МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждения высшего образования
«Юго-Западный государственный университет»
(ЮЗГУ)

Кафедра информационной безопасности

УТВЕРЖДАЮ
Проректор по учебной работе
_____ О.Г. Локтионова
«16» 05 2024 г.

Администрирование защищенных телекоммуникационных систем

Методические указания по выполнению лабораторных работ по дисциплине «Администрирование защищенных телекоммуникационных систем» для студентов специальности 10.05.02 Информационная безопасность телекоммуникационных систем

Курск 2024

УДК 004

Составители: Киселев А.В., Кулешова Е.А.

Рецензент

Кандидат технических наук, доцент, доцент кафедры программной инженерии Ю. А. Халин

Администрирование защищенных телекоммуникационных систем: методические указания по выполнению лабораторных работ по дисциплине «Администрирование защищенных телекоммуникационных систем» / Юго-Зап. гос. ун-т; сост.: А.В. Киселев, Е.А. Кулешова. – Курск, 2024. – 78 с.: Библиогр.: с. 78.

Содержат сведения по вопросам изучения технологий, методов и средств, необходимых для администрирования защищенных телекоммуникационных систем.

Методические указания по выполнению лабораторных работ по дисциплине «Администрирование защищенных телекоммуникационных систем» предназначены для студентов специальности 10.05.02 Информационная безопасность телекоммуникационных систем.

Текст печатается в авторской редакции
Подписано в печать 16.05.24 . Формат 60x84 1/16.
Усл. печ.л. 4,3. Уч. –изд.л. 4,1. Тираж 50 экз. Заказ 404
Бесплатно.
Юго-Западный государственный университет.
305040, г. Курск, ул. 50 лет Октября, 94.

Лабораторная работа №1
Знакомство со средой Cisco Packet Tracer.

Моделирование простой сети.

Целью данной лабораторной работы является знакомство с симулятором Cisco Packet Trace и получение базовых навыков по работе с ним.

Задачи:

- Спроектировать простейшую сеть;
- Ознакомиться с утилитой ping и запустить ping-процесс.

Теоретическая часть

Программные продукты Packet Tracer дают возможность создавать сетевые топологии из широкого спектра маршрутизаторов и коммутаторов компании Cisco, рабочих станций и сетевых соединений типа Ethernet, Serial, ISDN, Frame Relay. Эта функция может быть выполнена как для обучения, так и для работы. Например, чтобы сделать настройку сети ещё на этапе планирования или чтобы создать копию рабочей сети с целью устранения неисправности.

Для запуска Cisco Packet Tracer необходимо вызвать исполняемый файл, PacketTracer.exe. Общий вид программы можно увидеть на рис.5.1.

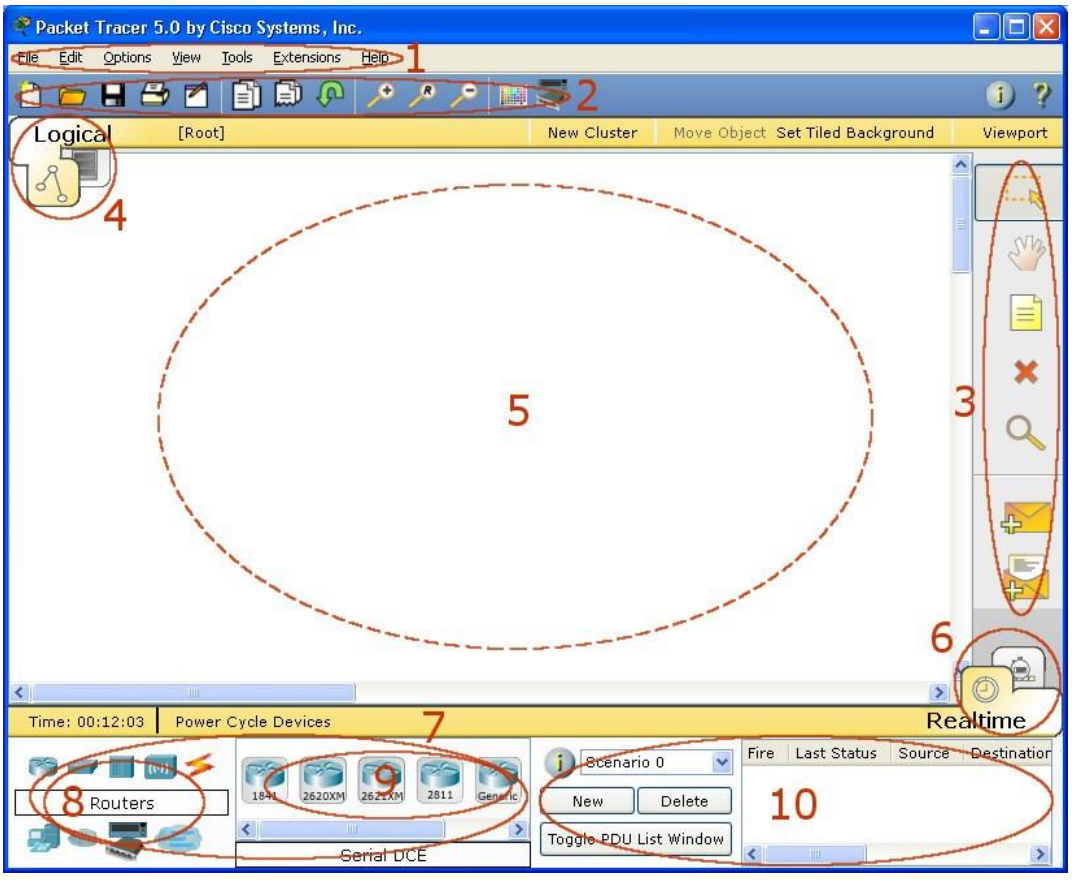

Рис.5.1. Общий вид программы Packet Tracer.

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 логическую, а также позволяет перемещаться между уровнями кластера.
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.
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.

Для создания топологии необходимо выбрать устройство из панели Network Component, а затем из панели Device-Type Selection выбрать тип выбранного устройства. После этого нужно нажать левую кнопку мыши в поле рабочей области программы (Workspace). Также можно переместить устройство прямо из области Device-Type Selection, но при этом будет выбрана модель устройства по умолчанию.

Для быстрого создания нескольких экземпляров одного и того же устройства нужно, удерживая кнопку Ctrl, нажать на устройство в области Device-Specific Selection и

отпустить кнопку Ctrl. После этого можно несколько раз нажать на рабочей области для добавления копий устройства.

В Packet Tracer представлены следующие типы устройств:

- Маршрутизаторы;
- Коммутаторы (в том числе и мосты);
- Хабы и повторители;
- Конечные устройства – ПК, серверы, принтеры, IP-телефоны;
- Беспроводные устройства: точки доступа и беспроводной маршрутизатор;
- Остальные устройства – облако, DSL-модем и кабельный модем.

Добавим необходимые элементы в рабочую область программы так, как показано на рис.5.2.

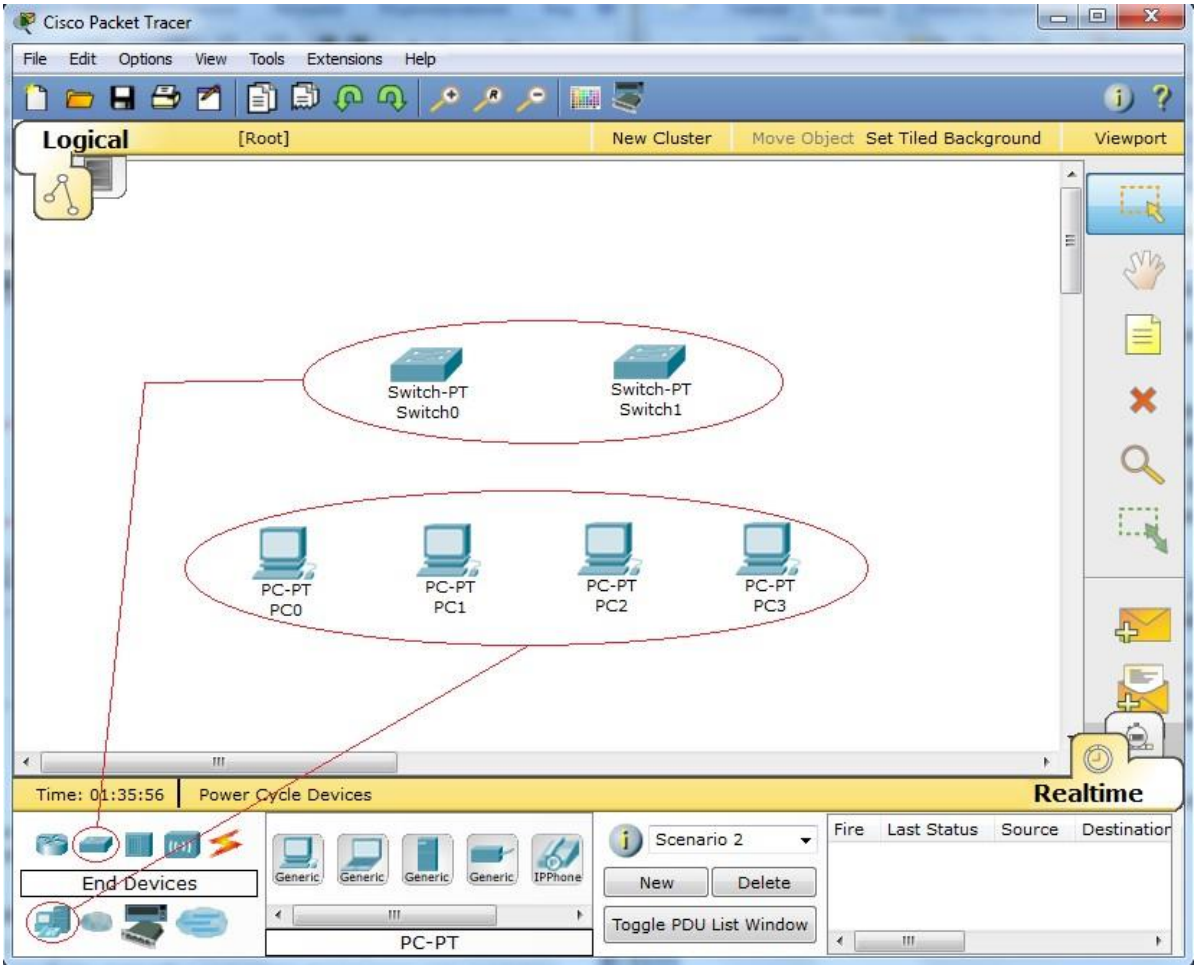

Рис.5.2. Добавление элементов сети.

При добавлении каждого элемента пользователь имеет возможность дать ему имя и установить необходимые параметры. Для этого необходимо нажать на нужный элемент левой кнопкой мыши (ЛКМ) и в диалоговом окне устройства перейти к вкладке Config.

Диалоговое окно свойств каждого элемента имеет две вкладки:

- Physical – содержит графический интерфейс устройства и позволяет симулировать работу с ним на физическом уровне.

- Config – содержит все необходимые параметры для настройки устройства и имеет удобный для этого интерфейс.

Также в зависимости от устройства, свойства могут иметь дополнительную вкладку для управления работой выбранного элемента: Desktop (если выбрано конечное устройство) или CLI (если выбран маршрутизатор) и т.д.

Для удаления ненужных устройств с рабочей области программы используется кнопка Delete (Del).

Свяжем добавленные элементы мы с помощью соединительных связей. Для этого необходимо выбрать вкладку Connections из панели Network Component Box. Мы увидим все возможные типы соединений между устройствами. Выберем подходящий тип кабеля. Указатель мыши изменится на курсор “connection” (имеет вид разъема). Нажмем на первом устройстве и выберем соответствующий интерфейс, с которым нужно выполнить соединение, а затем нажмем на второе устройство, выполнив ту же операцию. Можно также соединить с помощью Automatically Choose Connection Type (автоматически соединяет элементы в сети). Выберем и нажмем на каждом из устройств, которые нужно соединить. Между устройствами появится кабельное соединение, а индикаторы на каждом конце покажут статус соединения (для интерфейсов которые имеют индикатор).

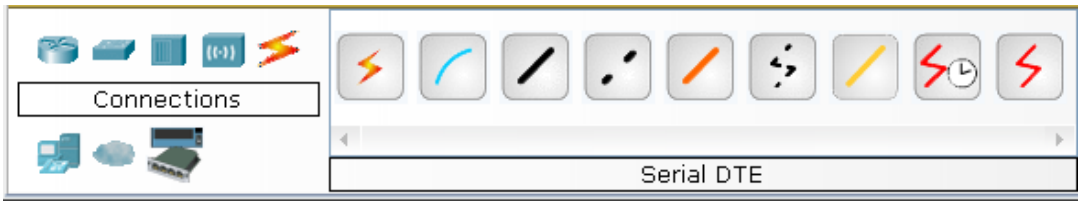

Рис. 5.3. Поддерживаемые в Packet Tracer типы кабелей.

Packet Tracer поддерживает широкий диапазон сетевых соединений (см. табл. 1). Каждый тип кабеля может быть соединен лишь с определенными типами интерфейсов.

Таблица 1. Типы соединений в Packet Tracer

Тип кабеля	Описание
Console	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 одинаковая, 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.
Copper Straight-through	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).
 Copper Cross-over	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).
 Fiber	Оптоволоконная среда используется для соединения между оптическими портами (100 Мбит/с или 1000 Мбит/с).
 Phone	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.
 Coaxial	Коаксиальная среда используется для соединения между коаксиальными портами, такие как кабельный модем, соединенный с облаком Packet Tracer.
  Serial DCE and DTE	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.

После создания сети ее нужно сохранить, выбрав пункт меню File -> Save или иконку Save на панели Main Tool Bar. Файл сохраненной топологии имеет расширение *.pkt .

Packet Tracer дает нам возможность симулировать работу с интерфейсом командной строки (ИКС) операционной системы IOS, установленной на всех коммутаторах и маршрутизаторах компании Cisco.

Подключившись к устройству, мы можем работать с ним так, как за консолью реального устройства. Симулятор обеспечивает поддержку практически всех команд, доступных на реальных устройствах.

Подключение к ИКС коммутаторов или маршрутизаторов можно произвести, нажав на необходимое устройство и перейдя в окно свойств к вкладке CLI.

Для симуляции работы командной строки на конечном устройстве (компьютере) необходимо в свойствах выбрать вкладку Desktop, а затем нажать на ярлык Command Prompt.

Работа с файлами в симуляторе

Packet Tracer дает возможность пользователю хранить конфигурацию некоторых устройств, таких как маршрутизаторы или свичи, в текстовых файлах. Для этого необходимо перейти к свойствам необходимого устройства и во вкладке Config нажать на кнопку “Export…” для экспорта конфигурации Startup Config или Running Config. Так получим диалоговое окно для сохранения необходимой конфигурации в файл, который будет иметь расширение *.txt . Текст файла с конфигурацией устройства running-config.txt (имя по умолчанию) аналогичен тексту информации полученной при использовании команды show running-config в IOS-устройствах.

Необходимо отметить, что конфигурация каждого устройства сохраняется в отдельном текстовом файле. Пользователь также имеет возможность изменять конфигурацию в сохраненном файле вручную с помощью произвольного текстового редактора. Для предоставления устройству сохраненных или отредактированных настроек нужно во вкладке Config нажать кнопку “Load...” для загрузки необходимой конфигурации Stàrtup Config или кнопку “Merge…” для загрузки конфигурации Running Config.

Практическая часть

Добавим на рабочую область программы 2 комутатора Switch-PT. По умолчанию они имеют имена – Switch0 и Switch1.Добавим на рабочее поле четыре компьютера с именами по умолчанию PC0, PC1, PC2, PC3. Соединим устройства в сеть Ethernet , как показано на рис.5.4. Сохраним созданную топологию, нажав кнопку Save (в меню File -> Save).

Откроем свойства устройства PC0, нажав на его изображение. Перейдем к вкладке Desktop и симулируем работу run, нажав Command Prompt.

Список команд получим, если введем «?» и нажмем Enter. Для конфигурирования компьютера воспользуемся командой ipconfig из командной строки, например:

ipconfig 192.168.1.2 255.255.255.0

IP адрес и маску сети также можно вводить в удобном графическом интерфейсе устройства (см. рис.1.5). Поле DEFAULT GATEWAY – адреса шлюза не важно, так как создаваемая сеть не требует маршрутизации.

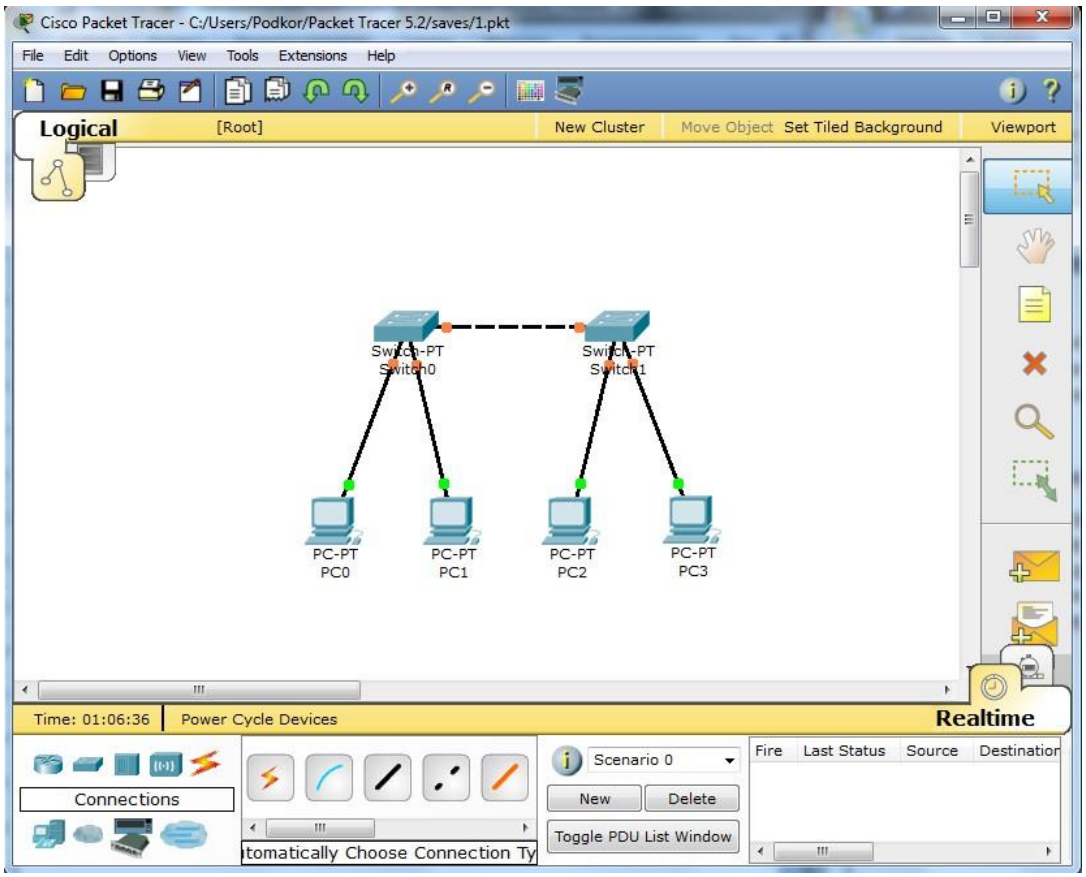

Рис.5.4. Экспериментальная модель сети

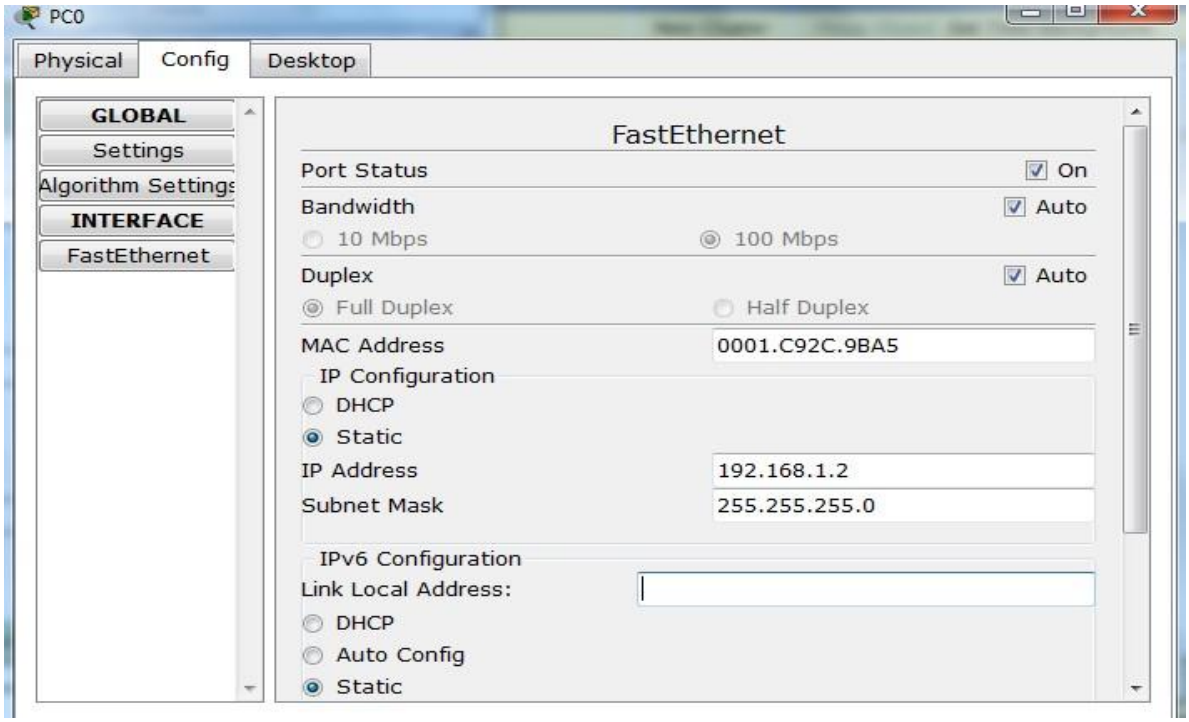

Рис.5.5.Настройка узла

Таким же путем настроим каждый компьютер.

Таблица 2

Устройство	IP ADRESS	SUBNET MASK
PC0	192.168.1.2	255.255.255.0
PC1	192.168.1.3	255.255.255.0
PC2	192.168.1.4	255.255.255.0
PC3	192.168.1.5	255.255.255.0

На каждом компьютере посмотрим назначенные адреса командой ipconfig без параметров.

В Packet Tracer 5.2 предусмотрен режим моделирования, в котором подробно описывается и показывается, как работает утилита Ping. Поэтому необходимо перейти в данный режим, нажав на одноименный значок в нижнем левом углу рабочей области, или по комбинации клавиш Shift+S. Откроется «Панель моделирования» (рис. 5.6.), в которой будут отображаться все события, связанные с выполнения ping-процесса.

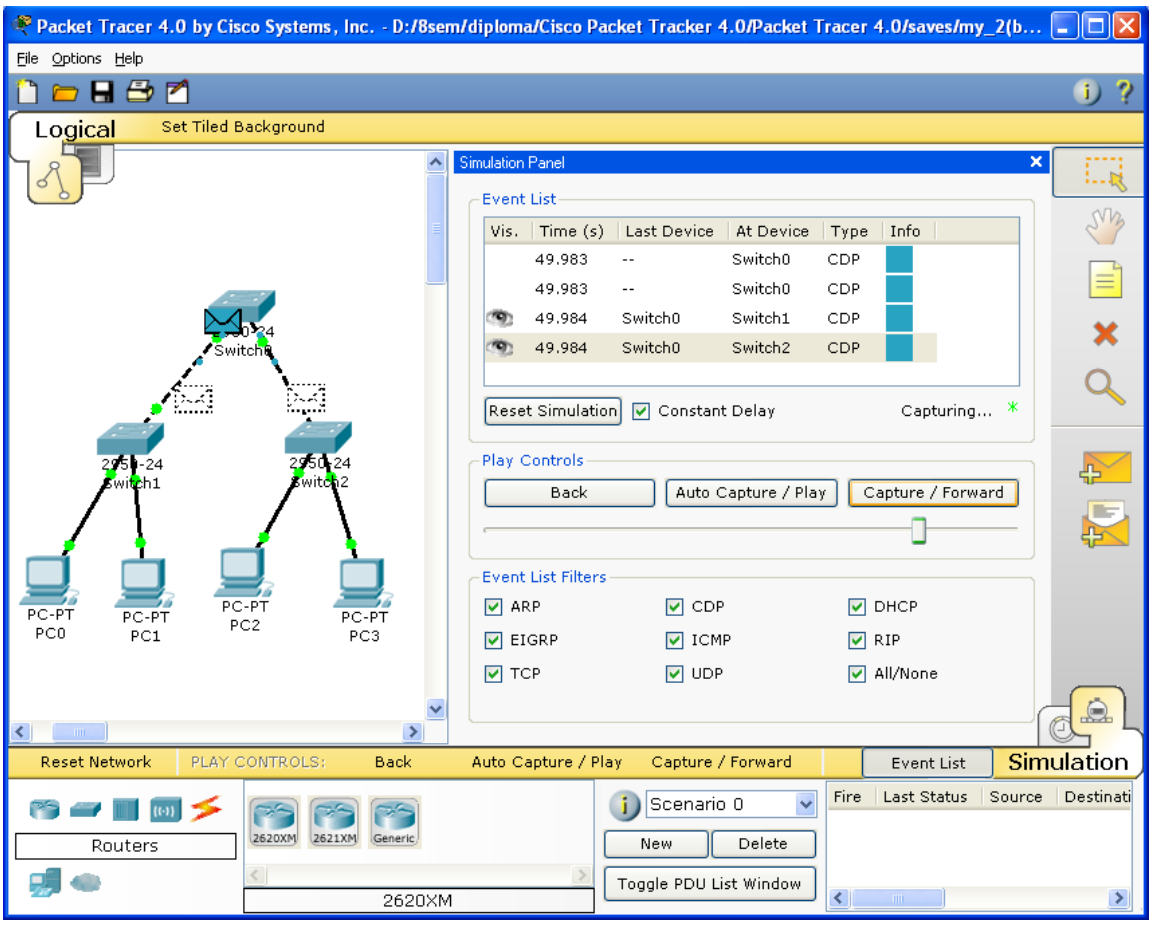

Рис.5.6. «Панель моделирования»

Теперь необходимо повторить запуск ping-процесса. После его запуска можно сдвинуть «Панель моделирования», чтобы на схеме спроектированной сети наблюдать за отправкой/приемкой пакетов.

Кнопка «Автоматически» подразумевает моделирование всего ping-процесса в едином процессе, тогда как «Пошагово» позволяет отображать его пошагово.

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

Моделирование прекращается либо при завершении ping-процесса, либо при закрытии окна «Редактирования» соответствующей рабочей станции.

Если все сделано правильно мы сможем пропинговать любой из любого компьютера. Например, зайдем на компьютер PC3 и пропингуем компьютер PC0. Мы должны увидеть отчет о пинге подобный рисунку 5.7.

Однако, это не все преимущества Packet Tracer: в «Режиме симуляции» можно не только отслеживать используемые протоколы, но и видеть, на каком из семи уровней модели OSI данный протокол задействован (см.рис.5.8).

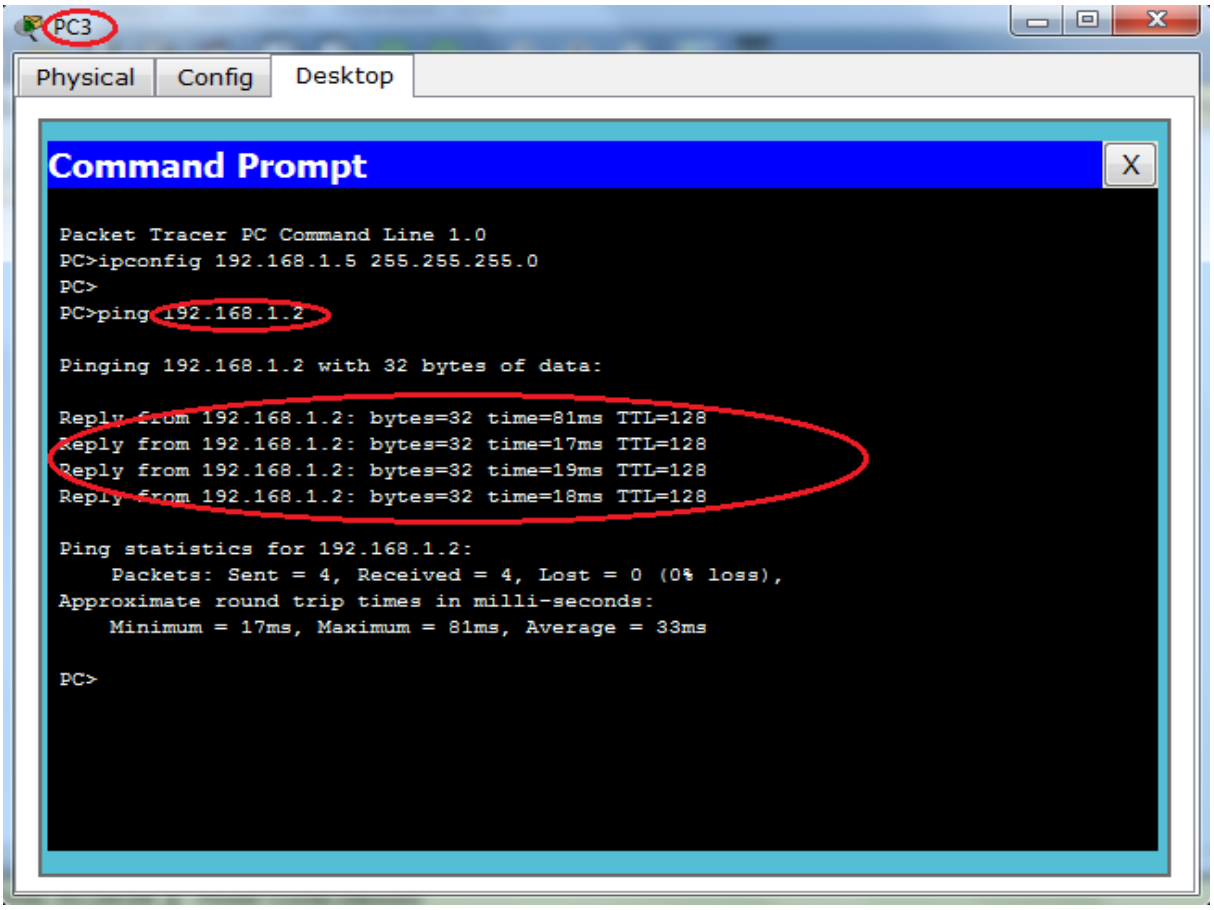

Рис.5.7. Выполнение команды ping в командной строке

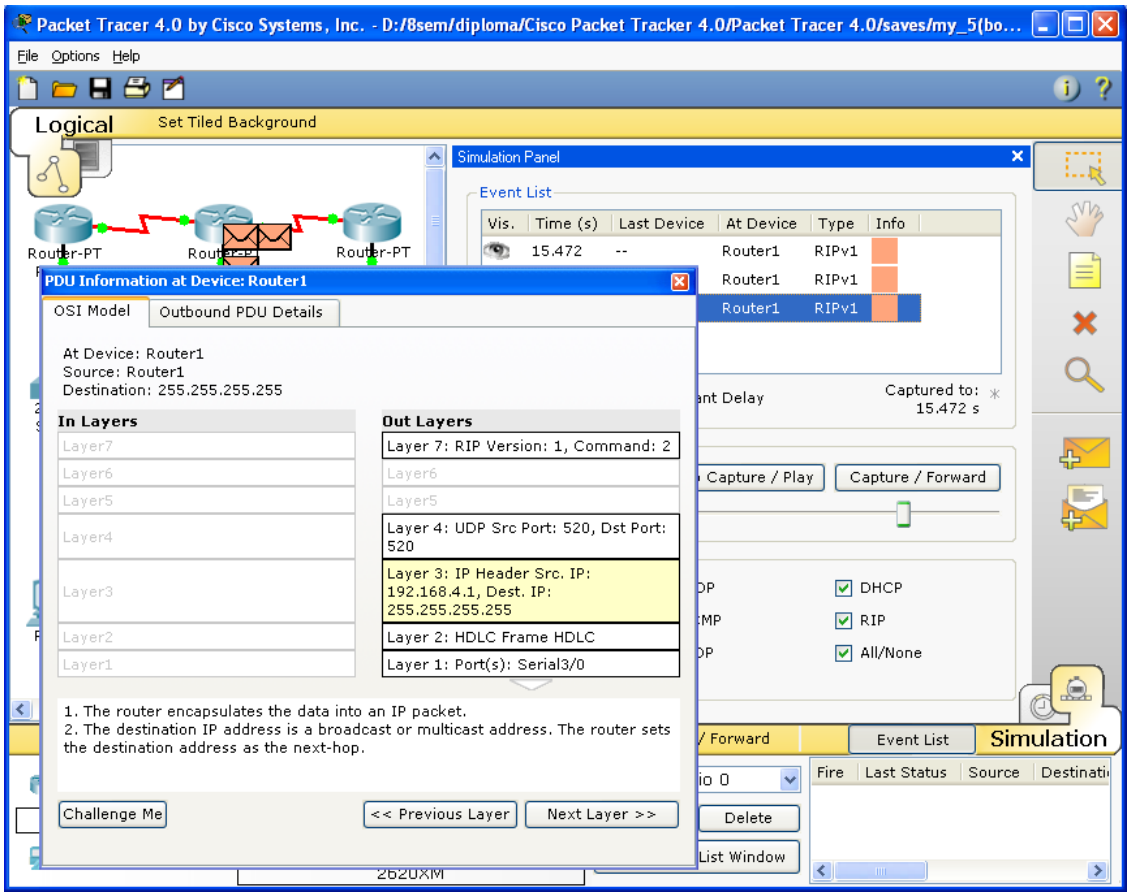

Рис.5.8 Анализ семиуровневой модели OSI в Cisco Packet Tracer 5.2.

Контрольные вопросы

1. Какие типы сетевых устройств и соединений можно использовать в Packet Tracer?
2. Каким способом можно перейти к интерфейсу командной строки устройства.
3. Как добавить в топологию и настроить новое устройство?
4. Как сохранить конфигурацию устройства в .txt файл?

Задание для самостоятельной работы:

1. Создайте топологию рис. 5.9.

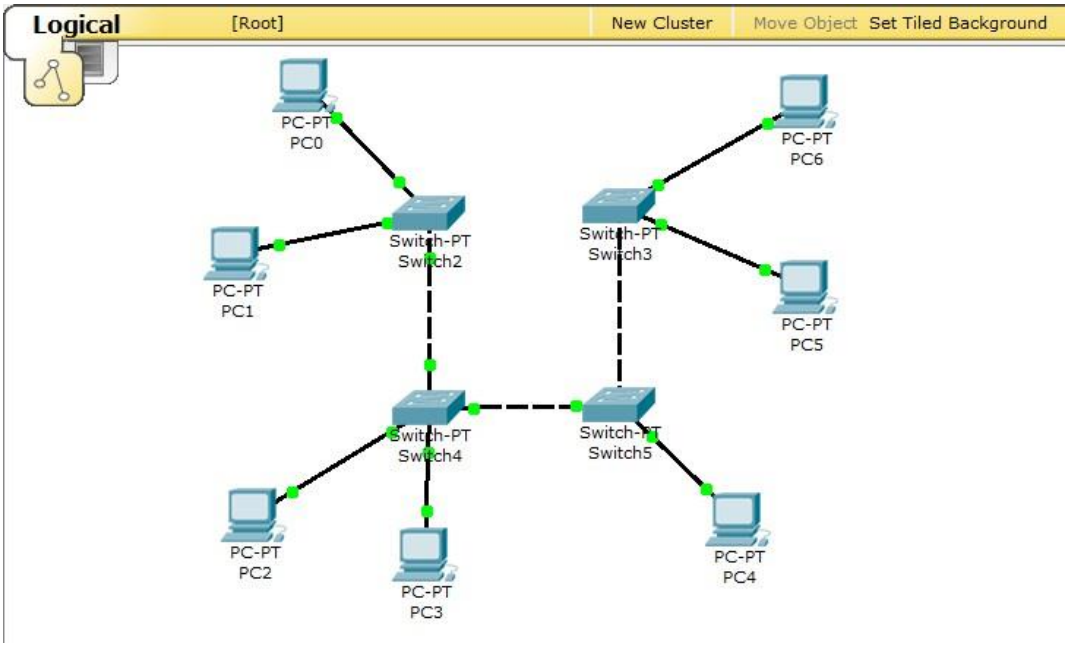

Рис 5.9. Топология сети для исследования

2. Назначьте компьютерам адреса, согласно варианту v

Таблица 3.

Устройство	IP ADDRESS	SUBNET MASK
PC1	v*10. v.1.1	Маска подсети определяется в зависимости от класса сети, к которому принадлежит IP адрес
PC2	v*10. v.1.2	
PC3	v*10. v.1.3	
PC4	v*10. v.1.4	
PC5	v*10. v.1.5	
PC6	v*10. v.1.6	

Например, для варианта 7 (v=7) и компьютера PC5 имеем IP ADDRESS 70.7.1.5, маска 255.0.0.0.

Если сделано всё правильно вы сможете пропинговать любой компьютер из любого.

3. Выполните утилиту ping, согласно табл.4.

Таблица 4.

Вариант v%7	Пинг из	Пинг в	Вариант v	Пинг из	Пинг в
1	PC1	PC6	8	PC6	PC5
2	PC2	PC6	9	PC1	PC6
3	PC3	PC1	10	PC2	PC6
4	PC4	PC2	11	PC3	PC1
5	PC5	PC3	12	PC4	PC2
6	PC6	PC4	13	PC5	PC3
7	PC6	PC5	14	PC6	PC4

4. В «Режиме симуляции» отследите движение пакетов и используемые протоколы, (см.рис 5.8).

5. Переключившись в «Режим симуляции» рассмотреть и пояснить процесс обмена данными по протоколу ICMP между устройствами (выполнив команду Ping с одного компьютера на другой п.3), пояснить роль протокола ARP в этом процессе. Детальное пояснение включить в отчет.

6. Убедиться в достижимости всех объектов сети по протоколу IP.

Содержание отчёта

Отчёт готовится в электронном виде и распечатывается. Отчёт содержит:

1. Титульный лист;
2. Задание (Скриншот топологии согласно варианту)
3. Схема сети.
4. Ход работы:
    a. Данный раздел состоит из последовательного описания значимых выполняемых шагов (с указанием их сути) Пояснения работы команды ping и **содержимго протоколов**.
    b. копий экранов (должна быть видна набранная команда и реакция системы, если она есть).
5. Выводы.

Лабораторная работа № 2

На сегодняшний день на рынке IT существуют не так уж и много сетевых симуляторов.

Широко известны такие симуляторы, как:

- BOSON NET SIM;
- CISCO Router eSim;
- Cisco Packet Tracker;
- Network Emulator;
- Dynamips;
- Cisco 7200 Simulator.

Из них наиболее распространенные в плане использования для обучения являются Boson NetSim, Cisco Packet Tracer и Network Emulator. Остановимся на них подробней.

1..1 Boson NetSim

Boson NetSim – программное обеспечение, которое моделирует работу сетевого оборудования Cisco, и разработано, чтобы помочь пользователю в изучении Cisco IOS.

Большинство других программных продуктов, «моделируя» поведение системы в заранее подготовленных лабораторных работах, фактически не могут отображать ситуаций, которые действительно могут случиться в сети. В отличие от них, NetSim использует технологии, специально разработанные компанией Boson, которые позволяют обойти этот недостаток и моделировать истинное поведение сети. Эти технологии позволят многим пользователям Boson NetSim выйти далеко за рамки выдуманных лабораторных работ, и лучше понять принципы функционирования Cisco IOS [5].

NetSim имеет очень развитую поддержку, обеспечивающую компанией Boson (это связано, конечно же, с бурными темпами развития телекоммуникационных сетей). В связи с этим, компания Cicso рекомендует использовать этот продукт для подготовки к сдачи экзаменов. Поэтому Boson выпускает различные версии NetSim’а, каждая из которых ориентирована на определенный экзамен и, соответственно, уровень знания пользователя.

Существует три версии NetSim’а для следующих экзаменов: NetSim для CCENT, NetSim для CCNA и NetSim для CCNP.

1.2 Cisco Packet Tracer

Данный программный продукт разработан компанией Cisco и рекомендован использоваться при изучении телекоммуникационных сетей и сетевого оборудования.

Packet Tracer 4.0 включает следующие особенности:

- моделирование логической топологии: рабочее пространство для того, чтобы создать сети любого размера на CCNA-уровне сложности;

- моделирование в режиме реального времени;
- режим симуляции;
- моделирование физической топологии: более понятное взаимодействие с физическими устройствами, используя такие понятия как город, здание, стойка и т.д.;
- улучшенный GUI, необходимый для более качественного понимания организации сети, принципов работы устройства;
- многоязыковая поддержка: возможность перевода данного программного продукта практически на любой язык, необходимый пользователю;
- усовершенствованное изображение сетевого оборудования со способностью добавлять / удалять различные компоненты;
- наличие Activity Wizard позволяет студентам и преподавателям создавать шаблоны сетей и использовать их в дальнейшем.

С помощью данного программного продукта преподаватели и студенты могут придумывать, строить, конфигурировать сети и производить в них поиск неисправностей. Packet Tracer дает возможность более подробно представлять новейшие технологии, тем самым делая учебный процесс чрезвычайно полезным с точки зрения усвоения полученного материала [7].

1.3 Network Emulator

Программа Network Emulator была задумана в начале 1997 года. Проект превратился, по сути, в программу, обучающую ее пользователя всем тонкостям технологии на разных уровнях: от базовых понятий до особенностей обработки отдельных полей сетевых пакетов. Программа прошла путь от простейшего «роутера пакетов» до интеллектуального организатора виртуальных машин: на любом из компьютеров можно запустить несколько программ-аналогов настоящих приложений. Все они будут исполняться одновременно.

В дальнейшем появилось и другое «призвание» Network Emulator: обучение студентов принципу администрирования IP-сетей. Данное направление использования было с успехом реализовано в процессе проведения лабораторных работ по предмету "Сети ЭВМ" в Ульяновском Государственном Техническом Университете.

Данный симулятор включает в себя следующие возможности и технологии:

- маршрутизация, система моделирования каналов, IP-фильтрация;
- типы пакетов: ICMP, UDP, TCP, а так же низкоуровневые ARP-запросы;
- концепция интерфейсов и сокетов (простой, дейтаграммный и потоковый);
- эмуляция хостов, коммутаторов второго уровня и концентраторов;
- установка уровня помех на канале;
- связывание нескольких Network Emulator через реальную сеть TCP/IP [10].

В рамках курса лабораторные работы будут выполняться на Cisco Packet Tracer 4.0.

Cisco Packet Tracer 4.0 специально разработан для начала изучения современных телекоммуникационных систем, и больше других симуляторов соответствует данной задаче.

2 Cisco Packet Tracer

Данный симулятор позволяет студентам проектировать свои собственные сети, создавая и отправляя различные пакеты данных, сохранять и комментировать свою работу. Студенты могут изучать и использовать такие сетевые устройства, как коммутаторы второго и третьего уровней, рабочие станции, определять типы связей между ними и соединять их. После того, как сеть спроектирована, студенты могут приступать к конфигурированию выбранных устройств посредством терминального доступа или командной строки (см. рис.2.1).

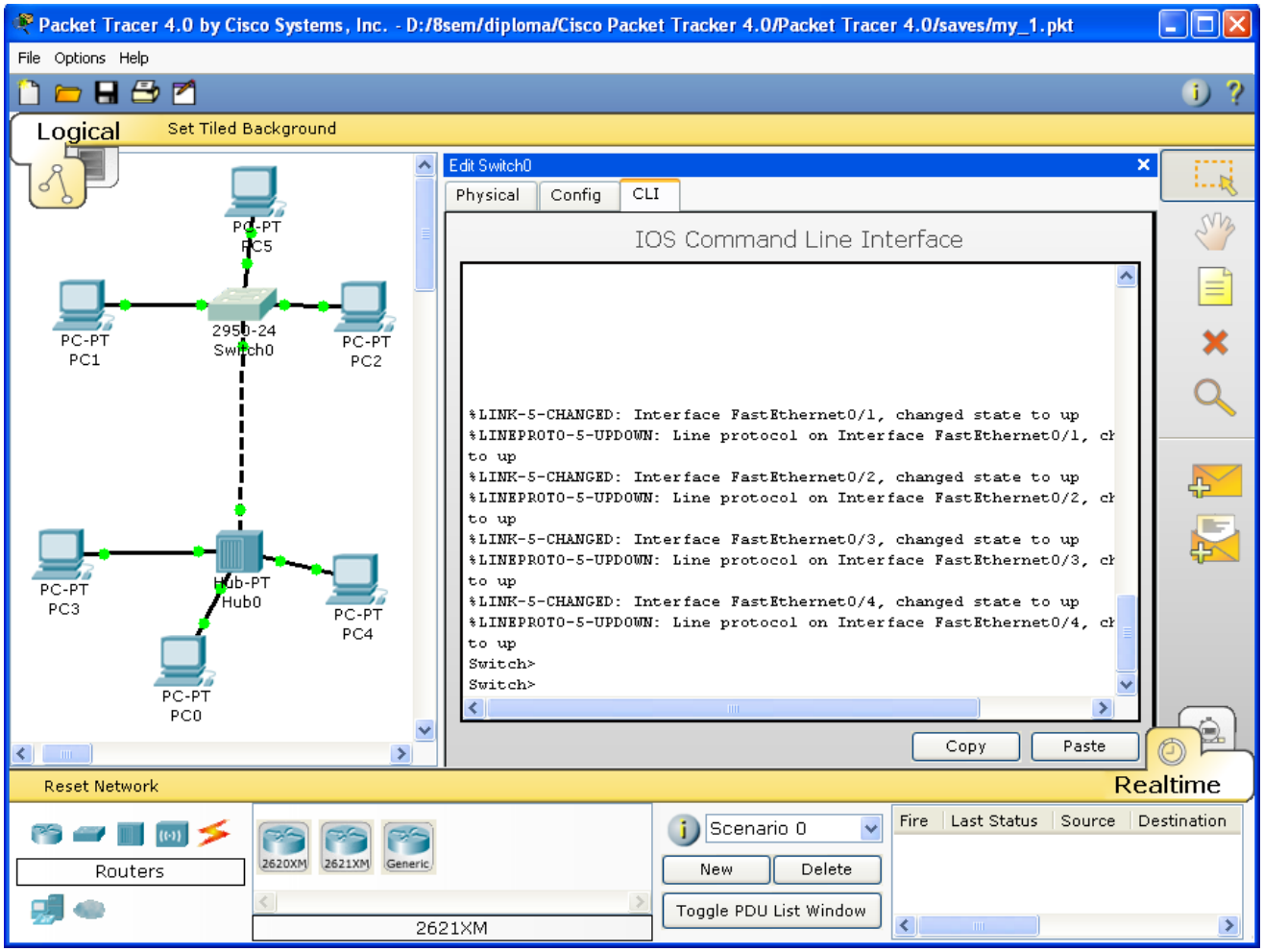

Рис.2.1 Cisco Packet Tracer 4.0

Отличительной особенностью данного симулятора является наличие в нем «Режима симуляции» (рис.2.2). В данном режиме все пакеты, пересылаемые внутри сети, отображаются графически. Эта возможность позволяет студентам наглядно продемонстрировать, по какому интерфейсу в данные момент перемещается пакет, какой протокол используется и т.д.

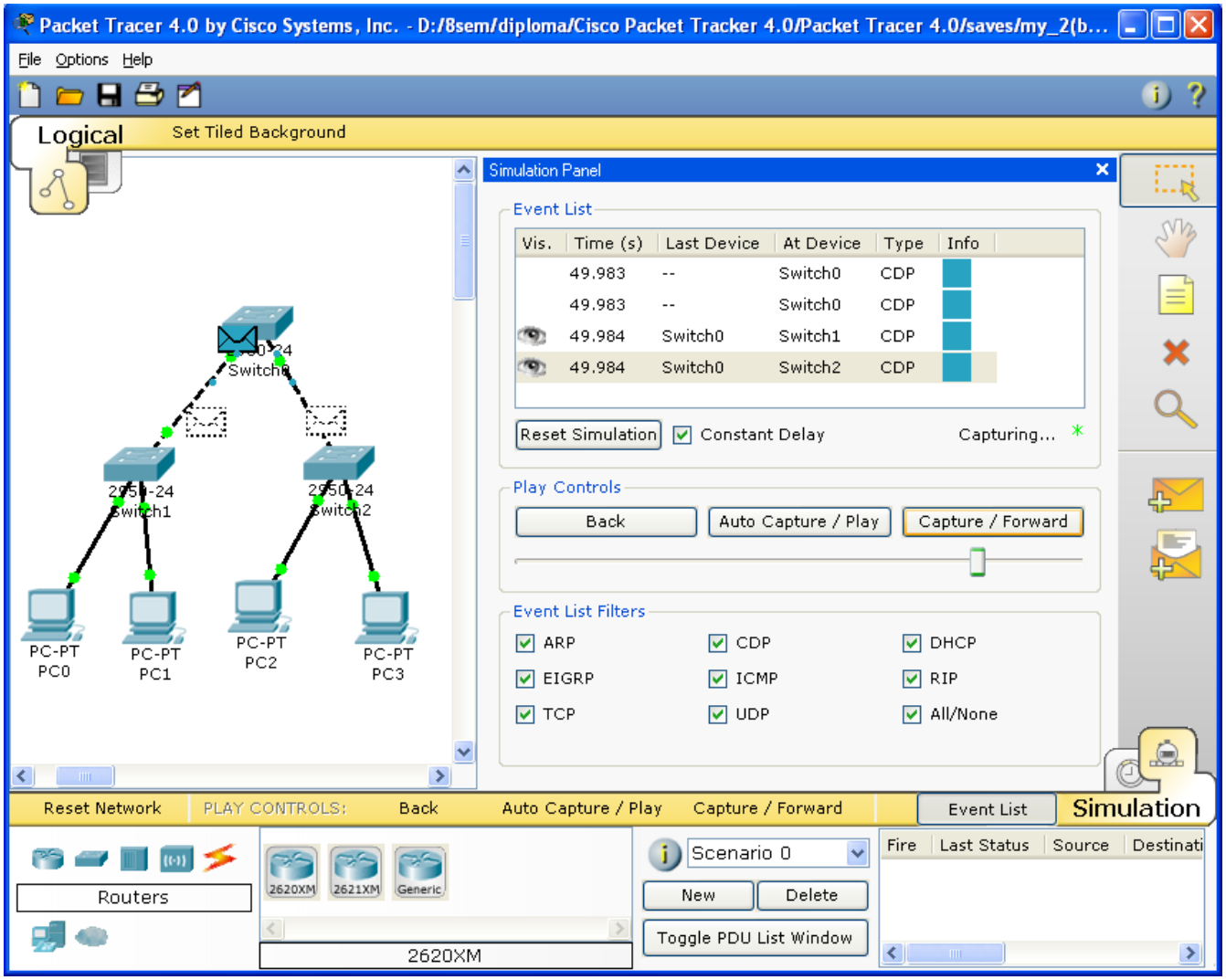

Рис.2.2 Режим «Симуляции» в Cisco Packet Tracer 4.0

Однако, это не все преимущества Packet Tracer: в «Режиме симуляции» студент может не только отслеживать используемые протоколы, но и видеть, на каком из семи уровней модели OSI данный протокол задействован (см.рис.2.3).

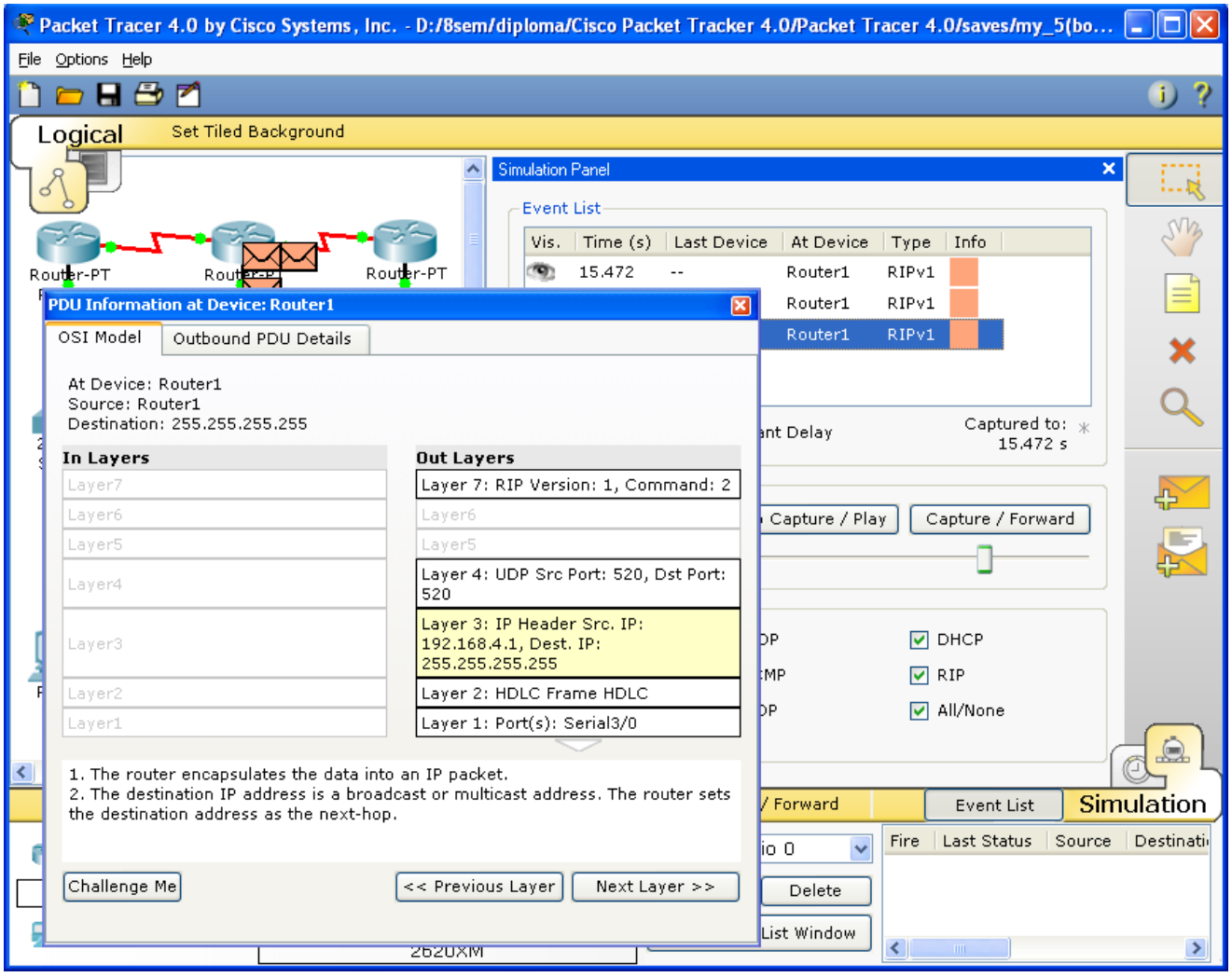

Рис.2.3 Анализ семиуровневой модели OSI в Cisco Packet Tracer 4.0

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 так же немало различных типов связей, что позволяет проектировать сети любого размера на высоком уровне сложности:

моделируемые устройства:

- коммутаторы третьего уровня:
  - Router 2620 XM;
  - Router 2621 XM;
  - Router-PT.
- Коммутаторы второго уровня:
  - Switch 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.

Типы связей:

- консоль;
- медный кабель без перекрещивания (прямой кабель);
- медный кабель с перекрещиванием (кросс-кабель);
- волоконно-оптический кабель;
- телефонная линия;
- Serial DCE;
- Serial DTE.

Так же целесообразно привести те протоколы, которые студент может отслеживать:

- ARP;
- CDP;
- DHCP;
- EIGRP;
- ICMP;
- RIP;
- TCP;
- UDP.

3 Описание терминального режима

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. Последний способ предпочтительнее, потому что процесс конфигурирования маршрутизатора может изменять параметры IP-интерфейсов, что приведет к потере соединения, установленного через Telnet. Кроме того, по соображениям безопасности доступ к маршрутизатору через Telnet следует запретить [8].

В рамках данного курса конфигурация маршрутизаторов будет осуществляться посредством терминала.

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**.

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 внтури других контекстов конфигурирования.

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

router(config)# /глобальный/
router(config-if)# /интерфейса/
rounter(config-router)# /динамической маршрутизации/
rounter(config-line)# /терминальной линии/

ВАЖНО! Студенты должны запомнить 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 студенты должны 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**. Кроме того, команда **end**, поданная в любом из контекстов конфигурирования немедленно завершает процесс конфигурирования и возвращает оператора в контекст администратора.

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

Упрощенная схема контекстов представлена на рис.3.1.

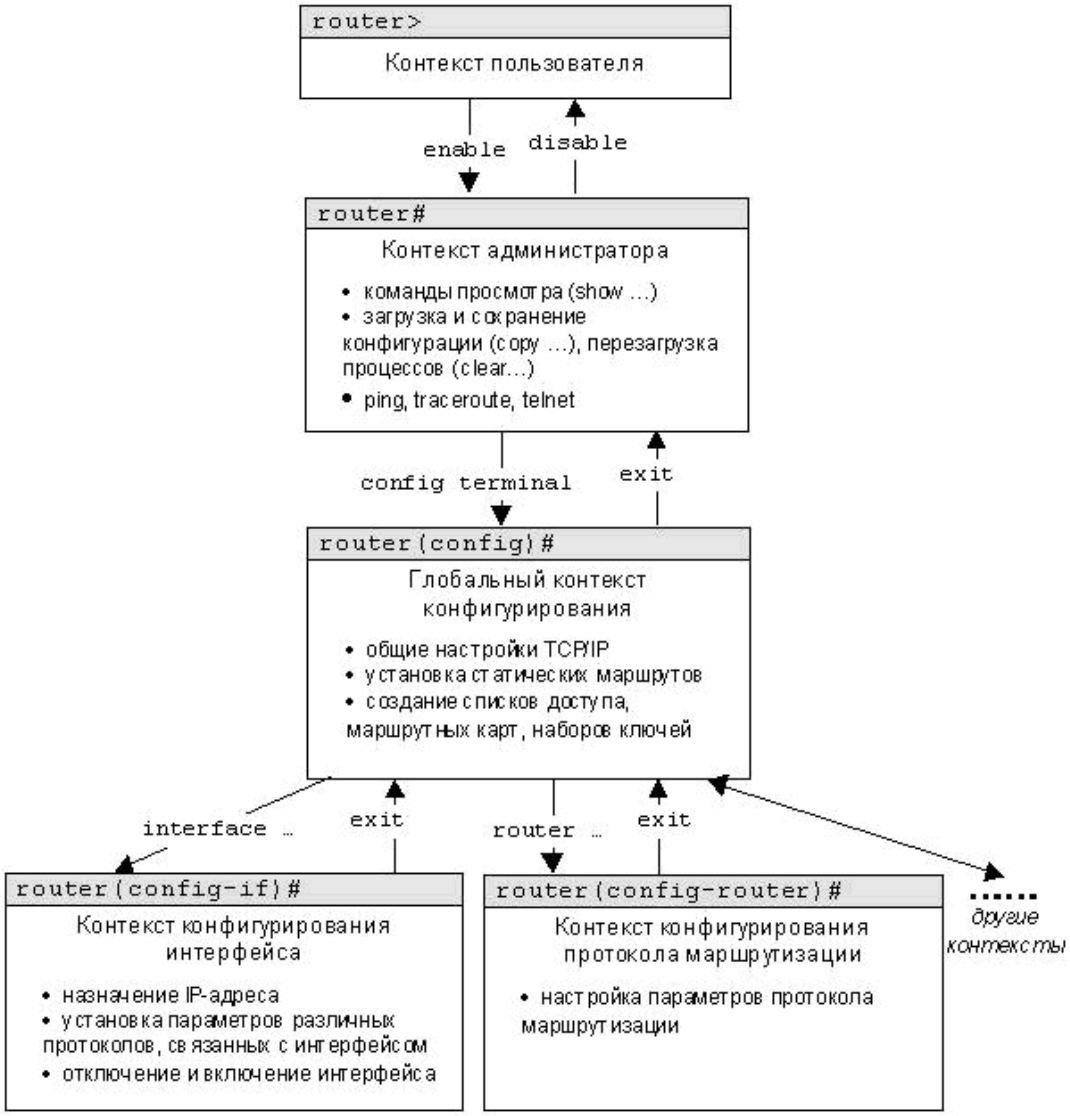

Рис.3.1. Схема контекстов Cisco IOS

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 [2].

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/

Подробнее о конфигурировании устройств можно узнать из [1], [2], [8].

4 Список команд

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

4.1 Глобальный контекст конфигурирования

4.1.1 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 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.

4.1.2 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*

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.

4.1.3 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)#

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.

4.1.4 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 выходной_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 Serial2/0
Router(config)#
```

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.

4.1.5 Команда «Hostname»

Данная команда используется для изменения имени конфигурируемого устройства.

Формат команды:

hostname *новое_имя*

Пример выполнения команды:

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

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

4.1.6 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)#
```

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

4.2 Контекст конфигурирования интерфейса

4.2.1 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 да выбранный интерфейс накладывается список доступа под номером 10: он будет проверять все входящие в интерфейс пакеты, так как выбран параметр in.

4.2.2 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*

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.

4.2.3 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 (расшифровать). 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 *татовая_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.

4.2.4 Команда «Ip address»

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

4.2.5 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 Interface Vlan1, changed state to up
Switch(config-if)#
```

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

4.3 Контекст администратора

4.3.1 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 лабораторного курса конфигурирование будет производиться **только** посредством терминала.

Из режима глобальной конфигурации можно делать изменения, который 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.

4.3.2 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 могу быть восстановлены или сброшены.

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.

4.3.3 Команда «Show»

Show (англ. - показывать) – одна из наиболее важных команд, использующихся 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.

4.3.3.1 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
...
```

На экран выводится текущие настройки коммутатора.

4.3.3.2 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 энергонезависим 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.

4.3.3.3 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
       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.

4.3.3.4 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
Incoming update filter list for all interfaces is not set
Redistributing: rip
Default version control: send version 1, receive 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.

4.3.4 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)
```

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

4.4 Контекст пользователя

4.4.1 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.

4.5 Контекст конфигурирования маршрутизации

4.5.1 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.

Подробнее об этих и о других командах можно узнать из [1], [2], [3], [6].

5 Лабораторные работы

5.2 Лабораторная работа №2. Основы работы с интерфейсом оборудования Cisco.

Целью данной лабораторной работы является получение базовых навыков по работе с командным интерфейсом коммутаторов Cisco. Рассматриваются приемы первичной настройки коммутаторов, обеспечения их защищенности и доступности для управления.

Новые приобретаемые навыки в работе с оборудованием Cisco:

- Изменение имени оборудования (hostname);
- Вход в привилегированный режим (enable);
- Вход в режим конфигурации настроек (configure terminal);
- Вход в режим конфигурирования линий (консоль, терминальные подключения) (line?);
- Вход в режим конфигурирования интерфейсов виртуальный сетей (interface VLAN ?);
- Задание пароля для перехода в привилегированный режим (enable secret?);
- Задание ip-адреса для интерфейса виртуальной сети коммутатором (ip address ?);
- Сохранение текущей конфигурации (copy running-config startup-config);
- Просмотр текущей работающей конфигурации (show running-config);
- Просмотр сохраненной конфигурации (show startup-config);
- Настройка ip-адресов персональных компьютеров (winipcfg, ipconfig ?);
- Выявление достижимости персональных компьютеров и коммутаторов в сети (ping?);
- Просмотр записей arp-таблицы персональных компьютеров (arp).

Схема сети:

- Коммутаторы S1, S2, S3 (3 шт.);
- Персональные компьютеры PC1, PC2, PC3, PC4 (4 шт.);
- Схема сети представлена на рис.5.2.

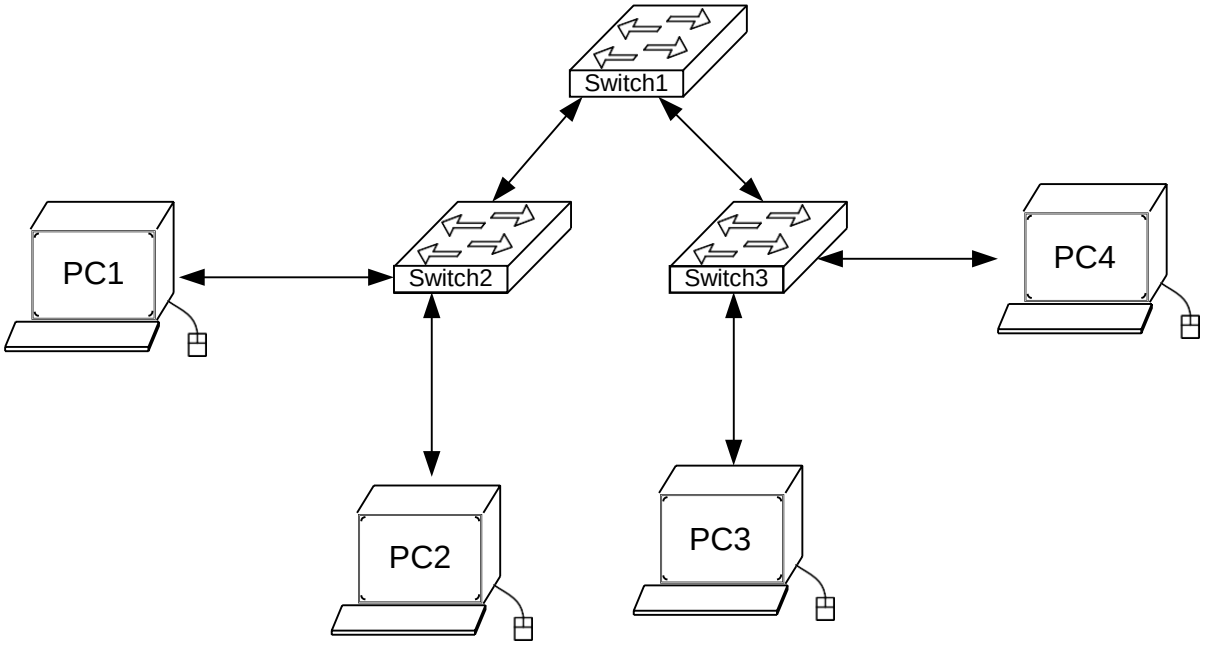

Рис.5.2. Схема сети

Задание:

- Изменить имя коммутаторам Cisco;
- 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);
- 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» (описанном в методических указаниях к предыдущей лабораторной работе) 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 копий экранов (должна быть видна набранная команда и реакция системы, если она есть).
- Выводы.

Лабораторная работа №3. Настройка статической маршрутизации на оборудовании Cisco.

Целью данной лабораторной работы является изучение процессов настройки статических маршрутов на маршрутизаторах Cisco.

Новые приобретаемые навыки в работе с оборудованием Cisco:

- Синхронизация времени для последовательных сетевых интерфейсов (clock rate ?);
- Задание статических маршрутов и маршрутов «по умолчанию» (ip route ?);
- Просмотр созданной таблицы маршрутов (show ip route ?).

Схема сети:

- Коммутаторы S1, S2, S3 (3 шт.);
- Маршрутизаторы R1, R2, R3 (3 шт.);
- Персональные компьютеры C1, C2, C3 (3 шт.);
- Схема сети представлена на рис.6.3.

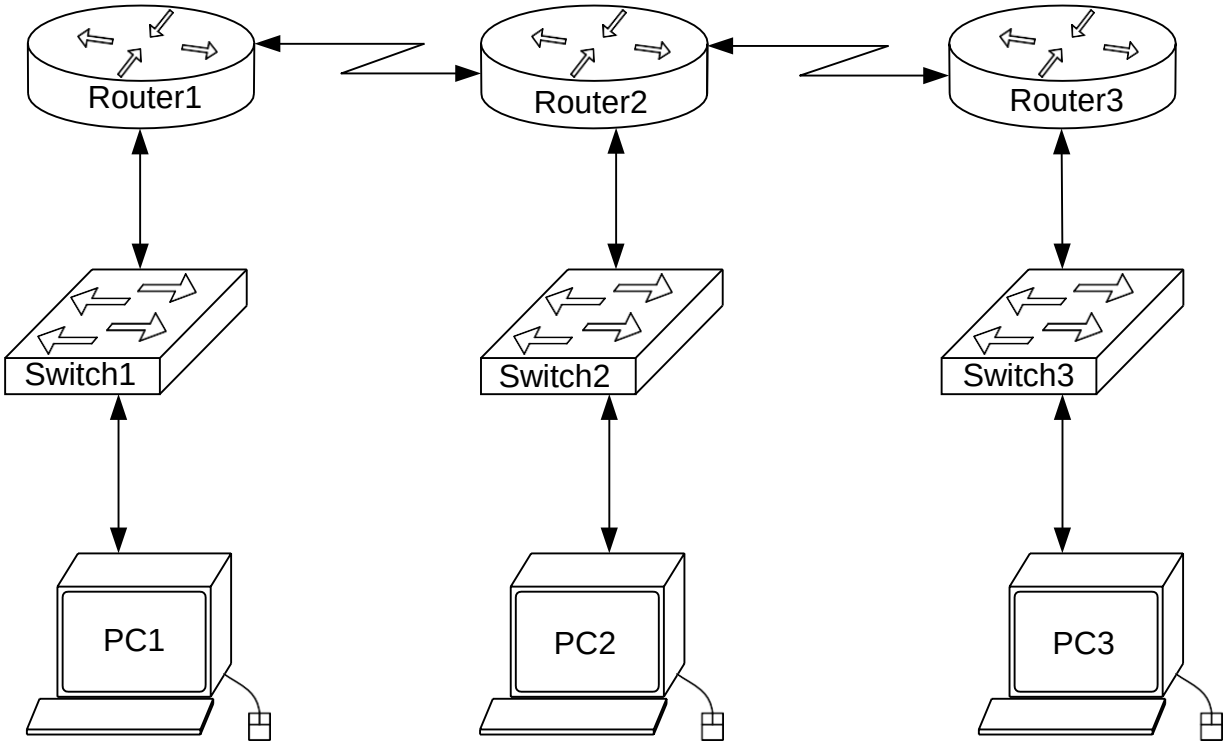

Рис.5.3. Схема сети

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.);
- 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 (ping);
- 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 Cisco, пояснить значение команд.
- Выводы.

Лабораторная работа №4. Настройка протоколов маршрутизации RIP на оборудовании Cisco.

Целью данной лабораторной работы является настройка протоколов динамической маршрутизации на оборудовании Cisco.

Новые приобретаемые навыки в работе с оборудованием Cisco:

- Включение на маршрутизаторе поддержки протокола RIP (router rip);
- Настройка протокола RIP на поддержку маршрутизации требуемых сетей (network?);
- Просмотр таблицы маршрутизации (show ip route);
- Просмотр работающих протоколов маршрутизации (show ip protocols).

Схема сети:

- Коммутаторы S1, S2, S3 (3 шт.);
- Маршрутизаторы R1, R2, R3 (3 шт.);
- Персональные компьютеры C1, C2, C3 (3 шт.);
- Схема сети представлена на рис.6.4.

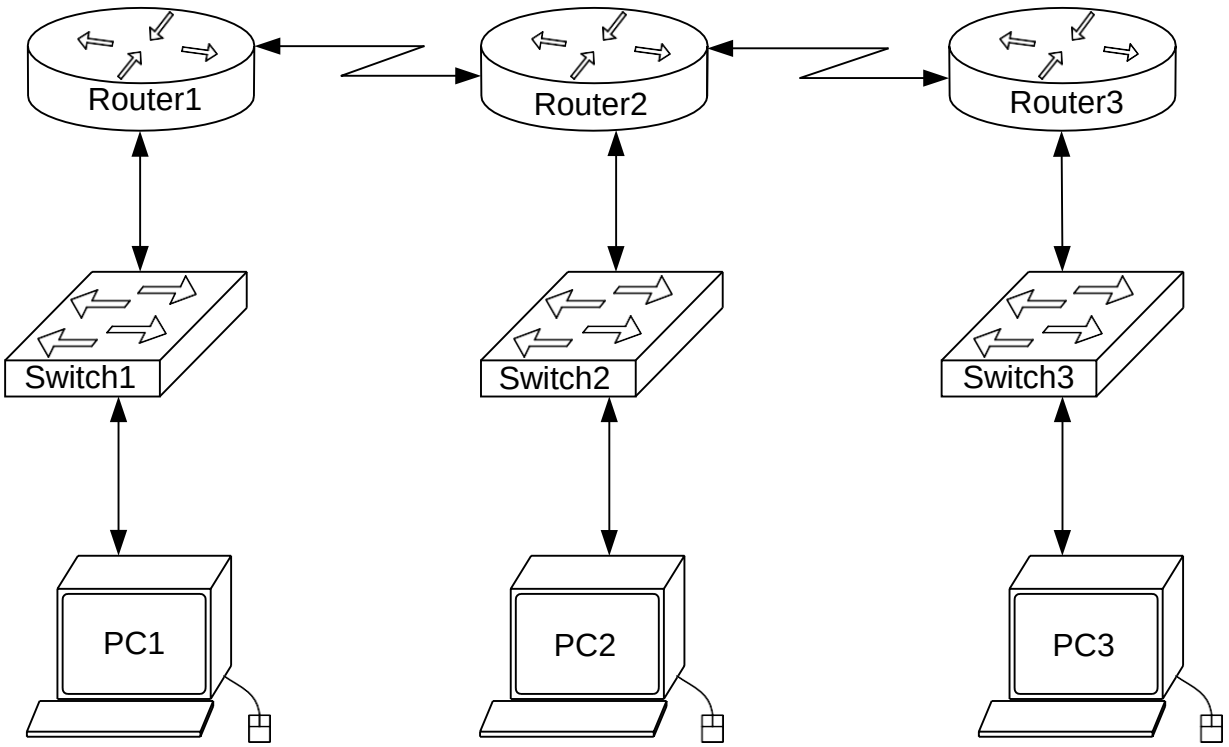

Рис.5.4. Схема сети

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;
- 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 (startup—config) для коммутаторов и маршрутизаторов Cisco, пояснить значение команд.
- Выводы.

Лабораторная работа №5. Применение списков доступа на оборудовании Cisco.

Целью данной лабораторной работы является настройка стандартных списков доступа на маршрутизаторах Cisco и знакомство с расширенными списками доступа.

Новые приобретаемые навыки в работе с оборудованием Cisco:

- Сопоставление интерфейсу маршрутизатора некоторой группы доступа (ip access-group ?);
- Создание списков доступа позволяющих или препятствующих передачи данных между узлами сети (access-list ?).

Схема сети:

- Коммутаторы S1, S2, S3 (3 шт.);
- Маршрутизаторы R1, R2, R3 (3 шт.);
- Персональные компьютеры PC1, PC2, PC3 (3 шт.);
- Схема сети представлена на рис.6.5.

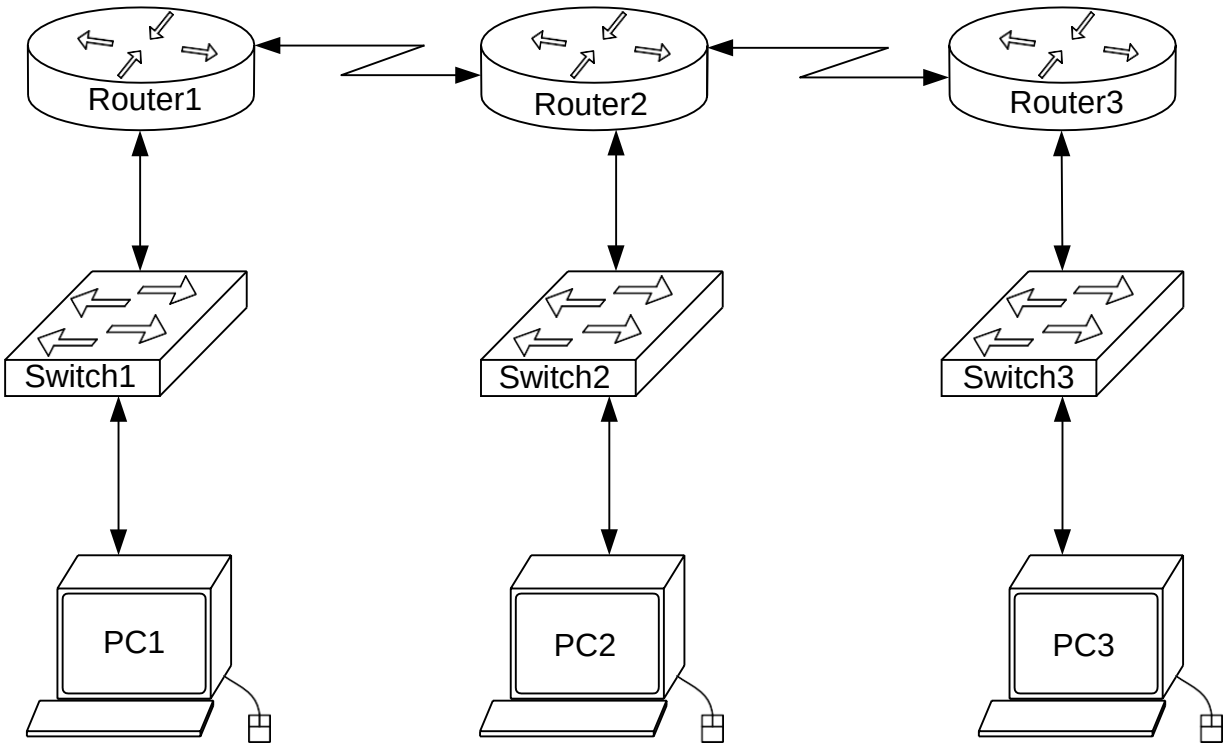

Рис.5.5. Схема сети

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 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 (startup—config) для коммутаторов и маршрутизаторов Cisco, пояснить значение команд.
- Выводы.

Лабораторная работа № 6.
Настройка динамической маршрутизации с помощью протокола RIP на устройствах Cisco.

Топология сети:

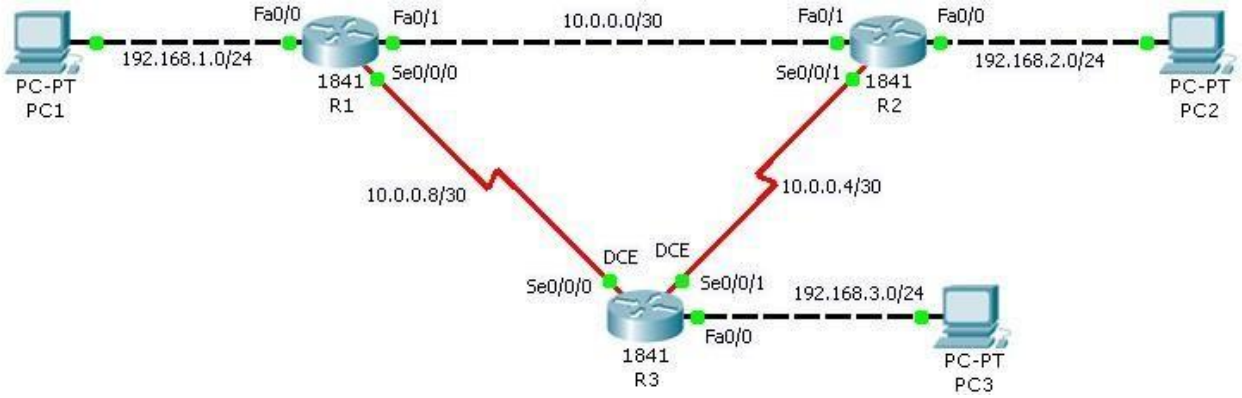

Таблица сетевых адресов.

Device	Interface	IP Address	Mask	Default Gateway
R1	**Fa0/0**	192.168.1.1	255.255.255.0	N/A
	Fa0/1	10.0.0.1	255.255.255.252	N/A
	Se0/0/0	10.0.0.9	255.255.255.252	N/A
R2	**Fa0/0**	192.168.2.1	255.255.255.0	N/A
	Fa0/1	10.0.0.2	255.255.255.252	N/A
	Se0/0/1	10.0.0.6	255.255.255.252	N/A
R3	**Fa0/0**	192.168.3.1	255.255.255.0	N/A
	Se0/0/0	10.0.0.10	255.255.255.252	N/A
	Se0/0/1	10.0.0.5	255.255.255.252	N/A
PC1	**N/A**	192.168.1.10	255.255.255.0	192.168.1.1
PC2	**N/A**	192.168.2.10	255.255.255.0	192.168.2.1
PC3	**N/A**	192.168.3.10	255.255.255.0	192.168.3.1

Цель работы.

Настроить динамическую маршрутизацию с помощью протокола RIP на устройствах R1, R2, R3. Обеспечить возможность взаимодействия конечных устройств PC1, PC2, PC3 между собой. С помощью команд

Этапы выполнения работы.

1. Откройте программу Packet Tracer и создайте схему сети**.**
2. Произведите начальную конфигурацию устройств R1, R2, R3.

Откройте эмулятор командной строки

Зайдите в режим **“privileged EXEC”.**

Router>**e**
nable
Router#

Зайдите в режим глобальной конфигурации маршрутизатора.

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

Отключите **DNS lookup.**

Router(config)#**no ip domain-lookup**
Router(config)#

Сконфигурируйте имя маршрутизатора в соответствии с названиями устройств на диаграмме.

Router(config)#**hostname** *имя_маршрутизатора*

Сконфигурируйте интерфейсы в соответствии со схемой адресации.

Router(config)#**interface** *тип_интерфейса номер_интерфейса*
Router(config-if)#**ip address** *сетевой_адрес маска_сети*
Router(config-if)#**no shutdown**
Router(config-
if)#**exit**
Router(config)
#

Для серийных интерфейсов (Serial, Se) со стороны DCE необходимо ввести команду:

Router(config-if)#**clock rate 64000**

3. Проверьте правильность начальной конфигурации устройств с помощью команд

С помощью команды **show ip interface brief,** проверьте адреса на интерфейсах настроены правильно, и что интерфейсы функционируют на физическом и канальном уровнях.

Router(config)#**exit**
R1#**show ip interface brief**

В помощью команды **show ip route** убедитесь, что каждый маршрутизатор видит все присоединённые к нему сети.

R1#**show ip route**

4. Сконфигурируйте сетевые интерфейсы конечных устройств (PC1, PC2, PC3) в соответствии со схемой адресации сети.

5. Настройте протокол RIP на маршрутизаторах R1, R2, R3

6. Проверка правильности работы протокола RIP.

Если протокол маршрутизации настроен правильно, то каждый маршрутизатор должен знать путь до каждой сети. Проверить этот факт можно с помощью команды **show ip route.**

7. Сохраните конфигурацию устройств.

Router#**copy running-config startup-config**

Destination filename [startup-config]? Building configuration...

[OK]

Router#

Лабораторная работа 7.

1. **Создание стандартного списка доступа**

Списки доступа бывают нескольких видов: стандартные, расширенные, динамические и другие. В стандартных *ACL* есть возможность задать только *IP адрес* источника пакетов для их запретов или разрешений.

На рис. 9.1 показаны две подсети: 192.168.0.0 и 10.0.0.0.

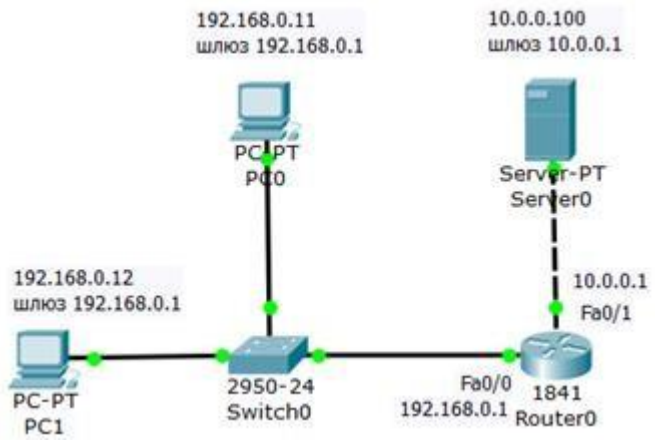

Рис. 9.1. Схема сети

Постановка задачи

Требуется разрешить доступ на сервер PC1 с адресом 192.168.0.12, а PC0 с адресом 192.168.0.11 – запретить (рис. 9.2).

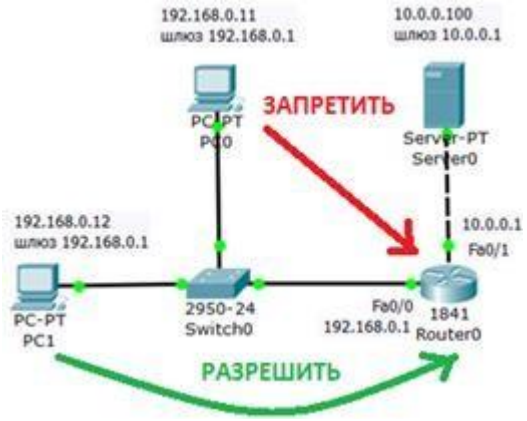

Рис. 9.2. Постановка задачи

Соберем данную схему и настроим ее. Настройку PC1 и PC2 выполните самостоятельно.

2. Расширенные списки доступа ACL

Стандартные *права* не так гибки, как хотелось бы. В отличие от стандартных списков, расширенные списки фильтруют трафик более "тонко". При создании расширенных списков в правилах доступа можно включать фильтрацию трафика по протоколам и портам. Для указания портов в правиле доступа указываются следующие обозначения ():

Таблица 9.1. Обозначение портов в ACL	
обозначение	**действие**
lt n	Все номера портов, меньшие n.
gt n	Все номера портов, большие n.
eq n	Порт n
neq n	Все порты, за исключением n.
range n m	Все порты от n до m включительно.

Расширенные списки доступа ACL

Соберите схему сети, показанную на рис. 9.10.

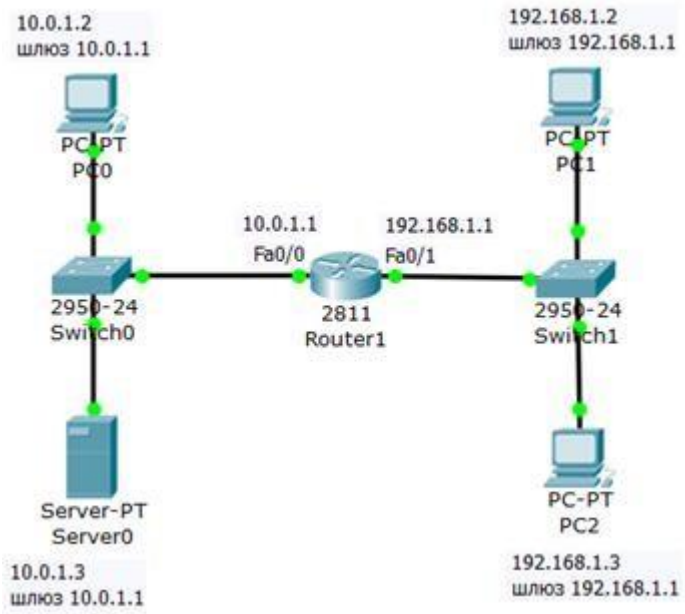

Рис. 9.10. Схема сети

Задача: разрешить *доступ* к *FTP* серверу 10.0.1.3 для узла 192.168.1.2 и запретить для узла 192.168.1.3.

Создаем расширенные списки доступа и запрещаем FTP трафик

Постановка задачи графически изображена на рис. 9.11.

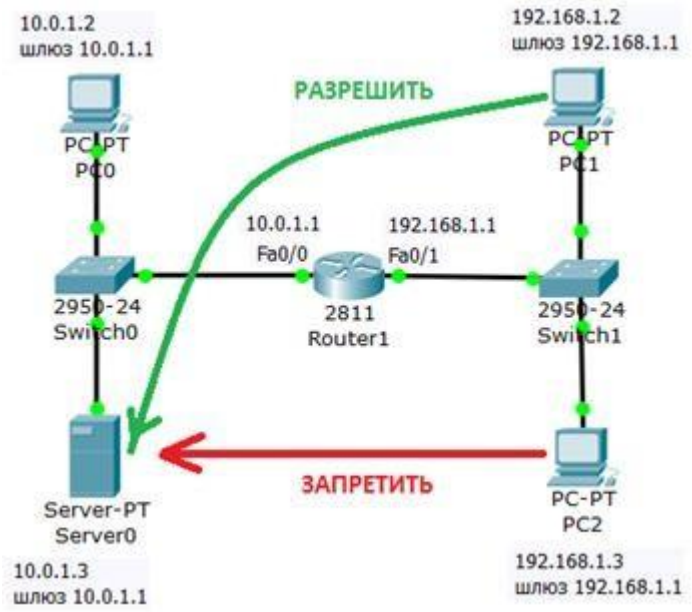

Рис. 9.11. Стрелками показана цель нашей работы

Изначально на сервере 10.0.1.3 FTP сервис поднят по умолчанию со значениями имя пользователя Cisco, пароль Cisco. Убедимся, что узел S0 доступен и FTP работает, для этого заходим на PC1 и связываемся с сервером (рис. 9.12). Выполняем какие-либо команды, например, DIR – чтение директории.

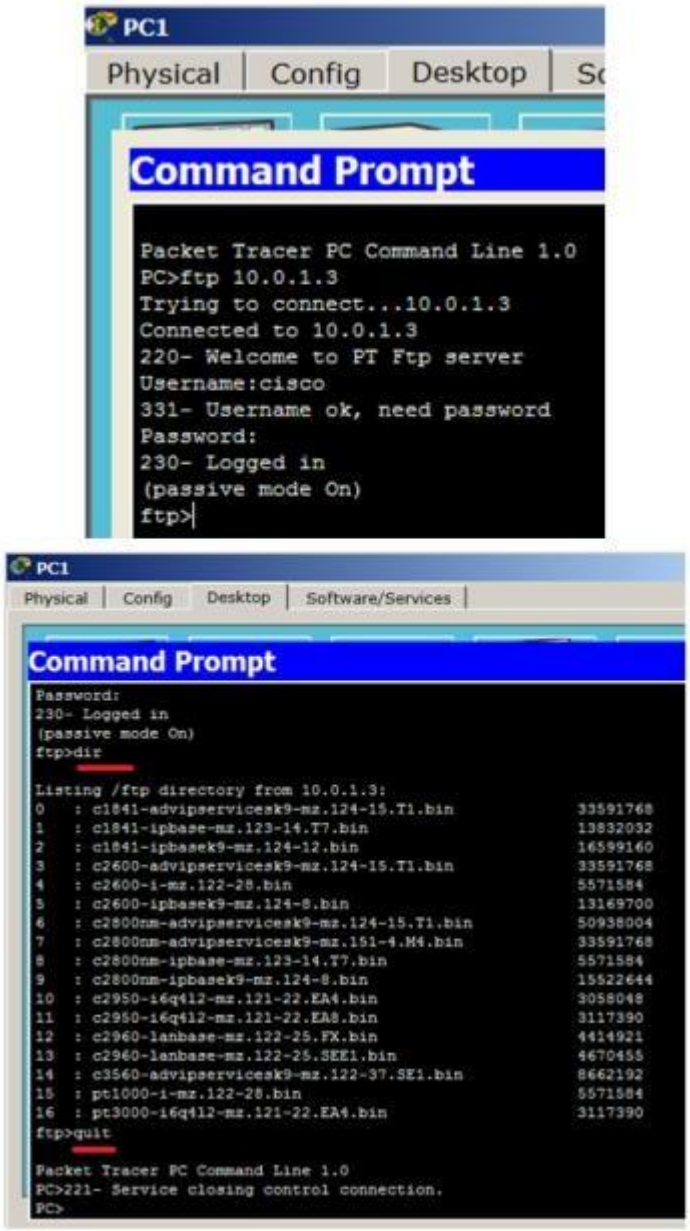

Рис. 9.12. FTPсервер доступен

Примечание

При наборе пароля на экране ничего не отображается.

Теперь создадим список правил с номером 101 в котором укажем 2 разрешающих и по 2 запрещающих правила для портов сервера 21 и 20 (Эти порты служат для FTP - передачи команд и данных) – рис. 9.13.

3. Статическая трансляция адресов NAT

На рис. 9.17 имеется внешний *адрес* 20.20.20.20 (внешний *интерфейс* fa0/1) и внутренняя *сеть* 10.10.10.0 (внутренний *интерфейс* fa0/0). Нужно настроить *NAT*. Предполагается, что адреса уже прописаны, и *сеть* поднята (рабочая).

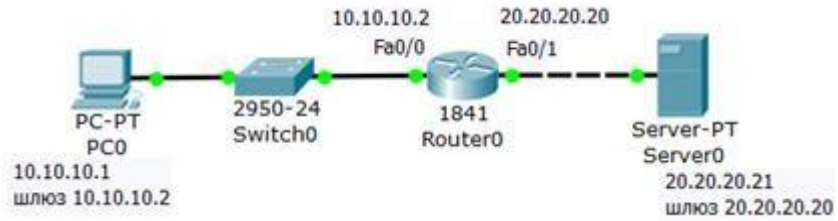

Рис. 9.17. Схема сети

На R0 добавляем access-list, разрешаем всё (any)

Разрешаем весь трафик, то есть, любой IP адрес (рис. 9.18).

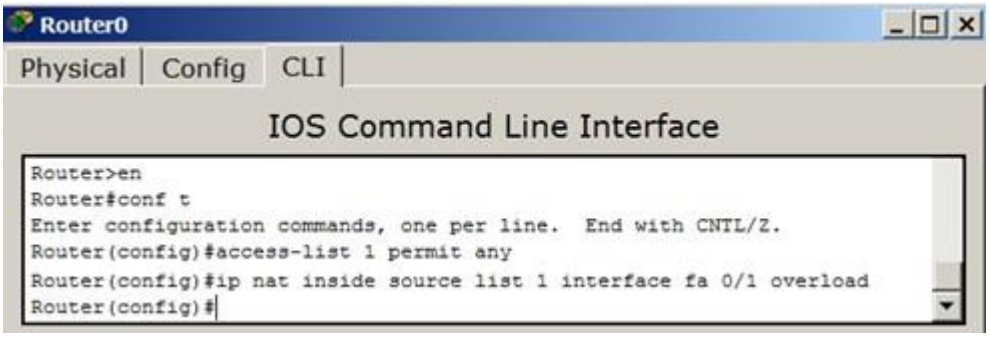

Рис. 9.18. Составляем лист допуска

Создаём правило трансляции

Теперь настроим трансляцию на интерфейсах (на внутреннем inside, на внешнем – outside), то есть, для R0 указываем внутренний и внешний порты (рис. 9.19).

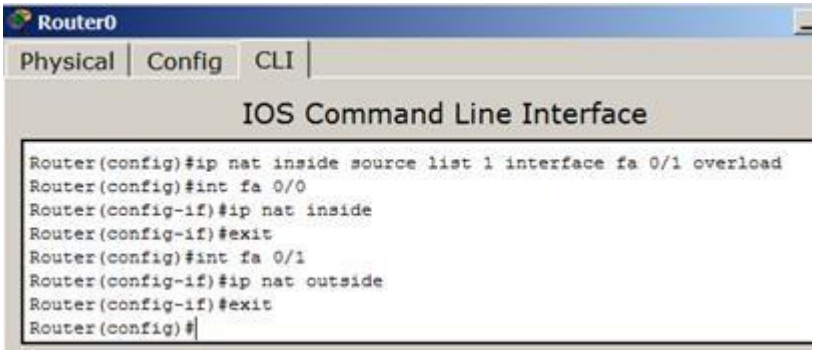

Рис. 9.19. Для R0 назначаем внутренний и внешний порты

Выходим из режима глобального конфигурирования и записываем настройки роутера в микросхему памяти (рис. 9.20).

Рис. 9.20. Сохраняем настройки в ОЗУ

Проверяем работу сети (просмотр состояния таблицы NAT)

С PC0 пингуем провайдера и убеждаемся, что PC0 и сервер могут общаться (рис. 9.21).

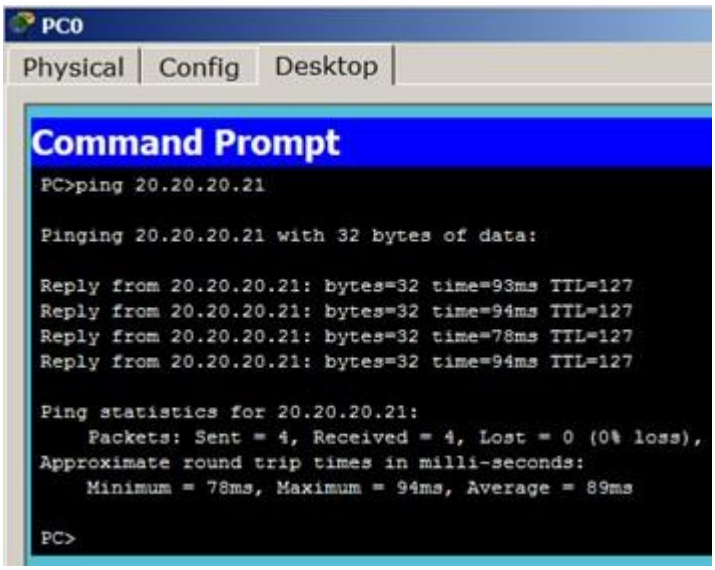

Рис. 9.21. Из внутренней сети пингуем внешнюю сеть

Для просмотра состояния таблицы NAT, одновременно с пингом используйте команду **Router#sh ip nat translations** (я запустил пинг с машины 10.10.10.1, т.е., с PC0 на адрес 20.20.20.21, т.е., на S0) – рис. 9.22.

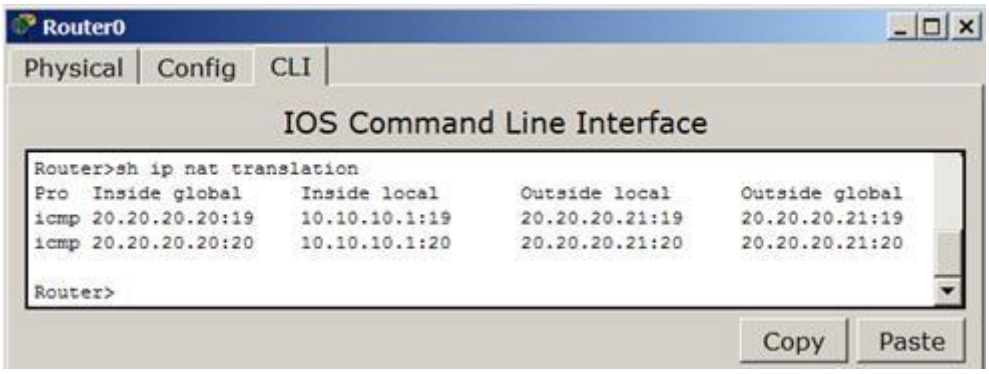

Рис. 9.22. Вовремя пинга просматриваем состояние таблицы NAT

Убеждаемся в успешной маршрутизации в режиме симуляции (рис. 9.23).

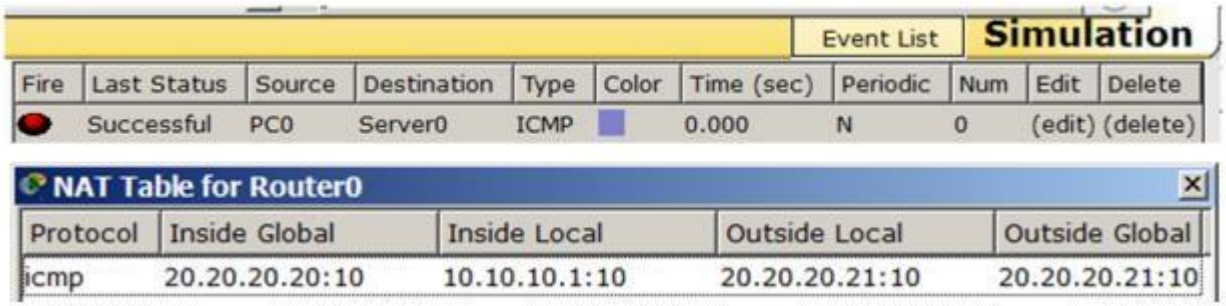

Рис. 9.23. Связь PC0 и S0 работает

Лабораторная работа №8. Протоколы SMTP и POP3

Цель работы: изучить принципы организации взаимодействия прикладных программ с помощью протоколов электронной почты SMTP и POP3 в режиме симуляции Cisco Packet Tracer.

Программа работы:

1. Построение топологии сети, настройка сетевых устройств;
2. Настройка почтового сервера;
3. Исследование прикладных почтовых протоколов в режиме симуляции;
4. Отправка письма по протоколу SMTP на сервер;
5. Получение письма по протоколу POP3 от сервера;
6. Выполнение индивидуального задания.

Теоретические сведения:

Протоколы SMTP и POP3

Схема взаимодействия с прикладными почтовыми протоколами представлена на рис. 4.83.

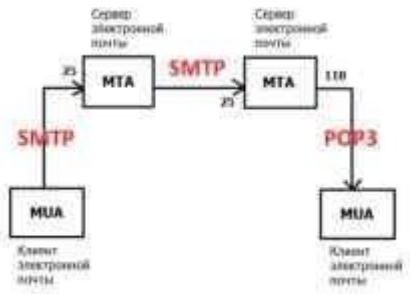

Рис. 4.83 Схема взаимодействия с прикладными почтовыми протоколами

Mail Transfer Agent (MTA) – агент передачи почты, являющийся основным компонентом системы передачи почты, представляет данный компьютер для сетевой системы электронной почты. Обычно пользователи не работают непосредственно с MTA, а используют Mail User Agent (MUA) – клиент электронной почты.

Для передачи сообщений по TCP-соединению большинство почтовых

агентов пользуются протоколом Simple Mail Transfer Protocol (SMTP).

SMTP принят в качестве стандартного метода передачи электронной почты в сети Internet. Действующий стандарт протокола описан в RFC 2821. В качестве транспортного протокола SMTP использует TCP, соединение устанавливается через порт с номером 25. Для обслуживания этого соединения используется специальная программа, которая именуется почтовым сервером. Для формирования сообщения и установления соединения используется почтовая программа пользователя. После установления соединения обмен информацией происходит посредством команд. Для пользователя эти команды не доступны, если при работе он использует клиент электронной почты [5].

Главной целью протокола SMTP является надежная и эффективная доставка электронных почтовых сообщений. Для реализации протокола требуется только надежный канал связи. Средой для SMTP может служить отдельная локальная сеть, система сетей или же всемирная сеть Internet.

Эта передача обычно осуществляется непосредственно с хоста отправителя на хост получателя, когда оба хоста используют один транспортный сервис. Если же хосты не подключены к общей транспортной системе, передача осуществляется с использованием одного или нескольких промежуточных серверов SMTP. Сегодня в Internet обычной практикой является представление исходного сообщения промежуточному серверу, который выполняет некоторые дополнительные функции. Промежуточный сервер в таких случаях действует как шлюз в другие среды передачи и выбирается обычно с использованием MX-записей DNS (служба доменных имен).

Протокол SMTP базируется на следующей модели коммуникаций: в ответ на запрос пользователя почтовая программа-отправитель сообщения устанавливает двустороннюю связь с программой-приемником (почтовым сервером). Получателем может быть оконечный или промежуточный адресат. Если необходимо, почтовый сервер может установить соединение с другим

сервером и передать сообщение дальше.

Для того чтобы получить сообщение из своего почтового ящика, почтовая программа пользователя соединяется с сервером уже не по протоколу SMTP, а по специальному почтовому протоколу получения сообщений. Такой протокол позволяет работать с почтовым ящиком: забирать сообщения, удалять сообщения, сортировать их и выполнять другие операции. Самым популярным в настоящее время протоколом такого рода является протокол Post Office Protocol v.3 (POP3).

Многие концепции, принципы и понятия протокола POP3 выглядят и функционируют подобно SMTP: взаимодействие происходит посредством команд. Сервер POP3 находится между агентом пользователя и почтовыми ящиками.

Он предусматривает соединение с почтовым сервером на основе транспортного протокола TCP через порт 110. Спецификация POP3 определена в документе RFC 1939. POP3 разработан с учетом специфики доставки почты на персональные компьютеры и имеет соответствующие операции для этого [6].

Конструкция протокола POP3 обеспечивает возможность пользователю обратиться к своему почтовому серверу и изъять накопившуюся для него почту. Пользователь может получить доступ к POP3-серверу из любой точки доступа к Internet. При этом он должен запустить специальный почтовый агент, работающий по протоколу POP3, и настроить его для работы со своим почтовым сервером. Сообщения доставляются клиенту по протоколу POP3, а посылаются при помощи SMTP. То есть на компьютере пользователя существуют два отдельных агента-интерфейса к почтовой системе – доставки (POP3) и отправки (SMTP).

Служба DNS

Данная лабораторная работа посвящена изучению прикладных протоколов электронной почты SMTP и POP3. Однако взаимодействие с системой электронной почты невозможно без системы доменных имен

(DNS). В задачи службы DNS входит:

1. Преобразование символических имен в IP-адреса;

2. Преобразование IP-адресов в символические имена.

Дополнительной функцией DNS является маршрутизация почты. Основная спецификация распределенной службы DNS указана в RFC 1034 и RFC 1035.

Единицами хранения и передачи информации в DNS являются ресурсные записи. Существует множество типов ресурсных записей, каждая из которых состоит из определенного числа полей. Для маршрутизации почты используется запись “MX”, при ее отсутствии запись типа “A”. Запись “A” (адресная запись) содержит параметры: доменное имя узла, соответствующий IP-адрес.

Пример: aivt IN A 195.19.212.16, где “IN” – это класс записи (интернет).

Запись “MX” содержит параметры: имя почтового домена, имя почтового сервера, приоритет.

Пример: aivt IN MX 20 mail.stu.neva.ru, где “IN” – это класс записи (интернет). [4]

При получении письма MTA анализирует его служебную информацию, в частности заголовок письма, определяя домен получателя (см. рис. 4.83). Если он относится к домену, который обслуживается данным MTA, производится поиск получателя и письмо помещается в его ящик.Если домен получателя не обслуживается этим MTA, формируется DNS-запрос, запрашивающий MX-записи для данного домена. MX-запись представляет особый вид DNS-записи, которая содержит имена почтовых серверов, обрабатывающих входящую почту для данного домена. MX-записей может быть несколько, в этом случае MTA пробует последовательно установить соединение, начиная с сервера с наибольшим приоритетом. При отсутствии MX-записи запрашивается A-запись (запись адреса, сопоставляющая доменное имя с IP-адресом) и выполняется попытка доставить почту на указанный там хост. При невозможности отправить сообщение, оно

возвращается отправителю (помещается в почтовый ящик пользователя) с сообщением об ошибке. [8]

Выполнение работы:

1. Построение топологии сети

Для исследования заданных прикладных протоколов построим тестовую топологию сети следующего вида (рис. 4.84):

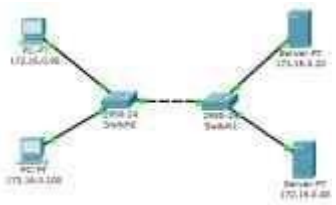

Рис. 4.84 Тестовая топология сети

Производим настройку сетевых устройств согласно заданным параметрам (таблица 4.4, таблица 4.5):

Таблица 4.4

Конечные узлы	IP-адрес	Маска сети	IP-адрес DNS-сервера
PC0	172.16.0.90	255.255.0.0	172.16.0.20
PC1	172.16.0.100	255.255.0.0	172.16.0.20

Таблица 4.5

Серверы	IP-адрес	Маска сети	IP-адрес DNS-сервера
Server0	172.16.0.20	255.255.0.0	172.16.0.20
Server1	172.16.0.40	255.255.0.0	172.16.0.20

Все устройства расположены в одном сегменте локальной сети, поэтому маршрутизация пакетов не используется, значит, IP-адрес шлюза по умолчанию указывать необязательно.

2. Настройка почтового сервера

В качестве серверов электронной почты выступают сервер 172.16.0.20 и сервер 172.16.0.40. Схема взаимодействия с прикладными почтовыми протоколами применительно к построенной сети представлена на рис. 4.85:

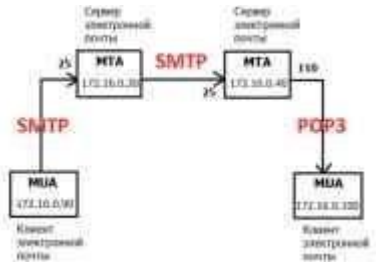

Рис. 4.85 Схема взаимодействия с прикладными почтовыми протоколами в исследуемой сети

На каждом из MTA будет поддерживаться smtp- и pop3-сервер. Подключиться к серверу может любой зарегистрированный пользователь. Чтобы отправить письмо, пользователь на сервере проходит авторизацию, после чего сервер готов отправлять письма от имени пользователя. По адресу назначения письма сервер определяет, кому следует передать его дальше. Нужный адрес сервер определяет с помощью службы DNS, в которой

содержится соответствующая ресурсная адресная запись, преобразовывающая имя домена в IP-адрес.

Подключим службу DNS на сервере 172.16.0.20:

1) Один клик по выбранному устройству.

2) Выбираем вкладку Config, Services -> DNS (рис. 4.86). Заносим данные о новой ресурсной записи: имя домена, IP-адрес, тип ресурсной записи. Симулятор не поддерживает ресурсную запись, предназначенную для почтовых серверов, MX, но ее можно заменить адресной (тип A).

Рис. 4.86 Настройка службы DNS на сервере

3) Нажимаем на кнопку “Add” будет добавлена новая запись в службу DNS (рис. 4.87).

Рис. 4.87 Настройка службы DNS на сервере

Повторим предыдущие действия и добавим еще одну ресурсную запись о почтовом сервере 172.16.0.40 (рис. 4.88).

Рис. 4.88 Настройка службы DNS на сервере

Теперь сконфигурируем почтовый сервер 172.16.0.20 с поддержкой smtp- и pop3-сервера:

1) Один клик по выбранному устройству.
2) Выбираем вкладку “Config”, Services -> EMAIL
3) Подключаем протоколы SMTP и POP3 и вводим имя домена электронной почты. Нажимаем кнопку “Set” (рис. 4.89).

Рис. 4.89 Конфигурация smtp- и pop3-сервера

4) Создадим учетную запись для одного пользователя, вводим логин и пароль. Занести запись в службу можно с помощью кнопки “+” (рис. 4.90).

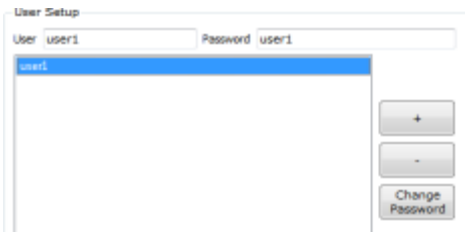

Рис. 4.90 Создание учетной записи

Smtp-сервер и pop3-сервер на машине 172.16.0.20 сконфигурированы, имеют одного зарегистрированного пользователя. Так же на нем

поддерживается служба DNS, в которой есть две ресурсных записи.

На сервере 172.16.0.40 так же необходимо настроить почтовый сервер с поддержкой SMTP и POP3 (рис. 4.91). В качестве DNS для него выступает сервер 172.16.0.20.

1) Один клик по выбранному устройству.

2) Выбираем вкладку “Config”, Services -> EMAIL

3) Подключаем протоколы SMTP и POP3 и вводим имя домена электронной почты - mail.ru. Нажимаем кнопку “Set”.

4) Создадим учетную запись для одного пользователя, вводим логин и пароль. Занести запись в службу можно с помощью кнопки “+”.

Рис. 4.91 Конфигурация smtp- и pop3-сервера

3. Настройка почтовой службы на конечных узлах

Для работы с почтовым smtp- или pop3-сервером на компьютере пользователя должен быть настроен клиент электронной почты, который и будет взаимодействовать с сервером (см. рис. 4.83).

Настроим на хосте 172.16.0.90 клиент электронной почты (рис. 4.92):

1) Один клик на хосте с IP-адресом 172.16.0.90.

2) Выбираем вкладку Desktop, программу “E-mail”. Появится окно конфигурации почтового сервиса. Вводим пользовательские данные в форму.

Рис. 4.92 Настройка клиента электронной почты

Нажимаем кнопку “Save”, закрываем окно, конфигурация клиента электронной почты завершена. Теперь для пользователя user1 доступен почтовый сервис в домене server.ru: отправка и получение писем.

Настроим почтовый сервис и на хосте 172.16.0.100, выполнив предыдущие действия (рис. 4.93). Вводим следующие пользовательские данные:

Теперь для пользователя user2 доступен почтовый сервис в домене mail.ru: отправка и получение писем.

Настройка всех устройств и необходимых служб завершена.

4. Исследование прикладных почтовых протоколов в режиме симуляции

Рис. 4.93 Настройка клиента электронной почты

Переходим в режим симуляции Cisco Packet Tracer. Добавляем фильтры на 2 протокола: SMTP и POP3 (рис. 4.94). Это значит, что пакеты только фильтруемых протоколов будут отображаться в сети.

Рис. 4.94 Окно событий режима симуляции

Отправим письмо с хоста 172.16.0.90 от user1 на хост 172.16.0.100 user2 (рис. 4.95):

1) Один клик по выбранному узлу (172.16.0.90).

2) Выбираем на вкладке “Desktop” программу “E-mail”.

3) Чтобы написать и отправить письмо, нажимаем на кнопку “Compose”. Появится форма, которую следует заполнить. В поле “To” задается адрес электронной почты, кому вы отправляете письмо. Поле “Subject” содержит заголовок письма. Текст письма можете сочинить самостоятельно.

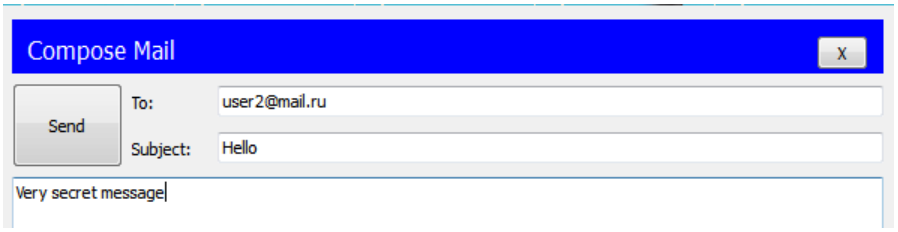

Рис. 4.95 Форма для отправления письма

Нажимаем на кнопку “Send”, начнется отправление письма.

Видим, что на хосте 172.16.0.90 сформировался пакет SMTP (рис. 4.96). Воспользовавшись кнопкой “Capture/Forward”, проследим за маршрутом пакета от устройства к устройству.

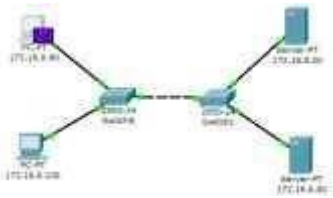

Рис. 4.96 Вид рабочей области

Посмотрим содержимое пакета, сформированного на узле (рис. 4.97).

Рис. 4.97 Формат пакета SMTP

Пакет адресован почтовому серверу по IP-адресу 172.16.0.20. В заголовке TCP содержится порт назначения – 25. Можно сделать вывод, что пакет сформирован верно. Пакет на пути своего следования к серверу проходит через два коммутатора (рис. 4.98). Убедитесь, что это так.

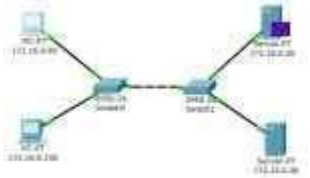

Рис. 4.98 Вид рабочей области

Когда пакет приходит на сервер, тот, обрабатывая его, определяет, что письмо адресовано домену mail.ru. Сервер 172.16.0.20 обращается к службе DNS за IP-адресом заданного сервера. По указанному адресу письмо перенаправляется на соответствующий почтовый сервер (рис. 4.99).

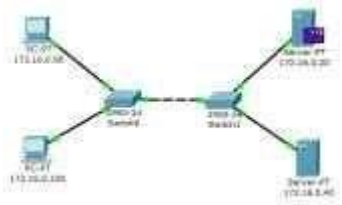

Рис. 4.99 Вид рабочей области

SMTP-пакет, сформированный сервером 172.16.0.20, содержит следующую информацию: IP-адрес назначения – 172.16.0.40, порт назначения – 25 (рис. 4.100).

Рис. 4.100 Формат пакета SMTP

Пакет проходит через коммутатор Switch1 и доставляется серверу 172.16.0.40 (рис. 4.101).

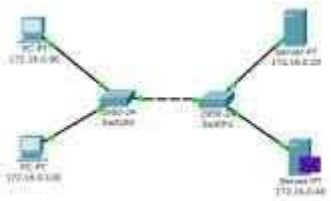

Рис. 4.101 Вид рабочей области

На сервере 172.16.0.40 формируется SMTP-ответ серверу 172.16.0.20 и отправляется на указанный адрес (рис. 4.102).

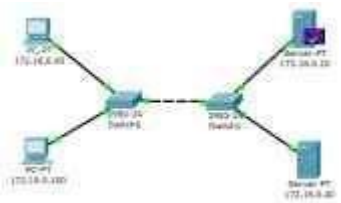

Рис. 4.102 Вид рабочей области

Из содержимого пакета, пришедшего обратно на сервер 172.16.0.20: IP-адрес источника – 172.16.0.40, порт источника – 25 (рис. 4.103).

С помощью протокола SMTP мы отправили письмо на сервер mail.ru, теперь оно хранится там.

Наш адресат (узел 172.16.0.100) еще не получил отправленное письмо, так как на сервер он еще не обратился по протоколу POP3. Для получения письма необходимо проделать следующие действия:

Рис. 4.103 Формат пакета SMTP

1) Один клик по узлу 172.16.0.100.
2) Выбираем на вкладке “Desktop” программу “E-mail”.
3) Нажимаем на кнопку “Receive”, чтобы прочитать письмо.

На хосте формируется пакет протокола POP3 (рис. 4.104). Воспользовавшись кнопкой “Capture/Forward”, проследим за маршрутом пакета от устройства к устройству.

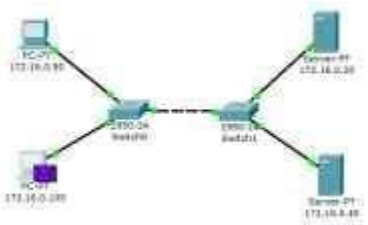

Рис. 4.104 Вид рабочей области

Посмотрим содержимое пакета, сформированного на узле (рис. 4.105).

Рис. 4.105 Формат пакета POP3

Пакет адресован почтовому серверу по IP-адресу 172.16.0.40. В заголовке TCP содержится порт назначения – 110. Можно сделать вывод, что пакет сформирован верно. Пакет на пути своего следования к серверу проходит через два коммутатора. Убедитесь, что это так. Когда пакет приходит на сервер, тот обрабатывает его и формирует пакет-ответ (рис. 4.106).

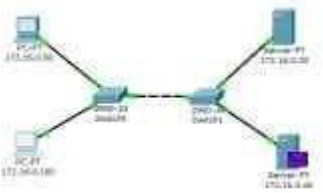

Рис. 4.106 Вид рабочей области

Пакет по тому же маршруту возвращается на узел 172.16.0.100 с ответом (письмом) от сервера. Посмотрим содержимое ответа (рис. 4.107).

Рис. 4.107 Формат пакета POP3

Порт-источник – 110. Ответ пришел от сервера 172.16.0.40 с некоторыми POP3-данными. С помощью протокола POP3 узел 172.16.0.100 получил письмо с сервера, отправленное туда узлом 172.16.0.90 (рис. 4.108).

Рис. 4.108 Форма чтения входящих писем

Как уже упоминалось в теоретических сведениях, почтовые протоколы SMTP и POP3 обмениваются информацией с помощью команд. Клиенту электронной почты, чтобы установить соединение с сервером, отправить письмо, разорвать соединение необходимо отправлять серверу соответствующие команды. Сервер электронной почты, в свою очередь, обрабатывает эти команды и формирует отклики для клиента. Отклики smtp-сервера содержат цифровой код ответа: успешно или с ошибкой обработана команда. Отклики pop3-сервера так же содержат два типа сообщений: успех или ошибка.

Обращая внимание на содержимое пакета SMTP или POP3 протокола, видно, что на прикладном уровне пакет детально не рассматривается.

Пример приведен на рис. 4.109.

Рис. 4.109 Данные прикладного уровня

Поэтому эксперимент посылки письма несуществующему пользователю не является содержательным, т.к. подробно увидеть ответ от smtp-сервера нам не удастся. Для подробного изучения взаимодействия между клиентом и smtp- или pop3-сервером следует обратиться к предложенной спецификации RFC 2821 и RFC 1939.

5. Индивидуальные задания

Исследуйте прикладные протоколы электронной почты SMTP и POP3 самостоятельно. Топологию сети для исследования оставьте прежней. Настройку сетевых устройств проделайте в соответствии с вариантом.

В отчете приведите маршруты пакетов, их содержимое и объясните полученные результаты. Отправителя и получателя определите сами.

Варианты заданий представлены в приложении 2.

ПРИЛОЖЕНИЕ 2

Варианты индивидуальных заданий к лабораторной работе №5 (таблица 1):

Таблица 1

Вариант 1			
Конечные узлы	IP-адрес	Маска сети	IP-адрес DNS-сервера
PC0	172.16.1.90	255.255.0.0	172.16.1.20
PC1	172.16.1.100	255.255.0.0	172.16.1.20
Серверы			
Server0	172.16.1.20	255.255.0.0	172.16.1.20
Server1	172.16.1.60	255.255.0.0	172.16.1.20
Вариант 2			
Конечные узлы	IP-адрес	Маска сети	IP-адрес DNS-сервера
PC0	172.16.0.12	255.255.0.0	172.16.0.50
PC1	172.16.0.13	255.255.0.0	172.16.0.50
Серверы			
Server0	172.16.0.50	255.255.0.0	172.16.0.50
Server1	172.16.0.10	255.255.0.0	172.16.0.50
Вариант 3			
Конечные узлы	IP-адрес	Маска сети	IP-адрес DNS-сервера
PC0	192.168.3.1	255.255.255.0	192.168.3.8
PC1	192.168.3.3	255.255.255.0	192.168.3.8
Серверы			
Server0	192.168.3.8	255.255.255.0	192.168.3.8
Server1	192.168.3.5	255.255.255.0	192.168.3.8
Вариант 4			
Конечные узлы	IP-адрес	Маска сети	IP-адрес DNS-сервера
PC0	172.16.2.90	255.255.0.0	172.16.2.25
PC1	172.16.2.10	255.255.0.0	172.16.2.25
Серверы			
Server0	172.16.2.25	255.255.0.0	172.16.2.25
Server1	172.16.2.40	255.255.0.0	172.16.2.25
Вариант 5			
Конечные узлы	IP-адрес	Маска сети	IP-адрес DNS-сервера
PC0	192.168.5.1	255.255.255.0	192.168.5.7
PC1	192.168.5.3	255.255.255.0	192.168.5.7
Серверы			
Server0	192.168.5.7	255.255.255.0	192.168.5.7
Server1	192.168.5.5	255.255.255.0	192.168.5.7

Вариант 6			
Конечные узлы	IP-адрес	Маска сети	IP-адрес DNS-сервера
PC0	192.168.4.1	255.255.255.0	192.168.4.9
PC1	192.168.4.3	255.255.255.0	192.168.4.9
Сервер			
Server0	192.168.4.9	255.255.255.0	192.168.4.9
Server1	192.168.4.6	255.255.255.0	192.168.4.9
Вариант 7			
Конечные узлы	IP-адрес	Маска сети	IP-адрес DNS-сервера
PC0	172.16.3.15	255.255.0.0	172.16.3.70
PC1	172.16.3.25	255.255.0.0	172.16.3.70
Серверы			
Server0	172.16.3.70	255.255.0.0	172.16.3.70
Server1	172.16.3.40	255.255.0.0	172.16.3.70
Вариант 8			
Конечные узлы	IP-адрес	Маска сети	IP-адрес DNS-сервера
PC0	172.16.4.90	255.255.0.0	172.16.4.30
PC1	172.16.4.10	255.255.0.0	172.16.4.30
Серверы			
Server0	172.16.4.30	255.255.0.0	172.16.4.30
Server1	172.16.4.100	255.255.0.0	172.16.4.30
Вариант 9			
Конечные узлы	IP-адрес	Маска сети	IP-адрес DNS-сервера
PC0	172.16.5.20	255.255.0.0	172.16.5.10
PC1	172.16.5.40	255.255.0.0	172.16.5.10
Серверы			
Server0	172.16.5.10	255.255.0.0	172.16.5.10
Server1	172.16.5.80	255.255.0.0	172.16.5.10
Вариант 10			
Конечные узлы	IP-адрес	Маска сети	IP-адрес DNS-сервера
PC0	172.16.6.20	255.255.0.0	172.16.6.40
PC1	172.16.6.10	255.255.0.0	172.16.6.40
Серверы			
Server0	172.16.6.40	255.255.0.0	172.16.6.40
Server1	172.16.6.30	255.255.0.0	172.16.6.40
Вариант 11			
Конечные узлы	IP-адрес	Маска сети	IP-адрес DNS-сервера
PC0	192.168.6.2	255.255.255.0	192.168.6.7
PC1	192.168.6.3	255.255.255.0	192.168.6.7
Серверы			
Server0	192.168.6.7	255.255.255.0	192.168.6.7

Server1	192.168.6.5	255.255.255.0	192.168.6.7
Вариант 12			
Конечные узлы	IP-адрес	Маска сети	IP-адрес DNS-сервера
PC0	192.168.7.2	255.255.255.0	192.168.7.5
PC1	192.168.7.4	255.255.255.0	192.168.7.5
Серверы			
Server0	192.168.7.5	255.255.255.0	192.168.7.5
Server1	192.168.7.8	255.255.255.0	192.168.7.5
Вариант 13			
Конечные узлы	IP-адрес	Маска сети	IP-адрес DNS-сервера
PC0	192.168.8.4	255.255.255.0	192.168.8.2
PC1	192.168.8.3	255.255.255.0	192.168.8.2
Серверы			
Server0	192.168.8.2	255.255.255.0	192.168.8.2
Server1	192.168.8.8	255.255.255.0	192.168.8.2
Вариант 14			
Конечные узлы	IP-адрес	Маска сети	IP-адрес DNS-сервера
PC0	192.168.9.3	255.255.255.0	192.168.9.6
PC1	192.168.9.4	255.255.255.0	192.168.9.6
Серверы			
Server0	192.168.9.6	255.255.255.0	192.168.9.6
Server1	192.168.9.7	255.255.255.0	192.168.9.6

Литература

1. Сысоев, Э. В. Администрирование компьютерных сетей : учебное пособие / Э. В. Сысоев, А. В. Терехов, Е. В. Бурцева. – Тамбов : Тамбовский государственный технический университет (ТГТУ), 2017. – 80 с. : ил. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=499414 (дата обращения: 15.05.2024). – Библиогр. в кн. – ISBN 978-5-8265-1802-1. – Текст : электронный.
2. Павлюк, В. Д. Типовые топологии вычислительных сетей / В. Д. Павлюк. – Москва : Лаборатория книги, 2011. – 105 с. : ил., табл., схем. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=142528 (дата обращения: 15.05.2024). – ISBN 978-5-504-00899-8. – Текст : электронный.
3. Терехов, А. В. ИТ- инфраструктура организации : учебное пособие / А. В. Терехов, В. Н. Чернышов, И. П. Рак ; Тамбовский государственный технический университет. – Тамбов : Тамбовский государственный технический университет (ТГТУ), 2017. – 97 с. : ил. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=499420 (дата обращения: 15.05.2024). – Библиогр.: с. 88-94. – ISBN 978-5-8265-1844-1. – Текст : электронный.
4. Горбунов, А. В. Проектирование защищённых оптических телекоммуникационных систем : учебное пособие : [16+] / А. В. Горбунов, Ю. В. Зачиняев, А. П. Плёнкин. – Ростов-на-Дону ; Таганрог : Южный федеральный университет, 2019. – 128 с. : ил., табл., схем. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=598665 (дата обращения: 15.05.2024). – Библиогр.: с. 116 - 120. – ISBN 978-5-9275-3431-9. – Текст : электронный.
5. Киренберг, А. Г. Системное администрирование и информационная безопасность сетей ЭВМ : учебное пособие / А. Г. Киренберг. — Кемерово : Кузбасский государственный технический университет имени Т.Ф. Горбачева, 2022. — 119 с. — ISBN 978-5-00137-292-9. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/128406.html (дата обращения: 15.05.2024). — Режим доступа: для авторизир. пользователей
6. Ларина, Т. Б. Администрирование сетей. Защита ресурсов и мониторинг : учебное пособие / Т. Б. Ларина. — Москва : Российский университет транспорта (МИИТ), 2018. — 92 с. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/116018.html (дата обращения: 15.05.2024). — Режим доступа: для авторизир. пользователей
7. Защита персональных данных : учебное пособие / О. М. Голембиовская, М. Ю. Рытов, Ю. Ю. Громов [и др.]. — Москва : Ай Пи Ар Медиа, 2024. — 156 с. — ISBN 978-5-4497-2644-5. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/135611.html (дата обращения: 15.05.2024). — Режим доступа: для авторизир. пользователей