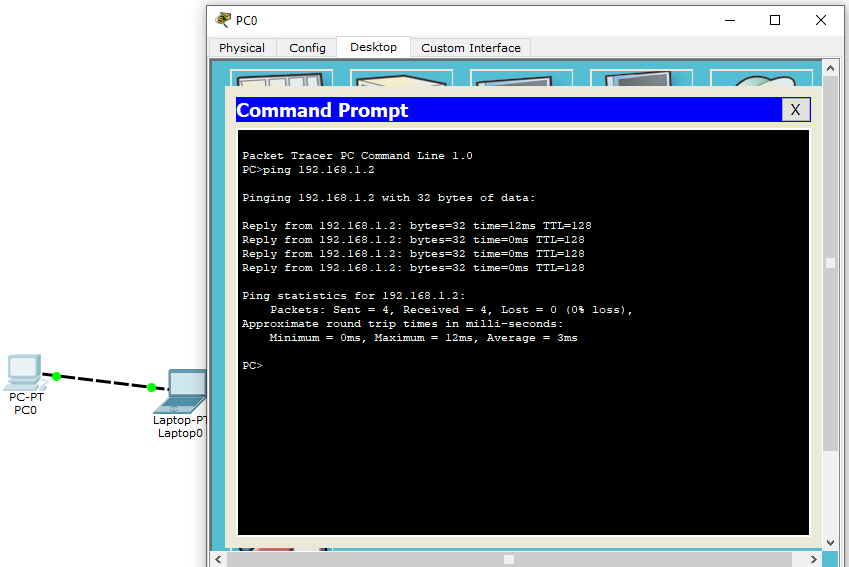
***Рисунок 1.3. Настольный ПК***

Для схемы IP-адреса шлюза по умолчанию и DNS-сервера могут быть отменены, поскольку они не требуются (схема состоит только из шлюза по умолчанию и DNS-сервера). DNS-сервер не требуется (схема состоит всего из двух компьютеров и не предполагает выхода в интернет или подключения к другим сетям, а также использования символьных имен).

Окно настройки компьютера закроется. Нажмите на изображение записной книжки и настройте записную книжку таким же образом. Убедитесь, что указанные IP-адреса находятся в одной подсети. Окно настройки IP-адреса закрывается, после чего открывается средство командной строки. С помощью инструмента ping выполняется проверка связности (рис. 1.5).



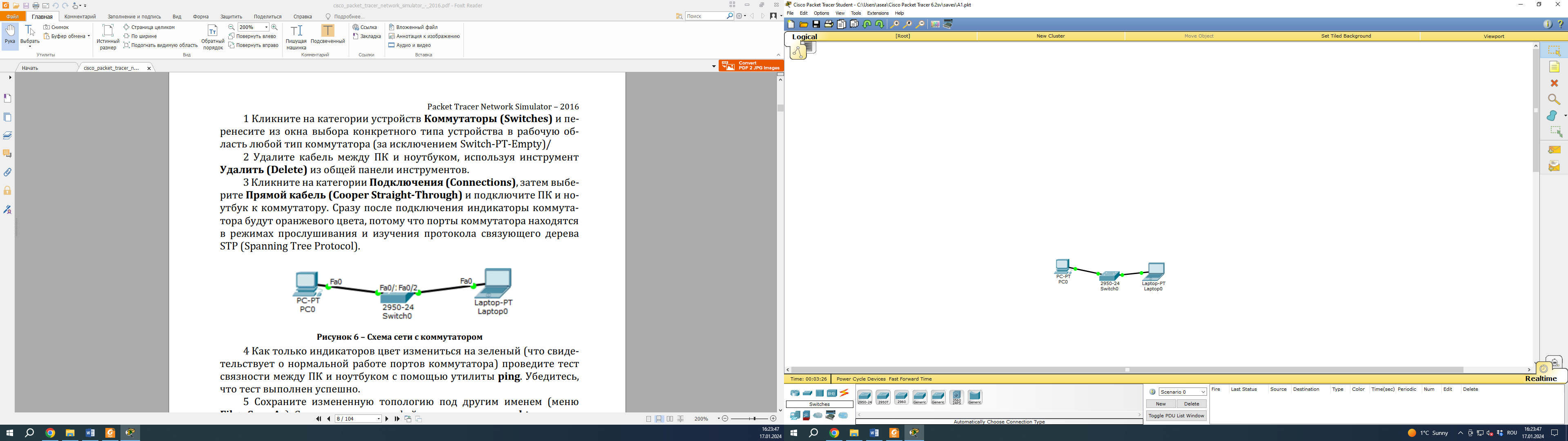
***Рисунок 1.4. Настройка IP-адреса и маски вашего ПК***



***Рисунок 1.5. Тест подключения устройства***

Рассматриваемая конфигурация сети относительно проста. В реальности современная сеть требует сетевого оборудования. Усложните топологию, добавив коммутатор Ethernet.

Для этого в категории устройств Переключатели выберите и перетащите любой тип переключателя (кроме Switch-PT-Empty) из окна выбора типа устройства в рабочую область. Сотрите кабель между компьютером и ноутбуком с помощью инструмента «Удалить» на общей панели инструментов. Щелкните категорию «Подключения», затем выберите Cooper Straight-Through и подключите ПК и ноутбук к коммутатору. При подключении индикаторы коммутатора загораются оранжевым цветом, так как порты коммутатора находятся в режимах прослушивания и настройки протокола связующего дерева (STP).



***Рисунок 1.6. Схема сети с коммутатором***

Как только светодиоды изменят цвет (указывая на то, что порты коммутатора работают правильно), будет выполнен тест на подключение между ПК и ноутбуком с помощью утилиты ping. Измененная топология будет сохранена под другим именем (меню «Файл> «Сохранить как»). Схема сохраняется в файле с расширением .pkt. Текущее состояние и настройки устройств запоминаются.

1. ***Командная строка***

Эта утилита имитирует командную строку операционной системы Microsoft Windows. Тем не менее, поддерживается ограниченный набор команд, которого достаточно для тестирования сети.

Доступны следующие команды:

*?* - используется для получения контекстной помощи, будет отображен список доступных опций или команд, которые можно ввести далее. Вы получите список команд, доступных на этом уровне. Это помогает ориентироваться в доступных командах, запоминать правильный синтаксис или узнавать параметры, доступные в этой конкретной команде;

*arp* – используется для отображения или манипулирования таблицей протокола разрешения адресов (ARP). Таблица ARP связывает IP-адреса с MAC-адресами в сетях Ethernet. Команду *arp* можно использовать с различными параметрами для выполнения различных действий. *Router> arp* – этакоманда отобразит текущую таблицу ARP с ассоциациями между IP-адресами и MAC-адресами. *Маршрутизатор> arp <adresa\_IP>,* замените <adresa\_IP> на IP-адрес, для которого вы хотите узнать связь с MAC-адресом. *Router> clear arp <adresa\_IP> –* Эта команда удаляет запись, соответствующую указанному IP-адресу, из таблицы ARP. *Router> clear arp —* эта команда удаляет все записи в таблице ARP. Стоит отметить, что точное поведение команды *arp*  может отличаться в зависимости от используемой платформы и версии Cisco Packet Tracer. Как правило, эти команды чаще используются в реальных сетевых средах;

*delete –* используется для удаления файла или каталога. Структура этой команды: *delete <nume\_fișier>,* где *<nume\_fișier>* — это имя файла или каталога, который необходимо удалить. В реальной среде эта команда может быть использована для удаления файлов конфигурации или других данных;

*dir –* используется для отображения списка файлов и директорий в текущей директории. Это специальная команда для просмотра содержимого каталога. Стоит упомянуть, что Cisco Packet Tracer, являясь симулятором для сетевых устройств Cisco, не моделирует все аспекты полноценной операционной системы. Команда *dir*  относится к файловой системе и каталогу и в данном контексте относится к просмотру файлов и каталогов в текущем каталоге устройства;

*ftp –* используется для инициирования FTP-соединения (File Transfer Protocol) с FTP-сервером. Это обеспечивает передачу файлов между устройством Cisco Packet Tracer и внешним FTP-сервером. Общая структура *команды ftp*  такова: *ftp <adresa\_server\_ftp> –* эта команда открывает сессию FTP и позволяет ввести логин и пароль для подключения к указанному FTP-серверу. После установки соединения можно выполнять такие операции, как загрузка и выгрузка файлов между устройством Cisco Packet Tracer и FTP-сервером;

*Справка –* используется для отображения списка доступных команд и предоставления краткой информации о том, как они используются. Он предоставляет сводку доступных команд и опций, позволяя пользователю изучить и понять функциональные возможности, предлагаемые симулятором;

*ipconfig –* специфичен для операционных систем Windows и используется для отображения информации о конфигурации сети, IP-адресах, шлюзах, маске подсети и других деталях, связанных с сетевым интерфейсом устройства;

*netstat –* работает совместно с командой *ifconfig*  для отображения состояния сетевого интерфейса TCP/IP. Например, команда *netstat* -*in*  и указатель *-i*  могут отображать информацию о сетевых интерфейсах, в то время как указатель *-n*  используется для вывода IP-адресов вместо имен хостов. Эта команда может быть использована для проверки интерфейсов, адресов и имен хостов SLIP;

*Ping –* используется для проверки связности между сетевыми устройствами. Когда используется команда ping, она отправляет пакеты протокола ICMP (Internet Control Message Protocol) на указанный IP-адрес или доменное имя и ожидает ответа. *Маршрутизатор> пинг 192.168.1.1,* или чтобы проверить доменное имя маршрутизатора *> пинг [www.google.com](http://www.google.com).* Он будет отправлять тестовые пакеты на IP-адрес, связанный с указанным устройством или доменным номером, и отображать информацию об успехе или неудаче связи;

*Snmpget* — относится к использованию протокола SNMP (Simple Network Management Protocol) для запроса управляемого объекта и получения информации о состоянии или конфигурации устройства. В реальной среде команда *snmpget* будет использоваться для запроса сетевых устройств с целью получения информации об их состоянии, такой как количество переданных пакетов, состояние интерфейсов и т.д. *Router> snmpget -v2c -c public 192.168.1.1 sysDescr.0:*

-v2c: Указывает версию SNMP;

-c public: сообщество SNMP (пароль, часто "public" в тестовых средах);

192.168.1.1: IP-адрес устройства;

sysDescr.0: идентификатор объекта SNMP (OID), определяющий информацию об устройстве;

*snmpgetbulk* в основном используется для минимизации количества SNMP-запросов, необходимых для получения большего объема данных, что позволяет более эффективно взаимодействовать между менеджером SNMP и управляемым устройством. Он особенно используется в ситуациях, когда необходимо получить большое количество переменных SNMP в одном запросе. *Router> snmpgetbulk -v2c -c public -Cn0 -Cr10 192.168.1.1 sysDescr:*

-v2c: Указывает версию SNMP;

-c public: сообщество SNMP (пароль, часто "public" в тестовых средах);

-Cn0: Минимальное количество переменных, возвращаемых в запросе;

-Cr10: Максимальное количество итераций переменных, возвращаемых в запросе;

192.168.1.1: IP-адрес устройства;

sysDescr: Идентификатор объекта SNMP (OID), определяющий информацию об описании системы;

*snmpset* - используется для установки значений некоторых объектов управления. Команда *snmpset*  является частью набора SNMP и используется для изменения значений переменных, хранящихся на управляемом устройстве. Команда *snmpset* может быть структурирована следующим образом: *snmpset -v:[версия] -c:[сообщество] -r:[adresa\_ip\_dispozitiv] [OID] [tip\_date] [значение];*

-v:[version]: Указывает версию SNMP (например, -v:2c для SNMPv2c);

-c:[community]: SNMP сообщество (пароль);

-r:[adresa\_ip\_dispozitiv]: IP-адрес управляемого устройства;

[OID]: идентификатор объекта SNMP (OID), указывающий на объект, которым необходимо управлять, и который мы хотим изменить;

[tip\_date]: Тип данных объекта SNMP;

[value]: Новое значение, которое мы хотим присвоить объекту SNMP, идентифицированному OID.

Команда *snmpset*  может повлиять на работу устройства, и ее следует использовать с осторожностью, учитывая права безопасности и доступ к управляемому устройству. Также важно, чтобы устройство поддерживало операцию настройки SNMP и чтобы сообщество SNMP было правильно настроено для разрешения изменений.

*Ssh* - часто используется в реальных средах для установления безопасного удаленного соединения с устройством или сервером, поддерживающим протокол SSH (Secure Shell). В реальной среде пользователь может использовать команду *ssh*  в терминале для подключения по защищенному каналу к устройству или серверу. *ssh [пользователь]@[adresa\_ip\_dispozitiv]:*

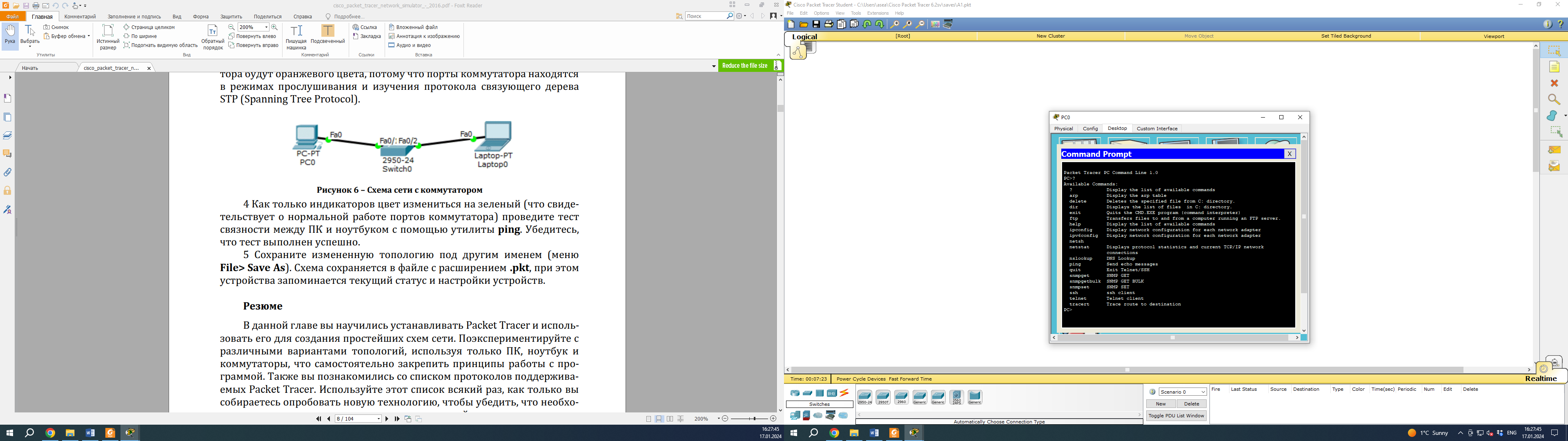
[user]: имя пользователя, с которым вы хотите войти на устройство.

[adresa\_ip\_dispozitiv]: IP-адрес устройства, к которому вы хотите подключиться;

*telnet* - может использоваться для имитации соединений Telnet с устройствами в сети. Эта команда используется для установки текстового (символьного) соединения с устройством, поддерживающим соединения Telnet. *telnet [adresa\_ip\_dispozitiv]. [adresa\_ip\_dispozitiv]* IP-адрес устройства, к которому вы хотите подключиться. Если подключение Telnet настроено с использованием пароля, вам будет предложено ввести данные для входа, такие как имя пользователя и пароль. Стоит отметить, что использование Telnet в производственной среде может быть сопряжено с рисками безопасности, так как информация передается в текстовом формате, без шифрования. В реальных средах рекомендуется использовать SSH (Secure Shell) вместо Telnet для защищенных соединений;

*Tracert / traceroute* - используется для трассировки пути пакета в сети, отображая все промежуточные узлы, через которые проходит пакет, чтобы достичь места назначения. *traceroute [adresa\_destinație].* *[adresa\_destinație]* – IP-адрес пункта назначения, до которого отслеживается маршрут. Эта команда предоставит список всех промежуточных узлов, через которые проходит пакет на пути к месту назначения. Он также покажет время отклика от каждого узла. Точное имя и синтаксис команды могут различаться в зависимости от версии Cisco Packet Tracer или образа платформы, на которой он используется.

Каждая команда поддерживает параметры, которые могут быть расшифрованы путем ввода команды без каких-либо опций, как показано на рис.1.7.



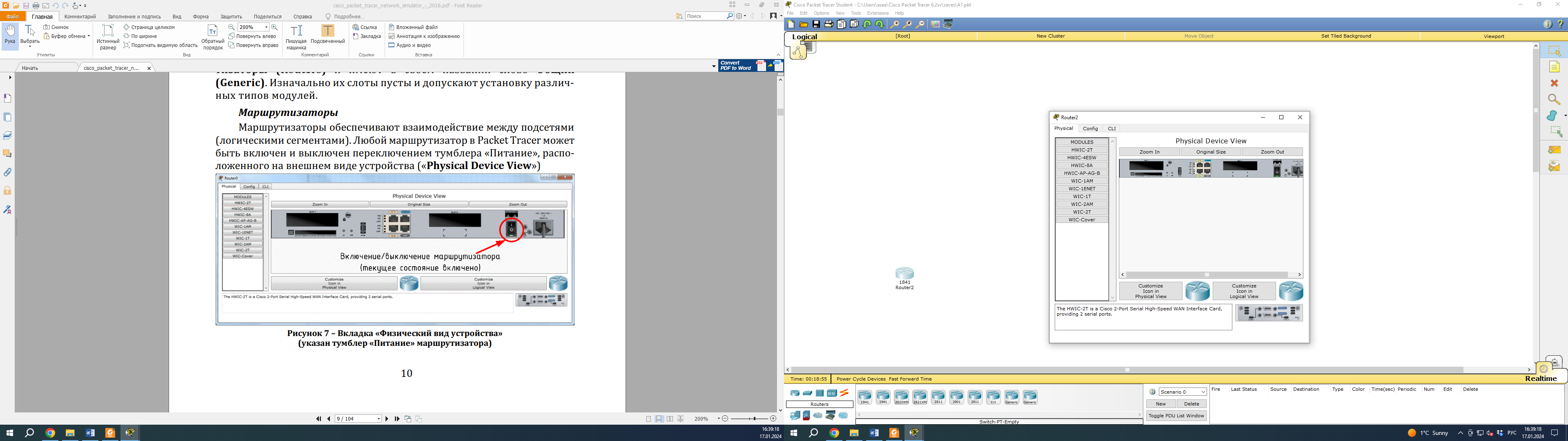
***Рисунок 1.7. Командная строка и основные команды верхнего уровня***

1. ***Сетевое оборудование Cisco и устройства трассировки пакетов***

Большинство устройств, показанных в Packet Tracer, более или менее соответствуют реальному оборудованию Cisco. Тем не менее, существуют устройства, которые являются уникальными для Packet Tracer. Эти устройства находятся в подразделах категорий «Коммутаторы» и «Маршрутизаторы» и имеют в своем названии слово «Общий». Изначально их слоты пусты и позволяют устанавливать различные типы модулей.

1. **Маршрутизаторы**

Маршрутизаторы обеспечивают связь между подсетями (логическими сегментами). Любой маршрутизатор в системе трассировки пакетов можно включать и выключать путем переключения переключателя "Power", расположенного во внешнем виде устройства ("Physical Device View") (рис. 1.8).



***Рисунок 1.8. вкладка «Физический вид устройства» (отображается тумблер «Питание» роутера)***

Возможность включения/выключения питания маршрутизаторов в Packet Tracer имитирует работу реальных устройств. Модуль устройства можно добавлять и удалять только после отключения питания устройства. Если текущая конфигурация не будет сохранена, выключение устройства приведет к потере выполненных настроек.

В Packet Tracer доступны следующие маршрутизаторы:

1. Циско 1841 года. Integrated Service Router (ISR), имеет два порта Fast Ethernet и два свободных слота для подключения интегральных плат, для высокоскоростных схем высокоскоростного подключения к глобальной сети.
2. Cisco 1941 (Циско 1941). Эта модель похожа на предыдущую, с той лишь разницей, что она работает под управлением Cisco IOS версии 15. Он также оснащен двумя портами Gigabit Ethernet.
3. Cisco 2620XM. Этот мультисервисный маршрутизатор имеет порт Fast Ethernet, два слота для установки интерфейса WAN, карты WAN и слот AIM.
4. Cisco 2621XM. Этот роутер похож на предыдущий, за исключением того, что имеет два порта Fast Ethernet.
5. Циско 2811. Маршрутизатор со встроенными службами имеет два порта Fast Ethernet, четыре слота WIC и два слота AIM.
6. Циско 2901. Этот маршрутизатор имеет два порта Gigabit Ethernet, четыре слота WIC и два слота DSP.
7. Циско 2911. Этот роутер имеет три порта Gigabit Ethernet Ethernet, в остальном он имеет те же функции, что и предыдущее устройство. Он работает под управлением Cisco IOS версии 15.
8. Генетический маршрутизатор-PT. Роутер с настройкой. Он имеет 10 слотов и несколько специальных модулей, название которых начинается с букв PT.
9. **Переключатели**

Коммутатор (ранее называвшийся многопортовым мостом) соединяет несколько конечных точек в сети. Каждый порт коммутатора является доменом коллизий. В Packet Tracer доступны следующие коммутаторы:

1. ЦИСКО 2950-24. Управляемый коммутатор, поддерживающий 24 порта Fast Ethernet.
2. Циско 2950Т-24. Этот коммутатор относится к семейству интеллектуальных коммутаторов Catalyst 2950 и имеет 24 порта Fast Ethernet и два порта Gigabit Ethernet с поддержкой модулей Gigabit Interface Converter (GBIC).
3. Циско 2960-24ТТ. Еще один коммутатор с 24 портами. В отличие от предыдущей модели, он имеет порты Gigabit Ethernet с поддержкой модулей SFP (Small Form-factor Pluggable). Однако эта разница существенна для реальных коммутаторов и не оказывает влияния при работе в Packet Tracer.
4. Циско 3560-24ПС. В отличие от других коммутаторов, это устройство является коммутатором уровня 3, и помимо стандартной функции коммутации, оно способно выполнять маршрутизацию. Последние две буквы PS означают поддержку Power over Ethernet PoE, который используется для питания IP-телефонов без отдельного источника питания.
5. Bridge PT. Это устройство используется для сегментации сети и имеет всего два порта.
6. Универсальный коммутатор PT. Это устройство существует только в трассировщике пакетов и является коммутатором, конфигурируемым пользователем. Он имеет 10 слотов и несколько специализированных модулей.

Как и в случае с Genetic Router-PT, о котором говорилось ранее, Generic PT Switch может быть отключен, что необходимо для смены модулей. Все остальные переключатели имеют фиксированную конструкцию и не предполагают кастомизации. Поэтому нет необходимости отключать блок питания.

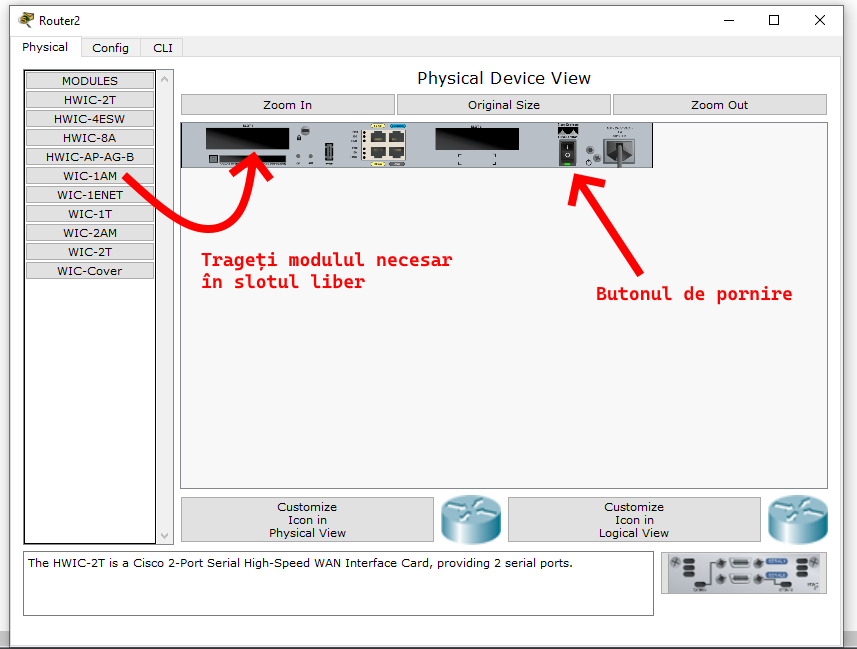
1. **Другие устройства**

Как видите, Packet Tracer поддерживает не только коммутаторы и маршрутизаторы, но и другие устройства. Эти устройства настраиваются и работают следующим образом:

1. Создание сетей на основе хаба — это область истории. Тем не менее, с помощью этого устройства рассматривается проблема диффузии и столкновений. В нем 10 слотов.
2. Повторитель. Используется для усиления и восстановления уровня и формы электрического сигнала. Он имеет два слота.
3. Коаксиальный разветвитель PT. Предназначен для разъема коаксиального соединения. Он имеет три порта для коаксиального подключения и не может быть настроен по индивидуальному заказу.
4. ***Подключение модулей сетевых устройств***

Модули сетевых устройств являются аппаратными реализациями общих интерфейсов. Например, модуль HWIC-4ESW содержит 4 порта Ethernet (10 Мбит/с). Как и в случае с реальным устройством, а также с устройством, представленным в Packet Tracer, для смены модуля необходимо отключить блок питания.

Чтобы выключить питание, производится одинарное нажатие на выключатель питания с правой стороны устройства. Чтобы установить модуль, перетащите любой из доступных модулей в списке модулей, установив его в любой свободный слот. Если модуль не может быть установлен в определенный слот, он будет автоматически возвращен в список.



***Рисунок 1.9. Добавление модуля маршрутизатора***

Чтобы извлечь модуль, его также нужно выключить и вытащить из слота обратно в список. После смены модуля устройство снова включается.

1. ***Система именования модулей***

Каждый маршрутизатор имеет более десятка модулей, которые можно идентифицировать по имени. Ниже перечислены модули, сгруппированные по типу кабельного подключения.

1. **Медный интерфейс Ethernet**

Они представляют собой стандартные интерфейсы LAN, к которым подключается медный кабель витой пары с разъемом RJ-45. Название этих интерфейсов основано на указании скорости: Etnernet (10 Мбит/с),

FastEtnernet (100 Мбит/с), GigabitEtnernet (1000 Мбит/с). Следовательно, названия модулей имеют сокращенную ссылку на скорость работы интерфейса: E, FE, GE, CFE или CGE. Так называемые SW-модули предназначены для роутеров и обеспечивают функции коммутации:

1. HWIC-4ESW - 4 коммутируемых порта Ethernet;
2. WIC-1ENET - одиночный порт Ethernet;
3. NM-1E - одиночный порт Ethernet;
4. NM-1FE-TX - один порт Fast Ethernet;
5. NM-4E - 4 порта Ethernet;
6. NM-ESW-161 - 16 коммутируемых портов Ethernet;
7. PT-ROUTER-NM-1CE, PT-ROUTER-NM-lCFE, PT-ROUTER-NM-1CGE - module de utilizator Packet Tracer.
8. **Оптический модуль Ethernet**

Этот тип модуля похож на предыдущий, за исключением того, что вместо медного кабеля в нем используется оптический кабель. Эти модули можно определить по наличию буквы F:

1. NM-1FE-FX - один порт Ethernet для оптической среды передачи;
2. PT-ROUTER-NM-1FFE, PT-ROUTER-NM-1FGE – персонализация, модуль Packet Tracer.
3. **Последовательный интерфейс**

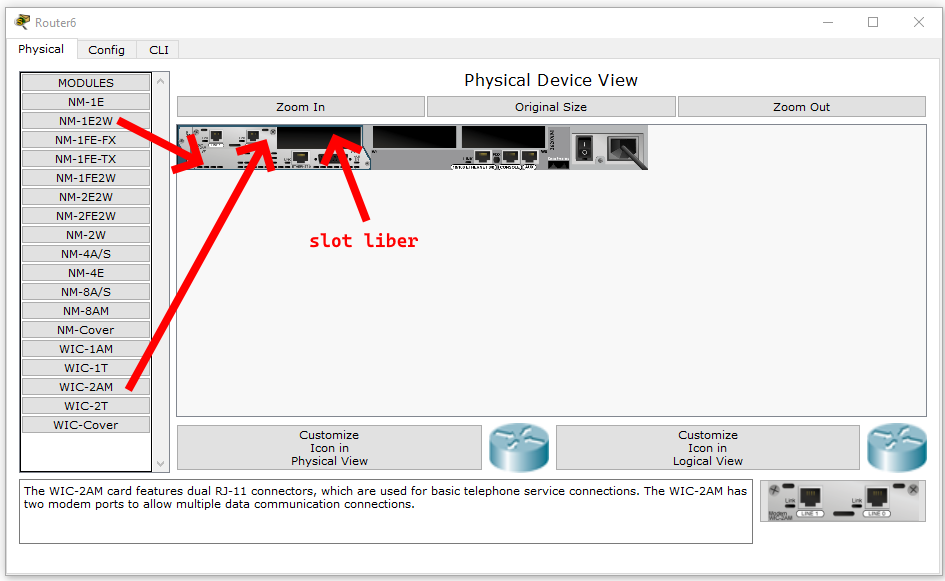
Имена этих модулей содержат букву T или пару символов A/S. Модули с буквой T являются синхронными, а модули с символьными символами A/S являются асинхронными. Разница в их работе очевидна для реального железа, в Packet Tracer разницы между ними нет:

1. WIC-1T, WIC-2T – одиночный или двойной синхронный последовательный порт;
2. NM-4A/S, NM-8A/S – четыре или восемь асинхронно-синхронных последовательных портов;
3. PT-ROUTER-NM-1S, PT-ROUTER-NM-1SS – module de utilizator Packet Tracer.
4. **Интерфейс модема**

Данный тип модуля имеет интерфейс RJ-11 для подключения телефонных кабелей. Такие модули можно идентифицировать по буквам AM, присутствующим в названии по цифре, обозначающей количество портов

1. WIC-1AM – двойной порт RJ-11 для подключения телефонов и модема;
2. WIC-2AM, WIC-8AM – два или восемь портов RJ-11;
3. PT-ROUTER-NM-1AM – пользовательский модуль трассировщика пакетов.
4. **Модуль WIC**

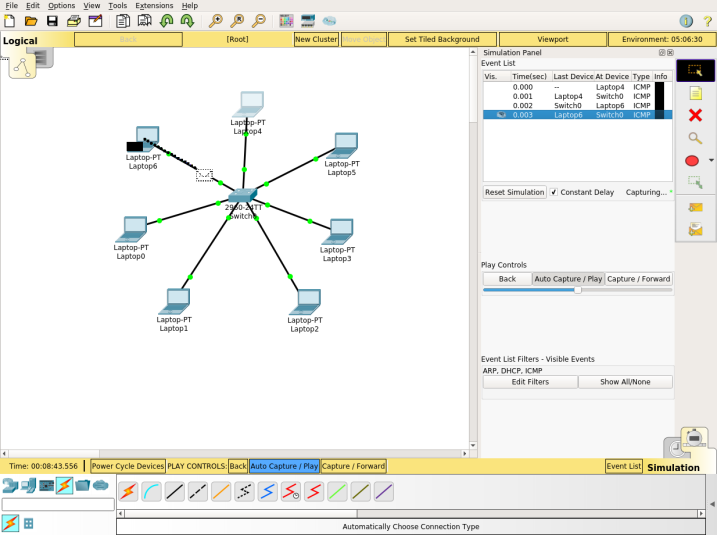
Сетевые модули WIC не занимают весь слот, модули (WIC внутри сетевых модулей (NM)) имеют дополнительные слоты для поддержки меньших модулей. Эти модули можно узнать по букве W в конце названия:



***Рисунок 1.10. Модули с поддержкой модулей WIC***

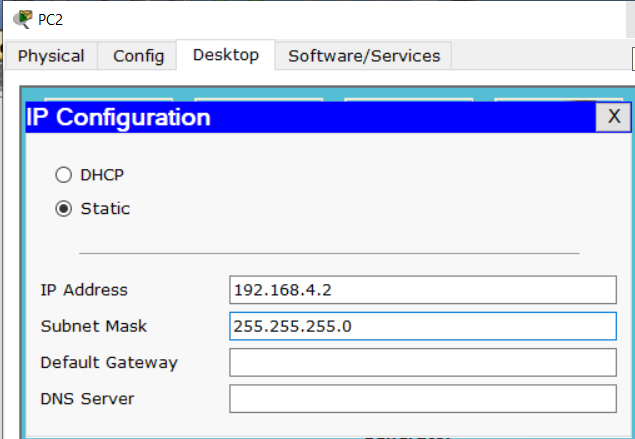
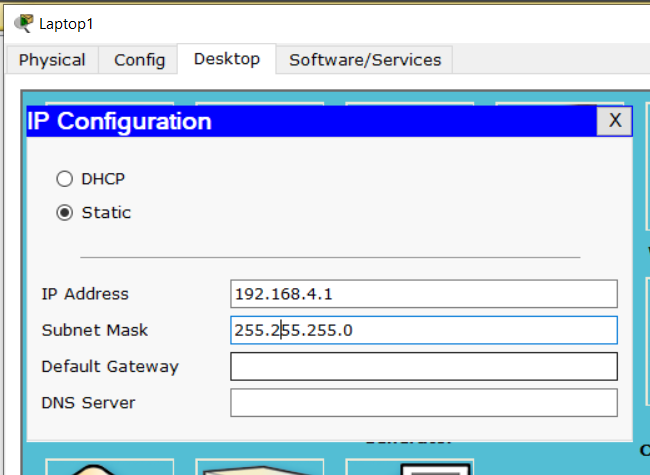
1. NM-1E2W, NM-1FE2W – один порт Ethernet/два порта Fast Ethernet с поддержкой двух слотов WIC; один порт Ethernet/два порта Fast Ethernet с поддержкой двух слотов WIC.
2. NM-2E2W, NM-2FE2W – два порта Ethernet/Fast Ethernet с двумя слотами WIC;
3. NM-2W – не имеет портов, рассчитан на поддержку двух слотов WIC.
4. **Порядок выполнения лабораторных работ**
5. Проектирование подсети на основе коммутатора (как показано на рисунке 1.11).
6. Назначьте IP-адреса и маску подсети в статическом режиме (рисунок 1.12).
7. Проверьте соединение между хостами, подключенными к подсети, с помощью команды ping в меню консоли (Рисунок 1.14).
8. Добавьте еще один коммутатор и несколько хостов (5-7) и установите IP-адреса и маску подсети для заданных хостов.
9. С помощью соединительного кабеля соедините переключатели друг с другом (рис. 1.15).
10. Проверьте соединение между хостами подсетей No1 и No2 с помощью команды ping (рис. 1.17).
11. Чтобы отметить и сделать выводы из вышеизложенных пунктов.
12. Подключите маршрутизатор к проектируемой подсети и введите в поле (CLI) команды для настройки маршрутизатора по назначению IP-адресов и динамической маскировке подсети.
13. С помощью команды ping проверьте соединения.
14. **Проведение лабораторных работ**

Требуется проектирование подсети на основе коммутатора на основе топологии, показанной на рисунке 1.11. Топология на рисунке служит основой для проектирования подсети, в которой коммутаторы играют центральную роль в управлении связностью между различными сегментами сети:



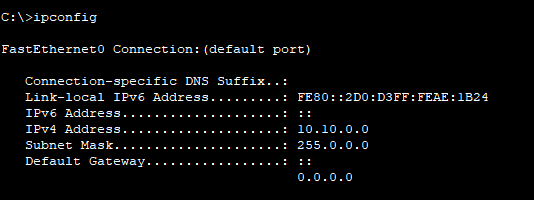
***Рисунок 1.11. Моделирование подсети на основе коммутатора в CISCO***

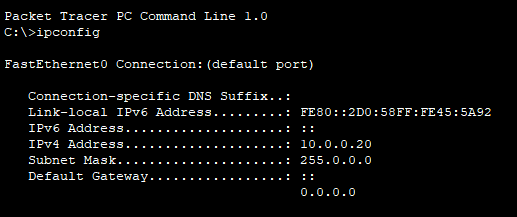
Необходимо настроить IP-адрес, чтобы разрешить связь между двумя устройствами в подсети. IP-адрес и маска должны быть установлены правильно, чтобы обеспечить эффективное подключение и обмен данными между двумя устройствами в этой подсети.



***Рисунок 1.12. Настройка IP-адресов и масок подсетей***

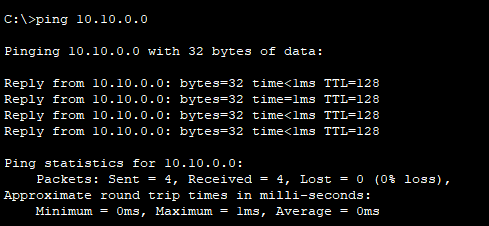
Чтобы проверить правильность адреса, воспользуйтесь *командой ipconfig.* Команда *ipconfig* предоставляет подробную информацию о конфигурации сети, включая назначенные IP-адреса. Анализируя результаты, полученные с помощью *команды ipconfig,* можно убедиться, что IP-адреса настроены правильно и что устройства в сети могут эффективно взаимодействовать.





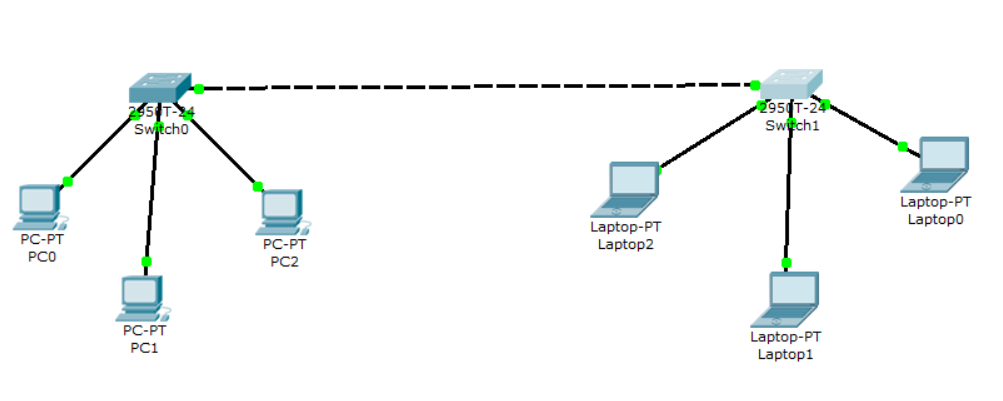
***Рисунок 1.13. Выполнение команды ipconfig***

После настройки IP-адреса и маски подсети между двумя устройствами необходимо проверить соединение между ними. Чтобы убедиться в правильности адреса, используйте команду *ipconfig* в командной строке системы. Используйте команду *ping* , чтобы проверить, есть ли рабочее соединение между двумя устройствами.



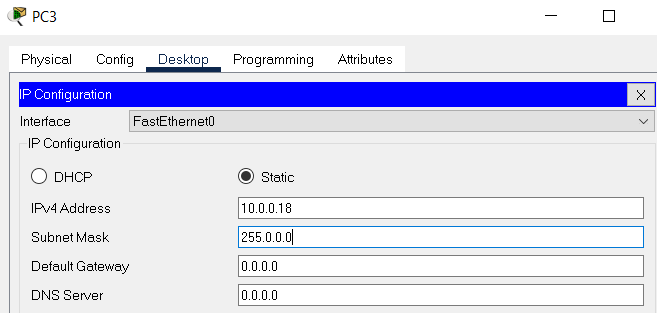
***Рисунок 1.14. Пинг выполнения заказа***

В Cisco Packet Tracer была создана новая подсеть, которая была подключена к существующей сети. Для этого в топологию был добавлен еще один коммутатор и настроены IP-адреса и маски подсети для всех 5-7 хостов. Хосты в новой подсети были подключены к новому коммутатору с помощью соответствующих сетевых кабелей. Впоследствии коммутаторы соединялись между собой с помощью сетевого кабеля. Такая конфигурация позволяла новой сети взаимодействовать с исходной сетью и использовать взаимосвязанные устройства для выполнения сетевых операций.

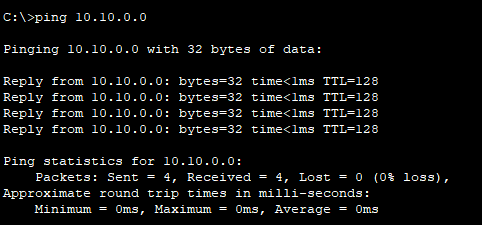


***Рисунок 1.15. Подсеть с 2 коммутаторами***

Для одного из устройств в новой подсети будет настроен IP-адрес и соответствующая маска подсети (рис. 1.16). С помощью команды *ping* в командном интерфейсе проверяется соединение между двумя хостами в исходной подсети и новой подсети (рис. 1.17). Эта проверка выполняется для того, чтобы убедиться, что узлы в двух подсетях могут взаимодействовать друг с другом. Если ответы на команды ping были оперативными и без потерь, это говорит о том, что соединение между подсетями работает правильно.



***Рисунок 1.16. Настройка ip и маски для терминального устройства***



***Рисунок 1.17. Результат проверки подключения к подсети***

В рамках проектируемой сетевой инфраструктуры был интегрирован маршрутизатор, выполняющий функцию DHCP-сервера. Данный маршрутизатор был подключен к спроектированной подсети, тем самым обеспечив функции маршрутизации и назначения IP-адресов через сервис DHCP. В командном интерфейсе маршрутизатора введены соответствующие команды для его динамической конфигурации, включая указание диапазона доступных IP-адресов и определение параметров аренды для IP-адресов, назначенных DHCP. Такая конфигурация маршрутизатора гарантирует, что устройства, подключенные к сети, автоматически получают IP-адрес и маску подсети от DHCP-сервера маршрутизатора. Служба DHCP маршрутизатора упрощает управление IP-адресами устройств в сети, упрощая добавление, изменение и удаление устройств без необходимости ручной настройки IP-адресов.

Код настройки маршрутизатора:

Маршрутизатор>включить

Маршрутизатор#настроить

Настройка из терминала, памяти или сети [терминал]?

Введите команды конфигурации, по одной на строку. Закончите на CNTL/Z.

Маршрутизатор(конфигурация)#interface g 0/1

Router(config-if)#ip адрес 192.168.4.1 255.255.255.0

Router(config-if)#নো выключение

Маршрутизатор (config-if)#

%LINK-5-ИЗМЕНЕНО: Интерфейс GigabitEthernet0/1, состояние изменено на вверх

Выход

Router(config)#ip dhcp pool tibrigan

Маршрутизатор (dhcp-config)#network 192.168.4.2 255.255.255.0

Маршрутизатор (dhcp-config)#default-маршрутизатор 192.168.4.1

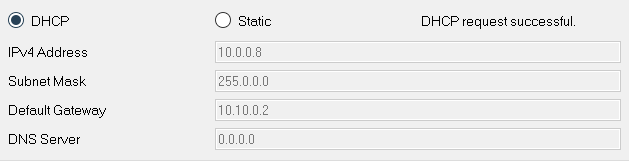
Маршрутизатор (dhcp-config)#exit

Маршрутизатор (конфигурация)#

%LINEPROTO-5-UPDOWN: Протокол линии на интерфейсе GigabitEthernet0/1, изменен статус на up

С целью предоставления услуг DHCP в рамках проектируемой подсети, для упрощения процесса назначения и управления IP-адресами для подключенных устройств, завершена настройка маршрутизатора. После завершения этой настройки каждое устройство, подключенное к подсетям, было настроено на использование DHCP для автоматического получения IP-адреса и маски подсети.

Этот подход к автоматизированной настройке, основанный на DHCP, устраняет необходимость вручную устанавливать IP-адреса и предоставляет масштабируемое и гибкое решение для расширения или модификации сети, тем самым облегчая администрирование сети.



***Рисунок 1.18. Настройка конфигурации DHCP***

1. **Содержание отчета**
2. Знакомство:
   1. Презентация цели работы: целью данной работы является проектирование подсети, с использованием коммутационных устройств для обеспечения эффективной связи между подключенным оборудованием.
3. Настройка коммутаторов:
   1. Подробные сведения о настройке параметров коммутатора, таких как IP-адрес, маска подсети и шлюз.
   2. Описание топологии подсети, включая количество подключенных коммутаторов и оборудования.
4. Подключение устройств к выключателю:
   1. Подробные инструкции по подключению оборудования к выключателям.
   2. Физическая проверка соединений и обеспечение надлежащей физической инфраструктуры.
5. Настройка IP-адресов:
   1. Инструкция по настройке IP-адресов для устройств, подключенных к коммутаторам.
   2. Использование специфических команд для настройки параметров сети.
6. Проверка соединений и тестирование связи:
   1. Использование таких команд, как ping, для проверки связности между оборудованием.
   2. Тестирование связи между различными устройствами для обеспечения правильной функциональности.
7. Возникшие проблемы и их решение:
   1. Выявление потенциальных проблем и описание путей их решения.
   2. Советы по оптимизации производительности подсети.
8. Выводы:
   1. Резюме полученных результатов в рамках диссертации.
   2. Общие замечания и выводы по проектированию и реализации подсети.
9. Ссылки:
   1. Упоминание всех ресурсов и документации, использованных в процессе проектирования и настройки подсети.
10. Приложения:
    1. Дополнительные сведения, скриншоты или диаграммы, дополняющие информацию в отчете.

**Контрольные вопросы**

1. Какие шаги были предприняты для настройки коммутаторов в подсети?
2. Как вы настраивали IP-адреса и маски подсети для коммутатора?
3. Каковы основные этапы подключения оборудования к коммутаторам?
4. Какие конкретно команды вы использовали для настройки IP-адресов устройств?
5. Как вы обеспечили уникальность IP-адресов в подсети?
6. Какие конкретно команды вы использовали для настройки IP-адресов устройств?
7. Как вы обеспечили уникальность IP-адресов в подсети?
8. Как вы документировали IP-адреса и конфигурации коммутаторов?
9. Как настроить IP-адрес на коммутаторе в определенной подсети?
10. Каковы шаги по назначению маски подсети коммутатору?
11. Какие команды необходимы для настройки IP-адреса на устройстве, подключенном к коммутатору?

**Библиография**

1. Таненбаум, Эндрю С. и Дэвид Дж. «Компьютерные сети». Пирсон, 2010.
2. Сиг. "Портативное руководство по командам маршрутизации и коммутации CCNA." Издательство Cisco, 2013.
3. Дойл, Джефф. "Маршрутизация TCP/IP, том 1." Издательство Cisco, 2017.
4. Ламмле, Тодд. «Полное учебное пособие по маршрутизации и коммутации CCNA». Wiley, 2016.
5. Одом, Уэнделл. «Официальное руководство по сертификации CCNA по маршрутизации и коммутации ICND2 200-105». Издательство Cisco, 2018.
6. Сперджен, Чарльз Э. «Ethernet: полное руководство». О'Рейли Медиа, 2014.
7. Гарг, Динеш К. и Рик Макдональд. "Основы коммутации и промежуточная маршрутизация CCNA 3 Companion Guide." Издательство Cisco, 2007.
8. Халаби, Сэм. «Архитектуры маршрутизации Интернета». Cisco Press, 1997.
9. Альбиц, Пол и Крикет Лю. «DNS и BIND». О'Рейли Медиа, 2017.
10. Таненбаум, Эндрю С. «Компьютерные сети». Пирсон, 2010.

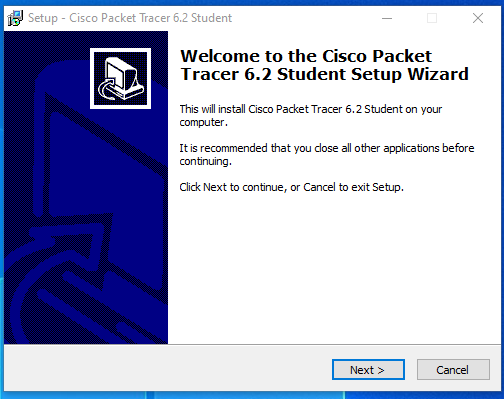
**ПРИСТРОЙКА**

**Подготовка к лабораторным работам**

**Установка Cisco Packet Tracer 6.2**

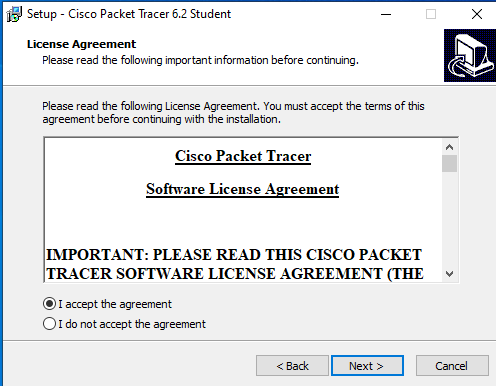
Установить программу в Windows просто. Необходимо найти соответствующий файл (например, с именем "Cisco Packet Tracer 6.2 for Windows Student Version.exe"). Просто откройте этот файл, чтобы запустить мастер установки, затем примите лицензионное соглашение, выберите местоположение и начните установку.

* 1. После копирования версии программы в соответствующую папку, двойной клик по программе *открывает окно установки*. Двойным щелчком мыши на скопированной программе процесс установки инициируется открытием специального окна. Открытие окна позволяет пользователю начать и завершить процесс установки соответствующей программы.



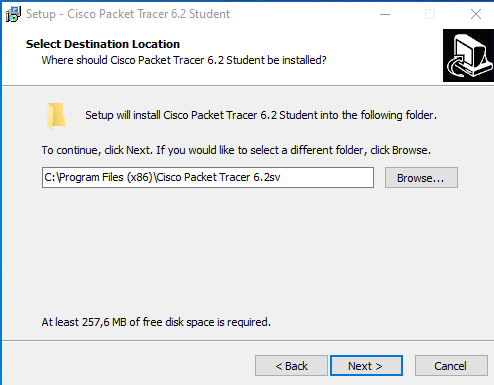
***Рисунок А1.1. Начало процесса установки программного обеспечения CISCO Packet Tracer***

* 1. Для продолжения процесса требуется принятие лицензионных условий.



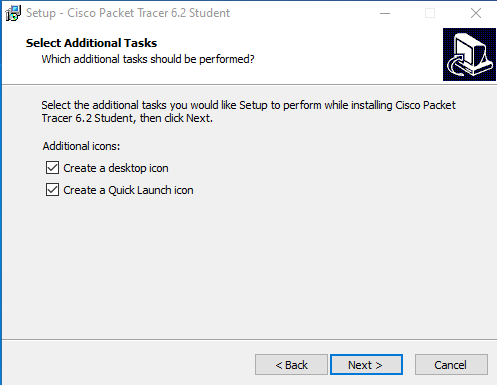
***Рисунок А1.2. Принятие условий лицензии***

* 1. Пользователю предлагается выбрать папку-получатель для установки программы.



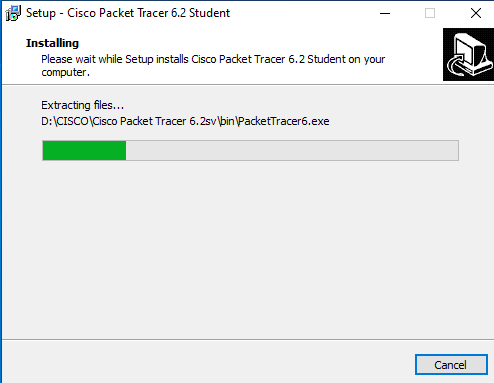
***Рисунок А1.3. Выбор места установки***

* 1. Пользователь должен определиться с формированием метки в процессе установки.



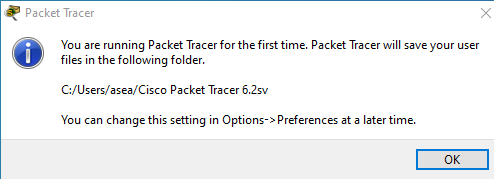
***Рисунок А1.4. Генерация этикеток***

* 1. Нажимаем на кнопку, чтобы начать установку программы.



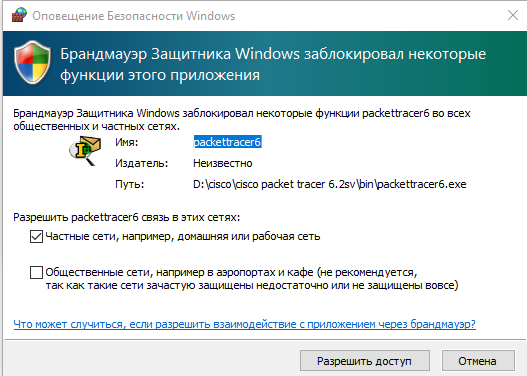
***Рисунок А1.5. Процесс установки***

* 1. Последним шагом является выбор папки назначения для хранения обработанных файлов в Cisco.



***Рисунок А1.6. Выбор папки для сохранения проработанных проектов***

* 1. В случае необходимости, поддерживается использование программы в рамках операционной системы Windows.



***Рисунок А1.7. Принятие программы в операционной системе***

* 1. После завершения монтажа программы завершается этап подготовки к завершению лабораторных работ.