

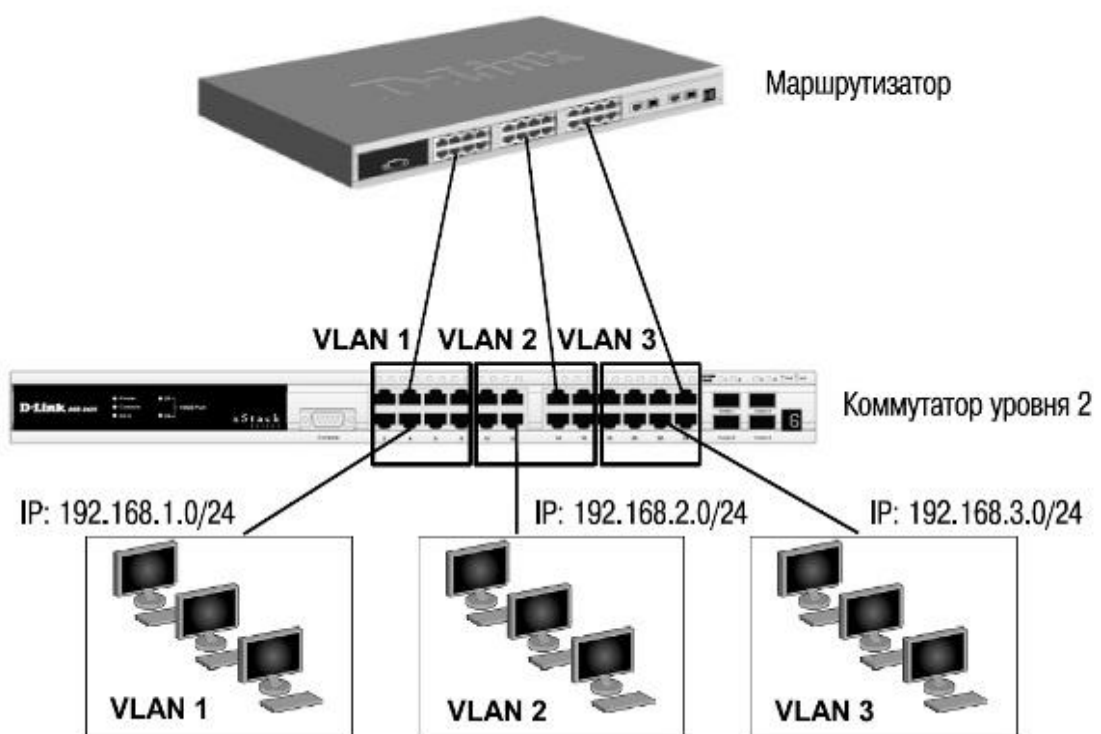
Владимирский государственный университет

КОМПЛЕКСНАЯ ЗАЩИТА ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ

КНИГА 30

М. М. Монахова

АДМИНИСТРИРОВАНИЕ БЕЗОПАСНОСТИ КОМПЬЮТЕРНЫХ СЕТЕЙ Моделирование



Владимир 2020

Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Владимирский государственный университет
имени Александра Григорьевича и Николая Григорьевича Столетовых»

КОМПЛЕКСНАЯ ЗАЩИТА ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ

КНИГА 30

М. М. МОНАХОВА

АДМИНИСТРИРОВАНИЕ БЕЗОПАСНОСТИ
КОМПЬЮТЕРНЫХ СЕТЕЙ
Моделирование

Практикум

Под редакцией профессора М. Ю. Монахова

Электронное издание



Владимир 2020

© ВлГУ, 2020
© Монахова М. М., 2020
ISBN 978-5-9984-1232-5

УДК 004.056:004.7
ББК 32.971.3

Редактор серии – доктор технических наук, профессор М. Ю. Монахов

Рецензенты:

Доктор технических наук, профессор
зав. кафедрой вычислительной техники и систем управления
Владимирского государственного университета
имени Александра Григорьевича и Николая Григорьевича Столетовых
В. Н. Ланцов

Кандидат технических наук
зав. кафедрой цифрового образования и информационной безопасности
Владимирского института развития образования имени Л. И. Новиковой
Д. В. Мишин

Монахова, М. М. Администрирование безопасности компьютерных сетей. Моделирование : практикум [Электронный ресурс] / М. М. Монахова ; под ред. проф. М. Ю. Монахова ; Владим. гос. ун-т им. А. Г. и Н. Г. Столетовых. – Владимир : Изд-во ВлГУ, 2020. – 238 с. – (Комплексная защита объектов информатизации. Кн. 30). – ISBN 978-5-9984-1232-5. – Электрон. дан. (7,99 Мб). – 1 электрон. опт. диск (CD-ROM). – Систем. требования: Intel от 1,3 ГГц ; Windows XP/7/8/10 ; Adobe Reader ; дисковод CD-ROM. – Загл. с титул. экрана.

Способствует формированию у обучающихся практических навыков построения, моделирования и оценки эффективности компьютерных сетей средствами Cisco Packet Tracer. Приведены практические задания и задания для самостоятельной работы.

Предназначен для студентов вузов направлений подготовки 10.03.01 «Информационная безопасность», 10.05.04 «Информационно-аналитические системы безопасности» и аспирантов. Полезен студентам других направлений подготовки, а также широкому кругу специалистов по информационным технологиям.

Рекомендовано для формирования профессиональных компетенций в соответствии с ФГОС ВО.

Табл. 3. Ил. 162. Библиогр.: 32 назв.

ISBN 978-5-9984-1232-5

© ВлГУ, 2020
© Монахова М. М., 2020

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ	7
Практическая работа 1. УСТАНОВКА CISCO PACKET TRACER....	22
<i>Упражнение 1.1.</i> Установка Cisco Packet Tracer на операционную систему Windows 10	22
<i>Упражнение 1.2.</i> Установка Cisco Packet Tracer 7.1 на дистрибутив Linux Ubuntu 16.04	30
<i>Упражнение 1.3.</i> Установка Cisco Packet Tracer 7.3.0 на дистрибутив Linux Ubuntu 19.10	41
Контрольные вопросы.....	45
Задание.....	45
Практическая работа 2. НАЧАЛЬНЫЕ СВЕДЕНИЯ ОБ ИСПОЛЬЗОВАНИИ ПРОГРАММЫ CISCO PACKET TRACER.....	46
2.1. Краткие сведения.....	46
2.2. Практические упражнения	61
<i>Упражнение 2.1.</i> Топологическая модель локальной сети между двумя компьютерами.....	61
<i>Упражнение 2.2.</i> Построение сети из нескольких компьютеров с заданной топологией.....	66
Контрольные вопросы.....	85
Задания.....	85
Практическая работа 3. МОДЕЛИРОВАНИЕ СЕТИ С ТОПОЛОГИЕЙ ЗВЕЗДА	87
3.1. Краткая теория.....	87
3.2. Практические упражнения	88

Оглавление

<i>Упражнение 3.1.</i> Моделирование сети с топологией звезда на базе концентратора	88
<i>Упражнение 3.2.</i> Моделирование сети с топологией звезда на базе коммутатора.....	95
<i>Упражнение 3.3.</i> Исследование качества передачи трафика по сети	96
Контрольные вопросы.....	103
Задания.....	103
Практическая работа 4. КОМАНДНАЯ СТРОКА УПРАВЛЕНИЯ УСТРОЙСТВАМИ И РЕЖИМ СИМУЛЯЦИИ	105
4.1. Командная строка управления устройствами CLI.....	105
4.2. Список команд	109
4.3. Практические упражнения	123
<i>Упражнение 4.1.</i> Знакомство с командами Cisco IOS	123
4.4. Режим симуляции в Cisco Packet Tracer.....	127
<i>Упражнение 4.2.</i> Режим симуляции работы сети	128
<i>Упражнение 4.3.</i> Настройка сетевых параметров ПК в его графическом интерфейсе	135
<i>Упражнение 4.4.</i> Режим симуляции	137
Контрольные вопросы.....	143
Задания.....	144
Практическая работа 5. МОДЕЛИРОВАНИЕ ВИРТУАЛЬНЫХ ЛОКАЛЬНЫХ СЕТЕЙ.....	146
5.1. Виртуальная локальная сеть.....	146
5.2. Практические упражнения	154
<i>Упражнение 5.1.</i> VLAN с одним коммутатором	154

Оглавление

<i>Упражнение 5.2.</i> Настройка виртуальной сети на коммутаторе 2960.....	161
<i>Упражнение 5.3.</i> VLAN с двумя коммутаторами. Разделяемый общий канал	166
<i>Упражнение 5.4.</i> Настройка виртуальной сети из двух свитчей и четырех ПК	172
<i>Упражнение 5.5.</i> Настройка VLAN в корпоративной сети	179
Контрольные вопросы.....	185
Задания.....	185
ПРАКТИЧЕСКОЕ ЗАДАНИЕ № 1	188
Методические рекомендации по выполнению практического задания	190
<i>Упражнение 1.</i> Задание имен всех устройств пользователя в соответствии с заданной топологией сети	190
<i>Упражнение 2.</i> Назначение для всех устройств пользователя доменного имени wsrvuz19.ru	192
<i>Упражнение 3.</i> Создание на всех устройствах пользователя wsrvuz19 с паролем cisco.....	192
<i>Упражнение 4.</i> Реализация для всех устройств модели AAA	193
<i>Упражнение 5.</i> Установка на всех устройствах пароля wsr на вход в привилегированный режим.....	206
ПРАКТИЧЕСКОЕ ЗАДАНИЕ № 2.....	208
Методические рекомендации по выполнению практического задания	210
<i>Упражнение 1.</i> Создание на всех устройствах виртуальных интерфейсов, подынтерфейсов и интерфейсов типа петля. Назначение IP-адресов в соответствии с топологией	211

Оглавление

<i>Упражнение 2.</i> Включение механизма SLAAC для выдачи IPv6-адресов в сети MNG на интерфейсе маршрутизатора RTR1.....	216
<i>Упражнение 3.</i> Назначение вручную на всех устройствах (кроме PC1 и WEB) link-local адресов.....	218
<i>Упражнение 4.</i> Отключение на всех коммутаторах всех неиспользуемых в задании портов.....	219
<i>Упражнение 5.</i> На коммутаторе SW1 включение блокировки на 1 минуту в случае двукратного неправильного ввода пароля в течение 30 секунд.....	221
<i>Упражнение 6.</i> Установка доступности всех устройств для управления по протоколу SSH версии 2.....	221
ЗАДАНИЯ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ	225
<i>Задание 1.</i> Работа с интерфейсом оборудования Cisco	225
<i>Задание 2.</i> Настройка статической маршрутизации на оборудовании Cisco	226
<i>Задание 3.</i> Настройка протоколов маршрутизации RIP на оборудовании Cisco	228
<i>Задание 4.</i> Применение списков доступа на оборудовании Cisco	230
ЗАКЛЮЧЕНИЕ	233
БИБЛИОГРАФИЧЕСКИЙ СПИСОК	235

ВВЕДЕНИЕ

Задачи сетевого администрирования состоят в обеспечении надежной, бесперебойной и безопасной работы корпоративной сети. Слово «корпорация» означает объединение предприятий, работающих под централизованным управлением и решающих общие задачи. Корпорация является сложной, многопрофильной структурой и вследствие этого имеет распределенную иерархическую систему управления. Для централизованного управления таким объединением предприятий используется корпоративная сеть.

Основная задача корпоративной сети заключается в обеспечении передачи информации между различными приложениями, используемыми в организации. Под приложением понимается программное обеспечение, которое непосредственно нужно пользователю.

Будем рассматривать корпоративную сеть как совокупность программных, аппаратных и коммуникационных средств, обеспечивающих эффективное распределение вычислительных ресурсов. Все сети можно условно разделить на 3 категории: локальные сети (LAN, Local Area Network), глобальные сети (WAN, Wide Area Network), городские сети (MAN, Metropolitan Area Network).

Обязательным компонентом корпоративной сети являются локальные сети, связанные между собой. Основное назначение LAN состоит в объединении пользователей (как правило, одной организации) для совместной работы. LAN обеспечивают наивысшую скорость обмена информацией между компьютерами.

Инфраструктура сети - это набор физических и логических компонентов, которые обеспечивают связь, безопасность, маршрутизацию, управление, доступ и другие обязательные свойства сети.

Сетевая инфраструктура строится из различных компонентов, которые условно можно разнести по следующим уровням:

Введение

1. кабельная система и средства коммуникаций;
2. активное сетевое оборудование;
3. сетевые протоколы;
4. сетевые службы;
5. сетевые приложения.

Каждый из этих уровней может состоять из различных подуровней и компонент. Например, кабельные системы могут быть построены на основе коаксиального кабеля («толстого» или «тонкого»), витой пары (экранированной и неэкранированной), оптоволоконна. Активное сетевое оборудование включает в себя такие виды устройств, как повторители (репитеры), мосты, концентраторы, коммутаторы, маршрутизаторы.

В корпоративной сети может быть использован богатый набор сетевых протоколов: TCP/IP, SPX/IPX, NetBEUI, AppleTalk и др.

Основу работы сети составляют сетевые службы (сервисы). Базовый набор сетевых служб любой корпоративной сети состоит из следующих служб:

- службы сетевой инфраструктуры DNS, DHCP, WINS;
- службы файлов и печати;
- службы каталогов (например, Novell NDS, MS Active Directory);
- службы обмена сообщениями;
- службы доступа к базам данных.

Самый верхний уровень функционирования сети — сетевые приложения.

Сопровождение, администрирование и управление логической инфраструктурой существующей сети требует глубокого знания многих сетевых технологий. Администратор сети даже в небольшой организации должен уметь создавать различные типы сетевых подключений, устанавливать и конфигурировать необходимые сетевые протоколы, знать методы ручной и автоматической адресации и методы разрешения имен и, наконец, устранять неполадки связи, адресации, доступа, безопасности и разрешения имен.

В средних и крупных сетях у администраторов более сложные задачи:

Введение

- настройка виртуальных частных сетей (VPN);
- создание, настройка и устранение неполадок интерфейсов и таблиц маршрутизации;
- создание и поддержка подсистемы безопасности на основе открытых ключей;
- обслуживание смешанных сетей с разными ОС, в том числе Microsoft Windows и UNIX.

Сеть позволяет легко взаимодействовать друг с другом самым различным видам компьютерных систем благодаря стандартизованным методам передачи данных, которые позволяют скрыть от пользователя все многообразие сетей и машин.

Для описания работы сети разработаны специальные модели. В настоящее время общепринятыми моделями являются модель OSI (Open System Interconnection) и модель TCP/IP.

Задачи сетевого администрирования:

Планирование сети - добавление или удаление рабочих станций, добавление или удаление сетевых протоколов, добавление или удаление сетевых служб, установка серверов, разбиение сети на сегменты, чтобы новые устройства, узлы или протоколы включались в сеть или исключались из нее без нарушения целостности сети, без снижения производительности, без нарушения инфраструктуры сетевых протоколов, служб и приложений.

Установка и настройка сетевых узлов (устройств активного сетевого оборудования, персональных компьютеров, серверов, средств коммуникаций) - замену сетевого адаптера в ПК с соответствующими настройками компьютера, перенос сетевого узла (ПК, сервера, активного оборудования) в другую подсеть с соответствующим изменением сетевых параметров узла, добавление или замена сетевого принтера с соответствующей настройкой рабочих мест.

Установка и настройка сетевых протоколов - планирование и настройка базовых сетевых протоколов корпоративной сети, тестирование работы сетевых протоколов, определение оптимальных конфигураций протоколов.

Введение

=====

Установка и настройка сетевых служб:

- установка и настройка служб сетевой инфраструктуры (службы DNS, DHCP, WINS, службы маршрутизации, удаленного доступа и виртуальных частных сетей);
- установка и настройка служб файлов и печати, которые в настоящее время составляют значительную часть всех сетевых служб;
- администрирование служб каталогов (Novell NDS, Microsoft Active Directory), составляющих основу корпоративной системы безопасности и управления доступом к сетевым ресурсам;
- администрирование служб обмена сообщениями (системы электронной почты);
- администрирование служб доступа к базам данных.

Поиск неисправностей. От неисправного сетевого адаптера на рабочей станции пользователя до сбоев отдельных портов коммутаторов и маршрутизаторов, а также неправильные настройки сетевых протоколов и служб.

Поиск узких мест сети и повышения эффективности работы сети - анализ работы сети и определение наиболее узких мест, требующих либо замены сетевого оборудования, либо модернизации рабочих мест, либо изменения конфигурации отдельных сегментов сети.

Мониторинг сетевых узлов - наблюдение за функционированием сетевых узлов и корректностью выполнения возложенных на данные узлы функций.

Мониторинг сетевого трафика позволяет обнаружить и ликвидировать: высокую загруженность отдельных сетевых сегментов, чрезмерную загруженность отдельных сетевых устройств, сбои в работе сетевых адаптеров или портов сетевых устройств, нежелательную активность или атаки злоумышленников (распространение вирусов, атаки хакеров и др.).

Введение

Обеспечение защиты данных:

- резервное копирование и восстановление данных;
- разработка и осуществление политик безопасности учетных записей пользователей и сетевых служб (требования к сложности паролей, частота смены паролей);
- построение защищенных коммуникаций (применение протокола IPSec, построение виртуальных частных сетей, защита беспроводных сетей);
- планирование, внедрение и обслуживание инфраструктуры открытых ключей (PKI).

Моделирование сети

Моделирование сети является обязательной частью любого проекта (модернизации) корпоративной сети.

Целями моделирования могут являться:

- определение оптимальной топологии;
- выбор сетевого оборудования;
- определение рабочих характеристик сети;
- проверка характеристик новых протоколов.

На модели можно проверить влияние всплесков загрузки, воздействие большого потока широковещательных запросов, что вряд ли кто-то может себе позволить в работающей сети.

Перечисленные задачи предъявляют различные требования к программам, моделирующим функционирование сети. При этом определение характеристик сети до того, как она будет введена в эксплуатацию, имеет первостепенное значение, так как позволяет отрегулировать характеристики локальной сети на стадии проектирования (модернизации). Решение этой проблемы возможно путем аналитического или статистического моделирования.

Введение

Аналитическое моделирование сети представляет собой совокупность математических соотношений, связывающих между собой входные и выходные характеристики сети. При выводе таких соотношений приходится пренебрегать малозначительными деталями или обстоятельствами.

Симуляционное (статистическое) моделирование служит для анализа системы с целью выявления критических элементов сети. Этот тип моделирования используется также для предсказания будущих характеристик системы. Процесс моделирования включает в себя формирование модели, отладку моделирующей программы и проверку корректности выбранной модели. Последний этап обычно состоит из сравнения расчетных результатов с экспериментальными данными, полученными для реальной сети.

Возможны разные подходы к моделированию. Классический подход заключается в воспроизведении событий в сети как можно точнее и поэтапном моделировании последствий этих событий.

Другим подходом может стать метод, где для каждого логического сегмента (зоны столкновений) сначала моделируется очередь событий.

Полное моделирование сети с учетом рабочих приложений предполагает использование следующих характеристик:

- характеристики узла;
- характеристики соединений;
- используемые протоколы;
- характеристики отправляемых пакетов.

Характеристики протоколов:

- длина пакета, посылаемого каждым узлом (длина сообщения + длина адресной части + длина дополнительной присоединяемой информации);
- длина сообщения;
- временное распределение моментов посылки пакетов.

Введение

Структура описания каждого из узлов включает в себя:

- номер узла (идентификатор);
- код типа узла;
- MAC-адрес;
- IP-адрес;
- байт статуса (узел ведет передачу; до узла дошел чужой пакет);
- код используемого протокола (IPv4 или IPv6; TCP, UDP, ICMP и т.д.);
- объем входного/выходного буфера. Тип буфера (FIFO, LIFO и т.д.).

В каждом из существующих способов моделирования есть свои недостатки. Осуществляя построение сети, необходимо помнить к каким результатам должна привести данная модель.

Для более детального анализа было решено использовать статистическое представление модели. Результаты, полученные с помощью моделирования всех процессов в сети, будут достаточным основанием для оценки качества построенной сети. Данная модель предполагает моделирование процессов в сети при помощи специальных программных средств.

Программа моделирования PacketTracer

Cisco Packet Tracer [3, 4, 6, 28] разработан компанией Cisco и рекомендован ею использоваться при изучении телекоммуникационных сетей и сетевого оборудования, а также для проведения лабораторного практикума в высших учебных заведениях.

Cisco Packet Tracer - это программный эмулятор сети, созданный компанией Cisco. Логотип программы представлен на рисунке В.1.

Cisco Packet Tracer позволяет строить и анализировать сети на разнообразном оборудовании в произвольных топологиях с поддержкой разных протоколов. В эмуляторе можно получить возможность

Введение

=====

изучать работу различных сетевых устройств: маршрутизаторов, коммутаторов, точек беспроводного доступа, персональных компьютеров, сетевых принтеров и т.д.

Данное программное приложение является наиболее простым и эффективным среди своих конкурентов. Так, например, создание нового проекта сети в Cisco Packet Tracer занимает существенно меньше времени, чем в аналогичной программе GNS3, кроме того, Cisco Packet Tracer проще в установке и настройке.



Рисунок В.1 - Логотип программы Cisco Packet Tracer

Введение

=====

Cisco Packet Tracer может быть востребован, чтобы не тратить деньги на лабораторные стенды для изучения компьютерных сетей. Профессиональное сетевое оборудование стоит немалых денег и не факт, что вложения предприятия в дальнейшем окупятся, если вы решите собрать реальных физический стенд.

Cisco Packet Tracer дает возможность собирать схемы, которые используются в реальных компьютерных сетях сегмента Enterprise (корпоративные сети) или в провайдерских сетях.

Основные возможности Packet Tracer:

- дружелюбный графический интерфейс (GUI), что способствует лучшему пониманию организации сети, принципов работы сетевого оборудования;

- возможность моделировать логическую топологию - рабочее пространство для того, чтобы создать сети любого размера на CCNA-уровне сложности. CCNA (Cisco Certified Network Associate) Routing and Switching – это самый распространённый сертификат в системе сертификации Cisco, де-факто являющийся почти обязательным для серьёзной работы с современным сетевым оборудованием. Обладание им означает, что специалист владеет необходимыми познаниями и навыками для того, чтобы устанавливать, конфигурировать и работать с сетями среднего и небольшого размера, а также выявлять и устранять возникающие в них проблемы. Получение статуса CCNA особенно выгодно для выпускников вузов и молодых специалистов, не имеющих внушительного портфолио, поскольку позволяет заметно выделиться на фоне других соискателей и гарантировать работодателю определённый уровень навыков и познаний;

- возможность моделировать сети в режиме реального времени, включая режим симуляции;

- многоязычность интерфейса Packet Tracer, что позволяет изучать программу на своем родном языке;

- усовершенствованное изображение сетевого оборудования со способностью добавлять / удалять в изображение сетевого оборудования различные компоненты;

- наличие Activity Wizard позволяет сетевым инженерам, студентам и преподавателям создавать шаблоны сетей и использовать их в дальнейшем.

Введение

=====

Отметим, что в Packet Tracer реализовано не очень большое количество устройств, а их функционал по сравнению с реальными аналогами урезан, но этого более чем достаточно для прохождения начальных курсов Cisco ICND1 и ICND2. Для прохождения дальнейших курсов могут потребоваться более универсальные решения, например, GNS3 или eve-NG.

В Cisco Packet Tracer маршрутизаторы и коммутаторы реализованы программно, то есть код приложения Cisco Packet Tracer просто реализует процессы, которые происходят в реальных компьютерных сетях, а вот eve-NG и GNS3 уже эмулируют сетевые устройства и для их работы требуются оригинальные образы операционных систем, которые работают на реальных коммутаторах и маршрутизаторах. И каждое из устройств в GNS3 или eve-NG будет «съедать» значительную часть ресурсов вашего компьютера.

Еще одна замечательная особенность Cisco Packet Tracer заключается в том, что это приложение позволяет заглянуть внутрь пакета, кадра, сегмента или сообщения на том или ином участке сети, это дает углубленное понимание того, как устроены компьютерные сети, но и тут стоит отметить, что некоторые фрагменты, передаваемые по сети Packet Tracer урезаны. В приложениях eve-NG или GNS3 коммутируются полноценные пакеты по спроектированной сети, но для того, чтобы увидеть их содержимое вам потребуется WireShark или аналогичное по своему функционалу приложение.

В общем, Cisco Packet Tracer позволяет моделировать фрагменты реальных компьютерных сетей, а также дает возможность поработать с оборудованием Cisco и попробовать его настроить. Стоит отметить, что eve-NG и GNS3 позволяют виртуализировать не только оборудование Cisco, но и устройства других производителей.

Широкий круг возможностей Cisco Packet Tracer позволяет сетевым инженерам: конфигурировать, отлаживать и строить вычислительную сеть.

Эмулятор сети позволяет сетевым инженерам проектировать сети любой сложности, создавая и отправляя различные пакеты данных, сохранять и комментировать свою работу. Специалисты могут изучать и использовать такие сетевые устройства, как коммутаторы второго и третьего уровней, рабочие станции, определять типы связей между ними и соединять их.

Введение

На заключительном этапе, после того как сеть спроектирована, специалист может приступить к конфигурированию выбранных устройств посредством терминального доступа или командной строки (рисунок В.2).

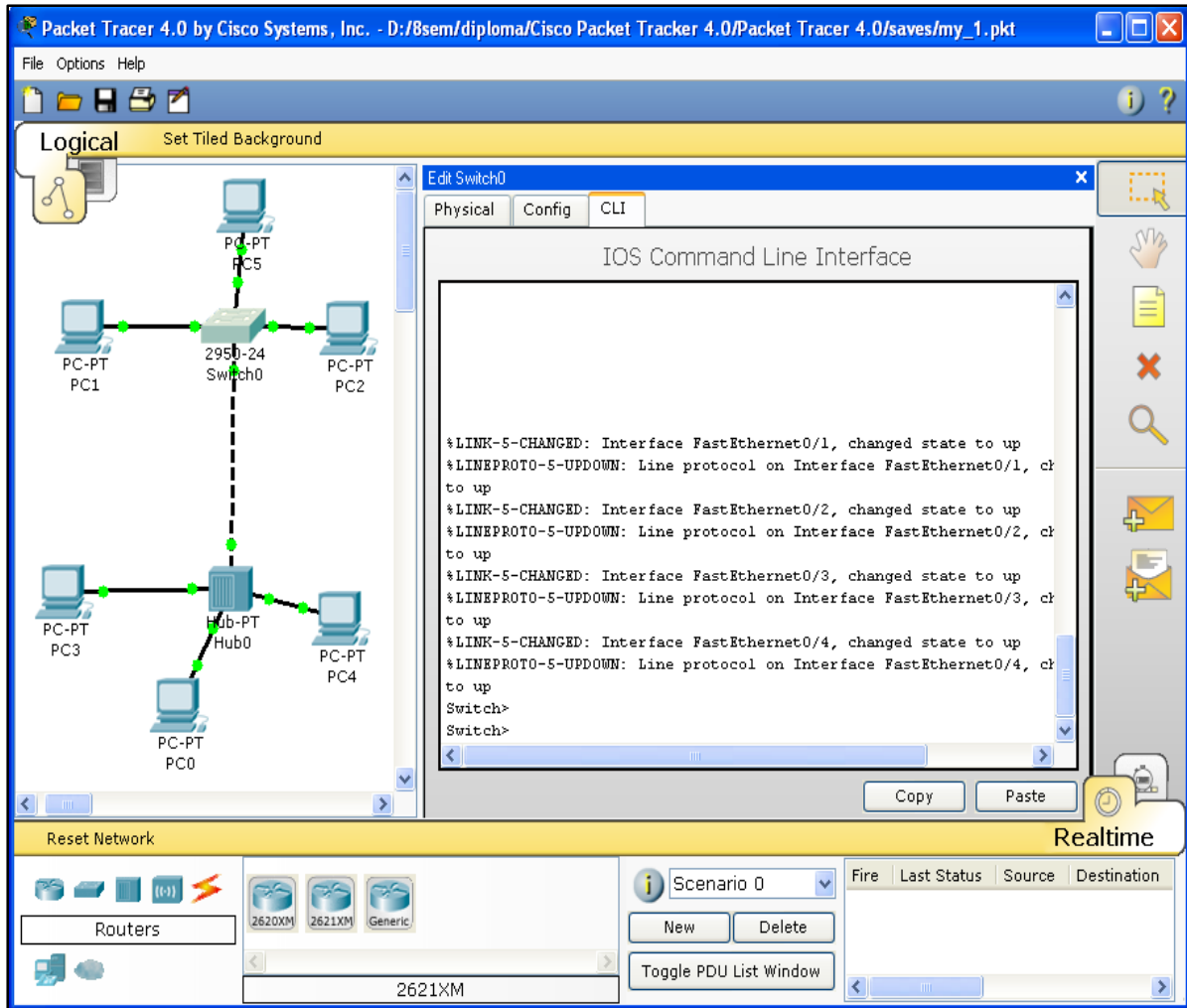


Рисунок В.2 - Cisco Packet Tracer

Одной из самых важных особенностей Packet Tracer является наличие в нем «Режима симуляции» (рисунок В.3). В данном режиме все пакеты, пересылаемые внутри сети, отображаются в графическом виде. Эта возможность позволяет сетевым специалистам наглядно продемонстрировать, по какому интерфейсу в данные момент перемещается пакет, какой протокол используется и т.д.

Введение

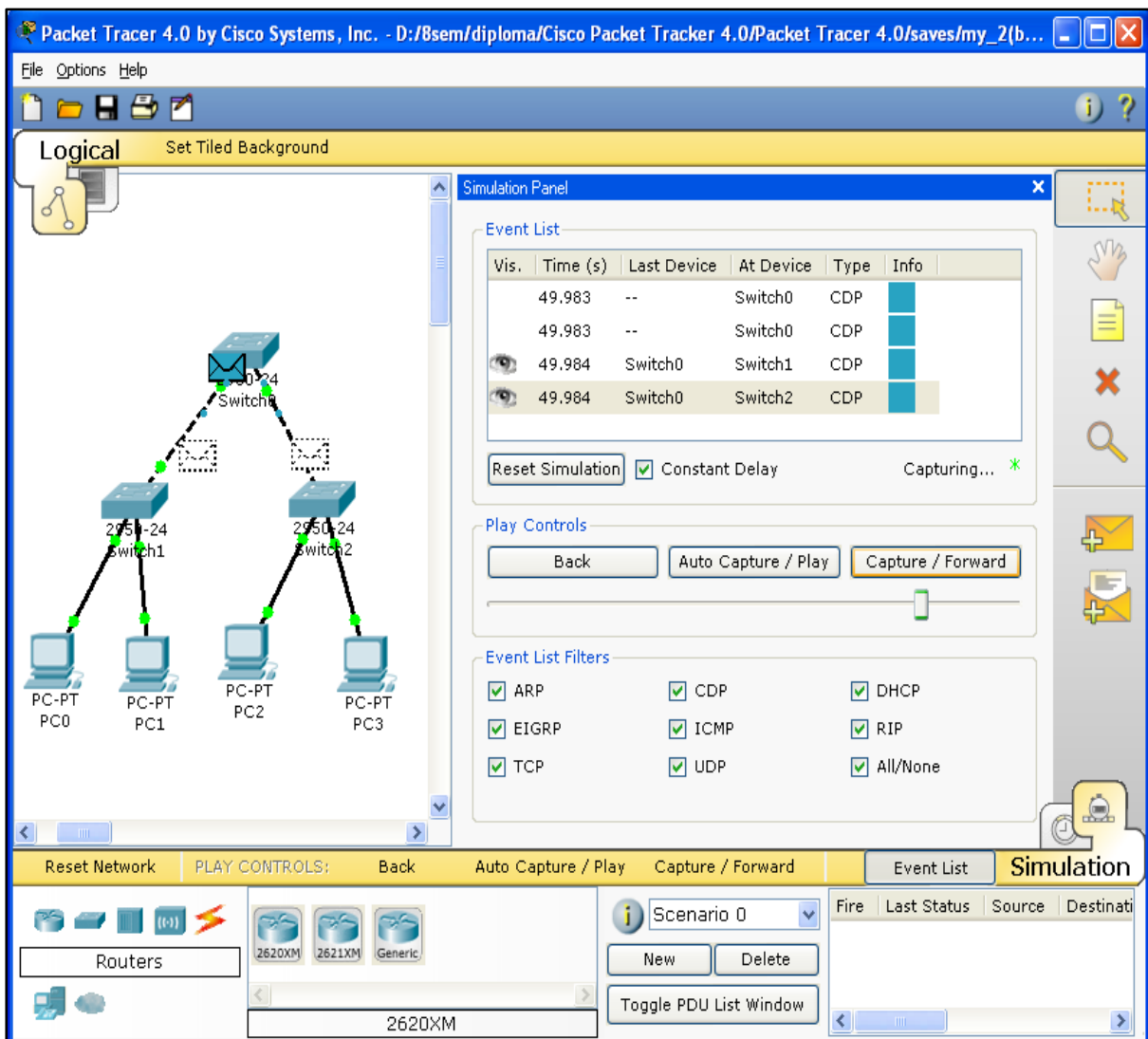


Рисунок В.3 - Режим «Симуляции» в Cisco Packet Tracer

Однако, это не все преимущества Packet Tracer: в «Режиме симуляции» сетевые инженеры могут не только отслеживать используемые протоколы, но и видеть, на каком из семи уровней модели OSI данный протокол задействован (рисунок В.4).

Такая кажущаяся на первый взгляд простота и наглядность делает практические занятия чрезвычайно полезными, совмещая в них как получение, так и закрепление полученного материала.

Packet Tracer способен моделировать большое количество устройств различного назначения, а также немало различных типов связей, что позволяет проектировать сети любого размера на высоком уровне сложности.

Введение

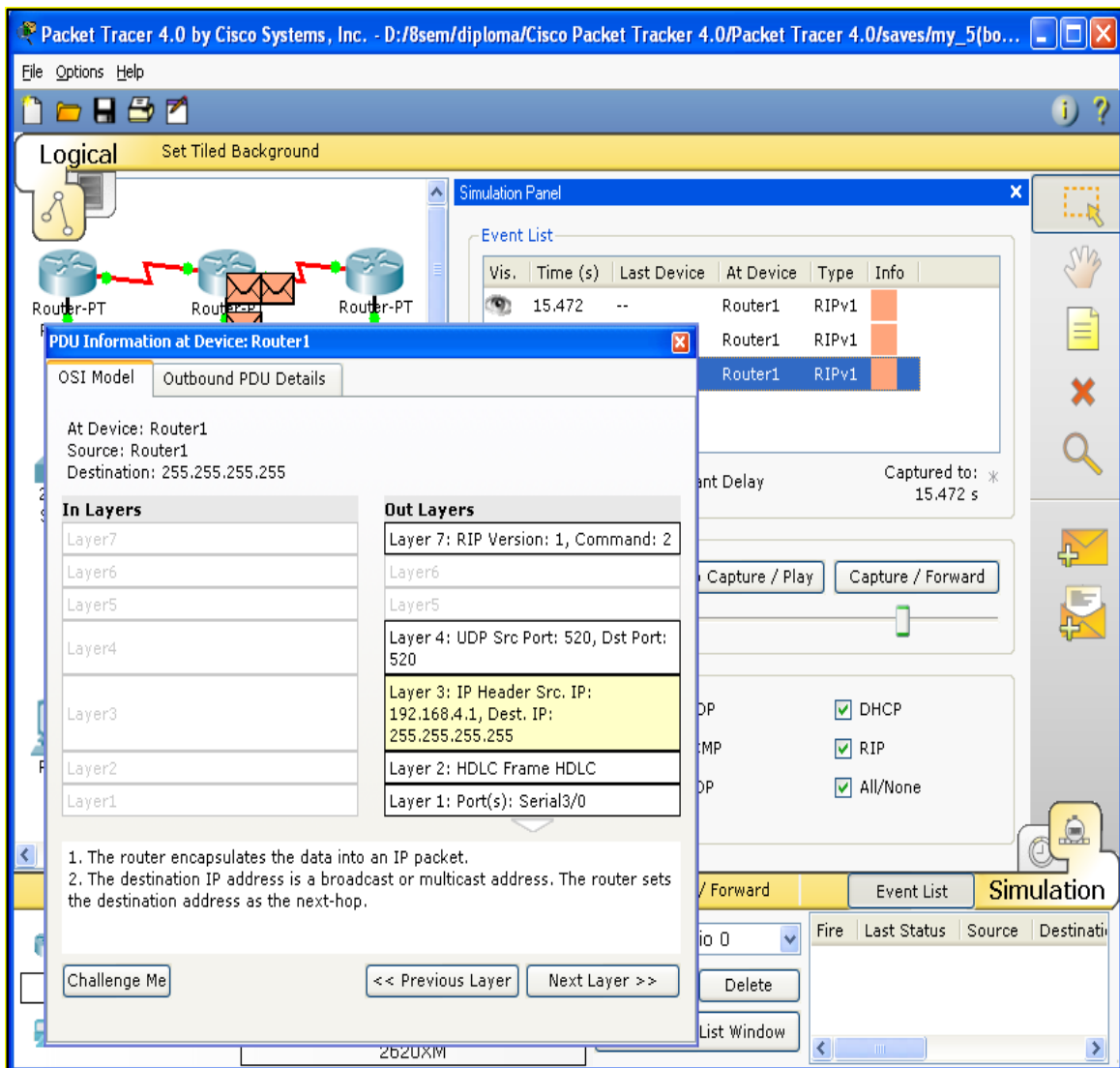


Рисунок В.4 - Анализ семиуровневой модели OSI в Cisco Packet Tracer

Моделируемые устройства:

- маршрутизаторы Cisco 4331, 4321, 2911, 2901, 1941, 2811, 1841;
- коммутаторы третьего уровня Cisco 3560-24PS, 3650-24PS;
- коммутаторы второго уровня Switch 2960-24, 2950-24, Switch 2950T, Switch-PT, соединение типа «мост» Bridge-PT;
- сетевые концентраторы Hub-PT, повторитель Repeater-PT;
- оконечные устройства рабочая станция PC-PT, сервер Server-PT, принтер Printer-PT;
- беспроводные устройства - точка доступа AccessPoint-PT;
- глобальная сеть WAN.

Введение

=====
Типы связей: консоль, медный кабель без перекрещивания (прямой кабель), медный кабель с перекрещиванием (кросс-кабель), волоконно-оптический кабель, телефонная линия, Serial DCE, Serial DTE.

Моделируемые протоколы: ARP, CDP, DHCP, EIGRP, ICMP, RIP, TCP, UDP.

Курс построен на изучении версии программы Cisco Packet Tracer 6.1.1. Поэтому примеры курса следует выполнять в этой версии программы или более поздней.

Практическая работа №1 посвящена описанию процедур установки Cisco Packet Tracer на операционную систему Windows 10 и на дистрибутив Linux Ubuntu 16.04.

Использование программы Cisco Packet Tracer, например, для построения сети из двух компьютеров и сети из нескольких компьютеров с заданной топологией составляет основное содержание практической работы №2

Приобретение практических навыков обучающимися в построении, моделировании и оценке эффективности компьютерных сетей, построенных на основе топологии «звезда» составляет главную цель практической работы №3. Здесь же анализируется два способа построения сети – на базе концентратора и на базе коммутатора.

Особенности работы с командной строкой управления устройствами в Cisco Packet Tracer составляет основное содержание практической работы №4.

Практическая работа №5 посвящена приобретению практических навыков обучающимися в построении, моделировании и оценке эффективности виртуальных локальных компьютерных сетей.

Приведены два практических задания по курсу. В первом для всех устройств требуется реализовать модель AAA. Во втором - создать виртуальные интерфейсы, подынтерфейсы и интерфейсы типа петля, включить механизм SLAAC.

Завешают практикум задания для самостоятельной работы.

Цель издания – формирование профессиональных навыков и компетенций будущих специалистов в области информационной без-

Введение

=====

опасности, системного администрирования, неотъемлемой частью которого является теория вычислительных систем и сетей с безопасностью информационных ресурсов. Стоит отметить, что концептуальное понимание изложенного материала служит базисом любой профессии в сфере информационных технологий. От читателей требуется выработка умений по поиску, обработке, систематизации и анализу информации. Необходимо научиться принимать взвешенные, конструктивные и аргументированные решения, в минимальные сроки изучать материал на концептуальном уровне и оперативно решать поставленные задачи.

Практическая работа 1. УСТАНОВКА CISCO PACKET TRACER

Цель работы – приобретение практических навыков обучающимися в установке Cisco Packet Tracer на операционную систему Windows 10 и на дистрибутив Linux Ubuntu 16.04.

Порядок выполнения работы – внимательно изучите теоретический материал, выполните все упражнения, включённые в данный раздел в пошаговом режиме. Если в промежуточных точках изображения Ваших моделей не совпадает с приводимыми в практикуме, вернитесь на 2-3 шага назад и все-таки добейтесь абсолютного соответствия. Самостоятельно выполните задание к практической работе.

Упражнение 1.1. Установка Cisco Packet Tracer на операционную систему Windows 10 [21, 30]

Скачивание официальной версии программы Cisco Packet Tracer

Скачать Cisco Packet Tracer можно с различных обменников или по ссылкам, которые дают блогеры в Интернете, но в этом случае Вам придется регистрировать копию своего приложения на официальном сайте академии Cisco. Отметим, что это единственный официальный источник для скачивания Cisco Packet Tracer.

Вот [ссылка](#), которая ведет на официальный сайт Cisco.

1. Кликните на ссылку. При переходе по ней Вы получите приглашение к регистрации аккаунта на сайте академии, а затем у Вас появится возможность скачать приложение и пройти дополнительные курсы, которые помогут изучить интерфейс Cisco Packet Tracer, заметим, что курсы эти на английском языке

На рисунке 1.1 показан фрагмент страницы с синей кнопкой и текстом, который поясняет, что после ее нажатия начнется процесс создания аккаунта на сайте академии.

Практическая работа 1. Установка Cisco Packet Tracer



Рисунок 1.1 - Фрагмент страницы, который поясняет процесс создания аккаунта на сайте академии

Учетные данные этого аккаунта будут нужны для регистрации Вашей копии приложения и снятия ограничений, связанных с незарегистрированной версией. Если не зарегистрировать копию Cisco Packet Tracer, то при каждом запуске приложения придется ждать 15 секунд, прежде чем начнется гостевой сеанс работы с приложением.

Создание аккаунта на сайте академии Cisco

2. После нажатия на кнопку с текстом «Зарегистрируйтесь, чтобы загрузить Cisco Packet Tracer», переходим к созданию аккаунта на сайте академии Cisco. Вы увидите небольшую форму в правой верхней части следующей веб-страницы, в эту форму нужно ввести e-mail для регистрации аккаунта, эта форма показана на рисунке 1.2.

3. В это поле введите свой e-mail. На Ваш адрес придет электронное письмо для подтверждения аккаунта на сайте Cisco, нажмите Submit.

Практическая работа 1. Установка Cisco Packet Tracer

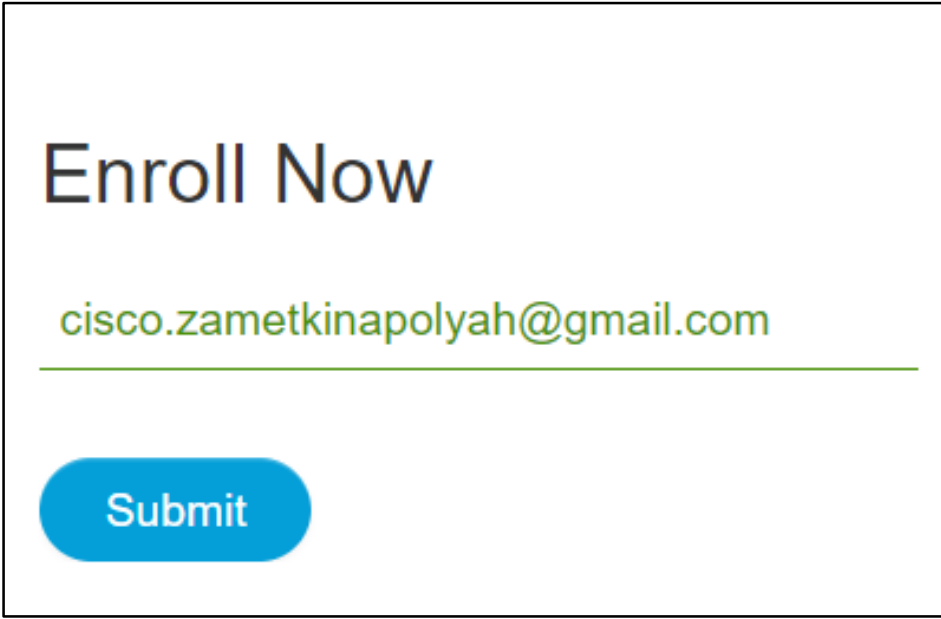


Рисунок 1.2 - Форма для ввода e-mail на сайте Cisco

4. После этого будет предложено заполнить небольшую анкету. Она нужна маркетологам Cisco. Данные в этой анкете могут быть и не настоящими, пример этой анкеты показан на рисунке 1.3.

Здесь нет ничего сложного, стоит только отметить, что русский язык анкеты можно выбрать в правом верхнем углу, дату рождения нужно вводить в формате 12/01/1993, то есть день, месяц и год должны быть отделены символом «/». Ну и пароль от вашего аккаунта должен состоять не менее, чем из 8 символов, при этом он должен содержать латинские буквы, как минимум, одна из этих букв должна быть заглавной, а также в пароле должна быть хотя бы одна цифра.

После заполнения анкеты вы попадете в свой личный кабинет, перед тем как продолжить, не забудьте зайти в указанный ранее почтовый ящик, на него придет письмо с ссылкой для активации учетной записи, переходите по ссылке и учетка будет подтверждена.

Практическая работа 1. Установка Cisco Packet Tracer

Sign Up For Introduction to Packet Tracer 0118

Мы рады, что вы присоединились к нам. Прежде чем вы начнете, мы хотели бы кое-что узнать о вас.

Русский

Имя: _____

Фамилия: _____

Адрес электронной почты: `cisco.zamelkinapolyah@gmail.com`

Я хочу получать мне важные письма от Сетевой академии Cisco

Создать пароль: _____

Пароль должен содержать не менее 8 символов.
При этом в нем должно быть не менее одной строчной буквы (abc), одной заглавной (ABC) и одной цифры (123).

Страна: Выберите один вариант

Штат/область: Выберите один вариант

Пол: Выберите один вариант

Каков Ваш практический опыт в области ИТ или сетевых технологий?

Дата рождения: `ДДММГГГГ`

Для подтверждения вашей личности при создании запроса на поддержку будет использоваться дата рождения.

Нажав «Создать учетную запись», вы соглашаетесь на наши Условия и подтверждаете, что ознакомились с Заявлением о конфиденциальности, включая нашу политику Cookies.

Создать учетную запись

Рисунок 1.3 - Анкета для регистрации аккаунта на сайте академии Cisco

Практическая работа 1. Установка Cisco Packet Tracer

5. Скачайте Cisco Packet Tracer. Необходимо обратить внимание на рисунок 1.4, здесь показан фрагмент меню, которое расположено в правом верхнем углу вашего личного кабинета.

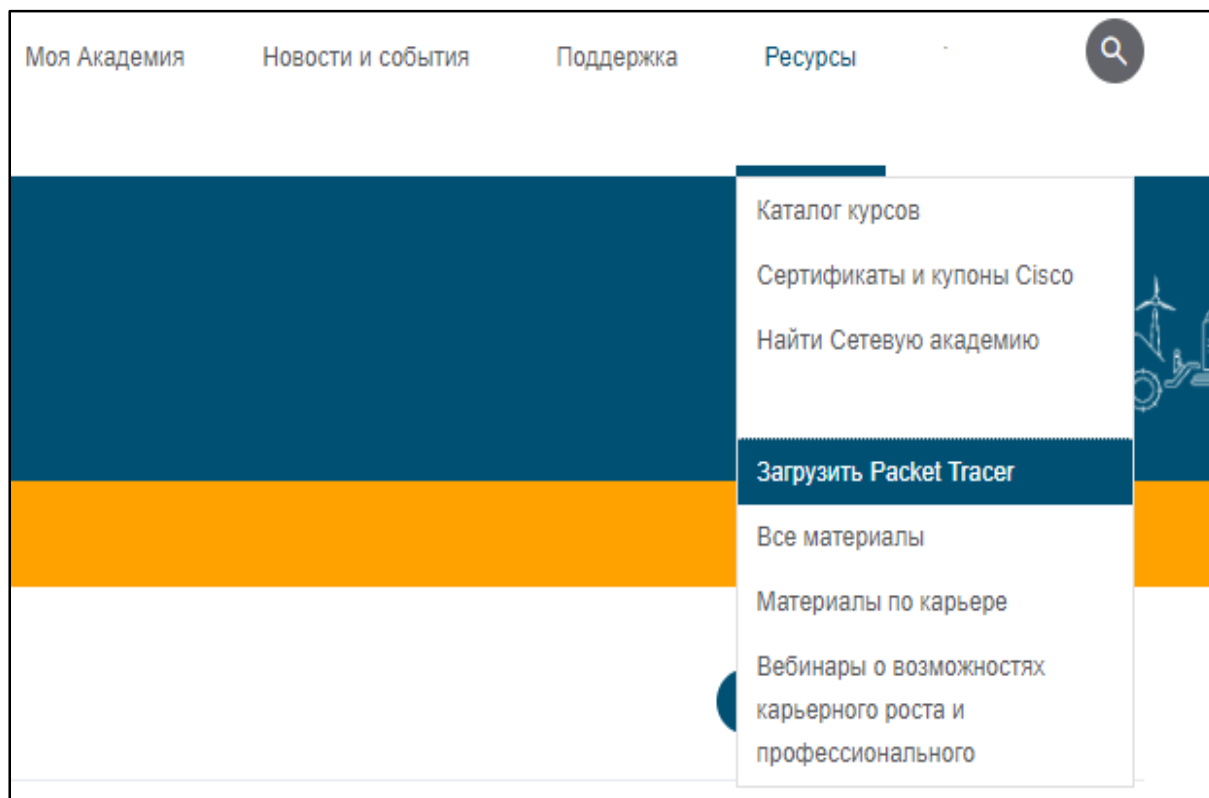


Рисунок 1.4 – Фрагмент меню личного кабинета пользователя Cisco Packet Tracer

Ссылка, ведущая к странице скачивания, подсвечена синим цветом.

6. Нажмите на нее. Вы перейдете на страницу, с которой можно скачать Packet Tracer для различных операционных систем: здесь есть версии для операционных систем семейства Windows, а также есть версия Cisco Packet Tracer для Ubuntu.

Фрагмент описанной страницы показан на рисунке 1.5.

Практическая работа 1. Установка Cisco Packet Tracer

Загрузить

Выберите операционную систему и загрузите соответствующие файлы. Посмотреть Ответы на часто задаваемые вопросы. Смотреть учебные материалы .

Для ПК на базе Windows, версии 7.1 на английском языке

Поддерживаемые версии ОС: Windows 7, 8.1, 10

Загрузка 64-
разрядной версии

Загрузка 32-
разрядной версии

Для ПК на базе Linux, версии 7.1 на английском языке

Ubuntu 14.04 поддерживается для 64-разрядной версии; Ubuntu 12.04 поддерживается для 32-разрядной версии

Загрузка 64-
разрядной версии

Для мобильных устройств

Для iOS, версии 3.0 на английском языке



Для Android, версии 3.0 на английском языке



Учебный курс Packet Tracer

Рисунок 1.5 - Страница с ссылками для скачивания Cisco Packet Tracer

Практическая работа 1. Установка Cisco Packet Tracer

Установка Cisco Packet Tracer 7.1 на Windows 10 [30]

7. Пусть актуальной является версия Cisco Packet Tracer 7.1. Подробно останавливаться на установке Packet Tracer на Windows 10 не имеет смысла, так как здесь все довольно просто: нужно согласиться с лицензией Cisco, указать папку, в которую Вы хотите установить приложение, а также совершить еще несколько простых действий, сопровождаемых нажатием кнопок «Next», «Install», «Finished».

Для пользователей Windows следует дать рекомендацию: перед установкой Cisco Packet Tracer выключите все браузеры.

После того, как программа будет установлена, вы увидите окно, которое показано на рисунке 1.6.

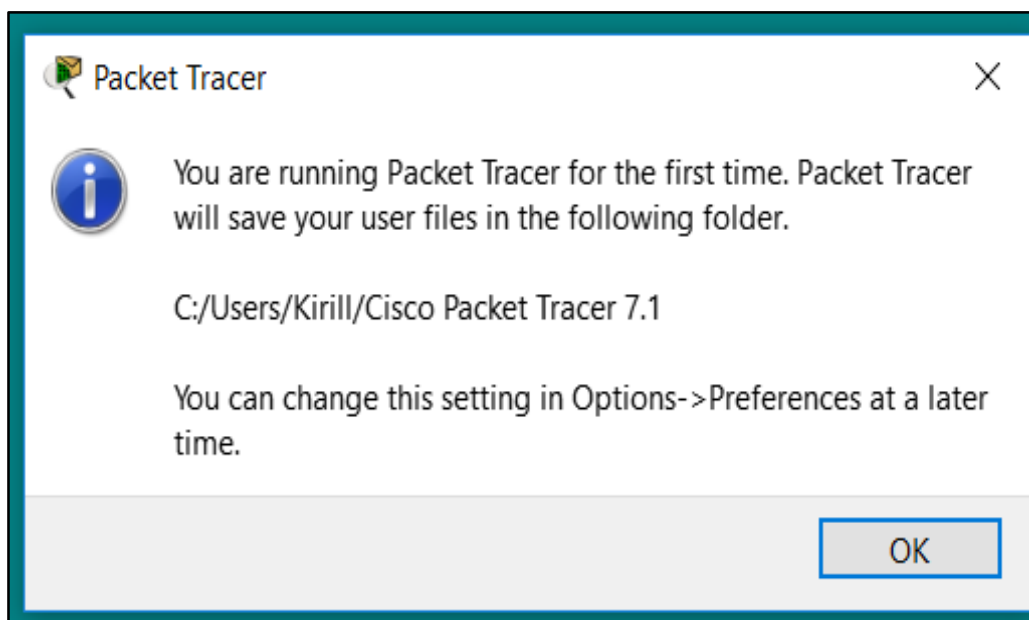


Рисунок 1.6 - Папка, в которой Cisco Packet Tracer будет хранить проекты

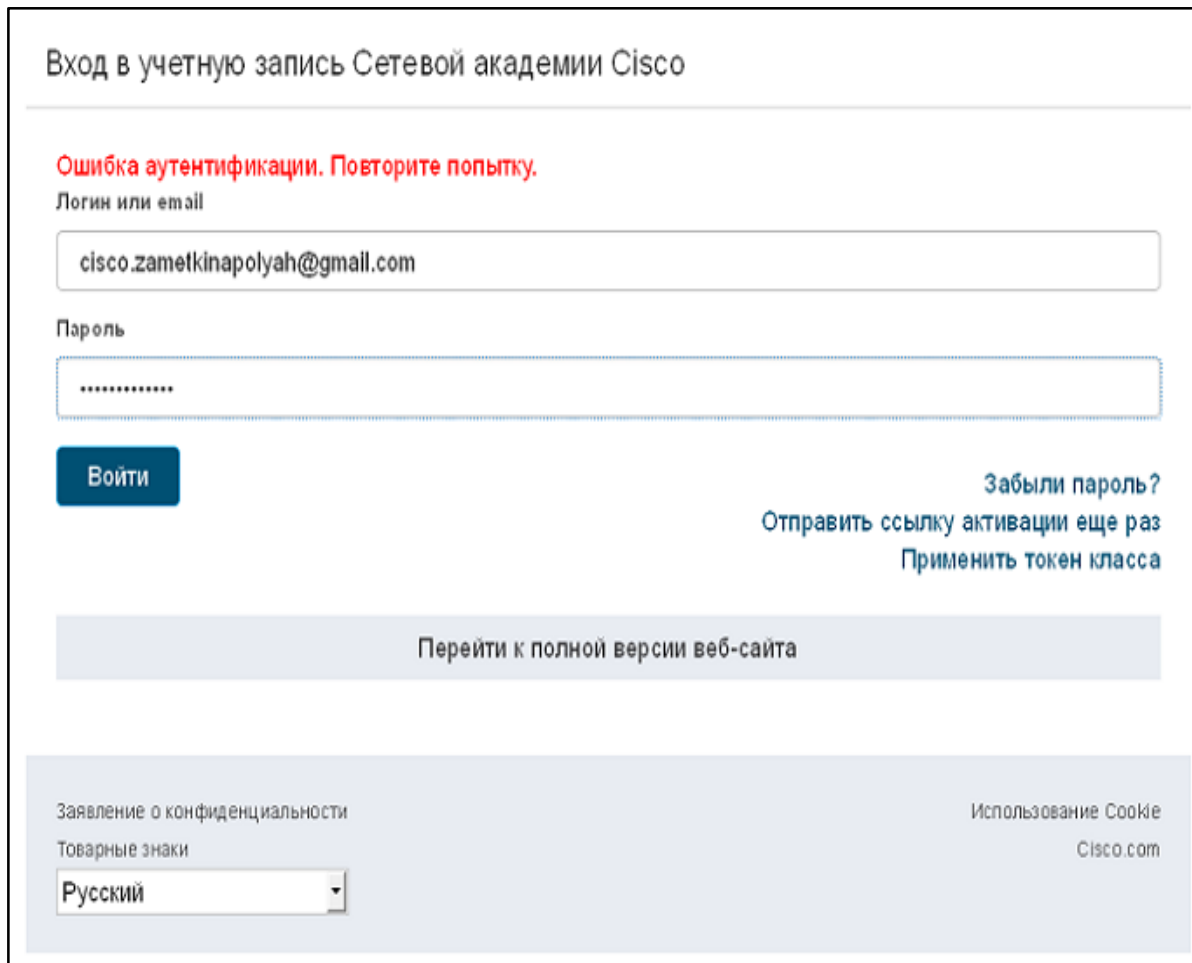
В этом окне указан путь, по которому Cisco Packet Tracer будет сохранять Ваши лабораторные проекты, в дальнейшем этот будет можно будет легко изменить.

Практическая работа 1. Установка Cisco Packet Tracer

Запуск Cisco Packet Tracer на Windows

8. Запустите Cisco Packet Tracer. При первом запуске приложение попросит указать логин и пароль от аккаунта в академии Cisco, будем полагать, что у Вас эти данные есть.

На рисунке 1.7 показан пример формы, которую предлагает заполнить Cisco Packet Tracer. После регистрации приложения Firewall вашего компьютера выдаст сообщение о неизвестном приложении.



Вход в учетную запись Сетевой академии Cisco

Ошибка аутентификации. Повторите попытку.

Логин или email

Пароль

Войти

[Забыли пароль?](#)
[Отправить ссылку активации еще раз](#)
[Применить токен класса](#)

[Перейти к полной версии веб-сайта](#)

Заявление о конфиденциальности [Использование Cookie](#)

Товарные знаки [Cisco.com](#)

Русский

Рисунок 1.7 - Регистрация копии Cisco Packet Tracer

9. Разрешите доступ для приложения Cisco Packet Tracer, рисунок 1.8 демонстрирует этот диалог.

Практическая работа 1. Установка Cisco Packet Tracer

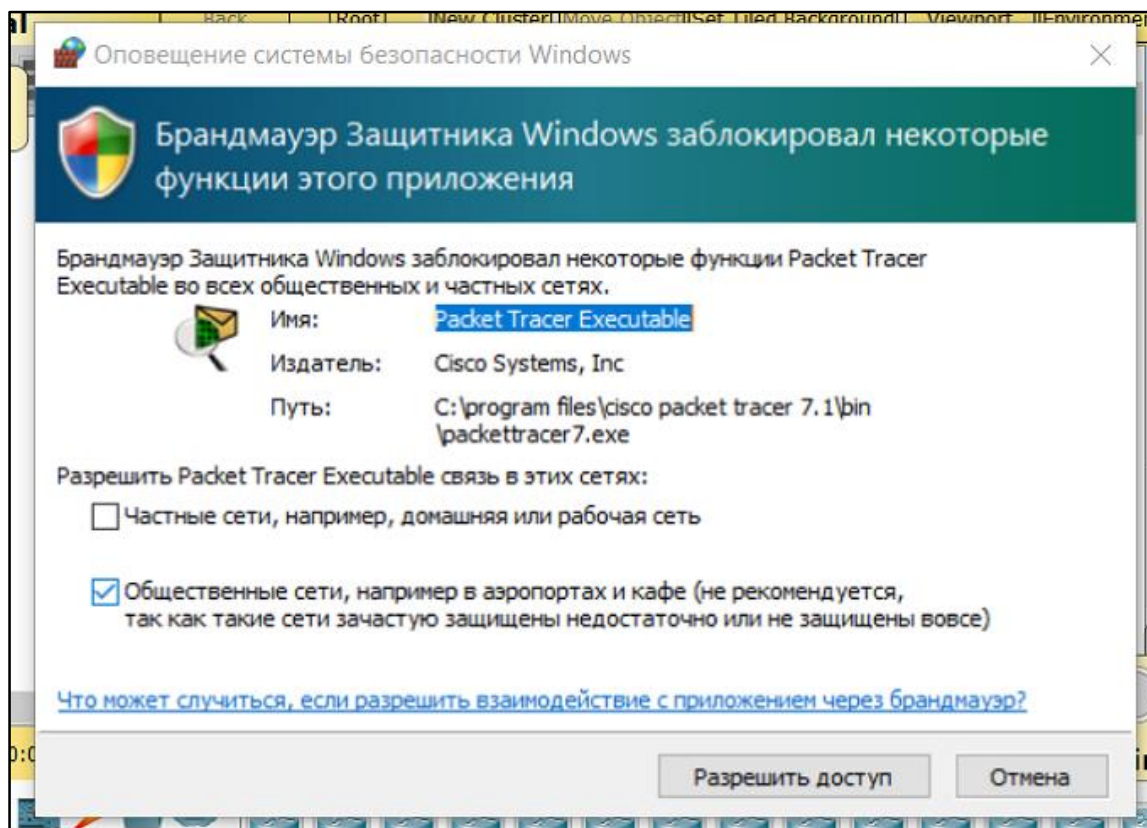


Рисунок 1.8 - Firewall Windows отреагировал на появление Cisco Packet Tracer

На этом запуск Cisco Packet Tracer в Windows завершен, Вы установили приложение, активировали его, тем самым мы получили полноценную версию приложения, с которой можно работать.

Упражнение 1.2. Установка Cisco Packet Tracer 7.1 на дистрибутив Linux Ubuntu 16.04 [29, 31, 32]

1. Этот процесс довольно прост и быстр. Первое, что нужно сделать: открыть, например, в Nautilus каталог, в который Вы скачали архив с программой и затем распаковать этот архив.

2. На рисунке 1.9 показан процесс распаковки архива, из контекстного меню, появляющегося по нажатию правой кнопки мыши по иконке архива. Вы можете распаковывать архив туда, куда вам удобно.

Практическая работа 1. Установка Cisco Packet Tracer

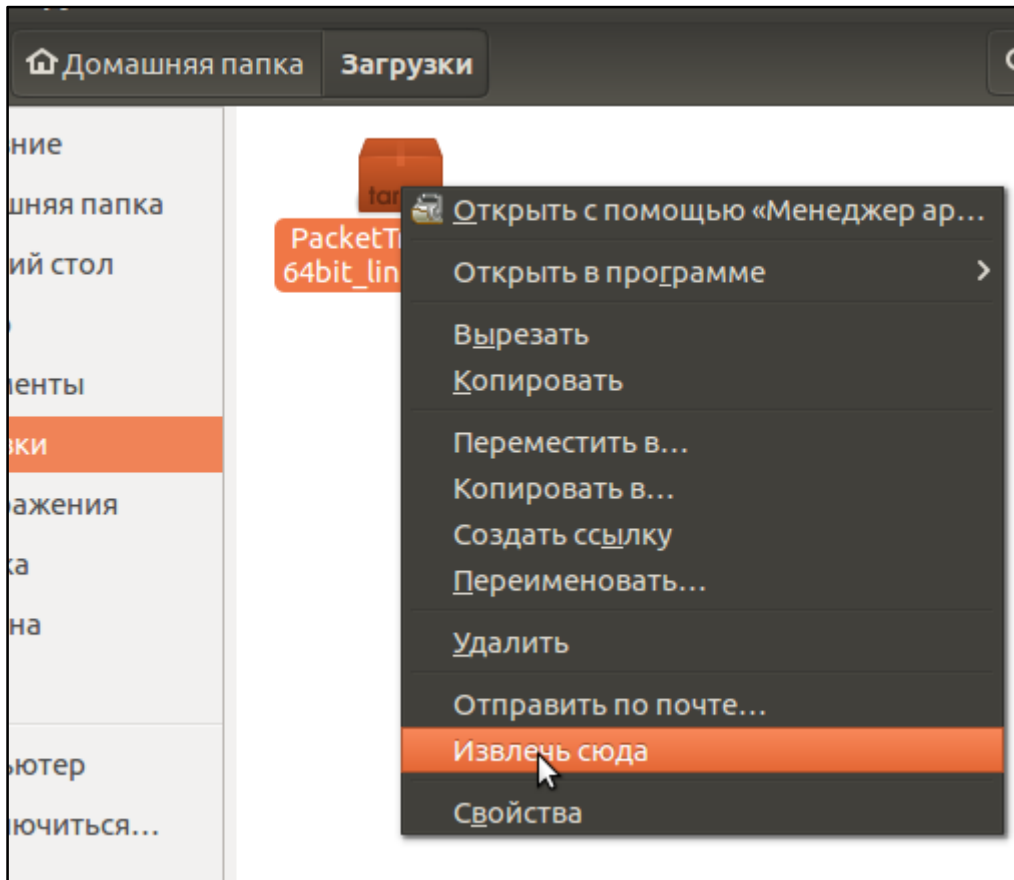


Рисунок 1.9 - Распаковка архива с программным приложением Cisco Packet Tracer

Как только архив будет извлечён, появится каталог с названием, похожим на это: **PacketTracer71_64bit_linux**.

3. Откройте эмулятор терминала, пользуясь горячими клавишами Ctrl+Alt+T. В терминале действуйте по алгоритму, описанному ниже.

4. Перейдите в каталог, который распаковали (команда **cd**) :

```
kirill@kirill-vm:~$ cd  
~/Загрузки/PacketTracer71_64bit_linux/
```

Замечание. Возможно, вместо «Загрузки» у Вас будет «Download».

Практическая работа 1. Установка Cisco Packet Tracer

=====

5. В каталоге **PacketTracer71_64bit_linux** есть файл с именем **install**, в котором находится скрипт-установщик, этому файлу нужно дать права на исполнение:

```
kirill@kirill-  
vm:~/Загрузки/PacketTracer71_64bit_linux$ sudo  
chmod +x install  
[sudo] пароль для kirill:
```

После ввода этой команды, введите пароль.

6. Исполните файл:

```
install: sudo ./install.
```

После этого Вы увидите приглашение к установке, примерно такой текст

```
Welcome to Cisco Packet Tracer 7.1 Installa-  
tion  
Read the following End User License Agreement  
"EULA" carefully. You must accept the terms of  
this EULA to install and use Cisco Packet Tracer.  
Press the Enter key to read the EULA.
```

7. Нажмите Enter, чтобы продолжить. После этого Вам предложат ознакомиться с пользовательским соглашением, которое пролистывается по нажатию клавиши «Пробел».

8. Листайте в конец соглашения и начните установку, введя в эмулятор терминала Y, а затем нажав Enter. После этого у Вас на экране терминала появится следующее сообщение

```
You have accepted the terms to the EULA. Con-  
gratulations. Packet Tracer will now be installed.  
Enter location to install Cisco Packet Tracer  
or press enter for default [/opt/pt]:
```

Практическая работа 1. Установка Cisco Packet Tracer

=====

9. Здесь система предлагает установить Cisco Packet Tracer в каталог `/opt/pt`, если устраивает, то нажмите Enter, если нет, введите путь к нужному каталогу и нажмите Enter. Пока идет процесс копирования файлов, можно видеть сообщение:

```
Installing into /opt/pt
Copied all files successfully to /opt/pt
```

Как только процесс завершится, в окне эмулятора терминала появится текст:

```
Should we create a symbolic link "packettracer" in /usr/local/bin for easy Cisco Packet Tracer startup? [Yn]
```

10. Здесь система установки предлагает создать ярлык приложения Packet Tracer в меню Ubuntu в разделе «Прочее». Введите символ Y и нажимайте Enter.

О том, что установка завершена, система сообщает выводом в терминал:

```
Type "packettracer" in a terminal to start
Cisco Packet Tracer
Writing PT7HOME environment variable to
/etc/profile
Writing QT_DEVICE_PIXEL_RATIO environment variable to /etc/profile
Cisco Packet Tracer 7.1 installed successfully
Please restart you computer for the Packet
Tracer settings to take effect
kirill@kirill-
vm:~/Загрузки/PacketTracer71_64bit_linux$
```

На этом, в принципе, заканчивается процесс установки Cisco Packet Tracer 7.1 на Ubuntu 16.04, но, скорее всего, у Вас возникнут трудности при запуске программы.

Практическая работа 1. Установка Cisco Packet Tracer

=====
11. Попробуйте запустить Cisco Packet Tracer, который установили на дистрибутив Ubuntu 16.04, для этого откройте терминал (Ctrl+Alt+T) и введите команду:

```
kirill@kirill-vm:~$ packettracer  
Starting Packet Tracer 7.1
```

Что делать, если Cisco Packet Tracer не запускается в Ubuntu?
Решение проблемы приведено в [29].

12. В терминале выполните действия:

```
kirill@kirill-vm:~$ cd /usr/local/bin/  
kirill@kirill-vm:/usr/local/bin$ ls  
packettracer  
kirill@kirill-vm:/usr/local/bin$ packettracer  
Starting Packet Tracer 7.1
```

13. Если Вы увидите последнюю строчку, то это означает, что Ваши действия к успеху не привели, и Packet Tracer не запущен. Тогда выполните последовательность команд:

```
kirill@kirill-vm:/usr/local/bin$ cd /opt/pt/  
kirill@kirill-vm:/opt/pt$ ls  
art extensions lib set_ptenv.sh tpl.linguist  
backgrounds help linguist set_qtenv.sh  
tpl.packettracer  
bin install packettracer Sounds  
eula.txt languages saves templates  
kirill@kirill-vm:/opt/pt$ ./packettracer  
Starting Packet Tracer 7.1
```

Судя по последней строке листинга, действия не увенчались успехом.

На многих русскоязычных сайтах этими рекомендациями ограничиваются, но проблема существует.

Практическая работа 1. Установка Cisco Packet Tracer

=====
14. Выполните команду:

```
kirill@kirill-vm:/opt/pt$  
/opt/pt/bin/./PacketTracer7  
/opt/pt/bin/./PacketTracer7: error while load-  
ing shared libraries: libQt5Script.so.5: cannot  
open shared object file: No such file or directory  
kirill@kirill-vm:/opt/pt$
```

Что-то не так с библиотекой, имя которой указано в предупре-
ждение (**libQt5Script.so.5**).

15. Можно попробовать так:

```
kirill@kirill-vm:/opt/pt/bin$ cd /opt/pt  
kirill@kirill-vm:/opt/pt$ cat packettracer  
#!/bin/bash  
echo Starting Packet Tracer 7.1  
PTDIR=/opt/pt  
export LD_LIBRARY_PATH=$PTDIR/lib  
pushd $PTDIR/bin > /dev/null  
./PacketTracer7 "$@" > /dev/null 2>&1  
popd > /dev/null  
kirill@kirill-vm:/opt/pt$
```

Здесь посмотрели содержимое файла **packettracer**, который находится в каталоге **/opt/pt**. И тут Вас должна заинтересовать стро-
ка: **export LD_LIBRARY_PATH=\$PTDIR/lib**.

Можно подумать, что проблема с библиотекой заключается в том, что Cisco Packet Tracer пытается ее найти в каталоге: **\$PTDIR/lib**, то есть это вот такой каталог: **/opt/pt/lib** и будто бы не находит там эту библиотеку.

16. Посмотрите содержимое каталога **/opt/pt/lib**:

Практическая работа 1. Установка Cisco Packet Tracer

```
=====
kirill@kirill-vm:/opt/pt/lib$ ls
libQt5Core.so libQt5ScriptTools.so
libQt5Core.so.5 libQt5ScriptTools.so.5
libQt5Core.so.5.5 libQt5ScriptTools.so.5.5
libQt5Core.so.5.5.1 libQt5ScriptTools.so.5.5.1
libQt5DBus.so libQt5Sensors.so
libQt5DBus.so.5 libQt5Sensors.so.5
libQt5DBus.so.5.5 libQt5Sensors.so.5.5
libQt5DBus.so.5.5.1 libQt5Sensors.so.5.5.1
libQt5Gui.so libQt5Sql.so
libQt5Gui.so.5 libQt5Sql.so.5
libQt5Gui.so.5.5 libQt5Sql.so.5.5
libQt5Gui.so.5.5.1 libQt5Sql.so.5.5.1
libQt5Multimedia.so libQt5Svg.so
libQt5Multimedia.so.5 libQt5Svg.so.5
libQt5Multimedia.so.5.5 libQt5Svg.so.5.5
libQt5Multimedia.so.5.5.1 libQt5Svg.so.5.5.1
libQt5MultimediaWidgets.so libQt5WebKit.so
libQt5MultimediaWidgets.so.5 libQt5WebKit.so.5
libQt5MultimediaWidgets.so.5.5
libQt5WebKit.so.5.5
libQt5MultimediaWidgets.so.5.5.1
libQt5WebKit.so.5.5.1
libQt5Network.so libQt5WebKitWidgets.so
libQt5Network.so.5 libQt5WebKitWidgets.so.5
libQt5Network.so.5.5
libQt5WebKitWidgets.so.5.5
libQt5Network.so.5.5.1
libQt5WebKitWidgets.so.5.5.1
libQt5Positioning.so libQt5Widgets.so
libQt5Positioning.so.5 libQt5Widgets.so.5
libQt5Positioning.so.5.5 libQt5Widgets.so.5.5
libQt5Positioning.so.5.5.1
libQt5Widgets.so.5.5.1
libQt5PrintSupport.so libQt5XcbQpa.so
```

Практическая работа 1. Установка Cisco Packet Tracer

```
=====
libQt5PrintSupport.so.5 libQt5XcbQpa.so.5
libQt5PrintSupport.so.5.5 libQt5XcbQpa.so.5.5
libQt5PrintSupport.so.5.5.1
libQt5XcbQpa.so.5.5.1
libQt5Script.so libQt5Xml.so
libQt5Script.so.5 libQt5Xml.so.5
libQt5Script.so.5.5 libQt5Xml.so.5.5
libQt5Script.so.5.5.1 libQt5Xml.so.5.5.1
kirill@kirill-vm:/opt/pt/lib$
```

В этом каталоге есть файл, который не может открыть Packet Tracer - `libQt5Script.so.5`. Видимо, с этим файлом что-то не так.

17. Измените путь, по которому Packet Tracer будет искать нужную библиотеку при запуске:

```
kirill@kirill-vm:~$
LD_LIBRARY_PATH=/opt/pt/lib
/opt/pt/bin/./PacketTracer7
/opt/pt/bin/./PacketTracer7: error while loading
shared libraries: libicui18n.so.52: cannot
open shared object file: No such file or directory
```

Но опять же, получаете ошибку и Packet Tracer не запускается.

18. Выполните поиск библиотеки, из-за которой возникли проблемы с запуском:

```
kirill@kirill-vm:/opt/pt$ sudo updatedb; locate libicui18n
/usr/lib/x86_64-linux-gnu/libicui18n.so.55
/usr/lib/x86_64-linux-gnu/libicui18n.so.55.1
kirill@kirill-vm:/opt/pt$
```

Практическая работа 1. Установка Cisco Packet Tracer

=====

Обратите внимание: на Ubuntu есть нужная библиотека для запуска Cisco Packet Tracer, но ее версия более новая, для СРТ7 требуется 52-я версия, а здесь установлена 55-я.

Чтобы Cisco Packet Tracer запустился, нужно установить более старую ее версию.

19. Выполните две команды:

```
kirill@kirill-vm:/opt/pt$ sudo wget
http://security.ubuntu.com/ubuntu/pool/main/i/icu/
libcui52_52.1-3ubuntu0.7_amd64.deb
kirill@kirill-vm:/opt/pt$ sudo dpkg -i li-
bui52_52.1-3ubuntu0.7_amd64.deb
```

20. Проверьте факт установки:

```
kirill@kirill-vm:/opt/pt$ sudo updatedb; lo-
cate libcui18n
/usr/lib/x86_64-linux-gnu/libcui18n.so.52
/usr/lib/x86_64-linux-gnu/libcui18n.so.52.1
/usr/lib/x86_64-linux-gnu/libcui18n.so.55
/usr/lib/x86_64-linux-gnu/libcui18n.so.55.1
kirill@kirill-vm:/opt/pt$
```

Все, теперь есть обе версии библиотеки и можно смело запускать **Cisco Packet Tracer 7.1** на **Ubuntu 16.04**.

21. Выполните это командой **packettracer** (рисунок 1.10).

Cisco Packet Tracer запустился, нужно теперь зарегистрировать приложение.

Практическая работа 1. Установка Cisco Packet Tracer

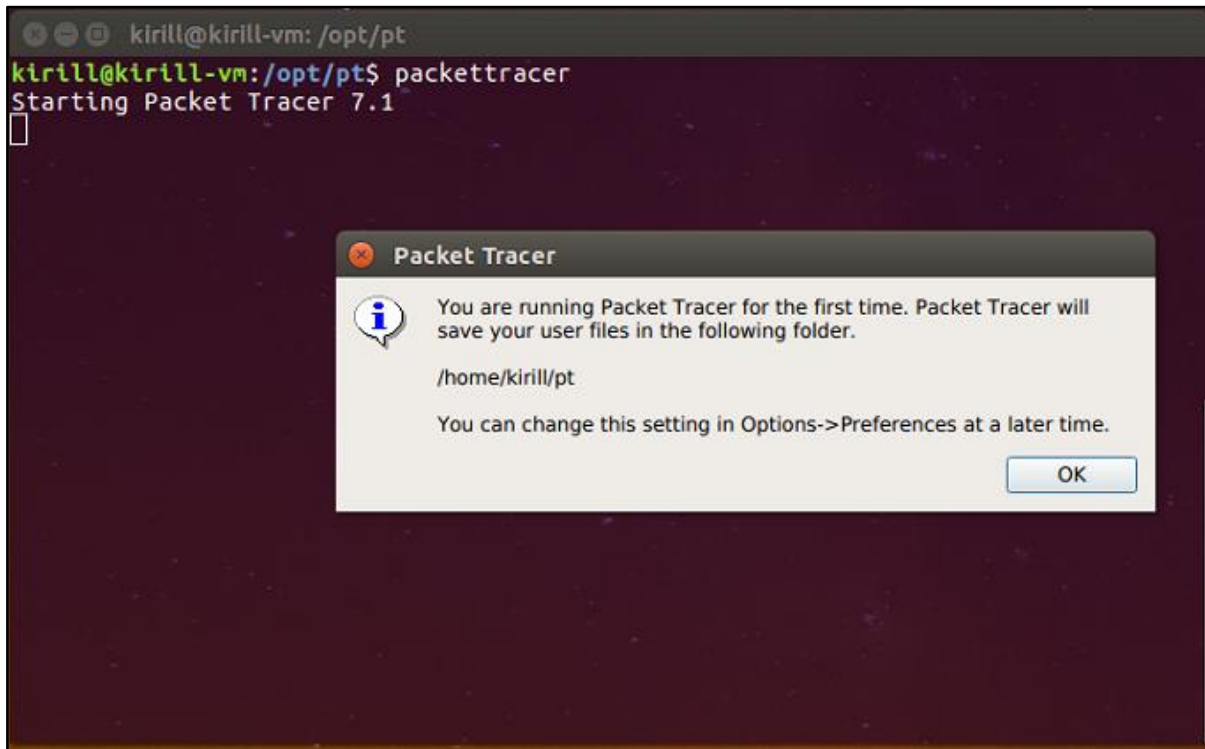


Рисунок 1.10 - Cisco Packet Tracer успешно запущен

Регистрация Cisco Packet Tracer

22. Зарегистрировать Cisco Packet Tracer просто: при первом запуске в форму, показанную на рисунке 1.11, нужно ввести e-mail и пароль, который использовали для регистрации на сайте академии Cisco.

Рисунок 1.12 демонстрирует, что Cisco Packet Tracer зарегистрирован и успешно запущен на Ubuntu 16.04.

Практическая работа 1. Установка Cisco Packet Tracer

Вход в учетную запись Сетевой академии Cisco

Логин или email

Пароль

[Забыли пароль?](#)
[Отправить ссылку активации еще раз](#)
[Применить токен класса](#)

Заявление о конфиденциальности
Товарные знаки
Использование Cookie
Cisco.com

Русский

Рисунок 1.11 - Регистрируем свою копию Cisco Packet Tracer



Рисунок 1.12 - Cisco Packet Tracer зарегистрирован и запущен

Практическая работа 1. Установка Cisco Packet Tracer

Упражнение 1.3 Установка Cisco Packet Tracer 7.3.0 на дистрибутив Linux Ubuntu 19.10 [27]

Следующие новые механизмы в Cisco Packet Tracer 7.3.0 расширяют возможности моделирования:

- поддержка пакета CCNA 7;
- новая тема (оформление);
- возможность управления позиционированием объектов (устройств) в рабочей области;
- возможность развертывания сетевых устройств в определенной стойке;
- обновлена поддержка новых устройств;
- возможность переименования стойки.

Доработаны протоколы:

- IP OSPF точка-точка на интерфейсе Ethernet;
- IPv6 OSPF точка-точка на интерфейсе Ethernet;
- динамическая проверка ARP;
- WLC GUI исправления и улучшения;
- исправления и улучшения отслеживания DHCP;
- модификатор вывода раздела для команд **show**;
- улучшения доступности, безопасности и удобства использования и оптимизации для всех платформ;
- модернизированная поддержка PTSA и PTMO;
- различные улучшения существующих протоколов.

Новые устройства в Packet Tracer 7.3.0:

- маршрутизатор с интегрированными сервисами Cisco 4331;
- контроллер беспроводной локальной сети Cisco 3504.

Установка Cisco Packet Tracer 7.3.0

1. Скачайте пакет Cisco Packet Tracer 7.3.0. Перейдите в домашнюю директорию в папку Загрузки и выполните в терминале следующие команды:

Практическая работа 1. Установка Cisco Packet Tracer

```
=====
cd ~/Загрузки/
sudo chmod a+x PacketTracer_730_amd64.deb
sudo dpkg -i PacketTracer_730_amd64.deb
cd /tmp && wget
http://ftp.br.debian.org/debian/pool/main/d/double-
-conversion/libdouble-conversion1_3.1.0-
3_amd64.deb &&
http://ftp.br.debian.org/debian/pool/main/q/qt-at-
spi/qt-at-spi_0.4.0-9_amd64.deb &&
http://archive.ubuntu.com/ubuntu/pool/main/libj/li
bjpeg-turbo/libjpeg-turbo8_2.0.3-
0ubuntu1_amd64.deb &&
http://archive.ubuntu.com/ubuntu/pool/main/libj/li
bjpeg8-empty/libjpeg8_8c-2ubuntu8_amd64.deb &&
chmod a+x *.deb && sudo dpkg -i *.deb
```

При установке пакета PacketTracer_730_amd64.deb у Вас запросят дать согласие на установку, кликните по клавише Tab и нажмите ОК (рисунок 1.13).

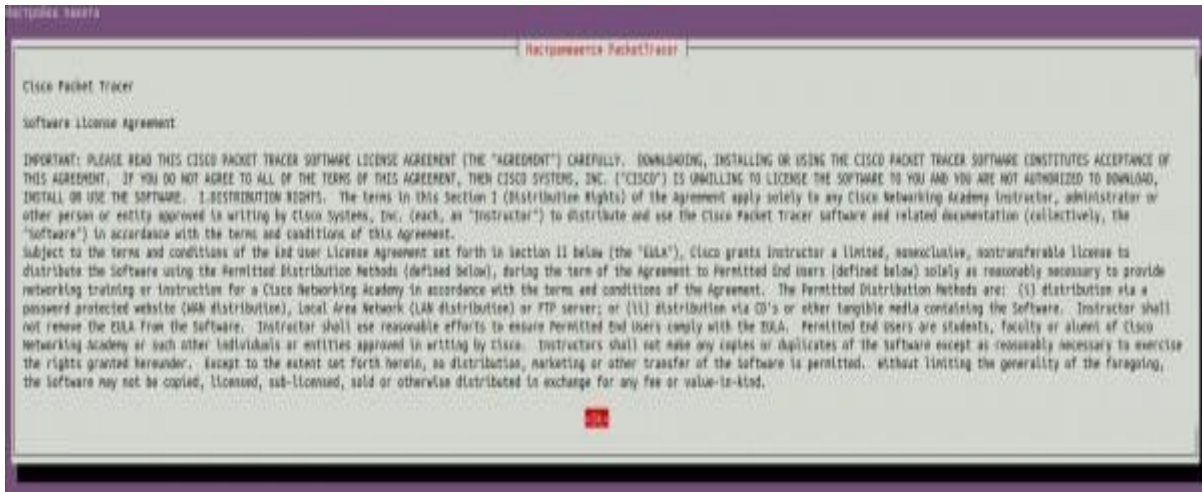


Рисунок 1.13 - Соглашение на установку

После аналогично соглашаемся с установкой выбирая пункт "Да".

Практическая работа 1. Установка Cisco Packet Tracer

2. В том случае если при попытке установки установщик будет писать ошибку «невозможности скачать пакет» (**qt-at-spi_0.4.0-9_amd64.deb**), тогда каждый по отдельности скачайте в папку загрузки, после просто с терминала перейдите в папку загрузки:

```
cd ~/Загрузки/  
sudo chmod a+x *.deb  
sudo dpkg -i *.deb  
sudo apt -f install
```

После установки вы сможете запустить Cisco Packet Tracer 7.3.0 (рисунок 1.14).

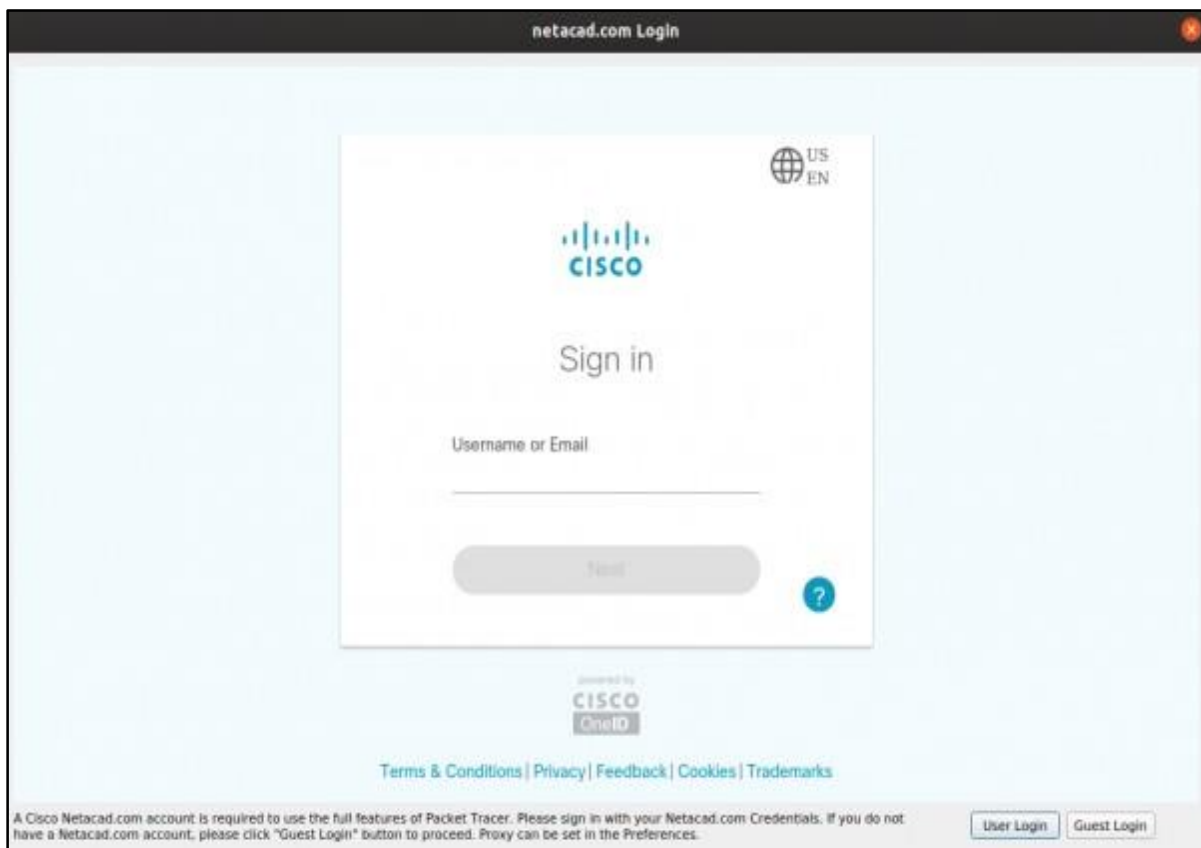


Рисунок 1.14 – Запуск Cisco Packet Tracer 7.3.0

Практическая работа 1. Установка Cisco Packet Tracer

3. При первом запуске Вас попросят авторизоваться с помощью своей учетной записи **netcad**. Авторизуйтесь и работайте в приложении.

Можно авторизоваться гостем в данном приложении, нажав на кнопку Guest Login. Через 15 секунд приложение Вас пустит, просто подтвердите вход нажав на кнопку Confirm Guest (рисунок 1.15).

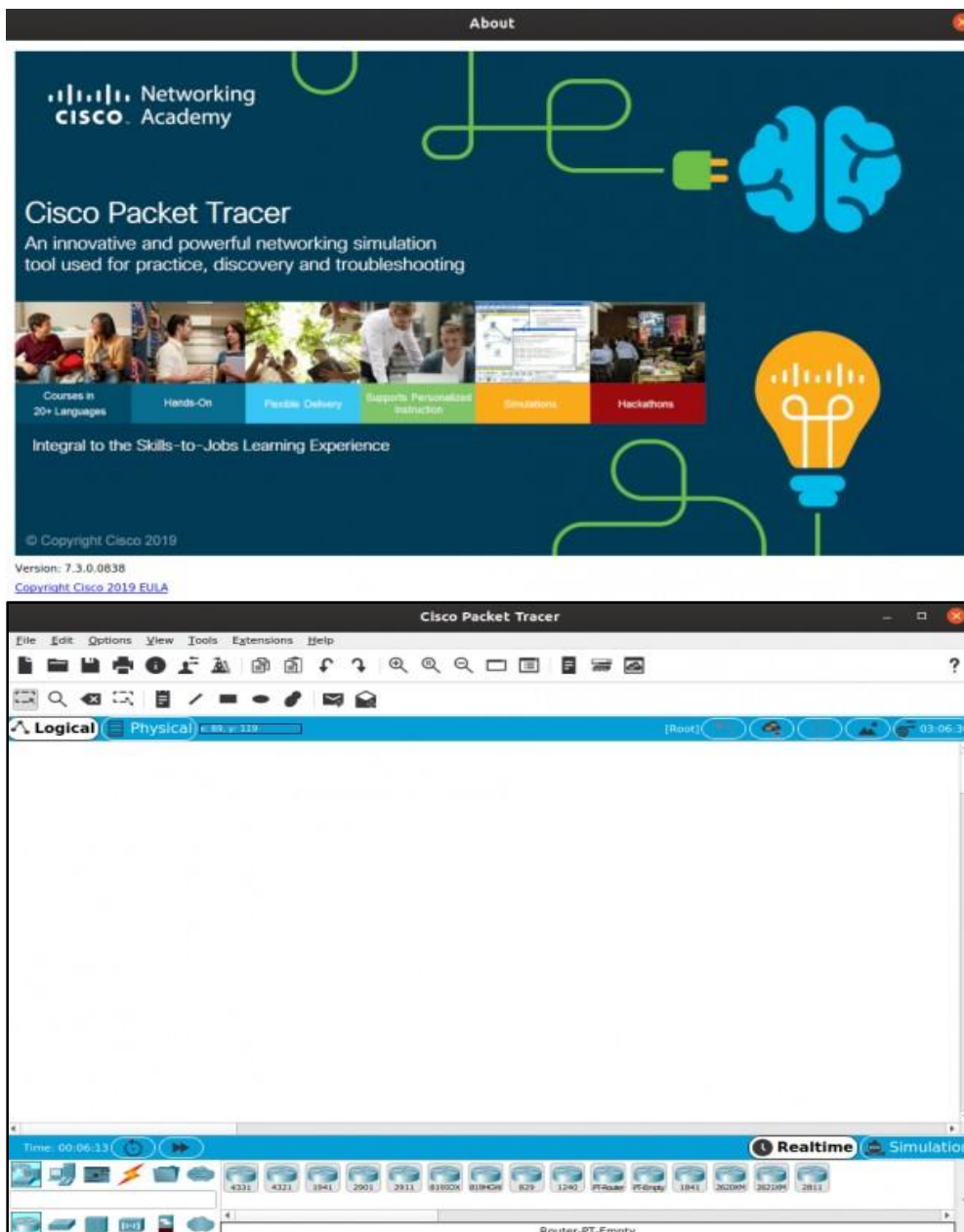


Рисунок 1.15 – Cisco Packet Tracer зарегистрирован и запущен

Практическая работа 1. Установка Cisco Packet Tracer

Контрольные вопросы

1. Каким образом можно скачать Cisco Packet Tracer?
2. Как создать аккаунт на сайте академии Cisco?
3. Что представляет собой личный кабинет пользователя Cisco?
4. Прокомментируйте особенности установки Cisco Packet Tracer 7.1 на Windows 10.
5. Как поступить если Firewall Вашего компьютера выдает сообщение о неизвестном приложении при установке Cisco Packet Tracer.
6. Прокомментируйте особенности установки Cisco Packet Tracer 7.1 на дистрибутив Linux Ubuntu 16.04.
7. Как зарегистрировать Вашу копию Cisco Packet Tracer?
8. Прокомментируйте особенности установки Cisco Packet Tracer 7.3.0 на дистрибутив Linux Ubuntu 19.10.

Задание

Выполните на своем компьютере все упражнения. Отчет должен содержать скриншоты с экрана вашего компьютера, позволяющие судить о том, что основные результаты последовательного выполнения упражнений выполнены корректно и в надлежащей последовательности.

Практическая работа 2. НАЧАЛЬНЫЕ СВЕДЕНИЯ ОБ ИСПОЛЬЗОВАНИИ ПРОГРАММЫ CISCO PACKET TRACER

Цель работы – приобретение начальных практических навыков обучающимися в использовании программы Cisco Packet Tracer, включая построение сети из двух компьютеров и сети из нескольких компьютеров с заданной топологией.

Порядок выполнения работы – внимательно изучите методический материал, выполните все упражнения, включённые в данный раздел в пошаговом режиме. Если в промежуточных точках изображения ваших моделей не совпадает с приводимыми в практикуме, вернитесь на 2-3 шага назад и все-таки добейтесь абсолютного соответствия. Самостоятельно выполните задание к практической работе.

2.1. Краткие сведения

Интерфейс программы Cisco Packet Tracer [1, 2, 8, 16, 19, 20]

Для запуска Cisco Packet Tracer необходимо вызвать исполняемый файл PacketTracer.exe. Общий вид программы можно увидеть на рисунке 2.1.

Рабочая область окна программы состоит из следующих элементов:

1. Menu Bar - панель, которая содержит меню File, Edit, Options, View, Tools, Extensions, Help.

2. Main Tool Bar содержит графические изображения ярлыков для доступа к командам меню File, Edit, View и Tools, а также кнопку Network Information.

3. Common Tools Bar - панель, которая обеспечивает доступ к наиболее используемым инструментам программы: Select, Move Layout, Place Note, Delete, Inspect, Add Simple PDU и Add Complex PDU.

4. Logical/Physical Workspace and Navigation Bar - Панель, которая дает возможность переключать рабочую область: физическую или

Практическая работа 2. Начальные сведения

логическую, а также позволяет перемещаться между уровнями кластера.

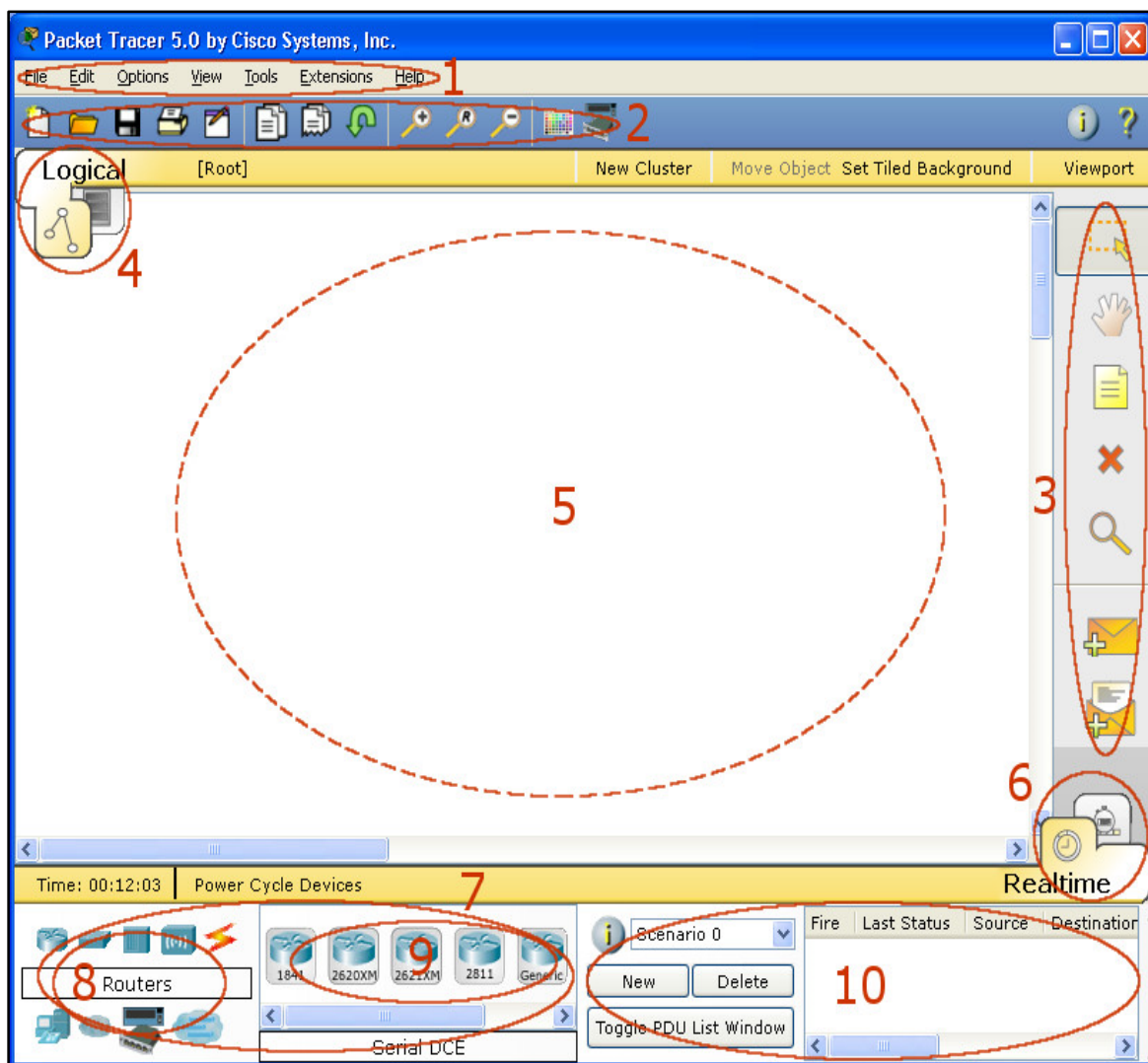


Рисунок 2.1 - Общий вид программы Cisco Packet Tracer

5. Workspace - область, в которой происходит создание сети, проводятся наблюдения за симуляцией и просматривается разная информация и статистика.

6. Realtime/Simulation Bar - с помощью закладок этой панели можно переключаться между режимом Realtime и режимом Simulation. Она также содержит кнопки, относящиеся к Power Cycle Devices, кнопки Play Control и переключатель Event List в режиме Simulation.

Практическая работа 2. Начальные сведения

7. Network Component Box - это область, в которой выбираются устройства и связи для размещения их на рабочем пространстве. Она содержит область Device-Type Selection и область Device-Specific Selection.

8. Device-Type Selection Box - эта область содержит доступные типы устройств и связей в Packet Tracer. Область Device-Specific Selection изменяется в зависимости от выбранного устройства

9. Device-Specific Selection Box - эта область используется для выбора конкретных устройств и соединений, необходимых для постройки в рабочем пространстве сети.

10. User Created Packet Window - это окно управляет пакетами, которые были созданы в сети во время симуляции сценария.


Главное меню показано на рисунке 2.2.



File Edit Options View Tools Extensions Help

Рисунок 2.2 - Главное меню интерфейса программы Cisco Packet Tracer

Главное меню содержит следующие пункты:

- File (Файл) – содержит операции открытия/сохранения документов;
- Edit (Правка) – содержит стандартные операции «копировать/вырезать, отменить/повторить»;
- Options (Настройки) – содержит настройки программы. В частности, здесь расположена кнопка , позволяющая производить локализацию программы на другие языки;
- View (Вид) - содержит инструменты изменения масштаба рабочей области и панели инструментов;
- Tools (Инструменты) - содержит цветовую палитру и окно пользовательских устройств;
- Exensions (Расширения) - содержит мастер проектов и ряд других инструментов;
- Help (Помощь) - содержит помощь по программе.

Практическая работа 2. Начальные сведения

Панель инструментов

Вид панели инструментов приведен на рисунке 2.3.



Рисунок 2.3 - Панель инструментов

Панель инструментов с помощью пиктограмм дублирует основные пункты главного меню программы.

Оборудование

Снизу, под рабочей областью, расположена панель оборудования. Данная панель содержит в своей левой части типы (классы) устройств, а в правой части – их наименование (модели). При наведении на каждое из устройств, в прямоугольнике, находящемся в центре между ними будет отображаться его тип. Типы оборудования представлены на рисунке 2.4.



Рисунок 2.4 - Панель оборудования Cisco Packet Tracer (Основные типы оборудования)

Основные типы оборудования:

- *маршрутизаторы* (роутеры) - используется для поиска оптимального маршрута передачи данных на основании специальных алгоритмов маршрутизации, например, выбор маршрута (пути) с наименьшим числом транзитных узлов. Работают на сетевом уровне модели OSI (рисунок 2.5);

Практическая работа 2. Начальные сведения



Рисунок 2.5 - Маршрутизатор (роутер)

- коммутаторы (рисунок_2.6) - устройства, предназначенные для объединения нескольких узлов в пределах одного или нескольких сегментах сети. Коммутатор (свитч) передаёт пакеты информации на основании таблицы коммутации, поэтому трафик идёт только на тот MAC-адрес, которому он предназначен, а не повторяется на всех портах, как на концентраторе (хабе);



Рисунок 2.6 – Коммутаторы

- концентраторы (рисунок 2.7). Концентратор повторяет пакет, принятый на одном порту на всех остальных портах.

Практическая работа 2. Начальные сведения



Рисунок 2.7 – Концентраторы

- *беспроводные устройства* (рисунок 2.8). Беспроводные технологии Wi-Fi и сети на их основе. Включает в себя точки доступа;



Рисунок 2.8 – Беспроводные устройства

- среди *конечных устройств* (рисунок 2.9) представлены персональный компьютер, ноутбук, сервер, принтер, телефоны и так далее;

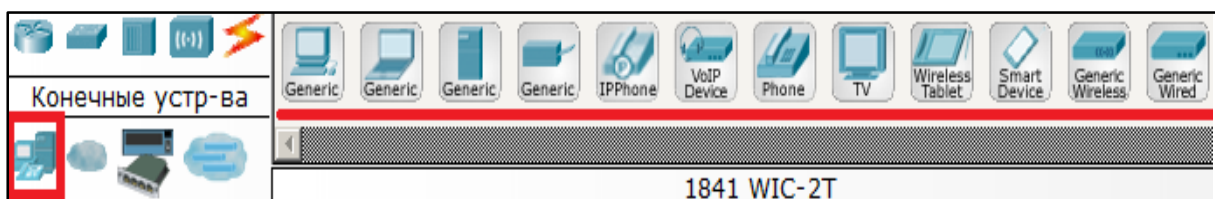


Рисунок 2.9 - Конечные устройства

- *Интернет* (рисунок 2.10) в программе представлен в виде облаков и модемов DSL.

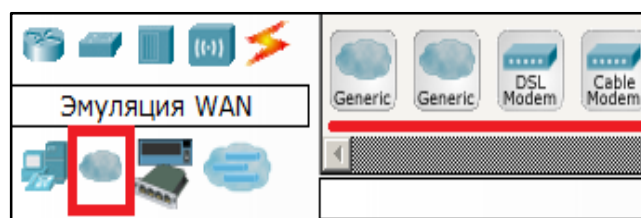


Рисунок 2.10 - Интернет

Практическая работа 2. Начальные сведения

Пользовательские устройства и облако для многопользовательской работы показаны на рисунке 2.11.



Рисунок 2.11 - Пользовательские устройства и облако для многопользовательской работы

Линии связи

С помощью линий связи создаются соединения узлов сети в единую топологию и при этом каждый тип кабеля может быть соединен лишь с определенными типами интерфейсов устройств (рисунок 2.12).






Рисунок 2.12 – Кнопки типов линий связи

С помощью этих компонентов создаются соединения узлов в единую схему.

Каждый тип кабеля может быть соединен лишь с определенными типами интерфейсов (см. таблицу).





Практическая работа 2. Начальные сведения

Типы кабелей

Тип кабеля	Описание
<p>Консоль</p> 	<p>Консольное соединение может быть выполнено между ПК и маршрутизаторами или коммутаторами. Должны быть выполнены некоторые требования для работы консольного сеанса с ПК: скорость соединения с обеих сторон должна быть одинаковой, должно быть 7 бит данных (или 8 бит) для обеих сторон, контроль четности должен быть одинаковый, должно быть 1 или 2 стоповых бита (но они не обязательно должны быть одинаковыми), а поток данных может быть чем угодно для обеих сторон.</p>
<p>Медный прямой</p> 	<p>Соединение медным кабелем типа <i>витая пара</i>, оба конца кабеля обжаты в одинаковой раскладке. Этот тип кабеля является стандартной средой передачи Ethernet для соединения устройств, который функционирует на разных уровнях OSI. Он должен быть соединен со следующими типами портов: медный 10 Мбит/с (Ethernet), медный 100 Мбит/с (Fast Ethernet) и медный 1000 Мбит/с (Gigabit Ethernet).</p>
<p>Медный кроссовер</p> 	<p>Этот тип кабеля является средой передачи Ethernet для соединения устройств, которые функционируют на одинаковых уровнях OSI. Он может быть соединен со следующими типами портов: медный 10 Мбит/с (Ethernet), медный 100 Мбит/с (Fast Ethernet) и медный 1000 Мбит/с (Gigabit Ethernet)</p>

Практическая работа 2. Начальные сведения

Окончание

<p>Телефонный кабель</p> 	<p>Соединение через телефонную линию может быть осуществлено только между устройствами, имеющими модемные порты. Стандартное представление модемного соединения - это конечное устройство (например, ПК), дозванивающееся в сетевое облако.</p>
<p>Коаксиальный кабель</p> 	<p>Соединение устройств с помощью коаксиального кабеля. Коаксиальная среда используется для соединения между коаксиальными портами, такие как кабельный модем, соединенный с облаком Packet Tracer.</p>
<p>Серийный DCE</p>  <p>Серийный DTE</p> 	<p>Соединения через последовательные порты, часто используются для связей WAN. Для настройки таких соединений необходимо установить синхронизацию на стороне DCE-устройства. Синхронизация DTE выполняется по выбору. Сторону DCE можно определить по маленькой иконке “часов” рядом с портом. При выборе типа соединения Serial DCE, первое устройство, к которому применяется соединение, становится DCE-устройством, а второе - автоматически станет стороной DTE. Возможно и обратное расположение сторон, если выбран тип соединения Serial DTE.</p>

Графическое меню

На рисунке 2.13 показано графическое меню программы.



Рисунок 2.13 - Графическое меню (повернуто)

Практическая работа 2. Начальные сведения

На этом рисунке показаны пиктограммы следующих инструментов (слева направо):

- Select (Выбрать) можно активировать клавишей Esc. Он используется для выделения одного или более объектов для дальнейшего их перемещения, копирования или удаления;
- Move Layout (Переместить слой, горячая клавиша M) используется для прокрутки больших проектов сетей;
- Place Note (Сделать пометку, горячая клавиша N) добавляет текст в рабочей области проекта;
- Delete (Удалить, клавиша Del) удаляет выделенный объект или группу объектов;
- Inspect (Проверка, клавиша I) позволяет, в зависимости от типа устройства, просматривать содержимое таблиц (ARP, NAT, таблицы маршрутизации);
- Drawapolygon (Нарисовать многоугольник) позволяет рисовать прямоугольники, эллипсы, линии и закрашивать их цветом;
- Resize Shape (Изменить размер формы, комбинация клавиш Alt+R) предназначен для изменения размеров нарисованных объектов (четыреугольников и окружностей).

Элементы анимации и симуляции

Эти элементы интерфейса показаны на рисунке 2.14.



Рисунок 2.14 - Элементы анимации и симуляции

Инструменты Add Simple PDU (Добавить простой PDU, клавиша P) и Add Complex PDU (Добавить комплексный PDU, клавиша C) предназначены для эмуляции отправки пакета с последующим отслеживанием его маршрута и данных внутри пакета.

Практическая работа 2. Начальные сведения

Физическое представление оборудования персонального компьютера

В программе возможно физическое представление оборудования персонального компьютера в виде его физической конфигурации (рисунок 2.15).



Рисунок 2.15 - Физическая конфигурация персонального компьютера

Для изменения комплектации оборудования персонального компьютера необходимо отключить его питание, кликнув мышью на кнопке питания и перетащить мышью нужный модуль в свободный слот, затем включить питание. В качестве примера показано добавление в физическую конфигурацию персонального компьютера

Практическая работа 2. Начальные сведения

микрофона (PT-MICROPHONE), в результате чего персональный компьютер изменил свой значок в программе (рисунок 2.16).

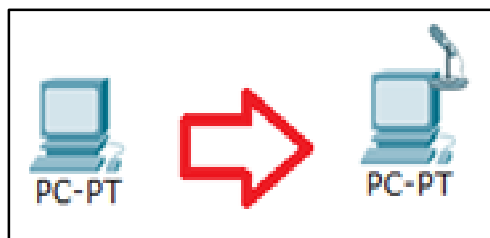


Рисунок 2.16 - Изменение пиктограммы персонального компьютера после подключения к нему микрофона

Остальные модули добавляются в устройства аналогично. Так, на персональный компьютер есть возможность добавить не только микрофон, но и, например, наушники или жесткий диск для хранения данных.

Физическая комплектация оборудования

Установите в рабочем поле роутер Cisco 1841. В настройках на роутере открываем его физическую конфигурацию (рисунок 2.17).

Слева - список модулей (цифра 2), которыми можно укомплектовать данный роутер. Сейчас в нем 2 пустоты (цифра 3). В них можно вложить эти модули. Разумеется, эту операцию нужно производить при выключенном питании (цифра 1).

Модули WIC (HWIC, VWIC) это платы расширения, увеличивающие функционал устройства:

1. WIC - WAN interface card, the first original models.
2. HWIC- high-speed wan interface card- the evolution of wic that is now in use on the ISR routers.
3. VIC - voice interface card, support voice only.
4. VIC2 - evolution of the above
5. VWIC - voice and wan interface card. An E1/T1 card that can be user for voice or data.
6. VWIC2 - evolution of the above.

Практическая работа 2. Начальные сведения

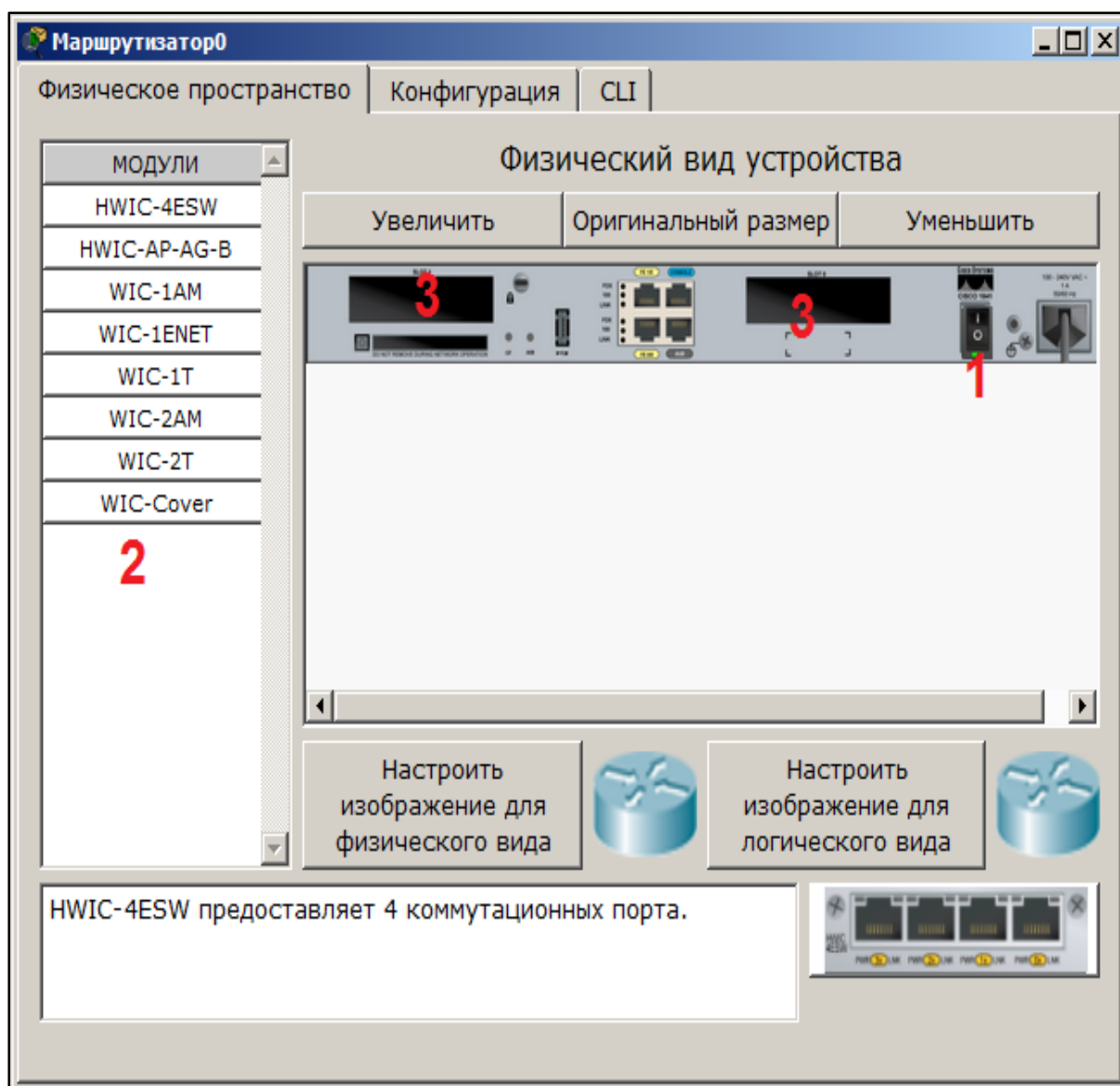


Рисунок 2.17 - Физическая конфигурация устройства

Например, для компьютера есть платы, подключаемые к PCI-шине (TV-тюнеры, звуковые карты, USB-разветвители, сетевые карты), так и здесь. Вообще, устройство Cisco - это тот же системный блок со своей операционкой и многими сетевыми картами, который может делать что-то только с сетью.

Ниже предствалена информация о каждом модуле:

- HWIC - 4ESW - высокопроизводительный модуль с четырьмя коммутационными портами Ethernet под разъем RJ-45. Позволяет сочетать в маршрутизаторе возможности коммутатора;

Практическая работа 2. Начальные сведения

- HWIC-AP-AG-B - это высокоскоростная WAN-карта, обеспечивающая функционал встроенной точки доступа для роутеров линейки Cisco 1800 (модульных), Cisco 2800 и Cisco 3800. Данный модуль поддерживает радиоканалы Single Band 802.11b/g или Dual Band 802.11a/b/g;

- WIC-1AM включает в себя два разъема RJ-11 (телефонка), используемых для подключения к базовой телефонной службе. Карта использует один порт для соединения с телефонной линией, другой может быть подключен к аналоговому телефону для звонков во время простоя модема;

- WIC-1ENET - это однопортовая 10 Мб/с Ethernet карта для 10BASE-T Ethernet LAN;

- WIC-1T предоставляет однопортовое последовательное подключение к удаленным офисам или устаревшим серийным сетевым устройствам, например, SDLC концентраторам, системам сигнализации и устройствам packet over SONET (POS);

- WIC-2AM содержит два разъема RJ-11, используемых для подключения к базовой телефонной службе. В WIC-2AM два модемных порта, что позволяет использовать оба канала для соединения одновременно;

- WIC-2T - 2-портовый синхронный/асинхронный серийный сетевой модуль предоставляет гибкую поддержку многих протоколов с индивидуальной настройкой каждого порта в синхронный или асинхронный режим. Применения для синхронной/асинхронной поддержки представляют:

- низкоскоростную агрегацию (до 128 Кб/с);

- поддержку dial-up модемов;

- синхронные или асинхронные соединения с портами управления другого оборудования и передачу устаревших протоколов типа Bi-sync и SDLC.

- WIC-Cover - стенка для WIC слота, необходима для защиты электронных компонентов и для улучшения циркуляции охлаждающего воздушного потока.

Для изменения комплектации оборудования необходимо:

отключить питание, кликнув мышью на кнопке питания, перетащить мышью модуль 4ESW в свободный слот и включить питание.

Практическая работа 2. Начальные сведения

Подождать окончания загрузки роутера. В конфигурации GUI можем увидеть появившиеся 4 новых интерфейса (рисунок 2.18).

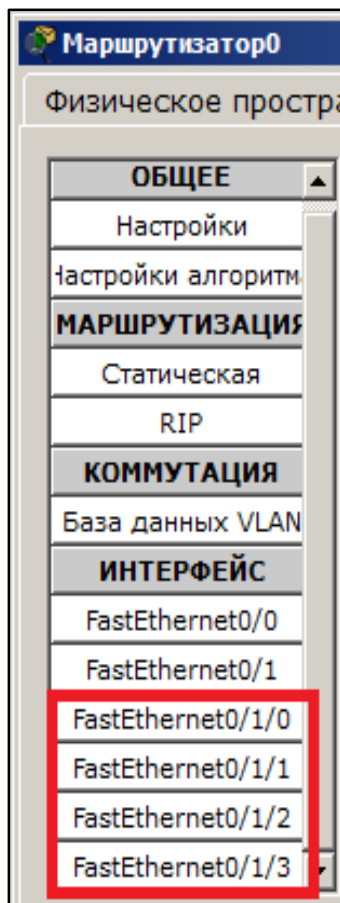


Рисунок 2.18 - Конфигурация интерфейсов устройства

Остальные устройства комплектуются аналогично. Добавляются новые модули Ethernet (10/100/1000), оптоволоконные разъемы нескольких типов, адаптеры беспроводной сети. На рабочий компьютер есть возможность добавить, например, микрофон с наушниками, жесткий диск для хранения данных.

Практическая работа 2. Начальные сведения

2.2. Практические упражнения

Упражнение 2.1. Топологическая модель локальной сети между двумя компьютерами

Разберем как настроить локальную сеть между двумя компьютерами. Это базовая ситуация, в которую попадает начинающий системный администратор.

1. Откройте Cisco Packet Tracer, выберите End Devices и «перетащите» в рабочую область два компьютера Generic (рисунок 2.19).

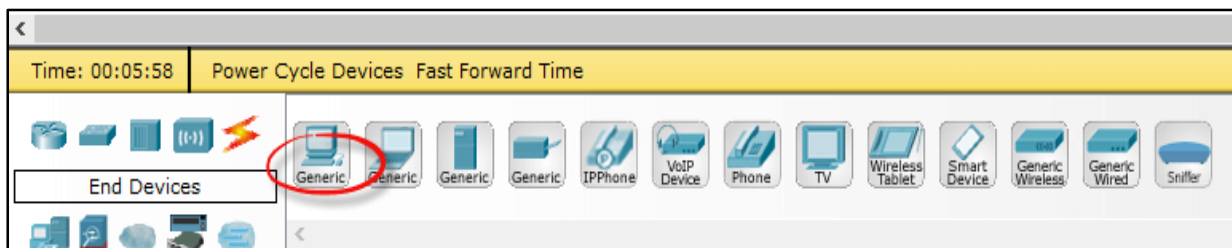


Рисунок 2.19 - выберите End Devices и «перетащите» в рабочую область два компьютера Generic

В итоге на рабочем поле приложения получаем картину (рисунок 2.20).

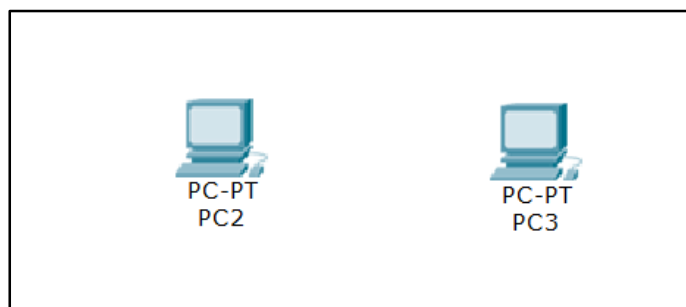


Рисунок 2.20 - Два компьютера в рабочей области

2. Соедините два компьютера пат кордом. Для этого необходимо выбрать Connections и перекрестный кабель (рисунок 2.21).

Практическая работа 2. Начальные сведения



Рисунок 2.21 - Выбрать Connections и перекрестный кабель

3. Кликните по первому компьютеру и подключите пат корд к FastEthernet0. В итоге на рабочем поле приложения должна получиться следующая картина (рисунок 2.22).

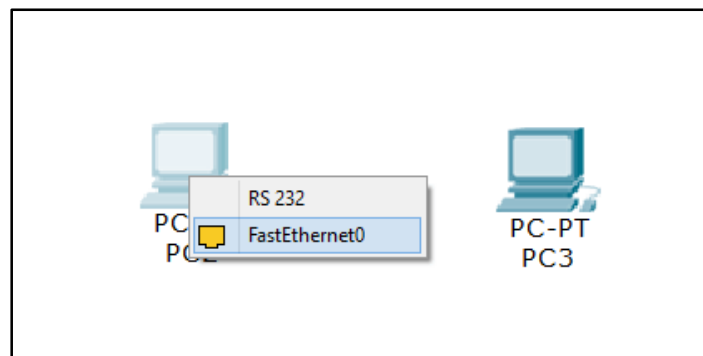


Рисунок 2.22 - Паткорд первого компьютера подключен к FastEthernet0

4. «Перетащите» связь на второй компьютер и выберите тоже FastEthernet0 (рисунок 2.23).

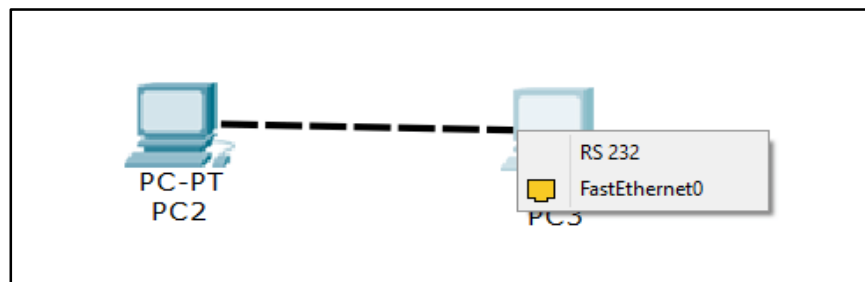


Рисунок 2.23 - Второй компьютер подключен

В итоге на рабочем поле приложения должны загореться зеленые лампочки, это означает, что локальная сеть между компьютерами заработала (рисунок 2.24).

Практическая работа 2. Начальные сведения

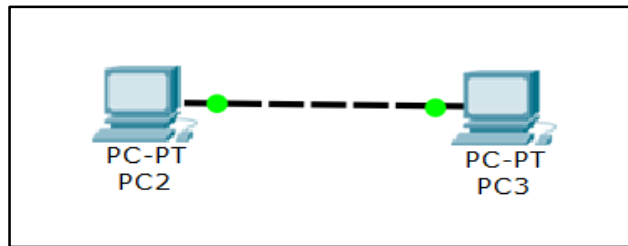


Рисунок 2.24 - Загорелись зеленые лампочки, это означает, что локальная сеть между компьютерами заработала

5. Настроить статический IP-адрес у компьютера, для этого щелкните по первому двойным кликом. Перешли в меню Desktop, далее необходимо выбирать IP Configuration (рисунок 2.25).

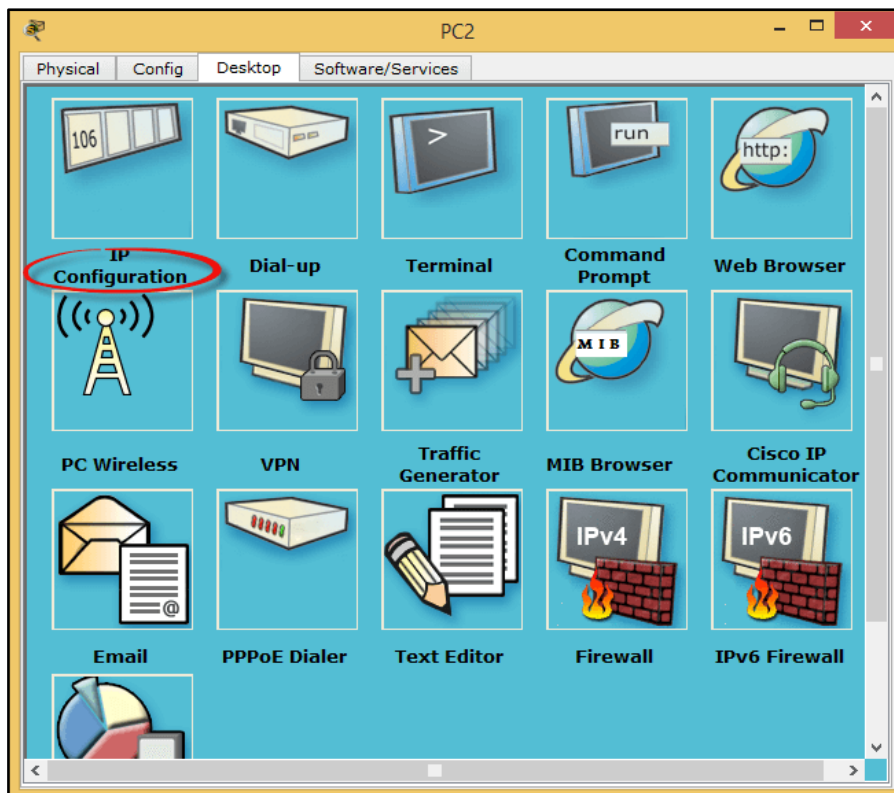


Рисунок 2.25 - Выбрать IP Configuration

6. Задать IP адрес и маску, пусть это будет 192.168.1.1, маска подсети 255.255.255.0. В итоге на рабочем поле приложения должна получиться следующая картина (рисунок 2.26).

Практическая работа 2. Начальные сведения

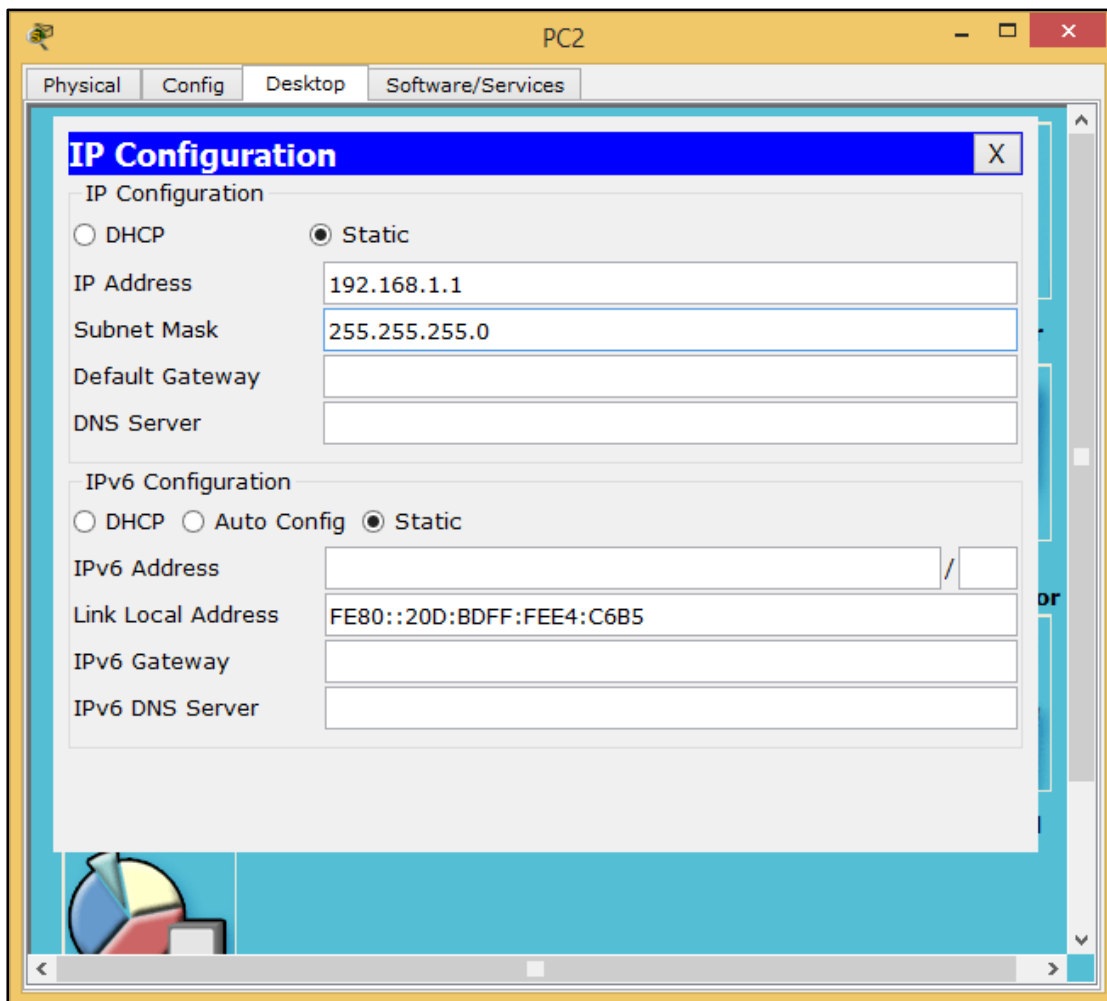


Рисунок 2.26 – Поля задания IP адреса и маски подсети

7. На втором компьютере сделайте тоже самое, но задать IP адрес 192.168.1.2.

8. Проверьте наличие связи между компьютерами и убедитесь, что они «видят» друг друга. Для этого на вкладке **Desktop** (Рабочий стол) перейдите в поле **run** (Командная строка) и пропингуйте соседний компьютер (рисунок 2.27).

Практическая работа 2. Начальные сведения

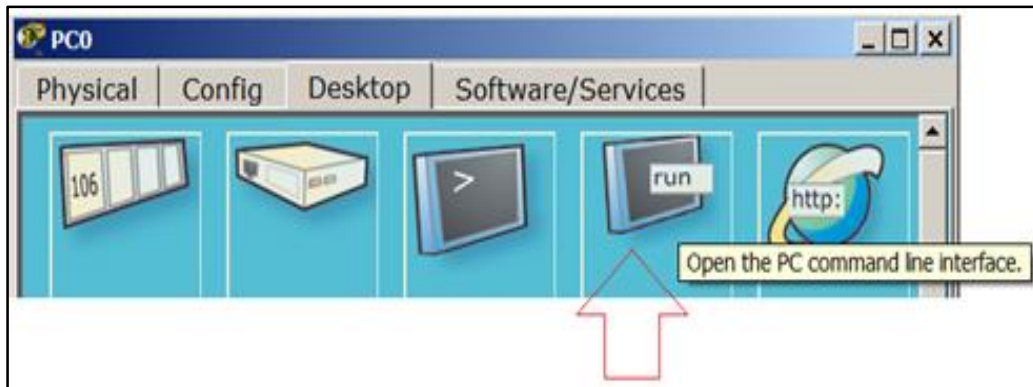


Рисунок 2.27 – Поля для «пропинговки» соседнего компьютера

Как видно из рисунка 2.28 связь между компьютерами присутствует (настроена).

```
Packet Tracer PC Command Line 1.0
PC>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Reply from 192.168.1.2: bytes=32 time=62ms TTL=128
Reply from 192.168.1.2: bytes=32 time=32ms TTL=128
Reply from 192.168.1.2: bytes=32 time=31ms TTL=128
Reply from 192.168.1.2: bytes=32 time=32ms TTL=128

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 31ms, Maximum = 62ms, Average = 39ms

PC>
```

Рисунок 2.28 - Связь между компьютерами присутствует

Практическая работа 2. Начальные сведения

Упражнение 2.2. Построение сети из нескольких компьютеров с заданной топологией

Рассмотрим создание в Cisco Packet Tracer локальной вычислительной сети из нескольких компьютеров с заданной топологией, сеть представлена на рисунке 2.29.

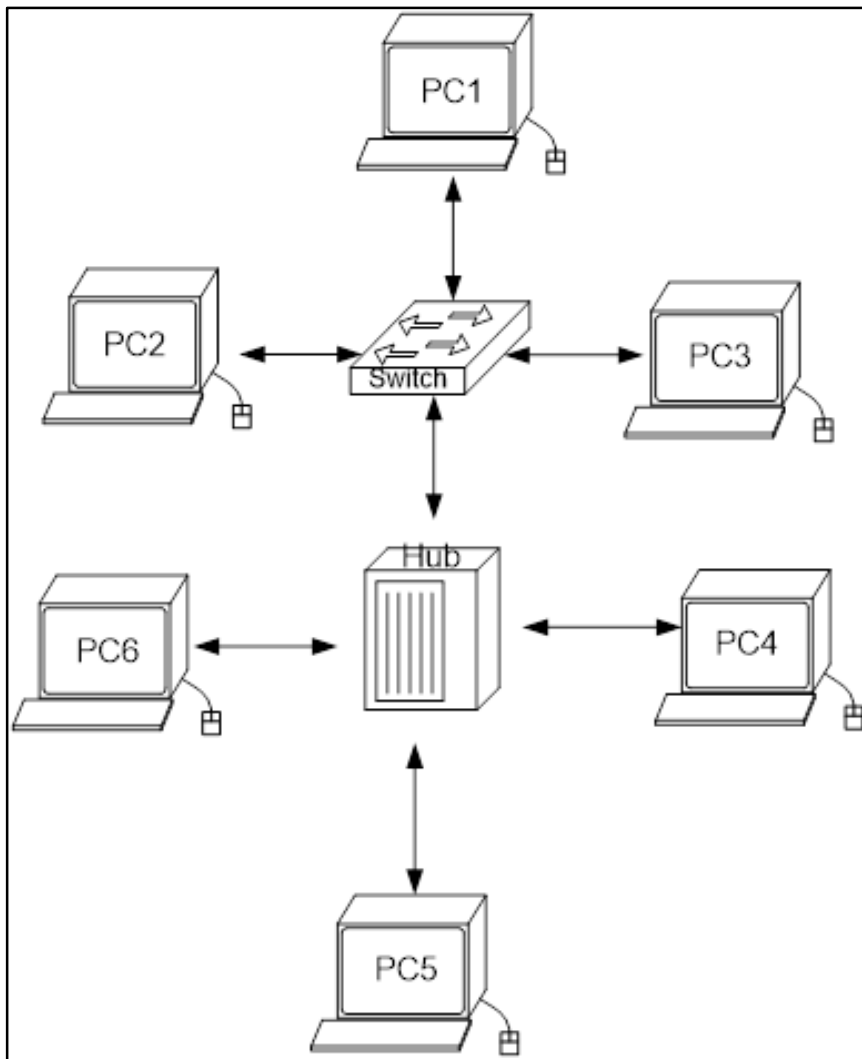


Рисунок 2.29 – Заданная топология сети

Локальная вычислительная сеть – это компьютерная сеть, покрывающая обычно относительно небольшую территорию или небольшую группу зданий. В нашем случае это всего-навсего 6 рабочих

Практическая работа 2. Начальные сведения

станций, определенным образом связанных между собой. Для этого используются сетевые концентраторы (хабы) и коммутаторы (свичи).

1. В нижнем левом углу Cisco Packet Tracer необходимо выбрать устройства «Сетевые коммутаторы», в списке справа, выберите коммутатор 2950-24, нажимая на него левой кнопкой мыши, вставьте его в рабочую область. В итоге на рабочем поле приложения должна получиться следующая картина (рисунок 2.30).

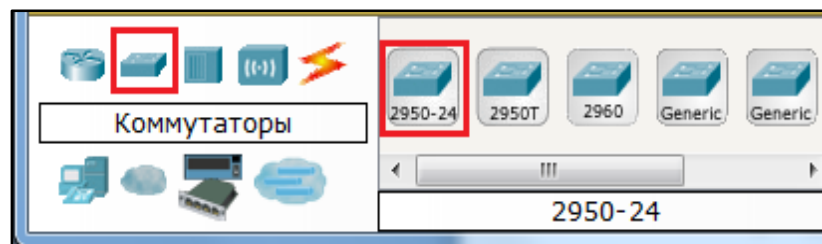


Рисунок 2.30 – Выбирается коммутатор 2950-24

2. Так же поступите с «Сетевым концентратором (Hub-PT)» и «Рабочими станциями (PC-PT)», в соответствии с рисунками 2.31, 2.32.

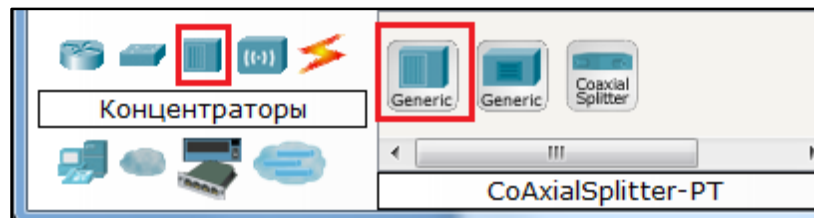


Рисунок 2.31 – Выбирается концентратор Hub-PT



Рисунок 2.32 – Выбирается персональный компьютер PC-PT

Практическая работа 2. Начальные сведения

Размещение компьютеров, коммутатора и концентратора на рабочей области должно быть такое как представлено на рисунке 2.33.

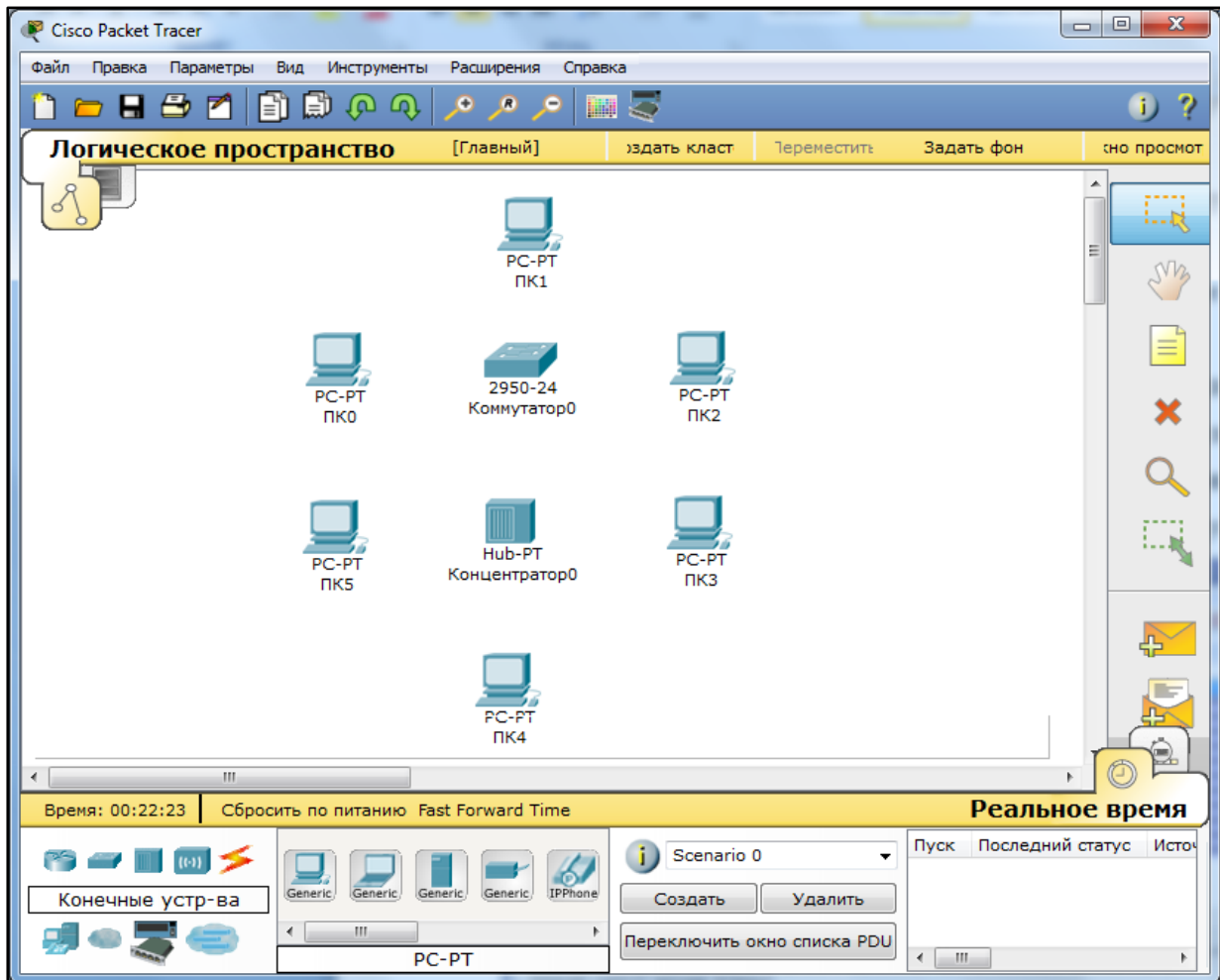


Рисунок 2.33 – Размещение компьютеров, коммутатора и концентратора на рабочей области

3. Соедините устройства, как показано на рисунке 2.29, используя соответствующий интерфейс. Для соединения компьютеров к коммутатору и концентратору используйте кабель типа «Медный прямой» в соответствии с рисунком 2.34.

Практическая работа 2. Начальные сведения



Рисунок 2.34 – Выбран тип кабеля «медный прямой»

4. Для соединения между собой коммутатора и концентратора используйте кабель «Медный кроссовер» в соответствии с рисунком 2.35.

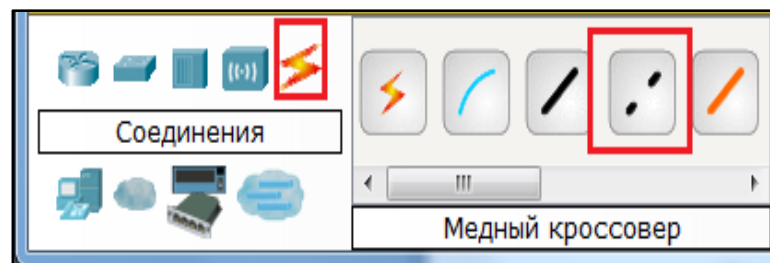


Рисунок 2.35 – Выбор типа кабеля «Медный кроссовер»

5. Для соединения двух устройств, необходимо выбрать соответствующий вид кабеля и нажать на одно устройство (выбрав произвольный свободный порт FastEthernet) и на другое устройство (также выбрав произвольный свободный порт FastEthernet), в соответствии с рисунками 2.36 – 2.38.

Практическая работа 2. Начальные сведения

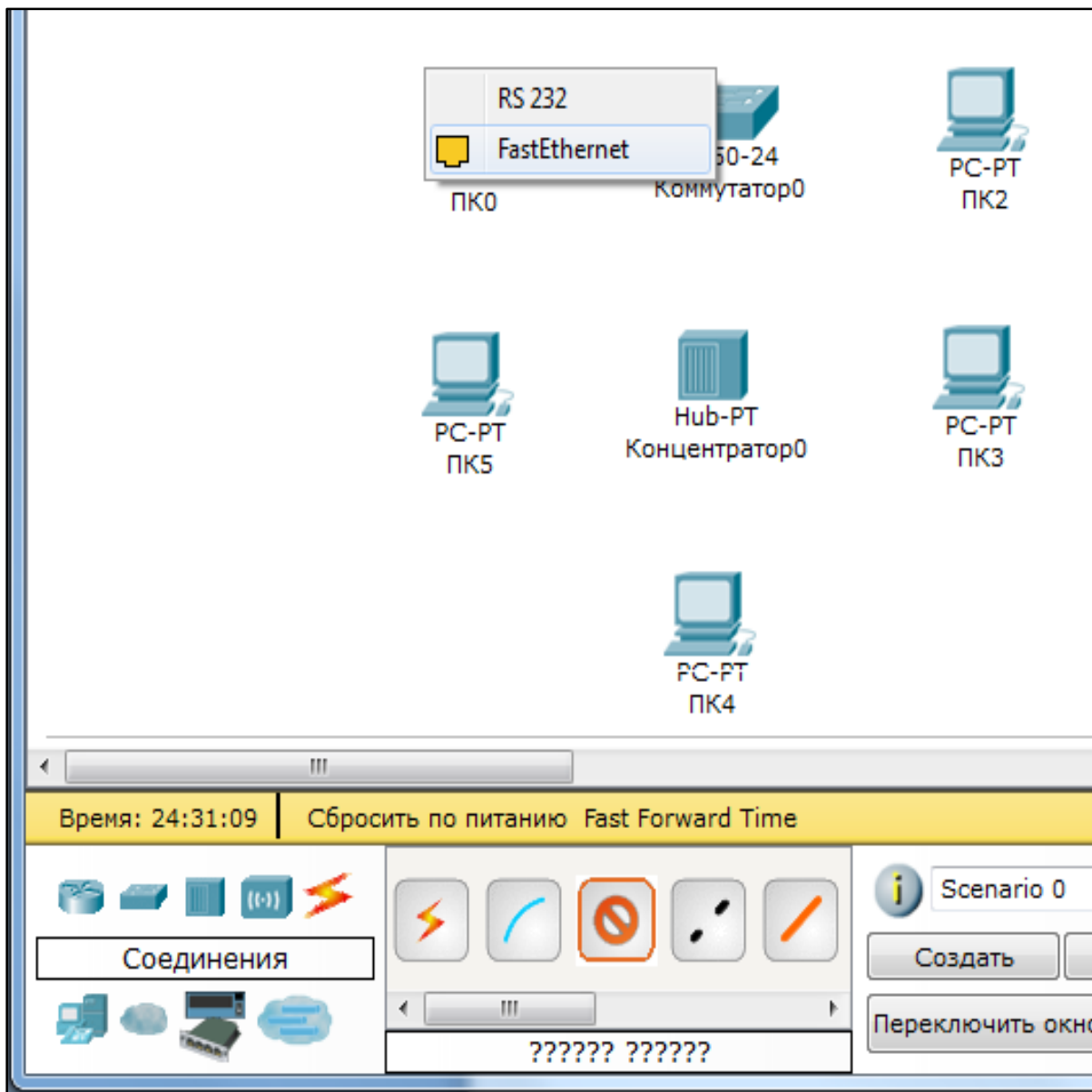


Рисунок 2.36 – Выбирается свободный порт на компьютере

Практическая работа 2. Начальные сведения

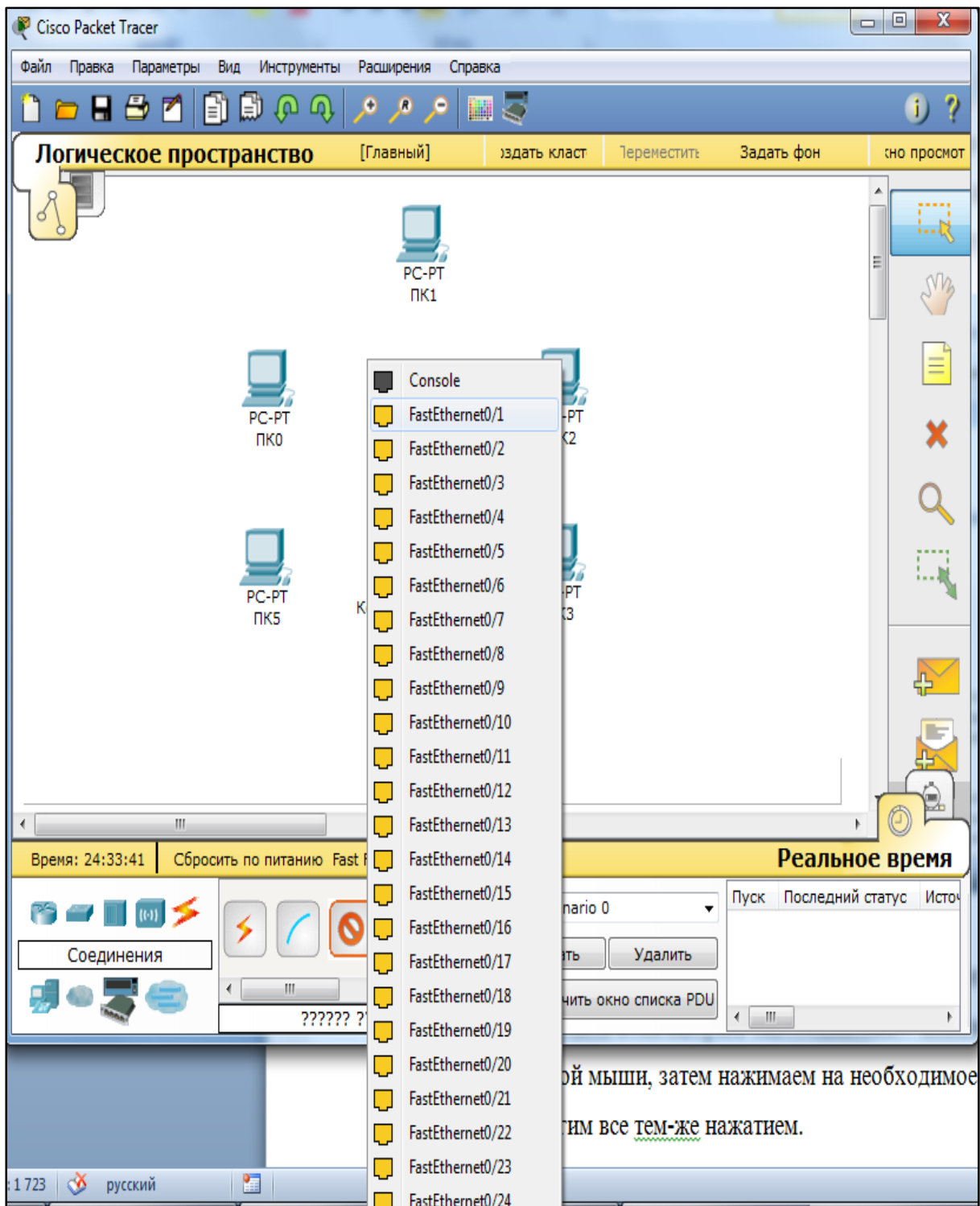


Рисунок 2.37 – Выбирается свободный порт на коммутаторе

Практическая работа 2. Начальные сведения

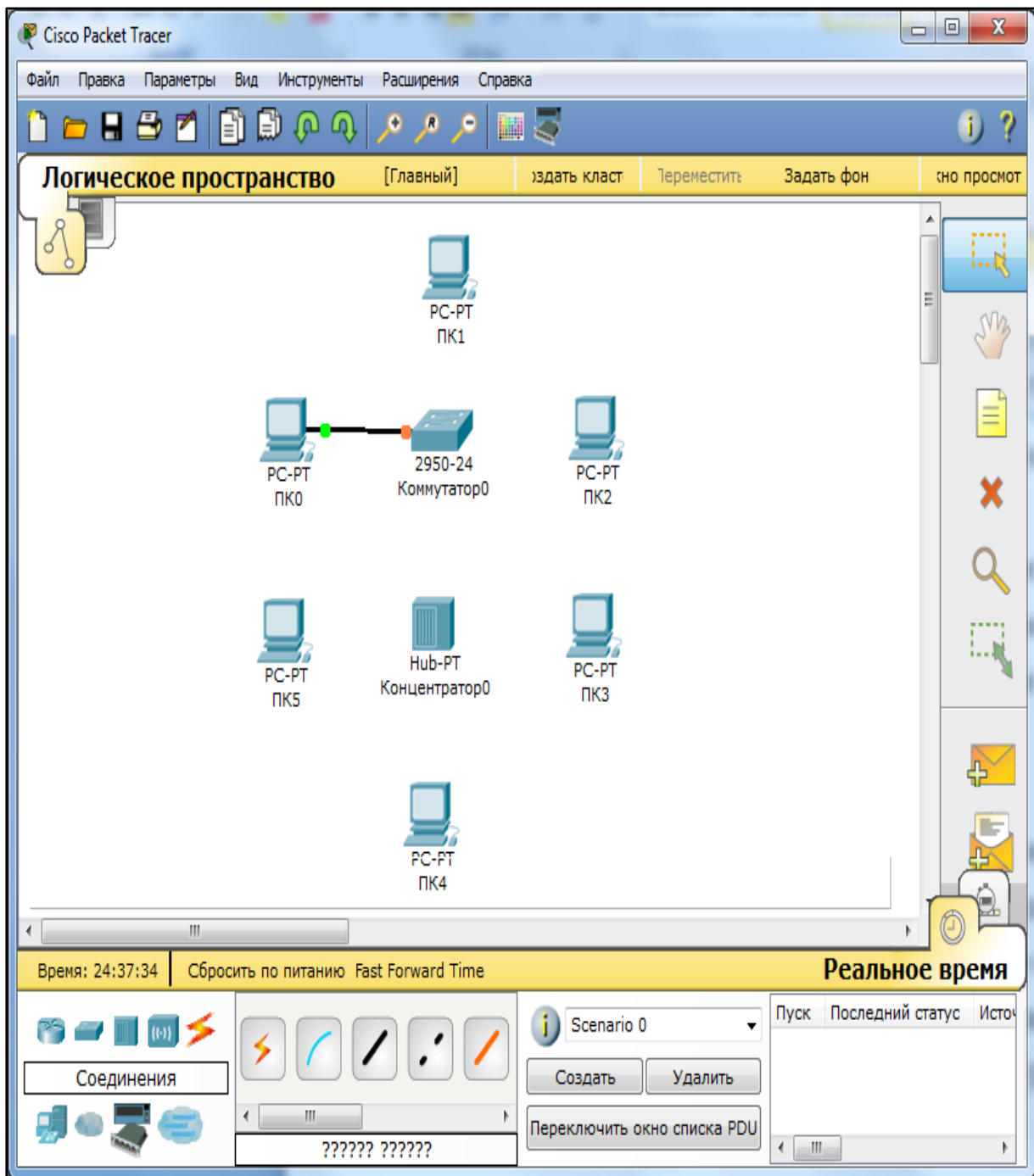


Рисунок 2.38 – Соединение медным прямым кабелем ПК 0 и коммутатор 0

6. Аналогично выполняется соединение для всех остальных устройств. Соединение между коммутатором и концентратором выполняется кроссовером.

Результат подключения устройств представлен на рисунке 2.39.

Практическая работа 2. Начальные сведения

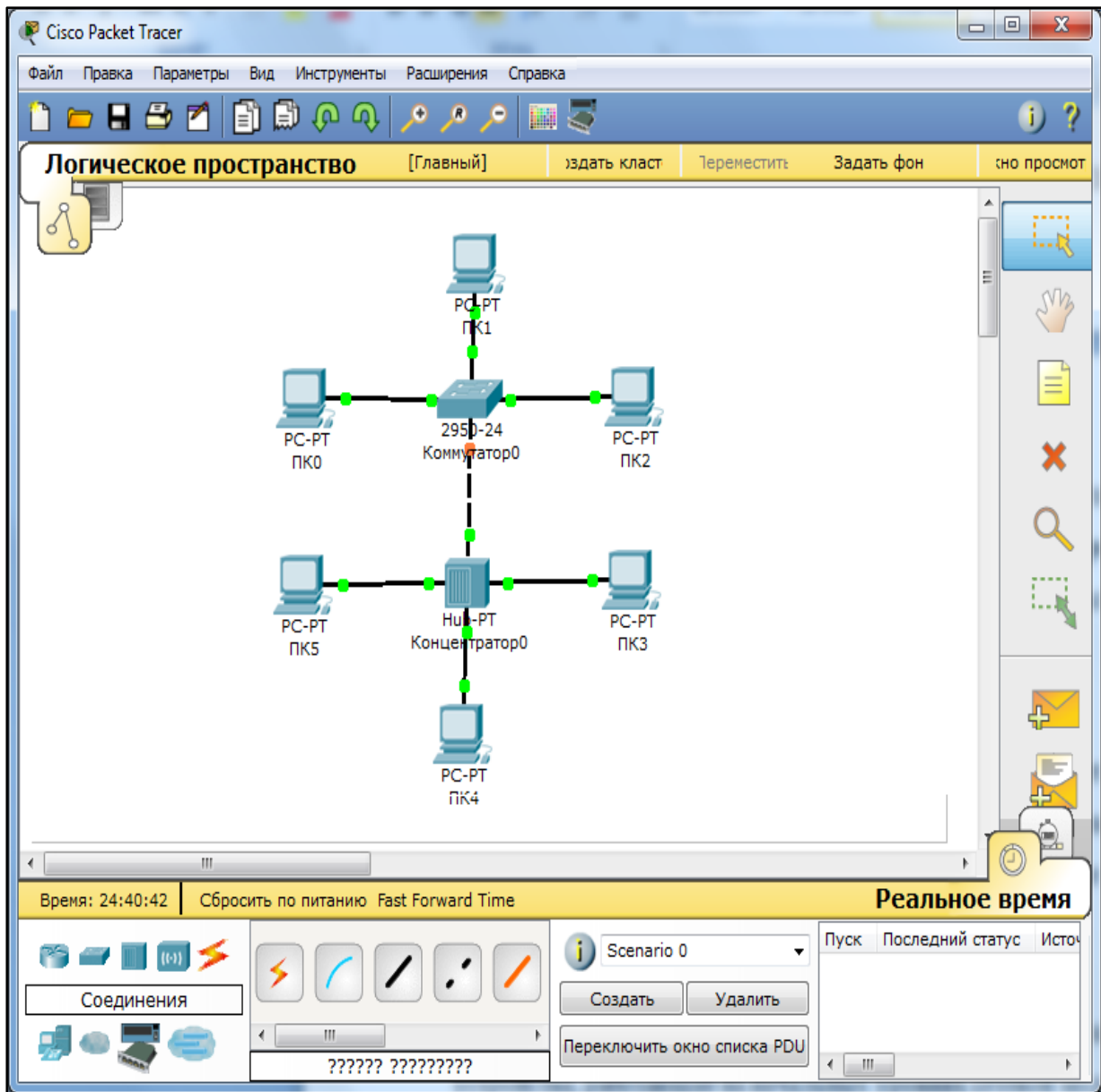


Рисунок 2.39 – Подключение устройств между собой

7. Далее идет этап настройки. Так как используются устройства, работающие на начальных уровнях сетевой модели OSI (коммутатор на втором, концентратор – на первом), то их настраивать не надо. Необходима лишь настройка рабочих станций, а именно: IP-адреса, маски подсети.

Практическая работа 2. Начальные сведения

Ниже приведена настройка лишь одной станции (PC1) – остальные настраиваются аналогично. Выполните двойной клик по нужной рабочей станции, в соответствии с рисунком 2.40. В открывшемся окне выбирать вкладку Рабочий стол, далее – «Настройка IP», в соответствии с рисунком 2.41.

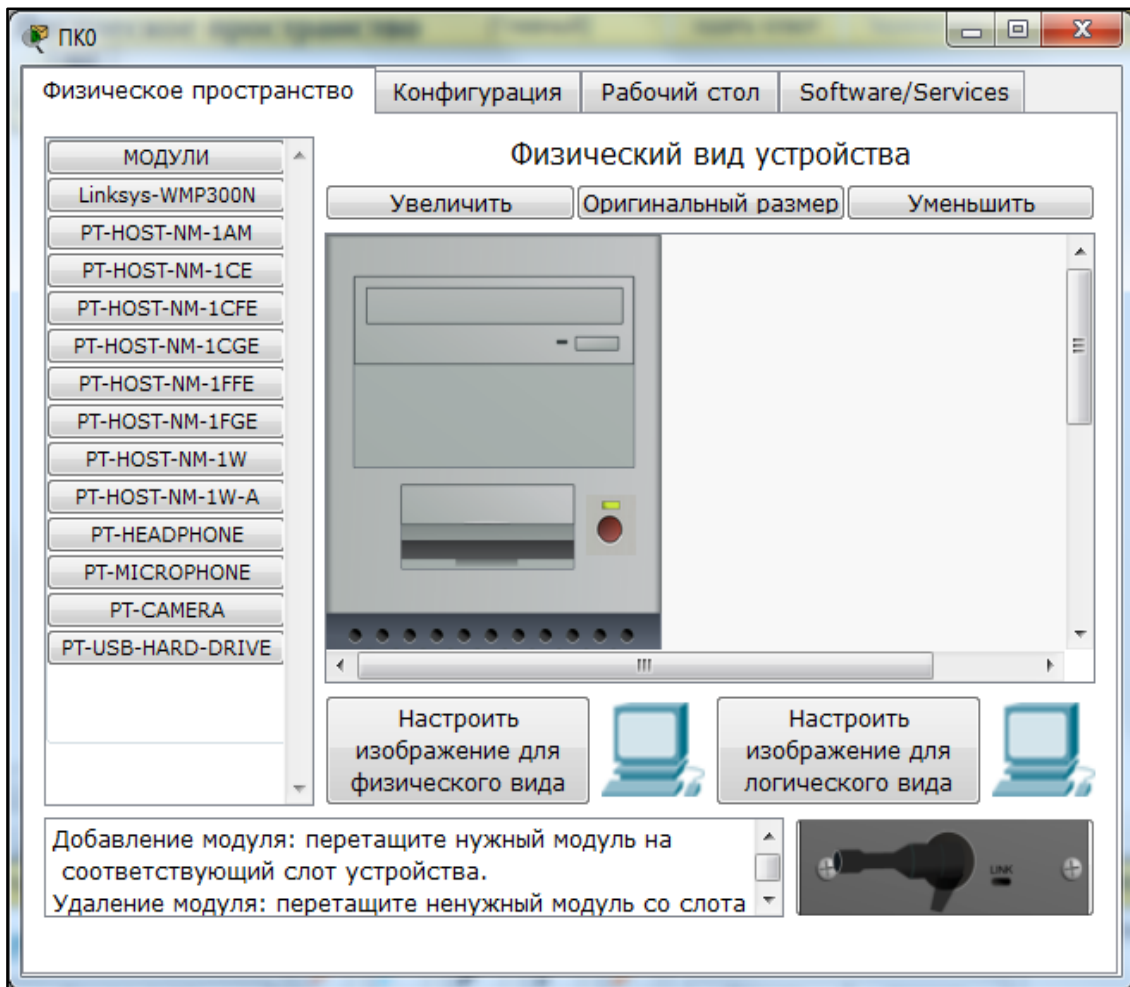


Рисунок 2.40 – Окно настройки компьютера PC0

Практическая работа 2. Начальные сведения



Рисунок 2.41 – Окно настройки компьютера PC0

Открывается окно, в соответствии с рисунком 2.42, где нужно ввести IP-адрес и маску.

8. Аналогично присваиваются IP-адреса всем остальным компьютерам. IP-адреса всех рабочих станций должны находиться в одной и той-же подсети (то есть из одного диапазона), иначе процесс ring не выполнится.

Шлюз и DNS-сервер. Поле можно не заполнять.

Практическая работа 2. Начальные сведения

9. Когда настройка завершена, выполните ping-процесс. Например, запускается с PC5 и проверять наличие связи с PC1.

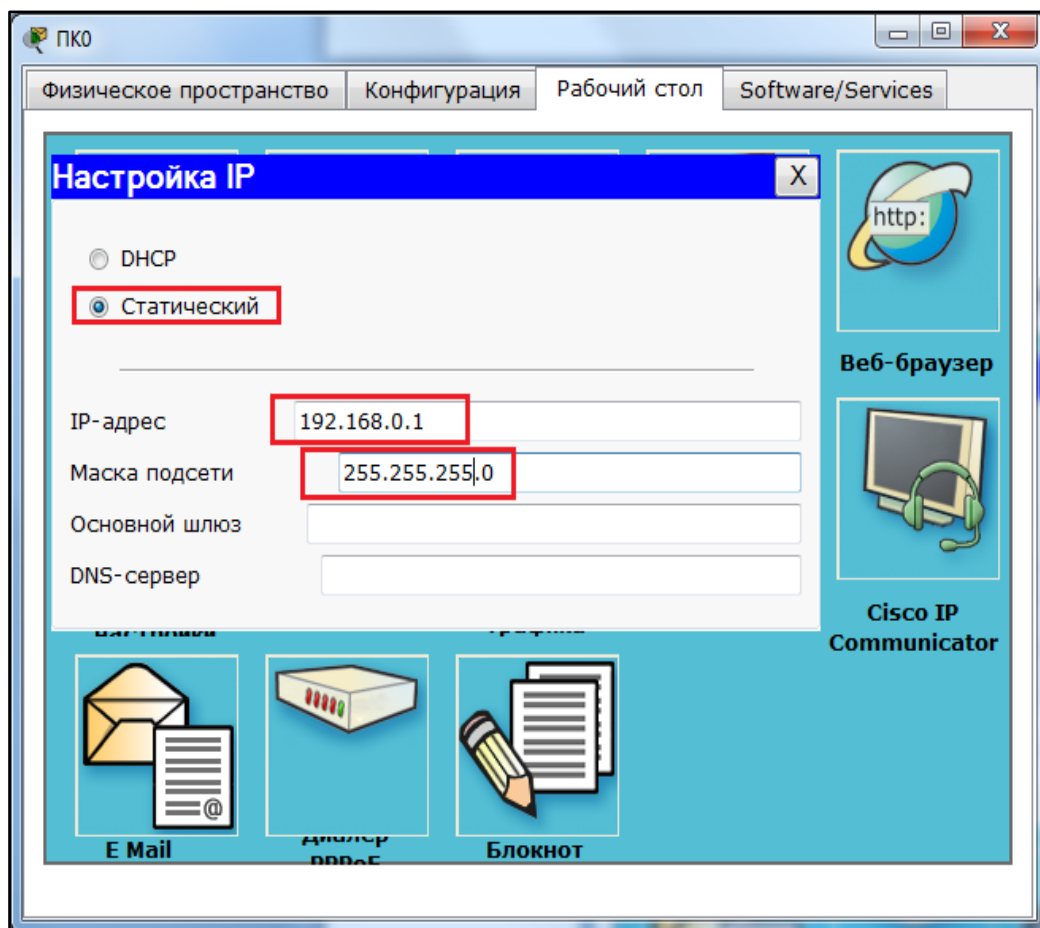


Рисунок 2.42 – Ввод статического IP-адреса и маски

Можно произвольно выбирать, откуда запускать ping-процесс, главное, чтобы выполнялось условие: пакеты должны обязательно пересылаться через коммутатор и концентратор. Для этого выполнить двойной клик по нужной рабочей станции, в открывшемся окне выбрать вкладку «Рабочий стол», далее – «Командная строка», в соответствии с рисунком 2.43. Откроется окно командной строки, в соответствии с рисунком 2.44.

Практическая работа 2. Начальные сведения

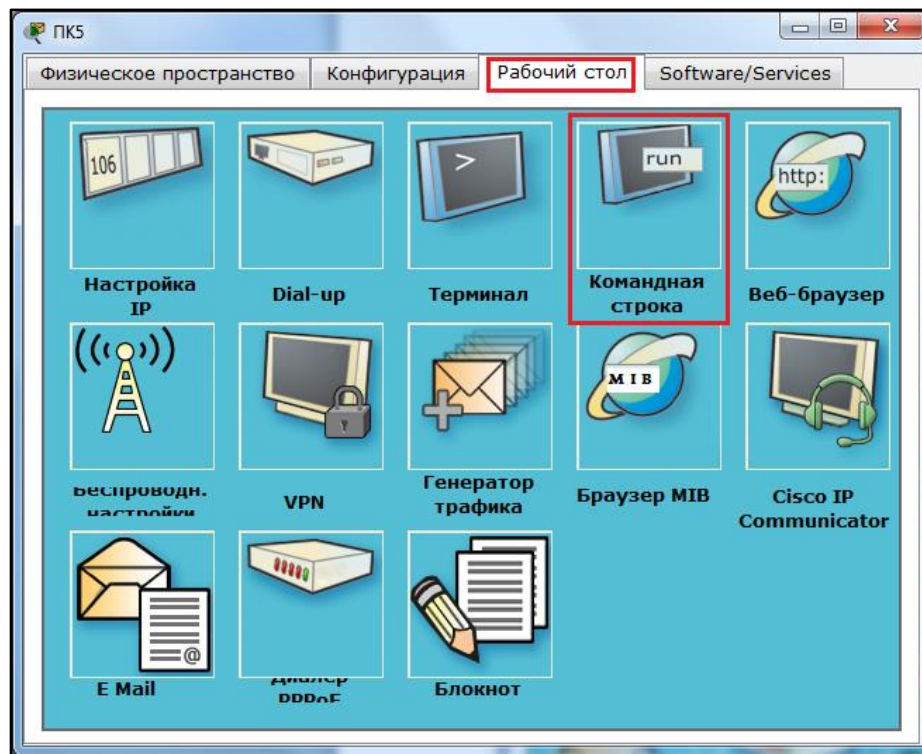


Рисунок 2.43 – Выбор режима «Командная строка»

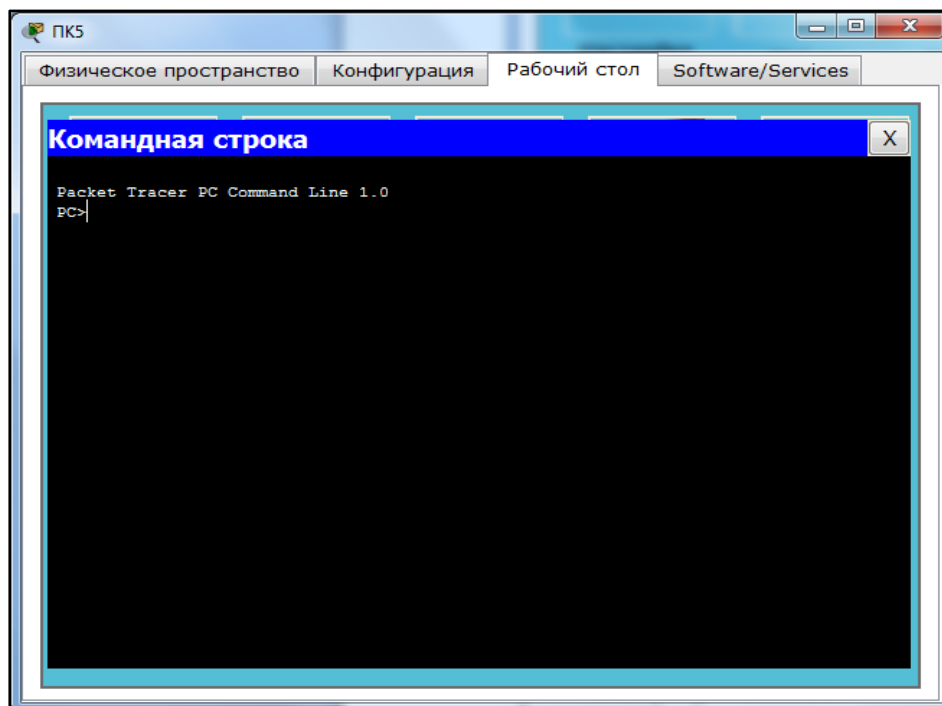


Рисунок 2.44 – Режим «Командная строка»

Практическая работа 2. Начальные сведения

10. Введите команду:

```
PC> ping 192.168.0.1
```

Нажмите клавишу Enter. Если все настроено верно, то увидите следующую информацию, представленную на рисунке 2.45.

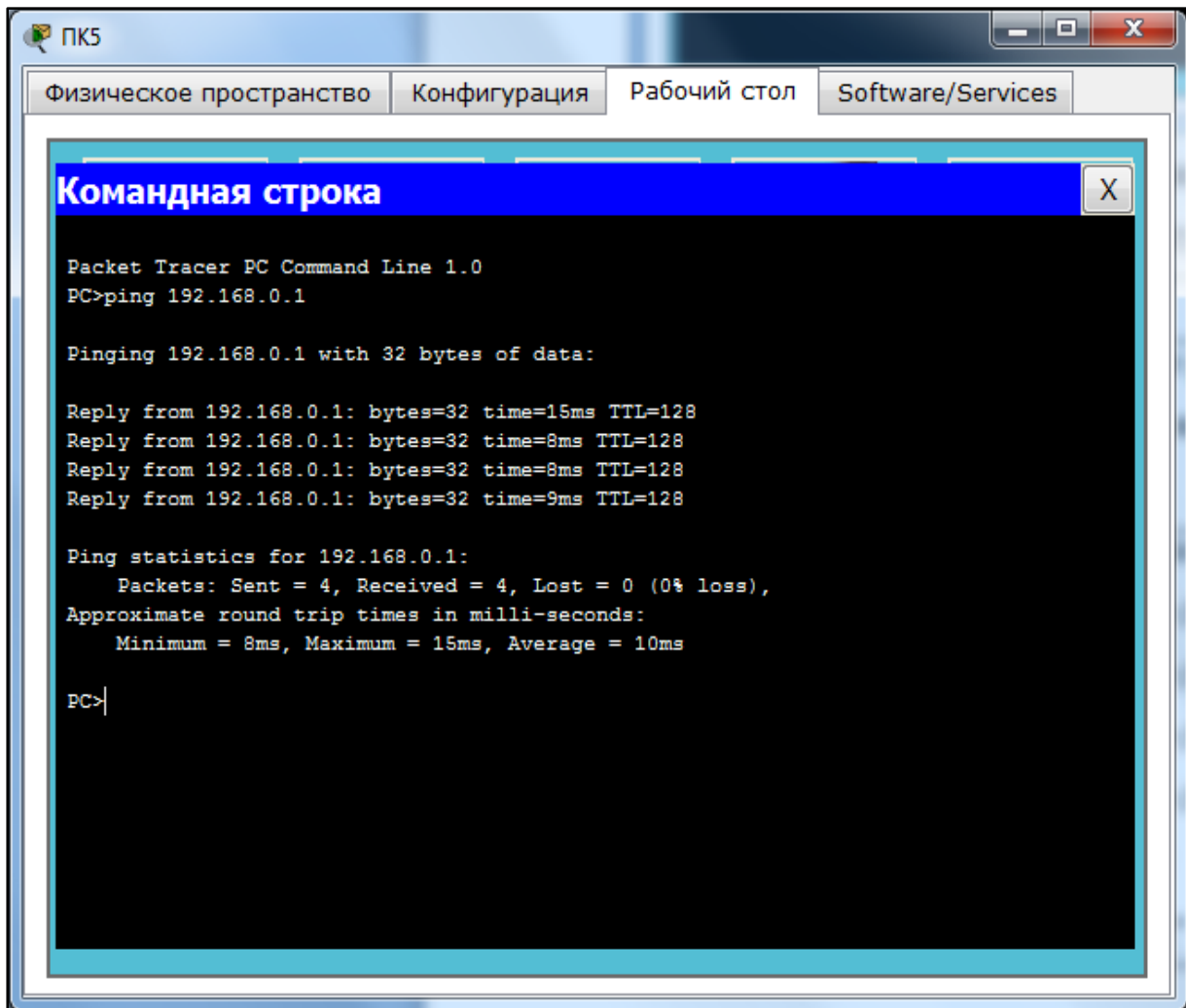


Рисунок 2.45 – Результат выполнения команды «ping»

Это означает, что связь установлена, и данный участок сети работает исправно.

Практическая работа 2. Начальные сведения

11. Cisco Packet Tracer позволяет выполнять команду «ping» значительно быстрее и удобнее. Для этого, выбирается на боковой панели сообщение в соответствии с рисунком 2.46.

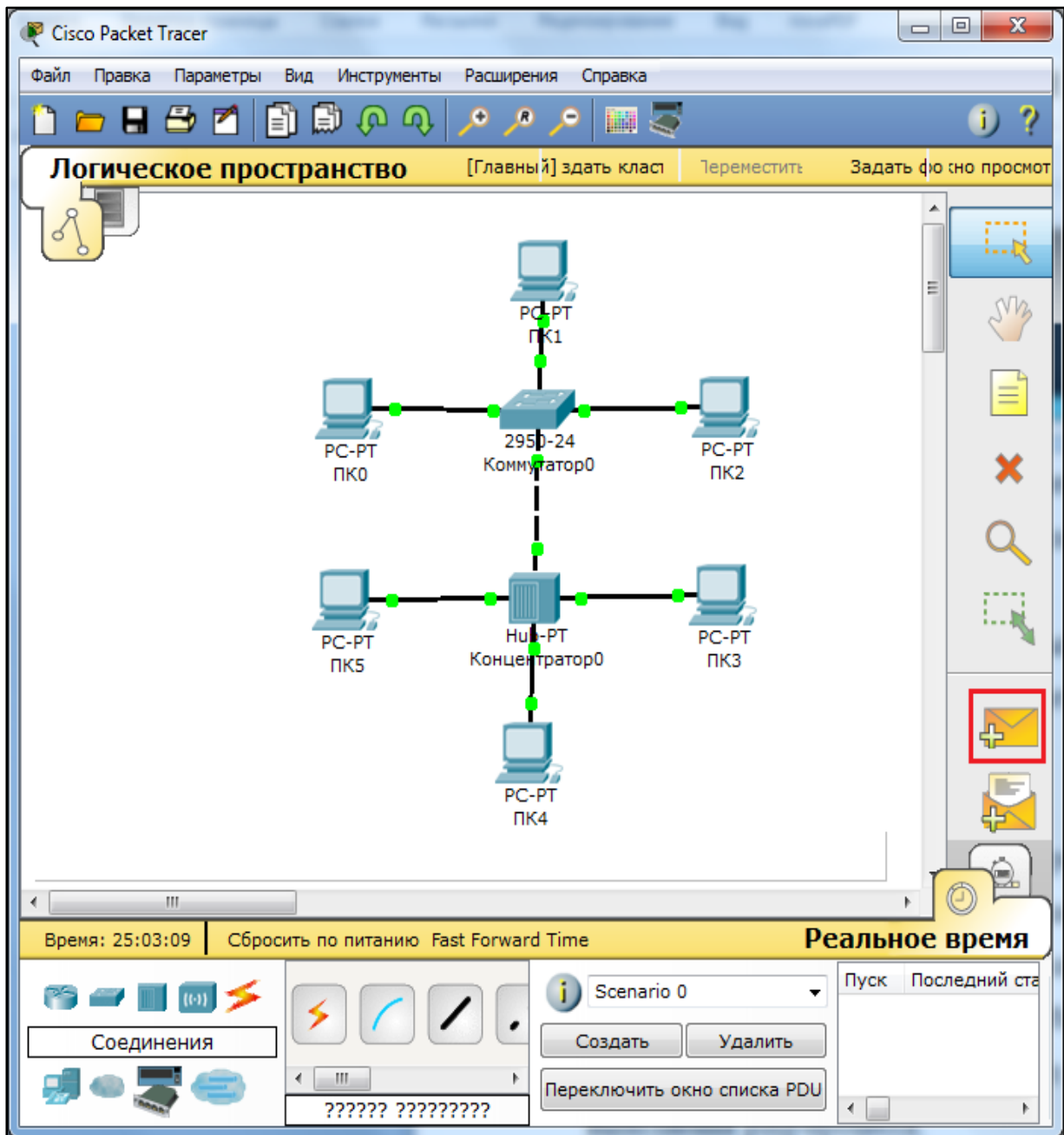


Рисунок 2.46 – Выбирается сообщение, для выполнения команды «ping»

Далее нужно кликнуть мышкой по компьютеру, от которого будет передаваться команда «ping» и еще раз щелкнуть по компьютеру,

Практическая работа 2. Начальные сведения

до которого будет выполняться «ping». В результате будет выполнена команда «ping», результат отобразится в нижнем правом углу (рисунок 2.47).

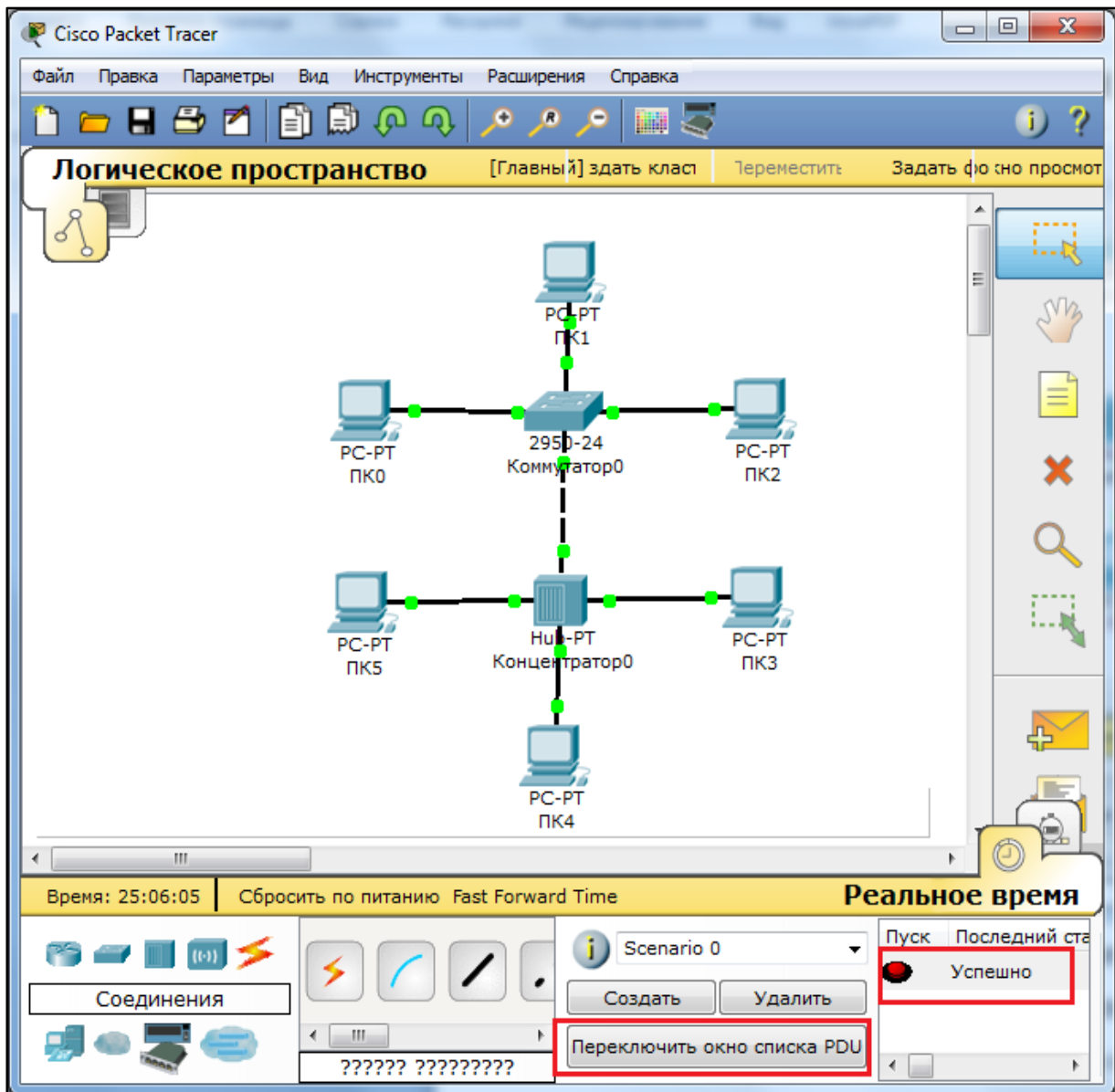


Рисунок 2.47 – Результат выполнения команды «ping»

12. Для более детального отображения результата выполнения команды выберите «Переключить окно списка PDU (рисунок 2.48).

Практическая работа 2. Начальные сведения

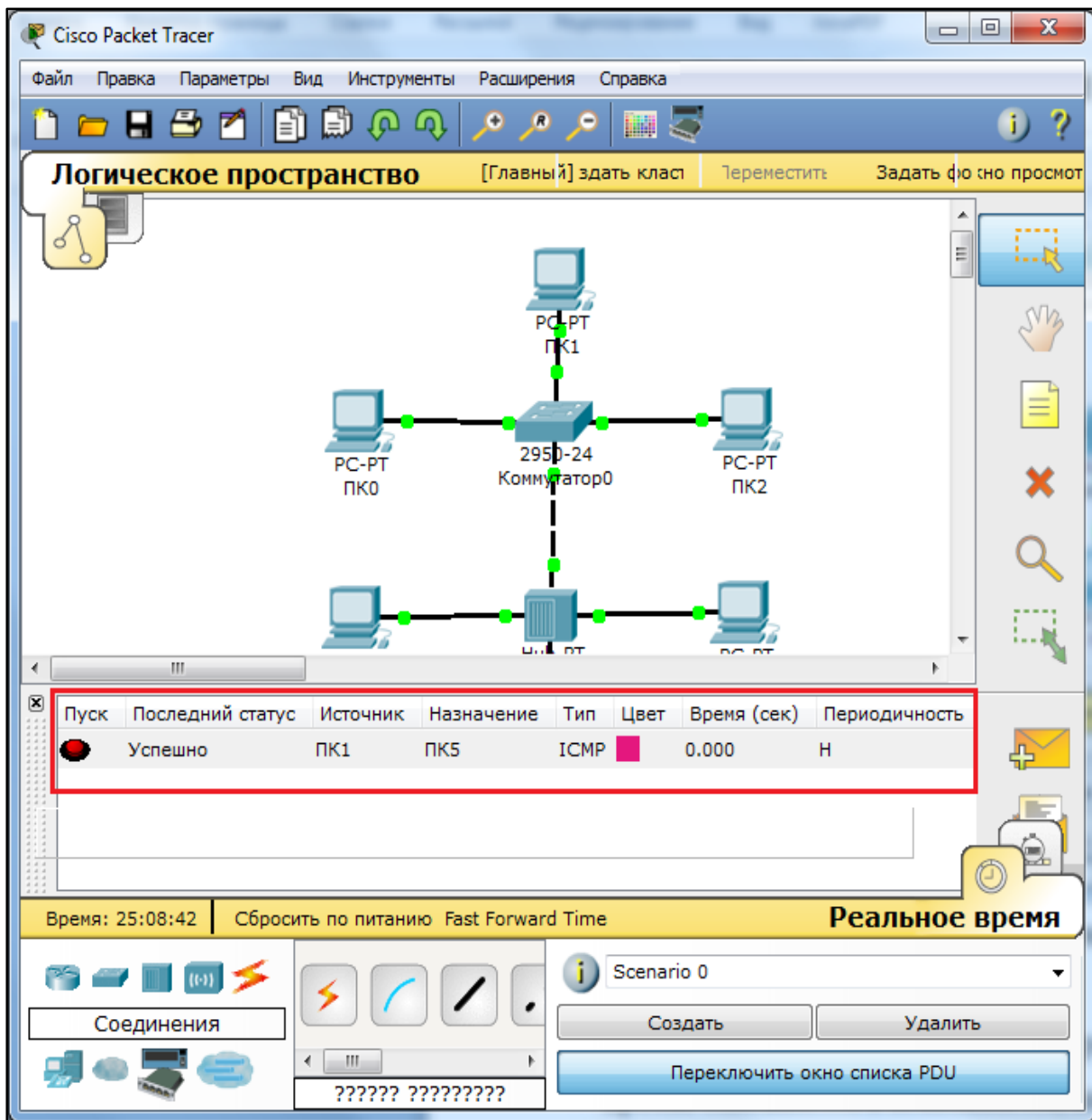


Рисунок 2.48 – Результат выполнения команды «ping»

13. В Cisco Packet Tracer предусмотрен режим моделирования, в котором подробно описывается и показывается, как работает утилита Ping. Поэтому необходимо перейти в «режим симуляции», нажав на одноименный значок в нижнем левом углу рабочей области, или по комбинации клавиш Shift+S. Откроется «Панель моделирования», в которой будут отображаться все события, связанные с выполнением ping-процесса (рисунок 2.49).

Практическая работа 2. Начальные сведения

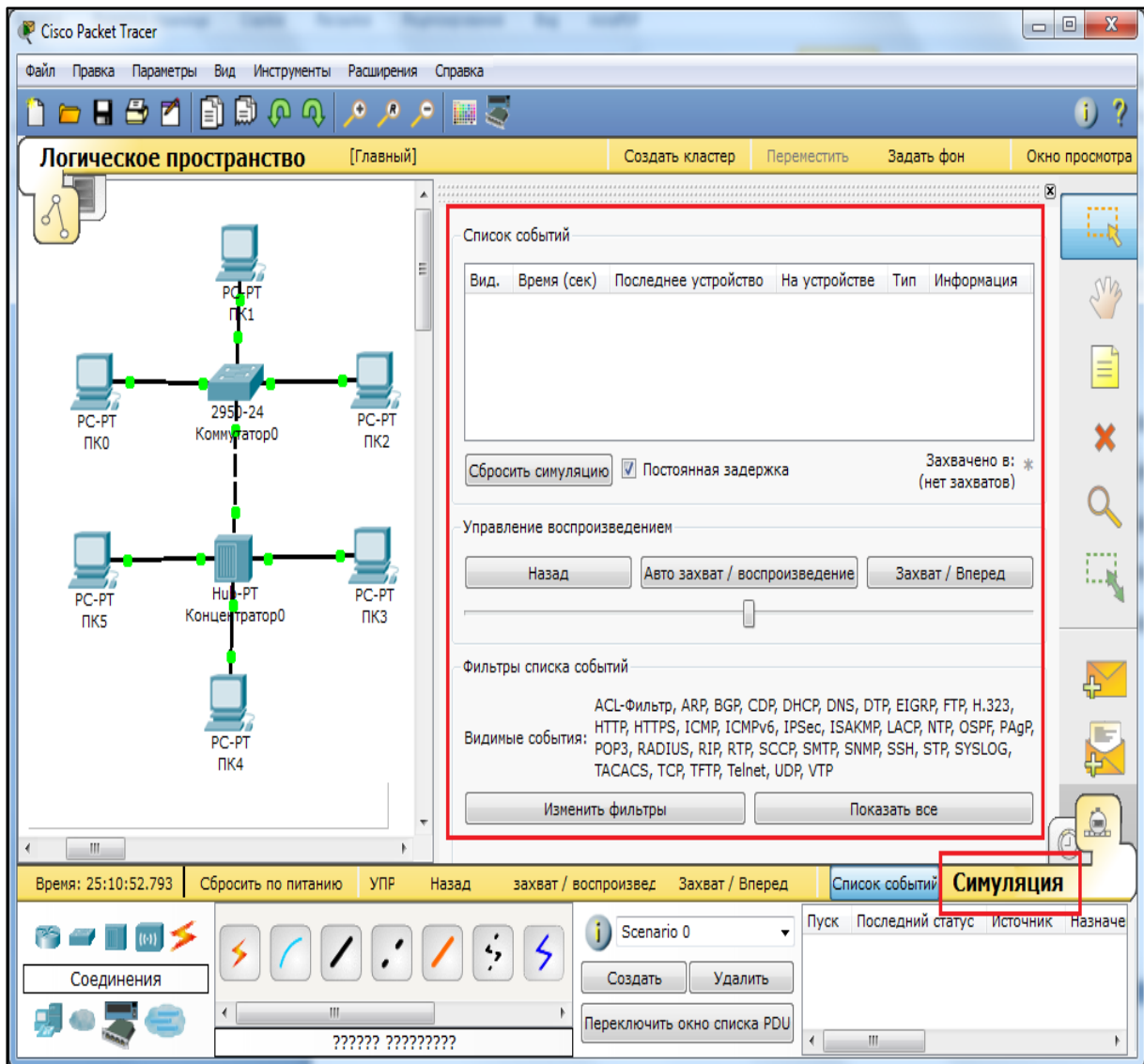


Рисунок 2.49 – Переход в «режим симуляции»

14. Перед выполнением симуляции необходимо задать фильтрацию пакетов. Для этого нужно нажать на кнопку «Изменить фильтры», откроется окно (рисунок 2.50), в котором нужно оставить только «ICMP» и «ARP».

Практическая работа 2. Начальные сведения

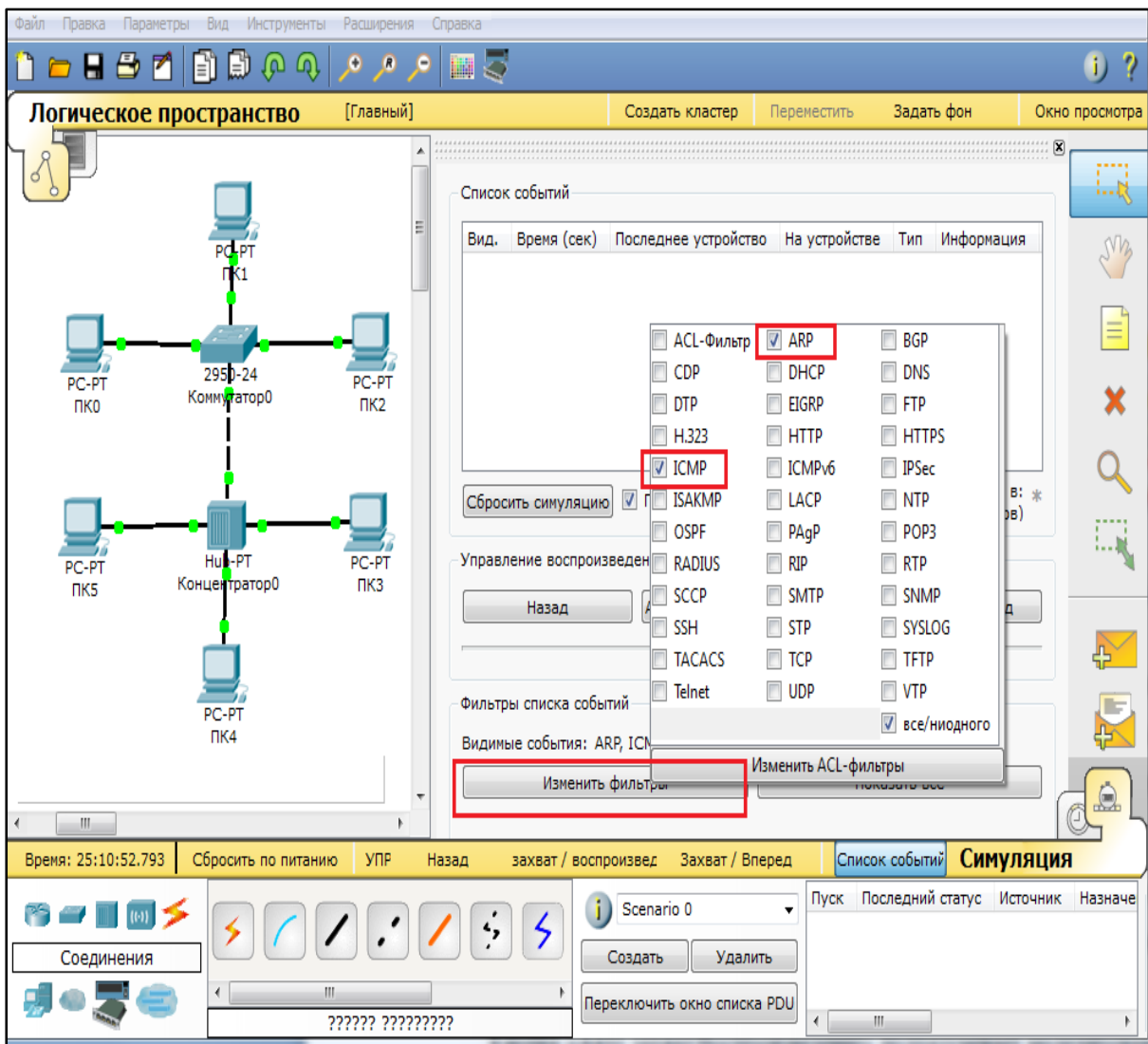


Рисунок 2.50 – Настройка фильтра - нужно оставить только «ICMP» и «ARP»

15. Повторите запуск ping-процесса. После его запуска можно сдвинуть «Панель моделирования», чтобы на схеме спроектированной сети наблюдать за отправкой/приемкой пакетов (рисунок 2.51).

Кнопка «Авто захват/Воспроизведение» подразумевает моделирование всего ping-процесса в едином процессе, тогда как «Захват/Вперед» позволяет отображать его пошагово.

16. Чтобы узнать информацию, которую несет в себе пакет, его структуру, достаточно нажать правой кнопкой мыши на цветной квадрат в графе «Информация».

Практическая работа 2. Начальные сведения

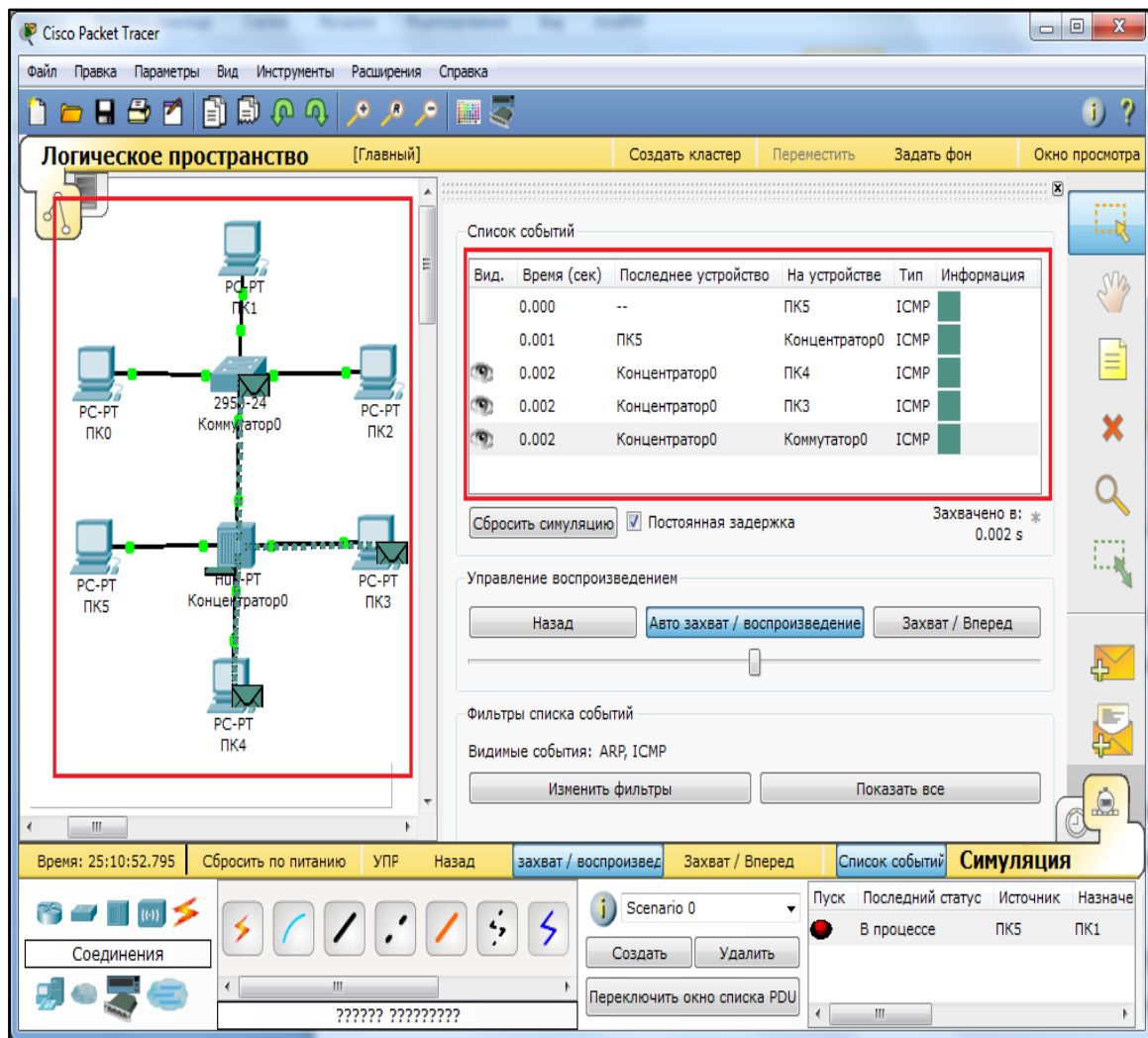


Рисунок 2.51 – Выполнение процесса симуляции

Моделирование прекращается либо при завершении ping-процесса, либо при закрытии окна «Редактирования» соответствующей рабочей станции. Для удаления задания нажимается кнопка «Удалить» в нижней части экрана.

Практическая работа 2. Начальные сведения

Контрольные вопросы

1. Какая плата расширения обеспечивает функционал встроенной точки доступа?
2. Какая плата расширения предоставляет однопортовое последовательное подключение к удаленным офисам или устаревшим серийным сетевым устройствам?
3. Как называется высокопроизводительный модуль с 4-мя коммутационными портами Ethernet под разъем RJ-45?
4. Перечислите сетевые карты, позволяющие подключаться к WAN сетям?
5. Какой тип интерфейса следует выбрать при создании кластера?
6. Назовите модели коммутаторов третьего уровня?
7. Какой тип кабеля следует использовать при соединении роутеров между собой?
8. Укажите серии магистральных маршрутизаторов.
9. В каких случаях используется интерфейс SERIAL?
10. Как организовать связь двух магистральных маршрутизаторов?
11. Перечислите все возможные режимы работы программы Cisco Paket Tracer?
12. Назовите модели коммутаторов второго уровня?
13. Перечислите все типы связей, используемых в Cisco Paket Tracer и укажите их назначение.

Задания

Задание 2.1

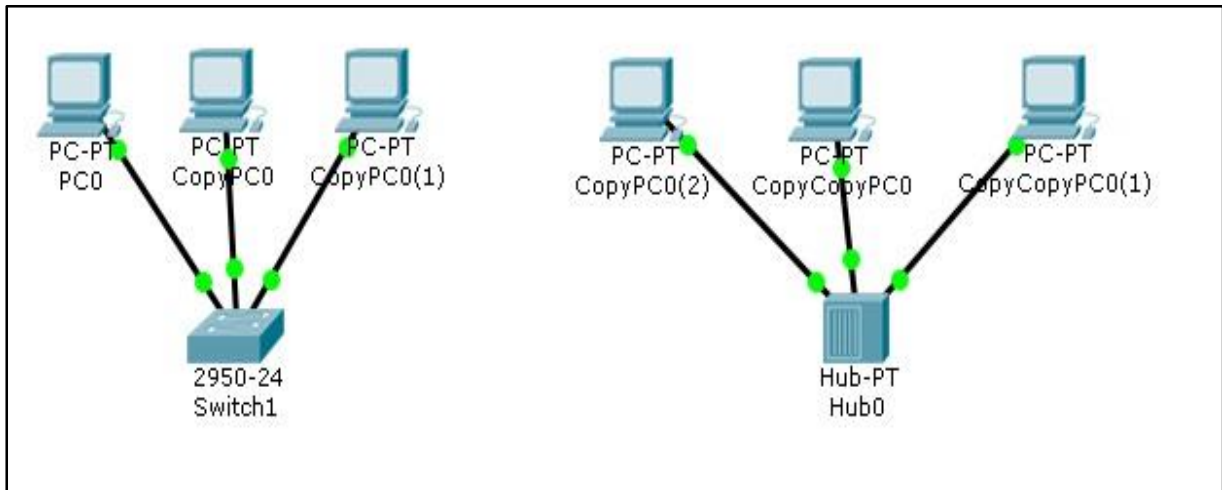
Выполните на своем компьютере все упражнения. Отчет должен содержать скриншоты с экрана вашего компьютера, позволяющие судить о том, что основные результаты последовательного выполнения упражнений выполнены корректно и в надлежащей последовательности.

Практическая работа 2. Начальные сведения

Задание 2.2

1. Создать сеть из 3 компьютеров со свитчем
2. Создать сеть из 3 компьютеров с хабом
3. Посмотреть симуляцию прохождения пакетов

Сама сеть будет выглядеть так:



Практическая работа 3. МОДЕЛИРОВАНИЕ СЕТИ С ТОПОЛОГИЕЙ ЗВЕЗДА

Цель работы – приобретение практических навыков обучающимся в построении, моделировании и оценке эффективности компьютерных сетей, построенных на основе топологии «звезда». Анализируется два способа построения сети – на базе концентратора и на базе коммутатора.

Порядок выполнения работы – внимательно изучите теоретический материал, выполните все упражнения, включённые в данный раздел в пошаговом режиме. Если в промежуточных точках изображения Ваших моделей не совпадает с приводимыми в практикуме, вернитесь на 2-3 шага назад и все-таки добейтесь абсолютного соответствия. Самостоятельно выполните задание к практической работе.

3.1. Краткая теория

Звезда – основная топология компьютерной сети, в которой все компьютеры сети присоединены к центральному узлу, образуя физический сегмент сети [7, 9, 10, 13]. Центральным узлом выступает концентратор, коммутатор или персональный компьютер.

Рабочая станция, с которой необходимо передать данные, отправляет их на концентратор. В определённый момент времени только одна машина в сети может пересылать данные, если на концентратор одновременно приходят два пакета, обе посылки оказываются не принятыми и отправителям нужно будет подождать случайный промежуток времени, чтобы возобновить передачу данных. Этот недостаток отсутствует на сетевом устройстве более высокого уровня – коммутаторе, который, в отличие от концентратора, подающего пакет на все порты, подает лишь на определенный порт – получателю. Одновременно может быть передано несколько пакетов. Сколько – зависит от коммутатора.

Достоинства звезды:

- выход из строя одной рабочей станции не отражается на работе всей сети в целом;

Практическая работа 3. Сети с топологией звезда

- =====
- лёгкий поиск неисправностей и обрывов в сети;
 - высокая производительность сети (при условии правильного проектирования);
 - гибкие возможности администрирования.

Недостатки звезды:

- выход из строя центрального концентратора обернется неработоспособностью сети (или сегмента сети) в целом;
- для прокладки сети зачастую требуется больше кабеля, чем для большинства других топологий;
- число рабочих станций в сети (или сегменте сети) ограничено количеством портов в центральном концентраторе.

Hub работает на первом уровне модели OSI и отправляет информацию во все порты, кроме порта – источника.

Switch работает на втором уровне OSI и отправляет информацию только в порт назначения за счет использования таблицы MAC адресов хостов.

В сетях IP существует 3 основных способа передачи данных: Unicast, Broadcast, Multicast.

- Unicast - процесс отправки пакета от одного хоста к другому хосту;
- Multicast – процесс отправки пакета от одного хоста к некоторой ограниченной группе хостов;
- Broadcast – процесс отправки пакета от одного хоста ко всем хостам в сети.

В некоторых случаях switch может отправлять фреймы как hub, например, если фрейм бродкастовый (*broadcast* - ширококовещание) или unknown unicast (неизвестному единственному адресату).

3.2. Практические упражнения

Упражнение 3.1. Моделирование сети с топологией звезда на базе концентратора [18]

В данном упражнении с помощью программного симулятора Cisco Packet Tracer построите сеть с топологией Звезда на базе концентратора (рисунок 3.1) и изучите ряд приемов работы в этой программе.

Практическая работа 3. Сети с топологией звезда

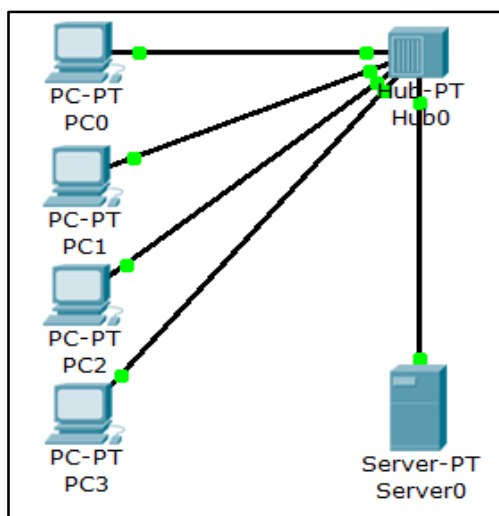


Рисунок 3.1 - Моделирование сети с топологией звезда на базе концентратора

В рабочей области komponуем узлы сети.

1. Выберите «Тип оборудования» Hub's (Концентраторы). В меню «Список устройств данного типа оборудования» необходимо выбрать конкретный концентратор - Hub-PT и «перетащить» его мышью в рабочую область программы.

2. Выбрать тип устройства End Devices (Конечные устройства) и в дополнительном меню выбрать персональный компьютер PC - PT и «перетащить» его мышью в рабочую область программы.

3. Таким же образом установить ещё три персональных компьютера и один сервер.

4. Подключите компьютеры и сервер к концентратору. Для подключения компьютеров и сервера к концентратору необходимо выбрать новый тип устройств Connections (Соединения), далее выбрать **Copper Straight-Through** (Медный прямой) тип кабеля.

Чтобы соединить сетевую карту компьютера с портом Hub, необходимо щелкнуть левой клавишей мыши по нужному компьютеру. В открывшемся графическом меню выбрать порт FastEthernet0 и «протянуть» кабель от ПК к концентратору, где в аналогичном меню выбрать любой свободный порт Fast Ethernet концентратора.

При этом желательно всегда придерживаться следующего правила:

Практическая работа 3. Сети с топологией звезда

- для сервера выбрать 0-й порт,
- для PC1 – 1-й порт,
- для PC2 - 2й порт и так далее.

5. Назначьте узлам сети IP адреса и маску. Для этого двойным щелчком откройте нужный компьютер, далее Config (Конфигурация) – Interface (Интерфейс) - FastEthernet0.

В группе параметров IP Configuration (Настройка IP) должен быть активирован переключатель Static (Статический), в поле IP Address необходимо ввести IP адрес компьютера, маска появится автоматически. Port status (Состояние порта) – On (Вкл).

6. Используя инструмент создания заметок Place Note (клавиша N), подписывайте все IP устройств. IP адреса следует скопировать из окна Config (Конфигурация).

7. Вверху рабочей области создайте заголовок Вашего проекта «Изучение топологии звезда» (рисунок 3.2).

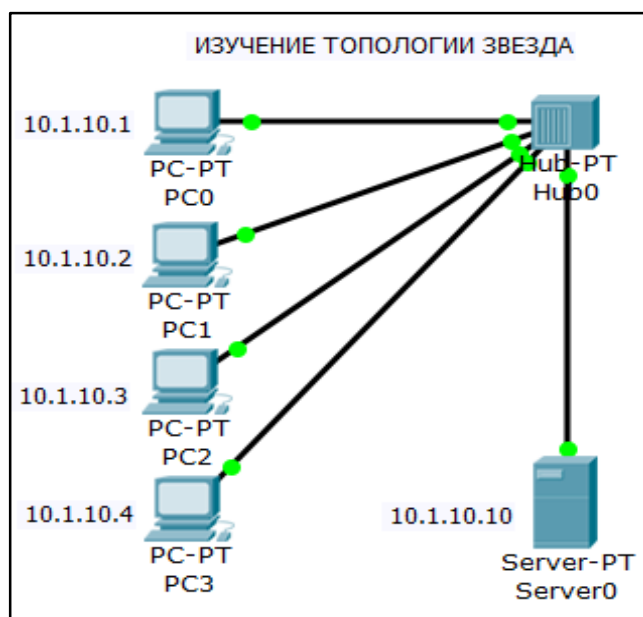


Рисунок 3.2 - Использование инструмента Place Note

8. С целью исключения нагромождения рабочей области надписями, уберите надписи (метки) типов устройств:

- откройте меню *Options* (Опции) в верхней части окна Cisco Packet Tracer,

Практическая работа 3. Сети с топологией звезда

- в ниспадающем списке выберите пункт Preferences (Настройки), а в диалоговом окне снимите флажок Show device model labels (Показать модели устройств).

На экране Вашего компьютера должно быть изображение, соответствующее рисунку 3.3.

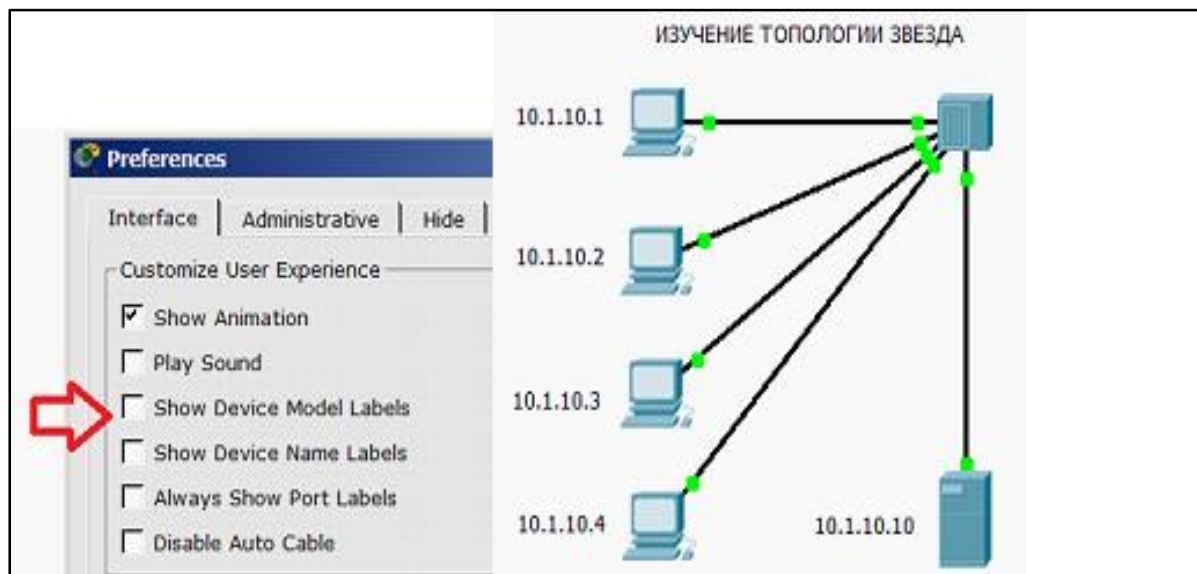


Рисунок 3.3 - Флажок Show device model labels в Preferences

9. Проверьте работоспособность сети. Для этого:

- отправьте с персонального компьютера на другой тестовый сигнал ping и переключитесь в режим Simulation (Симуляция);

- в окне Event list (Список событий), с помощью кнопки Edit filters (Редактировать фильтры), сначала очистите фильтры от всех типов сигнала, а затем установите тип контроля сигнала - только ICMP;

- окно Event list закрываем. На экране Вашего компьютера должно быть изображение, соответствующее рисунку 3.4.

Практическая работа 3. Сети с топологией звезда

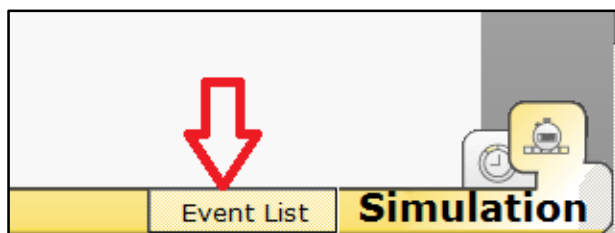


Рисунок 3.4 – Использование кнопки Event list

10. В правой части окна, в графическом меню выберите Add Simple PDU (P) (Простой PDU) (рисунок 3.5). PDU - обобщённое название фрагмента данных на разных уровнях Модели OSI: кадр Ethernet, IP-пакет, UDP - датаграмма, TCP-сегмент.

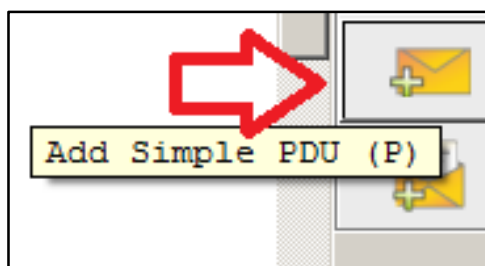


Рисунок 3.5 – Add Simple PDU (P)

11. Щелчками мыши установите его на персональный компьютер - выберите источник сигнала (например, PC3) и, затем, на узле назначения (пусть это будет сервер). Нажимая на кнопку **Capture / Forward** (Захват/Вперед) наблюдайте пошаговое продвижение пакета PDU (рисунок 3.6).

Конец упражнения.

Fire	Last Status	Source	Destination	Type	Color	Time(se)	Periodic	Num	Edit	Delete
	Successful	PC3	Server0	ICMP		0.000	N	0	(edit)	

Рисунок 3.6 – Успешное прохождение пакетов по сети

Полезный прием работы в Cisco Packet Tracer предложен в [16].

Практическая работа 3. Сети с топологией звезда

Предположим, что нужно спроектировать и настроить сеть, топология которой приведена на рисунке 3.7.

Рассмотрим, как можно ускорить и упростить этот процесс.

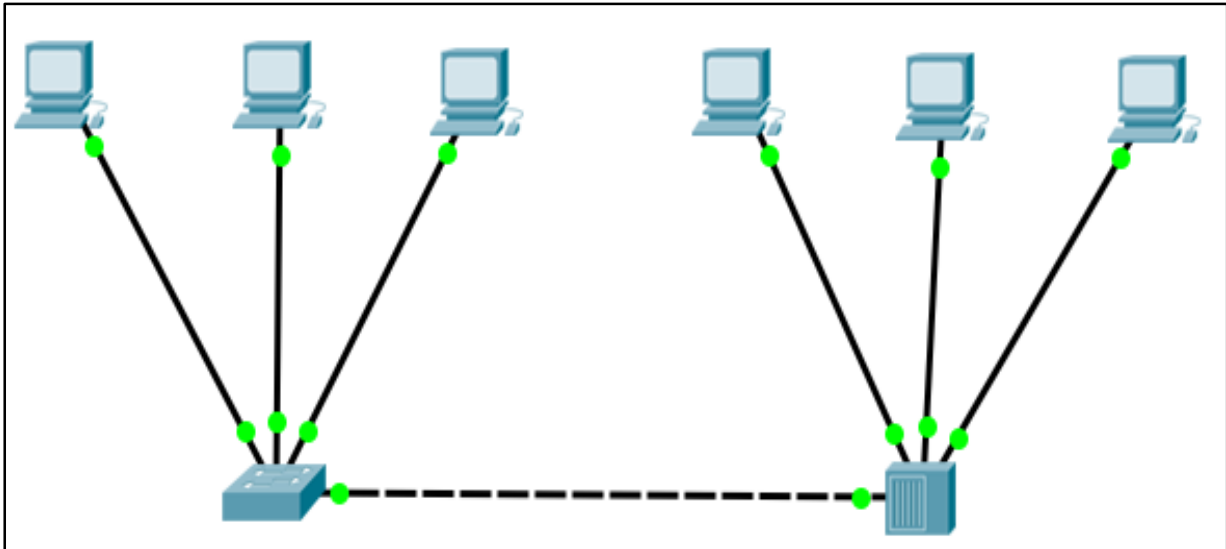


Рисунок 3.7 – Пример топологии сети

Поместите в рабочую область первый персональный компьютер (это будет PC0) и настройте его (рисунок 3.8).

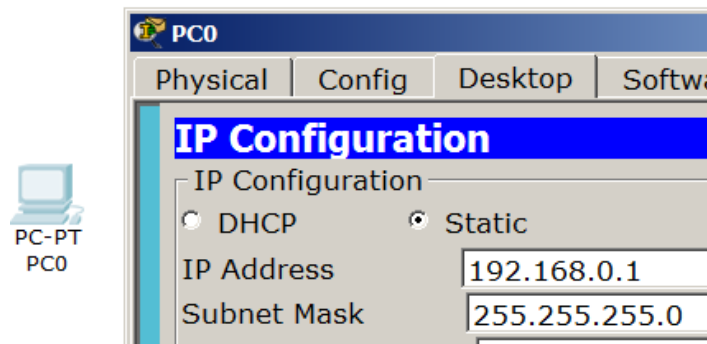


Рисунок 3.8 – Настройка PC0

Удерживая клавишу Ctrl скопируйте этот компьютер несколько раз и настройте остальные адреса компьютеров, меняя только последнюю цифру IP-адреса (рисунок 3.9).

Практическая работа 3. Сети с топологией звезда

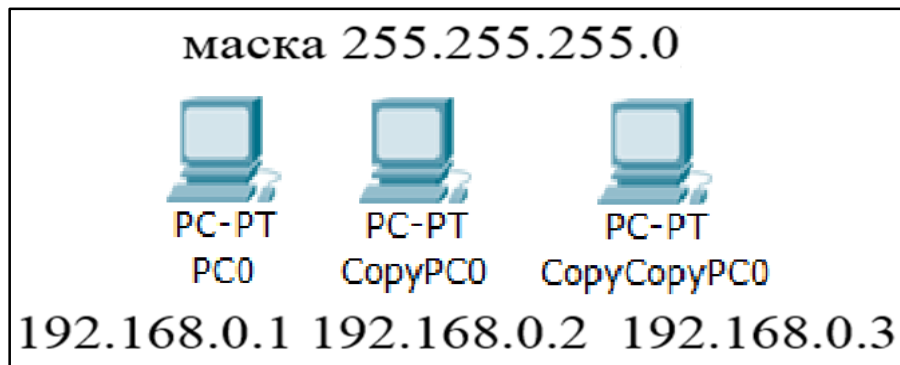


Рисунок 3.9 – Быстрое создание и настройка трех компьютеров в рабочем окне

Скопируйте, удерживая Ctrl, сразу три компьютера и настройте их также, меняя только последнюю цифру IP-адреса (рисунок 3.10).

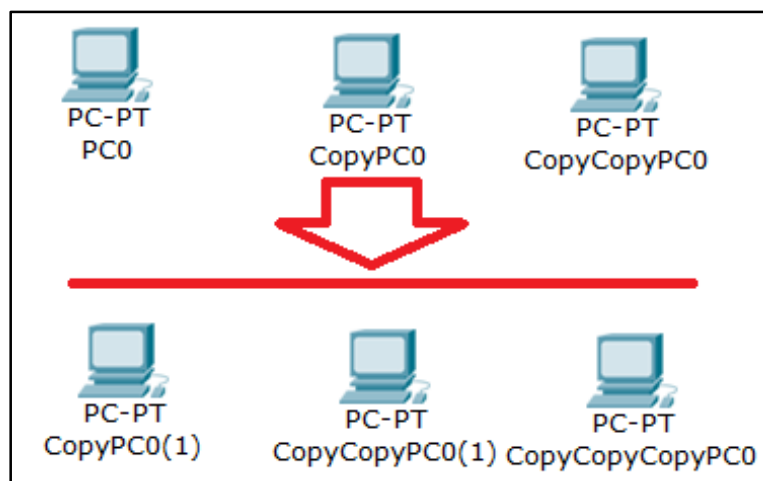


Рисунок 3.10 – Копирование всех трех компьютера сразу

Добавление свитча и хаба сделайте традиционно, а подключение кабеля - автоматическое.

Практическая работа 3. Сети с топологией звезда

Упражнение 3.2. Моделирование сети с топологией звезда на базе коммутатора [17]

Рассмотрим сеть на базе коммутатора (рисунок 3.11).

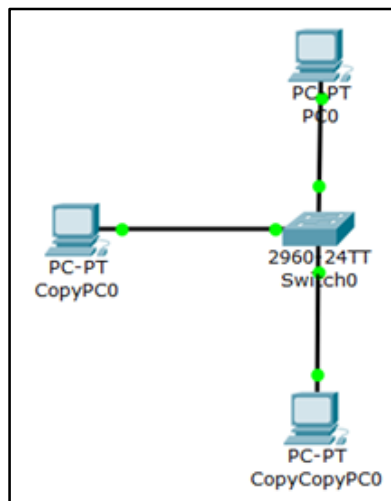


Рисунок 3.11 – Компьютерная сеть с топологией «Звезда» на базе коммутатора модели 2960

На вкладке Physical Вы можете посмотреть вид коммутатора, имеющего 24 порта Fast Ethernet и 2 порта Gigabit Ethernet (рисунок 3.12).

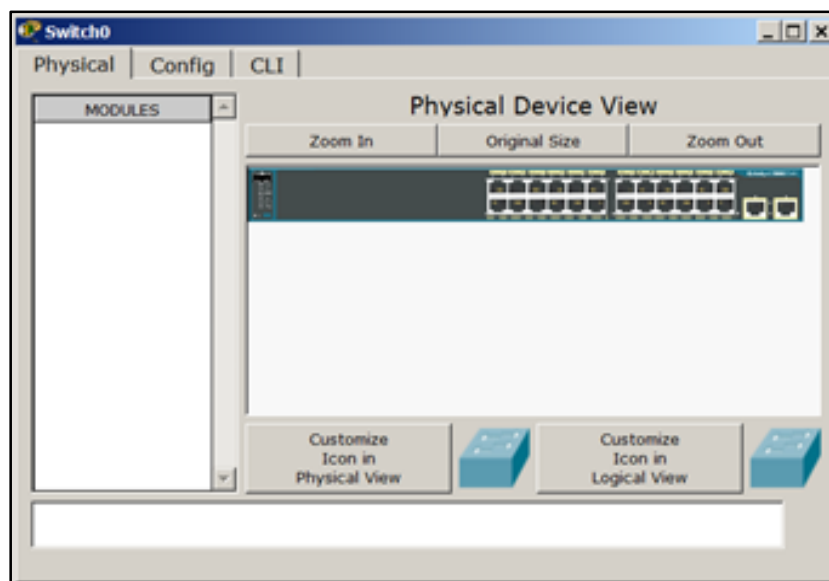


Рисунок 3.12 – Вид коммутатора модели 2960


Практическая работа 3. Сети с топологией звезда

В режиме Simulation настройте фильтры (рисунок 3.13).

IPv4	IPv6	Misc	
<input type="checkbox"/> ARP		<input type="checkbox"/> BGP	<input type="checkbox"/> DHCP
<input type="checkbox"/> DNS		<input type="checkbox"/> EIGRP	<input type="checkbox"/> HSRP
<input checked="" type="checkbox"/> ICMP		<input type="checkbox"/> OSPF	<input type="checkbox"/> RIP

Рисунок 3.13 – Фильтры в режиме Simulation



С помощью функции  просмотрите прохождение пакета между двумя ПК через коммутатор.

Как видим, маршруты пакета в концентраторе и коммутаторе будут разными: как в прямом, так и в обратном направлении хаб управляет всем, а коммутатор – только одному.

Упражнение 3.3. Исследование качества передачи трафика по сети

При исследовании пропускной способности компьютерной сети (качества передачи трафика по сети) желательно увеличивать размер пакета и отправлять запросы с коротким интервалом времени, не ожидая ответа от удаленного узла, для того, чтобы создать серьезную нагрузку на сеть. Однако, утилита ping не позволяет отправлять эхо-запрос без получения эхо-ответа на предыдущий запрос и до истечения времени ожидания. Поэтому для организации существенного трафика воспользуемся программой Traffic Generator.

1. Для работы создайте и настройте следующую сеть (рисунок 3.14).

Практическая работа 3. Сети с топологией звезда

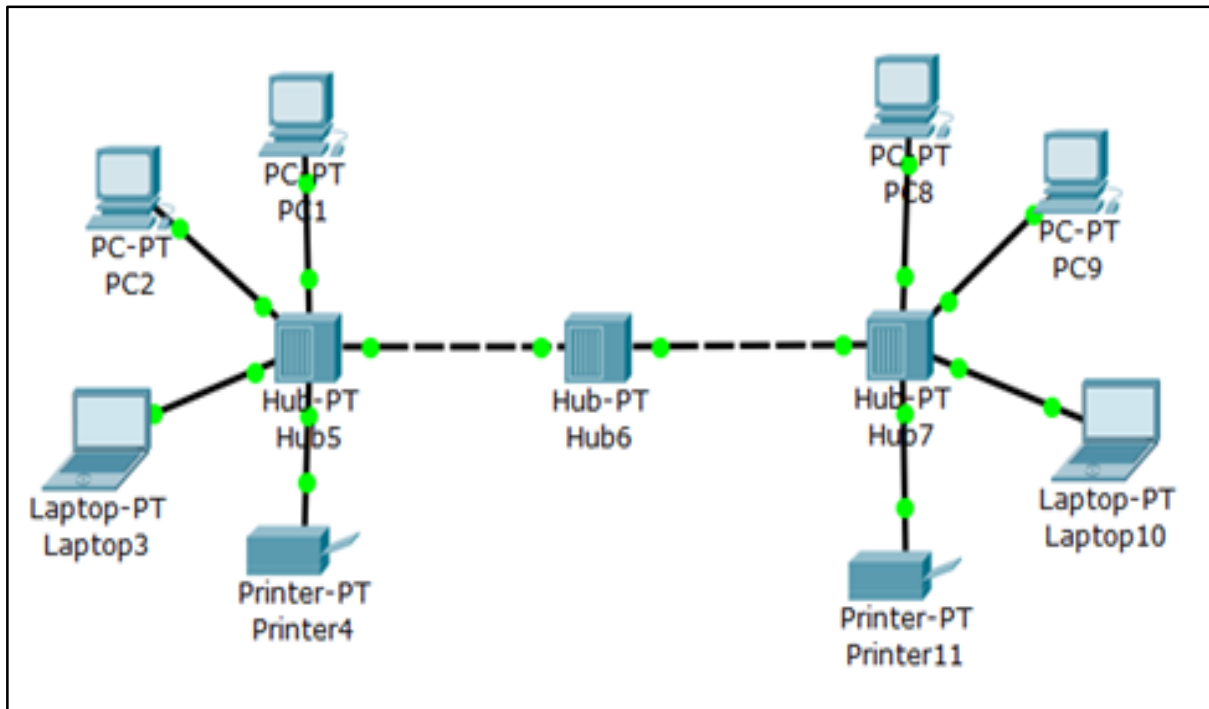


Рисунок 3.14 – Топология моделируемой сети

2. В окне управления PC1 во вкладке Desktop выберите приложение Traffic Generator и задайте настройки, как на рисунке 3.15 для передачи трафика от PC1 на PC8. Для ясности рядом с английской версией окна размещен тот же текст в русской версии программы Cisco Packet Tracer.

Итак, при помощи протокола ICMP мы сформировали трафик между компьютерами PC1 с адресом 192.168.0.1 и PC8 с адресом 192.168.0.8.

Практическая работа 3. Сети с топологией звезда

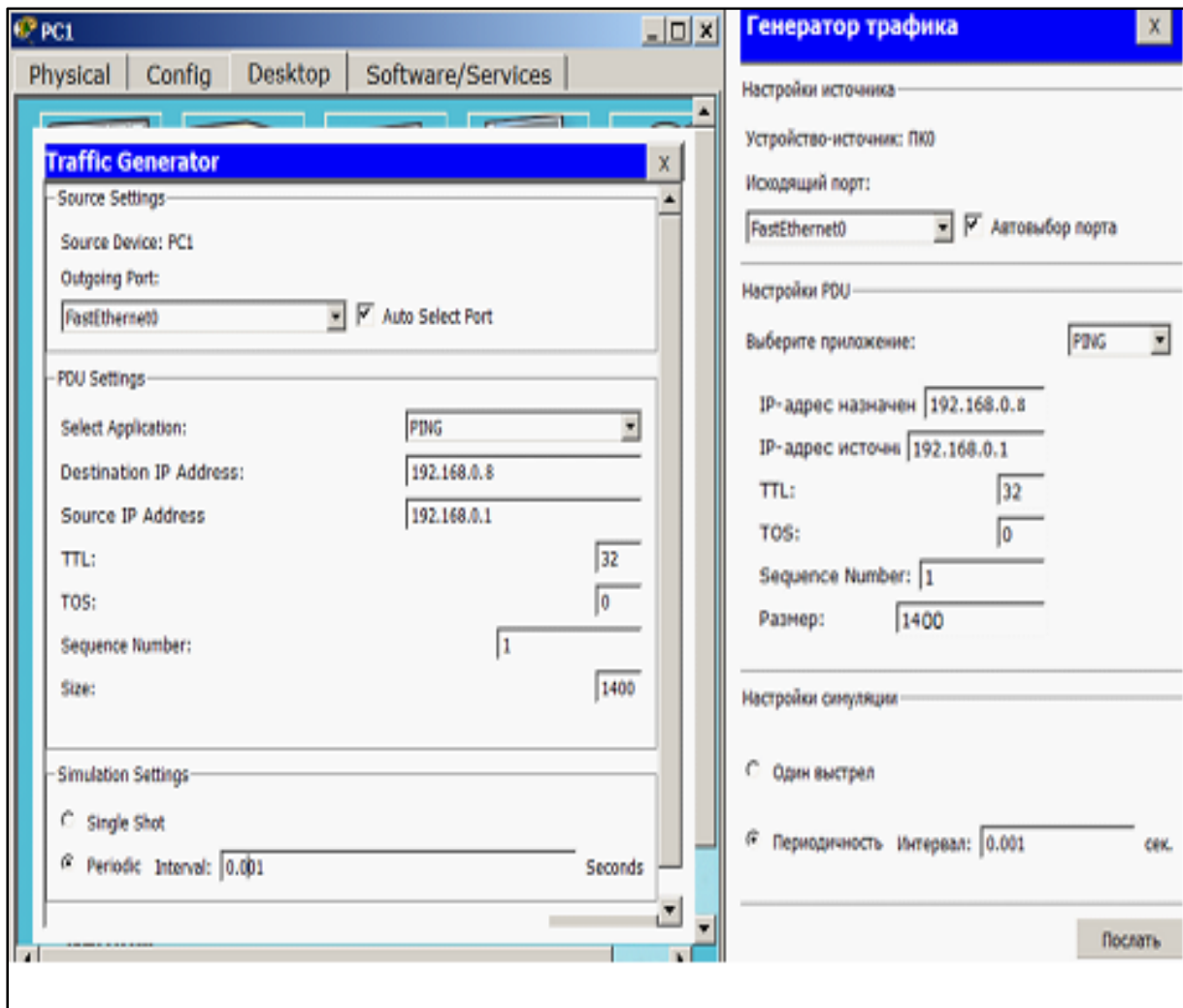


Рисунок 3.15 – Настройка генератора трафика (Вариант трафика от PC1 до PC8)

3. В разделе Source Settings (Настройки источника) необходимо установить флажок Auto Select Port (Автовыбор порта), а в разделе PDU Settings (настройки IP-пакета) задать следующие значения параметров этого поля:

Select application: PING

Destination: IPAddress: 192.168.0.8 (адрес получателя);

Source IP Address: 192.168.0.1 (адрес отправителя);

Практическая работа 3. Сети с топологией звезда

=====

TTL: 32 (время жизни пакета). Наличие этого параметра не позволяет пакету бесконечно ходить по сети. TTL уменьшается на единицу на каждом узле (хопе), через который проходит пакет;

TOS: 0 (тип обслуживания, "0" - обычный, без приоритета);

Sequence Number: 1 (начальное значение счетчика пакетов);

Size: 1400 (размер поля данных пакета в байтах);

Simulations Settings - здесь необходимо активировать переключатель;

Periodic Interval: 0.3 Seconds (период повторения пакетов)

Замечание

Не обязательно использовать те настройки, которые здесь приведены. Можете указать свои, например, **Size: 1500**, **PeriodicInterval: 0.5 Seconds**. Однако, если неверно укажете IP источника, то генератор работать не будет.

4. После нажатия на кнопку Send (Послать) между PC1 и PC8 начнется активный обмен данными. Не закрывайте окно генератора трафика настройки, чтобы не прервать поток трафика - лампочки должны постоянно мигать.

Исследование качества работы сети

5. Для оценки качества работы сети передадим поток пакетов между PC1 и PC8 при помощи команды **ping -n 200 192.168.0.8** и будем оценивать качество работы сети по числу потерянных пакетов.

Параметр "**-n**" позволяет задать количество передаваемых эхо-запросов (у нас их 200) – рисунок 3.16.

6. Одновременно с пингом, нагрузите сеть, включив генератор трафика на компьютере PC2 (узел назначения – PC8, размер поля данных 2500 байт, период повторения передачи - 0,1 сек (рисунок 3.17)).

Практическая работа 3. Сети с топологией звезда

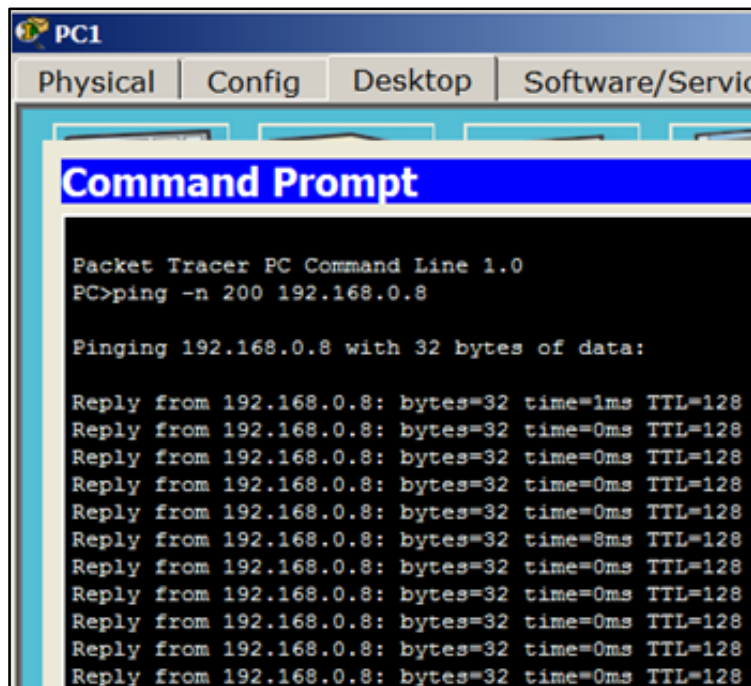


Рисунок 3.16 – Отправка 200 пакетов на PC8

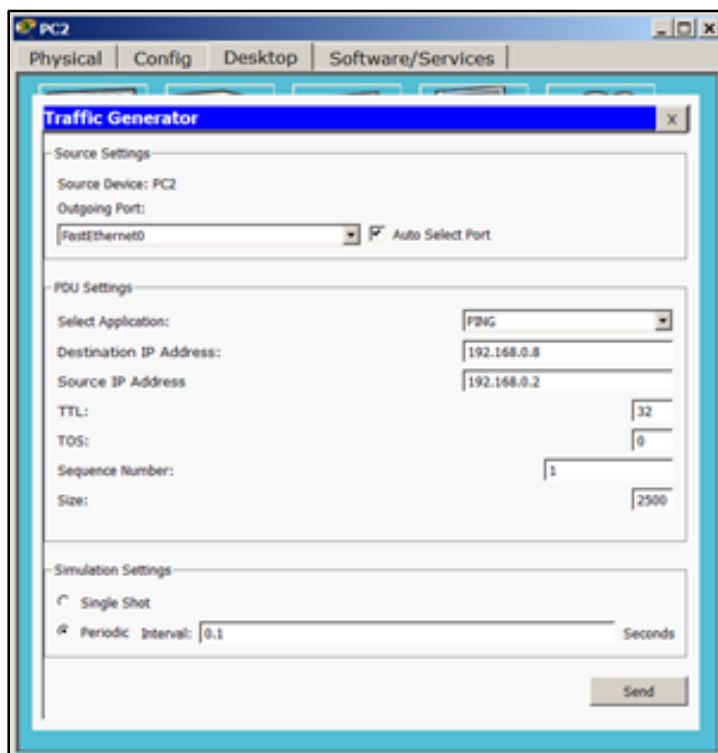
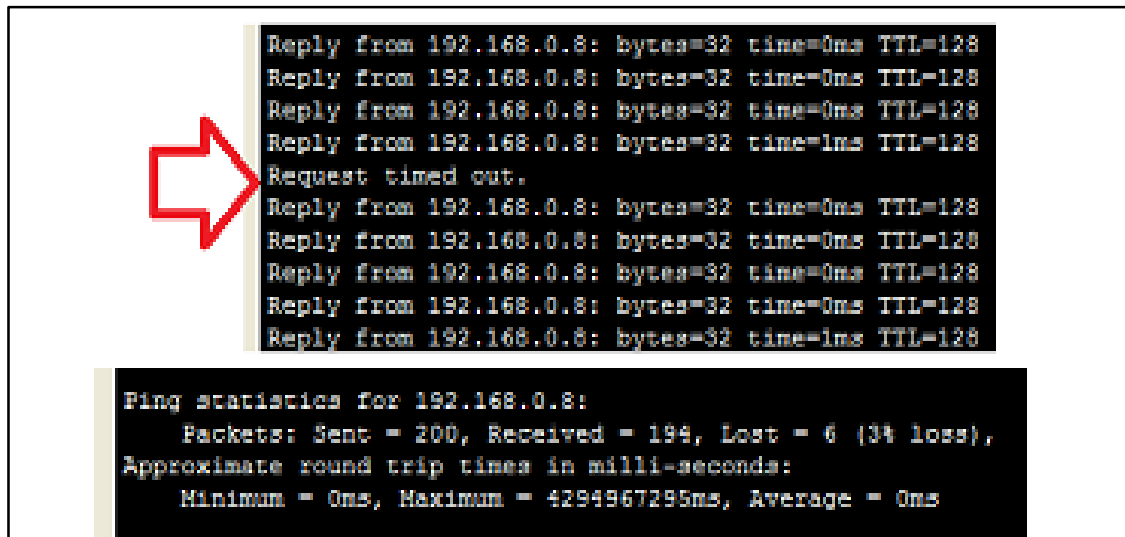


Рисунок 3.17 – Увеличение нагрузки на сеть

Практическая работа 3. Сети с топологией звезда

7. Для оценки качества работы сети - зафиксируйте число потерянных пакетов (рисунок 3.18).



```
Reply from 192.168.0.8: bytes=32 time=0ms TTL=128
Reply from 192.168.0.8: bytes=32 time=0ms TTL=128
Reply from 192.168.0.8: bytes=32 time=0ms TTL=128
Reply from 192.168.0.8: bytes=32 time=1ms TTL=128
Request timed out.
Reply from 192.168.0.8: bytes=32 time=0ms TTL=128
Reply from 192.168.0.8: bytes=32 time=0ms TTL=128
Reply from 192.168.0.8: bytes=32 time=0ms TTL=128
Reply from 192.168.0.8: bytes=32 time=0ms TTL=128
Reply from 192.168.0.8: bytes=32 time=1ms TTL=128

Ping statistics for 192.168.0.8:
    Packets: Sent = 200, Received = 194, Lost = 6 (3% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 4294967295ms, Average = 0ms
```

Рисунок 3.18 – Потеряно 6 пакетов

Замечание

Как вариант можно было бы загрузить сеть путем организации еще одного потока трафика между какими-либо узлами сети, например, включив генератор трафика еще на РСЗ.

8. Остановите Traffic Generator на всех узлах, нажав кнопку Stop.

Повышение пропускной способности локальной вычислительной сети

9. Проверим тот факт, что установка коммутаторов вместо хабов устраняет возможность возникновения коллизий между пакетами пользователей сети. Замените центральный концентратор на коммутатор (рисунок 3.19).

Убедитесь, что сеть находится в рабочем состоянии - все маркеры портов не красные, а зеленые.

Практическая работа 3. Сети с топологией звезда

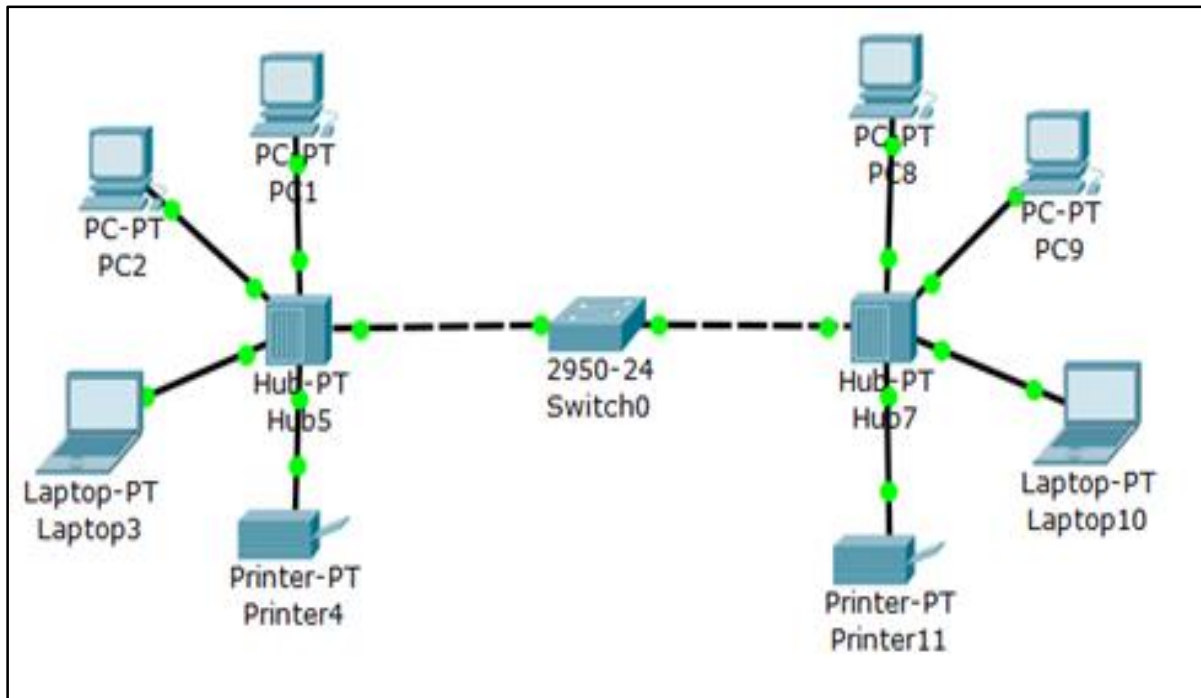


Рисунок 3.19 – Топология сети при замене центрального концентратора на коммутатор

10. Снова задайте поток пакетов между PC1 и PC8 при помощи команды **ping -n 200 192.168.0.8** и включите Traffic Generator на PC2.

11. Проследите работу нового варианта сети. Убедитесь, что за счет снижения паразитного трафика качество работы сети стало выше (рисунок 3.20).

```
Ping statistics for 192.168.0.8:  
Packets: Sent = 200, Received = 199, Lost = 1 (1% loss),  
Approximate round trip times in milli-seconds:  
Minimum = 0ms, Maximum = 4294967295ms, Average = 0ms
```

Рисунок 3.20 – Потерян 1 пакет

Практическая работа 3. Сети с топологией звезда

=====

Контрольные вопросы

1. Перечислите достоинства звезды как топологии сети
2. Перечислите недостатки звезды как топологии сети
3. Прокомментируйте особенности построения сети с топологией звезды на Hube
4. Прокомментируйте особенности построения сети с топологией звезды на Switch
5. В сетях IP существует 3 основных способа передачи данных. Назовите их

Задания

Задание 3.1

Выполните на своем компьютере все упражнения. Отчет должен содержать скриншоты с экрана вашего компьютера, позволяющие судить о том, что основные результаты последовательного выполнения упражнений выполнены корректно и в надлежащей последовательности.

Задание 3.2

Произведите проектирование локальной сети из хаба, коммутатора и четырех ПК (рисунок 3.21).

Произведите настройку и диагностику этой сети двумя способами (утилитой ping и в окне списка PDU. Убедитесь в успешности работы сети в режиме симуляции.

Замечание

Перед выполнением симуляции необходимо задать фильтрацию пакетов. Для этого нужно нажать на кнопку "Изменить фильтры", откроется окно, в котором нужно оставить только протоколы "ICMP" и "ARP". Кнопка "Автозахват/Воспроизведение" подразумевает моделирование всего ping-процесса в едином процессе, тогда как "Захват/Вперед" позволяет отображать его пошагово.

Практическая работа 3. Сети с топологией звезда

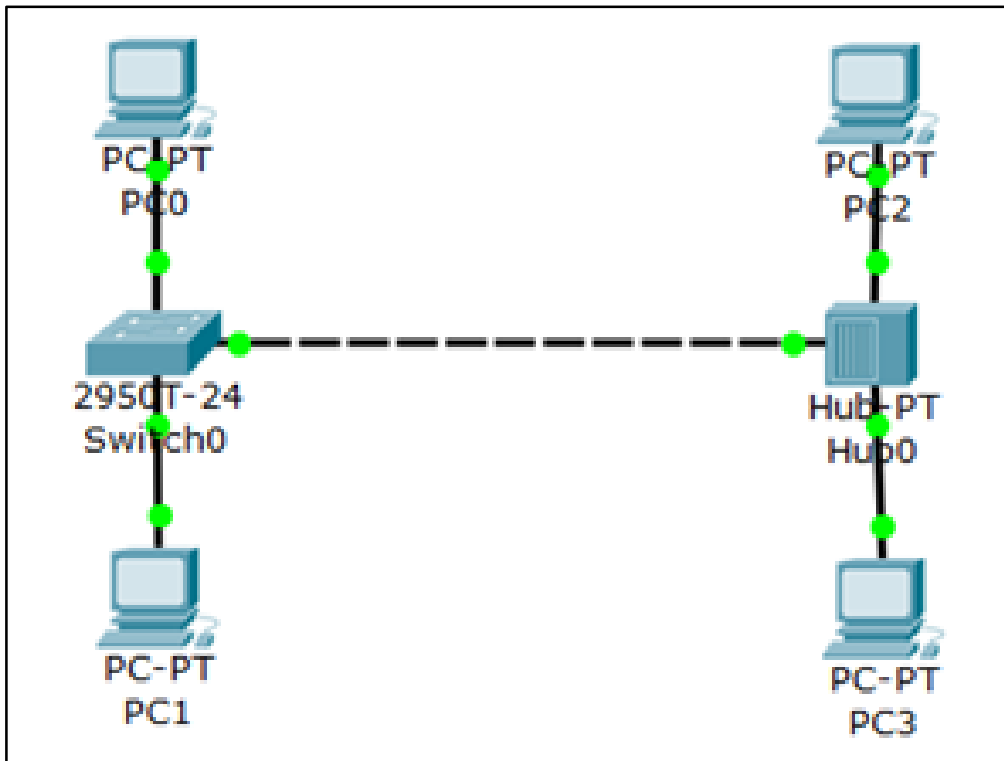


Рисунок 3.21 – Проектируемая сеть

Задание 3.3

Проверьте самостоятельно, что замена не одного, а всех хабов коммутаторами существенно улучшит качество передачи трафика в сети.

Практическая работа 4. КОМАНДНАЯ СТРОКА УПРАВЛЕНИЯ УСТРОЙСТВАМИ И РЕЖИМ СИМУЛЯЦИИ

Цель работы – приобретение практических навыков обучающимся в работе с командной строкой управления устройствами.

Порядок выполнения работы – внимательно изучите теоретический материал, выполните упражнения, включённые в данный раздел в пошаговом режиме. Если в промежуточных точках изображения Ваших моделей не совпадает с приводимыми в практикуме, вернитесь на 2-3 шага назад и все-таки добейтесь абсолютного соответствия. Самостоятельно выполните задания к практической работе.

4.1. Командная строка управления устройствами CLI

Краткая теория [3-5, 11-15]

Интерфейс командной строки (Command line interface, CLI) — разновидность текстового интерфейса между человеком и компьютером, в котором инструкции компьютеру даются в основном путём ввода с клавиатуры текстовых строк (команд), в UNIX-системах возможно применение мыши. Также известен под названиями «консоль» и «терминал».

Интерфейс командной строки противопоставляется системам управления программой на основе меню, а также различным реализациям графического интерфейса.

Формат вывода информации в интерфейсе командной строки не регламентируется; обычно это также простой текстовый вывод, но может быть и графическим.

Консоль

Большинство сетевых устройств компании CISCO допускают конфигурирование. Для этого администратор сети должен подклю-

Практическая работа 4. Командная строка и режим симуляции

=====
чаться к устройству через прямое кабельное (консольное) подключение (рисунок 4.1).

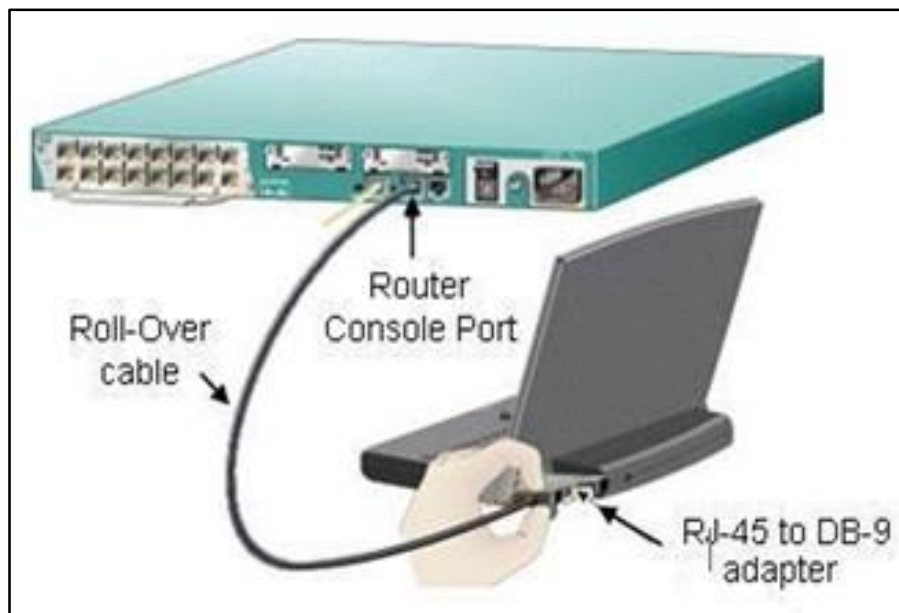


Рисунок 4.1 - Консольное подключение к сетевому устройству

Программирование устройств CISCO чаще всего производят через консольный порт *RJ-45*.

Классический консольный кабель имеет разъем DB9 для подключения к СОМ-порту компьютера и разъем RJ-45 для подключения к консольному порту маршрутизатора. Сейчас Cisco активно продвигает новые маршрутизаторы ISR G3 и т.д. В них предусмотрена возможность конфигурирования через USB-интерфейс (используются обычные USB-кабели).

Подключив консоль и получив доступ к устройству через командную строку, пользователь (администратор сети) может задавать различные команды и, тем самым, определять параметры конфигурации оборудования.

Маршрутизатор конфигурируется в командной строке операционной системы Cisco IOS. Подсоединение к маршрутизатору осуществляется через Telnet на IP-адрес любого из его интерфейсов или с помощью любой терминальной программы через последовательный порт компьютера, связанный с консольным портом маршрутизатора.

Практическая работа 4. Командная строка и режим симуляции

=====

Последний способ предпочтительнее, потому что процесс конфигурирования маршрутизатора может изменять параметры IP-интерфейсов, что приведет к потере соединения, установленного через Telnet.

При работе в командной строке Cisco IOS существует несколько контекстов (режимов ввода команд).

Контекст пользователя открывается при подсоединении к маршрутизатору; обычно при подключении через сеть требуется пароль, а при подключении через консольный порт пароль не нужен. В этот же контекст командная строка автоматически переходит при продолжительном отсутствии ввода в контексте администратора. В контексте пользователя доступны только простые команды (некоторые базовые операции для мониторинга), не влияющие на конфигурацию маршрутизатора. Вид приглашения командной строки:

```
router>
```

Вместо слова **router** выводится имя маршрутизатора, если оно установлено.

Контекст администратора (контекст "**exec**") открывается командой **enable**, поданной в контексте пользователя; при этом обычно требуется пароль администратора. В контексте администратора доступны команды, позволяющие получить полную информацию о конфигурации маршрутизатора и его состоянии, команды перехода в режим конфигурирования, команды сохранения и загрузки конфигурации. Вид приглашения командной строки:

```
router#
```

Обратный переход в контекст пользователя производится по команде **disable** или по истечении установленного времени неактивности. Завершение сеанса работы - команда **exit**.

Практическая работа 4. Командная строка и режим симуляции

=====

Глобальный контекст конфигурирования открывается командой **config terminal** ("конфигурировать через терминал"), поданной в контексте администратора. Глобальный контекст конфигурирования содержит как непосредственно команды конфигурирования маршрутизатора, так и команды перехода в контексты конфигурирования подсистем маршрутизатора, например:

- контекст конфигурирования интерфейса открывается командой **interface имя_интерфейса** (например, **interface serial0**), поданной в глобальном контексте конфигурирования;

- контекст конфигурирования процесса динамической маршрутизации открывается командой **router протокол номер_процесса** (например, **router ospf 1**, поданной в глобальном контексте конфигурирования).

Существует множество других контекстов конфигурирования. Некоторые контексты конфигурирования находятся внутри других контекстов конфигурирования.

Вид приглашения командной строки в контекстах конфигурирования, которые будут встречаться наиболее часто:

```
router(config)# /глобальный/  
router(config-if)# /интерфейса/  
router(config-router)# /динамической маршру-  
тизации/  
router(config-line)# /терминальной линии/
```

Запомните вид приглашений командой строки во всех вышеуказанных контекстах и правила перехода из контекста в контекст. В дальнейшем примеры команд всегда будут даваться вместе с приглашениями, из которых надо определять контекст, в котором подается команда.

Примеры не будут содержать указаний, как попасть в необходимый контекст.

Выход из глобального контекста конфигурирования в контекст администратора, а также выход из любого подконтекста конфигурирования в контекст верхнего уровня производится командой **exit** или **Ctrl-Z**.

Практическая работа 4. Командная строка и режим симуляции

=====

Кроме того, команда **end**, поданная в любом из контекстов конфигурирования немедленно завершает процесс конфигурирования и возвращает оператора в контекст администратора.

Любая команда конфигурации вступает в действие немедленно после ввода, а не после возврата в контекст администратора.

Все команды и параметры могут быть сокращены (например, "**enable**" - "**en**", "**configure terminal**" - "**conf t**"); если сокращение окажется неоднозначным, маршрутизатор сообщит об этом, а по нажатию табуляции выдаст варианты, соответствующие введенному фрагменту.

В любом месте командной строки для получения помощи может быть использован вопросительный знак:

router#? /список всех команд данного контекста с комментариями/

router#co? /список всех слов в этом контексте ввода, начинающихся на "co" - нет пробела перед "?"/

router#conf? /список всех параметров, которые могут следовать за командой **config** - перед "?" есть пробел/

4.2. Список команд

Данный список команд сгруппирован в соответствии с контекстами, в котором они применяются. В данном списке собраны те команды конфигурирования, которые необходимы для выполнения всех работ.

Глобальный контекст конфигурирования

Команда «Access-list»

Критерии фильтрации задаются в списке операторов разрешения и запрета, называемом списком доступа. Строки списка доступа сравниваются с IP-адресами и другой информацией пакета данных последовательно в том порядке, в котором были заданы, пока не будет найдено совпадение. При совпадении осуществляется выход из

Практическая работа 4. Командная строка и режим симуляции

=====

списка. При этом работа списка доступа напрямую зависит от порядка следования строк.

Списки доступа имеют 2 правила: **permit** – разрешить, и **deny** – запретить. Именно они определяют, пропустить пакет дальше или запретить ему доступ.

Списки доступа бывают 2-ух типов: **standard** – стандартные (номера с 1 до 99) и **extended** – расширенные (номера с 100 до 199). Различия заключаются в возможности фильтровать пакеты не только по ip-адресу, но и по другим параметрам.

Формат команды (стандартные списки доступа):

```
access-list номер_списка/имя правило A.B.C.D  
a.b.c.d ,
```

где **A.B.C.D a.b.c.d** – IP-адрес и подстановочная маска соответственно.

Пример выполнения команды:

```
Router(config)#access-list 10 deny 192.168.3.0  
0.0.0.3  
Router(config)#
```

Данная команда означает, что данный список доступа блокирует любые пакеты с IP-адресами 192.168.3.1 - 192.168.3.3.

Команда «**Enable secret**»

Обычно при входе в привилегированный режим требуется ввести пароль. Данная функция позволяет предотвратить несанкционированный доступ в данный режим, ведь именно из него можно изменять конфигурацию устройства. Данная команда позволяет установить такой пароль.

Формат команды:

```
enable secret пароль  
Router(config)#access-list 10 deny 192.168.3.0  
0.0.0.3
```

Практическая работа 4. Командная строка и режим симуляции

Router (config) #

Пример выполнения команды:

```
Switch (config)#enable secret 123
Switch (config)#
%SYS-5-CONFIG_I: Configured from console by
  console
Switch#exit
Switch con0 is now available
Press RETURN to get started.
Switch> enable
Password:
Switch#
```

После того, как был установлен пароль, при попытке входа в привилегированный режим, коммутатор будет требовать от пользователя его ввести

– в противном случае вход будет невозможен.

Команда «**Interface**»

Команда для входа в режим конфигурирования интерфейсов конфигурируемого устройства. Данный режим представляет собой одно из подмножеств режима глобального конфигурирования и позволяет настраивать один из доступных сетевых интерфейсов (fa 0/0, s 2/0 и т.д.). Все изменения, вносимые в конфигурацию коммутатора в данном режиме, относятся только к выбранному интерфейсу.

Формат команды (возможны 3 варианта):

```
interface тип порт
interface тип слот/порт
interface тип слот/подслот/порт
```

Примеры выполнения команды:

```
Switch(config)#interface vlan 1
Switch (config-if) #
```


Практическая работа 4. Командная строка и режим симуляции

```
Router (config) #interface s 3/0
Router(config-if) #
```

После введения данной команды с указанным интерфейсом пользователь имеет возможность приступить к его конфигурированию. Необходимо заметить, что, находясь в режиме конфигурирования интерфейса, вид приглашения командной строки не отображает имя данного интерфейса.

Команда «**Ip route**»

Статическая маршрутизация предполагает фиксированную структуру сети: каждый маршрутизатор в сети точно знает, куда нужно отправлять пакет, чтобы он был доставлен по назначению. Для этого можно прописать статические маршруты, используя данную команду. Команда может быть записана в двух форматах:

Первый формат команды:

```
ip route A.B.C.D a.b.c.d A1.B1.C1.D1 ,
```

где **A.B.C.D** и **a.b.c.d** – сетевой адрес и маска подсети, куда необходимо доставить пакеты,

A1 . B1 . C1 . D1 – IP-адрес следующего маршрутизатора в пути или адрес сети другого маршрутизатора из таблицы маршрутизации, куда должны переадресовываться пакеты.

Второй формат команды:

```
ip route A.B.C.D a.b.c. d выход-  
ной_интерфейс_текущего_маршрутизатора
```

Примеры выполнения команды:

```
Router(config)#ip route 76.115.253.0 255.0.0.0  
76.115.252.0  
Router (config) #  
Router (config) #ip route 0.0.0.0 0.0.0.0 Se-  
rial2/0  
Router(config) #
```

Практическая работа 4. Командная строка и режим симуляции

=====

Данной командой указывается маршрут, по которому пакеты из одной подсети будут доставляться в другую. Маршрут по умолчанию (**Router(config)#ip route 0.0.0.0 0.0.0.0 serial 2/0**) указывает, что пакеты, предназначенные узлам в другой подсети должны отправляться через данный шлюз.

Команда «**Hostname**»

Данная команда используется для изменения имени конфигурируемого устройства.

Формат команды:

```
hostname новое_имя
Router (config) #ip route 76.115.253.0
255.0.0.0 76.115.252.0
Router (config) #
Router (config) #ip route 0.0.0.0 0.0.0.0 Se-
rial2/0
Router(config) #
```

Пример выполнения команды:

```
Router (config) #hostname R1
R1 (config) #
```

Как видно, маршрутизатор поменял своё имя с **Router** на **R1**.

Команда «**Router rip**»

RIP – Routing Information Protocol – протокол динамической маршрутизации. При его использовании отпадает необходимость вручную прописывать все маршруты – необходимо лишь указать адреса сетей, с которыми нужно обмениваться данными. Данная команда позволяет включить rip-протокол.

Пример выполнения команды:

```
Router(config)#router rip
Router(config-router) #
```

Практическая работа 4. Командная строка и режим симуляции

Данная команда включает rip-протокол на данном маршрутизаторе. Дальнейшая настройка производится из соответствующего контекста маршрутизации, описанного отдельно.

Контекст конфигурирования интерфейса

Команда «Ip access-group»

Данная команда используется для наложения списков доступа. Список накладывается на конкретный интерфейс, и указывается один из 2-ух параметров: **in** (на входящие пакеты) или **out** (на исходящие). Необходимо знать, что на каждом интерфейсе может быть включен только один список доступа.

Формат команды:

```
ip access-group номер_списка/имя_параметр
```

Пример выполнения команды:

```
Router (config-if) # ip access group 10 in  
Router(config-if) #
```

В данном примере на выбранный интерфейс накладывается список доступа под номером 10: он будет проверять все входящие в интерфейс пакеты, так как выбран параметр **in**.

Команда «Bandwidth»

Данная команда используется только в последовательных интерфейсах и служит для установки ширины полосы пропускания. Значение устанавливается в килобитах.

Формат команды:

```
bandwidth ширина_полосы_пропускания
```

Практическая работа 4. Командная строка и режим симуляции

Пример выполнения команды:

```
Router (config) #interface serial 2/0
Router (config-if) #bandwidth 560
Router (config-if) #
```

После выполнения данной команды ширина полосы пропускания для serial 2/0 будет равна 560 kbits.

Команда «**Clock rate**»

Для корректной работы участка сети, где используется последовательный сетевой интерфейс, один из коммутаторов 3-его уровня должен предоставлять тактовую частоту. Это может быть оконечное кабельное устройство DCE. Так как маршрутизаторы CISCO являются по умолчанию устройствами DTE, то необходимо явно указать интерфейсу на предоставление тактовой частоты, если этот интерфейс работает в режиме DCE. Для этого используют данную команду (значение устанавливается в битах в секунду).

Формат команды:

```
clock rate тактовая_частота
```

Пример выполнения команды:

```
Router (config) #interface serial 2/0
Router (config-if) #clock rate 56000
Router (config-if) #
```

После выполнения данной команды тактовая частота для serial 2/0 будет равна 56000 bits per second.

Команда «**Ip address**»

Каждый интерфейс должен обладать своим уникальным ip-адресом – иначе взаимодействие устройств по данному интерфейсу не сможет быть осуществлено.

Практическая работа 4. Командная строка и режим симуляции

Данная команда используется для задания IP-адреса выбранному интерфейсу.

Формат команды:

```
ip address A.B.C.D a.b.c.d ,
```

где **A.B.C.D a.b.c.d** – IP-адрес и маска подсети соответственно.

Пример выполнения команды:

```
Switch (config) #interface vlan 1
Switch (config-if) #ip address 172.16.10.5
255.255.0.0
Switch (config-if) #
```

Результат можно проверить командой

```
Switch#show ip interface vlan 1
```

Данной командой интерфейсу **vlan 1** назначен IP-адрес 172.16.10.5 с маской подсети 255.255.0.0.

Команда «**No**»

Данная команда применяется в случае необходимости отменить действие какой-либо команды конфигурирования.

Формат команды:

```
no команда_которую_следует_отменить
```

Пример выполнения команды:

```
Switch (config-if)# no shutdown
%LINK-5-CHANGED: Interface Vlan1, changed
state to up
%LINEPROTO-5-UPDOWN: Line protocol on Inter-
face Vlan1, changed state to up
Switch(config-if) #
```

Практическая работа 4. Командная строка и режим симуляции

=====

В данном примере использовалась команда **shutdown**, которая отключает выбранный интерфейс. В итоге после выполнения **no shutdown** интерфейс включается.

Контекст администратора

Команда «**Configure terminal**»

Для конфигурирования устройства, работающего под управлением IOS, следует использовать привилегированную команду **configure**. Эта команда переводит контекст пользователя в так называемый «режим глобальной конфигурации» и имеет три варианта:

- конфигурирование с терминала;
- конфигурирование из памяти;
- конфигурирование через сеть.

В рамках данного курса конфигурирование будет производиться только посредством терминала.

Из режима глобальной конфигурации можно делать изменения, которые касаются устройства в целом. Также данный режим позволяет входить в режим конфигурирования определенного интерфейса.

Пример выполнения команды:

```
Router#configure terminal
Enter configuration commands, one per line.
End with CNTL/Z.
Router (config) #
```

Переход в режим глобальной конфигурации, о чем свидетельствует изменившийся вид приглашения командной строки.

Команда «**Copy**»

После настройки коммутатора рекомендуется сохранять его текущую конфигурацию. Информация помещается в энергонезависимую память и хранится там столько, сколько нужно. При необходимости все настройки могут быть восстановлены или сброшены.

Практическая работа 4. Командная строка и режим симуляции

Формат команды:

copy running-config startup-config – команда для сохранения конфигурации

copy startup-config running-config – команда для загрузки конфигурации

Пример выполнения команды:

```
Switch#copy running-config startup-config
Building configuration...
[OK]
Switch#
```

В данном примере текущая конфигурация коммутатора была сохранена в энергонезависимую память.

Команда «**Show**»

Show (показывать) – одна из наиболее важных команд, используемых при настройке коммутаторов. Она применяется для просмотра информации любого рода и применяется практически во всех контекстах. Эта команда имеет больше всех параметров.

Здесь будут рассмотрены только те параметры, которые требуются в рамках данного курса. Другие параметры студент может изучить самостоятельно.

Параметр «**running-config**» команды «**Show**»

Для просмотра текущей работающей конфигурации коммутатора используется данная команда.

Пример выполнения команды:

```
Switch#show running-config
!
version 12.1
!
hostname Switch
...
```

Практическая работа 4. Командная строка и режим симуляции

На экран выводится текущие настройки коммутатора.

Параметр **«startup-config»** команды **«Show»**

Для просмотра сохраненной конфигурации используется данная команда.

Пример выполнения команды:

```
Switch#show startup-config
Using 1540 bytes
!
version 12.1
!
...
```

Если энергонезависимая память не содержит информации, тогда коммутатор выдаст сообщение о том, что конфигурация не была сохранена.

Пример выполнения команды:

```
Switch #show startup-config
startup-config is not present
Switch #
```

Вывод сообщения о том, что в памяти отсутствует какая-либо информация.

Параметр **«ip route»** команды **«Show»**

Данная команда применяется для просмотра таблицы маршрутов.

Пример выполнения команды:

```
Router#show ip route
Codes: C - connected, S - static, I - IGRP,
       R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA
       - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF
       NSSA external type 2
```


Практическая работа 4. Командная строка и режим симуляции

```
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route
Gateway of last resort is 0.0.0.0 to network 0.0.0.0
C 192.168.1.0/24 is directly connected, FastEthernet0/0
C 192.168.2.0/24 is directly connected, Serial2/0
S 192.168.3.0/24 is directly connected, Serial2/0
S 192.168.4.0/24 is directly connected, Serial2/0
S 192.168.5.0/24 is directly connected, Serial2/0
S* 0.0.0.0/0 is directly connected, Serial2/0
Router#
```

Производится вывод таблицы маршрутизации.

Параметр «**ip protocols**» команды «**Show**»

Данная команда используется для просмотра протоколов маршрутизации, включенных на данном устройстве.

Пример выполнения команды:

```
Router#show ip protocols
Routing Protocol is "rip"
Sending updates every 30 seconds, next due in 18 seconds
Invalid after 180 seconds, hold down 180, flushed after 240
Outgoing update filter list for all interfaces is not set
```

Практическая работа 4. Командная строка и режим симуляции

```
Incoming update filter list for all interfaces
  is not set
Redistributing: rip
Default version control: send version 1, re-
  ceive any version
Interface Send Recv Triggered RIP Key-chain
FastEthernet0/0 1 2 1
Serial2/0 1 2 1
Automatic network summarization is in effect
Maximum path: 4
Routing for Networks:
  192.168.1.0
  192.168.2.0
Passive Interface(s) :
Routing Information Sources:
  Gateway Distance Last Update
  192.168.2.2 120
Distance: (default is 120)
Router#
```

Выводится информация о включенных протоколах маршрутизации.

Команда «**Ping**»

Для проверки связи между устройствами сети можно использовать данную команду. Она отправляет эхо-запросы указанному узлу сети и фиксирует поступающие ответы.

Формат команды:

```
ping A.B.C.D
```

Пример выполнения команды:

```
Router#ping 77.134.25.133
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to
  77.134.25.133, timeout is 2 seconds:
..!!!
Success rate is 60 percent (3/5)
```

Практическая работа 4. Командная строка и режим симуляции

Каждый ICMP-пакет, на который был получен ответ, обозначается восклицательным знаком, каждый потерянный пакет – точкой.

Контекст пользователя

Команда «**Enable**»

Выполнение конфигурационных или управляющих команд требует вхождения в привилегированный режим, используя данную команду.

Пример выполнения команды:

```
Router> enable
Router#
```

При вводе команды маршрутизатор перешел в привилегированный режим. Для выхода из данного режима используется команда **disable** или **exit**.

Также следует отметить, что в данном контексте можно пользоваться командой **show** для просмотра некоторой служебной информации.

Контекст конфигурирования маршрутизации

Команда «**Network**»

Данной командой указывают адреса сетей, которые будут доступны данному маршрутизатору.

Формат команды:

```
network A.B.C.D ,
где A.B.C.D – адрес сети
```

Пример выполнения команды:

```
Router(config-router) #network 192.168.3.0
```

Данная команда означает, что пакеты, направленные в подсеть 192.168.3.0 будут отправляться через данный шлюз.

4.3. Практические упражнения

Упражнение 4.1. Знакомство с командами Cisco IOS

В Cisco Packet Tracer интерфейс командной строки для устройств доступен в окне настроек параметров сетевого устройства на вкладке «CLI». Это окно имитирует прямое кабельное (консольное) подключение к сетевому устройству. Работа с командной строкой (CLI) для настройки (программирования) сетевого производится с помощью команд операционной системы Cisco IOS (рисунок 4.2).

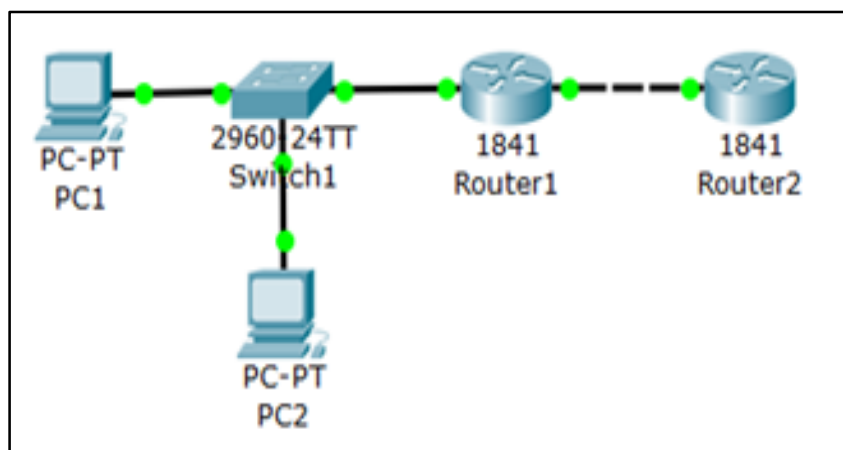


Рисунок 4.2 - Сеть для выполнения команд ОС Cisco IOS

Выше говорилось о режимах командного интерфейса – пользовательском, привилегированном и глобальной конфигурации. Прodefайте все команды входа и выхода в эти режимы для Router1. При входе в сетевое устройство Router1 и нажатии на клавишу Enter командная строка имеет вид как на рисунке 4.3. Выход из пользовательского режима – **logout**.

Практическая работа 4. Командная строка и режим симуляции

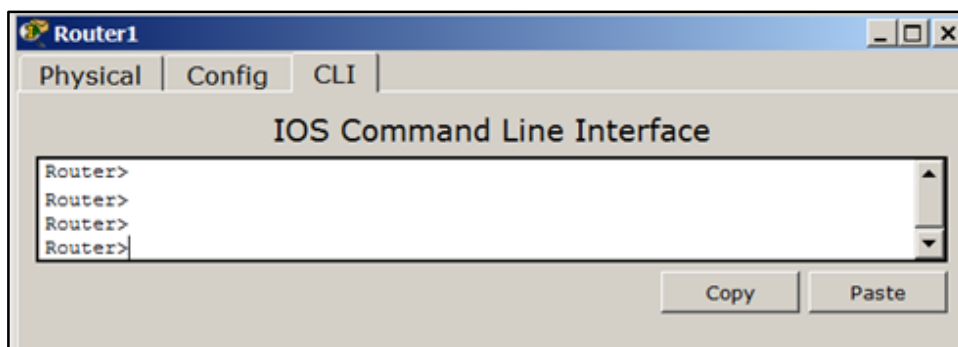


Рисунок 4.3 - Вид командной строки в пользовательском режиме

Чтобы получить доступ к полному набору команд, необходимо сначала активизировать привилегированный режим командой **enable**. О переходе в привилегированный режим будет свидетельствовать появление в командной строке приглашения в виде знака **#**. Выход из привилегированного режима производится командой **disable**.

Вместо **enable** можно было набрать **en**. Команды в любом режиме IOS распознаёт по первым уникальным символам.

Режим глобального конфигурирования реализует однострочные команды, которые решают задачи конфигурирования.

Для входа в режим глобального конфигурирования используется команда привилегированного режима **configure terminal**. Выход командой **exit** или **end**.

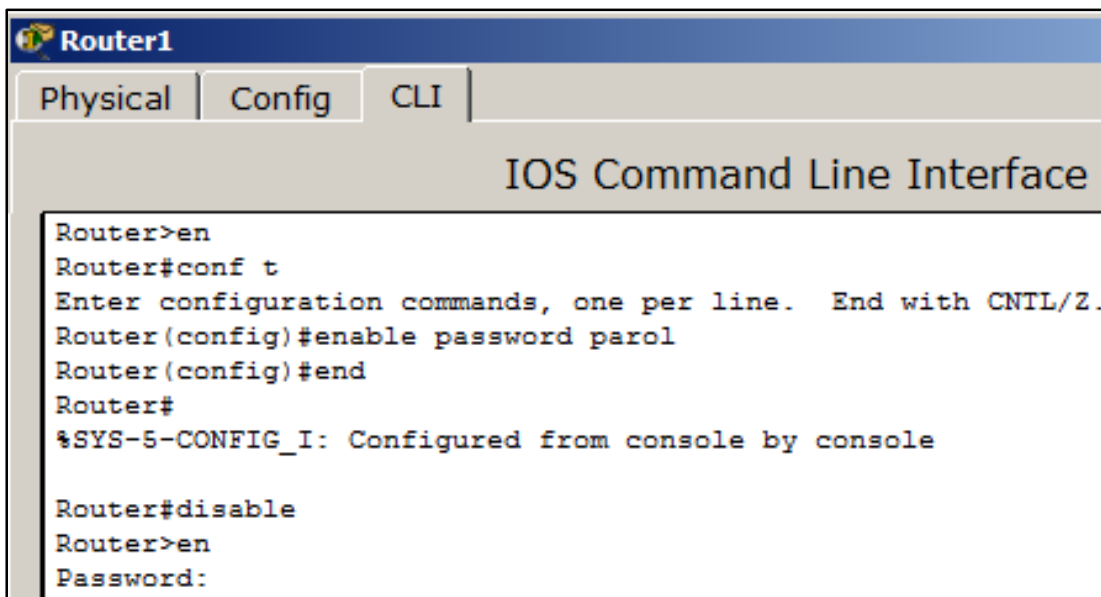
Установка пароля на вход в привилегированный режим

Пароль доступа позволяет контролировать доступ в привилегированный режим. Только в привилегированном режиме можно внести конфигурационные изменения.

1. На Router1 установите пароль доступа в этот режим как «parol» командой **Router1(config)#enable password parol**, затем выйдите из привилегированного режима сетевого устройства, то есть перейдите в пользовательский режим.

2. Попробуйте снова зайти в привилегированный режим. Как видите, без ввода пароля это теперь невозможно (рисунок 4.4).

Практическая работа 4. Командная строка и режим симуляции



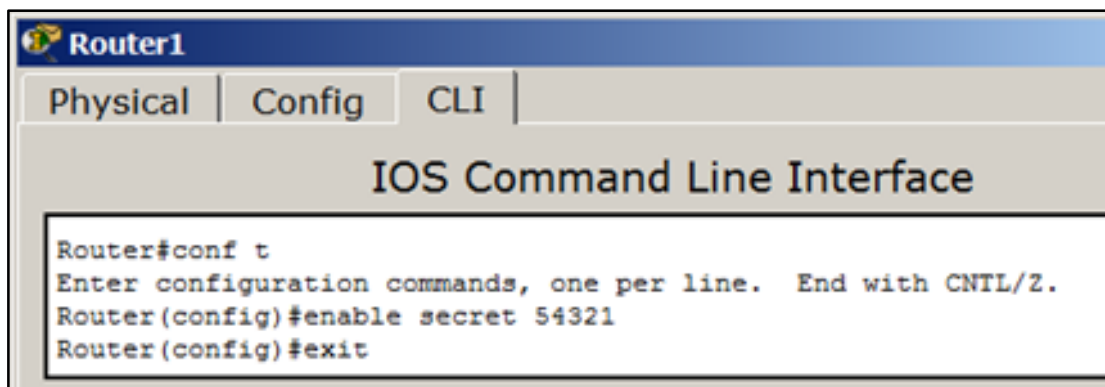
```
Router1
Physical | Config | CLI |
IOS Command Line Interface

Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#enable password parol
Router(config)#end
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#disable
Router>en
Password:
```

Рисунок 4.4 - Установка пароля на вход в привилегированный режим

3. Измените пароль. Для этого введите новый пароль привилегированного режима (рисунок 4.5).



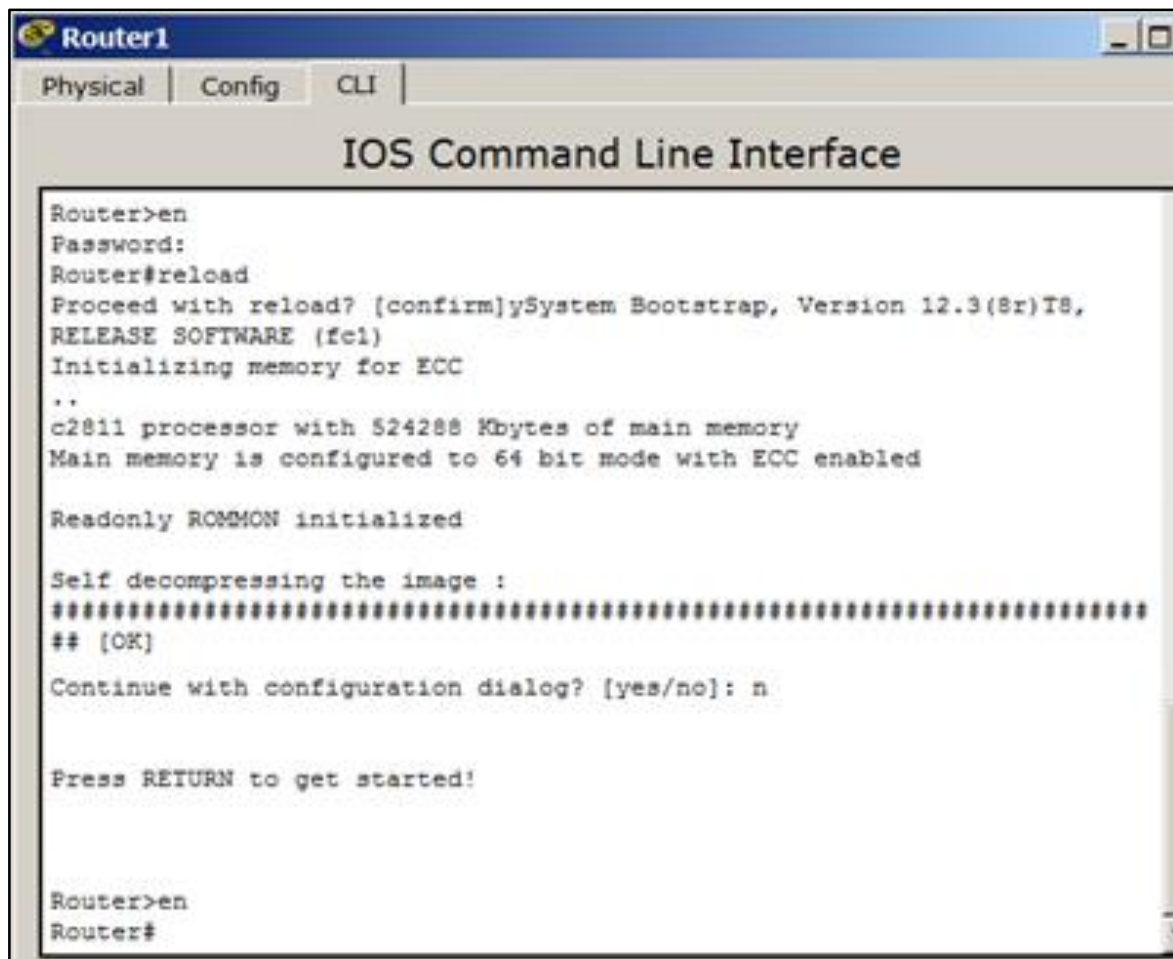
```
Router1
Physical | Config | CLI |
IOS Command Line Interface

Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#enable secret 54321
Router(config)#exit
```

Рисунок 4.5 - Был пароль 12345, стал пароль 54321

4. Для сброса пароля можно произвести перезагрузку роутера (рисунок 4.6).

Практическая работа 4. Командная строка и режим симуляции



```
Router1
Physical | Config | CLI |
IOS Command Line Interface

Router>en
Password:
Router#reload
Proceed with reload? [confirm]ySystem Bootstrap, Version 12.3(8r)T8,
RELEASE SOFTWARE (fc1)
Initializing memory for ECC
..
c2811 processor with 524288 Kbytes of main memory
Main memory is configured to 64 bit mode with ECC enabled

Readonly ROMMON initialized

Self decompressing the image :
#####
## [OK]

Continue with configuration dialog? [yes/no]: n

Press RETURN to get started!

Router>en
Router#
```

Рисунок 4.6 - Перезагрузка R1 командой reload

Советы при работе с CLI

Все команды в консоли можно сокращать, но важно, чтобы сокращение однозначно указывало на команду. Используйте клавишу Tab и знак вопроса (?). По нажатию Tab сокращенная команда дописывается до полной, а знак вопроса (?), следующий за командой, выводит список дальнейших возможностей и небольшую справку по ним. Можно перейти к следующей команде, сохранённой в буфере. Для этого нажмите на Стрелку вниз или Ctrl + N. Можно вернуться к командам, введённым ранее. Нажмите на Стрелку вверх или Ctrl + P.

Активная конфигурация автоматически не сохраняется и будет потеряна в случае сбоя электропитания. Чтобы сохранить настройки роутера используйте команду **write memory** (рисунок 4.7).

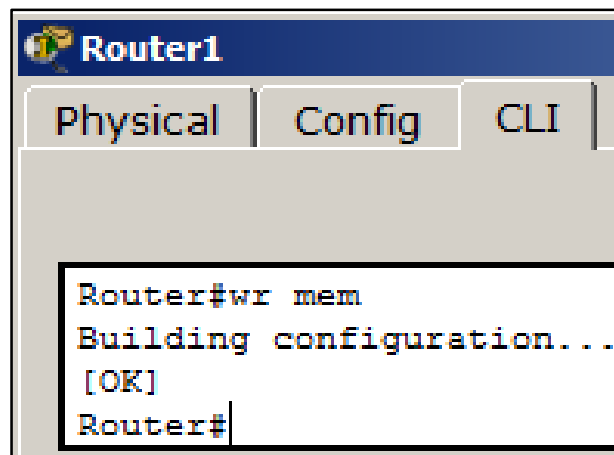


Рисунок 4.7 - Сохранение текущей конфигурации R1

4.4. Режим симуляции в Cisco Packet Tracer

Краткая теория [22, 23]

Cisco Packet Tracer содержит режим симуляции работы сети, в котором можно имитировать сетевые события. В основе функционирования режима лежит использование протокола ICMP.

ICMP (Internet Control Message Protocol — протокол межсетевых управляющих сообщений¹⁾) — сетевой протокол, входящий в стек протоколов TCP/IP. В основном ICMP используется для передачи сообщений об ошибках и других исключительных ситуациях, возникших при передаче данных, например, запрашиваемая услуга недоступна, или хост, или маршрутизатор не отвечают. Также на ICMP возлагаются некоторые сервисные функции.

Протокол ICMP описал в RFC 792 от 1981 года Jon Postel (с дополнениями в RFC 950). ICMP является стандартом Интернета (входит в стандарт STD 5 вместе с IP). Хотя формально протокол использует IP (ICMP-пакеты инкапсулируются в IP пакеты), он является неотъемлемой частью IP и обязателен при реализации стека TCP/IP. Текущая версия ICMP для IPv4 называется ICMPv4. В IPv6 существует аналогичный протокол ICMPv6.

ICMP-сообщение строится из IP-пакетов, сгенерировавших ICMP-ответ. Протокол IP инкапсулирует соответствующее ICMP-

Практическая работа 4. Командная строка и режим симуляции

=====

сообщение с новым заголовком IP (чтобы отправить ICMP-сообщение обратно отправителю) и передает полученные пакеты дальше.

Например, каждая машина (такая, как маршрутизатор), которая перенаправляет IP-пакеты, уменьшает Time to live (TTL) поля заголовка IP на единицу, если TTL достигает 0, ICMP-сообщение о превышении TTL отправляется на источник пакета.

ICMP основан на протоколе IP. Каждое ICMP-сообщение инкапсулируется непосредственно в пределах одного IP-пакета, и, таким образом, как и UDP и в отличие от TCP, ICMP является т. н. «ненадежным» (не контролирующим доставку и её правильность). В отличие от UDP, где реализация надёжности возложена на ПО прикладного уровня, ICMP (в силу специфики применения) обычно не нуждается в реализации надёжной доставки. Его цели отличны от целей транспортных протоколов, таких как TCP и UDP: он, как правило, не используется для передачи и приёма данных между конечными системами. ICMP не используется непосредственно в приложениях пользователей сети (исключение составляют инструменты Ping и Traceroute). Тот же Ping, например, служит обычно как раз для проверки потерь IP-пакетов на маршруте.

Упражнение 4.2. Режим симуляции работы сети

1. Сформируйте в рабочем пространстве программы сеть из четырех ПК и двух хабов. Задайте для ПК IP-адреса и маску сети 255.255.255.0 (рисунок 4.8).

2. Эту схему сохраните в виде картинки с расширением *PNG командой File-Print-Print to file.

Практическая работа 4. Командная строка и режим симуляции

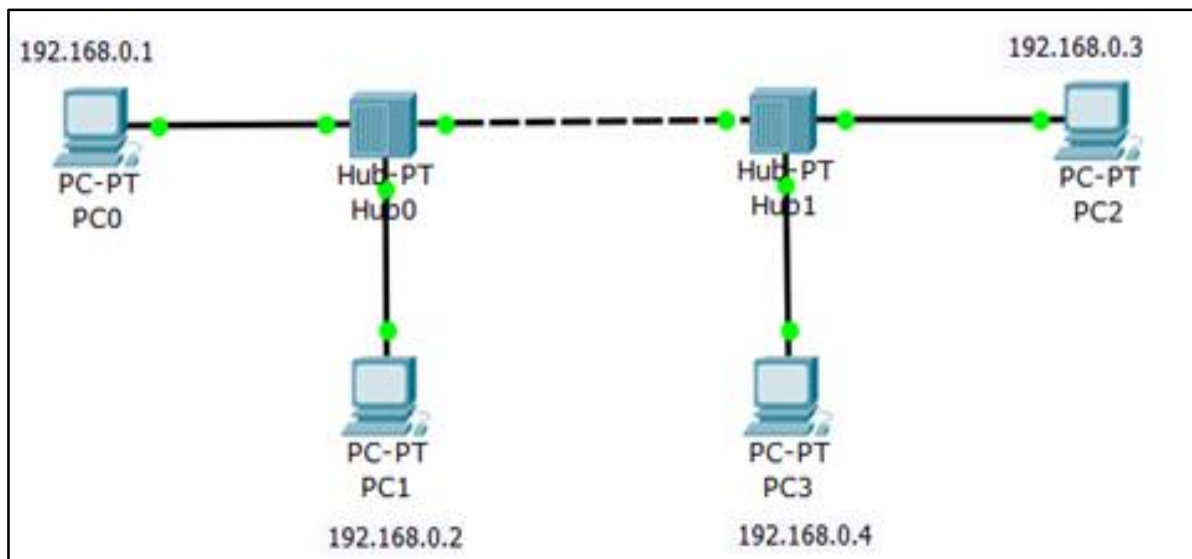


Рисунок 4.8 - Сеть из четырех ПК и двух хабов. Все ПК расположены в одной сети

3. Перейдите в режим симуляции комбинацией клавиш Shift+S, или, щелкнув мышью на иконку симуляции в правом нижнем углу рабочего пространства (рисунок 4.9).

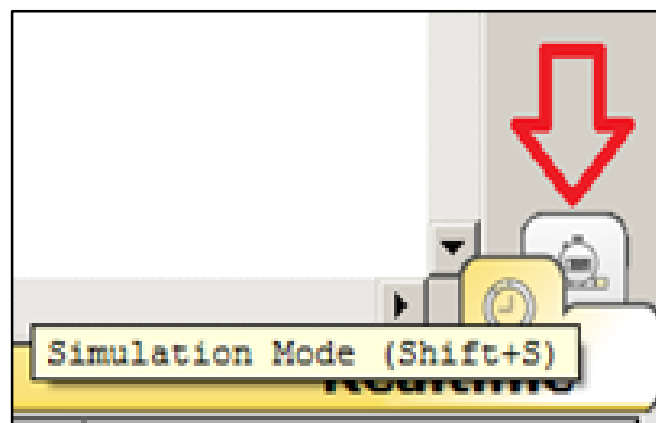


Рисунок 4.9 - Кнопка Симуляция

4. Нажмите на кнопку **Edit Filters** (Изменить фильтры) и исключите все сетевые протоколы, кроме ICMP (рисунок 4.10).

Практическая работа 4. Командная строка и режим симуляции

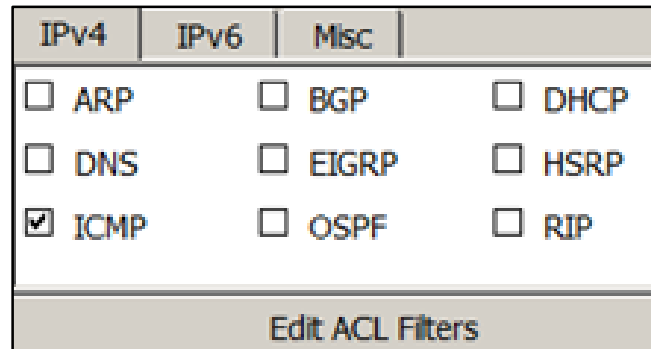


Рисунок 4.10 - Флажок ICMP активен

5. С одного из хостов пропингуем другой узел. Для этого выберем далеко расположенные друг от друга узлы для того, чтобы наглядней увидеть, как будут проходить пакеты по сети в режиме симуляции. С PC1 пингуем PC2 (рисунок 4.11).

Ping — утилита для проверки соединений в сетях на основе TCP/IP. Утилита отправляет запросы (ICMP Echo-Request) протокола ICMP указанному узлу сети и фиксирует поступающие ответы (ICMP Echo-Reply). Время между отправкой запроса и получением ответа (RTT) позволяет определять двусторонние задержки (RTT) по маршруту и частоту потери пакетов, то есть косвенно определять загруженность на каналах передачи данных и промежуточных устройствах.

Полное отсутствие ICMP-ответов может также означать, что удалённый узел (или какой-либо из промежуточных маршрутизаторов) блокирует ICMP Echo-Reply или игнорирует ICMP Echo-Request.

На PC1 образовался пакет (конвертик), который ждёт начала движения его по сети. Запустить продвижение пакет в сеть пошагово можно, нажав на кнопку **Capture / Forward** (Вперёд) в окне симуляции. Если нажать на кнопку **Auto Capture / Play** (воспроизведение), то мы увидим весь цикл прохождения пакета по сети.

В Event List (Список событий) мы можем видеть успешный результат пинга (рисунок 4.12).

Практическая работа 4. Командная строка и режим симуляции

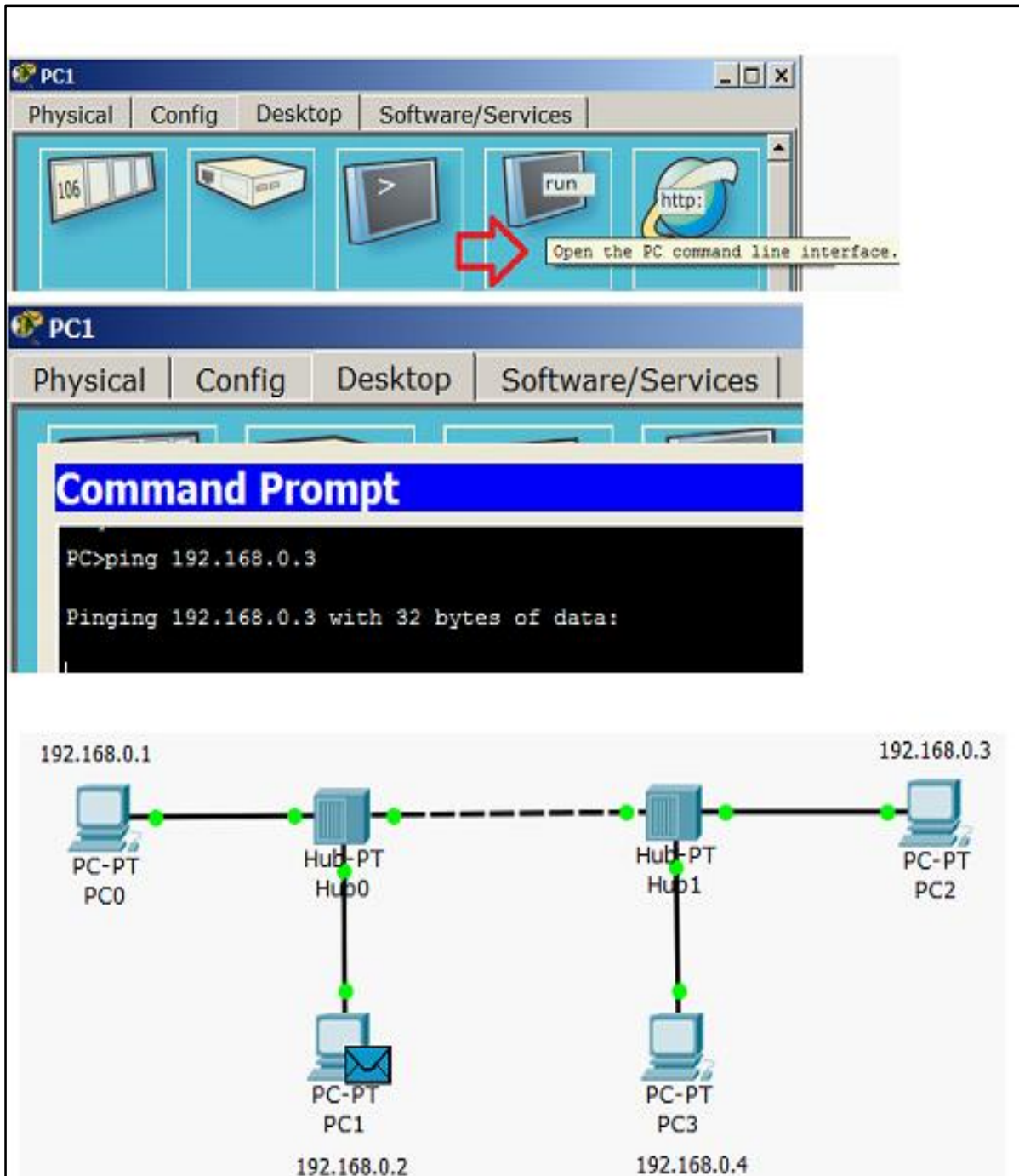
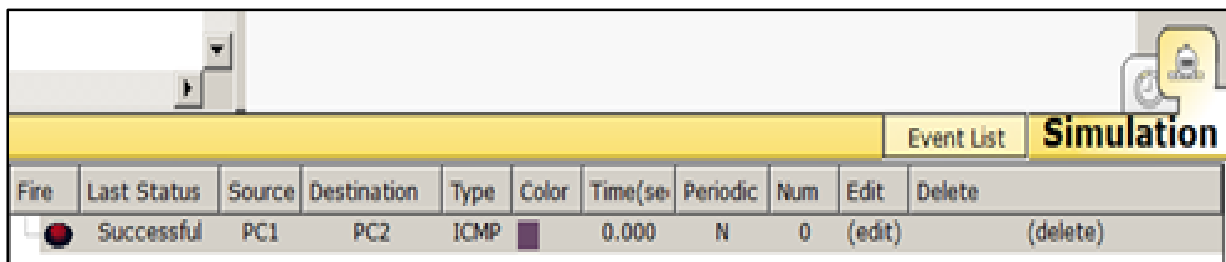


Рисунок 4.11 - PC1 пингует PC2 (начало процесса)

Практическая работа 4. Командная строка и режим симуляции



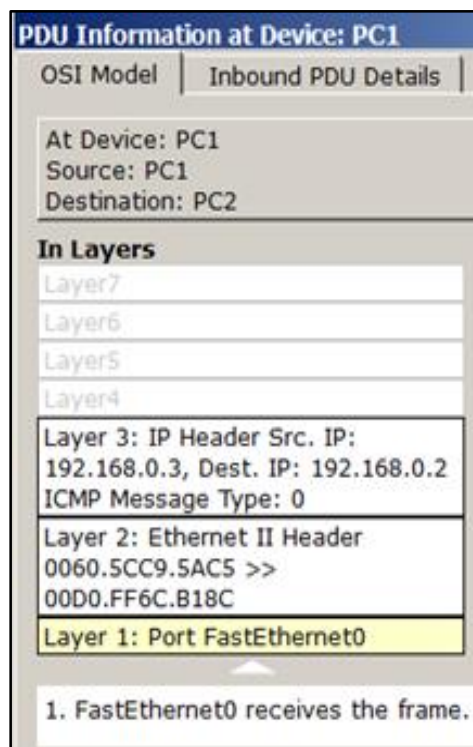
Fire	Last Status	Source	Destination	Type	Color	Time(se)	Periodic	Num	Edit	Delete
	Successful	PC1	PC2	ICMP		0.000	N	0	(edit)	(delete)

Рисунок 4.12 - В Event List успешный результат пинга. Связь PC1 и PC2 есть

Модель OSI в Cisco Packet Tracer

6. Щелчком мышью на конверте. Cisco Packet Tracer покажет дополнительную информацию о движении пакета по сети. При этом на первой вкладке мы увидим модель OSI (рисунок 4.13).

На вкладке OSI Model (Модель OSI) представлена информация об уровнях OSI, на которых работает данное сетевое устройство.



PDU Information at Device: PC1

OSI Model | Inbound PDU Details

At Device: PC1
Source: PC1
Destination: PC2

In Layers

Layer7
Layer6
Layer5
Layer4
Layer 3: IP Header Src. IP: 192.168.0.3, Dest. IP: 192.168.0.2
ICMP Message Type: 0
Layer 2: Ethernet II Header
0060.5CC9.5AC5 >>
00D0.FF6C.B18C
Layer 1: Port FastEthernet0

1. FastEthernet0 receives the frame.

Рисунок 4.13 - Мониторинг движения пакета на модели OSI

Практическая работа 4. Командная строка и режим симуляции

На другой вкладке можно посмотреть структуру пакета (рисунок 4.14).

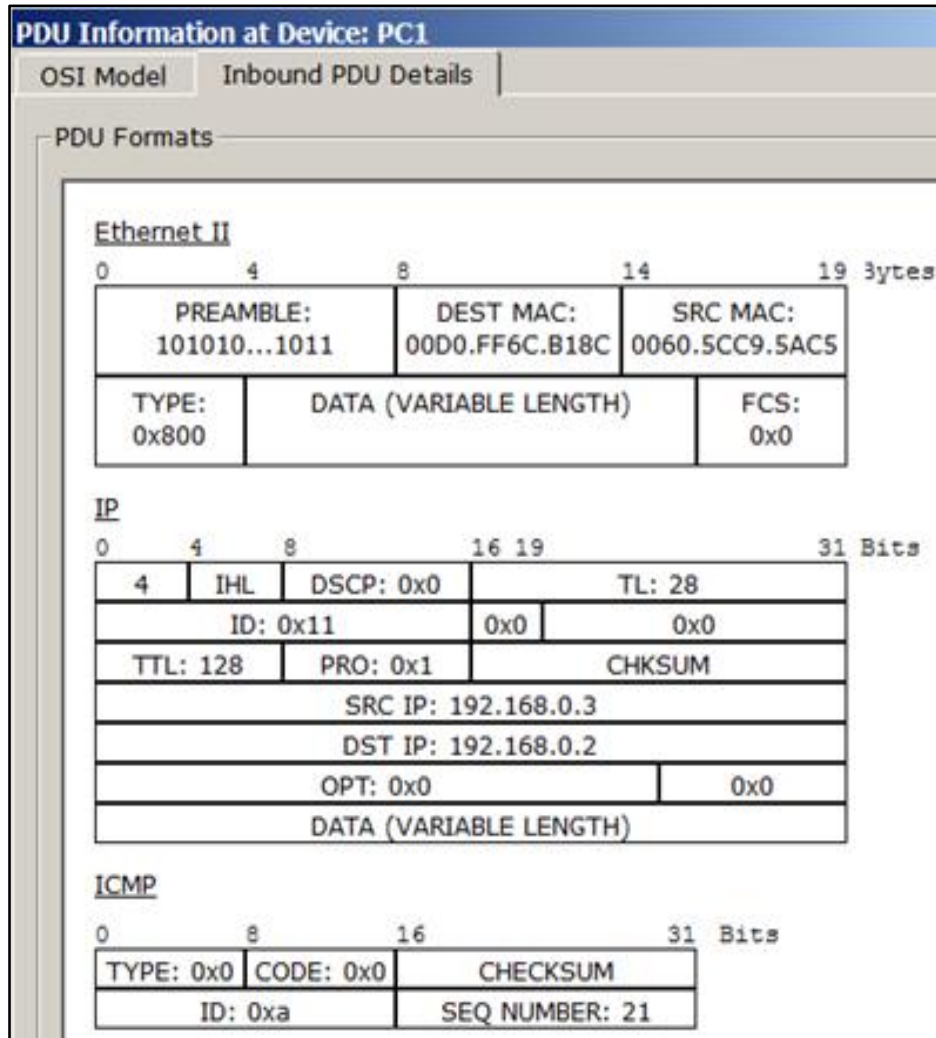


Рисунок 4.14 - Структура пакета

Подведем некий промежуточный итог. В Cisco Packet Tracer предусмотрен режим моделирования (Симуляции), в котором показывается, как работает утилита Ping. Чтобы перейти в данный режим, необходимо нажать на значок Simulation Mode (Симуляция) в нижнем правом углу рабочей области или комбинацию клавиш Shift+S. Откроется Simulation Panel (Панель симуляции), в которой будут отображаться все события, связанные с выполнения ping-процесса.

Практическая работа 4. Командная строка и режим симуляции

Моделирование прекращается либо при завершении *ping*-процесса, либо при закрытии окна симуляции. В режиме симуляции можно не только отслеживать используемые протоколы, но и видеть, на каком из семи уровней модели OSI данный протокол задействован. В процессе просмотра анимации мы увидели принцип работы хаба. Концентратор повторяет пакет на всех портах в надежде, что на одном из них есть получатель информации. Если пакеты каким-то узлам не предназначены, эти узлы игнорируют пакеты. А когда пакет вернётся отправителю, то мы увидим галочку «принятие пакета». (рисунок 4.15).

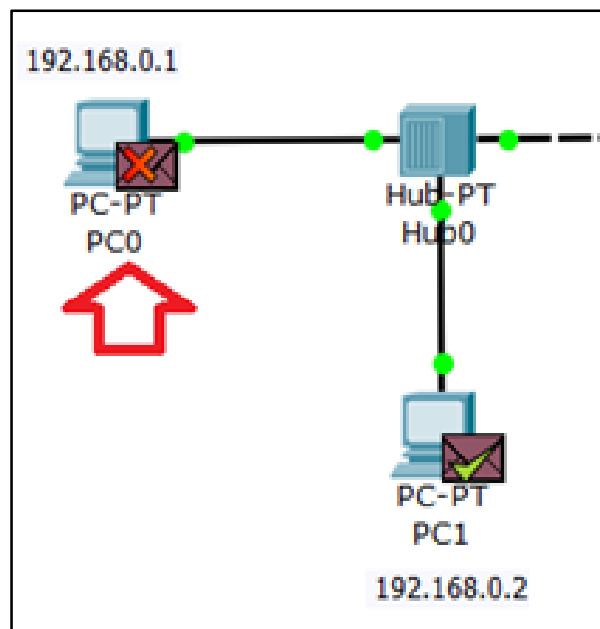
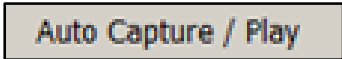


Рисунок 4.15 - Значки игнорирования пакетов и подтверждение соединения

Командная строка

7. Если нажать на кнопку  (воспроизведение), то мы увидим весь цикл прохождения пакета по сети. Процесс повторится 4 раза (рисунок 4.16).

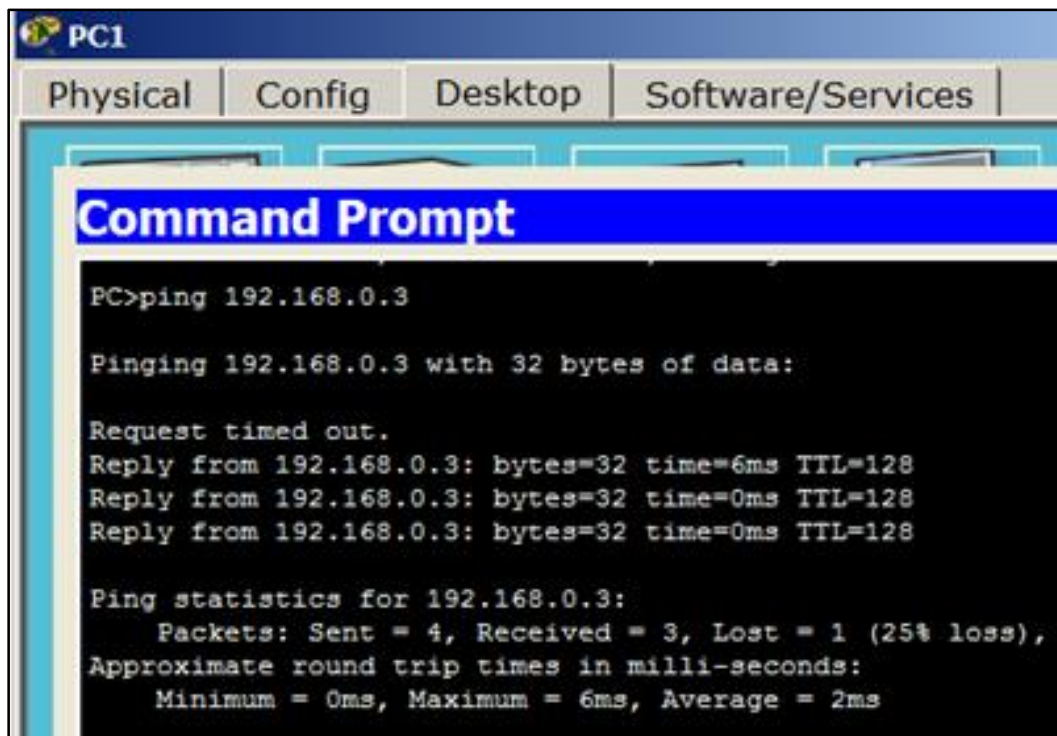


Рисунок 4.16 - Пинг от ПК1 до ПК2

Здесь:

TTL - время жизни отправленного пакета (определяет максимальное число маршрутизаторов, которое пакет может пройти при его продвижении по сети);

Time - время, потраченное на отправку запроса и получение ответа;

Min - минимальное время ответа;

Max - максимальное время ответа;

Avg - среднее время ответа.

Упражнение 4.3. Настройка сетевых параметров ПК в его графическом интерфейсе

1. Добавьте в моделируемую сеть еще один ПК – PC4.
2. Откройте свойства устройства PC4, нажав на его изображение. Для конфигурирования компьютера воспользуемся командой **ipconfig** из командной строки (рисунок 4.17).

Практическая работа 4. Командная строка и режим симуляции

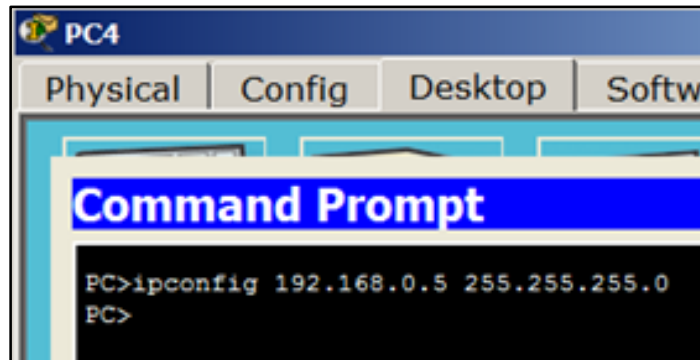


Рисунок 4.17 - Командой **ipconfig** назначены для ПК IP адрес и маска подсети

Как вариант, IP адрес и маску сети можно вводить в графическом интерфейсе устройства (рисунок 4.18).

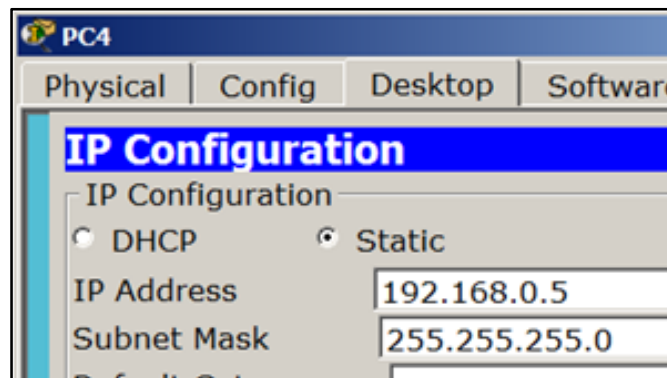


Рисунок 4.18 - Второй способ конфигурирования компьютера (настройки узла сети)

3. На каждом компьютере проверим назначенные параметры командой **ipconfig** (рисунок 4.19).

Практическая работа 4. Командная строка и режим симуляции

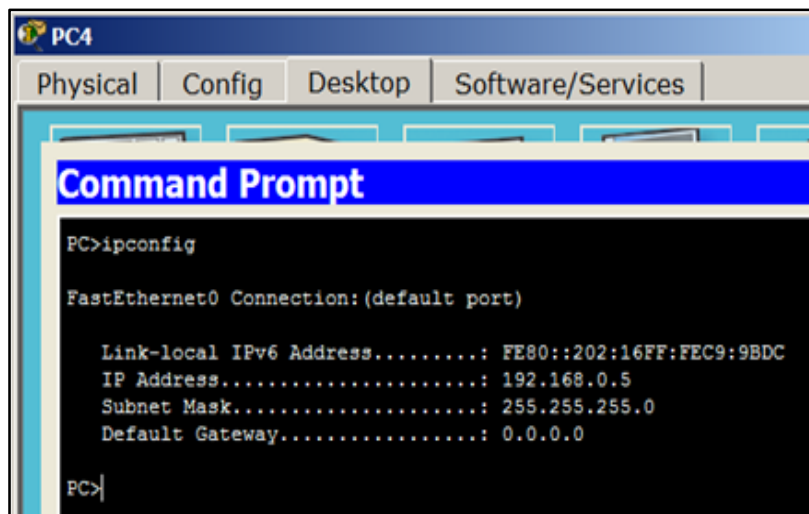


Рисунок 4.19 - Проверка конфигурирования ПК4 командой `ipconfig`

Упражнение 4.4. Режим симуляции

Состав сети: 4 узла, сервер, принтер и два концентратора. Концентраторы меж собой соединяются кроссоверным кабелем (рисунок 4.20).

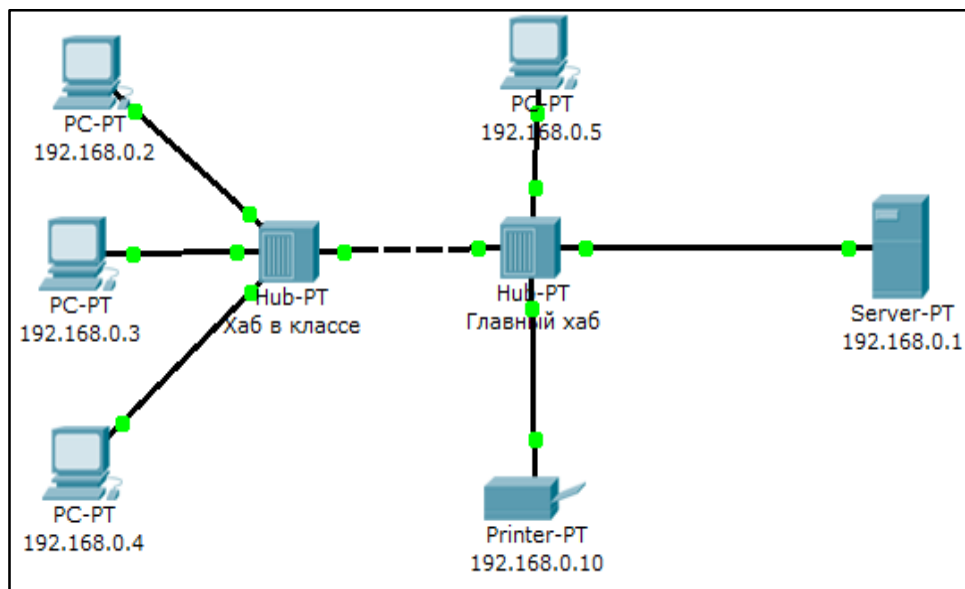


Рисунок 4.20 - Схема сети

Практическая работа 4. Командная строка и режим симуляции

1. Перейдите в режим симуляции (Shift+S) либо кликнув на иконку симуляции в правом нижнем углу рабочего пространства. Здесь изображено окно событий, кнопка сброса (очищает список событий), управление воспроизведением и фильтр протоколов. Предложено много протоколов, но требуется отфильтровать пока только ICMP, это исключит случайный трафик между узлами.

2. Для перехода к следующему событию используйте кнопку "Вперёд", либо автоматика (рисунок 4.21).

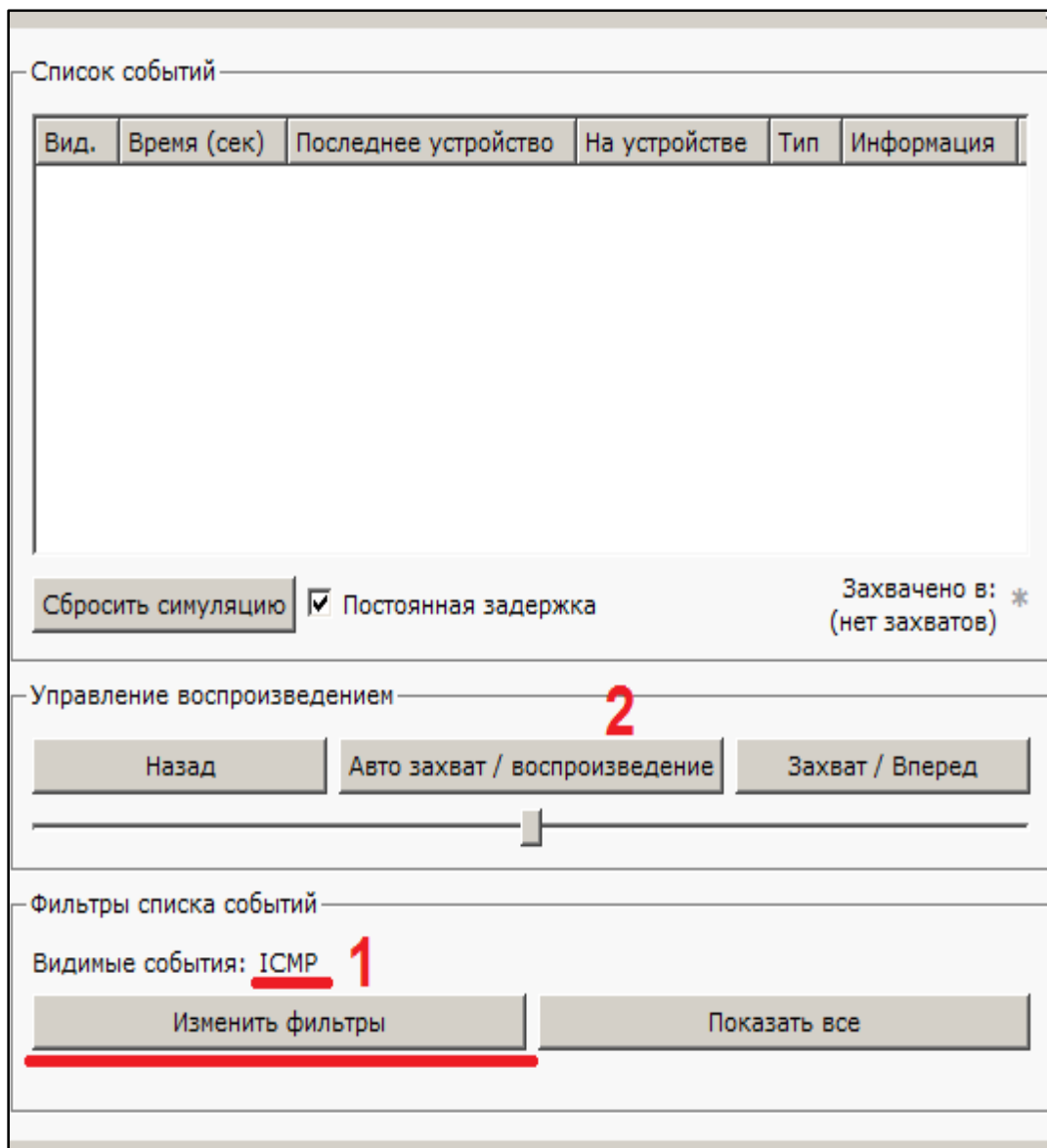


Рисунок 4.21 - Интерфейс симулятора

Практическая работа 4. Командная строка и режим симуляции

3. Пошлите PING-запрос. С одного из узлов попробуйте пропинговать другой узел. Выберите далеко расположенные узлы, чтобы наглядней увидеть, как будут проходить пакеты по сети в режиме симуляции. Войдите на узел 4 и пошлите пинг-запрос на узел 5.

4. С розового узла пингуйте зелёный. На розовом узле образовался пакет (конвертик), который ждёт (иконка паузы на нём). Запустить пакет в сеть можно нажав кнопку «Вперёд» в окне симуляции (рисунок 4.22).

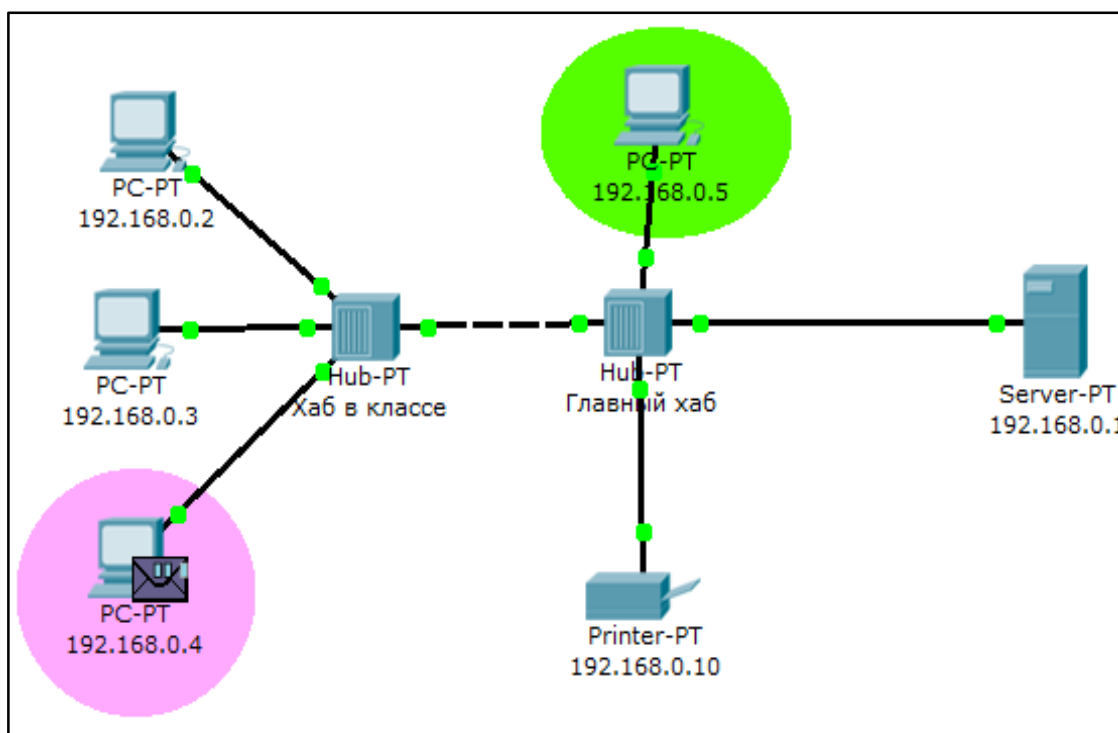


Рисунок 4.22 - Демонстрация работы симулятора

5. Также в окне симуляции увидите этот пакет, отметив его тип (ICMP) и источник (192.168.0.4). рабочее поле должно соответствовать рисунку 4.23.

6. Кликните на пакете. Увидите модель OSI. Сразу видно, что на 3-ем уровне (сетевой) возник пакет на исходящем направлении, который пойдёт до второго уровня, затем до первого, на физическую среду и передастся на следующий узел (рисунок 4.24).

Практическая работа 4. Командная строка и режим симуляции

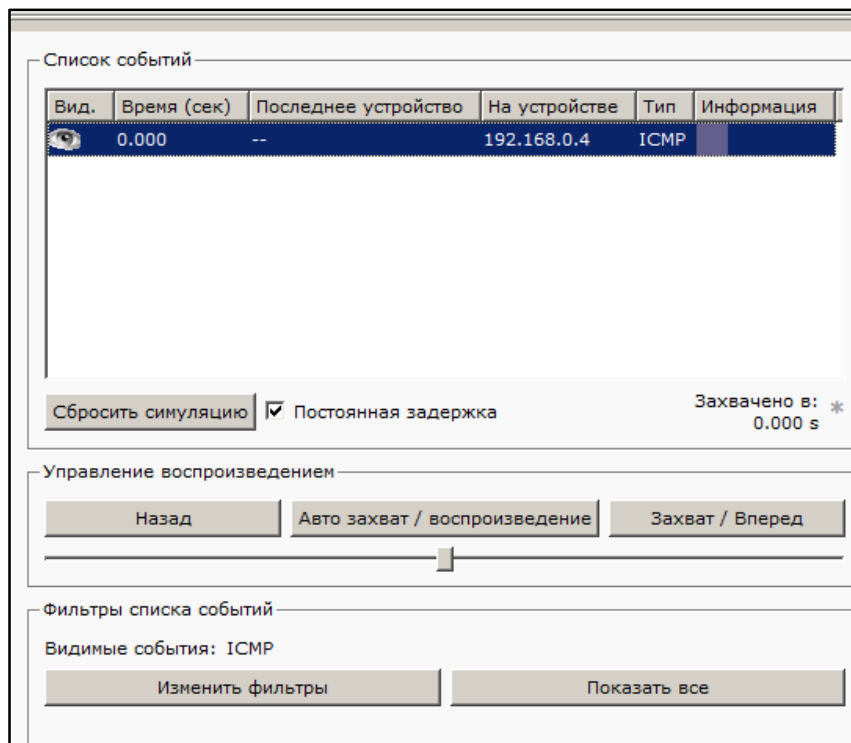


Рисунок 4.23 - Мониторинг работы протоколов

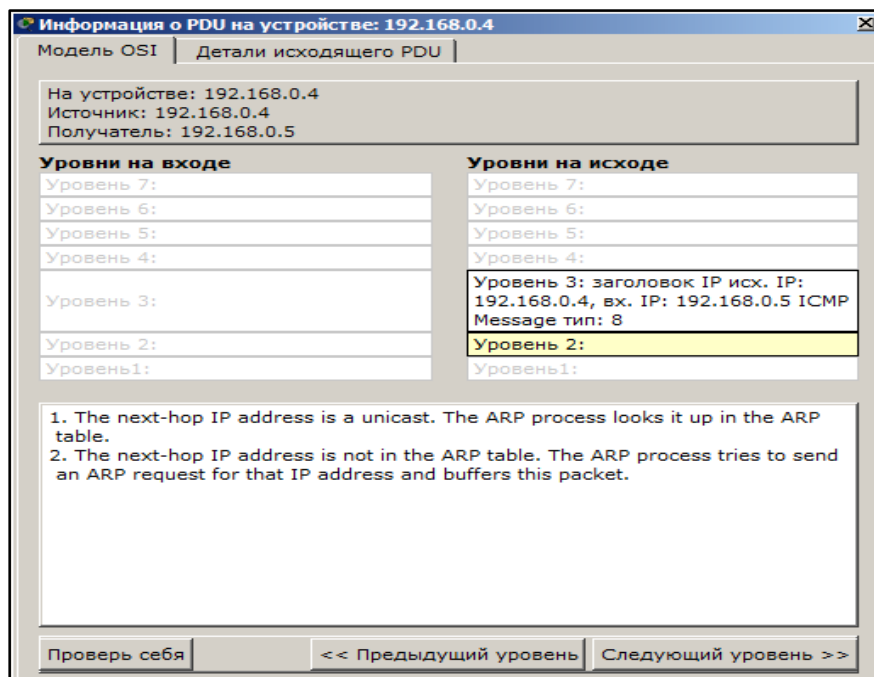


Рисунок 4.24 - Мониторинг работы на модели OSI.

Практическая работа 4. Командная строка и режим симуляции

На другой вкладке можно посмотреть структуру пакета (рисунк 4.25).

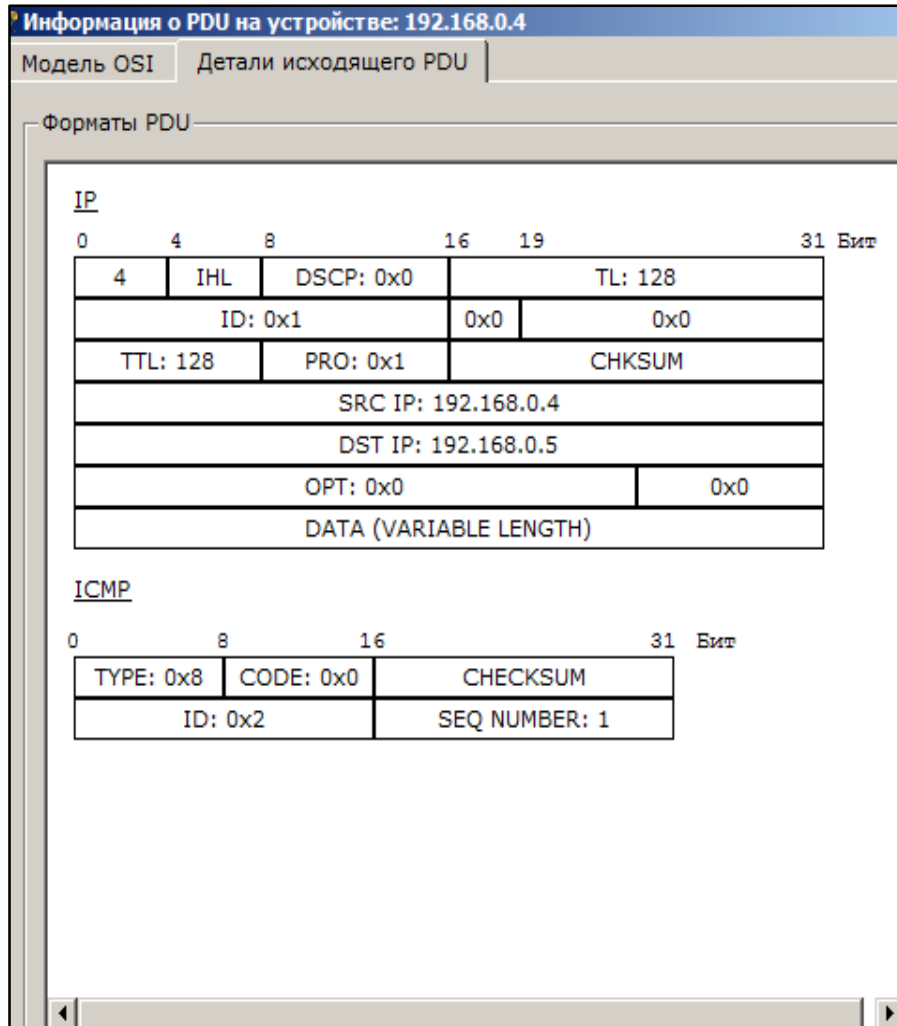


Рисунок 4.25 - Структура пакета

7. Нажмите кнопку «Вперёд» Пакет двинется к концентратору. Это единственное сетевое подключение с этой стороны (рисунок 4.26). Концентратор повторяет пакет на всех остальных портах в надежде, что на одном из них есть адресат (рисунок 4.27).

Практическая работа 4. Командная строка и режим симуляции

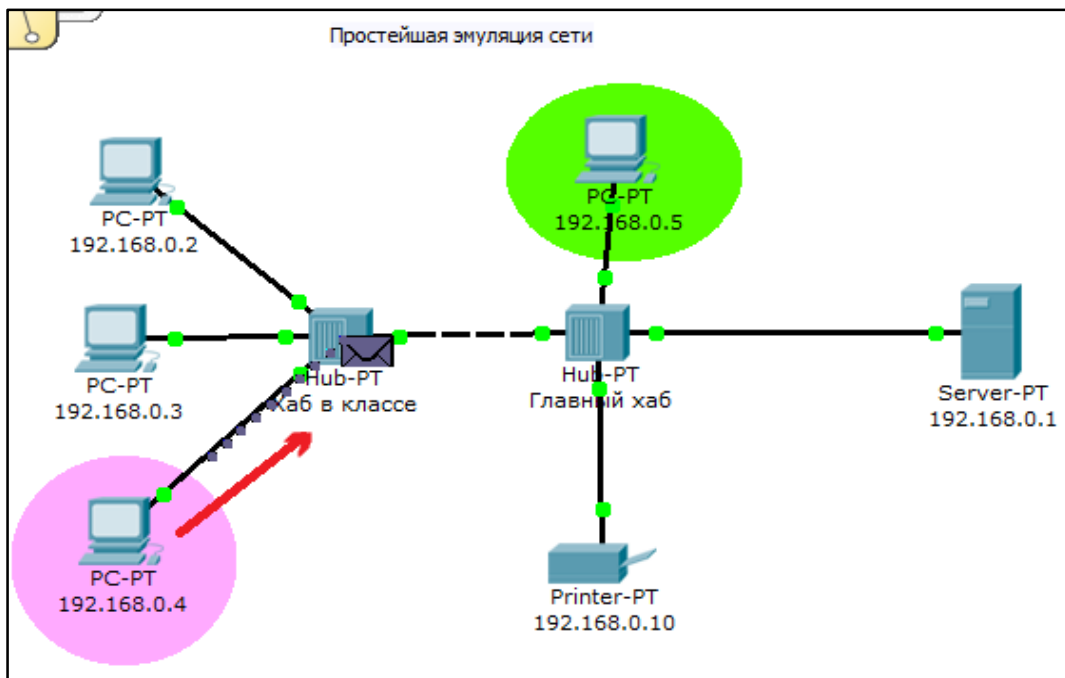


Рисунок 4.26 - Прохождение пакета. Первый этап

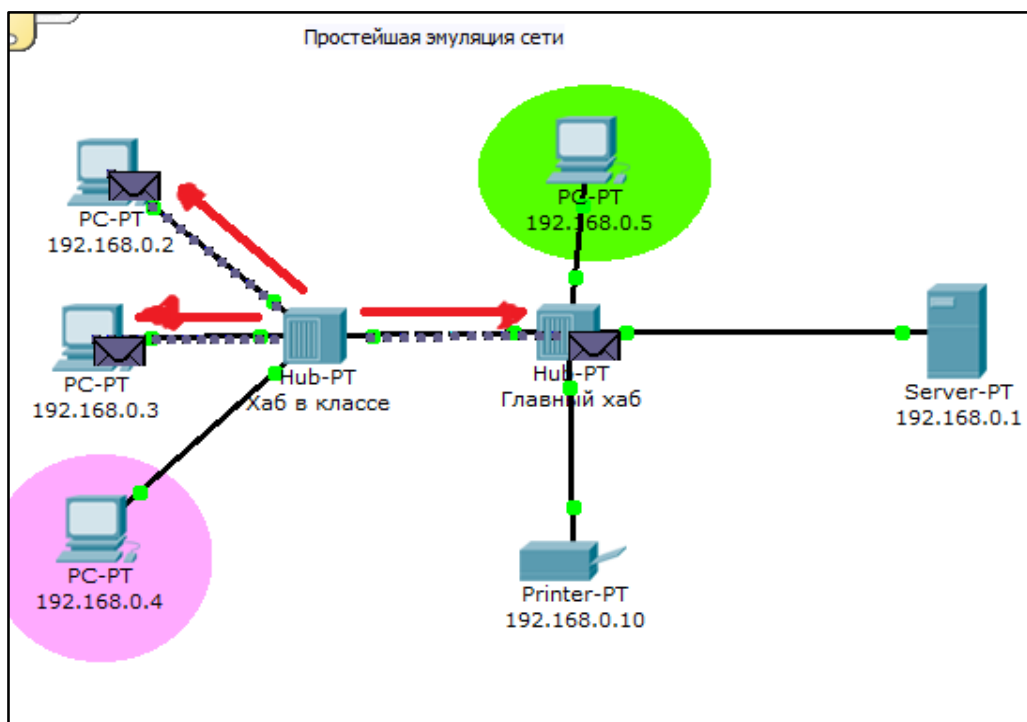


Рисунок 4.27 - Прохождение пакета. Второй этап

Практическая работа 4. Командная строка и режим симуляции

Если пакеты каким-то узлам не предназначены, они просто игнорируют их (рисунок 4.28).

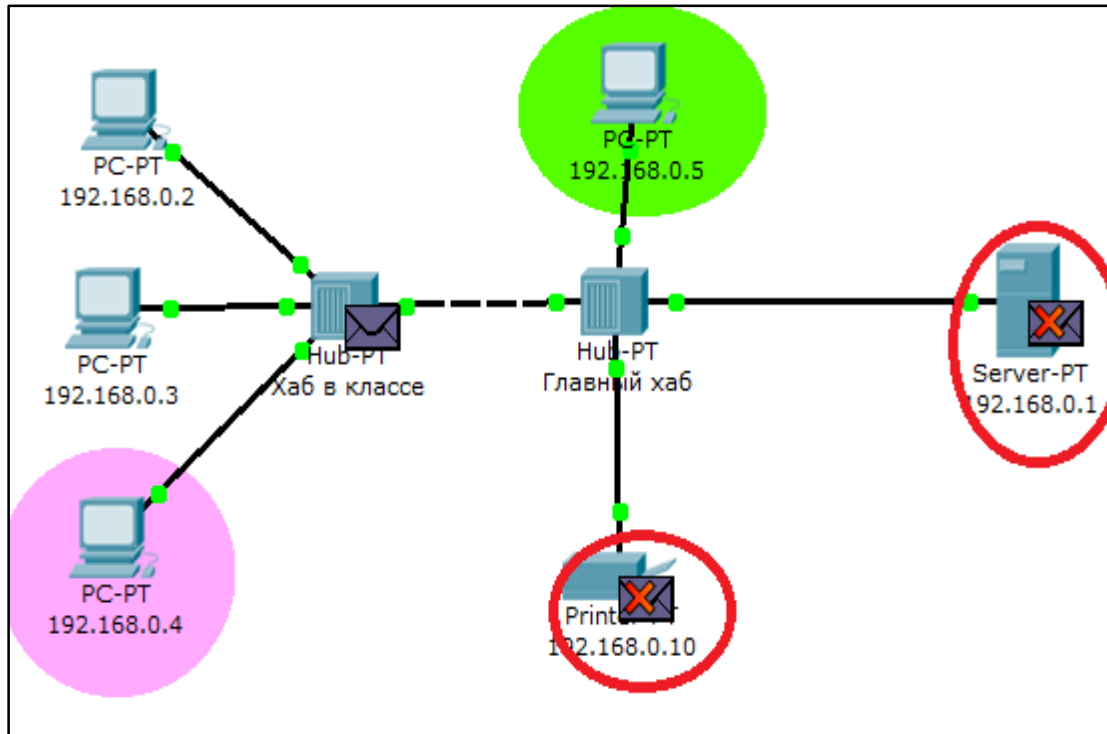


Рисунок 4.28 - Прохождение пакета. Третий этап

Когда пакет вернётся обратно, то увидим подтверждение соединения:

Контрольные вопросы

1. Какой командой можно посмотреть текущие настройки роутера?
2. Какими командами настраивается сетевой интерфейс роутера.
3. Как просмотреть конфигурационные настройки коммутатора?
4. Как определить распределение VLANов по портам коммутатора?

Практическая работа 4. Командная строка и режим симуляции

5. Перечислите основные режимы конфигурации при настройке коммутатора.
6. Перечислите основные режимы конфигурации при настройке роутера.
7. Как посмотреть таблицу маршрутизации на роутере?
8. Какие команды формируют таблицу маршрутизации роутера?
9. Какими командами настраиваются вилланы на коммутаторе?
10. Какими командами настраивается взаимодействие между вилланами?
11. Как просмотреть прохождение пакета по уровням модели OSI?
12. Можно ли определить причину того, что посланный в режиме симуляции пакет не дошел до адресата и на каком этапе произошел сбой работы сети?
13. Укажите в составе пакета IP адреса отправителя и получателя.
14. Как изменить фильтры списка событий?
15. Как в режиме симуляции определить, какие протоколы были задействованы в работе сети?
16. Как в режиме симуляции проследить изменение содержимого пакета при прохождении его по сети?
17. Перечислите основные возможности режима симуляции

Задания

Задание 4.1

Выполните на своем компьютере все упражнения. Отчет должен содержать скриншоты с экрана вашего компьютера, позволяющие судить о том, что основные результаты последовательного выполнения упражнений выполнены корректно и в надлежащей последовательности.

Задание 4.2

Дана схема сети, показанная на рисунке 4.29.

Практическая работа 4. Командная строка и режим симуляции

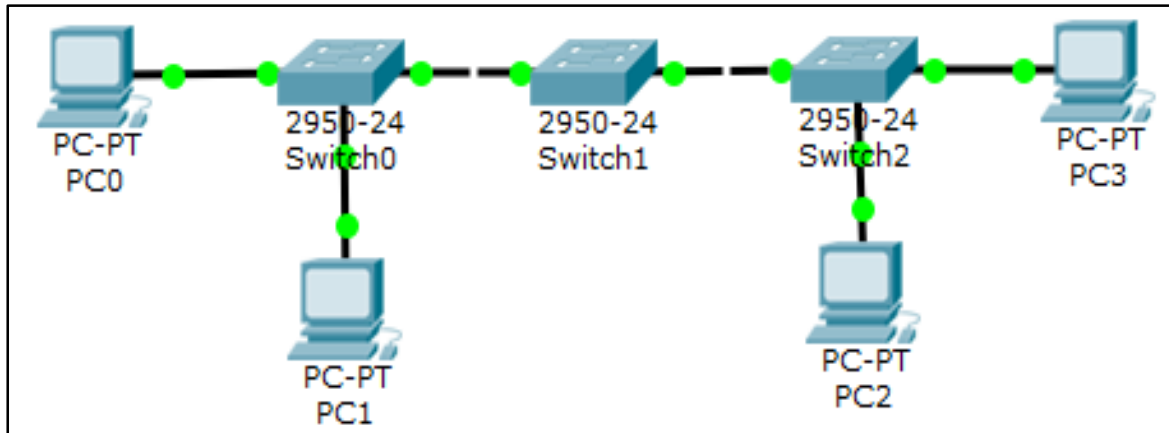


Рисунок 4.29 - Схема сети

Нужно:

1. Построить такую сеть
2. Изменить имя коммутаторов Cisco;
3. Обеспечить парольный доступ к привилегированному режиму на коммутаторах;
4. Задать ip-адреса и маски коммутаторам (172.16.1.11/24, 172.16.1.12/24, 172.16.1.13/24);
5. Задать ip-адреса и маски сетей персональным компьютерам. (172.16.1.1/24, 172.16.1.2/24, 172.16.1.3/24, 172.16.1.4/24);
6. Убедиться в достижимости всех объектов сети по протоколу IP;
7. Переключившись в «Режим симуляции» и рассмотреть и пояснить процесс обмена данными по протоколу ICMP между устройствами (выполнив команду Ping с одного компьютера на другой).

=====

Практическая работа 5. МОДЕЛИРОВАНИЕ ВИРТУАЛЬНЫХ ЛОКАЛЬНЫХ СЕТЕЙ

Цель работы – приобретение практических навыков обучающимися в построении, моделировании и оценке эффективности виртуальных локальных компьютерных сетей.

Порядок выполнения работы – внимательно изучите теоретический материал, выполните все упражнения, включённые в данный раздел в пошаговом режиме. Если в промежуточных точках изображения Ваших моделей не совпадает с приводимыми в практикуме, вернитесь на 2-3 шага назад и все-таки добейтесь абсолютного соответствия. Самостоятельно выполните задания к практической работе.

5.1. Виртуальная локальная сеть

Краткая теория [3, 4, 10, 25]

Виртуальная локальная сеть VLAN (Virtual Local Area Network) - логическая группа узлов сети, трафик которой на канальном уровне полностью изолирован от других узлов сети.

Это означает, что передача кадров между разными виртуальными сетями на основании MAC-адреса невозможна независимо от типа адреса - уникального, группового или широковещательного. В то же время внутри виртуальной сети кадры передаются только на тот порт, который связан с адресом назначения кадра. Таким образом, с помощью виртуальных сетей решается проблема распространения широковещательных кадров и вызываемых ими последствий, которые могут развиваться в широковещательные штормы и существенно снизить производительность сети.

VLAN обладают следующими преимуществами:

- гибкость внедрения. VLAN являются эффективным способом группировки сетевых пользователей в виртуальные рабочие группы, несмотря на их физическое размещение в сети;

Практическая работа 5. Моделирование виртуальных сетей

=====

- VLAN обеспечивают возможность контроля широковещательных сообщений, что увеличивает полосу пропускания, доступную для пользователя;

- VLAN позволяют повысить безопасность сети, определив с помощью фильтров, настроенных на коммутаторе или маршрутизаторе, политику взаимодействия пользователей из разных виртуальных сетей.

В коммутаторах могут быть реализованы следующие типы VLAN:

- на основе портов;
- на основе стандарта IEEE 802.1Q;
- на основе стандарта IEEE 802.1ad (Q-in-Q VLAN);
- на основе портов и протоколов IEEE 802.1v;
- на основе MAC-адресов;
- асимметричные.

Также для сегментирования сети на канальном уровне модели OSI в коммутаторах могут использоваться другие функции, например, функция Traffic Segmentation.

VLAN на основе портов (Port-based VLAN)

При использовании VLAN на основе портов каждый порт назначается в определенную VLAN, независимо от того, какой пользователь или компьютер подключен к этому порту. Это означает, что все пользователи, подключенные к этому порту, будут членами одной VLAN. Конфигурация портов статическая и может быть изменена только вручную.

Объединение VLAN с помощью маршрутизирующего устройства представлено на рисунке 5.1.

Практическая работа 5. Моделирование виртуальных сетей

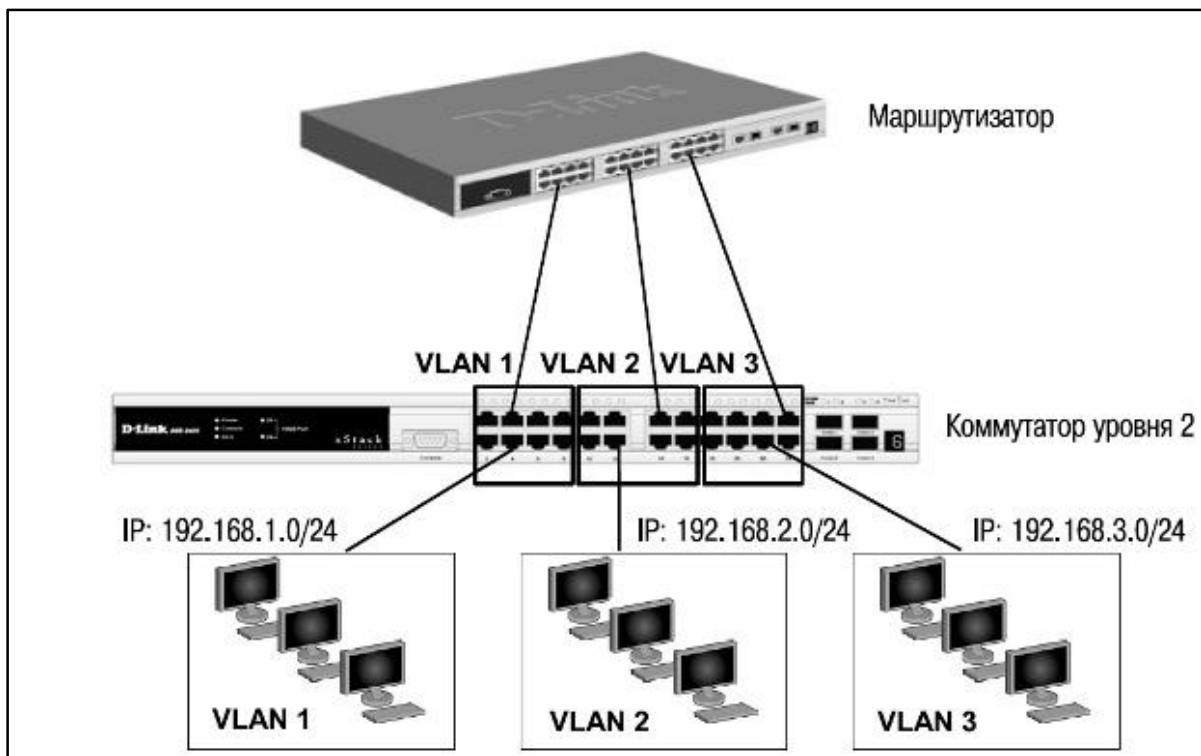


Рисунок 5.1 - Объединение VLAN с помощью маршрутизирующего устройства

Основные характеристики VLAN на основе портов:

- применяются в пределах одного коммутатора. Если необходимо организовать несколько рабочих групп в пределах небольшой сети на основе одного коммутатора, например, необходимо разнести два или несколько отделов предприятия, то решение VLAN на базе портов оптимально подходит для данной задачи;

- простота настройки. Создание виртуальных сетей на основе группирования портов не требует от администратора большого объема ручной работы - достаточно всем портам, помещаемым в одну VLAN, присвоить одинаковый идентификатор VLAN (VLAN ID);

- возможность изменения логической топологии сети без физического перемещения станций. Для этого достаточно изменить настройки порта с одной VLAN на другую, и рабочая станция сразу же получает возможность совместно использовать ресурсы с членами новой VLAN.

Практическая работа 5. Моделирование виртуальных сетей

=====

Таким образом, VLAN обеспечивают гибкость при перемещениях, изменениях и наращивании сети. Каждый порт может входить только в одну VLAN.

Для объединения виртуальных подсетей как внутри одного коммутатора, так и между двумя коммутаторами нужно использовать сетевой уровень OSI-модели. Один из портов каждой VLAN подключается к интерфейсу маршрутизатора, который создает таблицу маршрутизации для пересылки кадров из одной VLAN - подсети в другую (IP-адреса подсетей должны быть разными).

Недостатком такого решения является то, что один порт каждой VLAN необходимо подключать к маршрутизатору. Это приводит к дополнительным расходам на покупку кабелей и маршрутизаторов, а также порты коммутатора используются очень расточительно.

Решить данную проблему можно если использовать коммутаторы, которые на основе фирменного решения позволяют включать порт в несколько VLAN или использовать коммутаторы уровня 3.

VLAN на основе стандарта IEEE 802.1Q

Виртуальные локальные сети, построенные на основе стандарта IEEE 802.1Q, используют дополнительные поля кадра для хранения информации о принадлежности к VLAN при его перемещении по сети. С точки зрения удобства и гибкости настроек VLAN стандарта IEEE 802.1Q является лучшим решением по сравнению с VLAN на основе портов.

Преимущества VLAN на основе стандарта IEEE 802.1Q:

- гибкость и удобство в настройке - можно создавать необходимые комбинации VLAN как в пределах одного коммутатора, так и во всей сети, построенной на коммутаторах с поддержкой стандарта IEEE 802.1Q;

- способность добавления тегов позволяет информации о VLAN распространяться через множество 802.1Q - совместимых коммутаторов по одному физическому соединению (магистральному каналу, Trunk Link);

- позволяет активизировать алгоритм связующего дерева (Spanning Tree) на всех портах и работать в обычном режиме. Прото-

Практическая работа 5. Моделирование виртуальных сетей

=====
кол Spanning Tree позволяет коммутаторам автоматически определять древовидную конфигурацию связей в сети при произвольном соединении портов между собой. Для нормальной работы коммутатора требуется отсутствие замкнутых маршрутов в сети. Эти маршруты могут создаваться администратором специально для образования резервных связей или же возникать случайным образом, что вполне возможно, если сеть имеет многочисленные связи, а кабельная система плохо структурирована или документирована. С помощью протокола Spanning Tree коммутаторы после построения схемы сети блокируют избыточные маршруты. Таким образом, автоматически предотвращается возникновение петель в сети;

- способность VLAN IEEE 802.1Q добавлять и извлекать теги из заголовков кадров позволяет использовать в сети коммутаторы и сетевые устройства, которые не поддерживают стандарт IEEE 802.1Q. Устройства разных производителей, поддерживающие стандарт, могут работать вместе, независимо от какого-либо фирменного решения.

Чтобы связать подсети на сетевом уровне, необходим маршрутизатор или коммутатор L3. Однако для более простых случаев, например, для организации доступа к серверу из различных VLAN, маршрутизатор не потребуется. Нужно включить порт коммутатора, к которому подключен сервер, во все подсети, а сетевой адаптер сервера должен поддерживать стандарт IEEE 802.1Q.-

Некоторые определения IEEE 802.1Q:

- Tagging («Маркировка кадра») — процесс добавления информации о принадлежности к 802.1Q VLAN в заголовок кадра;

- Untagging («Извлечение тега из кадра») — процесс извлечения информации о принадлежности к 802.1Q VLAN из заголовка кадра;

- VLAN ID (VID) — идентификатор VLAN;

- Port VLAN ID (PVID) — идентификатор порта VLAN. I

- Ingress port («Входной порт») — порт коммутатора, на который поступают кадры, и при этом принимается решение о принадлежности к VLAN;

- Egress port («Выходной порт») — порт коммутатора, с которого кадры передаются на другие сетевые устройства, коммутаторы или рабочие станции, и, соответственно, на нем должно приниматься решение о маркировке.

Практическая работа 5. Моделирование виртуальных сетей

Любой порт коммутатора может быть настроен как tagged (маркированный) или как untagged (немаркированный). Функция untagging позволяет работать с теми сетевыми устройствами виртуальной сети, которые не понимают тегов в заголовке кадра Ethernet. Функция tagging позволяет настраивать VLAN между несколькими коммутаторами, поддерживающими стандарт IEEE 802.1Q. Маркированные и немаркированные порты VLAN представлены рисунком 5.2.

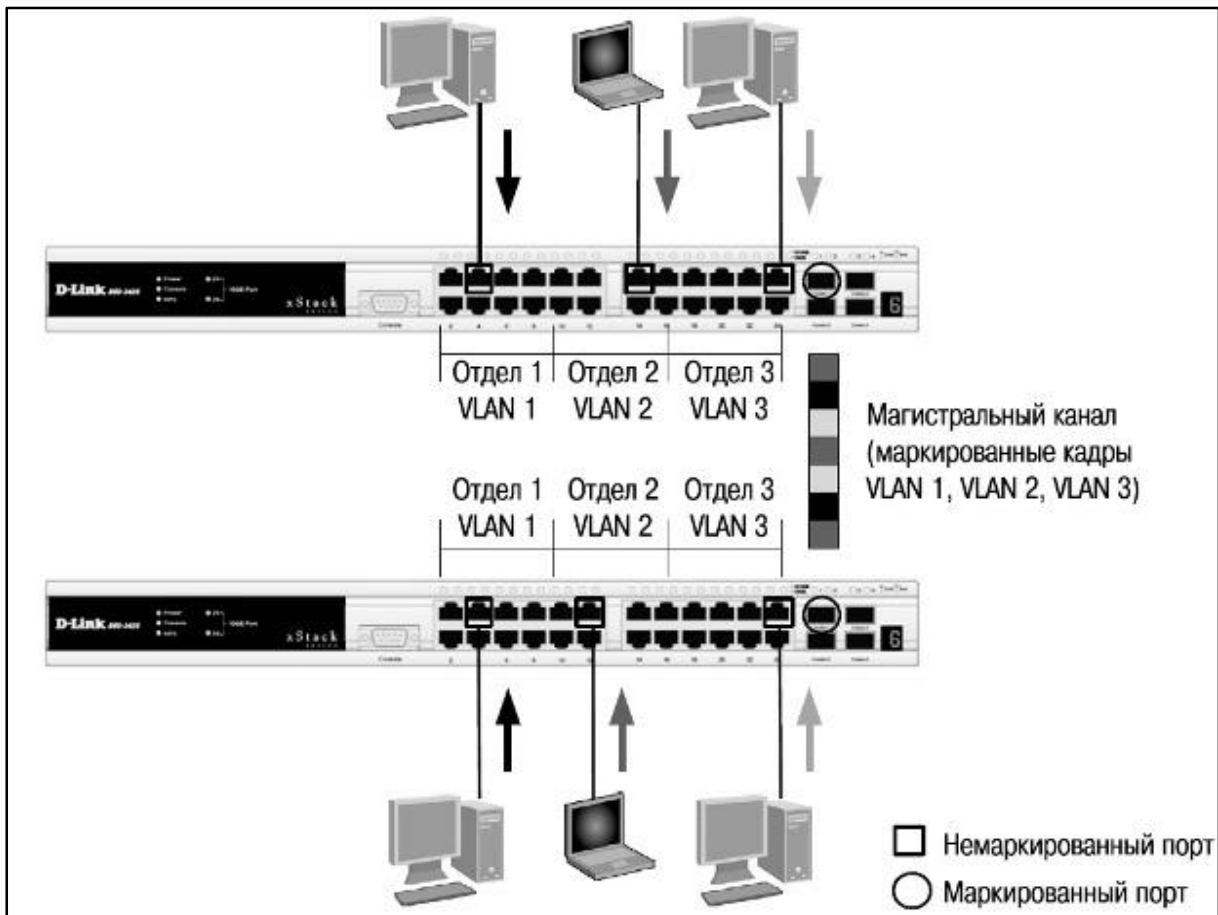


Рисунок 5.2 - Маркированные и немаркированные порты VLAN

Тег VLAN IEEE 802.1Q

Тег — метка-идентификатор, добавляемая к Ethernet-пакетам и используемая при выделении разных виртуальных каналов данных в одном физическом канале. Стандарт IEEE 802.1Q определяет изменения в структуре кадра Ethernet, позволяющие передавать информа-

Практическая работа 5. Моделирование виртуальных сетей

цию о VLAN по сети. На рисунке 5.3 изображен формат тега 802.1Q VLAN.

К кадру Ethernet добавлены 32 бита (4 байта), которые увеличивают его размер до 1522 байт. Первые 2 байта (поле Tag Protocol Identifier, TPID) с фиксированным значением 0x8100 определяют, что кадр содержит тег протокола 802.1Q.



Рисунок 5.3 - Формат тега 802.1Q VLAN Ethernet

Остальные 2 байта содержат следующую информацию:

- Priority («Приоритет») — 3 бита поля приоритета передачи кодируют до восьми уровней приоритета (от 0 до 7, где 7 — наивысший приоритет), которые используются в стандарте 802.1p;
- Format Indicator (CFI) — 1 бит индикатора канонического формата зарезервирован для обозначения кадров сетей других типов (Token Ring, FDDI), передаваемых по магистрали Ethernet;
- VID (VLAN ID) — 12-битный идентификатор VLAN определяет, какой VLAN принадлежит трафик. Поскольку под поле VID отведено 12 бит, то можно задать 4094 уникальных VLAN (VID 0 и VID 4095 зарезервированы).

Практическая работа 5. Моделирование виртуальных сетей

Port VLAN ID

Каждый физический порт коммутатора имеет параметр, называемый идентификатор порта VLAN (PVID). Этот параметр используется для того, чтобы определить, в какую VLAN коммутатор направит входящий немаркированный кадр с подключенного к порту сегмента, когда кадр нужно передать на другой порт (внутри коммутатора в заголовки всех немаркированных кадров добавляется идентификатор VID, равный PVID порта, на который они были приняты). Этот механизм позволяет одновременно существовать в одной сети устройствам с поддержкой и без поддержки стандарта IEEE 802.1Q. Коммутаторы, поддерживающие протокол IEEE 802.1Q, должны хранить таблицу, связывающую идентификаторы портов PVID с идентификаторами VID сети. При этом каждый порт такого коммутатора может иметь только один PVID и столько идентификаторов VID, сколько поддерживает данная модель коммутатора. Если на коммутаторе не настроены VLAN, то все порты по умолчанию входят в одну VLAN с PVID = 1.

Продвижение кадров VLAN IEEE 802.1Q

Решение о продвижении кадра внутри виртуальной локальной сети принимается на основе трех следующих видов правил:

- правила входящего трафика (ingress rules) — классификация получаемых кадров относительно принадлежности к VLAN;
- правила продвижения между портами (forwarding rules) — принятие решения о продвижении или отбрасывании кадра;
- правила исходящего трафика (egress rules) — принятие решения о сохранении или удалении в заголовке кадра тега 802.1Q перед его передачей.

Правила входящего трафика выполняют классификацию каждого получаемого кадра относительно принадлежности к определенной VLAN, а также могут служить для принятия решения о приеме кадра для дальнейшей обработки или его отбрасывании на основе формата принятого кадра. Классификация кадра по принадлежности VLAN осуществляется следующим образом: если кадр не содержит инфор-

Практическая работа 5. Моделирование виртуальных сетей

=====
мацию о VLAN (немаркированный кадр), то в его заголовок коммутатор добавляет тег с идентификатором VID, равным идентификатору PVID порта, через который этот кадр был принят. Если кадр содержит информацию о VLAN (маркированный кадр), то его принадлежность к конкретной VLAN определяется по идентификатору VID в заголовке кадра. Значение тега в нем не изменяется.

Активизировав функцию проверки формата кадра на входе, администратор сети может указать, кадры каких форматов будут приниматься коммутатором для дальнейшей обработки.

5.2. Практические упражнения

Упражнение 5.1. VLAN с одним коммутатором

1. Для рисования персональных компьютеров (ПК) выберите в конечных устройствах настольный компьютер и, удерживая Ctrl, кликните на ПК, а затем рисуйте нужное количество ПК, щелкая мышкой (рисунок 5.4).

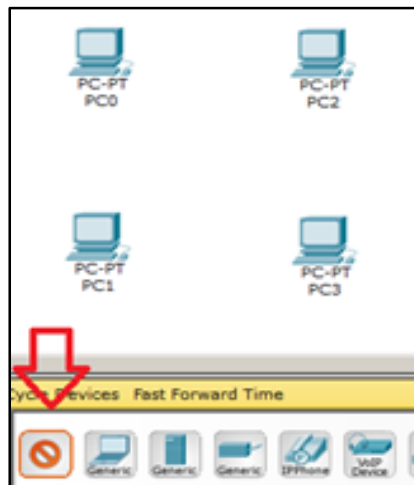


Рисунок 5.4 - Выбор устройств

2. Установите коммутатор и, удерживая Ctrl, создайте подключение прямым кабелем, выбирая порты коммутатора. После инициализации портов все лампы загорятся зеленым.

Практическая работа 5. Моделирование виртуальных сетей

=====

На схеме в рабочем поле программы Cisco Packet Tracer будет изображены две подсети (рисунок 5.5). Имя VLAN1 используется по умолчанию, его лучше в нашем примере не использовать.

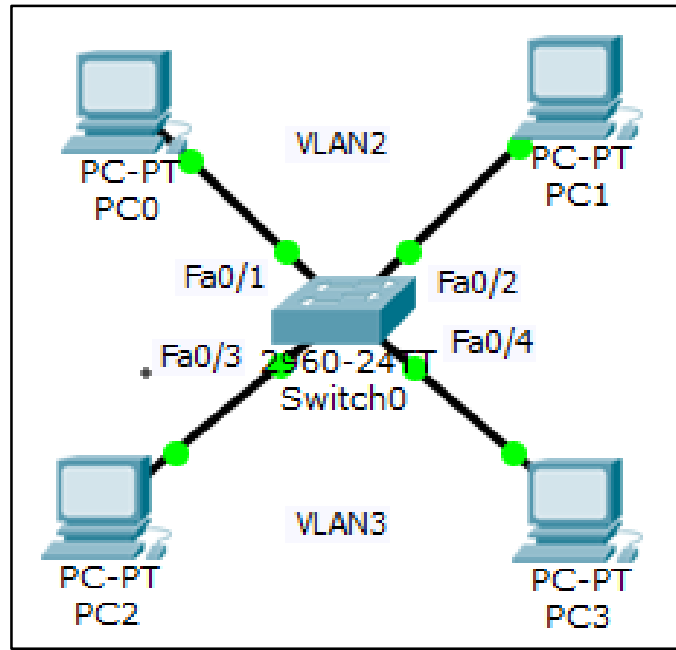


Рисунок 5.5 - Две подсети: VLAN2 и VLAN3

3. На коммутаторе наберите команду **enable** и войдите в привилегированный режим.

4. Наберите команду **conf t** для входа в режим глобального конфигурирования. Если подвести курсор мыши к портам коммутатора, то Вы можете увидеть какие порты в каком сегменте задействованы.

Для VLAN3 – это Fa0/3 и Fa0/4 (**buh**) и для VLAN2 – это Fa0/1 и Fa0/2 (**sklad**).

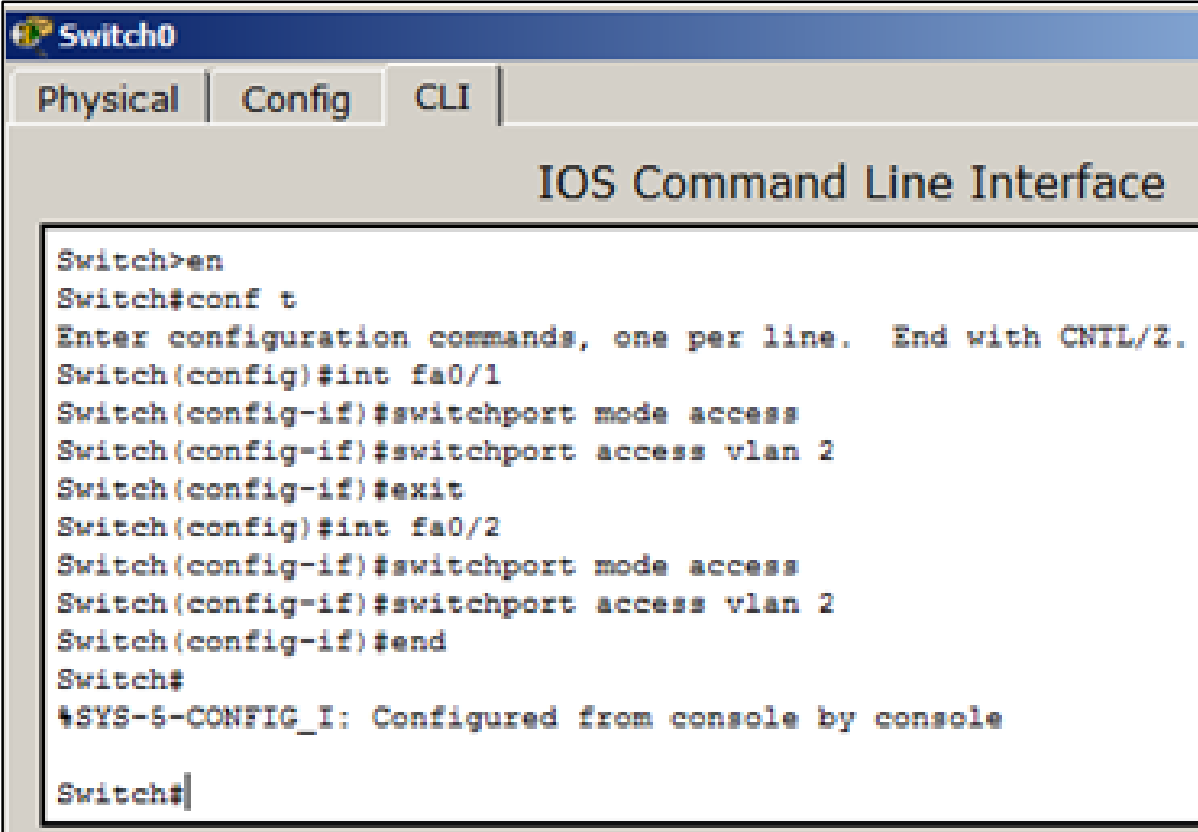
5. Сначала сконфигурируйте второй сегмент сети VLAN2 (**sklad**) – рисунок 5.6.

Практическая работа 5. Моделирование виртуальных сетей

```
Switch#
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#vlan 2
Switch(config-vlan)#name sklad
```

Рисунок 5.6 - VLAN2

6. В виртуальной сети VLAN2 настройте порты коммутатора Fa0/1 и Fa0/2 как access порты, т.е. порты для подключения пользователей (рисунок 5.7).



```
Switch0
Physical | Config | CLI |
IOS Command Line Interface

Switch>en
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#int fa0/1
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 2
Switch(config-if)#exit
Switch(config)#int fa0/2
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 2
Switch(config-if)#end
Switch#
%SYS-5-CONFIG_I: Configured from console by console

Switch#
```

Рисунок 5.7 - Порты коммутатора для подключения пользователей

7. Командой **show vlan** проверьте результат (рисунок 5.8).

Практическая работа 5. Моделирование виртуальных сетей

```
Switch0
Physical | Config | CLI
IOS Command Line Interface

Switch#show vlan

VLAN Name                Status    Ports
-----
1    default                active    Fa0/3, Fa0/4, Fa0/5, Fa0/6
                                           Fa0/7, Fa0/8, Fa0/9, Fa0/10
                                           Fa0/11, Fa0/12, Fa0/13, Fa0/14
                                           Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                           Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                           Fa0/23, Fa0/24, Gig0/1, Gig0/2
2    sklad                  active    Fa0/1, Fa0/2
1002 fddi-default         act/unsup
1003 token-ring-default   act/unsup
1004 fddinet-default      act/unsup
1005 trnet-default        act/unsup
```

Рисунок 5.8 - Подсеть VLAN2 настроена

8. Работаем с VLAN3. Выполните последовательность команд (рисунок 5.9).

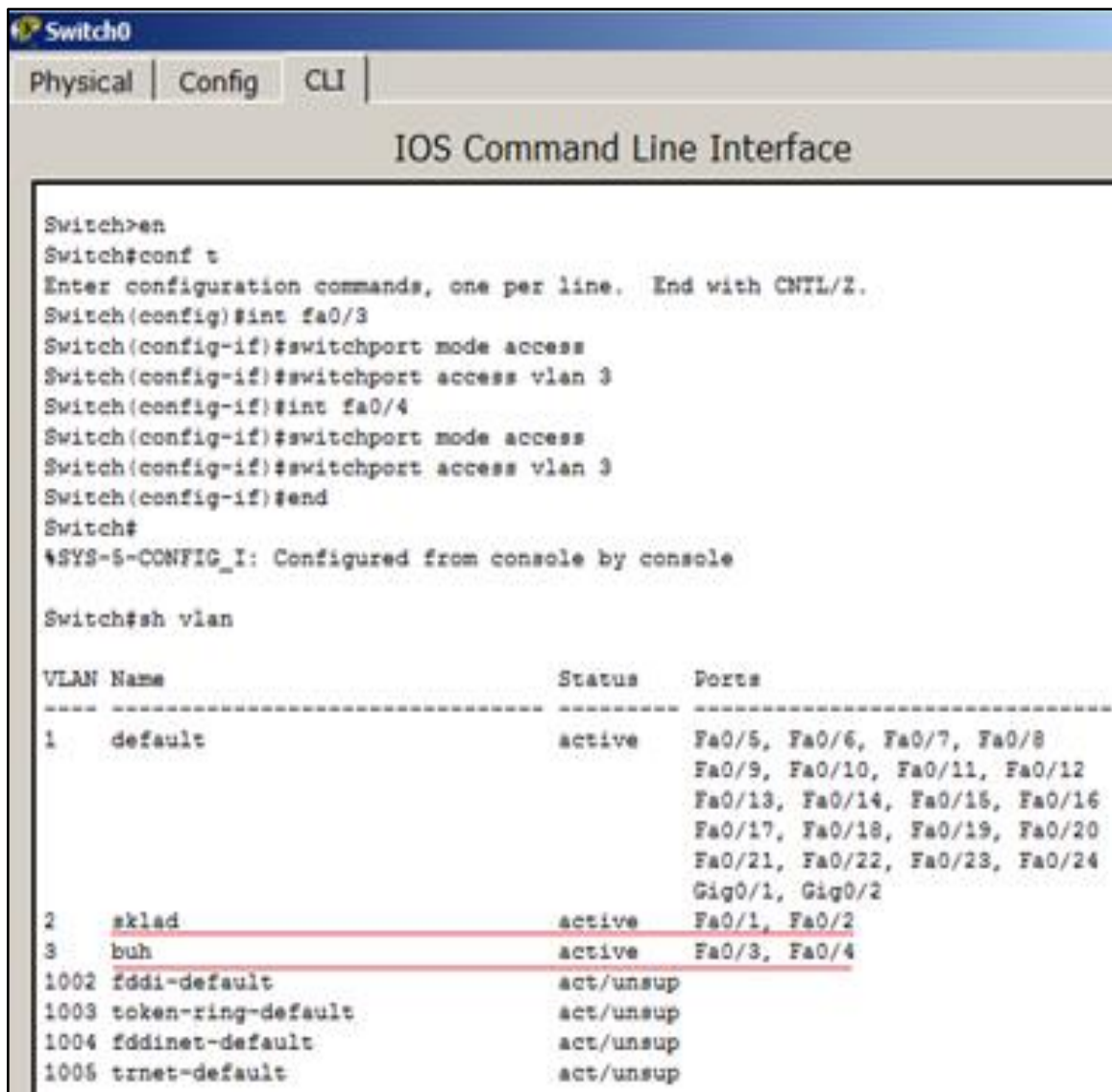
```
Switch#
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config-vlan)#vlan 3
Switch(config-vlan)#name buh
Switch(config-vlan)#exit
Switch(config)#
```

Рисунок 5.9 - Конфигурация VLAN3

Практическая работа 5. Моделирование виртуальных сетей

9. В виртуальной сети VLAN3 настройте порты коммутатора Fa0/3 и Fa0/4 как access порты, т.е. порты для подключения пользователей, затем командой **show vlan** можно проверить и убедиться, что в сети созданы 2 сегмента на разные порты коммутатора (рисунок 5.10).

10. Настройте IP адреса компьютеров – для VLAN2 из сети 192.168.2.0, а для VLAN3 из сети 192.168.3.0 (рисунок 5.11).



```
Switch0
Physical | Config | CLI |
IOS Command Line Interface

Switch>en
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#int fa0/3
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 3
Switch(config-if)#int fa0/4
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 3
Switch(config-if)#end
Switch#
%SYS-5-CONFIG_I: Configured from console by console

Switch#sh vlan

VLAN Name                Status    Ports
-----
1    default                 active    Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                           Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                           Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                           Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                           Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                           Gig0/1, Gig0/2
2    sklad                   active    Fa0/1, Fa0/2
3    buh                     active    Fa0/3, Fa0/4
1002 fddi-default           act/unsup
1003 token-ring-default   act/unsup
1004 fddinet-default       act/unsup
1005 trnet-default         act/unsup
```

Рисунок 5.10 - Подсети VLAN2 VLAN2

Практическая работа 5. Моделирование виртуальных сетей

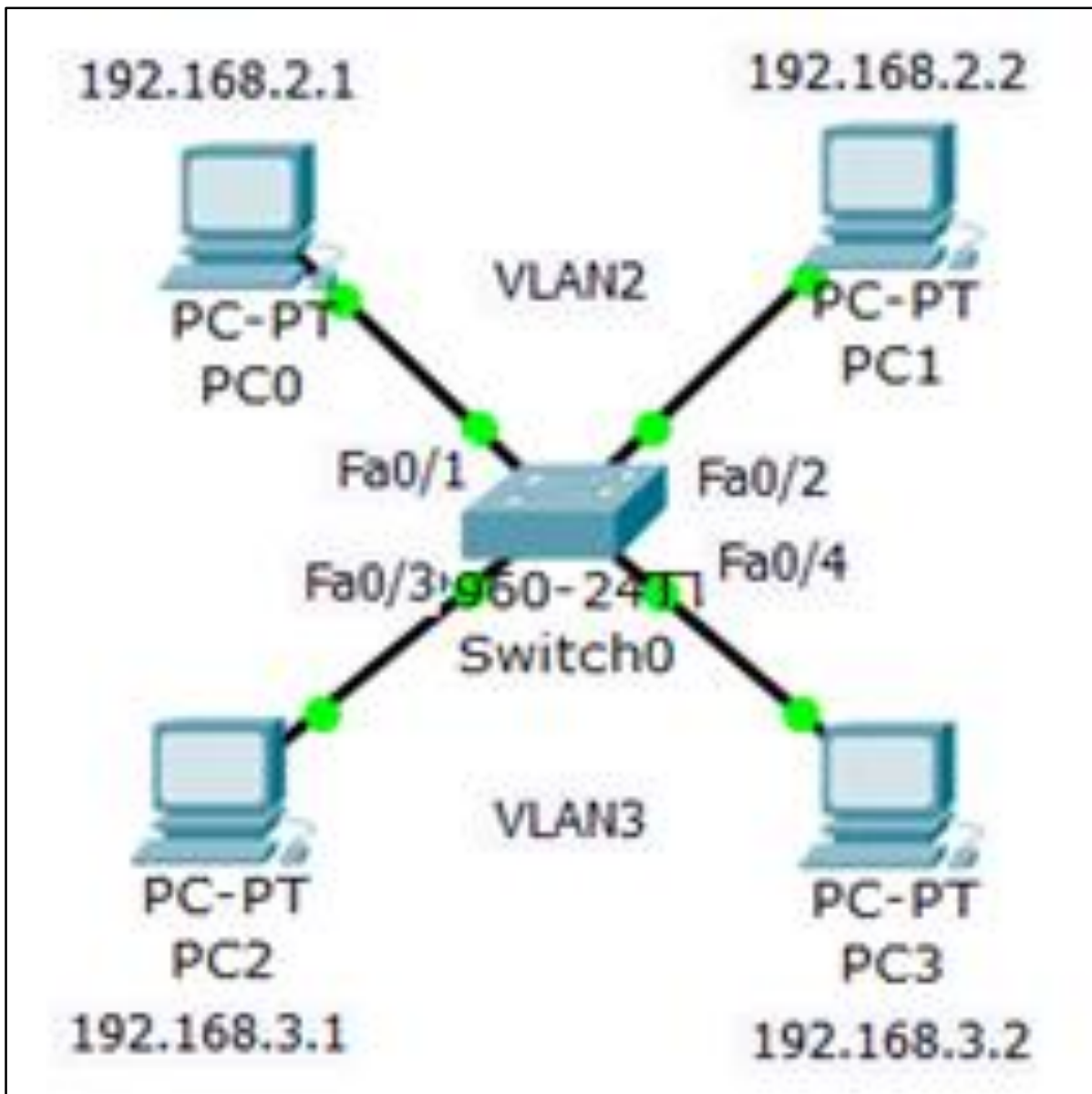


Рисунок 5.11 - IP адреса компьютеров

11. Проверьте связь ПК в пределах VLAN и отсутствие связи между VLAN2 и VLAN3 (рисунок 5.12).

Итак, Вы должны убедиться, что компьютер в своем сегменте видит другой компьютер, а в другом сегменте – нет.

Практическая работа 5. Моделирование виртуальных сетей

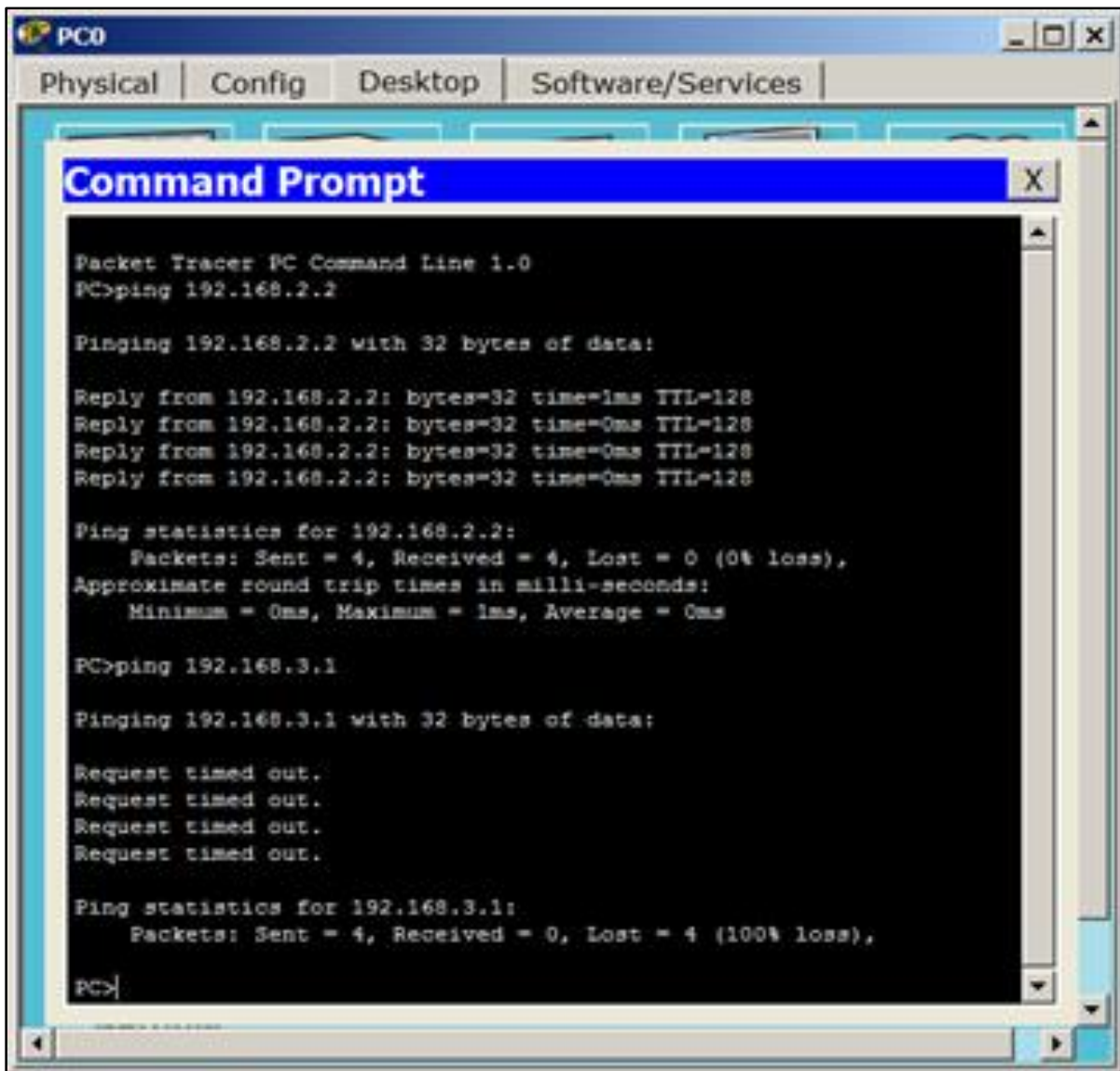


Рисунок 5.12 - Проверка связи ПК в пределах одной VLAN и отсутствие связи между VLAN2 и VLAN3

Практическая работа 5. Моделирование виртуальных сетей

Упражнение 5.2. Настройка виртуальной сети на коммутаторе 2960

Задачей упражнения является приобретение навыка в создании двух независимых групп компьютеров: ПК1-ПК3 должны быть доступны только друг для друга, вторая независимая группа - компьютеры ПК4 и ПК5.

1. Создадим сеть, топология которой представлена на рисунке 5.13.

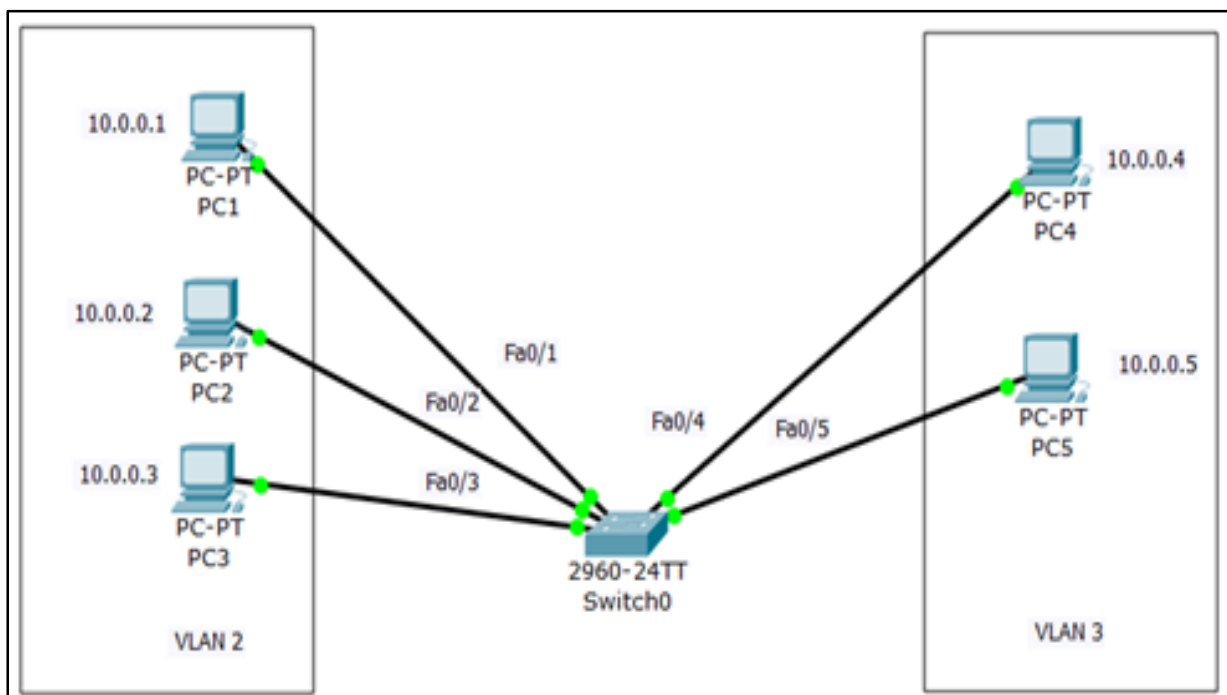


Рисунок 5.13 - Схема сети с одним коммутатором

Настройка коммутатора

2. Сформируйте VLAN2. Дважды щелкните левой кнопкой мыши по коммутатору. В открывшемся окне перейдите на вкладку CLI. Вы увидите окно консоли. Нажмите на клавишу Enter для того, чтобы приступить к вводу команд. Перейдем в привилегированный режим, выполнив команду **enable**:

```
Switch> en.
```

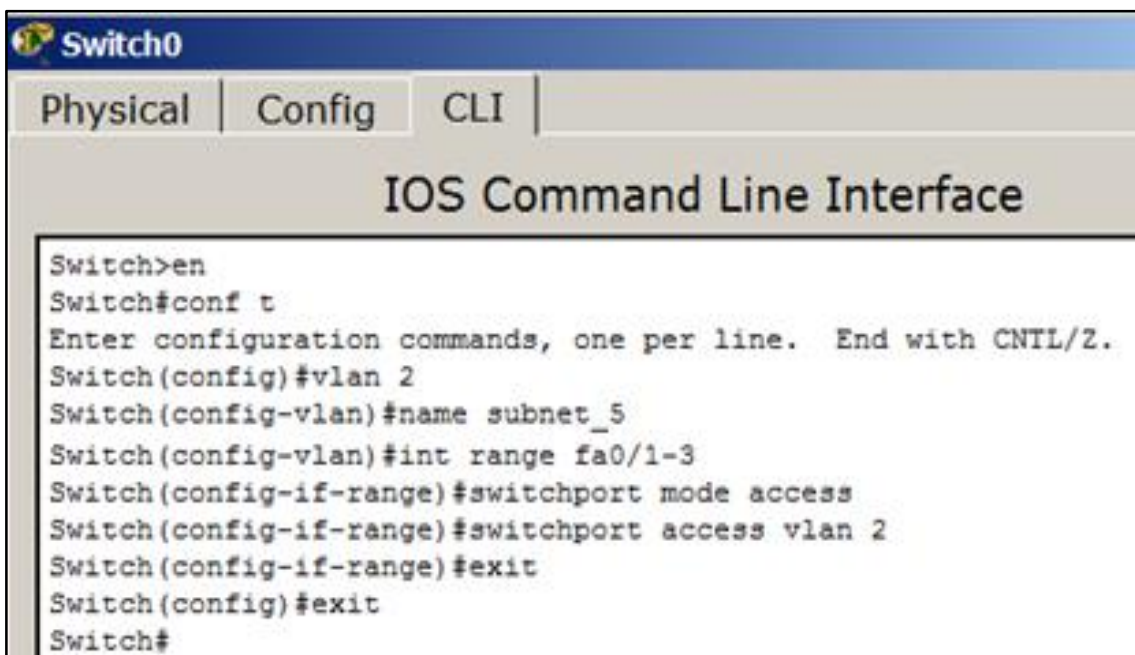
Практическая работа 5. Моделирование виртуальных сетей

3. По умолчанию все ПК объединены в VLAN1. Для реализации сети, которую мы запланировали, создадим на коммутаторе еще два VLAN (2 и 3). Для этого в привилегированном режиме выполните следующую команду для перехода в режим конфигурации:

```
Switch#conf t.
```

4. Введите команду VLAN 2. Данной командой Вы создадите на коммутаторе подсеть VLAN с номером 2. Указатель ввода **Switch (config)#** изменится на **Switch (config-vlan) #**.

Это свидетельствует о том, что Вы конфигурируете уже не весь коммутатор в целом, а только отдельный VLAN, в данном случае VLAN 2 (рисунок 5.14).



```
Switch0
Physical | Config | CLI |
IOS Command Line Interface
Switch>en
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#vlan 2
Switch(config-vlan)#name subnet_5
Switch(config-vlan)#int range fa0/1-3
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 2
Switch(config-if-range)#exit
Switch(config)#exit
Switch#
```

Рисунок 5.14 - Листинг команд для формирования VLAN2

Командой **VLAN2** создайте на коммутаторе новый VLAN с номером 2.

Команда **name subnet_5** присваивает имя **subnet_5** виртуальной сети номер 2.

Практическая работа 5. Моделирование виртуальных сетей

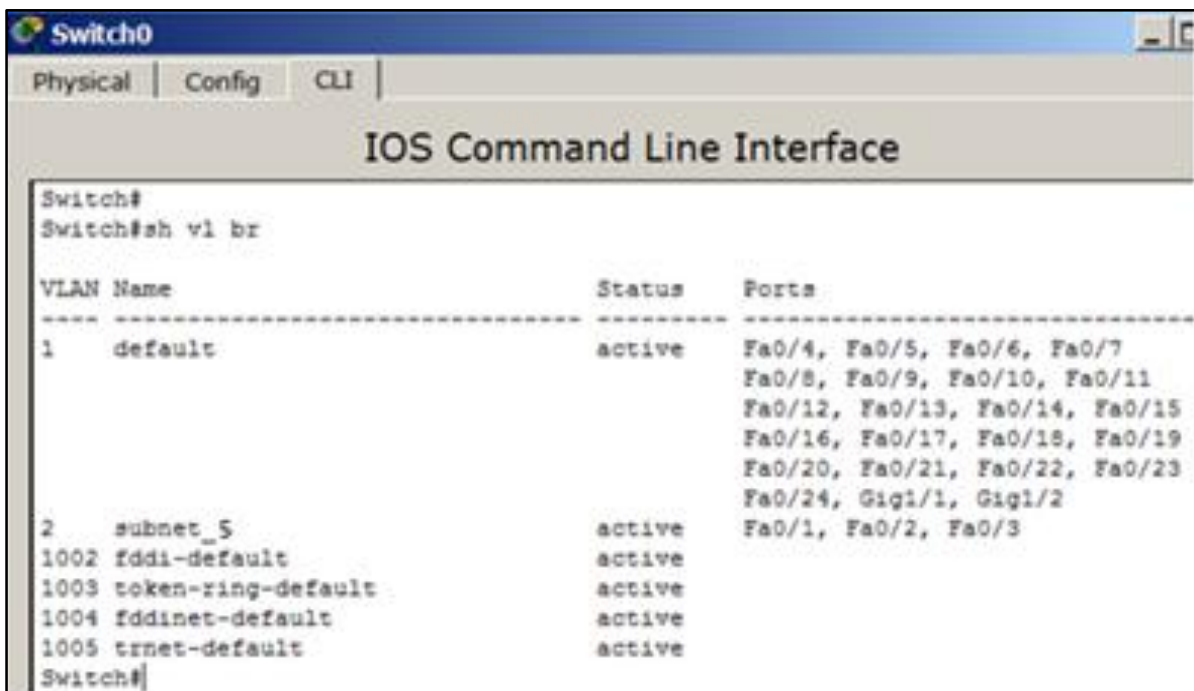
Выполняя команду **interface range fast Ethernet 0/1-3** перейдите к конфигурированию интерфейсов fastEthernet 0/1, fastEthernet 0/2 и fastEthernet 0/3 коммутатора. Слово **range** в данной команде, указывает на то, что конфигурируется не один порт, а диапазон портов.

Команда **switch port mode access** конфигурирует выбранный порт коммутатора, как порт доступа (access порт).

Команда **switch port access vlan 2** указывает, что данный порт является портом доступа для VLAN номер 2.

5. Выйдите из режима конфигурирования, дважды набрав команду **exit** и просмотрите результат конфигурирования, выполнив команду **sh vl br**.

Заметьте (рисунок 5.15), что на коммутаторе появился VLAN с номером 2 и именем **subnet_5**, портами доступа которого являются **fastEthernet 0/1**, **fastEthernet 0/2** и **fastEthernet 0/3**.



```
Switch0
Physical | Config | CLI |
IOS Command Line Interface
Switch#
Switch#sh vl br
VLAN Name                Status   Ports
-----
1    default                 active   Fa0/4, Fa0/5, Fa0/6, Fa0/7
                                           Fa0/8, Fa0/9, Fa0/10, Fa0/11
                                           Fa0/12, Fa0/13, Fa0/14, Fa0/15
                                           Fa0/16, Fa0/17, Fa0/18, Fa0/19
                                           Fa0/20, Fa0/21, Fa0/22, Fa0/23
                                           Fa0/24, Gig1/1, Gig1/2
2    subnet_5                 active   Fa0/1, Fa0/2, Fa0/3
1002 fddi-default          active
1003 token-ring-default    active
1004 fddinet-default       active
1005 trnet-default         active
Switch#
```

Рисунок 5.15 - Информация о VLAN на коммутаторе

Практическая работа 5. Моделирование виртуальных сетей

Команда **shvlbr** выводит информацию о существующих на коммутаторе VLAN-ах. В результате выполнения команды на экране появится: *номера VLAN* (первый столбец), *название VLAN* (второй столбец), *состояние VLAN* (работает он или нет) – третий столбец, *порты*, принадлежащие к данному VLAN (четвертый столбец).

6. Аналогичным образом создайте VLAN 3 с именем **subnet_6** и сделайте его портами доступа интерфейсов **fastEthernet 0/4** и **fastEthernet 0/5**.

Результат показан на рисунке 5.16.

```
Switch>en
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#vlan 3
Switch(config-vlan)#name subnet_6
Switch(config-vlan)#int range fa0/4-5
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 3
Switch(config-if-range)#exit
Switch(config)#exit
Switch#
%SYS-5-CONFIG_I: Configured from console by console

Switch#sh vl br
VLAN Name                Status      Ports
-----
1      default                active     Fa0/6, Fa0/7, Fa0/8,
Fa0/9
                               Fa0/10, Fa0/11, Fa0/12,
Fa0/13
                               Fa0/14, Fa0/15, Fa0/16,
Fa0/17
                               Fa0/18, Fa0/19, Fa0/20,
Fa0/21
                               Fa0/22, Fa0/23, Fa0/24,
Gig0/1
                               Gig0/2
2      subnet_5                active     Fa0/1, Fa0/2, Fa0/3
3      subnet_6                active     Fa0/4, Fa0/5
1002  fddi-default            active
1003  token-ring-default      active
1004  fddinet-default         active
1005  trnet-default           active
Switch#
```

Рисунок 5.16 - Результат настройки на коммутаторе VLAN2 и VLAN3

Практическая работа 5. Моделирование виртуальных сетей

Проверка результатов работы

Сеть настроена и нужно ее протестировать. Результат положительный, если в пределах своей VLAN компьютеры доступны, а компьютеры из разных VLAN не доступны (рисунок 5.17). У нас все пять компьютеров находятся в одной сети 10.0.0.0/8, но они находятся в разных виртуальных локальных сетях.

```
Packet Tracer PC Command Line 1.0
PC>ping 10.0.0.3

Pinging 10.0.0.3 with 32 bytes of data:

Reply from 10.0.0.3: bytes=32 time=1ms TTL=128
Reply from 10.0.0.3: bytes=32 time=0ms TTL=128
Reply from 10.0.0.3: bytes=32 time=0ms TTL=128
Reply from 10.0.0.3: bytes=32 time=0ms TTL=128

Ping statistics for 10.0.0.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

PC>ping 10.0.0.4

Pinging 10.0.0.4 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 10.0.0.4:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Рисунок 5.17 - Пинг с PC1 на PC3 и PC4

Практическая работа 5. Моделирование виртуальных сетей

Упражнение 5.3. VLAN с двумя коммутаторами.

Разделяемый общий канал

На практике часто возникает задача разделения устройств, подключенных к одному или нескольким коммутаторам на несколько непересекающихся локальных сетей. В случае, если используется только один коммутатор, то эта задача решается путем конфигурирования портов коммутатора, указав каждому порту к какой локальной сети он относится. Если же используется несколько коммутаторов, то необходимо между коммутаторами помимо данных передавать информацию к какой локальной сети относится кадр. был разработан стандарт 802.1Q.

1. Произведите дублирование нашей моделируемой сети, той, которая была показана ранее (рисунок 5.13 - Схема сети с одним коммутатором). Для этого выделите всю сеть инструментом Select, и, удерживая клавишу Ctrl, перетащите на новое место в рабочей области программы (рисунок 5.18).

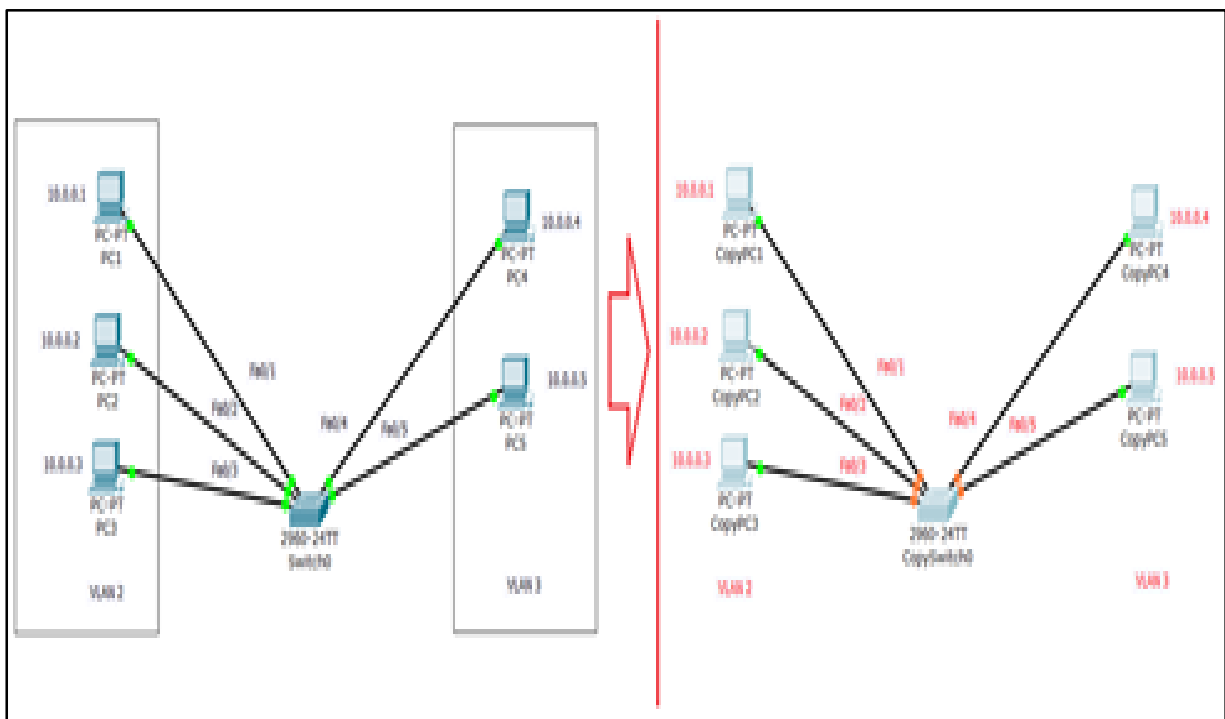


Рисунок 5.18 - Дублируем сеть с одним коммутатором

Практическая работа 5. Моделирование виртуальных сетей

2. Соедините коммутаторы перекрестным кабелем (кроссом) через самые производительные порты – Gigabit Ethernet (рисунок 5.19).

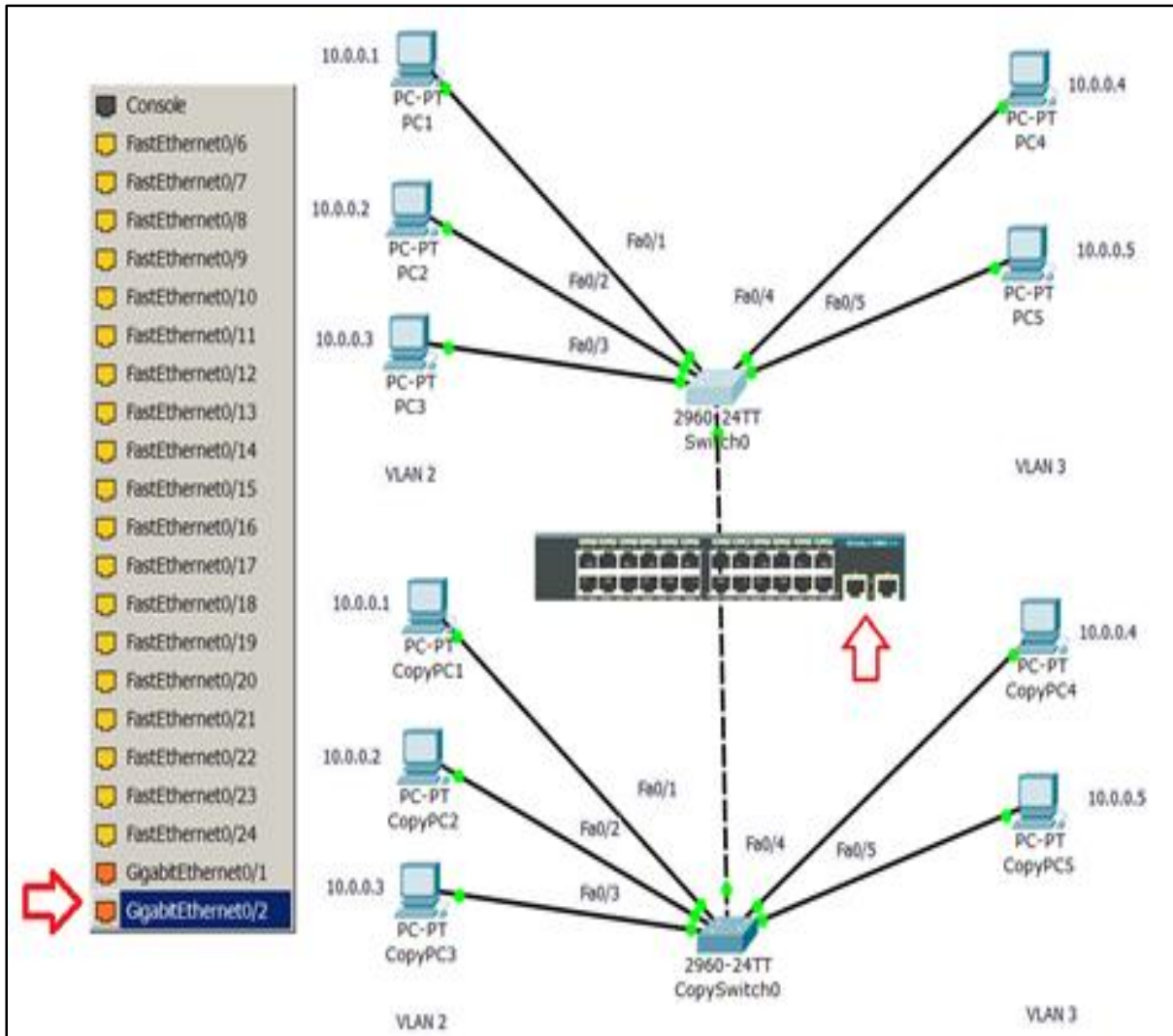


Рисунок 5.19 - Соединение коммутаторов через Gigabit Ethernet порты

Практическая работа 5. Моделирование виртуальных сетей

3. Поправьте настройки на дубликате исходной сети (рисунок 5.20).

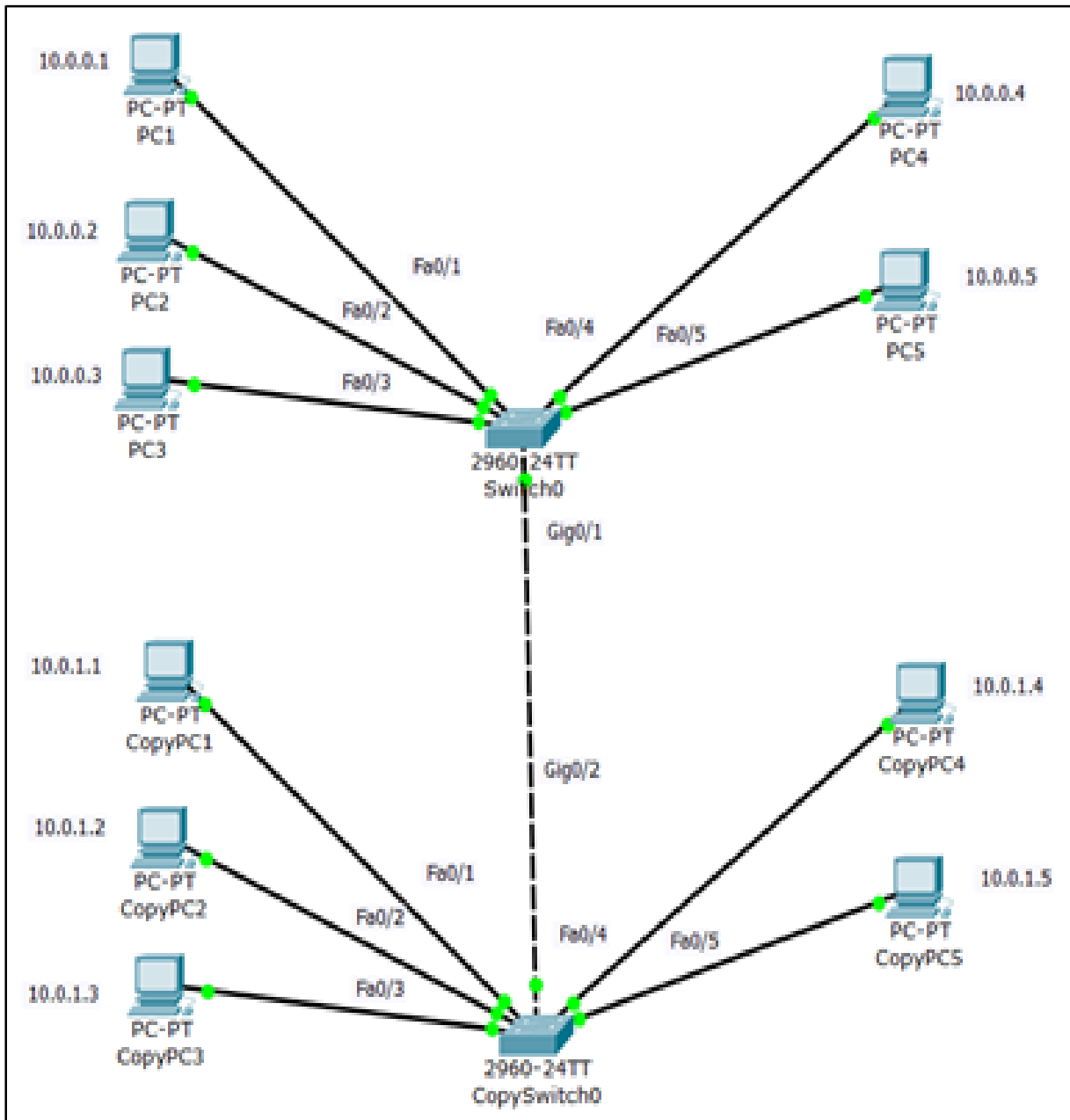


Рисунок 5.20 - Настройка сети-дубликата

4. Укажите новый вариант подсетей VLAN2 и VLAN3, а также выделите trunk связь коммутаторов (рисунок 5.21).

Практическая работа 5. Моделирование виртуальных сетей

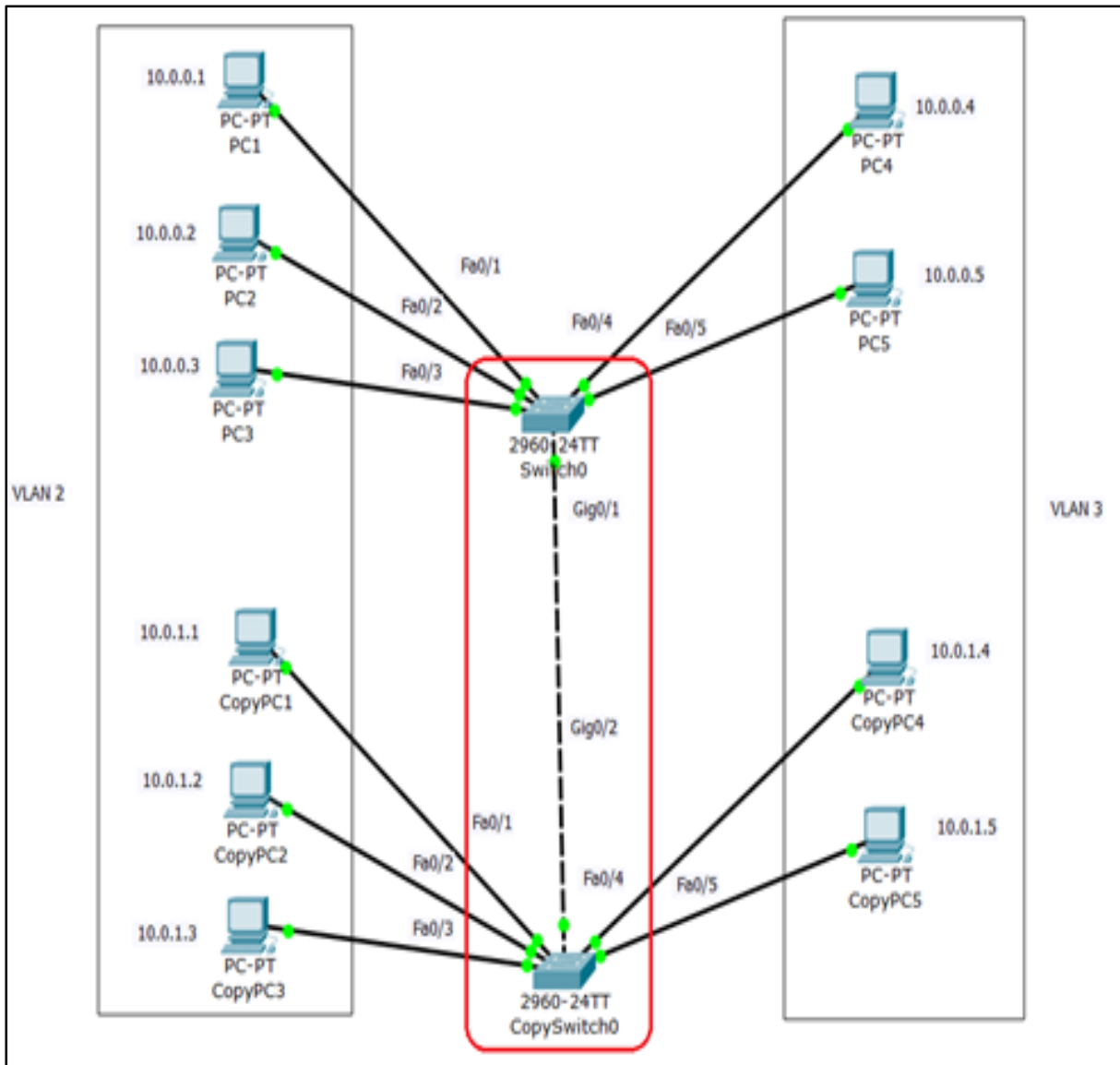
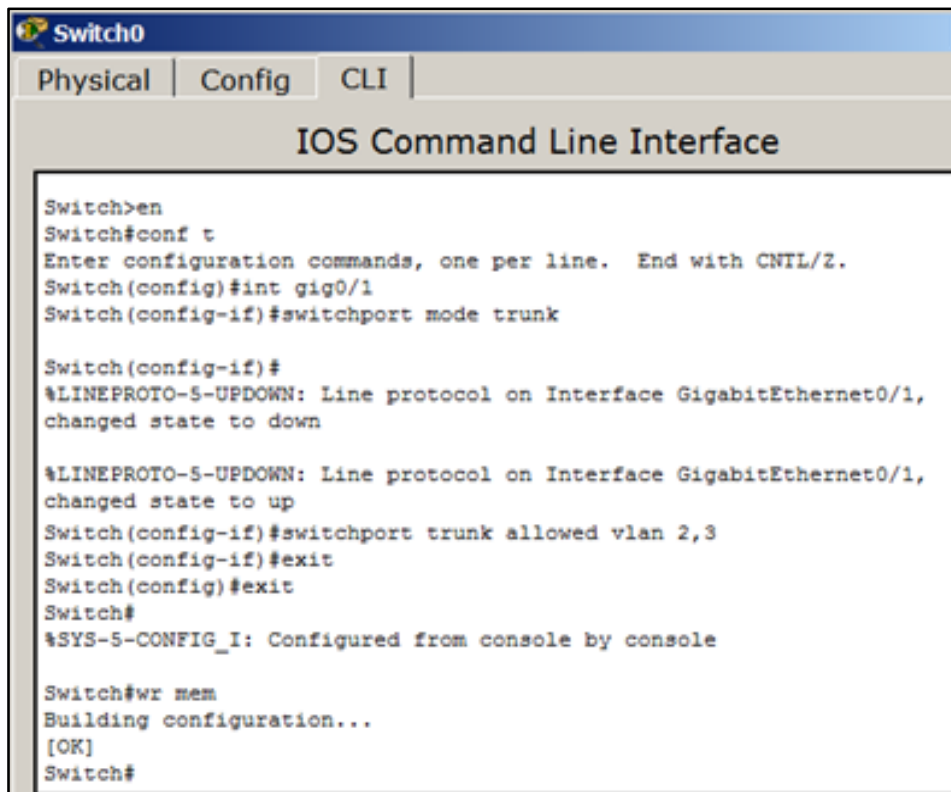


Рисунок 5.21 - Подсети VLAN2 и VLAN3

Настройка транк порта Gig0/1

5. Поменяйте состояние порта и укажите **vlan 2** и **vlan 3** для работы с ним (рисунок 5.22).

Практическая работа 5. Моделирование виртуальных сетей



```
Switch0
Physical | Config | CLI
IOS Command Line Interface

Switch>en
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#int gig0/1
Switch(config-if)#switchport mode trunk

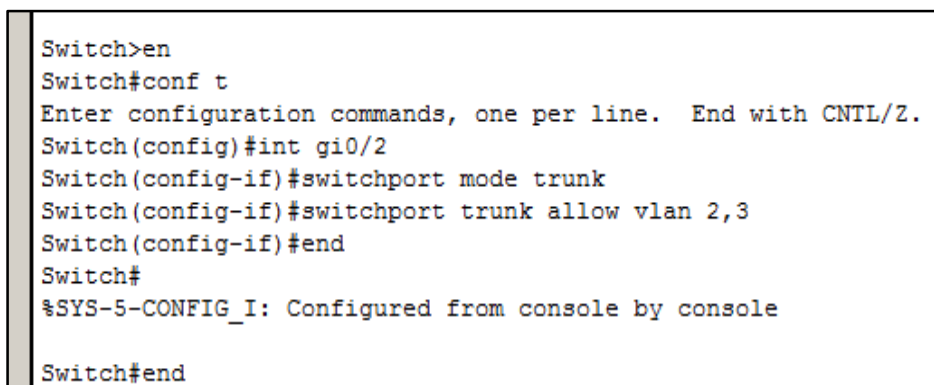
Switch(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1,
changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1,
changed state to up
Switch(config-if)#switchport trunk allowed vlan 2,3
Switch(config-if)#exit
Switch(config)#exit
Switch#
%SYS-5-CONFIG_I: Configured from console by console

Switch#wr mem
Building configuration...
[OK]
Switch#
```

Рисунок 5.22 - Настройка транк порта Gig0/1 на коммутаторе Switch0

6. Транк порт Gig0/2 на коммутаторе CopySwitch0 настройте аналогично (рисунок 5.23).



```
Switch>en
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#int gi0/2
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk allow vlan 2,3
Switch(config-if)#end
Switch#
%SYS-5-CONFIG_I: Configured from console by console

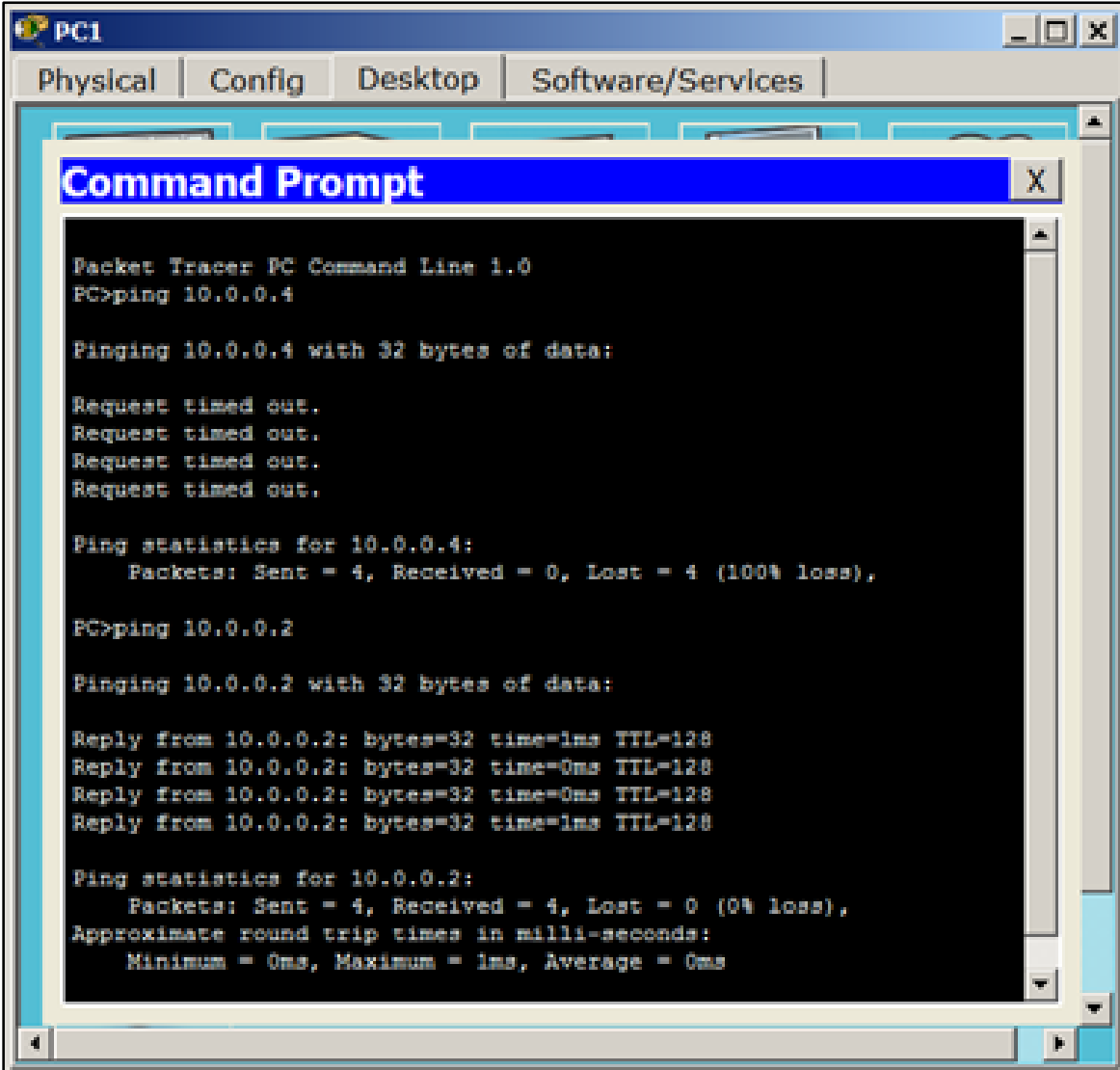
Switch#end
```

Рисунок 5.23 - Настройка trunk порта Gig0/2

Практическая работа 5. Моделирование виртуальных сетей

Диагностика результатов работы

7. Проверьте пинг с PC1 в разные vlan (рисунок 5.24). В пределах своей vlan персональные компьютеры должны быть доступны, а между персональными компьютерами разных vlan связи не должно быть.



```
PC1
Physical | Config | Desktop | Software/Services
-----
Command Prompt
Packet Tracer PC Command Line 1.0
PC>ping 10.0.0.4

Pinging 10.0.0.4 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 10.0.0.4:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

PC>ping 10.0.0.2

Pinging 10.0.0.2 with 32 bytes of data:

Reply from 10.0.0.2: bytes=32 time=1ms TTL=128
Reply from 10.0.0.2: bytes=32 time=0ms TTL=128
Reply from 10.0.0.2: bytes=32 time=0ms TTL=128
Reply from 10.0.0.2: bytes=32 time=1ms TTL=128

Ping statistics for 10.0.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Рисунок 5.24 - Диагностика результатов работы - пинг с PC1 в разные vlan

Практическая работа 5. Моделирование виртуальных сетей

Упражнение 5.4. Настройка виртуальной сети из двух свитчей и четырех ПК

1. Создайте сеть, топология которой представлена на рисунке 5.24. Пока в сети 10.0.0.0 нет разделения на VLAN - все компьютеры доступны между собой.

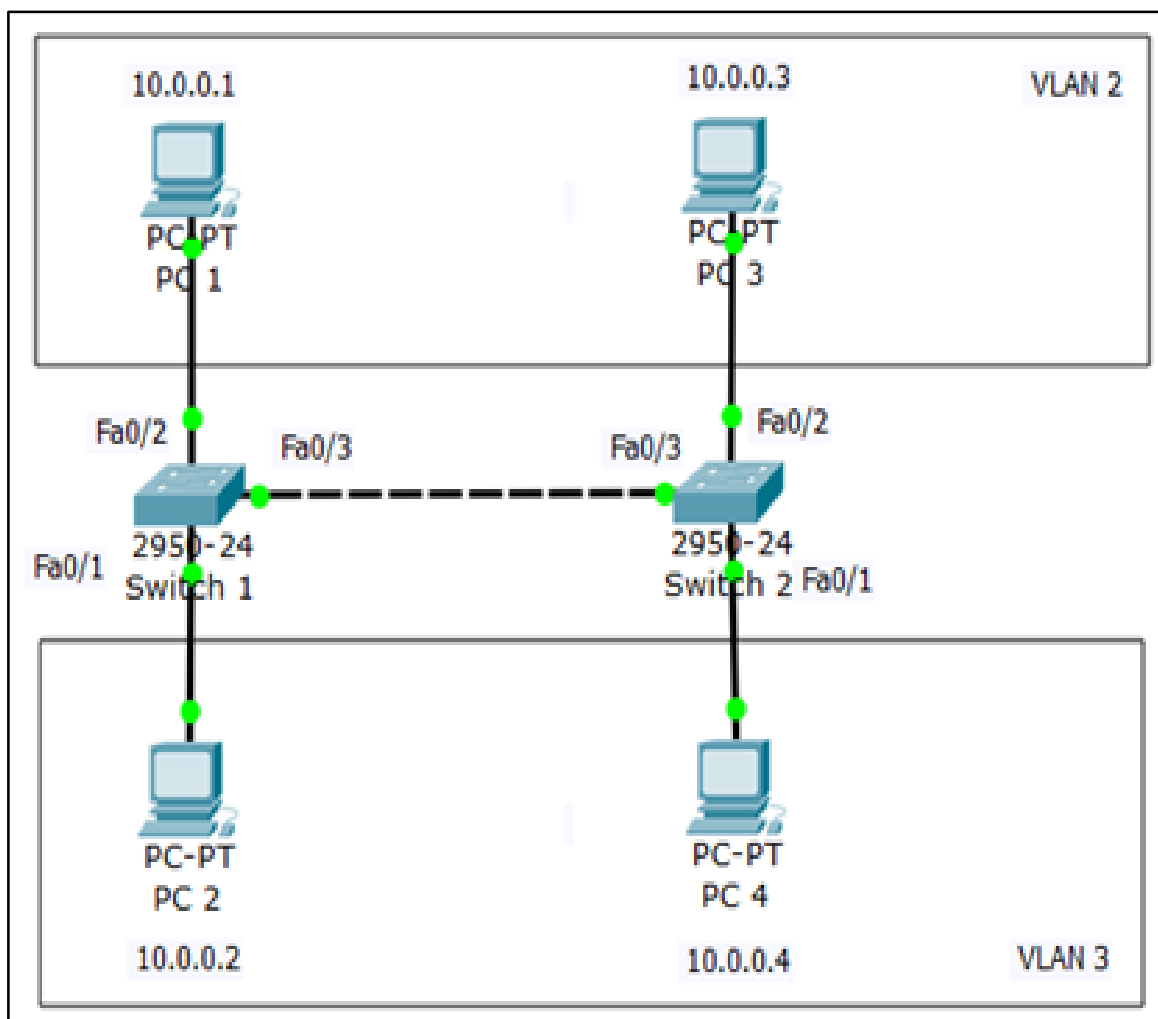


Рисунок 5.25 - Схема сети

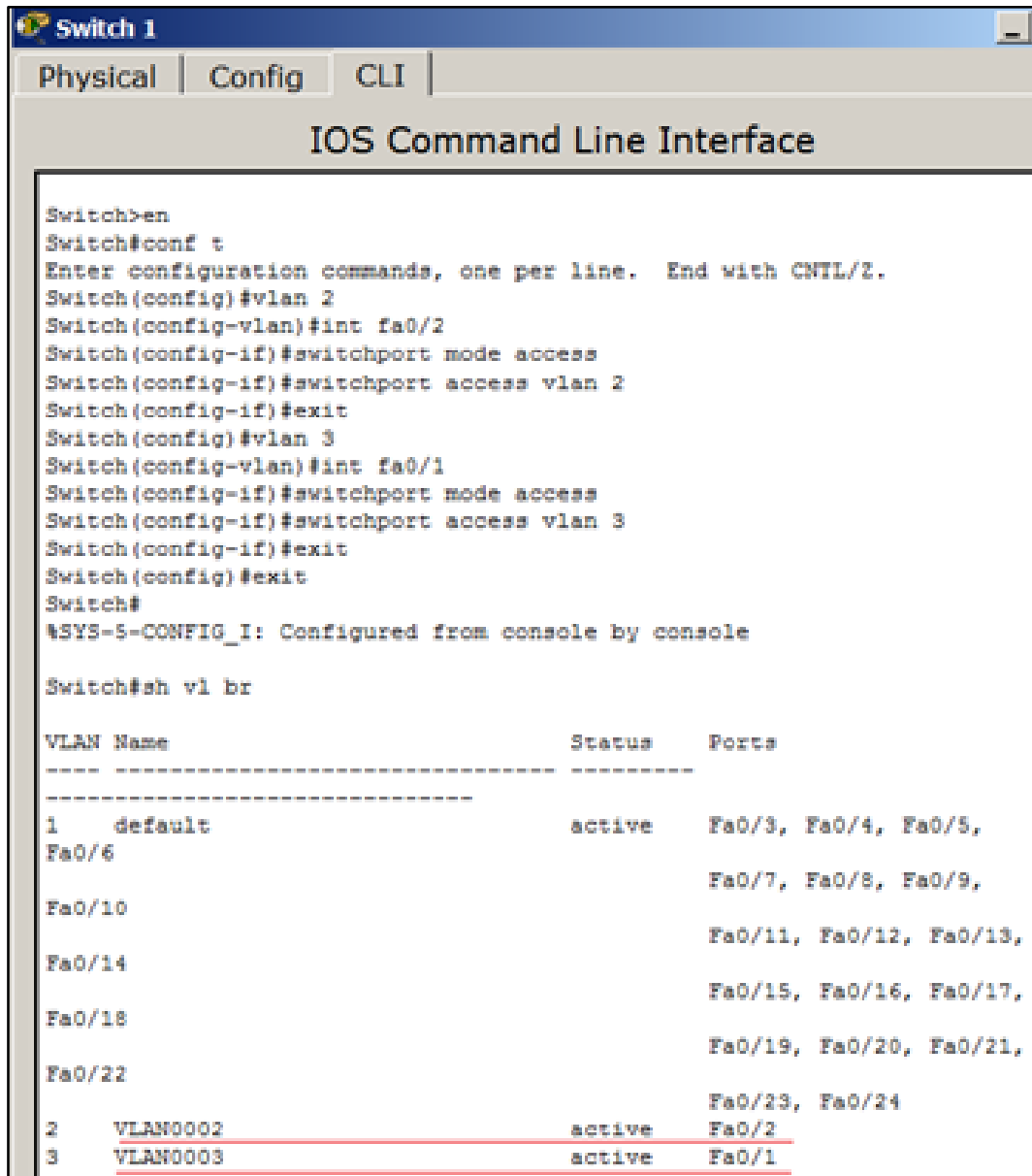
Подсети Vlan 2 принадлежат порты коммутаторов Fa0/2, а Vlan 3 принадлежат порты коммутаторов Fa0/1.

Настройка VLAN 2 и VLAN3

Практическая работа 5. Моделирование виртуальных сетей

2. Настройка коммутатора Switch1. Откройте его консоль. В открывшемся окне перейдите на вкладку CLI, войдите в привилегированный режим и настройте VLAN 2 и VLAN3.

3. Просмотрите информацию о существующих на коммутаторе VLAN-ах командой: **Switch1#sh vl br** (рисунок 5.26).



```
Switch 1
Physical | Config | CLI |
IOS Command Line Interface

Switch>en
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#vlan 2
Switch(config-vlan)#int fa0/2
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 2
Switch(config-if)#exit
Switch(config)#vlan 3
Switch(config-vlan)#int fa0/1
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 3
Switch(config-if)#exit
Switch(config)#exit
Switch#
%SYS-5-CONFIG_I: Configured from console by console

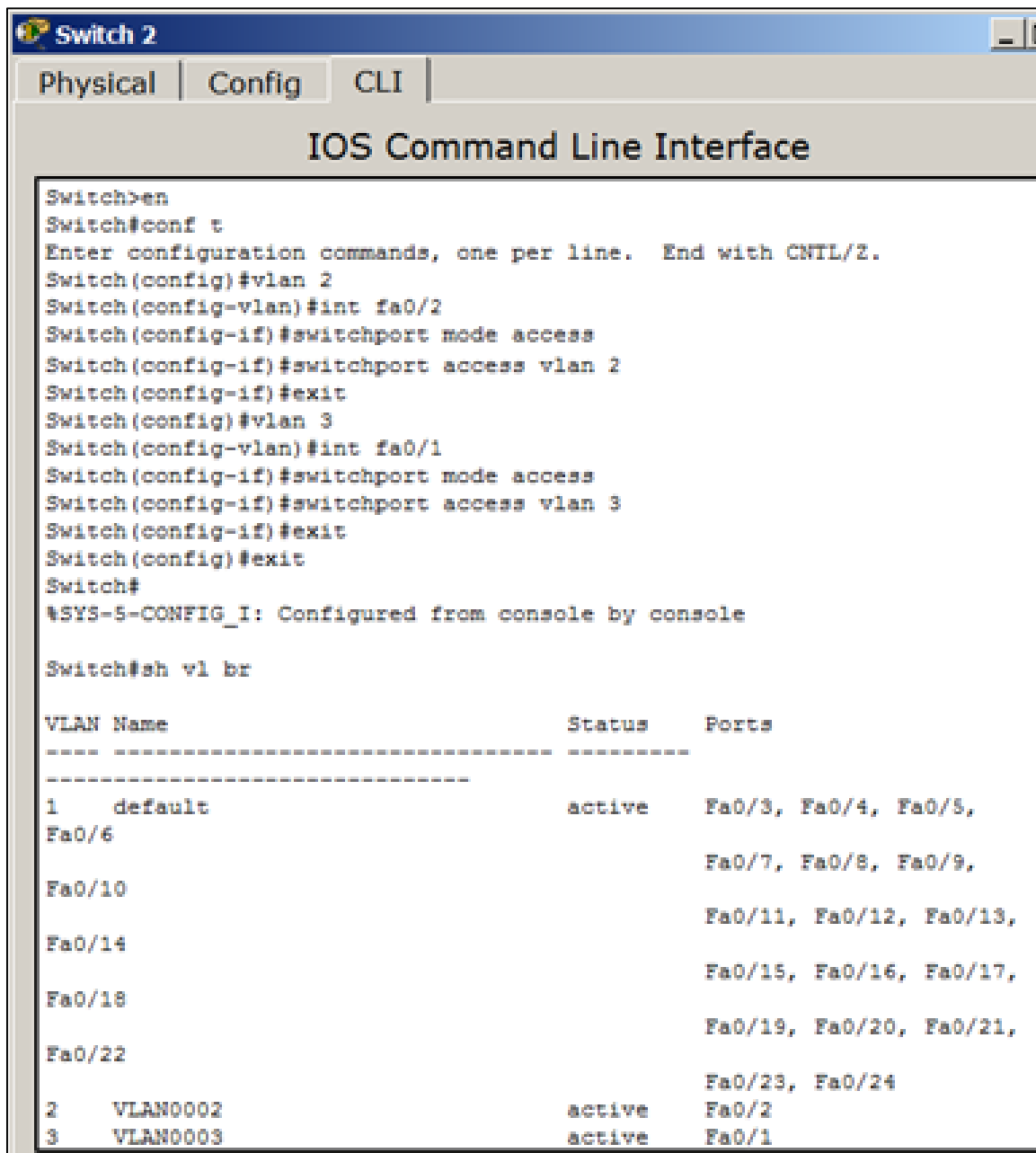
Switch#sh vl br

VLAN Name                Status    Ports
-----
1    default                active    Fa0/3, Fa0/4, Fa0/5,
Fa0/6                    Fa0/7, Fa0/8, Fa0/9,
Fa0/10                   Fa0/11, Fa0/12, Fa0/13,
Fa0/14                   Fa0/15, Fa0/16, Fa0/17,
Fa0/18                   Fa0/19, Fa0/20, Fa0/21,
Fa0/22                   Fa0/23, Fa0/24
2    VLAN0002               active    Fa0/2
3    VLAN0003               active    Fa0/1
```

Рисунок 5.26 - Конфигурация Switch1

Практическая работа 5. Моделирование виртуальных сетей

4. Аналогичным образом сконфигурируйте Switch2, исходя из того, что по условиям задачи у нас Fa0/2 расположен в Vlan2, а Fa0/1 находится в Vlan 3. Результат конфигурирования Switch2 показан на рисунке 5.27.



```
Switch 2
Physical | Config | CLI
IOS Command Line Interface

Switch>en
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#vlan 2
Switch(config-vlan)#int fa0/2
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 2
Switch(config-if)#exit
Switch(config)#vlan 3
Switch(config-vlan)#int fa0/1
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 3
Switch(config-if)#exit
Switch(config)#exit
Switch#
%SYS-5-CONFIG_I: Configured from console by console

Switch#sh vl br

VLAN Name                Status    Ports
-----
1    default                active    Fa0/3, Fa0/4, Fa0/5,
Fa0/6                    Fa0/7, Fa0/8, Fa0/9,
Fa0/10                   Fa0/11, Fa0/12, Fa0/13,
Fa0/14                   Fa0/15, Fa0/16, Fa0/17,
Fa0/18                   Fa0/19, Fa0/20, Fa0/21,
Fa0/22                   Fa0/23, Fa0/24
2    VLAN0002               active    Fa0/2
3    VLAN0003               active    Fa0/1
```

Рисунок 5.27 - Конфигурация Switch2

Практическая работа 5. Моделирование виртуальных сетей

Итак, подсети Vlan 2 принадлежат порты коммутаторов Fa0/2, а Vlan 3 принадлежат порты коммутаторов Fa0/1. Поскольку в данный момент нет обмена информации о подсетях, то все компьютеры разобщены (рисунок 5.28).

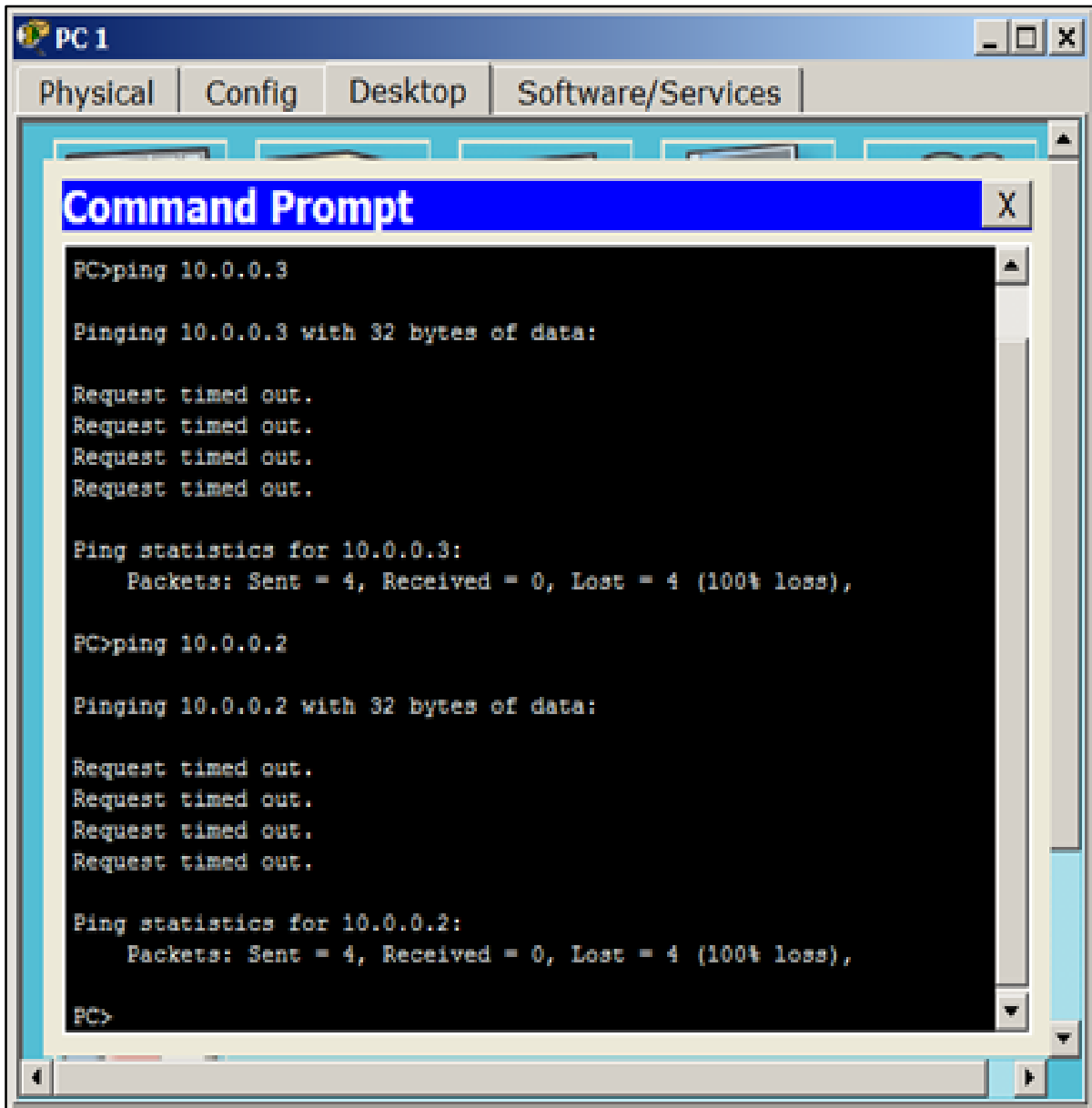
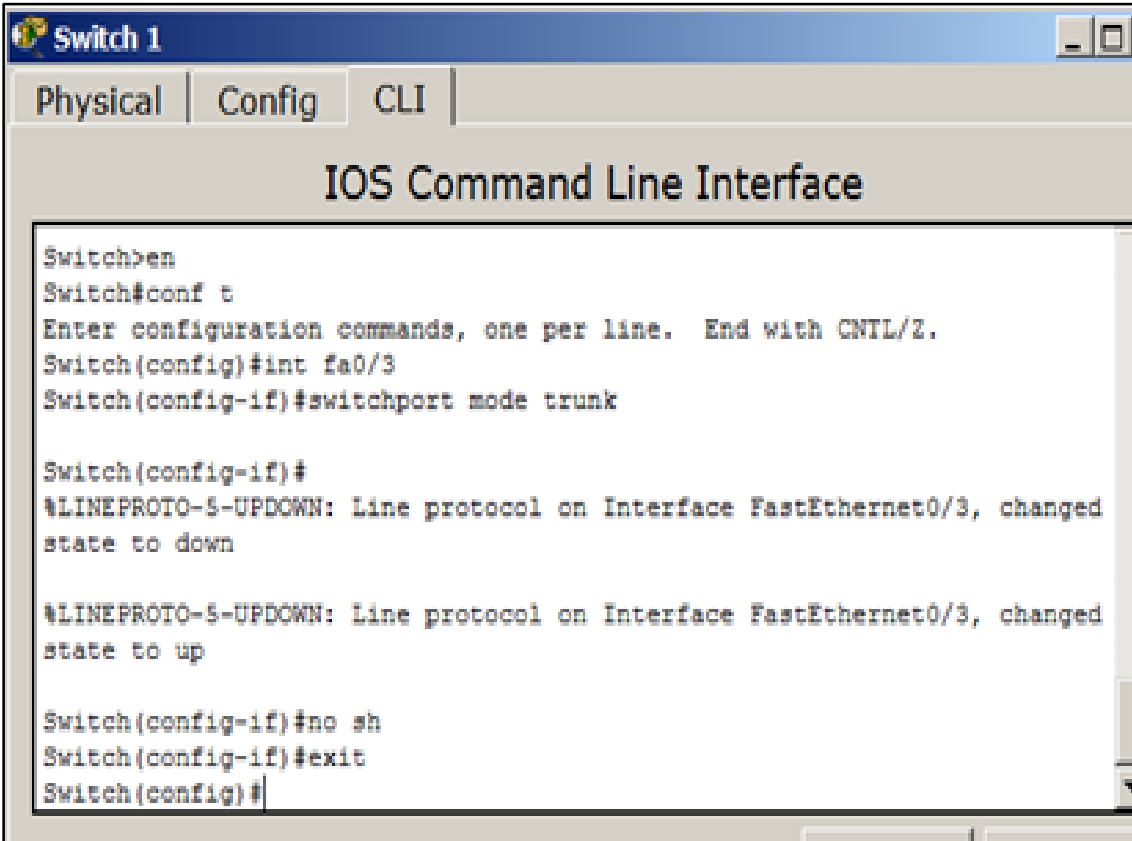


Рисунок 5.28 - Связей между ПК нет

Практическая работа 5. Моделирование виртуальных сетей

Настройка связи коммутаторов через транковый порт

5. Настройте третий порт Fa0/3 на каждом коммутаторе как транковый. Войдите в консоль коммутатора Switch1 и задайте транковый порт (рисунок 5.29).



```
Switch 1
Physical | Config | CLI
IOS Command Line Interface

Switch>en
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#int fa0/3
Switch(config-if)#switchport mode trunk

Switch(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed
state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed
state to up

Switch(config-if)#no sh
Switch(config-if)#exit
Switch(config)#
```

Рисунок 5.29 - Транковый порт на Switch 1

6. Откройте конфигурацию коммутатора Switch 1 на интерфейсе FastEthernet 0/3 и убедитесь, что порт транковый (рисунок 5.30).

Практическая работа 5. Моделирование виртуальных сетей

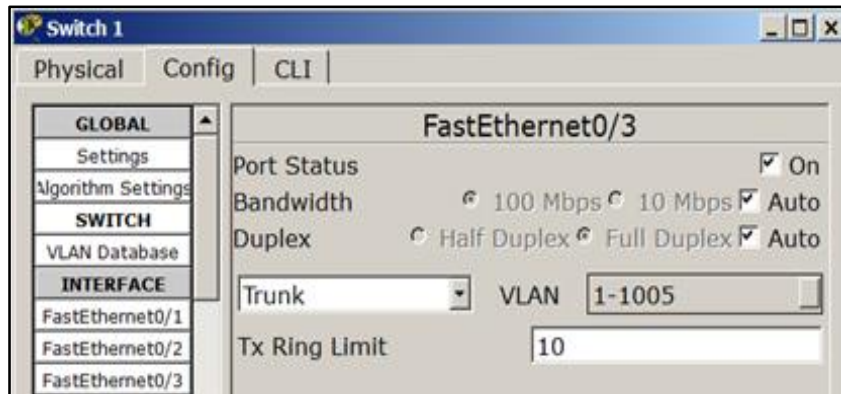


Рисунок 5.30 - Конфигурация интерфейса FastEthernet0/3 на Switch1

7. На коммутаторе Switch2 интерфейс FastEthernet 0/3 автоматически настроится как транковый (рисунок 5.31). Теперь компьютеры, входящие в одну виртуальную сеть, должны пинговаться, а компьютеры в разных подсетях будут взаимно недоступны (рисунок 5.32).

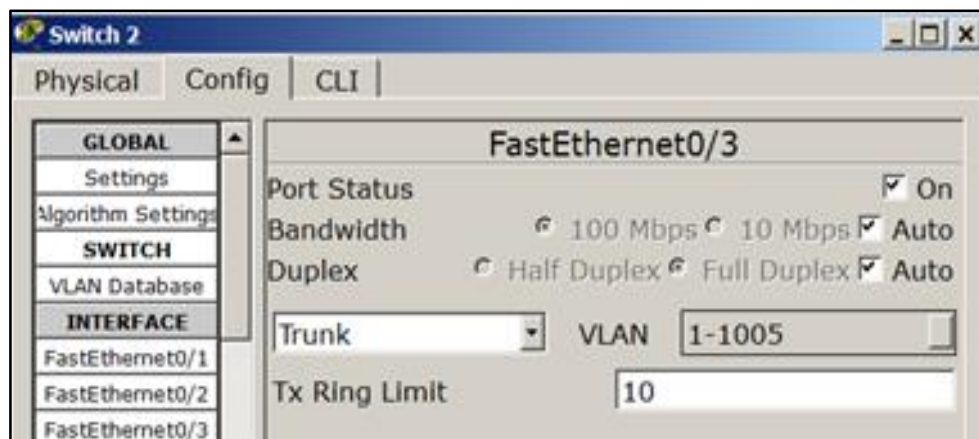


Рисунок 5.31 - Конфигурация интерфейса FastEthernet0/3 на Switch2

Практическая работа 5. Моделирование виртуальных сетей

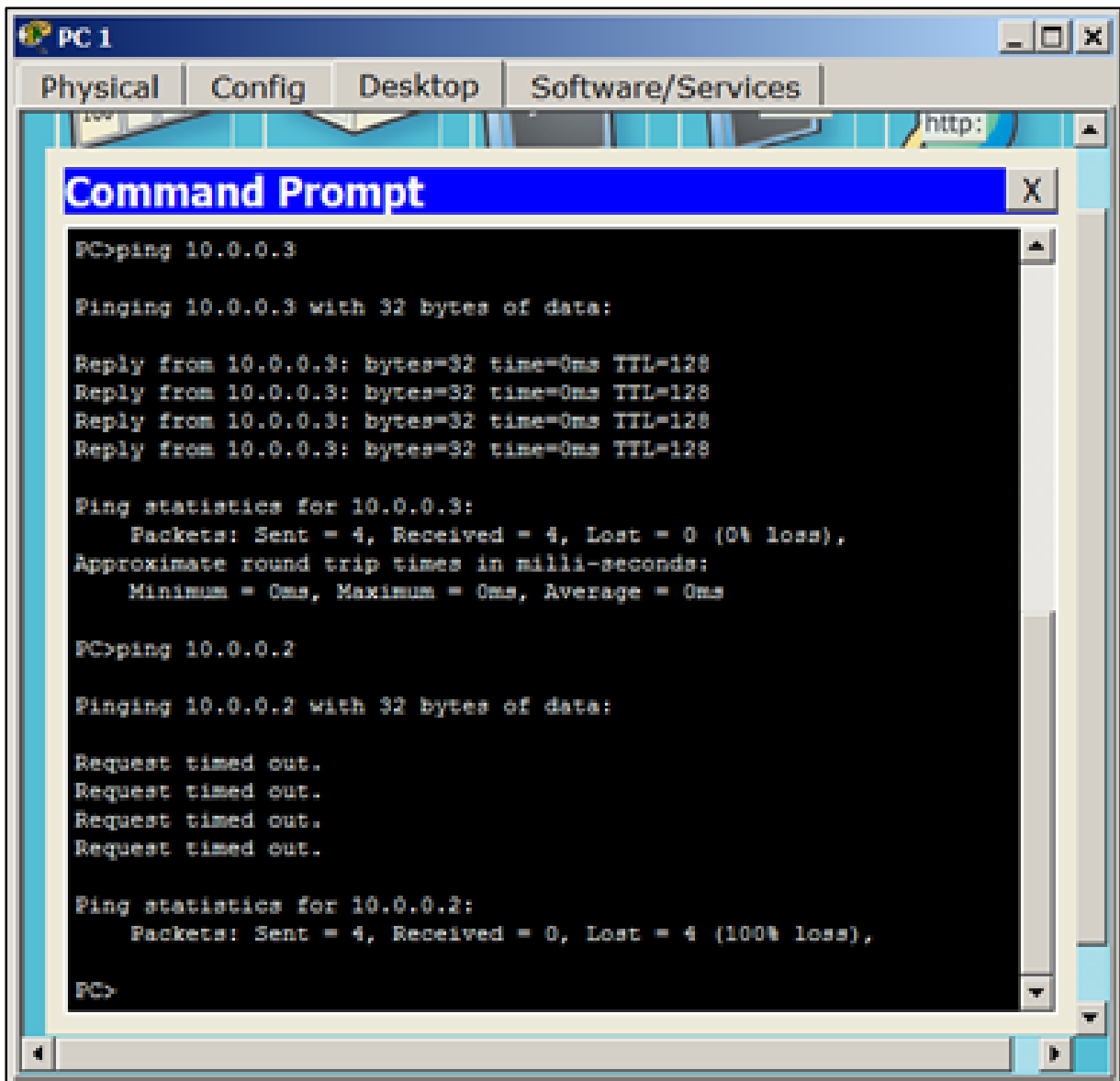


Рисунок 5. 32 - Проверка связи PC1 с ПК в VLAN 2 и VLAN 3

Практическая работа 5. Моделирование виртуальных сетей

Упражнение 5.5. Настройка VLAN в корпоративной сети

Создайте следующую схему сети (рисунок 5.33):

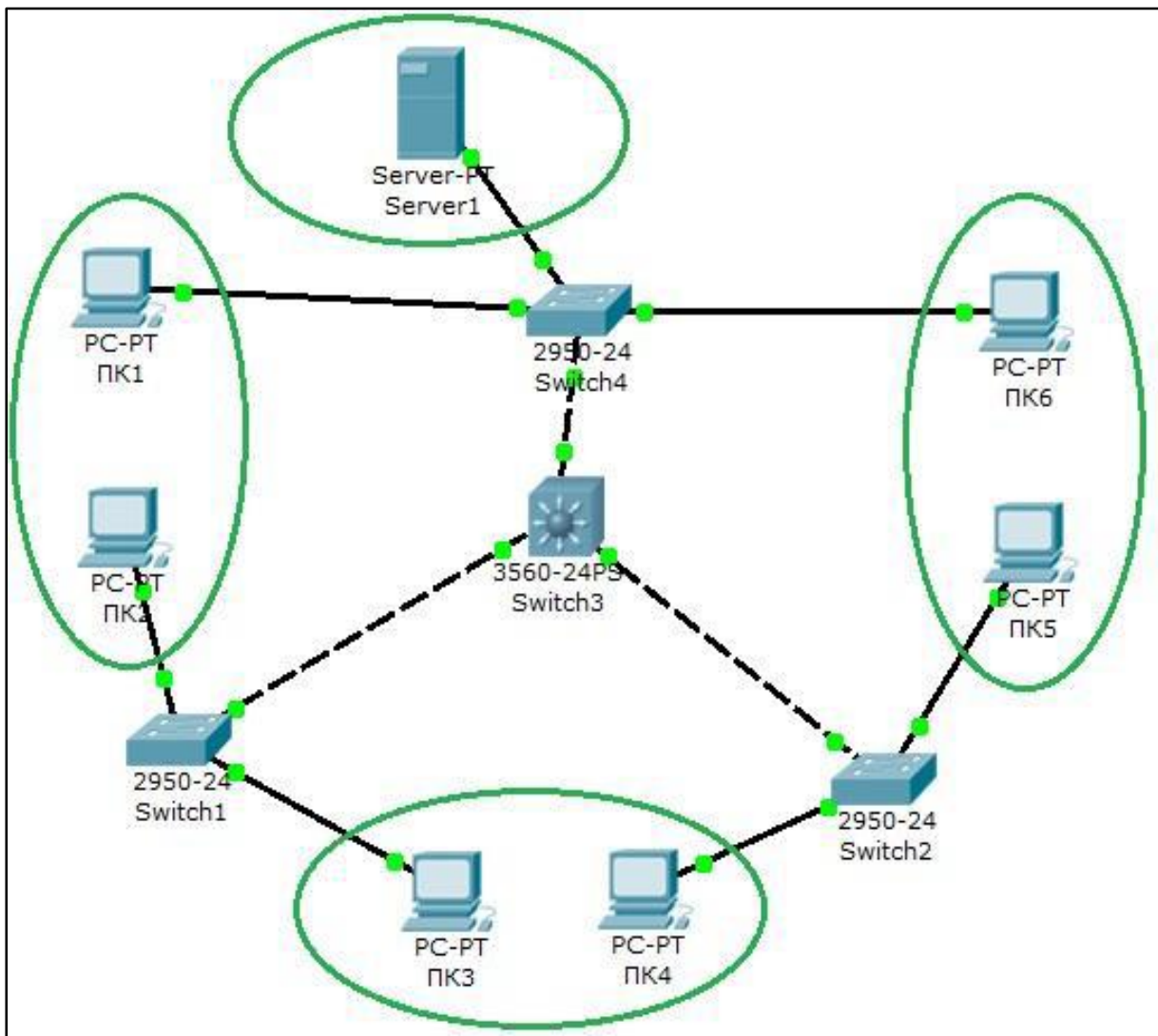


Рисунок 5. 33 - Схема корпоративной сети

Состав сети:

- три коммутатора второго уровня распределения 2950-24 (Switch1, Switch2, Switch4);
- центральный коммутатор третьего уровня 3560-24PS (Switch3), выполняющий роль роутера;

Практическая работа 5. Моделирование виртуальных сетей

=====

- сервер (Server1);
- три подсети по два узла в каждой

Задача:

Для любого вилана могут быть доступны только узлы этого же вилана и сервер Server1.

В таблице 5.1 и 5.2 приведены данные для установки параметров компьютеров и коммутаторов.

Таблица 5.1 - Конфигурация компьютеров

Компьютер	IP адрес	Коммутатор	Порт коммутатора	VLAN
ПК1	10.11.0.11/16	Switch4	4	VLAN 11
ПК2	10.11.0.2/16	Switch1	1	VLAN 11
ПК3	10.13.0.3/16	Switch1	2	VLAN 13
ПК4	10.13.0.4/16	Switch2	1	VLAN 13
ПК5	10.12.0.5/16	Switch2	2	VLAN 12
ПК6	10.12.0.6/16	Switch4	2	VLAN 12
Server1	10.10.0.7/16	Switch4	1	VLAN 10

Таблица 5.2 - Связь коммутаторов по портам

Порт центрального коммутатора Switch3	Порт коммутатора второго уровня распределения
1	Switch1 – 3 порт
2	Switch4 – 3 порт
3	Switch2 – 3 порт

После настройки всех коммутаторов установите шлюзы на всех компьютерах и сервере.

Сконфигурируйте центральный коммутатор:

Этап 1. Перейдите к конфигурации центрального коммутатора **Switch3** и создайте на нем базу VLAN.

1. Создайте VLAN 10:

Практическая работа 5. Моделирование виртуальных сетей

```
Switch3>en
Switch3#conf t
Switch3 (config) #vlan 10
Switch3 (config-vlan) #exit
```

2. Создайте VLAN 11, VLAN 12 и VLAN 13.
3. Настройте протокол VTP в режиме сервера:

```
Switch3 (config) #vtp domain HOME
Switch3 (config) #vtp password HOME
Switch3 (config) #vtp mode server
```

4. Просмотрите информацию о конфигурации VTP:

```
Switch#sh vtp status
```

5. Настройте все интерфейсы на транк:

```
Switch3 (config) #int fa0/1
Switch3 (config-if) #switchport mode trunk
Switch3(config-if) #exit
```

и повторите эти настройки для второго и третьего интерфейсов.

Этап 2. Перейдите к конфигурации коммутатора **Switch4** и переведите его в режим **client**:

1. Создайте на коммутаторе VLAN 10 и задайте в нем порт 1 как **access** порт:

```
Switch4>en
Switch4#conf t
Switch4 (config) #vlan 10
Switch4 (config-vlan) #exit
Switch4 (config) #int fa0/1
Switch4 (config-if) #switchport access vlan 10
Switch4 (config-if) #switchport mode access
Switch4(config-if) #no shut
```

Практическая работа 5. Моделирование виртуальных сетей

=====

2. Создайте на коммутаторе VLAN 11 и задайте в нем порт 4 как **access** порт.

3. Создайте на коммутаторе VLAN 12 и задайте в нем порт 2 как **access** порт.

4. Переведите коммутатор в режим **clint**:

```
Switch4 (config) #vtp domain HOME
Switch4 (config) #vtp password HOME
Switch4 (config) #vtp mode client
```

При вводе имени домена и пароля соблюдайте нужный регистр.

Этап 4. Перейдите к конфигурации коммутатора **Switch1** и выполните следующие настройки:

1. Создайте на коммутаторе VLAN 11 и задайте в нем порт 1 как **access** порт.

2. Создайте на коммутаторе VLAN 13 и задайте в нем порт 2 как **access** порт.

3. Переведите коммутатор в режим **client**.

Этап 5. Перейдите к конфигурации коммутатора **Switch2**.

1. Создайте на коммутаторе VLAN 12 и задайте в нем порт 2 как **access** порт.

2. Создайте на коммутаторе VLAN 13 и задайте в нем порт 1 как **access** порт.

3. Переведите коммутатор в режим **client**.

Этап 6. Проверьте работоспособность сети на канальном уровне модели OSI.

После установки всех настроек таблица VLAN разойдется по коммутаторам с помощью протокола VTP.

В результате компьютеры, расположенные в одном виллане, будут доступны друг для друга, а другие компьютеры недоступны. Проверьте связь командой PING между следующими парами компьютеров:

- ПК1 – ПК2;
- ПК3 – ПК4;
- ПК5 – ПК6.

Практическая работа 5. Моделирование виртуальных сетей

=====

Если Вы все сделали правильно, то ping между парами пройдет, если нет – проверьте следующие установки:

- транковыми портами являются: на **Switch3** все порты, на **Switch1**, **Switch2** и **Switch4** – третий порт;
- соединения интерфейсов на коммутаторах;
- названия и пароли доменов на каждом коммутаторе (команда **sh vtp status**);
- привязку интерфейсов к вилланам на коммутаторах (команда **sh vl br**).

Этап 7. Настройка маршрутизации на центральном коммутаторе. Создадим интерфейсы для каждого VLAN.

Настройка интерфейса для **vlan 10** (шлюз по умолчанию):

```
Switch3 (config) #int vlan 10
Switch3 (config-if) #ip address 10.10.0.1
255.255.0.0
Switch3 (config-if) #no shut
Switch3 (config-if) #exit
```

Повторите эти настройки для каждого VLAN, задавая адрес IP: 10. [VLAN].0.1 и маску /16.

После этого зайдите в настройки каждого компьютера и установите нужный шлюз по умолчанию. Например, для ПК1 – 10.11.0.1.

Включите маршрутизацию командой:

```
Switch3(config)#ip routing
```

Этап 8. Проверьте работоспособность сети на сетевом уровне модели OSI.

После включения маршрутизации все компьютеры будут доступны с любого хоста.

Этап 9. Выполним основную задачу работы: для любого вилана могут быть доступны только узлы этого же вилана и сервер **Server1**.

Для этого введем следующие ограничения на трафик сети:

- 1 - Разрешить пакеты от любого хоста к серверу.
- 2 - Разрешить пакеты от сервера до любого хоста.
- 3 – Трафик от одной подсети к этой же подсети разрешить.

Практическая работа 5. Моделирование виртуальных сетей

4 – Правило по умолчанию: запретить всё остальное.

Ограничения на трафик сети задаются с помощью команды фильтрации **access-list**. Данная команда задает критерии фильтрации в списке опций разрешения и запрета, называемом списком доступа. Списки доступа имеют два правила: **permit** – разрешить и **deny** – запретить. Данные правила либо пропускают пакет дальше по сети, либо блокируют его доступ.

Открываем центральный коммутатор (**Switch3**) и меняем его конфигурацию с помощью команды фильтрации **access-list**:

```
Switch3 (config) #ip access-list extended 100
(создается расширенный список доступа под номером 100)
Switch3 (config-ext-nacl) #permit ip any
    10.10.0.0 0.0.0.255
Switch3 (config-ext-nacl) #permit ip 10.10.0.0
    0.0.0.255 any
(разрешается доступ к сети 10.10.0.0/24)
Switch3 (config-ext-nacl) #permit ip 10.11.0.0
    0.0.0.255 10.11.0.0 0.0.0.255
Switch3 (config-ext-nacl) #permit ip 10.12.0.0
    0.0.0.255 10.12.0.0 0.0.0.255
Switch3 (config-ext-nacl) #permit ip 10.13.0.0
    0.0.0.255 10.13.0.0 0.0.0.255
(разрешается: доступ из сети 10.11.0.0/24 в эту же сеть;
доступ из сети 10.12.0.0/24 в эту же сеть;
доступ из сети 10.13.0.0/24 в эту же сеть).
Switch3 (config-ext-nacl) #exit
```

Теперь этот **access-list** наложим на конкретный интерфейс и применим ко всем VLAN-ам на входящий трафик (опция **in** – на входящий трафик, **out** – на исходящий трафик):

```
Switch3 (config) #int vlan 10
Switch3 (config-if) #ip access-group 100 in
```

Этот шаг повторяем для каждого из VLAN-ов.

Практическая работа 5. Моделирование виртуальных сетей

=====

В результате получим: для любого вилана могут быть доступны только узлы этого же вилана и сервер **Server1**.

Контрольные вопросы

1. Для чего создаются виртуальные локальные сети? Каковы их достоинства?
2. Как связываются между собой VLAN и порты коммутатора?
3. Как обеспечивается общение между узлами разных виртуальных сетей?
4. Как обеспечивается управление виртуальными локальными сетями?
5. Можно ли построить VLAN на нескольких коммутаторах? Как это сделать?
6. Для чего служит идентификатор кадра (tag)? Где он размещается?
7. Что такое транк? Как он создается на коммутаторе и маршрутизаторе?
8. Какие команды используются для назначения VLAN на интерфейсы?
9. Какие команды используются для создания транковых соединений?
10. Какие команды используются для верификации VLAN?

Задания

Задание 5.1

Выполните на своем компьютере все упражнения. Отчет должен содержать скриншоты с экрана вашего компьютера, позволяющие судить о том, что основные результаты последовательного выполнения упражнений выполнены корректно и в надлежащей последовательности.

Практическая работа 5. Моделирование виртуальных сетей

Задание 5.2

На предприятии имеется два отдела, схема сетей которых представлена на рисунке 5.34.

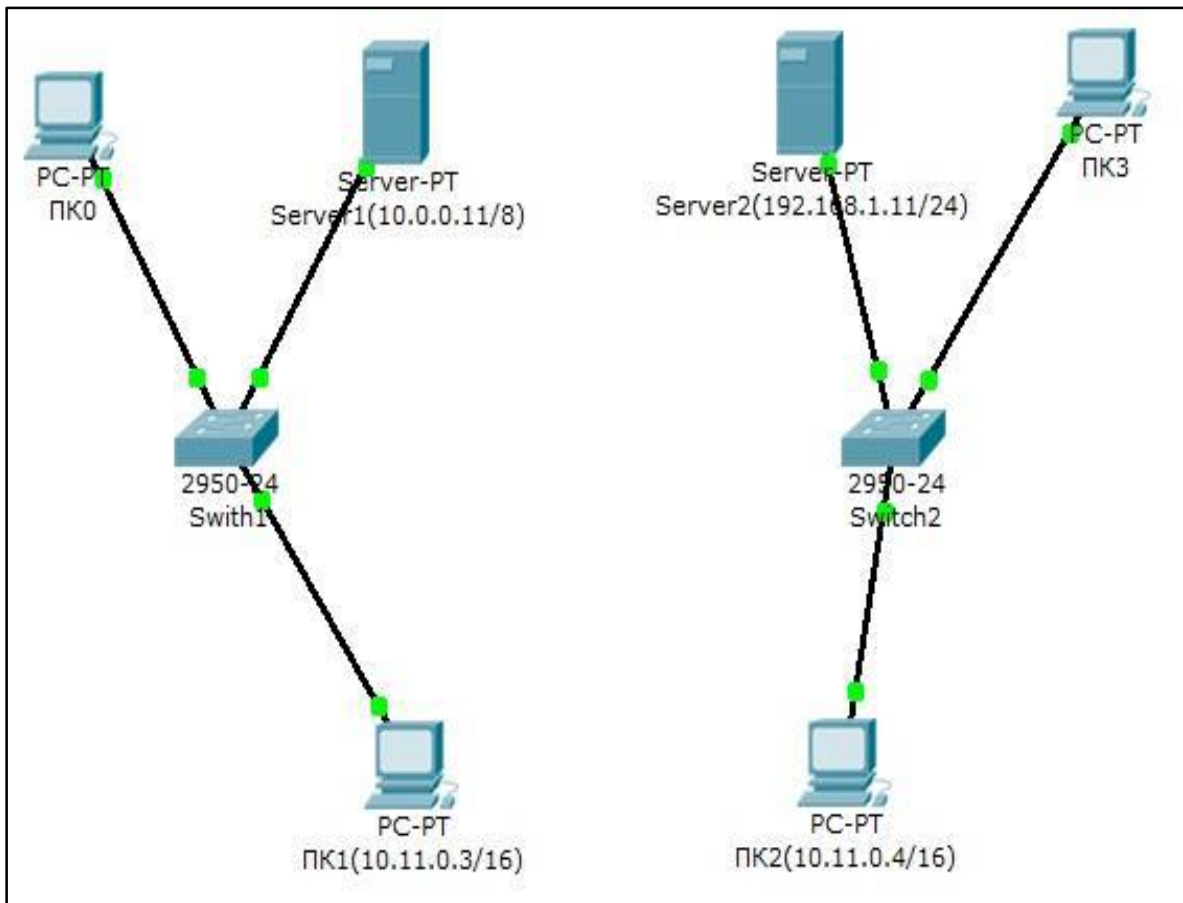


Рисунок 5.34 - Схема сетей отделов предприятия

Отдел 1 – Switch1, отдел 2 – Switch2.

В каждой сети имеется сервер со службами DHCP, DNS и HTTP (на серверах Server1 и Server2 расположены интернет-сайты отделов).

Компьютеры ПК0 и ПК3 с DHCP серверов своих сетей получают параметры IP адреса и шлюз.

Компьютеры ПК1 и ПК2 находятся в отдельной сети в одном VLAN.

Практическая работа 5. Моделирование виртуальных сетей

=====

Задание:

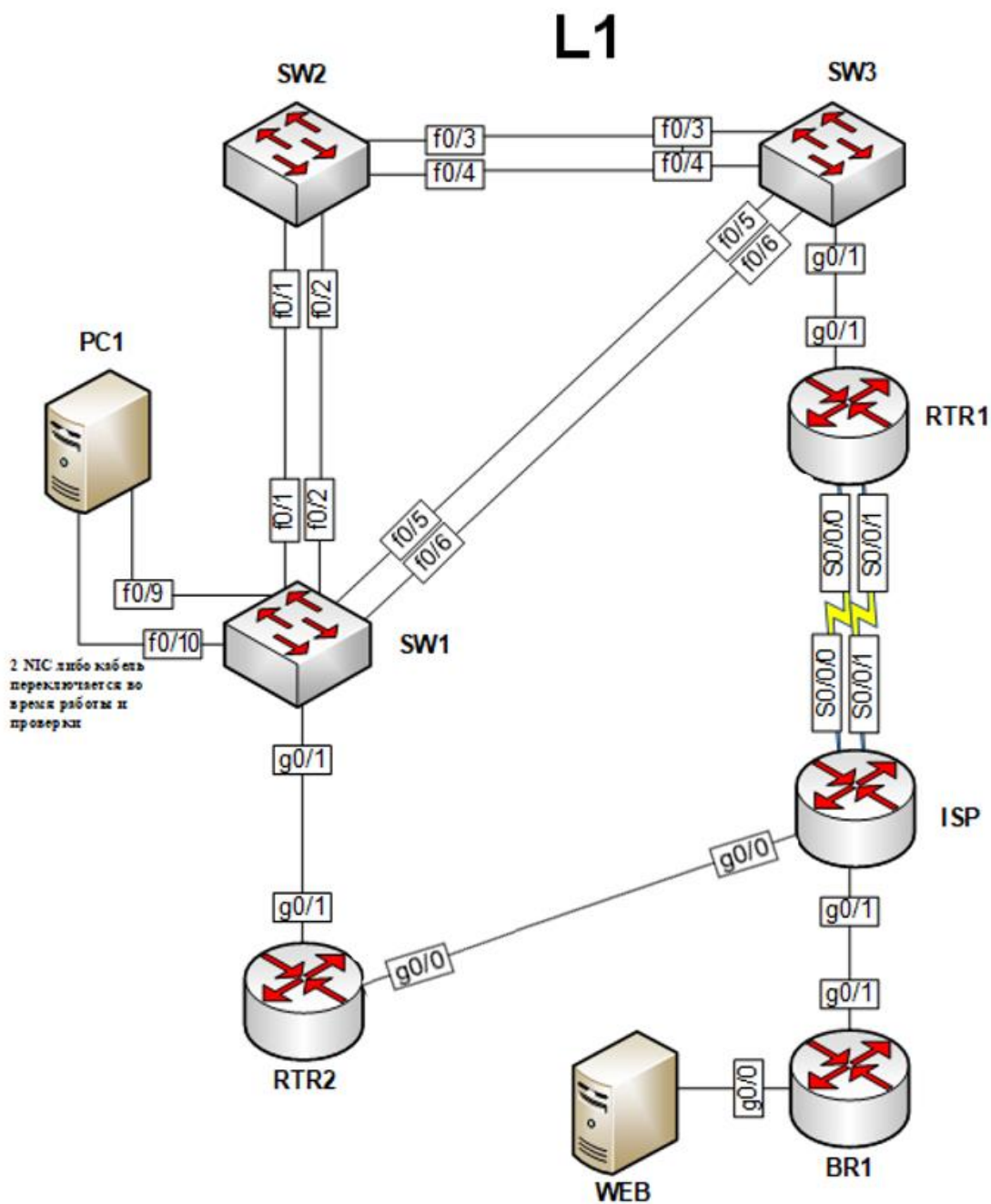
Дополните схему сети маршрутизатором или коммутатором третьего уровня, чтобы обеспечить работу корпоративной сети в следующих режимах:

1 - компьютеры ПК0 и ПК3 должны открывать сайты каждого отдела;

2 – компьютеры ПК1 и ПК2 должны быть доступны только друг для друга.

ПРАКТИЧЕСКОЕ ЗАДАНИЕ № 1

Дана топология сети (см. рисунок).



Заданная топология сети

Практические задания по курсу

Выполнить следующие задачи в Cisco Packet Tracer:

1. Задать имена всех устройств пользователя в соответствии с заданной топологией сети.

2. Назначить для всех устройств пользователя доменное имя **wsrvuz19.ru**.

3. Создать на всех устройствах пользователя **wsrvuz19** с паролем **cisco** следующим образом:

- пароль пользователя должен храниться в конфигурации в виде результата хэш-функции.

- пользователь должен обладать максимальным уровнем привилегий.

4. Для всех устройств реализовать модель AAA следующим образом:

- аутентификация на удаленной консоли должна производиться с использованием локальной базы данных (кроме устройства RTR1 и RTR2);

- после успешной аутентификации при входе с удаленной консоли пользователь должен попадать в режим с максимальным уровнем привилегий;

- должна быть настроена аутентификация на локальной консоли;

- после успешной аутентификации на локальной консоли пользователь должен попадать в режим с минимальным уровнем привилегий;

- на BR1 при успешной аутентификации на локальной консоли пользователь должен попадать в режим с максимальным уровнем привилегий.

5. На всех устройствах установить пароль **wsr** на вход в привилегированный режим:

- пароль должен храниться в конфигурации не в виде результата хэш-функции;

- необходимо настроить режим, при котором все пароли в конфигурации хранятся в зашифрованном виде.

**Методические рекомендации по выполнению
практического задания**

**Упражнение 1. Задание имен всех устройств пользователя
в соответствии с заданной топологией сети**

Режим глобальной конфигурации

Основной режим конфигурации называется глобальным режимом конфигурации. В режиме глобальной конфигурации выполняются изменения конфигурации интерфейса командной строки (CLI), влияющие на работу устройства в целом. Перед доступом к специализированным режимам конфигурации нужно войти в режим глобальной конфигурации.

Чтобы перевести устройство из привилегированного режима в режим глобальной конфигурации и выполнить ввод команд конфигурации из терминала, используется следующая команда интерфейса командной строки:

Switch# configure terminal.

После ввода команды командная строка изменяется таким образом, чтобы показать, что он находится в режиме глобальной конфигурации:

Switch(config) #

При использовании интерфейса командной строки (CLI) режим определяется по командной строке, которая является уникальной для каждого режима. По умолчанию каждая командная строка начинается с имени устройства. После имени следует остаток командной строки, который определяет режим. Например, запрос по умолчанию для режима глобальной конфигурации на коммутаторе выглядит так:

Switch(config) #

Практические задания по курсу

По мере выполнения команд и изменения режимов изменяется и командная строка, которая отражает текущие контекстные данные.

1. Чтобы задать имя устройства (**hostname**) введите из режима глобальной конфигурации команду **hostname SW1**, где вместо **SW1** необходимо написать название оборудования, данное в заданиях.

2. Проверьте настройку: вместо предустановленного **Switch** стало **SW1**:

```
Switch (config) # hostname SW1
SW1 (config) #
```

3. После проведения любых настроек одной из главных становится задача сохранения конфигурации из энергозависимой памяти устройства в энергонезависимую во избежание потерь внесенных изменений.

Сделаем это следующим образом:

- из режима глобальной конфигурации командой **do write**:

```
SW1 (config) # do write
Building configuration...
Compressed configuration from 2142 bytes to
1161 bytes [OK];
```

- из привилегированного режима командой **write**:

```
SW1# write
Building configuration...
Compressed configuration from 2142 bytes to
1161 bytes [OK]
```


Практические задания по курсу

Упражнение 2. Назначение для всех устройств пользователя доменного имени **wsrvuz19.ru**

1. Задайте доменное имя **wsrvuz19.ru** по умолчанию можно из режима глобальной конфигурации командой **ip domain-name wsrvuz19.ru**.

2. Проверку выполните с использованием команды **do show hosts summary** из режима глобальной конфигурации:

```
SW1(config)# ip domain-name wsrvuz19.ru
SW1(config)# do show hosts summary
Name lookup view: Global
Default domain is wsrvuz19.ru
...
```

3. Назначьте для всех устройств пользователя доменное имя **wsrvuz19.ru**.

Упражнение 3. Создание на всех устройствах пользователя **wsrvuz19** с паролем **cisco**

1. Необходимо создать такого пользователя, чтобы он обладал максимальным уровнем привилегий, а пароль хранился в виде хэш-функции. Все эти условия учитываются командой

```
username wsrvuz19 privilege 15 secret cisco,
```

здесь:

```
username wsrvuz19 - имя пользователя;
privilege 15 — уровень привилегий (0 — минимальный
уровень, 15 — максимальный уровень);
secret cisco — хранение пароля в виде MD5 хэш-функции.
```

Выполните данную команду.

2. Команда **show running-config** позволяет проверить настройки текущей конфигурации, где можно найти строку с добав-

Практические задания по курсу

=====

ленным пользователем и убедиться в том, что пароль хранится в зашифрованном виде:

```
SW1(config)# username wsrvuz19 privilege 15
secret cisco
SW1(config)# do show running-config
...
username wsrvuz19 privilege 15 secret 5
$1$EFRK$RNvRqTPt5wbB9sCj1Baf4.
...
```

Выполните данную команду.

Упражнение 4. Реализация для всех устройств модели AAA

Модель AAA (Authentication, Authorization and Accounting) — система аутентификации, авторизации и учета событий. Покажем, как настроить аутентификацию, авторизацию и учет AAA на маршрутизаторе Cisco с использованием протоколов Radius или TACACS+.

Включение AAA

Чтобы включить AAA, выполните в глобальной конфигурации команду **aaa new-model**. Пока эта команда не активирована, все другие команды AAA скрыты.

Команда **aaa new-model** сразу применяет локальную аутентификацию ко всем линиям и интерфейсам (кроме консольной линии **line con 0**). Если сеанс Telnet установлен с маршрутизатором после активации этой команды (или если время ожидания соединения истекло и требуется повторное соединение), пользователь должен пройти аутентификацию с использованием локальной базы данных маршрутизатора. Чтобы избежать блокировки маршрутизатором, перед началом настройки AAA рекомендуется определить на сервере доступа имя пользователя и пароль.

Сделайте это следующим образом:

```
Router(config)# username xxx password yyy
```

Практические задания по курсу

Сохраните конфигурацию до настройки команд AAA. Только после того, как вы полностью завершите настройку AAA (и удостоверитесь в правильности работы), можно сохранить конфигурацию снова. Это позволяет проводить восстановление после непредвиденных блокировок (до сохранения конфигурации) путем перезагрузки маршрутизатора.

Выбор внешнего сервера AAA

В глобальной конфигурации определите протокол безопасности, используемый с функциями AAA (Radius, TACACS+). Если эти два протокола не подходят, можно использовать локальную базу данных на маршрутизаторе.

Если вы используете протокол TACACS+, введите команду:

```
tacacs-server host <IP-адрес_сервера_AAA>  
<ключ>.
```

Если вы используете протокол Radius, введите команду

```
radius-server host <IP-адрес_сервера_AAA>  
<ключ>.
```

Настройка сервера AAA

На сервере AAA настройте следующие параметры:

- имя сервера доступа;
- IP-адрес, который сервер доступа использует для связи с сервером AAA. Если оба устройства расположены в одной и той же сети Ethernet, то по умолчанию при отправке пакета AAA сервер доступа использует IP-адрес, определенный в интерфейсе Ethernet. Эта проблема становится важной, когда маршрутизатор имеет несколько (и соответственно несколько адресов);
- тот же ключ **<ключ>**, что и заданный на сервере доступа. Ключ интерпретируется с учетом регистра символов;
- протокол, используемый сервером доступа (TACACS+ или RADIUS).

Практические задания по курсу

Точная процедура, используемая для настройки указанных выше параметров, описана в документации сервера AAA. Если сервер AAA настроен неверно, запросы AAA от сетевого устройства хранения данных будут игнорироваться сервером AAA и подключение может быть прервано.

Сервер AAA должен быть доступен по IP-протоколу с сервера доступа.

Настройка аутентификации

Аутентификация служит для проверки личности пользователей, прежде чем им будет предоставлен доступ к сети и к сетевым сервисам.

Настройка аутентификации AAA:

1. Определить именованный список способов аутентификации (в режиме глобальной конфигурации).
2. Применить данный список к одному или нескольким интерфейсам (в режиме конфигурации интерфейса).

Единственным исключением является список методов по умолчанию (который называется «**default**»). Список методов по умолчанию автоматически применяется ко всем интерфейсам, кроме тех, у которых есть явно определенный именованный список методов. Определенный список методов переопределяет список методов по умолчанию.

Ниже приведены примеры аутентификации по протоколу Radius, при входе в систему и по протоколу PPP (наиболее часто используемый способ), чтобы объяснить методы и именованные списки. Во всех примерах протокол TACACS+ может быть заменен Radius или локальной аутентификацией.

Программное обеспечение Cisco IOS использует для аутентификации пользователей первый метод. Если этот метод не отвечает (о чем сообщает слово ERROR), программное обеспечение Cisco IOS выбирает следующий метод аутентификации из списка методов. Этот процесс продолжается до тех пор, пока посредством указанного в списке метода не будет установлено соединение или пока не будет осуществлена попытка подключения всеми указанными способами.

Практические задания по курсу

Важно отметить, что программное обеспечение Cisco IOS пытается выполнить аутентификацию с помощью следующего метода из списка, только если предыдущий метод не дал результатов. Если произошел сбой аутентификации на любом этапе цикла, то есть, сервер AAA или локальная база данных имен пользователей отказывается предоставить доступ пользователю (на что указывает слово FAIL), процесс аутентификации останавливается и другие методы не применяются.

Для выполнения аутентификации пользователей необходимо настроить имя пользователя и пароль в сервере AAA.

Аутентификация при входе в систему

При помощи команды **aaa authentication login** можно выполнить аутентификацию пользователей, которым требуется доступ к серверу доступа с правами выполнения (TTY, VTY, консоль и AUX).

Доступ с правами выполнения с использованием протокола Radius, затем локального метода

```
Router(config)# aaa authentication login default group radius local
```

здесь:

- именованный список — это список по умолчанию (**default**).
- существуют два метода аутентификации (групповой RADIUS и локальный).

Все пользователи проходят аутентификацию на сервере Radius (первый метод). Если сервер Radius не отвечает, то используется локальная база данных маршрутизатора (второй метод).

Для локальной аутентификации определите имя пользователя и пароль:

```
Router(config)# username xxx password yyy
```

Практические задания по курсу

=====

Так как используется список по умолчанию в команде **aaa authentication login**, аутентификация при входе в систему будет автоматически выполнена для всех соединений при входе в систему (TTY, VTY, консоль и AUX).

Сервер (Radius или TACACS+) не отвечает на запрос **aaa authentication**, отправленный сервером доступа, если отсутствует IP-соединение, если сервер доступа неправильно определен на сервере AAA, либо если сервер AAA неправильно определен на сервере доступа.

Если использовать пример, приведенный выше, не включая ключевое слово «**local**», то получится следующее:

```
Router(config)# aaa authentication login default group radius
```

Если сервер AAA не отвечает на запрос проверки подлинности, аутентификация закончится неудачно (поскольку маршрутизатор не имеет альтернативного способа).

Доступ к консоли с использованием пароля линии

Расширим конфигурацию так чтобы при входе на консоль выполнялась только аутентификация по паролю, заданному для линии консоли 0.

Список CONSOLE определен и применяется к линии консоли 0. Вводим следующее:

```
Router(config)# aaa authentication login CONSOLE line
```

здесь:

- именованный список – это **CONSOLE**.
- существует только один способ аутентификации (линейный).

Практические задания по курсу

=====

После того, как создан именованный список (в данном случае **CONSOLE**), чтобы он вступил в силу, его необходимо применить к линии или интерфейсу.

Для этого используется команда **login authentication имя_списка**:

```
Router (config) # line con 0
Router (config-line) # exec-timeout 0 0
Router (config-line) # password cisco
Router (config-line) # login authentication CONSOLE
```

Список **CONSOLE** переопределяет список методов по умолчанию для линии консоли 0. Чтобы получить доступ к консоли, введите пароль «**cisco**» (настроен для линии консоли 0). Список по умолчанию по-прежнему используется для соединений TTY, VTY и AUX.

Для аутентификации доступа к консоли по локальному имени пользователя и паролю используйте следующую команду:

```
Router (config) # aaa authentication login CONSOLE local
```

В этом случае в локальной базе данных маршрутизатора должны быть настроены имя пользователя и пароль. Список необходимо также применить к линии или интерфейсу.

Чтобы аутентификация отсутствовала, используйте команду

```
Router(config)# aaa authentication login CONSOLE none
```

В данном случае аутентификация при доступе к консоли отсутствует. Список необходимо также применить к линии или интерфейсу.

Практические задания по курсу

=====

Переход в привилегированный режим (enable) с использованием внешнего сервера AAA

Чтобы перейти в режим **enable**, введите команды аутентификации (привилегии уровня 15).

Введите следующее:

```
Router(config)# aaa authentication enable default group radius enable
```

Будет запрашиваться только пароль, имя пользователя — **\$enab15\$**. Следовательно, имя пользователя **\$enab15\$** должно быть определено на сервере AAA.

Если сервер Radius не отвечает, нужно ввести разрешающий пароль, локально настроенный на маршрутизаторе.

Настройка авторизации

Авторизация — это процесс, который позволяет контролировать, что пользователь может и не может делать.

Правила авторизации AAA идентичны правилам аутентификации. Списки методов зависят от запрошенного типа авторизации. Здесь рассматриваются авторизация выполнения и авторизация сети.

Авторизация выполнения

Команда **aaa authorization exec** определяет, обладает ли пользователь правами на запуск оболочки EXEC. Это средство должно вернуть информацию о профиле пользователя, такую как данные автокоманд, время ожидания простоя, таймаут сеанса, список доступа, привилегии и другие факторы, индивидуальные для каждого пользователя.

Авторизация выполнения выполняется только по линиям VTU и TTY.

В следующем примере используется Radius.

Сначала используется команда аутентификации:

Практические задания по курсу

```
=====
Router(config)# aaa authentication login default group radius local.
```

Все пользователи, которые хотят войти на сервер доступа, должны авторизоваться, используя Radius (первый метод) или локальную базу данных (второй метод).

Введите следующее:

```
Router(config)# aaa authorization exec default group radius local
```

На сервере AAA необходимо выбрать **Service-Type=1 (login)**.

В этом примере, если не указано ключевое слово **local** и сервер AAA не отвечает, то авторизация никогда не будет возможной и произойдет сбой соединения.

В приведенных ниже примерах добавлять какие-либо команды на маршрутизаторе не требуется, а нужно только настроить профиль на сервере доступа.

Назначение уровней привилегий выполнения с сервера AAA

Если пользователю, выполняющему вход на сервер доступа, разрешено непосредственно входить в привилегированный режим **enable**, настройте следующую AV-пару Cisco на сервере AAA:

```
shell:priv-lvl=15
```

Это означает, что пользователь перейдет непосредственно в режим **enable**. Если для первого метода ответ не получен, то используется локальная база данных. Однако пользователь не войдет непосредственно в режим **enable**, ему придется ввести команду **enable** и указать разрешающий пароль (**enable**).

Практические задания по курсу

Назначение времени ожидания простоя от сервера AAA

Для настройки времени ожидания простоя (так, чтобы в случае отсутствия трафика по истечении этого времени сеанс прекращался) используйте атрибут **RADIUS IETF 28: Idle-Timeout** для профиля пользователя.

Авторизация сети

Применение пользовательских атрибутов. Можно использовать сервер AAA для назначения атрибутов каждого пользователя, таких как IP-адрес, номер обратного вызова, значение времени ожидания простоя номераабирателя или список доступа. В этом случае сетевое устройство хранения данных будет загружать соответствующие атрибуты из профиля пользователя с сервера AAA.

Настройка учета

Функция учета AAA позволяет отслеживать сервисы, к которым пользователи получают доступ, а также потребляемый объем сетевых ресурсов.

Правила учета AAA идентичны правилам аутентификации и авторизации: сначала следует определить именованный список методов учета, далее применить данный список к одному или нескольким интерфейсам (за исключением стандартного списка методов), используется первый метод в списке, в случае сбоя используется второй метод и т. д.

Учет ресурсов сети служит для предоставления данных всем сеансам PPP (Point-to-Point Protocol), SLIP (Serial Line Internet Protocol) и ARAP (AppleTalk Remote Access Protocol): количество пакетов, количество октетов, время сеанса, время начала и окончания.

Учет выполнения предоставляет данные о пользовательских сеансах терминала выполнения (например, о сеансе Telnet) для сервера доступа к сети: время сеанса, время начала и окончания.

Нижеприведенные примеры показывают, как можно отправлять данные на сервер AAA.

Практические задания по курсу

Создание записей учета начала и окончания сеанса

Для каждого удаленного сеанса PPP учетные данные передаются на сервер AAA после аутентификации клиента и после отключения с использованием ключевого слова **start-stop**:

```
Router(config)# aaa accounting network default  
start-stop group radius local
```

Создание только записей учета окончания сеанса

Если учетные данные нужно послать только после отключения клиента, используйте ключевое слово **stop** и введите следующую строку:

```
Router(config)# aaa accounting network default  
stop group radius local
```

Создание записей учета ресурсов для ошибок согласования и аутентификации

До этого момента учет AAA поддерживал записи начала и окончания сеанса для вызовов, прошедших пользовательскую аутентификацию. В случае ошибок аутентификации или согласования PPP запись аутентификации отсутствует. В качестве решения можно использовать учет окончания сеанса для ошибок ресурса AAA:

```
Router(config)# aaa accounting send stop-  
record authentication failure
```

На сервер AAA посылается запись об окончании сеанса.

Включение полного учета ресурсов

Для включения функции полного учета ресурсов, которая формирует запись начала сеанса при установлении вызова и запись окон-

Практические задания по курсу

=====
чания сеанса при завершении вызова, настройте следующие параметры:

```
Router(config)# aaa accounting resource start-stop
```

С помощью этой команды запись учета начала и окончания сеанса при установлении и завершении вызова позволяет отслеживать подключение ресурсов к устройству. Отдельная запись учета начала и окончания сеанса при аутентификации пользователя отслеживает процесс управления пользователями. Эти два набора записей учета связаны посредством уникального идентификатора сеанса для вызова.

Вернемся к нашему заданию для анализируемой схемы сети.

1. Первым делом необходимо включить модель AAA и указать, что аутентификация будет производиться с использованием локальной базы данных:

```
SW1(config)# aaa new-model  
SW1(config)# aaa authentication login default local.
```

2. Аутентификация на удаленной консоли производится с использованием локальной базы данных (кроме устройства RTR1 и RTR2). В заданиях определяются два вида консолей: локальная и удаленная. Удаленная консоль позволяет реализовывать удаленные подключения, например, по протоколам SSH или Telnet.

Чтобы выполнить это задание необходимо ввести следующие команды:

```
SW1(config)# line vty 0 4  
SW1(config-line)# login authentication default  
SW1(config-line)# exit  
SW1(config)#
```

Командой `line vty 0 4` производится переход к настройке линий виртуальных терминалов с 0 по 4.

Практические задания по курсу

=====

Команда **login authentication default** включает режим аутентификации по умолчанию на виртуальной консоли, а режим по умолчанию был задан в прошлом задании командой **aaa authentication login default local**.

Выход из режима настройки удаленной консоли выполняется с помощью команды **exit**.

3. Выполните проверку. Надежной проверкой будет тестовое подключение по протоколу Telnet с одного устройства на другое. Стоит учитывать, что для этого должна быть настроена базовая конфигурация и IP-адресация на выбранном оборудовании:

```
SW3#telnet 2001:100::10
User Access Verification
Username: wsrvuz19
Password:
SW1>.
```

4. После успешной аутентификации при входе с удаленной консоли пользователь сразу должен попадать в режим с максимальным уровнем привилегий.

Для решения этой задачи необходимо снова перейти к настройке линий виртуальных терминалов и задать уровень привилегий командой **privilege level 15**, где 15 - максимальный уровень (0 — минимальный уровень привилегий):

```
SW1(config)# line vty 0 4
SW1(config-line)# privilege level 15
SW1(config-line)# exit
SW1(config)#.
```

5. Выполните проверку. Проверкой будет служить решение из прошлого подпункта - удаленное подключение по Telnet:

```
SW3#telnet 2001:100::10
User Access Verification
Username: wsrvuz19
Password:
SW1#.
```

Практические задания по курсу

=====

После аутентификации пользователь сразу попадает в привилегированный режим, минуя непривилегированный, значит, задание выполнено корректно.

6. Настроим состояние сети, где при успешной аутентификации пользователь должен попадать в режим с минимальным уровнем привилегий.

Структура команд в этих заданиях совпадает с ранее решенными заданиями. Команда **line vty 0 4** заменяется на **console 0**:

```
SW1 (config)# line console 0
SW1 (config-line)# login authentication default
SW1 (config-line)# privilege level 0
SW1 (config-line)# exit
SW1 (config)#
```

Как уже было сказано, минимальный уровень привилегий определяется числом 0.

7. Выполните проверку. Проверку можно произвести следующим образом:

```
SW1# exit
User Access Verification
Username: wsrvuz19
Password:
SW1>
```

После аутентификации пользователь попадает в непривилегированный режим, как и требуется в заданиях.

8. На BR1 при успешной аутентификации на локальной консоли пользователь должен попадать в режим с максимальным уровнем привилегий. Настройка локальной консоли на BR1 будет иметь следующий вид:

```
BR1 (config)# line console 0
BR1 (config-line)# login authentication default
BR1 (config-line)# privilege level 15
BR1 (config-line)# exit
BR1 (config)#
```

Практические задания по курсу

9. Проверка осуществляется тем же способом, что и в предыдущем пункте:

```
BR1# exit
User Access Verification
Username: wsrvuz19
Password:
BR1#
```

После аутентификации происходит переход в привилегированный режим.

Упражнение 5. Установка на всех устройствах пароля **wsr** на вход в привилегированный режим

В задании сказано, что пароль на привилегированный режим должен храниться стандартно в открытом виде, но при этом режим шифрования всех паролей не будет позволять посмотреть пароль в открытом виде.

1. Для установки пароля на вход в привилегированный режим нужно использовать команду **enable password wsr**. Используя ключевое слово **password**, определяется вид, в котором будет храниться пароль. Если при создании пользователя пароль должен быть зашифрован, то ключевым словом было слово **secret**, а для хранения в открытом виде используется **password**.

Проверить настройки можно из просмотра текущей конфигурации:

```
SW1(config)# enable password wsr
SW1(config)# do show running-config
...
enable password wsr
!
username wsrvuz19 privilege 15 secret 5
$1$5I66$TB48YmLoCk9be4jSAH8500
...
```

Практические задания по курсу

=====
Видно, что пароль пользователя хранится в зашифрованном виде, а пароль на вход в привилегированный режим хранится в открытом виде, как и сказано в заданиях.

2. Для того, чтобы все пароли хранились в зашифрованном виде, следует использовать команду **service password-encryption**. Просмотр текущей конфигурации будет выглядеть теперь следующим образом:

```
SW1(config)# do show running-config
...
enable password 7 03134819
!
username wsrvuz19 privilege 15 secret 5
$1$5I66$TB48YmLoCk9be4jSAH8500
```

...
Пароль больше не доступен для просмотра в открытом виде.

ПРАКТИЧЕСКОЕ ЗАДАНИЕ № 2

Дана топология сети (рисунок 1 и рисунок 2).

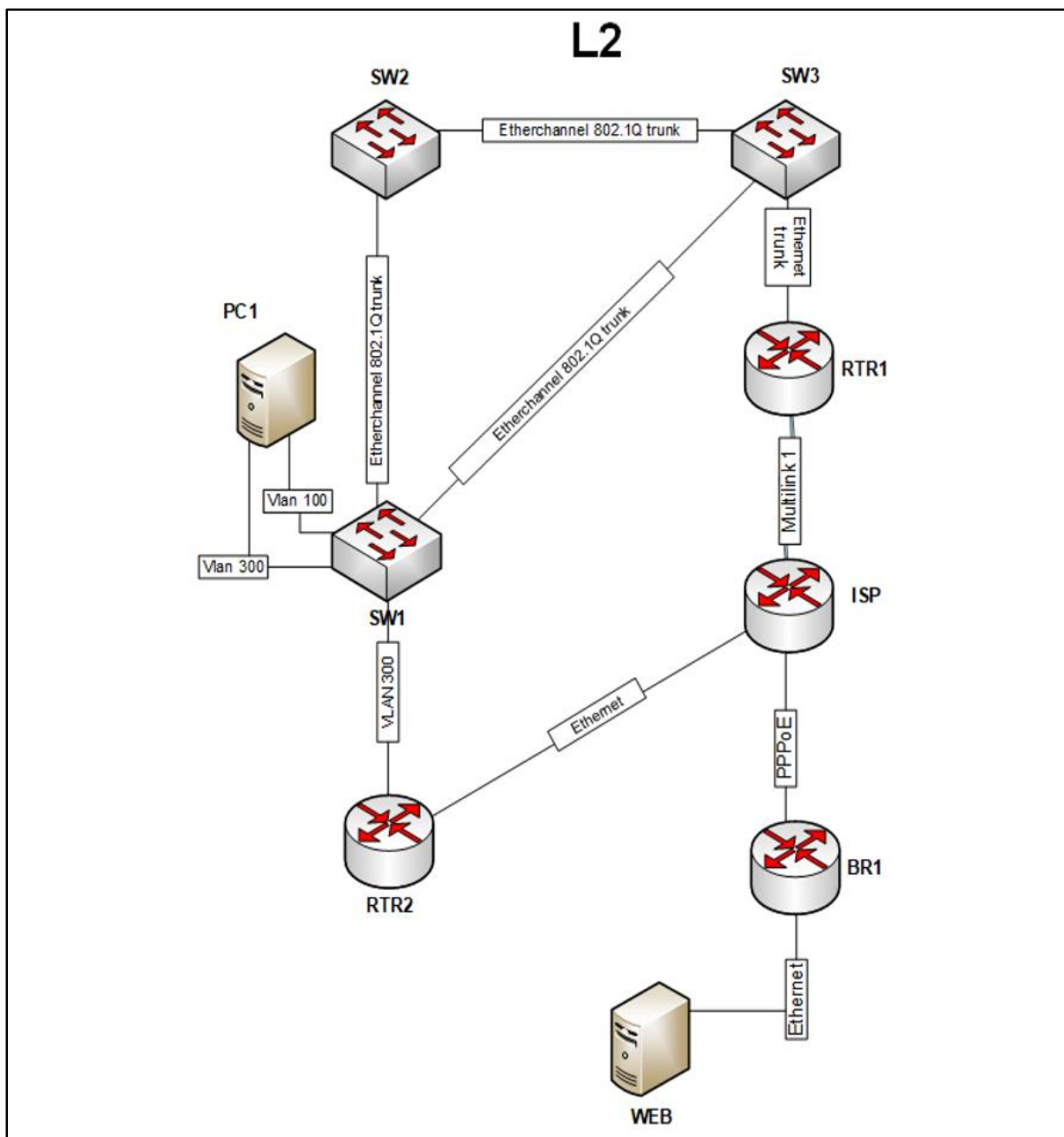


Рисунок 1 - Заданная топология сети

L3

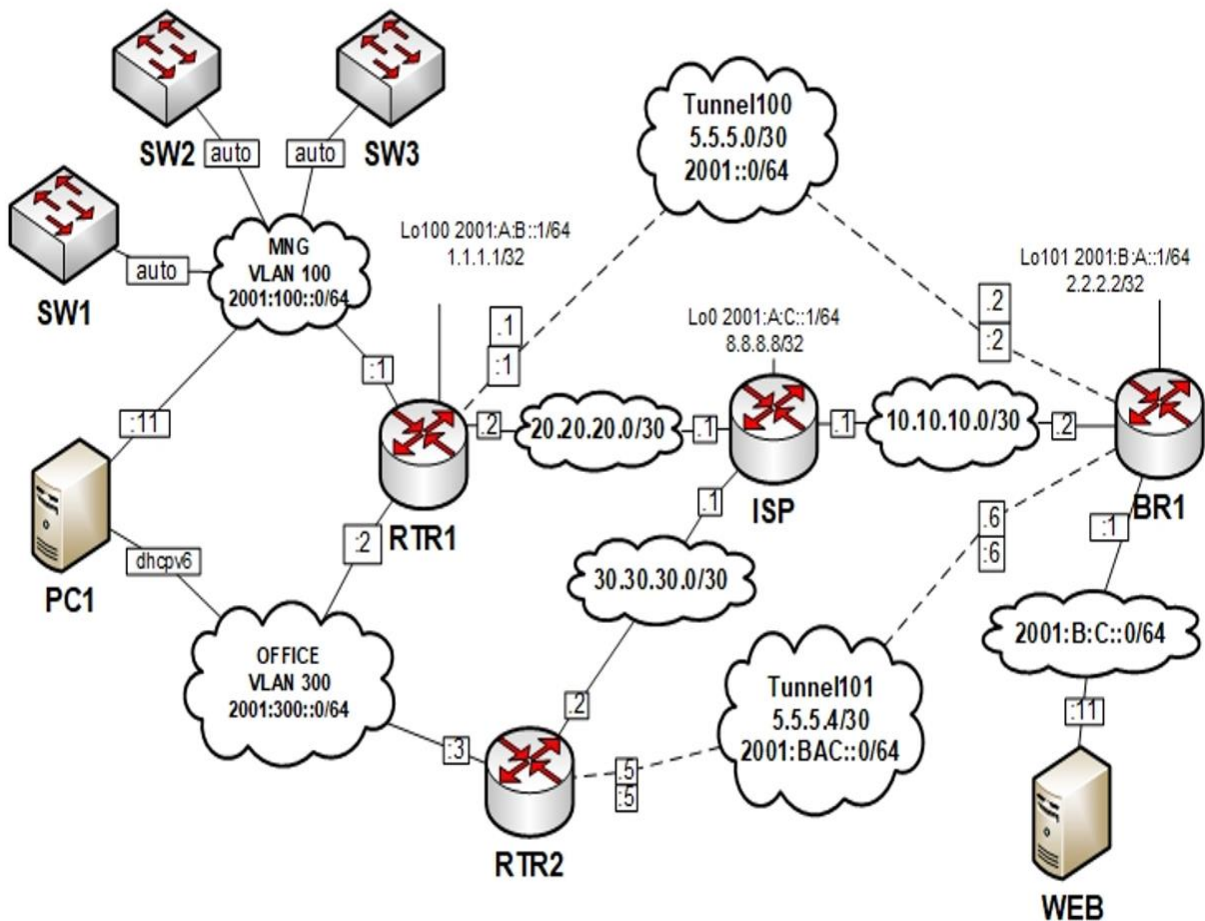


Рисунок 2 - Заданная топология сети

Выполнить следующие задачи:

1. На всех устройствах создать виртуальные интерфейсы, подынтерфейсы и интерфейсы типа петля. Назначьте IP-адреса в соответствии с топологией.

2. Включить механизм SLAAC для выдачи IPv6-адресов в сети MNG на интерфейсе маршрутизатора RTR1. На виртуальных интерфейсах в VLAN 100 (MNG) на коммутаторах SW1, SW2, SW3 включить режим автоконфигурации IPv6;

3. На всех устройствах (кроме PC1 и WEB) вручную назначить link-local адреса;

4. На всех коммутаторах отключить все неиспользуемые в задании порты и переведите в VLAN 99;

Практические задания по курсу

5. На коммутаторе SW1 включить блокировку на 1 минуту в случае двукратного неправильного ввода пароля в течение 30 секунд.

6. Все устройства должны быть доступны для управления по протоколу SSH версии 2.

Методические рекомендации по выполнению практического задания

Предварительная настройка

Перед выполнением заданий стоит настроить базовую коммутацию на коммутаторах SW1-SW3, так как будет удобнее проверять в дальнейшем их настройки. Зададим необходимые настройки.

Первым делом необходимо создать виртуальные сети VLAN с номерами 99, 100 и 300 на всех коммутаторах:

```
SW1 (config) #vlan 99
SW1 (config-vlan) #exit
SW1 (config) #vlan 100
SW1 (config-vlan) #exit
SW1 (config) #vlan 300
SW1 (config-vlan) #exit
```

Следующим шагом будет перевод интерфейса g0/1 на SW1 в VLAN с номером 300:

```
SW1 (config) #interface gigabitEthernet 0/1
SW1 (config-if) #switchport mode access
SW1 (config-if) #switchport access vlan 300
SW1 (config-if) #exit
```

Интерфейсы f0/1-2, f0/5-6, которые «смотрят» в сторону других коммутаторов, следует перевести в режим **trunk**:

```
SW1 (config) #interface range fastEthernet
0/1-2, fastEthernet 0/5-6
```

Практические задания по курсу

```
=====
SW1 (config-if-range) #switchport trunk encapsulation dot1q
SW1 (config-if-range) #switchport mode trunk
SW1 (config-if-range) #exit
```

На коммутаторе SW2 в режиме **trunk** будут интерфейсы f0/1-4:

```
SW2 (config) #interface range fastEthernet 0/1-4
SW2 (config-if-range) #switchport trunk encapsulation dot1q
SW2 (config-if-range) #switchport mode trunk
SW2 (config-if-range) #exit
```

На коммутаторе SW3 в режиме **trunk** будут интерфейсы f0/3-6, g0/1:

```
SW3 (config) #interface range fastEthernet 0/3-6, gigabitEthernet 0/1
SW3 (config-if-range) #switchport trunk encapsulation dot1q
SW3 (config-if-range) #switchport mode trunk
SW3 (config-if-range) #exit
```

На данном этапе настройки коммутаторов будут позволять обмениваться тегированными пакетами, что потребуется для выполнения заданий.

Упражнение 1. Создание на всех устройствах виртуальных интерфейсов, подынтерфейсов и интерфейсов типа петля. Назначение IP-адресов в соответствии с топологией

1. Первым будет настраиваться маршрутизатор BR1. Согласно топологии L3 здесь необходимо настроить интерфейс типа петля, он же **loopback**, под номером 101:

Практические задания по курсу

```
=====
// Создание loopback
BR1 (config) #interface loopback 101
// Назначение ipv4-адреса
BR1 (config-if) #ip address 2.2.2.2
255.255.255.255
// Включение ipv6 на интерфейсе
BR1 (config-if) #ipv6 enable
// Назначение ipv6-адреса
BR1 (config-if) #ipv6 address 2001: B: A: 1/64
// Выход из режима конфигурирования интерфейса
BR1 (config-if) #exit
BR1 (config) #
```

2. Выполните проверку. Чтобы проверить состояние созданного интерфейса можно использовать команду **show ipv6 interface brief**:

```
BR1#show ipv6 interface brief
...
Loopback101                [up/up]
    FE80::2D0:97FF:FE94:5022 //link-local
адрес
    2001: B: A::1           //IPv6-адрес
...
BR1#
```

Здесь видно, что **loopback** активен, его состояние **UP**. Если посмотреть ниже, то можно увидеть два **IPv6-адреса**, хотя была использована только одна команда для установки **IPv6-адреса**. Дело в том, что **FE80::2D0:97FF:FE94:5022** — это **link-local** адрес, который присваивается при включении **ipv6** на интерфейсе командой **ipv6 enable**.

3. Для просмотра **IPv4**-адреса используем похожую команду:

```
BR1#show ip interface brief
...
Loopback101    2.2.2.2    YES manual up    up
```

Практические задания по курсу

```
...  
BR1#
```

4. Для BR1 сразу же стоит настроить интерфейс **g0/0**, здесь необходимо просто задать **IPv6**-адрес:

```
// Переход в режим конфигурирования интерфейса  
BR1 (config) #interface gigabitEthernet 0/0  
// Включение интерфейса  
BR1 (config-if) #no shutdown  
BR1 (config-if) #ipv6 enable  
BR1 (config-if) #ipv6 address 2001: B: C: 1/64  
BR1 (config-if) #exit  
BR1 (config) #
```

5. Проверьте настройки той же командой **show ipv6 interface brief**:

```
BR1#show ipv6 interface brief  
GigabitEthernet0/0          [up/up]  
    FE80::290:CFF:FE9D:4624 //link-local адрес  
    2001:B:C::1              //IPv6-адрес  
  
...  
Loopback101                 [up/up]  
    FE80::2D0:97FF:FE94:5022 //link-local  
адрес  
    2001:B:A::1              //IPv6-адрес
```

6. Настройте маршрутизатор ISP. Здесь по заданию будет настроен **loopback** с номером 0, но кроме этого предпочтительнее настроить интерфейс **g0/0**, на котором должен быть адрес 30.30.30.1, по той причине, что в последующих заданиях ничего не будет сказано о настройке этих интерфейсов. Сначала настраивается **loopback** с номером 0:

Практические задания по курсу

```
=====
ISP (config) #interface loopback 0
ISP (config-if) #ip address 8.8.8.8
255.255.255.255
ISP (config-if) #ipv6 enable
ISP (config-if) #ipv6 address 2001: A: C: 1/64
ISP (config-if) #exit
ISP (config) #
```

7. Командой **show ipv6 interface brief** можно убедиться в правильности настройки интерфейса. Затем настраивается интерфейс g0/0:

```
BR1 (config) #interface gigabitEthernet 0/0
BR1 (config-if) #no shutdown
BR1 (config-if) #ip address 30.30.30.1
255.255.255.252
BR1 (config-if) #exit
BR1 (config) #
```

8. Далее будет настроен маршрутизатор RTR1. Здесь так же нужно создать **loopback** под номером 100:

```
BR1 (config) #interface loopback 100
BR1 (config-if) #ip address 1.1.1.1
255.255.255.255
BR1 (config-if) #ipv6 enable
BR1 (config-if) #ipv6 address 2001: A: B: 1/64
BR1 (config-if) #exit
BR1 (config) #
```

9. На RTR1 необходимо создать 2 виртуальных подынтерфейса для VLAN 100 и VLAN 300. Сделать это можно следующим образом.

Для начала следует включить физический интерфейс g0/1 командой **no shutdown**:

```
RTR1 (config) #interface gigabitEthernet 0/1
RTR1 (config-if) #no shutdown
RTR1 (config-if) #exit
```

Практические задания по курсу

=====

Затем создаются и настраиваются подынтерфейсы с номерами 100 и 300:

```
// Создание подынтерфейса с номером 100 и пе-
реход к его настройке
RTR1 (config) #interface gigabitEthernet
0/1.100
// Установка инкапсуляции типа dot1q с номером
vlan 100
RTR1 (config-subif) #encapsulation dot1Q 100
RTR1 (config-subif) #ipv6 enable
RTR1 (config-subif) #ipv6 address 2001:100:
1/64
RTR1 (config-subif) #exit
// Создание подынтерфейса с номером 300 и пе-
реход к его настройке
RTR1 (config) #interface gigabitEthernet
0/1.300
// Установка инкапсуляции типа dot1q с номером
vlan 100
RTR1 (config-subif) #encapsulation dot1Q 300
RTR1 (config-subif) #ipv6 enable
RTR1 (config-subif) #ipv6 address 2001:300:
2/64
RTR1 (config-subif) #exit
```

Номер подынтерфейса может отличаться от номера VLAN, в котором он будет работать, но для удобства лучше использовать номер подынтерфейса, совпадающий с номером VLAN.

В случае установки типа инкапсуляции при настройке подынтерфейса, следует указывать номер, совпадающий с номером VLAN. Так после команды **encapsulation dot1Q 300** подынтерфейс будет пропускать только пакеты VLAN с номером 300.

10. Заключительным в этом задании будет маршрутизатор RTR2. Соединение между SW1 и RTR2 должно быть в режиме **access**, интерфейс коммутатора будет пропускать в сторону RTR2 только пакеты, предназначенные для VLAN 300, об этом сказано в задании на топологии L2. Следовательно на маршрутизаторе RTR2 бу-

Практические задания по курсу

=====
дет настраиваться только физический интерфейс без создания подын-
терфейсов:

```
RTR2 (config) #interface gigabitEthernet 0/1
RTR2 (config-if) #no shutdown
RTR2 (config-if) #ipv6 enable
RTR2 (config-if) #ipv6 address 2001:300::3/64
RTR2 (config-if) #exit
RTR2 (config) #
```

11. Затем настраивается интерфейс g0/0:

```
BR1 (config) #interface gigabitEthernet 0/0
BR1 (config-if) #no shutdown
BR1 (config-if) #ip address 30.30.30.2
255.255.255.252
BR1 (config-if) #exit
BR1 (config) #
```

На этом настройка интерфейсов маршрутизаторов по текущему заданию закончена. Настройка остальных интерфейсов будет осуществлена уже по мере выполнения следующих заданий.

Упражнение 2. Включение механизма SLAAC для выдачи IPv6-адресов в сети MNG на интерфейсе маршрутизатора RTR1

Механизм SLAAC позволяет маршрутизатору назначать устройствам адреса даже если в сети нет DHCPv6 (DHCPv6 — это сетевой протокол для конфигурации узлов версии 6 (IPv6) Протокола Интернет с IP-адресами, префиксами IP и другими данными конфигурации, которые необходимы для работы в сети IPv6. Это новая версия протокола DHCP для работы в сетях на основе IPv6).

Маршрутизатор Cisco с рабочим IPv6 интерфейсом рассылает в сеть информацию об этой сети, включающую в себя сетевую часть IP адреса и длину префикса.

Практические задания по курсу

1. Механизм SLAAC включен по умолчанию. Единственное, что нужно сделать — это включить IPv6 маршрутизацию. Сделать это можно следующей командой:

```
RTR1 (config-subif)#ipv6 unicast-routing
```

Без этой команды оборудование выполняет роль хоста. Другими словами, благодаря вышеупомянутой команде, появляется возможность использовать дополнительные функции **ipv6**, в том числе выдавать **ipv6**-адреса, настраивать маршрутизацию и прочее.

2. На виртуальных интерфейсах в VLAN 100 (MNG) на коммутаторах SW1, SW2, SW3 включим режим автоконфигурации **IPv6**.

Из топологии L3 видно, что коммутаторы подключены к сети VLAN 100. Это значит, что на коммутаторах необходимо создать виртуальные интерфейсы, а уже затем назначить там получение **ipv6**-адресов по умолчанию. Первоначальная настройка была сделана именно для того, чтобы коммутаторы смогли получить от RTR1 адреса по умолчанию. Выполнить это задание можно следующим перечнем команд, подходящих для всех трех коммутаторов:

3. Проверить можно все той же командой **show ipv6 interface brief**:

```
SW1#show ipv6 interface brief
...
Vlan100                [up/up]
    FE80::A8BB:CCFF:FE80:C000    // link-
local адрес
    2001:100::A8BB:CCFF:FE80:C000 // получен-
ный IPv6-адрес
```

Кроме **link-local** адреса появился **ipv6**-адрес, полученный от RTR1. Данное задание успешно выполнено, а на остальных коммутаторах необходимо написать те же самые команды.

Практические задания по курсу

Упражнение 3. Назначение вручную на всех устройствах (кроме PC1 и WEB) link-local адресов

Тридцатизначные **ipv6**-адреса не доставляют удовольствия администраторам, поэтому есть возможность изменить вручную **link-local**, сократив его длину до минимального значения. В заданиях ничего не сказано о том, какие именно выбирать адреса, поэтому здесь предоставляется свободный выбор.

1. Например, на коммутаторе SW1 зададим **link-local** адрес fe80::10. Сделать это можно следующей командой из режима конфигурирования выбранного интерфейса:

```
// Вход в виртуальный интерфейс vlan 100
SW1(config)#interface vlan 100
// Ручная установка link-local адреса
SW1(config-if)#ipv6 address fe80::10 link-
local
SW1(config-if)#exit
```

Теперь адресация выглядит намного привлекательнее:

```
SW1#show ipv6 interface brief
...
Vlan100                [up/up]
    FE80::10           //link-local адрес
    2001:100::10       //IPv6-адрес
```

Кроме **link-local** адреса поменялся и полученный **IPv6**-адрес, так как адрес выдается на основе **link-local** адреса.

2. На коммутаторе SW1 необходимо было задать **link-local** адрес только на одном интерфейсе.

3. С маршрутизатором RTR1 нужно произвести больше настроек — необходимо задать **link-local** на двух подынтерфейсах на **loopback**, а в последующих настройках ещё появится интерфейс **tunnel 100**.

4. Чтобы избежать лишнего написания команд, можно задать один и тот же **link-local** адрес на всех интерфейсах сразу. Сде-

Практические задания по курсу

=====

Лать это можно с помощью ключевого слова **range** с последующим перечислением всех интерфейсов:

```
// Переход к настройке нескольких интерфейсов
RTR1(config)#interface range gigabitEthernet
0/1.100, gigabitEthernet 0/1.300, loopback 100
// Ручная установка link-local адреса
RTR1(config-if)#ipv6 address fe80::1 link-
local
RTR1(config-if)#exit
```

5. При проверке интерфейсов можно будет увидеть, что на всех выбранных интерфейсах были изменены **link-local** адреса:

```
RTR1#show ipv6 interface brief
gigabitEthernet 0/1.100      [up/up]
    FE80::1
    2001:100::1
gigabitEthernet 0/1.300      [up/up]
    FE80::1
    2001:300::2
Loopback100                  [up/up]
    FE80::1
    2001:A:B::1
```

Все остальные устройства настраиваются аналогичным способом.

Упражнение 4. Отключение на всех коммутаторах всех неиспользуемых в задании портов

Основная идея заключается в том же способе выбора нескольких интерфейсов для конфигурирования с помощью команды **range**, а уже затем следует писать команды перевода в нужный VLAN и последующего выключения интерфейсов.

Практические задания по курсу

=====

1. Например, у коммутатора SW1, согласно топологии L1, будут выключены порты f0/3-4, f0/7-8, f0/11-24 и g0/2. Для этого примера настройка будет следующая:

```
// Выбор всех неиспользуемых портов
SW1 (config)#interface range fastEthernet 0/3-
4, fastEthernet 0/7-8, fastEthernet 0/11-24, giga-
bitEthernet 0/2
// Установка режима access на интерфейсах
SW1 (config-if-range) #switchport mode access
// Перевод в VLAN 99 интерфейсов
SW1 (config-if-range) #switchport access vlan
99
// Выключение интерфейсов
SW1 (config-if-range) #shutdown
SW1 (config-if-range) #exit
```

2. Проверяя настройки уже известной командой, стоит обратить внимание, что у всех неиспользуемых портов должен быть статус **administratively down**, оповещающий о том, что порт выключен:

```
SW1#show ip interface brief
Interface IP-Address OK? Method Status  Proto-
col
...
fastEthernet 0/3 unassigned YES unset adminis-
tratively down  down
```

3. Чтобы посмотреть, в какой VLAN находится порт можно использовать другую команду:

```
SW1#show ip vlan
...
99      VLAN0099  active  Fa0/3,  Fa0/4,  Fa0/7,
Fa0/8
Fa0/11, Fa0/12, Fa0/13, Fa0/14
Fa0/15, Fa0/16, Fa0/17, Fa0/18
```

Практические задания по курсу

```
Fa0/19, Fa0/20, Fa0/21, Fa0/22
Fa0/23, Fa0/24, Gig0/2
...
```

Здесь должны быть все неиспользуемые интерфейсы. Стоит отметить, что перевести интерфейсы в **vlan** не удастся, если такой VLAN не создан. Именно для этого в первоначальной настройке создавались все необходимые для работы VLAN.

Упражнение 5. На коммутаторе SW1 включение блокировки на 1 минуту в случае двукратного неправильного ввода пароля в течение 30 секунд

1. Сделать это можно следующей командой:

```
// Блокировка на 60с; Попытки: 2; В течение:
30с
SW1#login block-for 60 attempts 2 within 30
```

2. Проверить эти настройки следующим образом:

```
SW1#show login
...
If more than 2 login failures occur in 30
seconds or less,
logins will be disabled for 60 seconds.
...
```

Здесь доходчиво объяснено, что после двух неудачных попыток в течение 30 или менее секунд, возможность входа будет заблокирована на 60 секунд.

Упражнение 6. Установка доступности всех устройств для управления по протоколу SSH версии 2

SSH — это протокол прикладного уровня. SSH-сервер обычно прослушивает соединения на TCP-порту 22. Спецификация протокола SSH-2 содержится в RFC 4251. Для аутентификации сервера в SSH

Практические задания по курсу

=====

используется протокол аутентификации сторон на основе алгоритмов электронно-цифровой подписи RSA или DSA, но допускается также аутентификация при помощи пароля (режим обратной совместимости с Telnet) и даже IP-адреса хоста

Аутентификация по паролю наиболее распространена. При каждом подключении подобно https вырабатывается общий секретный ключ для шифрования трафика.

При аутентификации по ключевой паре предварительно генерируется пара открытого и закрытого ключей для определённого пользователя. На машине, с которой требуется произвести подключение, хранится закрытый ключ, а на удалённой машине — открытый. Эти файлы не передаются при аутентификации, система лишь проверяет, что владелец открытого ключа также владеет и закрытым. При данном подходе, как правило, настраивается автоматический вход от имени конкретного пользователя в ОС.

Аутентификация по IP-адресу небезопасна, эту возможность чаще всего отключают.

Для создания общего секрета (сеансового ключа) используется алгоритм Диффи — Хеллмана. Для шифрования передаваемых данных используется симметричное шифрование, алгоритмы AES, Blowfish или 3DES. Целостность передачи данных проверяется с помощью CRC32 в SSH1 или HMAC-SHA1/HMAC-MD5 в SSH2.

1. Чтобы устройства были доступны по SSH версии 2, необходимо предварительно настроить оборудование, поэтому в целях информативности сначала будет настраиваться оборудование с заводскими настройками.

Изменить версию прокола можно следующим образом:

```
// Установить версию SSH версии 2  
Router (config) #ip ssh version 2  
Please create RSA keys (of at least 768 bits  
size) to enable SSH v2.  
Router (config) #
```

Система просит создать RSA ключи для работоспособности SSH версии 2.

Практические задания по курсу

2. Следуя совету системы, создать ключи RSA можно следующей командой:

```
// Создание RSA ключей
Router (config) #crypto key generate rsa
% Please define a hostname other than Router.
Router (config) #
```

3. Система не позволяет выполнить команду по причине того, что не изменен **hostname**. После изменения **hostname** нужно написать команду генерации ключей ещё раз:

```
Router (config) #hostname R1
R1 (config) #crypto key generate rsa
% Please define a domain-name first.
R1 (config) #
```

4. Теперь система не позволяет создать ключи RSA, по причине отсутствия доменного имени. И уже после установки доменного имени появится возможность создать ключи RSA. Длина ключей RSA должна быть не менее 768 бит для работоспособности SSH версии 2:

```
R1 (config) #ip domain-name wsrvuz19.ru
R1 (config) #crypto key generate rsa
How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be
non-exportable... [OK]
```

В итоге получается, что для работоспособности SSHv2 необходимо:

- изменить **hostname**;
- изменить доменное имя;
- сгенерировать ключи RSA.

5. В прошлой работе была приведена настройка изменения **hostname** и доменного имени на всех устройствах, поэтому, продолжая настройку текущих устройств, необходимо только сгенерировать ключи RSA:

Практические задания по курсу

```
=====
RTR1 (config) #crypto key generate rsa
How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be
non-exportable... [OK]
```

6. SSH версии 2 активен, но устройства ещё не настроены полностью. Заключительным этапом будет настройка виртуальных консолей:

```
// Переход к настройке виртуальных консолей
R1 (config) #line vty 0 4
// Разрешение удаленного подключения только по
протоколу SSH:
RTR1 (config-line) #transport input ssh
RTR1 (config-line) #exit
```

7. Ранее была настроена модель AAA, где на виртуальных консолях была задана аутентификация с использованием локальной базы данных, и пользователь после аутентификации должен был попадать сразу в привилегированный режим. Самая простая проверка работоспособности SSH — попытка подключиться на свое же оборудование. На RTR1 есть **loopback** с IP-адресом 1.1.1.1, можно попробовать подключиться по этому адресу:

```
//Подключение по ssh
RTR1 (config) #do ssh -l wsrvuz19 1.1.1.1
Password:
RTR1#
```

После ключа **-l** вводится логин существующего пользователя, а затем пароль. После аутентификации происходит переход сразу в привилегированный режим, а это значит, что SSH настроен корректно.

ЗАДАНИЯ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ

Задание 1. Работа с интерфейсом оборудования Cisco

Состав сети:

- коммутаторы S1, S2, S3 (3 шт.);
- персональные компьютеры PC1, PC2, PC3, PC4 (4 шт.).

Схема сети представлена на рисунке 1.

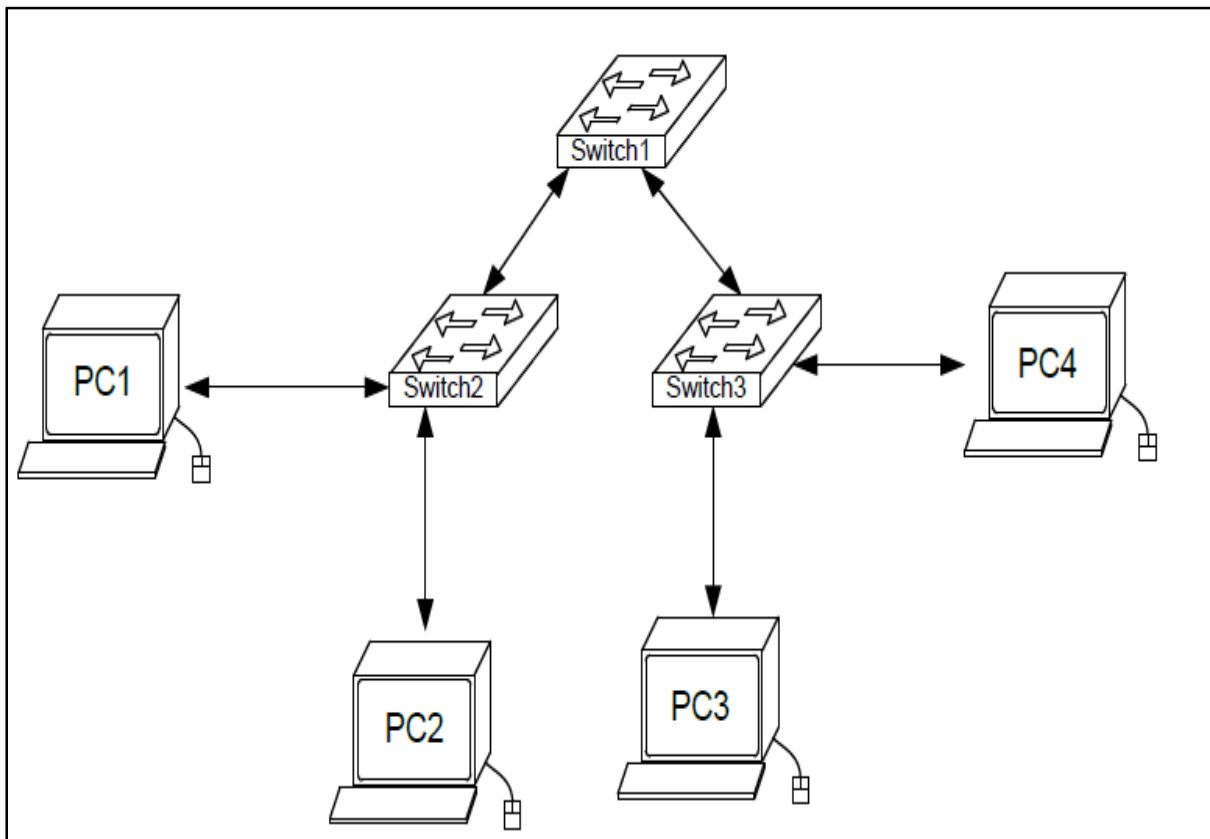


Рисунок 1 - Схема сети

Задание:

- изменить имя коммутаторам;
- обеспечить парольный доступ к привилегированному режиму на коммутаторах;
- задать IP-адреса и маски коммутаторам (172.16.1.11/24, 172.16.1.12/24, 172.16.1.13/24);

Задания для самостоятельной работы

- =====
- задать IP-адреса и маски сетей персональным компьютерам. (172.16.1.1/24, 172.16.1.2/24, 172.16.1.3/24, 172.16.1.4/24);
 - убедиться в достижимости всех объектов сети по протоколу IP;
 - переключившись в «Режим симуляции» рассмотреть и пояснить процесс обмена данными по протоколу ICMP между устройствами (выполнив команду **ping** с одного компьютера на другой), пояснить роль протокола ARP в этом процессе. Детальное пояснение включить в отчет.

Структура отчета по работе:

- титульный лист;
- задание;
- схема сети;
- ход работы. Данный раздел состоит из последовательного описания значимых выполняемых шагов (с указанием их сути) и скриншоты экранов (должна быть видна набранная команда и реакция системы, если она есть);
- выводы.

Задание 2. Настройка статической маршрутизации на оборудовании Cisco

(Синхронизация времени для последовательных сетевых интерфейсов. Задание статических маршрутов и маршрутов «по умолчанию». Просмотр созданной таблицы маршрутов)

Состав сети:

- коммутаторы S1, S2, S3 (3 шт.);
- маршрутизаторы R1, R2, R3 (3 шт.);
- персональные компьютеры C1, C2, C3 (3 шт.).

Схема сети представлена на рисунке 2.

Задания для самостоятельной работы

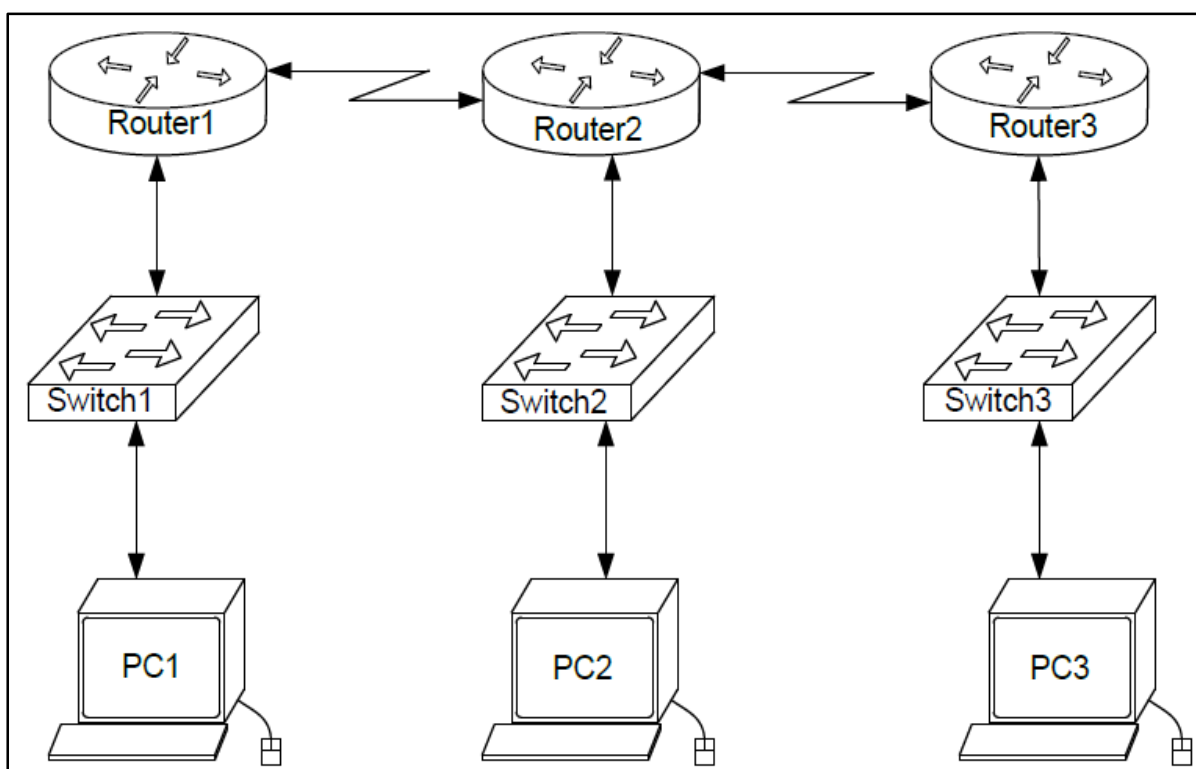


Рисунок 2 - Схема сети

Задание:

- задать IP адреса сетевым интерфейсам маршрутизаторов, интерфейсам управления коммутаторов и сетевым интерфейсам локальных компьютеров;
- установить связь на физическом и канальном уровнях между соседними маршрутизаторами по последовательному сетевому интерфейсу;
- добиться возможности пересылки данных по протоколу IP между соседними объектами сети (C1-S1, C1-R1, S1-R1, R1-R2, R2-S2, R2-C2, и т.д.);
- настроить на маршрутизаторе R2 статические маршруты к сетям локальных компьютеров C1, C3;
- настроить на маршрутизаторах R1, R3 маршруты «по умолчанию» к сетям локальных компьютеров C2-C3 и C1-C2 соответственно;
- добиться возможности пересылки данных по протоколу IP между любыми объектами сети;

Задания для самостоятельной работы

=====

- переключившись в «Режим симуляции» рассмотреть и пояснить процесс обмена данными по протоколу ICMP между устройствами (выполнив команду **ping** с одного компьютера на другой), пояснить роль протокола ARP в этом процессе. Детальное пояснение включить в отчет.

Структура отчета по работе:

- титульный лист;
- задание;
- топологическая схема сети. Указать на схеме наименования узлов сети, адреса и типы сетевых интерфейсов;
- ход работы: данный раздел состоит из последовательного описания значимых выполняемых шагов (с указанием их сути) и копий экранов (должна быть видна набранная команда и реакция системы, если она есть). Конфигурации оборудования: привести значимые фрагменты конфигурационных файлов (startup - config) для коммутаторов и маршрутизаторов, пояснить значение команд;
- выводы.

Задание 3. Настройка протоколов маршрутизации RIP на оборудовании Cisco

(Включение на маршрутизаторе поддержки протокола RIP. Настройка протокола RIP на поддержку маршрутизации требуемых сетей. Просмотр таблицы маршрутизации. Просмотр работающих протоколов маршрутизации).

Состав сети:

- коммутаторы S1, S2, S3 (3 шт.);
 - маршрутизаторы R1, R2, R3 (3 шт.);
 - персональные компьютеры C1, C2, C3 (3 шт.).
- Схема сети представлена на рисунке 3.

Задания для самостоятельной работы

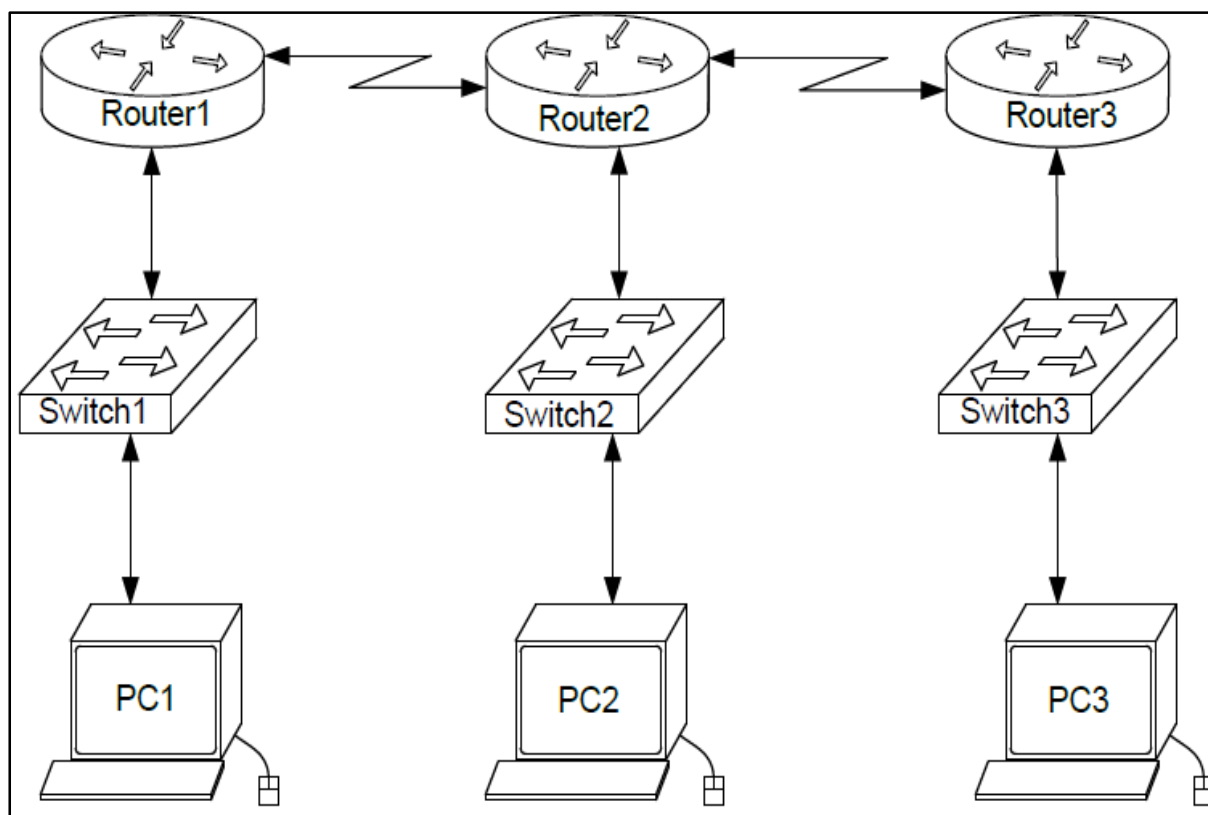


Рисунок 3 - Схема сети

Задание:

- задать IP адреса сетевым интерфейсам маршрутизаторов, интерфейсам управления коммутаторов и сетевым интерфейсам локальных компьютеров;
- установить связь на физическом и канальном уровнях между соседними маршрутизаторами по последовательному сетевому интерфейсу;
- добиться возможности пересылки данных по протоколу IP между соседними объектами сети (C1-S1, C1-R1, S1-R1, R1-R2, R2-S2, R2-C2, и т.д.);
- выявить невозможность пересылки данных по протоколу IP между удаленными объектами сети;
- просмотреть существующую таблицу маршрутизации;
- включить поддержку протокола RIP на всех маршрутизаторах сети;
- подключить к протоколу RIP требуемые сети;

Задания для самостоятельной работы

- просмотреть обновленную таблицу маршрутизации;
- посмотреть список протоколов маршрутизации работающих на узлах сети;
- удостовериться в возможности пересылки данных по протоколу IP между любыми объектами сети.

Структура отчета по работе:

Титульный лист;

Задание;

- топологическая схема сети: указать на схеме наименования узлов сети, адреса и типы сетевых интерфейсов;
- ход работы. Данный раздел состоит из последовательного описания значимых выполняемых шагов (с указанием их сути) и копий экранов (должна быть видна набранная команда и реакция системы, если она есть);
- конфигурации оборудования: привести значимые фрагменты конфигурационных файлов для коммутаторов и маршрутизаторов Cisco, пояснить значение команд;
- выводы.

Задание 4. Применение списков доступа на оборудовании Cisco

(Сопоставление интерфейсу маршрутизатора некоторой группы доступа. Создание списков доступа позволяющих или препятствующих передачи данных между узлами сети).

Состав сети:

- коммутаторы S1, S2, S3 (3 шт.);
- маршрутизаторы R1, R2, R3 (3 шт.);
- персональные компьютеры C1, C2, C3 (3 шт.).

Схема сети представлена на рисунке 4.

Задания для самостоятельной работы

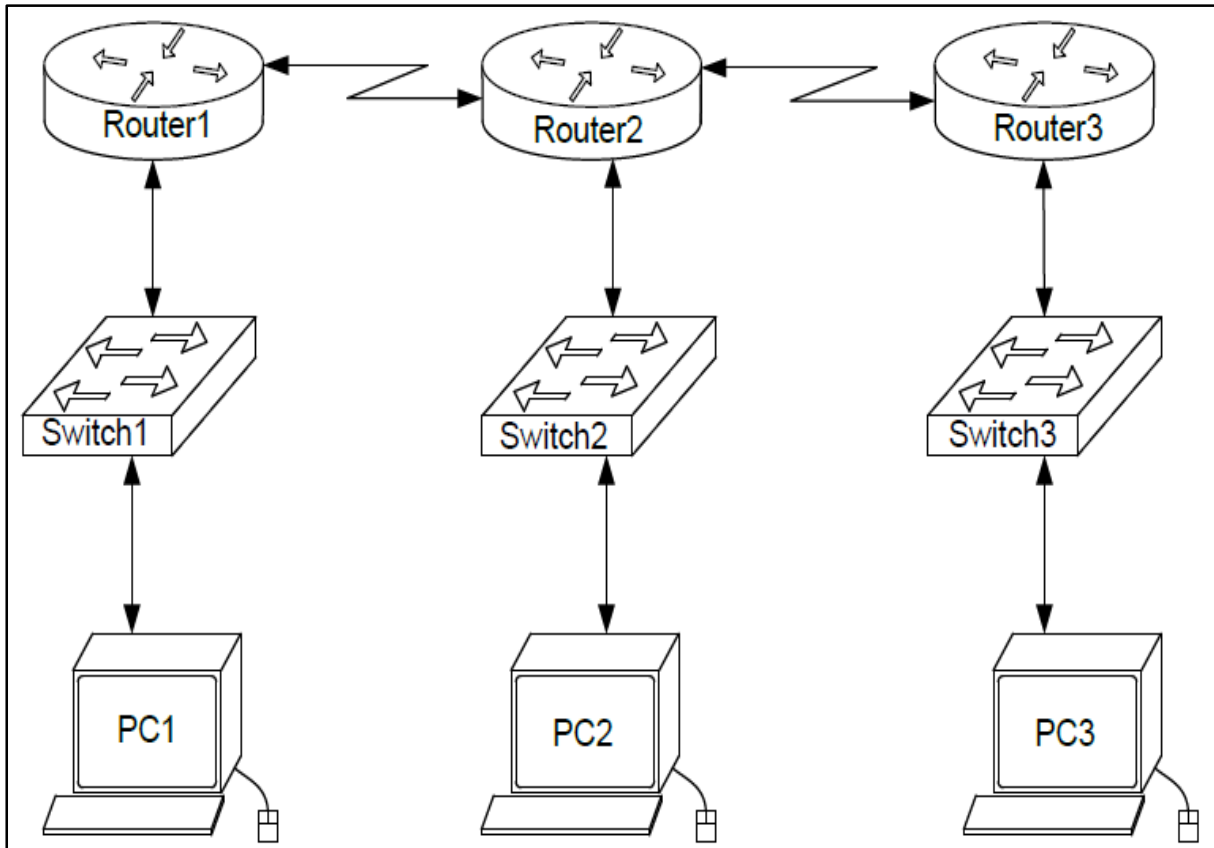


Рисунок 4 - Схема сети

Задание:

- задать всем узлам сети IP адреса;
- настроить динамическую или статическую маршрутизацию всеми узлами сети;
- выявить возможность пересылки данных по протоколу IP между любыми объектами сети;
- разработать и применить на маршрутизаторах списки доступа: запрещающие маршрутизаторам R0 и R2 обмениваться ICMP-пакетами по последовательному сетевому интерфейсу; запрещающие компьютерам PC0 и PC1 обмениваться ICMP-пакетами по интерфейсу Ethernet;
- переключившись в «Режим симуляции» рассмотреть и пояснить процесс обмена данными по протоколу RIP (в случае динамической маршрутизации) между устройствами (выполнив команду Ping с

Задания для самостоятельной работы

=====

одного компьютера на другой). Детальное пояснение включить в отчет.

Структура отчета по работе:

- титульный лист;
- задание;
- топологическая схема сети: указать на схеме наименования узлов сети, адреса и типы сетевых интерфейсов;
- ход работы. Данный раздел состоит из последовательного описания значимых выполняемых шагов (с указанием их сути) и копий экранов (должна быть видна набранная команда и реакция системы, если она есть);
- конфигурации оборудования: привести значимые фрагменты конфигурационных файлов для коммутаторов и маршрутизаторов Cisco, пояснить значение команд;
- выводы.

=====

ЗАКЛЮЧЕНИЕ

Сопровождение, администрирование и управление логической инфраструктурой существующей сети требует глубокого знания многих сетевых технологий. Администратор сети даже в небольшой организации должен уметь создавать различные типы сетевых подключений, устанавливать и конфигурировать необходимые сетевые протоколы, знать методы ручной и автоматической адресации и методы разрешения имен и, наконец, устранять неполадки связи, адресации, доступа, безопасности и разрешения имен.

Моделирование сети является обязательной частью любого администратора безопасности, который всегда является соавтором проекта создания или модернизации корпоративной сети. Целями моделирования могут являться: определение оптимальной топологии, выбор сетевого оборудования, проверка характеристик настраиваемых протоколов. На модели можно проверить влияние всплесков загрузки, воздействие большого потока широковещательных запросов, что вряд ли кто-то может себе позволить в работающей сети.

Cisco Packet Tracer позволяет имитировать работу различных сетевых устройств: маршрутизаторов, коммутаторов, точек беспроводного доступа, персональных компьютеров, сетевых принтеров, IP-телефонов и т.д. Работа с интерактивным симулятором дает ощущение настройки реальной сети, состоящей из десятков или даже сотен устройств. Благодаря такому свойству Cisco Packet Tracer, как режим визуализации, пользователь может отследить перемещение данных по сети, появление и изменение параметров IP-пакетов при прохождении данных через сетевые устройства, скорость и пути перемещения IP-пакетов. Анализ событий, происходящих в сети, позволяет понять механизм ее работы и обнаружить инциденты безопасности.

Заключение

Cisco Packet Tracer может быть использован как сетевое приложение для симулирования виртуальной сети через реальную сеть, в том числе Интернет. Пользователи разных компьютеров, независимо от их местоположения, могут работать над одной сетевой топологией, производя ее настройку или устраняя проблемы.

Автор убежден в том, что у каждого студента имеется возможность освоить представленный в практикуме материал самостоятельно. Последовательность и логика изложения и закрепления учебного материала должны помочь студенту понять важность не только процессов сетевого моделирования, но и процесса их представления в удобном для пользователя виде. И, что тоже немаловажно, специалисты в этой области будут востребованы и имеют прекрасные перспективы получения интересной, достаточно престижной и хорошо оплачиваемой работы.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Cisco ICND 1. Руководство для студента. Изд. Cisco, 2009.
2. Аксенов А. Н. «Проектирование и анализ вычислительных сетей в программном продукте Cisco Packet Tracer». М.: Бука, 2011.
3. Амато В. Ос новы организации сетей Cisco. Том 1. - С.-П.: Вильямс, 2002.
4. Амато В. Основы организации сетей Cisco. Том 2. – С.-П.: Вильямс, 2002.
5. Боллапрагада В., Мёрфи К., Уайт Р. Структура операционной системы Cisco IOS. С.-П.: Вилямс, 2002.
6. Бони Д. Руководство по Cisco IOS. – С.-П.: Питер, Русская Редакция, 2008.
7. Димарцио Д. Ф. Маршрутизаторы CISCO. Пособие для самостоятельного изучения. - С.-П.: Символ-Плюс, 2003.
8. Знакомство с Cisco Packet Tracer // <https://liti-admin.ru/cisco/znaomstvo-s-cisco-packet-tracer.html>.
9. Иванов С.Ю. Маршрутизаторы Cisco. Пособие для самостоятельного изучения. - М.: Символ-Плюс, 2003.
10. Кеннеди К., Гамильтон К. Принципы коммутации в локальных сетях Cisco. - М.: Вильямс, 2003.
11. Командная строка управления устройствами CLI. Виртуальные локальные сети VLAN // <https://www.intuit.ru/studies/courses/3549/791/lecture/29219>.
12. Леинванд А., Пински Б. Конфигурирование маршрутизаторов Cisco. - С.-П.: Вильямс, 2001.
13. Лекции по сетевым технологиям Cisco. С.-П.: Компьютерная академия «Шаг», 2009.
14. Лэмпл Т., Одом Ш., Уоллес К. CCNP. Маршрутизация. Учебное руководство. - С.-П.: Лори, 2015.
15. Маршрутизация на примере одного маршрутизатора // <http://www.netza.ru/2012/11/blog-post.html>.

Библиографический список

- =====
16. Методические указания к лабораторным работам по дисциплине «Вычислительные комплексы и системы» // http://vostok.kai.ru/sveden/files/Metod_V1.V.DV.10.01_09.03.01_LR.pdf.
 17. Моделирование сети с топологией звезда на базе коммутатора // <https://www.intuit.ru/studies/courses/3549/791/lecture/29217>.
 18. Моделирование сети с топологией звезда на базе концентратора // <https://www.intuit.ru/studies/courses/3549/791/lecture/29215>.
 19. Молочков В. Работа в программе Cisco Packet Tracer // <https://www.intuit.ru/studies/courses/3549/791/info>.
 20. Молочков В.П. Работа в программе Cisco Packet Tracer // <http://mayoroven.ru/docum/intuit/course-778-html/>
 21. Морев А. Гайд по установке Cisco Packet Tracer // https://linuxhint.com/install_packet_tracer_ubuntu_1804/.
 22. Основы использования симулятора сетей Cisco Packet Tracer // <https://winitpro.ru/index.php/2019/06/05/ispolzovanie-simulyatora-setej-cisco-packet-tracer/>.
 23. Режим симуляции в Cisco Packet Tracer // <https://www.intuit.ru/studies/courses/3549/791/lecture/29213>
 24. Руденко И.В. Маршрутизаторы CISCO для IP-сетей. - С.-П.: КУДИЦ-ОБРАЗ, 2003.
 25. Соединяем две сети. // <http://habrahabr.ru/blogs/cisconetworks/42986/>.
 26. Хабракен Д. Как работать с маршрутизаторами Cisco. - С.-П.: ДМК-Пресс, 2005.
 27. Герук Ю. Как установить Cisco Packet Tracer 7.3.0 в Ubuntu 19.10? // <https://blogas.info/kak-ustanovit-cisco-packet-tracer-7-3-0-v-ubuntu-19-10>.
 28. Cisco. Второй выпуск. Используем Packet Tracer 5.0 для моделирования сети <http://habrahabr.ru/blogs/cisconetworks/43566/>.
 29. Установка Cisco Packet Tracer 7.1 на дистрибутив Linux Ubuntu 16.04 // <https://zametkinapolyah.ru/kompyuternye-seti/packet-tracer-7-ubuntu-16-04.html>.

Библиографический список

- =====
30. Установка Cisco Packet Tracer 7.1 на операционную систему Windows 10 // <https://zametkinapolyah.ru/kompyuternye-seti/ustanovka-cisco-packet-tracer.html>.
 31. Установка Cisco Packet Tracer 7.1 или 7.2 на Linux // <https://geekbrains.ru/topics/5608>.
 32. [Установка Cisco Packet Tracer 6.0.1 на Ubuntu](http://blog.netskills.ru/2013/12/cisco-packet-tracer-601-ubuntu-install.html) // <http://blog.netskills.ru/2013/12/cisco-packet-tracer-601-ubuntu-install.html>.

Учебное электронное издание

Комплексная защита объектов информатизации. Книга 30

МОНАХОВА Мария Михайловна

АДМИНИСТРИРОВАНИЕ БЕЗОПАСНОСТИ КОМПЬЮТЕРНЫХ СЕТЕЙ
Моделирование

Практикум

Издается в авторской редакции

Системные требования: Intel от 1,3 ГГц; Windows XP/7/8/10; Adobe Reader;
дисковод CD-ROM.

Тираж 25 экз.

Владимирский государственный университет
имени Александра Григорьевича и Николая Григорьевича Столетовых
Изд-во ВлГУ
rio.vlgu@yandex.ru

Институт информационных технологий и радиоэлектроники
кафедра информатики и защиты информации
mariya.monakhova@gmail.com