Министерство науки и высшего образования РФ
ФГБОУ ВО «Ульяновский государственный университет»
Факультет математики, информационных и авиационных технологий
Кафедра телекоммуникационных технологий и сетей

Курилова Оксана Леонидовна

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ

для лабораторных работ по дисциплине

«Инфокоммуникационные системы и сети»
для студентов направлений
09.03.02 «Информационные системы и технологии»
«Основы сетевых технологий в инфокоммуникационных системах и сервисах»
11.03.02 «Инфокоммуникационные технологии и системы связи»
«Информационные сети»
для студентов направлений
09.03.03 «Информационная сфера»
02.03.03 «Технология программирования»
«Компьютерные сети передачи данных»
11.04.02 «Инфокоммуникационные технологии и системы связи»
«Компьютерные сети»
10.05.01 «Компьютерная безопасность»
10.05.03 «Информационная безопасность автоматизированных систем»

Ульяновск

2023

Методические рекомендации для лабораторных работ по дисциплине «Инфокоммуникационные системы и сети», «Информационные сети» / составитель: О.Л. Курилова - Ульяновск: УлГУ, 2023 – 86 с.

Настоящие методические рекомендации предназначены для студентов направлений обучения 09.03.02 «Информационные системы и технологии», 09.03.03 «Информационная сфера», 02.03.03 «Технология программирования», 11.03.02 «Инфокоммуникационные технологии и системы связи», 11.04.02 «Инфокоммуникационные технологии и системы связи», 10.05.01 «Компьютерная безопасность», 10.05.03 «Информационная безопасность автоматизированных систем». Пособие является руководством к лабораторному практикуму по дисциплине «Инфокоммуникационные системы и сети», «Информационные сети», «Компьютерные сети передачи данных», «Основы сетевых технологий в инфокоммуникационных системах и сервисах», «Компьютерные сети».

Также лабораторный практикум будет интересен и полезен для студентов вузов, обучающихся по специальностям в области информационных технологий и сетей, преподавателям и специалистам в области построения компьютерных сетей.

Рекомендованы к введению в образовательный процесс

Учёным советом факультета математики, информационных и авиационных технологий УлГУ

протокол № **3/23** от «18» апреля 2023 г.

Содержание

Введение

В настоящее время компьютерные сети являются ключевой составляющей современных информационно-телекоммуникационных систем. Лабораторный практикум позволит наиболее глубоко и подробно изучить возможности современных сетевых технологий, протоколов и маршрутизаторов.

Целью лабораторного практикума является формирование у студентов системы знаний по общей теории инфокоммуникационных систем и сетей с учетом тенденций современного развития.

Изучение лабораторного практикума базируется на успешно усвоенных базовых понятиях дисциплин математического и естественно-научного цикла и дисциплин профессионального цикла: «Информатика», «Операционные системы и среды», «Архитектура информационных систем».

Описание каждой лабораторной работы включает: название, цель, краткие теоретические сведения, постановку задачи, последовательность действий исполнителя, а также вопросы и задания для самостоятельных исследований.

Лабораторный практикум подготовлен на кафедре «Телекоммуникационных технологий и сетей».

Лабораторная работа №1. «Введение в программу Cisco Packet Tracer (CPT)»

Цель работы: Знакомство с программой Cisco Packet Tracer, создание топологии, назначение компьютерам адресов, пингование компьютеров.

Теоретическая часть.

Cisco Packet Tracer – это эмулятор сети, созданный компанией Cisco. Программа позволяет строить и анализировать сети на разнообразном оборудовании в произвольных топологиях с поддержкой разных протоколов. В ней вы получаете возможность изучать работу различных сетевых устройств: маршрутизаторов, коммутаторов, точек беспроводного доступа, персональных компьютеров, сетевых принтеров и т.д. Данное приложение является наиболее простым и эффективным среди своих конкурентов. Так, например, создание нового проекта сети в Cisco Packet Tracer занимает существенно меньше времени, чем в аналогичной программе - GNS3, Packet Tracer проще в установке и настройке. Курс построен на изучении версии программы Cisco Packet Tracer 6.1.1. Поэтому примеры курса следует выполнять в этой версии программы или более поздней. Cisco Packet Tracer это то, с чего стоит начинать изучать оборудование Cisco (рис. 1).

Рис. 1 *Логотип программы CPT*

Интерфейс программы Cisco Packet Tracer

На рис.2 представлен интерфейс (главное окно) программы Cisco Packet Tracer.

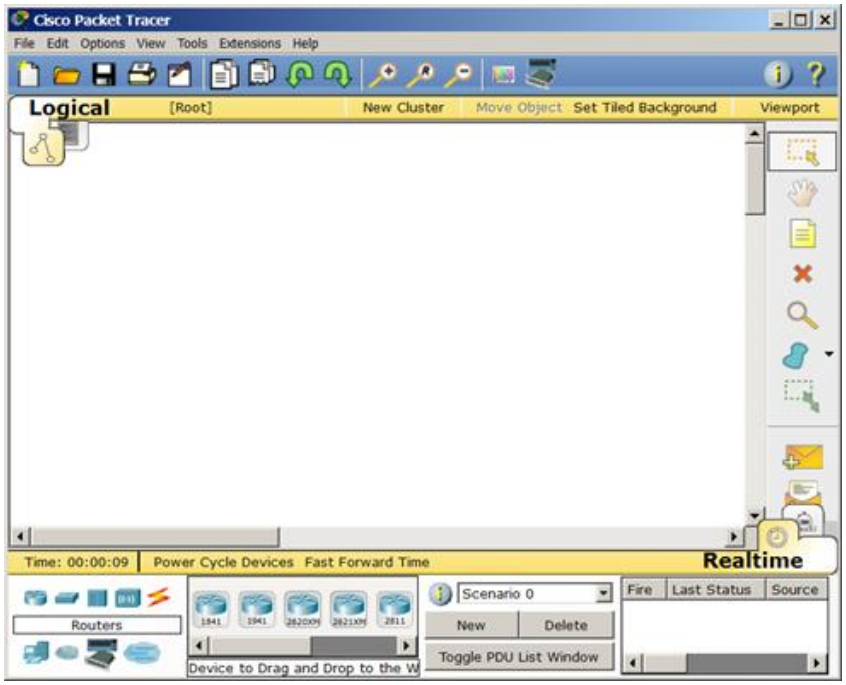


Рис. 2 *Интерфейс программы Cisco Packet Tracer (CPT)*

Главное меню показано на рис.3.

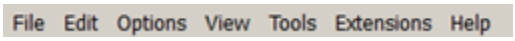


Рис. 3 *Главное меню*

File (Файл) - содержит операции открытия/сохранения документов.

Edit (Правка) - содержит стандартные операции "копировать/вырезать, отменить/повторить".

Options (Настройки) – содержит настройки программы. В частности, здесь расположена кнопка Change Language, позволяющая изменять интерфейс программы на другие языки.

View (Вид) - содержит инструменты изменения масштаба рабочей области и панели инструментов;

Tools (Инструменты) - содержит цветовую палитру и окно пользовательских устройств;

Exensions (Расширения) - содержит мастер проектов и ряд других инструментов;

Help (Помощь)–содержит помощь по программе.

Панель инструментов приведена на рис. 4.

Рис. 4. *Панель инструментов*

Оборудование

Снизу, под рабочей областью, расположена панель оборудования. Данная панель содержит в своей левой части типы (классы) устройств, а в правой части – их наименование (модели). При наведении на каждое из устройств, в прямоугольнике, находящемся в центре между ними будет отображаться его тип. Типы оборудования представлены на рис.5.

Рис. 5 *Панель оборудования Packet Tracer (Основные типы оборудования)*

Маршрутизаторы (роутеры) используется для поиска оптимального маршрута передачи данных на основании алгоритмов маршрутизации.

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

Беспроводные устройства в программе представлены беспроводным маршрутизатором и тремя точками доступа.

Среди **конечных устройств** можно увидеть ПК, ноутбук, сервер, принтер, телефоны и так далее.

Интернет в программе представлен в виде облаков и модемов DSL.

Пользовательские устройства и облако для многопользовательской работы показаны на рис.6.

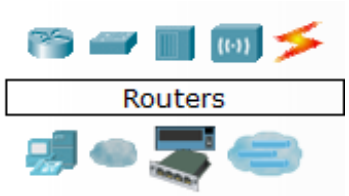


Рис. 6 *Пользовательские устройства и облако для многопользовательской работы*

Линии связи

С помощью линий связи создаются соединения узлов сети в единую топологию и при этом каждый тип кабеля может быть соединен лишь с определенными типами интерфейсов устройств (рис.7).

Рис. 7 *Типы линий связи*

Автоматический тип – при данном типе соединения Packet Tracer автоматически выбирает наиболее предпочтительные тип соединения для выбранных устройств.

Консоль – консольные соединение. Консольное соединение может быть выполнено между ПК и маршрутизаторами или коммутаторами.

Медный прямой – соединение медным кабелем типа витая пара, оба конца кабеля обжаты в одинаковой раскладке.

Медный кроссовер – соединение медным кабелем типа витая пара, концы кабеля обжаты, как кроссовер.

Оптика – соединение при помощи оптического кабеля, необходимо для соединения устройств, имеющих оптические интерфейсы.

Телефонный кабель – кабель для подключения телефонных аппаратов. Соединение через телефонную линию может быть осуществлено между устройствами, имеющими модемные порты. Пример - ПК, дозванивающийся в сетевое облако.

Коаксиальный кабель – соединение устройств с помощью коаксиального кабеля. Используется для соединения между кабельным модемом и облаком.

Серийный DCE и серийный DTE - соединения через последовательные порты для связей Интернет. Для настройки таких соединений необходимо установить синхронизацию на стороне DCE-устройства. Сторону DCE можно определить по маленькой иконке "часов" рядом с портом.

Графическое меню

На рис. 8 показано графическое меню программы.

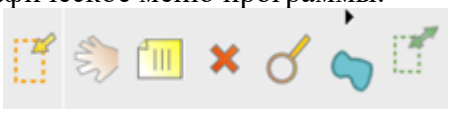


Рис. 8 *Графическое меню (перевернуто)*

На рис. 8 слева направо:

Инструмент **Select** (Выбрать) можно активировать клавишей Esc. Он используется для выделения одного или более объектов для дальнейшего их перемещения, копирования или удаления.

Инструмент **Move Layout** (Переместить слой, горячая клавиша M) используется для прокрутки больших проектов сетей.

Инструмент **Place Note** (Сделать пометку, клавиша N) добавляет текст в рабочей области проекта.

Инструмент **Delete** (Удалить, клавиша Del) удаляет выделенный объект или группу объектов.

Инструмент **Inspect** (Проверка, клавиша I) позволяет, в зависимости от типа устройства, просматривать содержимое таблиц (ARP, NAT, таблицы маршрутизациии др.).

Инструмент **Drawapolygon** (Нарисовать многоугольник) позволяет рисовать прямоугольники, эллипсы, линии и закрашивать их цветом.

Инструмент **Resize Shape** (Изменить размер формы, комбинация клавиш Alt+R) предназначен для изменения размеров рисованных объектов (четырехугольников и окружностей).

Элементы анимации и симуляции

Эти элементы интерфейса показаны на рис.9.

Рис. 9 *Элементы анимации и симуляции*

Инструменты **Add Simple PDU** (Добавить простой PDU, клавиша P) и **Add Complex PDU** (Добавить комплексный PDU, клавиша C) предназначены для эмулирования отправки

пакета с последующим отслеживанием его маршрута и данных внутри пакета.

Физическое представление оборудования

В программе возможно физическое представление оборудования в виде его физической конфигурации (рис. 10), для этого необходимо дважды щелкнуть по устройству .

Рис. 10 *Физическая конфигурация ПК*

Для изменения комплектации оборудования необходимо перейти на вкладку Zoom In, перетащить мышью нужный модуль в свободный слот, затем включить питание. В качестве примера было добавлено в физическую конфигурацию ПК (Рис.11) микрофон (PT-MICROPHONE) и наушники (PT HEADPHONE), в результате чего ПК изменил свой значок в программе (Рис. 12).

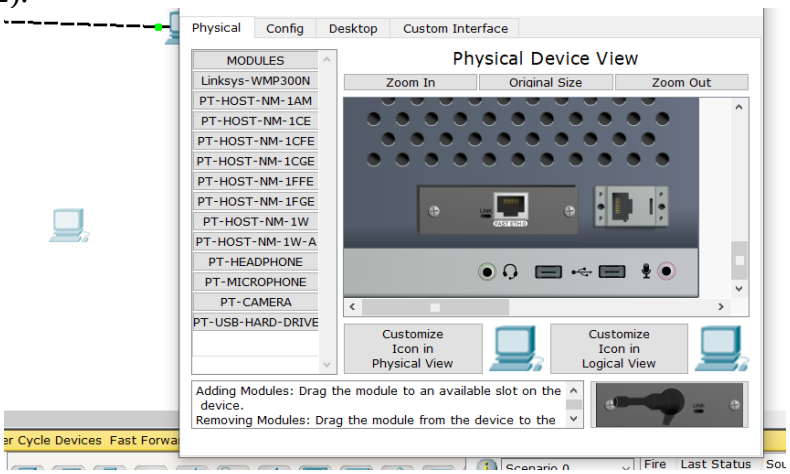


Рис.11 Физическая конфигурация ПК без подключенного оборудования

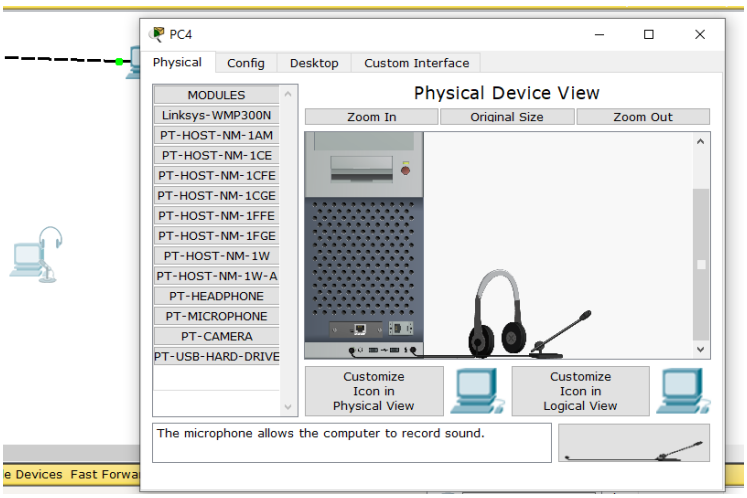


Рис.12 Физическая конфигурация ПК с микрофоном и наушниками

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

Создание сети из двух ПК в программе Cisco Parket Tracer

В качестве примера для начального знакомства с программой построим простейшую сеть из двух ПК, соединенных кроссовым кабелем (рис. 13).

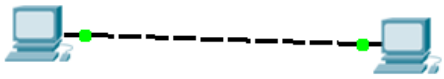


Рис. 13 *Сеть из двух ПК*

Для решения нашей задачи в левой нижней части программы на вкладке END Devices (Ctrl+Alt+V) выбираем тип компьютера (PC-PT) и переносим его мышью в рабочую область программы (рис. 14).

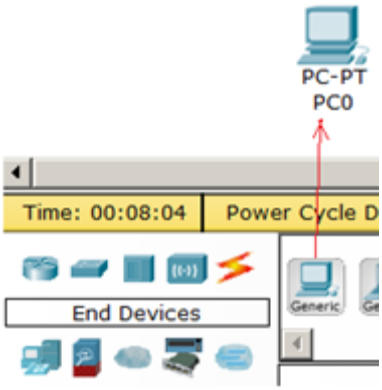


Рис. 14 *Устанавливаем в рабочую область программы первый ПК*

Компьютеры соединяем, выбрав тип соединения **Автоматически** (рис.15).

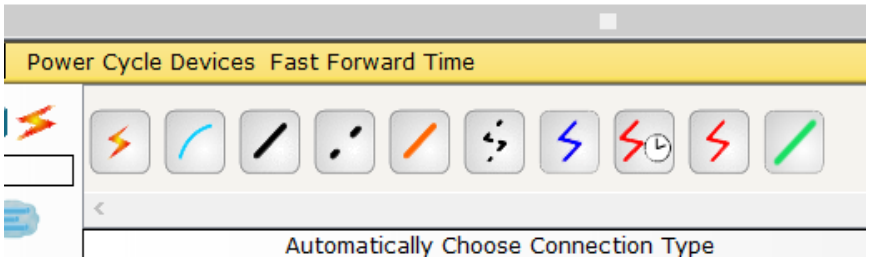


Рис. 15 *Выбор типа соединения* ***Автоматически***

Теперь приступим к настройке левого ПК: щелкаем на нем мышью, на вкладке **Desktop** переходим на вкладку **Ip Configuration** (Настройка IP) - рис. 16.

Рис. 16 *Панель настройки ПК*

Для первого ПК вводим IP адрес 192.168.1.1 и маску подсети 255.255.255.0, окно закрываем (рис. 17). Аналогично настраиваем второй ПК на адрес 192.168.1.2 и ту же маску.

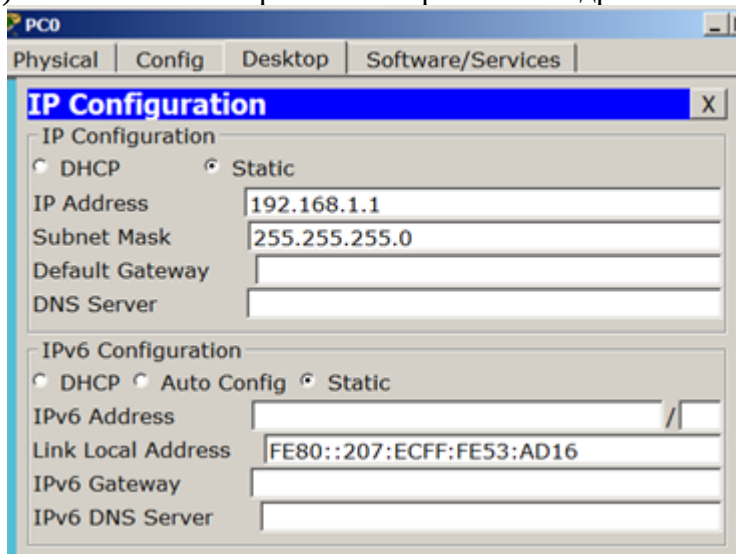


Рис. 17 *Окно настройки PC0*

При наведении мыши на ПК появляется окно подсказок о конфигурации компьютера (рис.18).

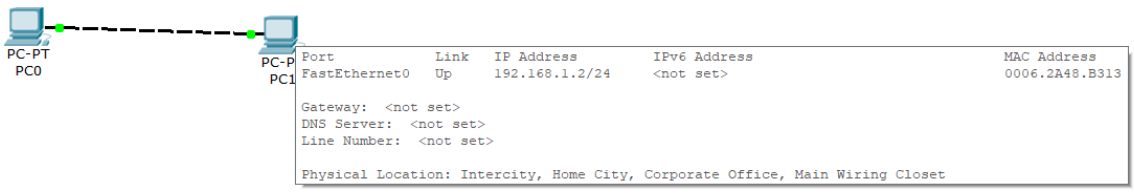


Рис. 18 *Окно настройки PC0*

Далее проверим наличие связи ПК и убедимся, что ПК0 и ПК1 видят друг друга. Для этого на вкладке **Desktop** (**Рабочий стол**) перейдем в поле run (Командная строка) и пропингуем соседний ПК (рис. 19).

Ping — утилита для проверки соединений в сетях на основе TCP/IP. Утилита отправляет запросы (ICMP Echo-Request) протокола ICMP указанному узлу сети и фиксирует поступающие ответы (ICMP Echo-Reply). Время между отправкой запроса и получением ответа (RTT) позволяет определять двусторонние задержки (RTT) по маршруту и частоту потери пакетов, то есть косвенно определять загруженность на каналах передачи данных и промежуточных устройствах. Полное отсутствие ICMP-ответов может также означать, что удалённый узел (или какой-либо из промежуточных маршрутизаторов) блокирует ICMP Echo-Reply или игнорирует ICMP Echo-Request.

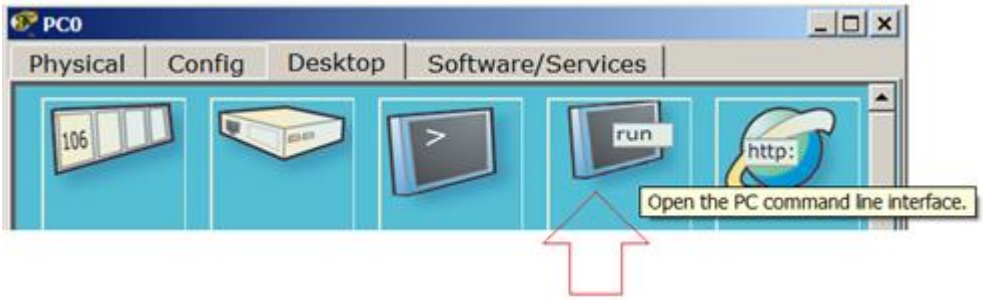


Рис. 19 *Вызов командной строки (Command Prompt)*

Написав команду **ping 192.168.1.2**, видно из рис. 20, что связь между ПК присутствует (настроена) и наблюдается 0% потерь (%loss).

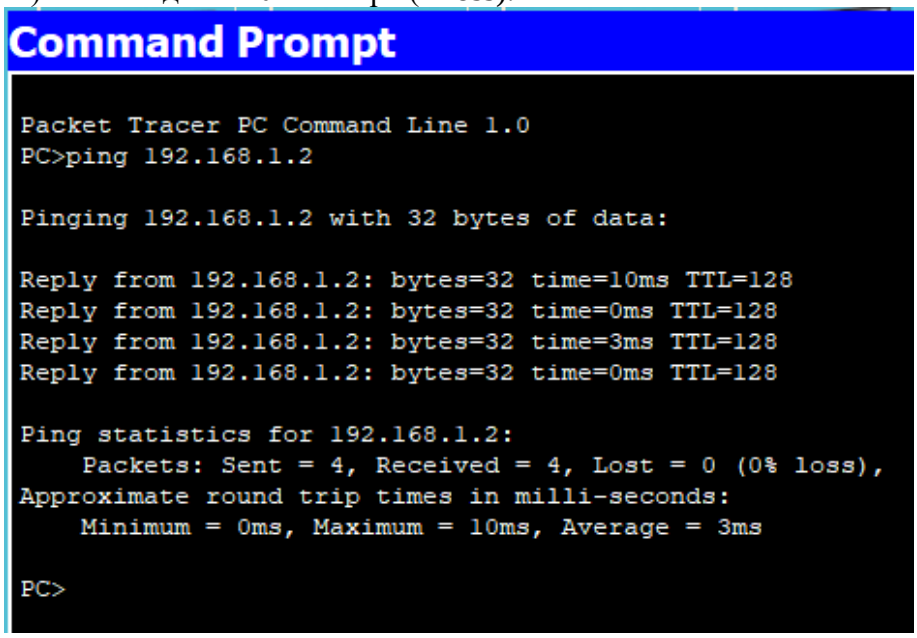


Рис. 20 *Успешное выполнение комманды ping.*

Чтобы ускорить процесс создания топологии из однотипных элементов, можно добавить один элемент сети (например, ПК), осуществить его настройку (задать IP адрес, маску), а затем при нажатии на клавишу Ctrl и на значок ПК размножить ПК. В свойствах появившихся ПК, изменить IP-адреса и другие настройки; при двойном щелчке по названию компьютера изменить его название.

Создание сети из двух коммутаторов и четырех ПК в программе Cisco Parket Tracer

Построим простейшую сеть из двух коммутаторов (свитч) и четырех ПК (рис. 21).

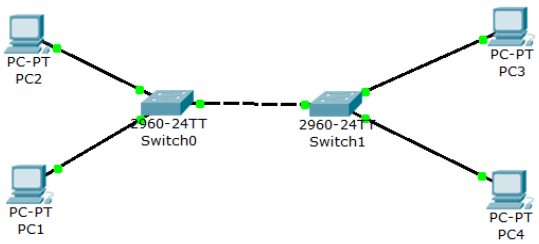


Рис. 21 *Топология из двух Switch и четырех ПК*

Добавим четыре ПК, используя для копирования Ctrl. Зададим для них IP-адреса: 192.168.1.1 - 192.168.1.8.

Добавим два Switch 2960. Между Switch установим автоматическую связь (Connections Automatically) – первоначально загораются красные точки, через несколько секунд они приобретают зеленый цвет.

От компьютера до Switch устанавливаем прямое соединение выбирая линию связи **Медный прямой** (Cooper Straight Through – медный кабель, типа витая пара) (рис.22).

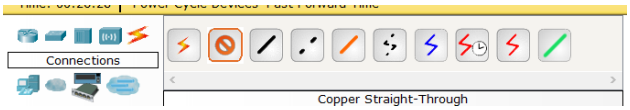


Рис. 22 *Выбор линии связи* ***Медный прямой***.

Выбрав нужную линию связи и щелкнув по ПК выбираем Fast Ethernet (рис.23).

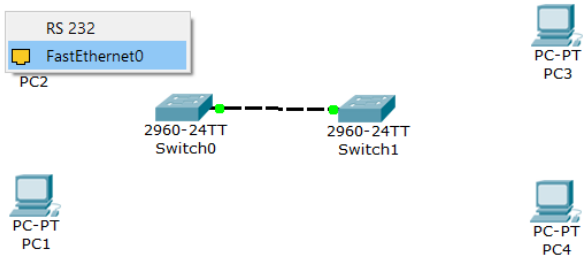


Рис. 23 *Настройка линии связи с со стороны ПК*

Затем при нажатии на Switch выбираем первый свободный интерфейс в верхней части списка (рис.24).

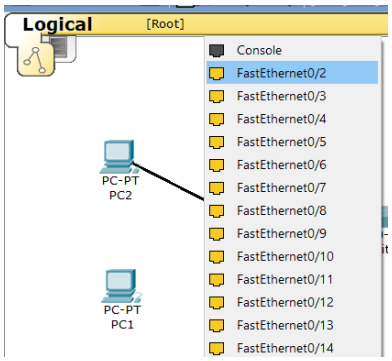


Рис. 24 *Настройка линии связи с со стороны Switch*

Далее производим аналогичные настройки линий связи для других ПК. Дожидаемся, чтобы все интерфейсы загорелись зелеными точками.

Чтобы убрать лишние надписи рядом с устройствами необходимо выбрать меню

Options/Preferences/Interface и снять галочки Show Device Model Labels и Show Device Name Labels (рис. 25).

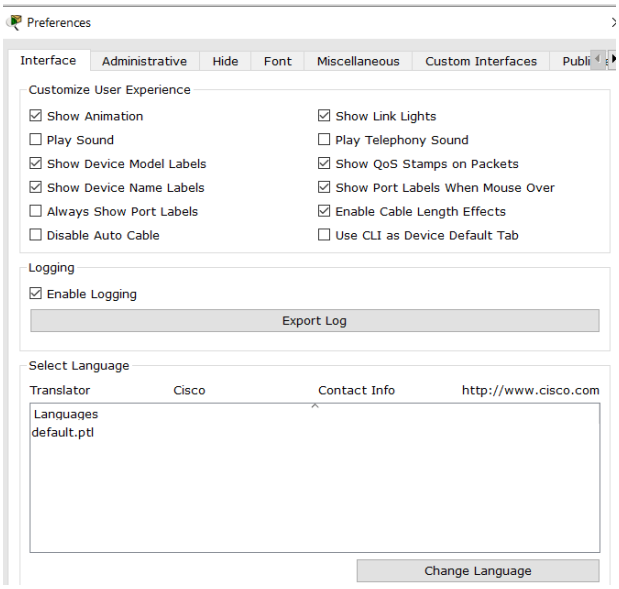


Рис. 25 *Изменение настроек надписей устройств.*

Чтобы рядом с ПК появился IP-адрес необходимо скопировать адрес из IP Configuratios, а затем с помощью инструмента Создание заметок (Place Note – клавиша N) (рис. 26) вставить IP адрес в поле надписи.

Рис. 26 *Создание заметок*

В итоге должна появиться следующая топология (рис.27).

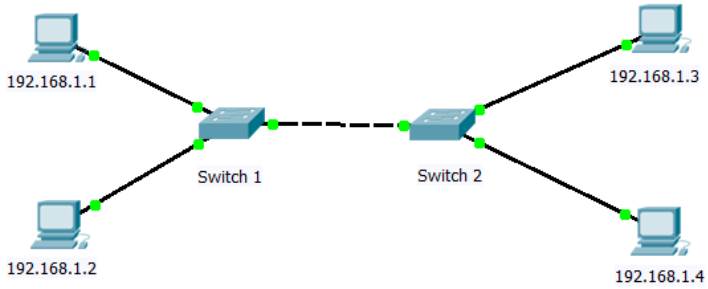


Рис. 27 *Топология из двух Switch и четырех ПК с надписями IP-адресов*

Cisco Packet Tracer содержит режим симуляции работы сети, в котором можно имитировать сетевые события.

Чтобы перейти в режим симуляции нужно нажать комбинацию клавиш **Shift+S**, или, щелкнуть мышью на иконку симуляции в правом нижнем углу рабочего пространства (рис.28).

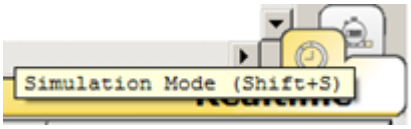


Рис. 28 *Кнопка Симуляция*

Затем можно изменить фильтры, нажав на кнопку Edit Filters (Изменить фильтры) и исключите все сетевые протоколы, кроме ICMP (рис.29).

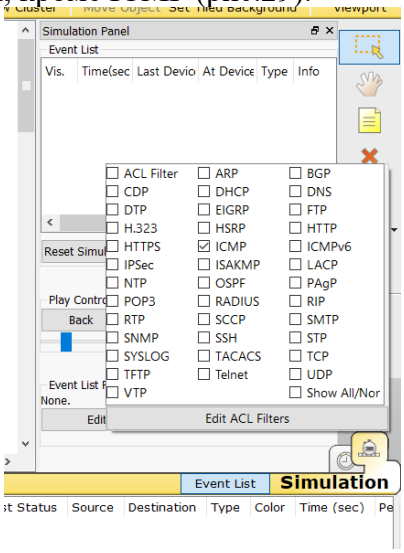


Рис. 29 *Флажок ICMP активен*

ICMP (Internet Control Message Protocol) — сетевой протокол, входящий в стек протоколов TCP/IP. В основном ICMP используется для передачи сообщений об ошибках и других исключительных ситуациях, возникших при передаче данных.

Выбираем в режиме симуляции конверт (рис. 30) и отмечаем ПК отправителя и ПК получателя.

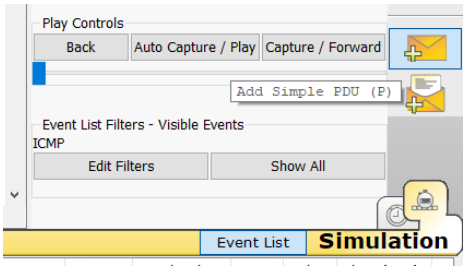


Рис. 30 *Выбор конверта в режиме симуляции*

На ПК отправителя образовался пакет (конвертик), который ждёт начала движения его по сети. Запустить продвижение пакет в сеть пошагово можно, нажав на кнопку Capture / Forward (Вперёд) в окне симуляции. Если нажать на кнопку Auto Capture / Play (воспроизведение), то мы увидим весь цикл прохождения пакета по сети (рис.31).

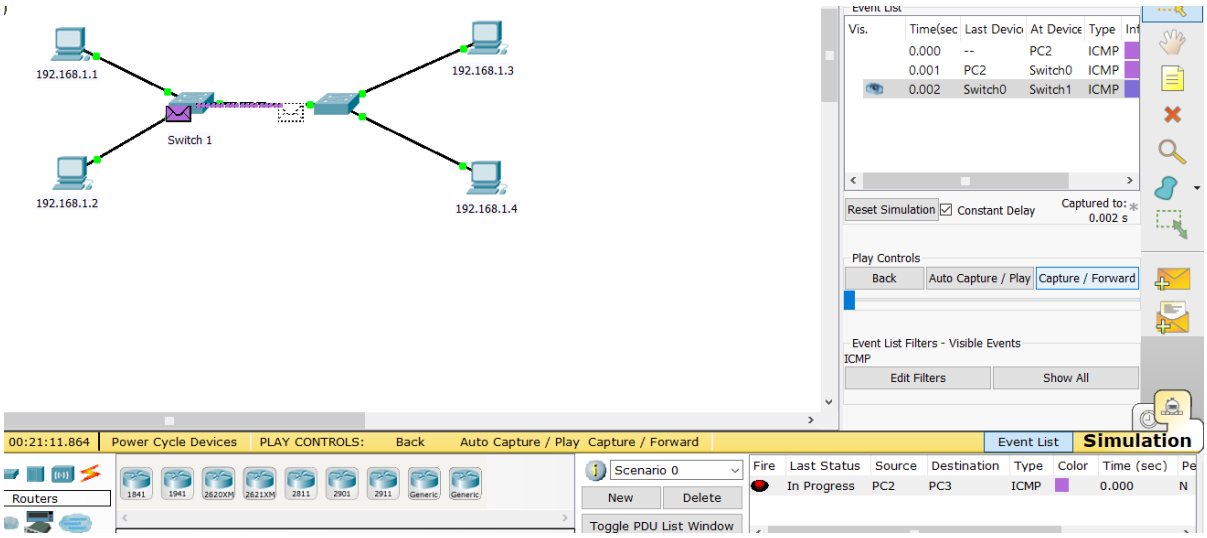


Рис. 31 *Продвижение пакетов в режиме симуляции.*

В Event List (Список событий) можно видеть успешный результат продвижения пакетов (рис.32).

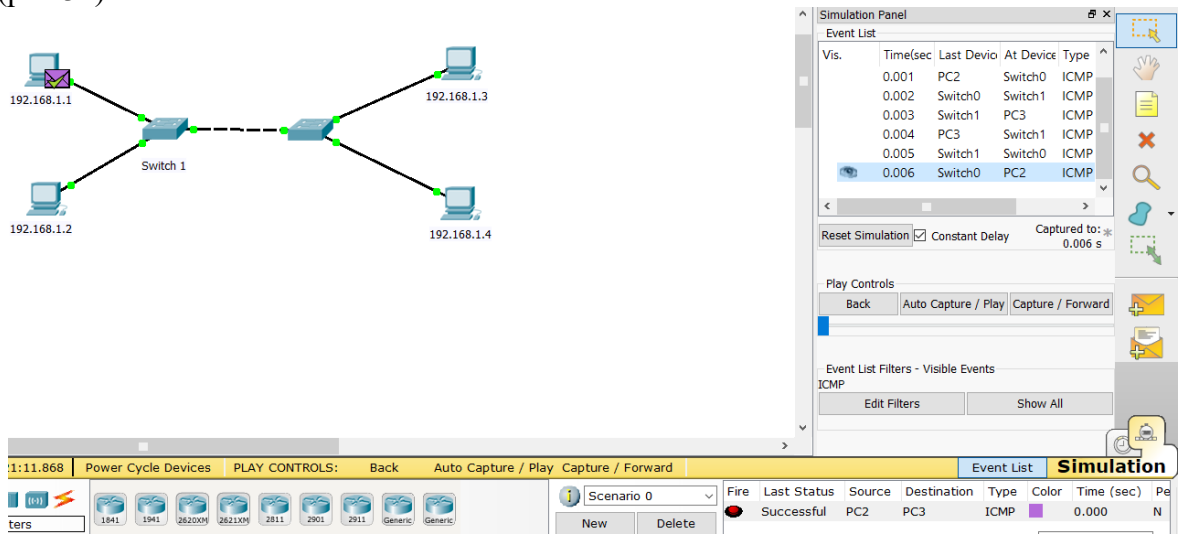


Рис. 32 *Список событий в режиме симуляции.*

Щелчок мышью на конверте покажет нам дополнительную информацию о движении пакета по сети. При этом на первой вкладке увидим **модель OSI** (рис.33). На вкладке OSI Model (Модель OSI) представлена информация об уровнях OSI, на которых работает данное сетевое устройство.

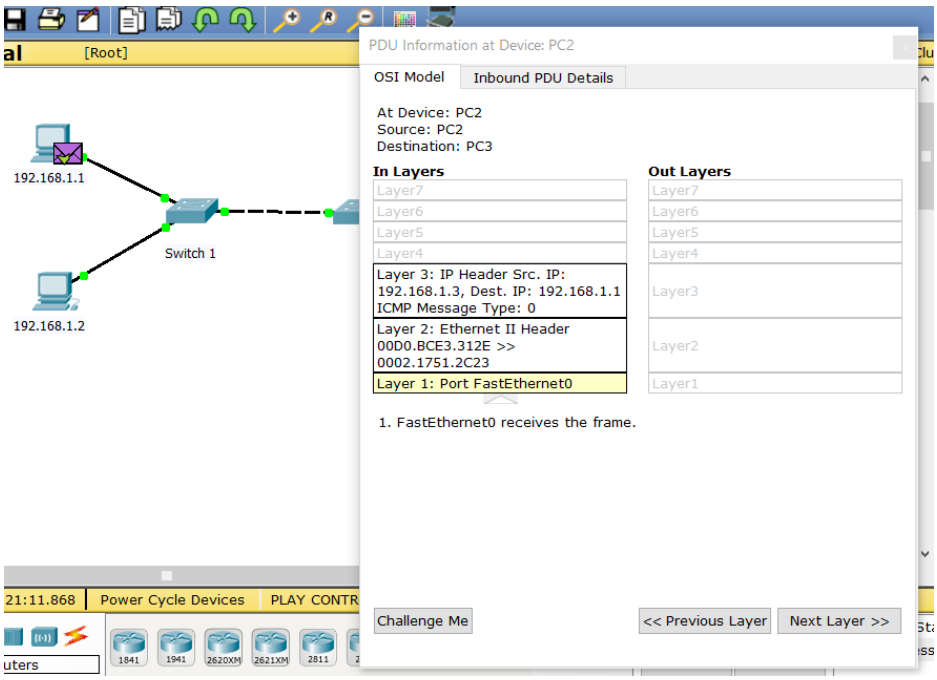


Рис. 33 *Мониторинг движения пакета на модели OSI*

На другой вкладке можно посмотреть структуру пакета (рис. 34).

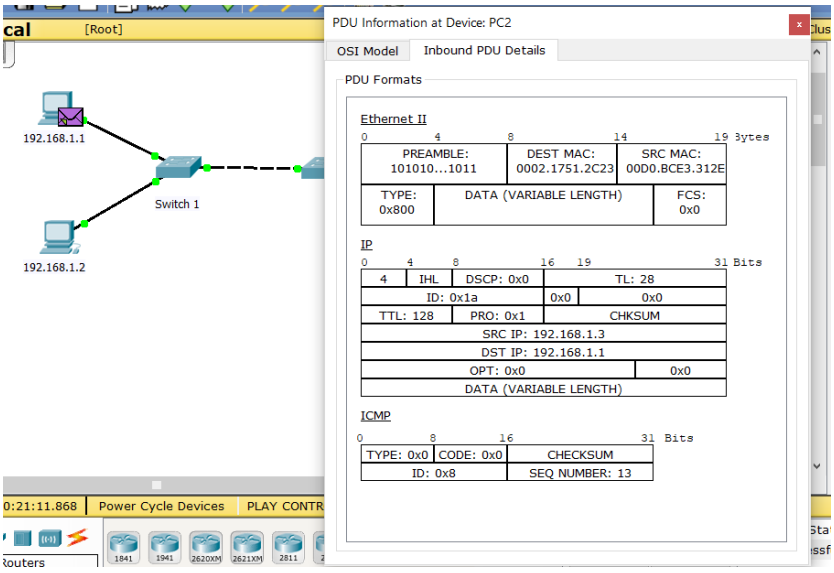


Рис. 34 *Структура пакета*

Вывод: в Packet Tracer предусмотрен режим моделирования (Симуляции), в котором показывается, как работает утилита Ping (рис.35). Чтобы перейти в данный режим, необходимо нажать на значок **Simulation Mode** (Симуляция) в нижнем правом углу рабочей области или комбинацию клавиш **Shift+S**. Откроется **Simulation Panel** (Панель симуляции), в которой будут отображаться все события, связанные с выполнения ping-процесса. Моделирование прекращается либо при завершении ping-процесса, либо при закрытии окна симуляции. В режиме симуляции можно не только отслеживать используемые протоколы, но и видеть, на каком из семи уровней модели OSI данный протокол задействован. Когда пакет возвращается отправителю, то появляется галочка - "принятие пакета".

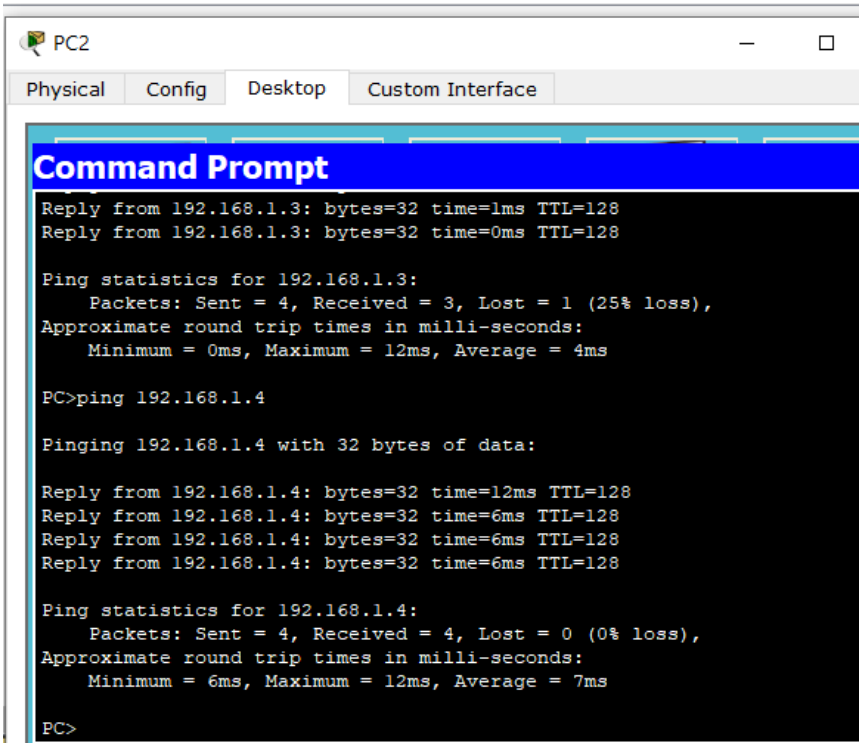


Рис. 35 *Операция ping с ПК2 на ПК4*

На рис. 35:

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

time - время, потраченное на отправку запроса и получение ответа,

min - минимальное время ответа,

max - максимальное время ответа,

avg - среднее время ответа.

Для устройств, у которых не назначены были ранее IP адреса, в режиме командной строки команда **ipconfig** позволяет назначать IP адреса и маски (рис.36).

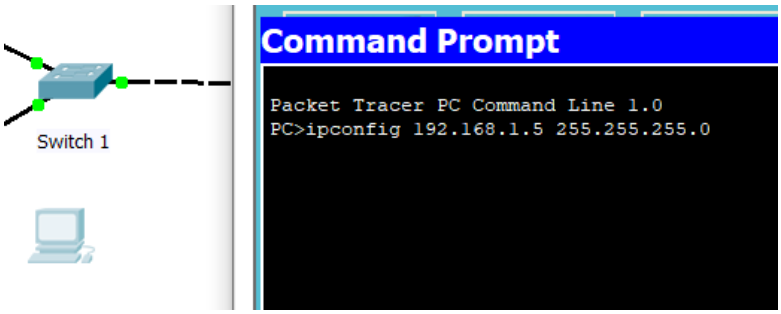


Рис. 36 *Назначение IP иадреса и маски новому ПК*

А для устройств, у которых адреса и маски были назначены команда **ipconfig** позволяет проверять IP адреса и маски (рис.37).

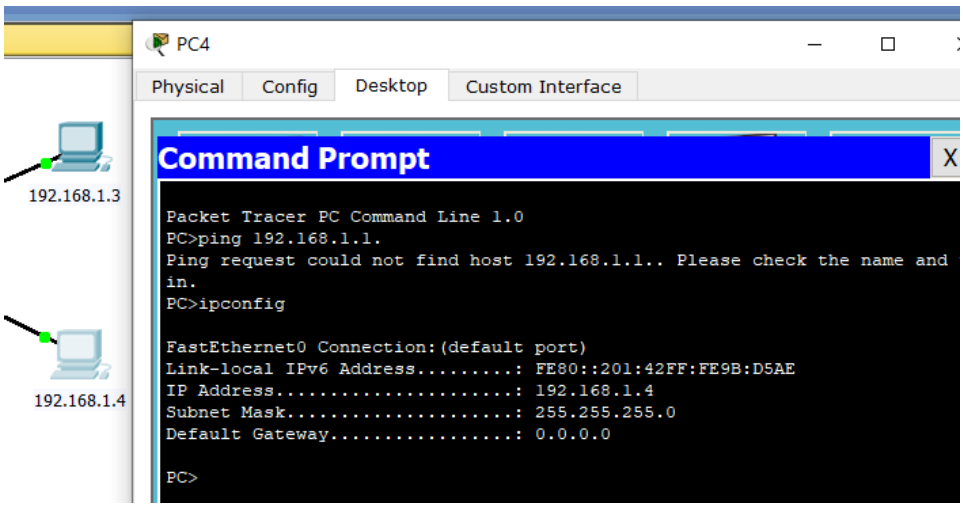


Рис. 37 *Проверка IP адреса и маски ПК*

<u>Задание для самостоятельной работы</u>

1. Создайте топологию, аналогичную топологии на Рис 2.1

2. Назначьте компьютерам адреса, согласно варианту 192.168.v.1 - 192.168.v.n (v=1-25). Нумерация компьютеров для каждого студента уникальна и соответствует номеру студента (v) в списке преподавателя.

Например, для варианта 7 (v=7) и компьютера PC1 имеем IP ADDRESS 192.168.7.1, а для PC8 - 192.168.7.8.

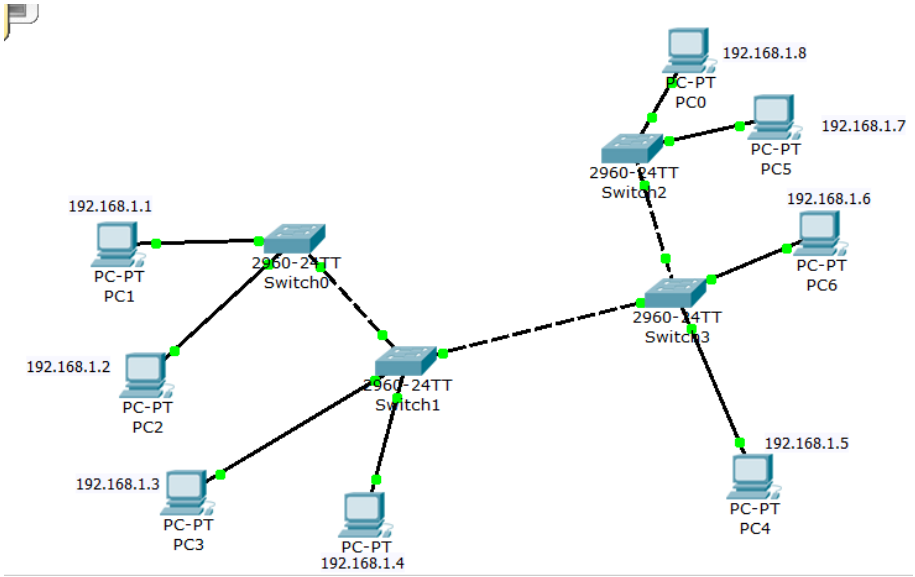


Рис. 2.1 Пример топологии

3. Назначьте компьютерам имена, соответствующие их IP адресам, лишние надписи уберите. Измените комплектацию некоторых компьютеров – добавьте наушники, гарнитуру, винчестеры и т.д.

4. Если сделано всё правильно, то вы сможете пропинговать любой компьютер из любого компьютера.

5. Запустите процесс симуляции движения пакетов от источника информации к получателю, отфильтруйте протоколы для режима симуляции.

6. Поработайте с командой ipconfig, используя обе ее функциональные возможности.

7. Сохраните файл топологии и конфигурации сети, какое расширение он имеет?

8. Пригласите преподавателя и покажите результат работы.

Лабораторная работа №2. «Моделирование сети с топологией звезда на базе концентратора и коммутатора»

Цель работы: Знакомство с моделированием сети на основе концентратора и коммутатора в программе Cisco Packet Tracer. Анализ доставки информации в сетях на основе концентратора и коммутатора, четкое понимание отличий, определение достоинств и недостатков топологий этих двух видов.

Теоретическая часть.

Звезда — базовая топология компьютерной сети, в которой все компьютеры сети присоединены к центральному узлу, образуя физический сегмент сети. Центральным узлом выступает концентратор, коммутатор или ПК. Рабочая станция, с которой необходимо передать данные, отсылает их на концентратор. В определённый момент времени только одна машина в сети может пересылать данные, если на концентратор одновременно приходят два пакета, обе посылки оказываются не принятыми и отправителям нужно будет подождать случайный промежуток времени, чтобы возобновить передачу данных. Этот недостаток отсутствует на сетевом устройстве более высокого уровня — коммутаторе, который, в отличие от концентратора, подающего пакет на все порты, подает лишь на определенный порт — получателю. Одновременно может быть передано несколько пакетов. Сколько — зависит от коммутатора.

Достоинства звезды:

- выход из строя одной рабочей станции не отражается на работе всей сети в целом;
- лёгкий поиск неисправностей и обрывов в сети;
- высокая производительность сети (при условии правильного проектирования);
- гибкие возможности администрирования.

Недостатки звезды:

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

Моделирование сети с топологией звезда на базе концентратора

С помощью программного симулятора Cisco Packet Tracer построим сеть с топологией Звезда на базе концентратора (рис.1).

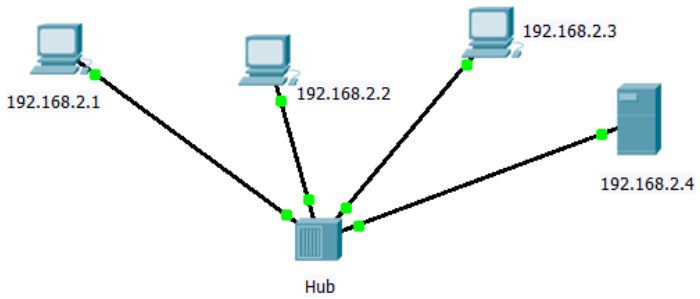


Рис. 1 *Моделирование сети с топологией звезда на базе концентратора*

Выбираем тип оборудования **Hub's** (Концентраторы). В меню "список устройств данного типа оборудования" выбираем конкретный концентратор - Hub-PT и перетаскиваем его мышью в рабочую область программы (рис.2).

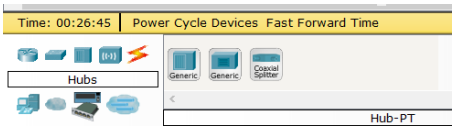


Рис. 2 *Выбор концентратора (Hub)*

Далее выбираем тип устройства **End Devices** (Конечные устройства) и в дополнительном меню выбираем настольный компьютер PC-PT и перетаскиваем его мышью в рабочую область программы. Таким образом, устанавливаем ещё три компьютера и один сервер. Для подключения компьютеров и сервера к концентратору выбираем новый тип устройств **Connections** (Соединения), далее выбираем Copper Straight-Through (Медный прямой) тип кабеля. Чтобы соединить сетевую карту компьютера с портом Hub-а, необходимо щелкнуть левой клавишей мыши по нужному компьютеру. В открывшимся графическом меню выбрать порт FastEthernet0 и протянуть кабель от ПК к концентратору, где в аналогичном меню выбрать любой свободный порт Fast Ethernet концентратора. При этом желательно всегда придерживаться следующего правила: для сервера выбираем 0-й порт, для PC1 - 1й порт, для PC2 - 2й порт и так далее.

Назначаем узлам сети IP адреса и маску. Для этого двойным щелчком открываем нужный компьютер, далее **Desktop**. В группе параметров **IP Configuration** (Настройка IP) должен быть активирован переключатель **Static** (Статический) в поле **IP Address** необходимо ввести IP-адрес компьютера, маска появится автоматически.

Используя инструмент создания заметок **Place Note** (клавиша N), подписываем все IP устройств, а вверху рабочей области создаем заголовок нашего проекта "Топология на основе концентратора" (рис. 3).

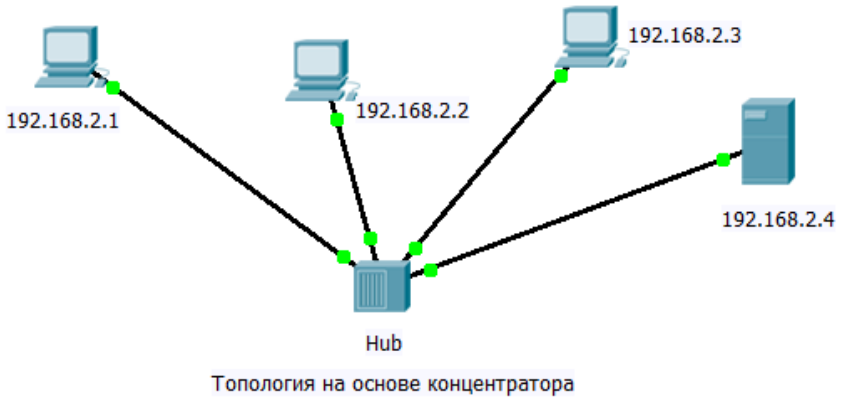


Рис. 3 *Использование инструмент Place Note (Заметка)*

IP адреса можно скопировать из окна Ip **Configuration** (Конфигурация). При этом активировав, инструмент **Place Note** (Заметка).

С целью исключения нагромождения рабочей области надписями, уберем надписи (метки) типов устройств: откроем меню **Options** (Опции) в верхней части окна Packet Tracer, затем в ниспадающем списке выберем пункт **Preferens** (Настройки), а в диалоговом окне снимем флажок **Show device model labels** (Показать модели устройств) и **Show device name labels** (Показать имена устройств).

Для проверки работоспособности сети отправим с компьютера на другой ПК тестовый сигнал ping (рис.4).

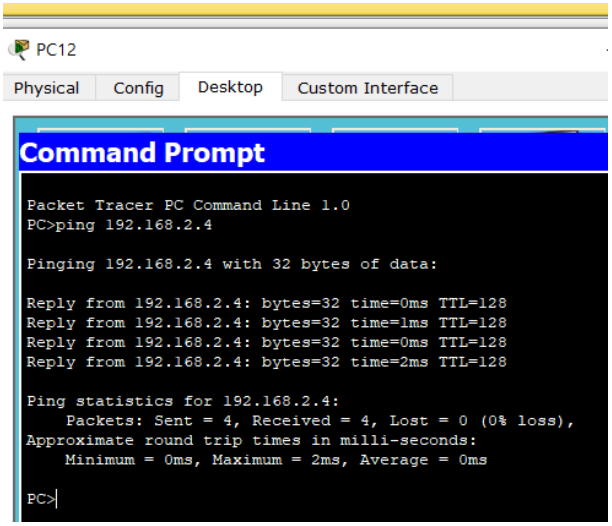


Рис. 4 *Проверка работоспособности сети*

Затем переключимся в режим **Simulation** (Симуляция). В окне **Event list** (Список событий), с помощью кнопки **Edit filters** (Изменить фильтры), сначала очистите фильтры от всех типов сигнала, а затем установим тип контроля сигнала: только ICMP.

В правой части окна, в графическом меню выбираем простой конверт (Простой PDU) и щелчками мыши, устанавливаем его на ПК - источник сигнала (например, PC3) и, затем, на узле назначения (пусть это будет сервер). Нажимая на кнопку Capture / Forward (Захват/Вперед) наблюдаем пошаговое продвижение пакета PDU .

PDU - обобщённое название фрагмента данных на разных уровнях Модели OSI: кадр Ethernet, ip-пакет, udp-датаграмма, tcp-сегмент и т. д.

Для ускоренного моделирования сети состоящей из однотипных компьютеров достаточно настроить один компьютер, а затем удерживая клавишу Ctrl можно скопировать этот ПК несколько раз и настройте остальные адреса ПК, меняя только последнюю цифру IP адреса. Также можно копировать группы компьютеров и целые фрагменты сетей, предварительно выделив их.

Моделирование сети с топологией звезда на базе коммутатора (switch)

Hub работает на первом уровне модели OSI и отправляет информацию во все порты, кроме порта – источника. Switch работает на втором уровне OSI и отправляет информацию только в порт назначения за счет использования таблицы MAC адресов хостов. В сетях IP существует 3 основных способа передачи данных:

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

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

Работу сети с топологией звезда на базе концентратора мы уже изучили. Теперь рассмотрим аналогичную сеть на базе коммутатора (рис.5).

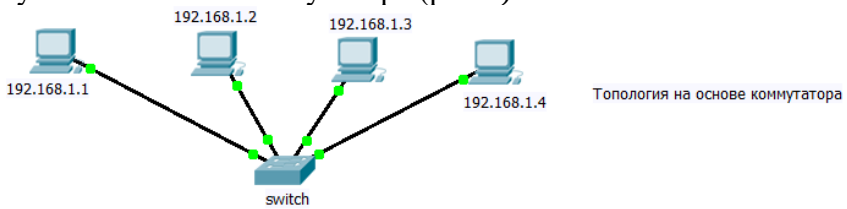


Рис. 5 *Звезда на базе коммутатора модели 2960*

Аналогично предыдущим рекомендациям моделируем сеть с использование switch 2960.

На вкладке Physical вы можете посмотреть вид коммутатора switch 2960, имеющего 24 порта Fast Ethernet и 2 порта Gigabit Ethernet (рис.6).

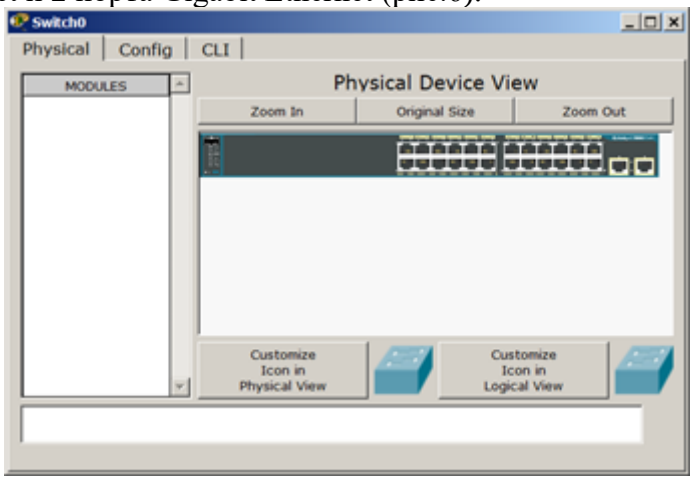


Рис. 6 *Физический внешний вид коммутатора модели 2960*

Switch отправляет пакеты только в определенный порт за счет использования таблицы MAC адресов (рис.7).

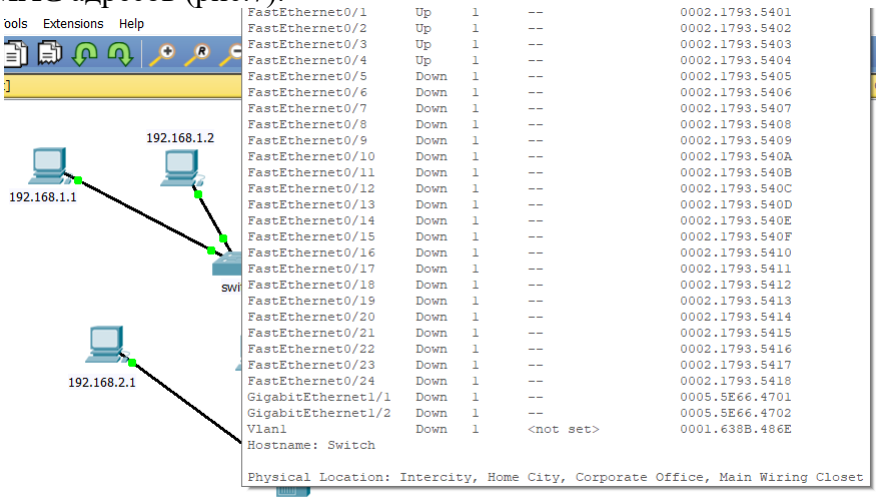


Рис. 7 *Таблица MAC адресов switch.*

В режиме **Simulation** нужно настроить фильтры и с помощью функции  , просмотреть прохождение пакета между двумя ПК через коммутатор. Как видим, маршруты пакета в концентраторе и коммутаторе будут разными: как в прямом, так и в обратном направлении хаб отправляет всем, а коммутатор – только одному

<u>Задание для самостоятельной работы</u>

1. Создайте две топологии. Одна с концентратором, другая с коммутатором. Каждая топология должна содержать не менее 6 ПК, сервер, можно по желанию добавить ноутбуки (laptop).

2. Назначьте компьютерам и серверам адреса, согласно варианту 192.168.v.1 - 192.168.v.n (v=1-25). Нумерация компьютеров для каждого студента уникальна и соответствует номеру студента (v) в списке преподавателя.

Например, для варианта 7 (v=7) и компьютера PC1 имеем IP ADDRESS 192.168.7.1, а для PC8 - 192.168.7.8.

3. Дайте компьютерам имена, соответствующие их IP адресам, лишние надписи уберите. Измените комплектацию некоторых компьютеров – добавьте наушники, гарнитуру, винчестеры и т.д.

4. Произведите настройку и диагностику этих сетей двумя способами (утилитой ping и с помощью конверта PDU). Убедитесь в успешности работы сети в режиме симуляции.

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

5. Запустив процессы симуляции движения пакетов от источника информации к получателю, обратите внимание на разные способы доставки пакетов в этих двух сетях.

6. Сохраните файл топологии и конфигурации сети.

7. Пригласите преподавателя и покажите результат работы.

Лабораторная работа №3. «Исследование качества передачи трафика по сети»

Цель работы: Исследование качества передачи трафика по сети, знакомство с программой организации существенного трафика Traffic Generator, повышение пропускной способности локальной сети за счет использования разных комбинаций коммутаторов и концентраторов. Анализ качества передачи трафика в сетях на основе концентратора и коммутатора, четкое понимание отличий.

Теоретическая и практическая часть.

При исследовании пропускной способности ЛВС (качества передачи трафика по сети) желательно увеличить размер пакета и отправлять запросы с коротким интервалом времени, не ожидая ответа от удаленного узла, для того, чтобы создать серьезную нагрузку на сеть. Однако, утилита ping не позволяет отправлять эхо-запрос без получения эхо-ответа на предыдущий запрос и до истечения времени ожидания. Поэтому для организации существенного трафика воспользуемся программой **Traffic Generator**. Для работы создайте и настройте следующую сеть (рис.1).

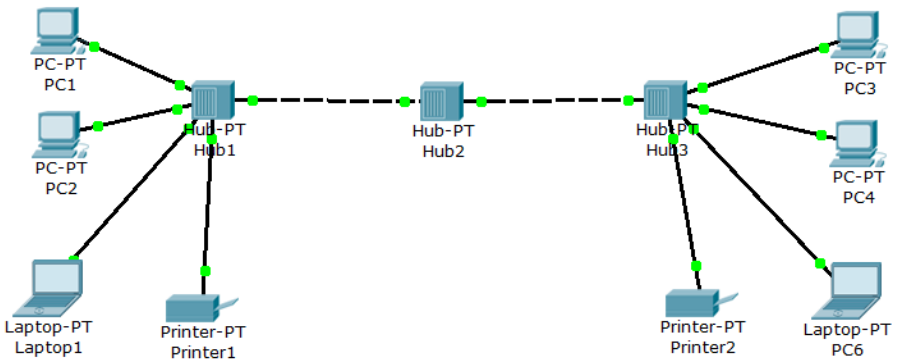


Рис. 1 *Топология сети*

Первое знакомство с Traffic Generator

В окне управления PC1 во вкладке **Desktop** выберите приложение **Traffic Generator** и задайте настройки, как на рис.2 для передачи трафика от PC1 на PC6.

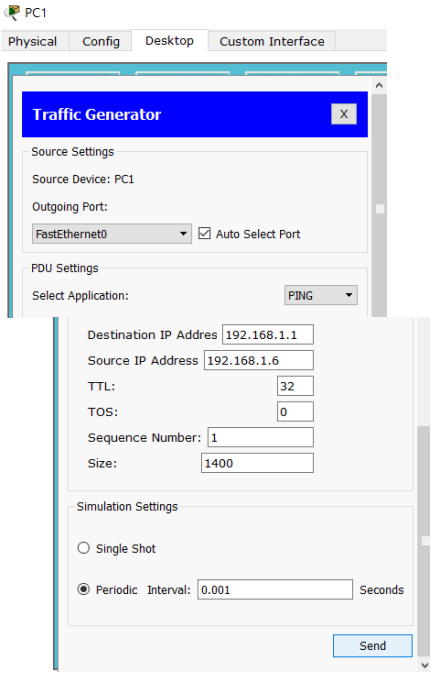


***Рис.2** Настройка генератора трафика (от PC1 до PC6)*

Итак, при помощи протокола ICMP был сформирован трафик между компьютерами PC1 с адресом 192.168.1.1 и PC6 с адресом 192.168.1.6. При этом в разделе **Source Settings** (Настройки источника) необходимо установить флажок **Auto Select Port** (Автовыбор порта), а в разделе **PDU Settings** (настройки IP-пакета) задать следующие значения параметров этого поля:

Select application: PING
Destination: IPAddress: 192.168.1.6 (адрес получателя);
Source IP Address: 192.168.1.1 (адрес отправителя);
TTL:32 (время жизни пакета);
TOS: 0 (тип обслуживания, "0" - обычный, без приоритета);
Sequence Number: 1 (начальное значение счетчика пакетов);
Size: 1400 (размер поля данных пакета в байтах);
Simulations Settings - здесь необходимо активировать переключатель;
Periodic Interval: 0.001 Seconds (период повторения пакетов)

Не обязательно использовать эти настройки. Можно указать, например, Size: 1500, Periodic Interval: 0.5 Seconds. Однако, если неверно укажете IP источника, то генератор работать не будет.

После нажатия на кнопку **Send** (Послать) между PC1 и PC6 начнется активный обмен данными. Не закрывайте окно генератора трафика настройки, чтобы не прервать поток трафика - лампочки должны постоянно мигать!

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

Исследование качества работы сети

Для оценки качества работы сети передадим поток пакетов между PC1 и PC6 при помощи команды ping –n 200 192.168.1.6 и будем оценивать качество работы сети по числу потерянных пакетов. Параметр "–n" позволяет задать количество передаваемых эхо-запросов (у нас их 200) – рис.3.

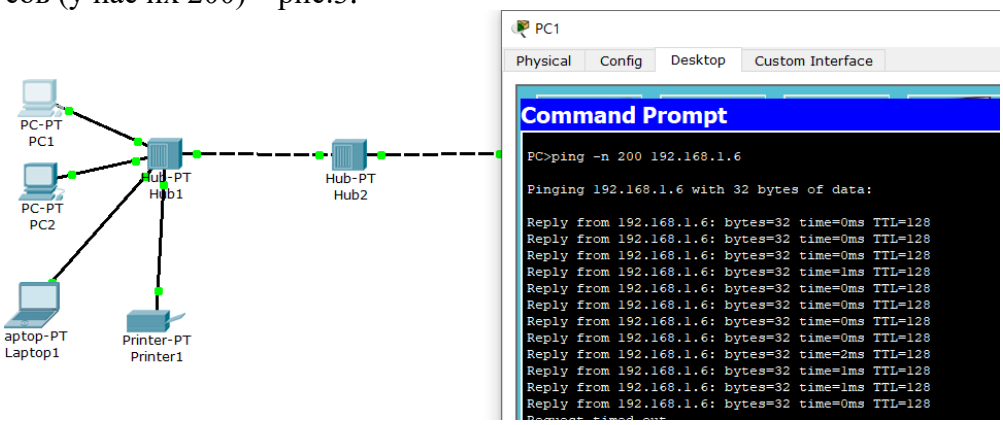


***Рис. 3** Отправляем 200 пакетов на PC6*

Одновременно с «пингом», нагрузите сеть, включив генератор трафика на компьютере PC2 (узел назначения – PC6, размер поля данных–2500 байт, период повторения передачи - 0,1 сек. – рис.4.

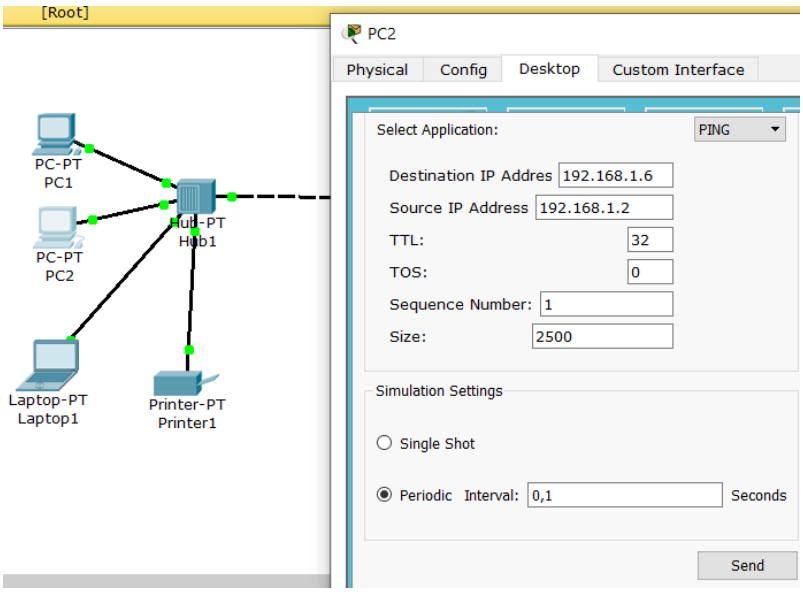


Рис. 4 *Увеличение нагрузки на сеть*

Для оценки качества работы сети - зафиксируйте число потерянных пакетов (рис.5).

```
Reply from 192.168.1.6: bytes=32 time=2ms TTL=128
Request timed out.
Reply from 192.168.1.6: bytes=32 time=0ms TTL=128
Reply from 192.168.1.6: bytes=32 time=1ms TTL=128
Reply from 192.168.1.6: bytes=32 time=1ms TTL=128
Reply from 192.168.1.6: bytes=32 time=0ms TTL=128

Ping statistics for 192.168.1.6:
    Packets: Sent = 200, Received = 185, Lost = 15 (8% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 4294967294ms, Average = 0ms

PC>
```

Рис.5 *Потеряно 15 пакетов*

Также можно было бы загрузить сеть путем организации еще одного потока трафика между какими-либо узлами сети, например, включив генератор трафика еще на ноутбуке Laptop1.

В заключение этой части работы остановить Traffic Generator на всех узлах, нажав кнопку **Stop**.

Повышение пропускной способности локальной вычислительной сети

Проверим тот факт, что установка коммутаторов вместо хабов устраняет возможность возникновения коллизий между пакетами пользователей сети. Замените центральный концентратор на коммутатор (рис.6). Немного подождите и убедитесь, что сеть находится в рабочем состоянии - все маркеры портов не красные, а зеленые.

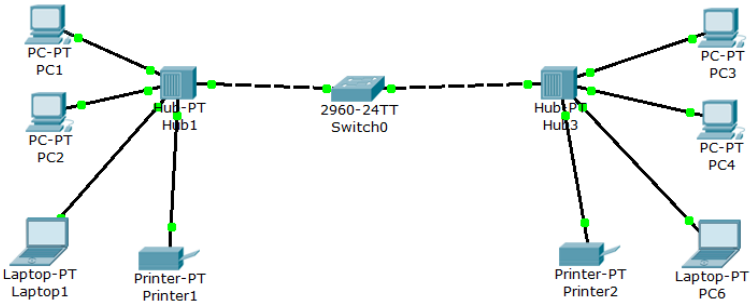


Рис. 6 *Топология сети при замене центрального концентратора на коммутатор*

Снова задайте поток пакетов между PC1 и PC6 при помощи команды ping –n 200 192.168.1.6 и включите Traffic Generator на PC2 и Laptop1. Проследите работу нового варианта сети. Убедитесь, что за счет снижения паразитного трафика качество работы сети стало выше (рис.7.).

```
Reply from 192.168.1.6: bytes=32 time=0ms TTL=128
Reply from 192.168.1.6: bytes=32 time=1ms TTL=128
Reply from 192.168.1.6: bytes=32 time=0ms TTL=128
Reply from 192.168.1.6: bytes=32 time=0ms TTL=128
Reply from 192.168.1.6: bytes=32 time=10ms TTL=128
Reply from 192.168.1.6: bytes=32 time=2ms TTL=128
Reply from 192.168.1.6: bytes=32 time=0ms TTL=128
Reply from 192.168.1.6: bytes=32 time=0ms TTL=128

Ping statistics for 192.168.1.6:
    Packets: Sent = 200, Received = 195, Lost = 5 (3% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 4294967295ms, Average = 0ms
```

***Рис. 7** Потеряно 5 пакет*

Далее, если заменить не один, а все хабы коммутаторами, то это существенно улучшит качество передачи трафика в сети. Замените все концентраторы на коммутаторы (рис.8). Немного подождите и убедитесь, что сеть находится в рабочем состоянии - все маркеры портов не красные, а зеленые.

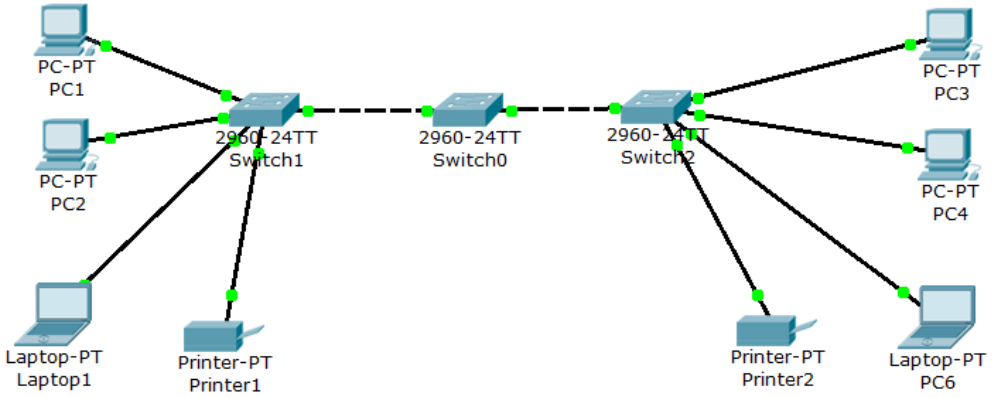


***Рис. 8** Топология сети при замене концентраторов на коммутаторы*

Снова задайте поток пакетов между PC1 и PC6 при помощи команды ping –n 200 192.168.1.6 и включите Traffic Generator на PC2 и Laptop1. Проследите работу нового варианта сети. Убедитесь, что качество работы сети стало выше (рис.9).

```
Reply from 192.168.1.6: bytes=32 time=0ms TTL=128
Reply from 192.168.1.6: bytes=32 time=0ms TTL=128
Reply from 192.168.1.6: bytes=32 time=0ms TTL=128
Reply from 192.168.1.6: bytes=32 time=0ms TTL=128
Reply from 192.168.1.6: bytes=32 time=9ms TTL=128
Reply from 192.168.1.6: bytes=32 time=0ms TTL=128
Reply from 192.168.1.6: bytes=32 time=0ms TTL=128

Ping statistics for 192.168.1.6:
    Packets: Sent = 200, Received = 200, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 41ms, Average = 3ms
```

***Рис. 9** Потеряно 0 пакетов.*

Задание для самостоятельной работы

1. Создайте три топологии, сохраните их в отдельных файлах. Одна с тремя хабами, другая - с центральным коммутатором и двумя хабами, третья – со всеми коммутаторами.

Каждая топология должна содержать не менее 6 устройств (ПК, принтеры, ноутбуки).

2. Назначьте компьютерам и ноутбукам адреса, согласно варианту 192.168.v.1 - 192.168.v.n (v=1-25). Нумерация компьютеров для каждого студента уникальна и соответствует номеру студента (v) в списке преподавателя.

Например, для варианта 7 (v=7) и компьютера PC1 имеем IP ADDRESS 192.168.7.1, а для PC8 - 192.168.7.8.

3. Дайте компьютерам имена, соответствующие их IP адресам, лишние надписи уберите.

4. Для каждой топологии выполните п.5 –п.6.

5. Нагрузите сеть, настроив и включив Traffic Generator на двух устройствах. Как можно понять, что сеть нагружена?

6. Задайте поток пакетов между двумя компьютерами, например, PC1 и PC10 при помощи команды ping –n 200 192.168.1.10. Данные в строке ping можно изменять по собственному желанию.

7. Дождитесь останова работы программы ping, зафиксируйте количество потерянных пакетов.

8. Занесите принтскрины результатов работы ping (количество потерь) для каждой топологии в отчет. Сделайте выводы о том, какая топология обладает наилучшей пропускной способностью.

9. Пригласите преподавателя и покажите результат работы.

Лабораторная работа №4. «Подключение к сетевому оборудованию Cisco. Командная строка управления устройствами CLI. Построение простейшей сети.»

Цель работы: Исследование процесса подключения к коммутатору по консоли, изучение различных режимов конфигурирования сети, создание паролей и пользователей для конфигурирования сети в привилегированном режиме, умение задавать адресацию устройствам, настройка виртуальных терминальных линий, построение простейшей сети, поднятие интерфейса на роутере.

Теоретическая и практическая часть

Консоль

Большинство сетевых устройств компании CISCO допускают конфигурирование. Для этого администратор сети должен подключиться к устройству через прямое кабельное (консольное) подключение (рис.1).

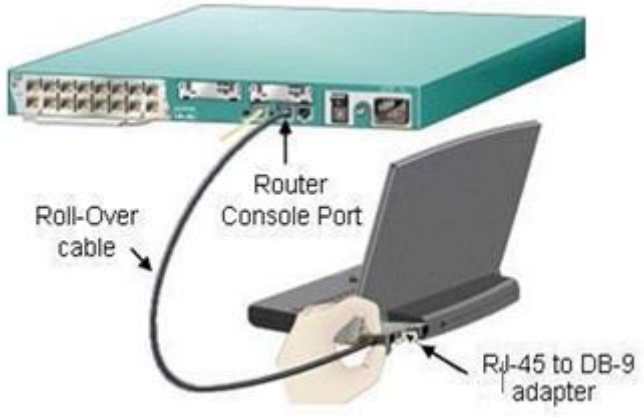


Рис. 1 *Консольное подключение к сетевому устройству*

Итак, программирование устройств CISCO чаще всего производят через консольный порт RJ-45. На рис.2 и рис.3 приведены фотографии консольных разъёмов на маршрутизаторе и 2 варианта консольного кабеля.

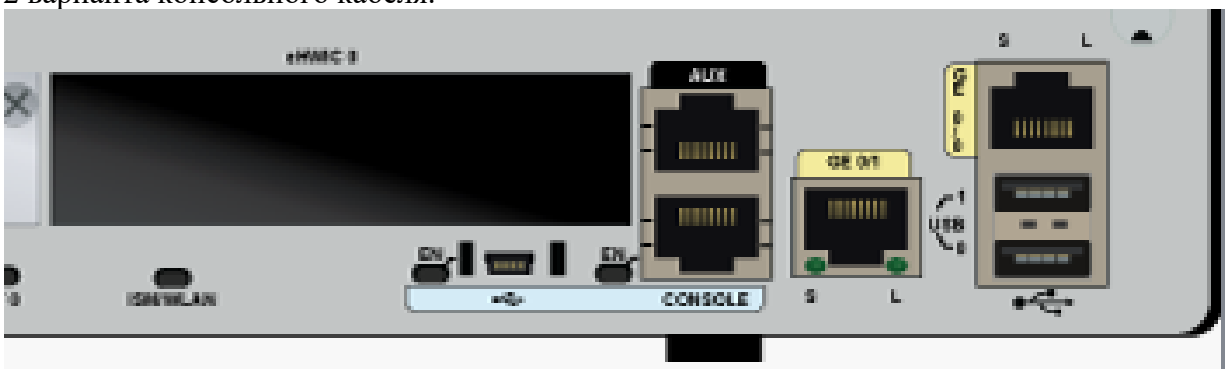


Рис. 2 *Синим цветом показаны разъёмы под управляющий (консольный) кабель*

Рис. 3 *Варианты консольных кабелей*

Классический консольный кабель имеет разъем DB9 для подключения к COM-порту компьютера и разъем RG-45 для подключения к консольному порту маршрутизатора.

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

Подключение к сетевому оборудованию Cisco

Возможные способы подключения:

- с помощью консольного кабеля;
- по Telnet/SSH;
- Web-интерфейс;
- специализированное ПО (SDM, CSM, IME).

Режимы работы с устройством при использовании CLI (интерфейс командной строки - Command Line Interface)

В командную строку пользователь вводит символы, формирующие управляющее воздействие. Работа с командной строкой осуществляется в нескольких режимах (табл.1).

Таблица 1 Режимы командного интерфейса

Режим	Переход в режим	Вид командной строки	Выход из режима
Пользовательский	Подключение	Router>	logout
Привилегированный	Enable.	Router#	disable
Глобальная конфигурация	Configure terminal	Router(config)#	exit,end или Ctrl-Z
Настройка интерфейсов	Interface	Router(config-if)	exit

Виды командной строки:

Router> - приглашение, которое характеризует **пользовательский режим,** в котором можно просматривать некоторую статистику и проводить самые простые операции вроде пинга. Это режим для сетевого оператора, инженера первой линии техподдержки, чтобы он ничего не повредил и лишнего не узнал. Иными словами, команды в этом режиме позволяют выводить на экран информацию без смены установок сетевого устройства.

Router# - приглашение в **привилегированный режим**. Привилегированный режим поддерживает команды настройки и тестирования, детальную проверку сетевого устройства, манипуляцию с конфигурационными файлами и доступ в режим конфигурирования. Попасть в него можно, введя команду enable.

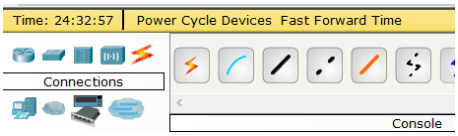
Router(config)# - приглашение в **режим глобальной конфигурации**. Он позволяет нам вносить изменения в настройки устройства. Команды режима глобального конфигурирования определяют поведение системы в целом. Активируется командой #configure terminal из привилегированного режима.

Алгоритм действий для подключения к коммутатору в программе Cisco Packet Tracert

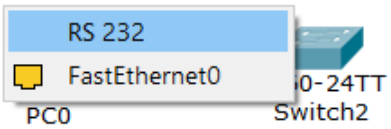
1. Подключаемся по консоли.
2. Задаем пароль на привилегированный режим.
3. Создаем пользователя.
4. Задаем авторизацию на подключение к консоли.
5. Задаем IP-адрес устройствам
6. Выбираем тип удаленного подключения (Telnet/SSH)
7. Включаем авторизацию для удаленных подключений.

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

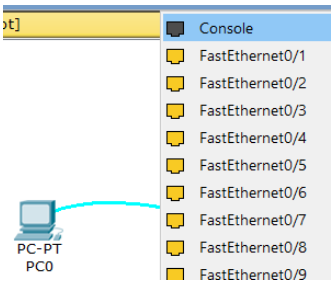
Построим простую сеть из одного компьютера и Switch (2960), соединенных консольным кабелем (рис.4 а)-в)).



а) *Выбираем консольный кабель*



б) *На компьютере выбор порта RS 232*



в) *На роутере выбор порта Console*

Рис. 4 *Топология сети с использованием консольного кабеля*

1. *Подключение к консоли*

Далее для в конфигурации компьютера PC0 выбираем Desktop/Terminal и на вкладке Terminal Configuration оставляем все по умолчанию (рис.5) и нажимаем OK. Происходит переход в окно конфигурации PC0 (рис.6).

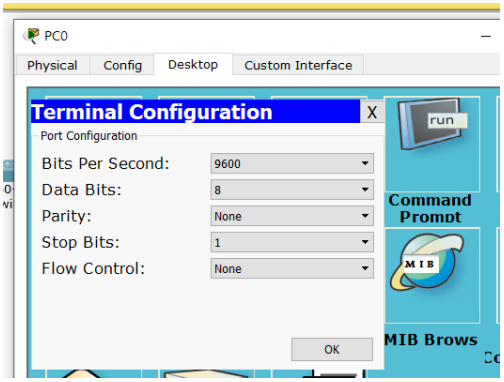


Рис. 5 *Основные параметры COM-порта*

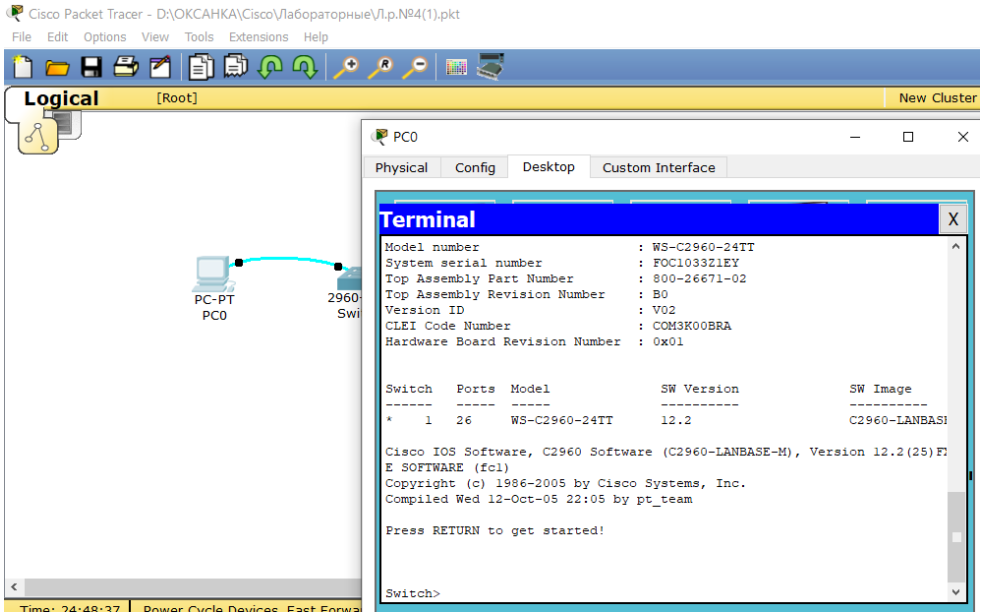


Рис. 6 *Окно конфигурации PC0*

Просмотр всех возможных команд в пользовательском режиме возможен при нажатии на «?» (рис.7).

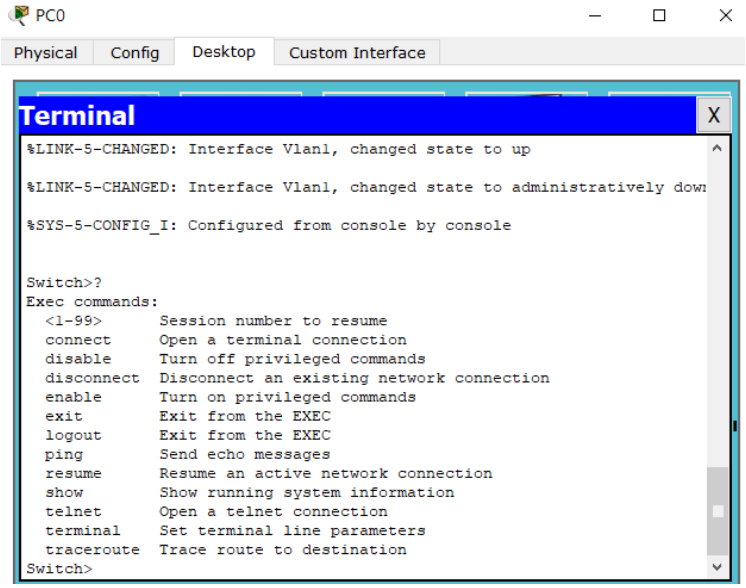


Рис. 7 *Просмотр доступных команд в пользовательском режиме*

Для перехода в привилегированней режим нажимаем Enable. Знак «#» свидетельствует о том, что это привилегированный режим (рис.8) Для выхода из этого режима

нажимаем Desable или Exit.

```
  terminal    Set terminal line parameters
  traceroute  Trace route to destination
Switch>
Switch>enable
Switch#
```

Рис. 8 *Переход в привилегированный режим*

Для просмотра всех команд в привилегированном режиме нажимаем «?» (рис.9). Видим, что их стало гораздо больше.

Terminal

```
Switch>enable
Switch#?
Exec commands:
  <1-99>      Session number to resume
  clear       Reset functions
  clock       Manage the system clock
  configure   Enter configuration mode
  connect     Open a terminal connection
  copy        Copy from one file to another
  debug       Debugging functions (see also 'undebug')
  delete      Delete a file
  dir         List files on a filesystem
  disable     Turn off privileged commands
  disconnect  Disconnect an existing network connection
  enable      Turn on privileged commands
  erase       Erase a filesystem
  exit        Exit from the EXEC
  logout      Exit from the EXEC
  more        Display the contents of a file
  no          Disable debugging informations
  ping        Send echo messages
  reload      Halt and perform a cold restart
  resume      Resume an active network connection
```

Рис. 9 *Просмотр доступных команд в привилегированном режиме*

При написании команд удобно использовать кнопку Tab, т.е. написав несколько начальных букв команды и нажав Tab, программа автоматически допишет ее в командной строке.

В привилегированном режиме можно посмотреть текущую конфигурацию устройства, набрав команду *Show running config* (или *Show run*) (рис.10).

Terminal

```
Switch>en
Switch#show ru
Switch#show running-config
Building configuration...

Current configuration : 1037 bytes
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Switch
!
!
!
!
spanning-tree mode pvst
!
interface FastEthernet0/1
!
interface FastEthernet0/2
!
interface FastEthernet0/3
!
interface FastEthernet0/4
!
interface FastEthernet0/5
!
interface FastEthernet0/6
!
interface FastEthernet0/7
!
```

Рис. 10 *Просмотр конфигурации устройства.*

Для перехода в режим глобального конфигурирования надо написать команду *Configure terminal* (или *Conf t*) (рис.11). Выход осуществляется командой **exit** или **end**.

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

Рис. 11 *Переход в режим глобального конфигурирования*

2. *Установка пароля на вход в привилегированный режим*

Для безопасности зададим пароль для входа в привилегированный режим.

Пароль доступа позволяет вам контролировать доступ в привилегированный режим от неопытных пользователей и злоумышленников. Напомним, что только в привилегированном режиме можно вносить конфигурационные изменения.

В режиме глобального конфигурирования пишем команду *Enable password Пароль* (рис.12).

```
Switch>en
Switch>enable
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#enable password cisco
Switch(config)#
```

Рис. 12 *Определение пароля для входа в привилегированный режим*

Затем после выхода в пользовательский режим, чтобы войти в привилегированный режим программа требует ввод пароля (рис.13).

```
Switch>en
Password:
```

Рис. 13 *Требование ввода пароля для входа в привилегированный режим*

Необходимо ввести пароль и только тогда возможен вход в привилегированный режим. Но такая форма определения пароля ненадежна, т.к. в привилегированном режиме при выполнении команды для просмотра текущей конфигурации Show run заданный пароль виден на экране (рис.14), т.е. хранится в открытом виде.

```
Switch#show ru
Building configuration...

Current configuration : 1061 bytes
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Switch
!
enable password cisco
!
!
!
!
spanning-tree mode pvst
!
interface FastEthernet0/1
!
```

Рис. 13 *Просмотр пароля в текущей конфигурации устройства*

Чтобы закодировать пароль надо ввести команду ***Service password-encryption*** (рис.14), которая позволит закодировать пароль (рис.15) – видно из просмотра конфигурации.

```
Switch(config)#service pass
Switch(config)#service password-encryption
```

Рис. 14 *Команда кодирования пароля*

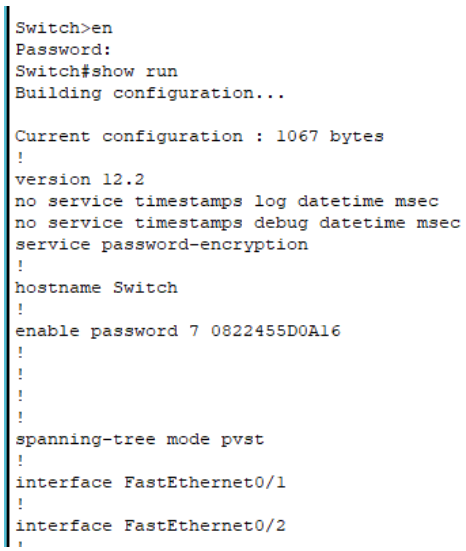


Рис. 15 *Просмотр закодированного пароля в текущей конфигурации устройства*

Из режима глобального конфигурирования можно задать сразу закодированный пароль командой ***enable secret ПАРОЛЬ***, и чтобы не переходить в привилегированный режим, а посмотреть конфигурацию сразу можно выполнить команду ***do show run*** и увидеть две строки с закодированными паролями (рис.16), причем наибольший приоритет имеет пароль, заданный командой **enable secret ПАРОЛЬ** (рис.17).

```
Switch(config)#enable secret cisco2
Switch(config)#do show run
Building configuration...

Current configuration : 1114 bytes
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname Switch
!
enable secret 5 $1$mERr$yG9qv7LLYVv0YzwRYtdTM/
enable password 7 0822455D0A16
!
!
!
!
spanning-tree mode pvst
!
interface FastEthernet0/1
!
interface FastEthernet0/2
```

Рис. 16 *Определение закодированного пароля для входа в привилегированный режим и его просмотр*

```
Switch>en
Password:
Password:
Switch#
```

Рис. 17 *Требование ввода закодированного пароля*

Для сброса пароля можно произвести перезагрузку командой ***reload*** (рис.18).

```
Switch>en
Password:
Switch#reload
Proceed with reload? [confirm]
C2960 Boot Loader (C2960-HBOOT-M) Version 12.2(25r)FX, RELEASE SOFTWARE (
Cisco WS-C2960-24TT (RC32300) processor (revision C0) with 21039K bytes o
y.
2960-24TT starting...
Base ethernet MAC Address: 0030.A390.D08D
Xmodem file system is available.
Initializing Flash...
flashfs[0]: 1 files, 0 directories
flashfs[0]: 0 orphaned files, 0 orphaned directories
flashfs[0]: Total bytes: 64016384
flashfs[0]: Bytes used: 4414921
flashfs[0]: Bytes available: 59601463
flashfs[0]: flashfs fsck took 1 seconds.
...done Initializing Flash.

Boot Sector Filesystem (bs:) installed, fsid: 3
Parameter Block Filesystem (pb:) installed, fsid: 4


Loading "flash:/c2960-lanbase-mz.122-25.FX.bin"...
###########################################################################
              Restricted Rights Legend

Use, duplication, or disclosure by the Government is
subject to restrictions as set forth in subparagraph
(c) of the Commercial Computer Software - Restricted
Rights clause at FAR sec. 52.227-19 and subparagraph
(c) (1) (ii) of the Rights in Technical Data and Computer
Software clause at DFARS sec. 252.227-7013.
```

Рис. 18 *Перезагрузка R0 командой reload*

Советы при работе с CLI

Все команды в консоли можно сокращать, но, важно, чтобы сокращение однозначно указывало на команду. Используйте клавишу **Tab** и знак вопроса (?). По нажатию Tab сокращенная команда дописывается до полной, а знак вопроса (?), следующий за командой, выводит список дальнейших возможностей и небольшую справку по ним. Можно перейти к следующей команде, сохранённой в буфере. Для этого нажмите на Стрелку вниз или **Ctrl + N**. Можно вернуться к командам, введённым ранее. Нажмите на Стрелку вверх или **Ctrl + P** (рис.19).

Рис. 19 *Стрелки Вверх или Вниз на клавиатуре позволяют листать ранее использованные вами команды*

3. Создание пользователя

Для создания пользователя, а также чтобы задать ему уровень привилегий (от 1 до 15) и пароль нужно выполнить команду из режима глобального конфигурирования (рис.20).

```
Switch(config)#username admin privilege 15 password cisco
Switch(config)#
```

Рис. 19 *Создание пользователя с уровнем привилегий и паролем*

4. Авторизация на подключение к консоли

Необходимо войти в режим конфигурирования терминальных линий. На рис.20

показано, как постепенно с помощью справок написать итоговую команду. Команда login local означает, что будет использоваться локальная база.

```
Switch(config)#line
% Incomplete command.
Switch(config)#line ?
  <0-16>   First Line number
  console  Primary terminal line
  vty      Virtual terminal
Switch(config)#line consol ?
  <0-0>  First Line number
Switch(config)#line consol 0
Switch(config-line)#login ?
  local  Local password checking
  <cr>
Switch(config-line)#login local
Switch(config-line)#
```

Рис. 20 *Конфигурирование терминльных линий*

Для выхода из всех режимов конфигураций удобно использовать команду **end.**

В итоге для перехода в привилегированный режим необходимо ввести имя пользователя и пароль (рис. 21).

```
Username: admin
Password:

Switch#
```

Рис. 21 *Ввод имени пользователя и пароля для входа в привилегированный режим*

5. Задаем IP-адреса устройствам

Первоначально смотрим имеющиеся интерфейсы. По умолчанию все коммутаторы настраиваются на логические интерфейсы Vlan1. Команда **interface Vlan1** позволяет перейти в режим конфигурирования интерфейсов и смотрим все доступные команды (рис.22).

```
Switch# show run
Building configuration...

Current configuration : 1186 bytes
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Switch
!
enable secret 5 $1$mERr$hx5rVt7rPNoS4wqbXKX7m0
!
!
!
!
username Admin privilege 15 password 0
username admin privilege 15 password 0 cisco
!
spanning-tree mode pvst
!
interface FastEthernet0/1
```

```
interface FastEthernet0/24
!
interface GigabitEthernet1/1
!
interface GigabitEthernet1/2
!
interface Vlan1
 no ip address
 shutdown
!
!
line con 0
 login local
!
line vty 0 4
 login
line vty 5 15
 login
!
!
end


Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#interface Vlan1
Switch(config-if)#?
Interface configuration commands:
  arp          Set arp type (arpa, probe, snap) or timeout
  description  Interface specific description
  exit         Exit from interface configuration mode
  ip           Interface Internet Protocol config commands
  no           Negate a command or set its defaults
  shutdown     Shutdown the selected interface
  standby      HSRP interface configuration commands
Switch(config-if)#
```

Рис. 22 *Режим конфигурирования интерфейсов*

Добавляем IP адреса и маску. Затем команда **no shutdown** поднимает интерфейс (рис.23). Далее выходим из режима конфигурирования интерфейсов.

```
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#interface Vlan1
Switch(config-if)#?
Interface configuration commands:
  arp          Set arp type (arpa, probe, snap) or timeout
  description  Interface specific description
  exit         Exit from interface configuration mode
  ip           Interface Internet Protocol config commands
  no           Negate a command or set its defaults
  shutdown     Shutdown the selected interface
  standby      HSRP interface configuration commands
Switch(config-if)#ip ?
  address         Set the IP address of an interface
  helper-address  Specify a destination address for UDP broadcasts
Switch(config-if)#ip addr
Switch(config-if)#ip address 192.168.0.1 255.255.255.0
Switch(config-if)#
```

Рис. 23 *Добавление IP адреса и поднятие интерфейса*

Настраиваем виртуальные терминальные линии

Настроим виртуальные терминальные линии, из режима глобального конфигурирования пишем команду line vty 0 4 и входим в режим конфигурирования терминальных линий (рис.24).

```
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#line
% Incomplete command.
Switch(config)#line ?
  <0-16>   First Line number
  console  Primary terminal line
  vty      Virtual terminal
Switch(config)#line vty
% Incomplete command.
Switch(config)#line vty ?
  <0-15>  First Line number
Switch(config)#line vty 0 4
Switch(config-line)#?
Virtual Line configuration commands:
  access-class  Filter connections based on an IP access list
  databits      Set number of data bits per character
  exec-timeout  Set the EXEC timeout
  exit          Exit from line configuration mode
  flowcontrol   Set the flow control
  history       Enable and control the command history function
  ipv6          IPv6 options
  logging       Modify message logging facilities
  login         Enable password checking
  motd-banner   Enable the display of the MOTD banner
  no            Negate a command or set its defaults
  parity        Set terminal parity
  password      Set a password
  privilege     Change privilege level for line
  speed         Set the transmit and receive speeds
  stopbits      Set async line stop bits
  transport     Define transport protocols for line
Switch(config-line)#
```

Рис. 24 *Режим конфигурирования терминальных линий*

Далее просматриваем возможные команды, выбираем входящий транспортный протокол **telnet**. Написав команду **transport input telnet**, сконфигурируем **telnet**. Затем зададим пароль на вход, тоже используя локальную базу **login local** (рис.25).

Настройка окончена, выходим из режима конфигурации.

```
Switch(config-line)#?
Virtual Line configuration commands:
  access-class  Filter connections based on an IP access list
  databits      Set number of data bits per character
  exec-timeout  Set the EXEC timeout
  exit          Exit from line configuration mode
  flowcontrol   Set the flow control
  history       Enable and control the command history function
  ipv6          IPv6 options
  logging       Modify message logging facilities
  login         Enable password checking
  motd-banner   Enable the display of the MOTD banner
  no            Negate a command or set its defaults
  parity        Set terminal parity
  password      Set a password
  privilege     Change privilege level for line
  speed         Set the transmit and receive speeds
  stopbits      Set async line stop bits
  transport     Define transport protocols for line
Switch(config-line)#transport ?
  input   Define which protocols to use when connecting to the terminal
  output  Define which protocols to use for outgoing connections
Switch(config-line)#transport input ?
  all     All protocols
  none    No protocols
  ssh     TCP/IP SSH protocol
  telnet  TCP/IP Telnet protocol
Switch(config-line)#transport input telnet
Switch(config-line)#login ?
  local  Local password checking
  <cr>
Switch(config-line)#login local
Switch(config-line)#
```

Рис. 25 Конфигурирование Telnet

Затем необходимо сохранить конфигурацию. Чтобы сохранить настройки используйте команду **write memory** (рис.26).

```
Switch#write memory
Building configuration...
[OK]
Switch#
```

Рис. 25 *Сохранение текущей конфигурации*

Далее проверим, как работает наша конфигурация. От компьютера к коммутатору проводим Ethernet подключение, задаем адрес компьютеру из той же сети, что и коммутатор 192.168.0.2 (рис.26).

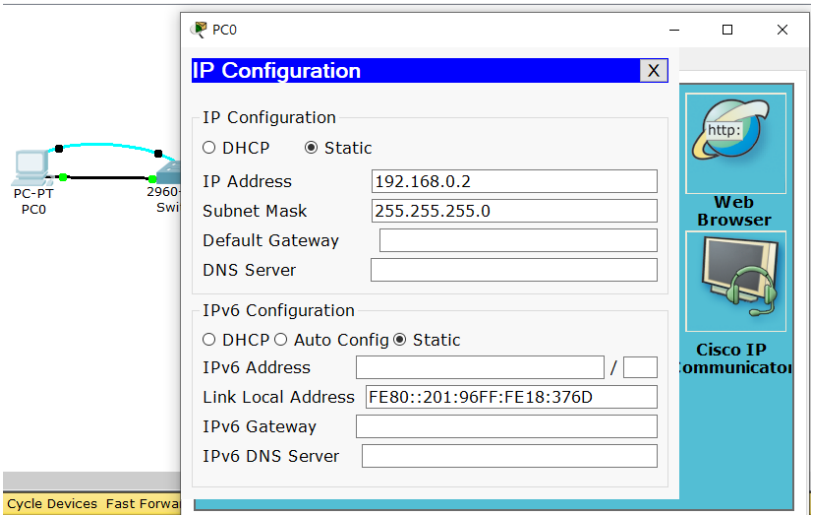
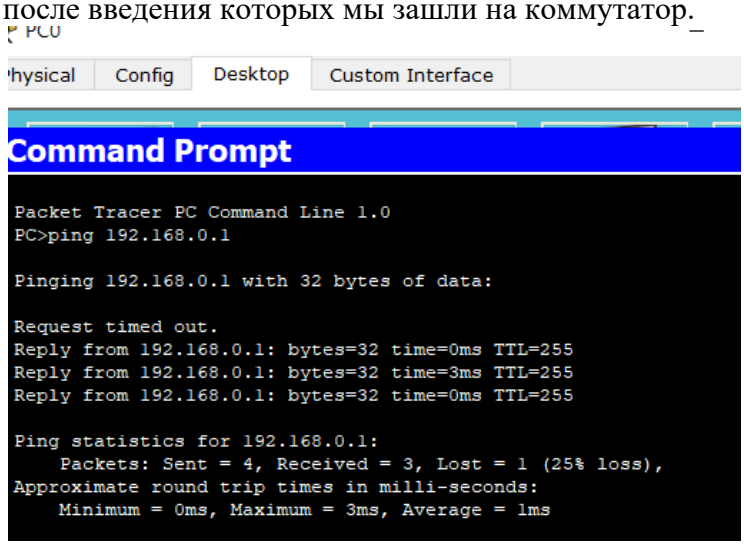


Рис. 25 *Определение адреса компьютеру*

Далее заходим в режим командной строки и пингуем коммутатор, затем выполняем команду telnet 192.168.0.1, причем коммутатор запросил аутентификационные данные: имя и пароль (рис.26), после введения которых мы зашли на коммутатор.



```
PC>telnet 192.168.0.1
Trying 192.168.0.1 ...Open


User Access Verification

Username: admin
Password:
% Login invalid

Username: admin
Password:
Switch#

[Connection to 192.168.0.1 closed by foreign host]
PC>
```

Рис. 26 *Выполнение коиманд со стороны ПК*

К коммутатору можно подключиться также, используя функционал программы Cisco Packet Tracer (рис.27).

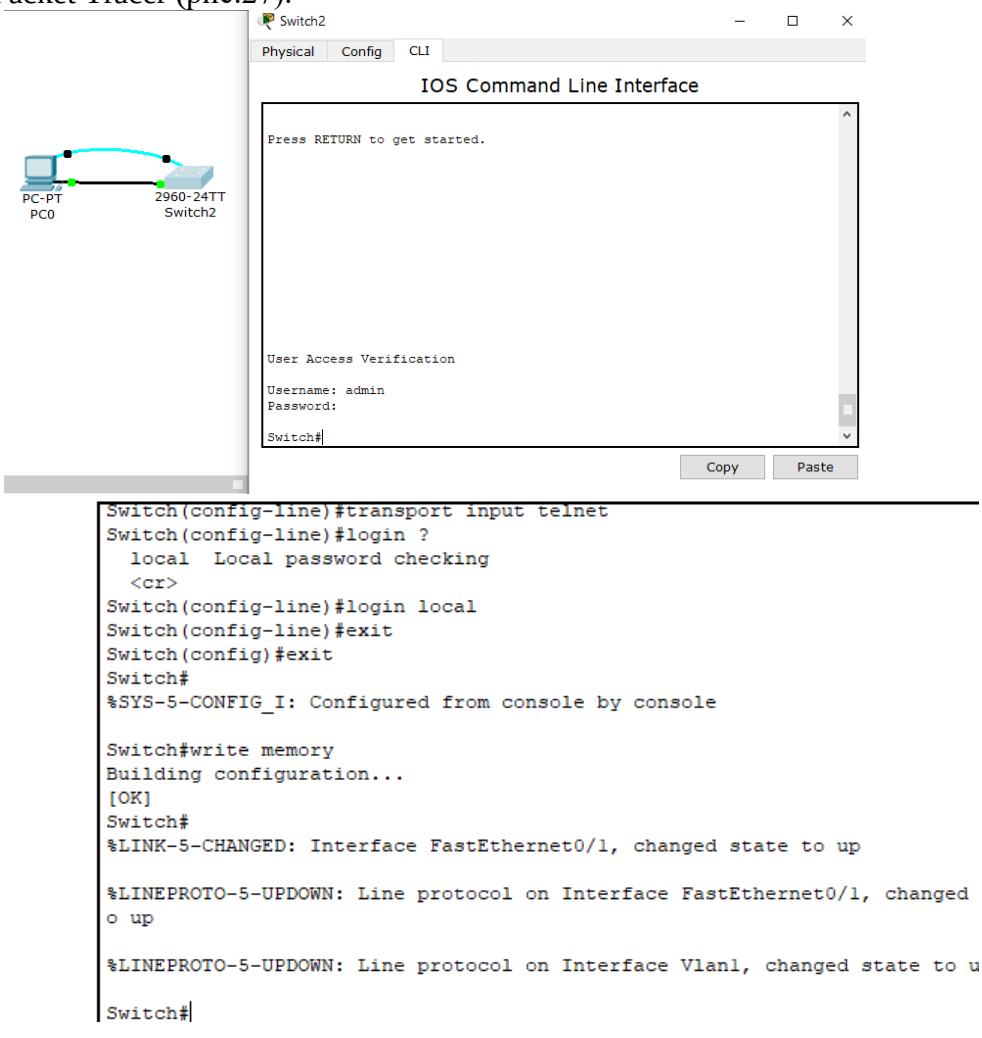


Рис. 27 *Интерфейс командной строки для коммутатора*

Практическая часть

Построим топологию с двумя сетями, с двумя рабочими станциями в каждой подсетке. Первоначально линки от ПК к коммутаторам согласованы, а между коммутаторами и роутером нет, т.к. у роутера интерфейсы не подняты (рис.28).

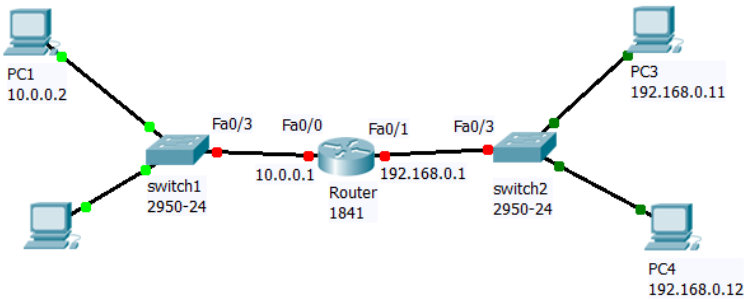


Рис.28 Первоначальная топология сети

Перед началом поднятия интерфейсов необходимо выполнить команду, чтобы маршрутизатор игнорировал неправильно введенные команды, т.к. маршрутизатор будет воспринимать все неверные команды, как доменные имена, будет обращаться к DNS серверу, все это потребует времени и будет казаться, что маршрутизатор «висит»:

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

Поднимем интерфейс FastEthernet0/0 роутера в левой подсети, а также зададим адрес 10.0.0.1.

Continue with configuration dialog? [yes/no]: n
Press RETURN to get started!
Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#int fa
*Router(config)#**int fastEthernet 0/0***
*Router(config-if)#**no sh***
Router(config-if)#
*%LINK-5-CHANGED: Interface FastEthernet0/0, changed state **to up***
*%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state **to up***
Router(config-if)#ip adr
Router(config-if)#ip addr
*Router(config-if)#**ip address 10.0.0.1 255.0.0.0***

Аналогично поднимем интерфейс FastEthernet0/1 роутера в правой подсети, а также зададим адрес 192.168.0.1.

*Router(config)#**int fastEthernet 0/1***
*Router(config-if)#**no sh***
Router(config-if)#
*%LINK-5-CHANGED: Interface FastEthernet0/1, changed state **to up***
*%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state **to up***
Router(config-if)#ip addr
*Router(config-if)#**ip address 192.168.0.1 255.255.255.0***

В итоге интерфейсы подняты и загораются зеленые линки (рис.29)

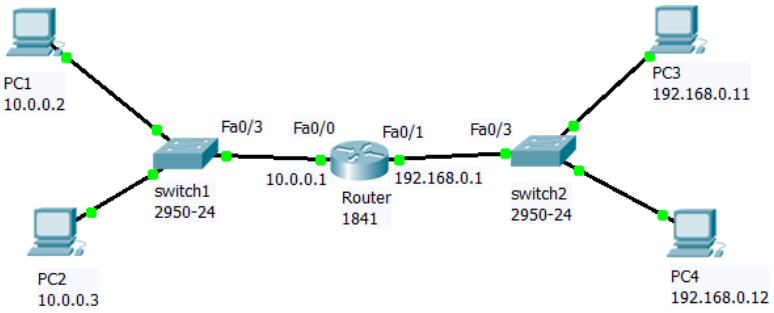


Рис.29 Топология сети с поднятыми интерфейсами

Таблицу маршрутизации можно посмотреть с помощью команды *sh ip route:*

*Router#**sh 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 not set
C 10.0.0.0/8 is directly connected, FastEthernet0/0
C 192.168.0.0/24 is directly connected, FastEthernet0/1

Из этого листинга программы видны подсети и интерфейсы.

Далее необходимо назначить IP адреса компьютерам в левой подсети (рис.30).

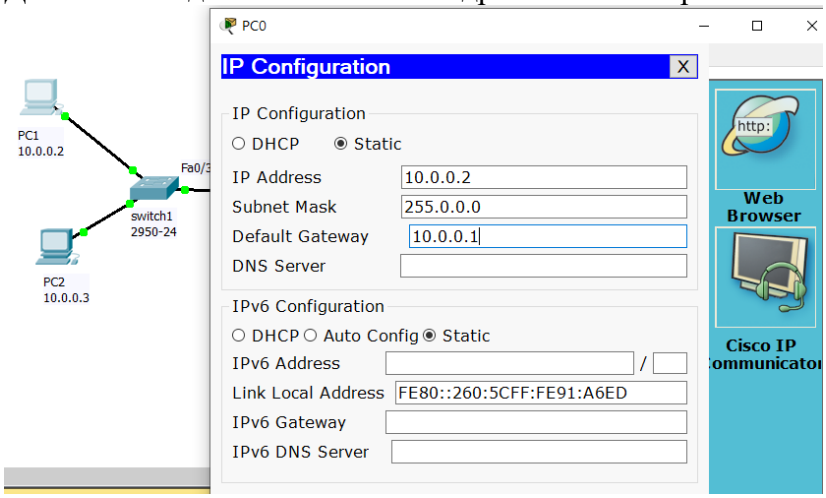


Рис.30 Назначение адреса для PC1

Аналогично для ПК2 зададим адресацию (рис.31).

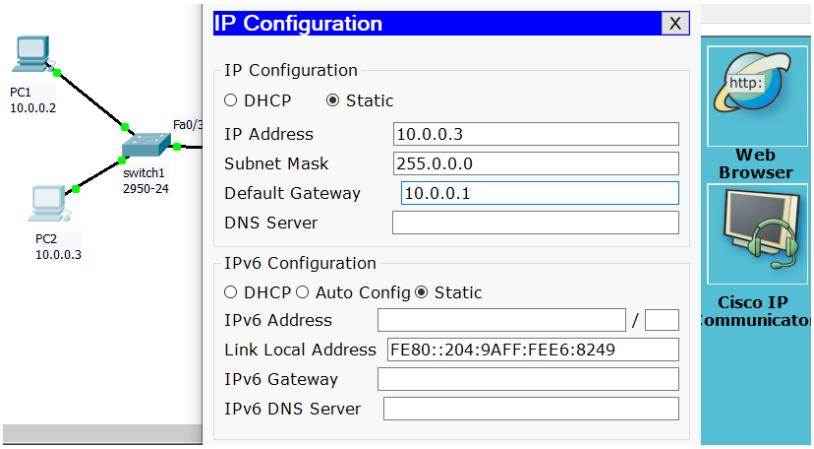


Рис.31 Назначение адреса для PC2

Далее для компьютеров в правой подсетке зададим адресацию с помощью DHCP сервера, который автоматически назначает IP адреса.

Router(config)#ip dhcp pool

Router(config)#ip dhcp pool ?

WORD Pool name

*Router(config)#**ip dhcp pool home*** – создание *DHCP* пула с именем *home*

Router(dhcp-config)#net

*Router(dhcp-config)#**network 192.168.0.0 255.255.255.0*** – определение сети

Router(dhcp-config)#defa

*Router(dhcp-config)#**default-router 192.168.0.1*** – определение роутера

Router(dhcp-config)#exit

Router(config)#ip dh

Router(config)#ip dhcp ex

*Router(config)#**ip dhcp excluded-address 192.168.0.1 192.168.0.10*** – диапазон адресов исключенных из автоматического распределения, где первый адрес принадлежит роутеру, поэтому ПК должны иметь адреса, начиная с 192.168.0.11.

Далее проверим, как произошло распределение адресов (рис.32) – заходим на PC3 на вкладку *IP Configuration* и включаем DHCP.

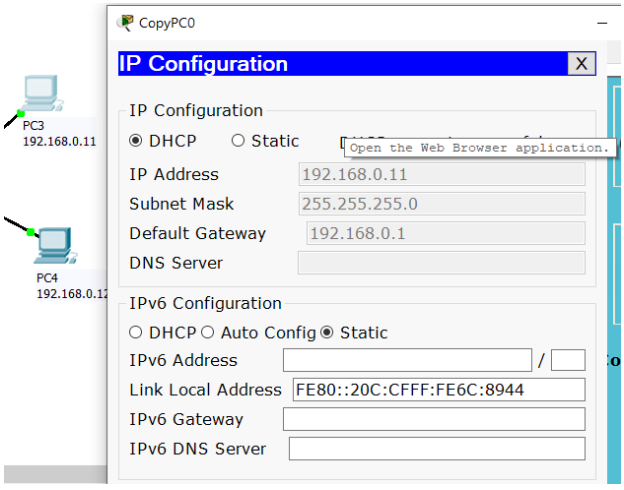


Рис. 32 Адресация для PC3

Аналогично проверьте и для PC4 (рис.33).

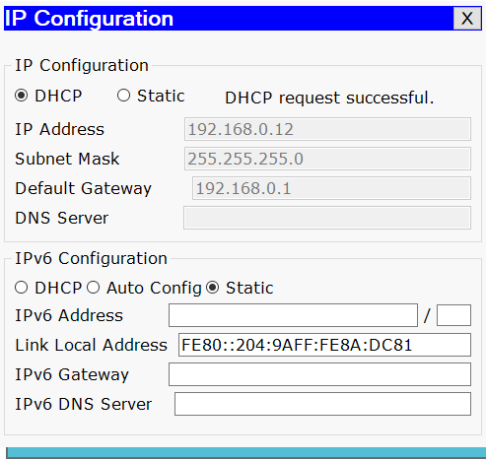


Рис.33 Адресация для PC4

Далее проверим, как работает вся сеть, попингуем разные компьютеры (рис.34).

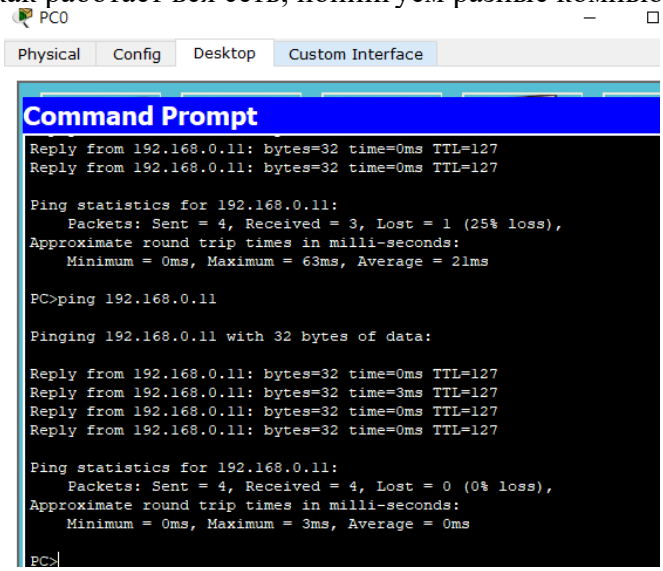


Рис. 34 Выполнение программы ping

Чтобы получить информацию о всех ПК с адресами, распределенными DHCP сервером выполним:

Router>en

Router#sh ip dhcp b

*Router#**sh ip dhcp binding***

IP address	*Client-ID/ Hardware address*	*Lease expiration*	*Type*
192.168.0.11	***000C.CF6C.8944***	*--*	***Automatic***
192.168.0.12	***0004.9A8A.DC81***	*--*	***Automatic***

Далее, используя вкладку роутера Global Settings, возможно всю конфигурацию сети из эмулятора загрузить на реальные устройства и наоборот, используя кнопки Load и Export (рис.35).

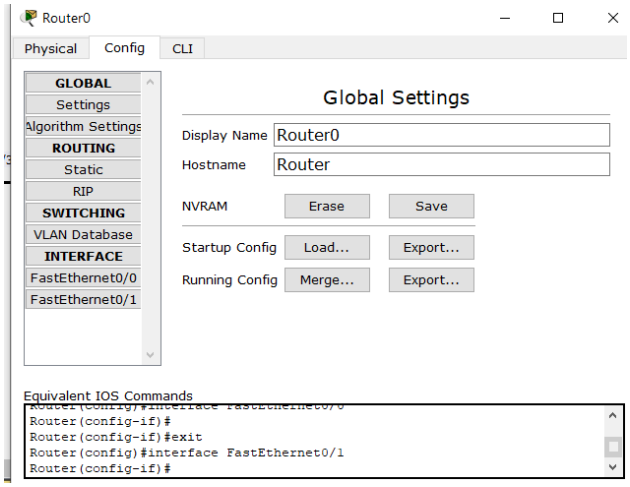


Рис.35 Вкладка роутера Global Settings

Все настройки конфигурации сети сохраняются в Running Config (аналог оперативной памяти) (рис.35), поэтому в случае отключения электропитания они исчезают, следовательно необходимо сохранять настройки в Startup Config при помощи команды ***do wr***:

Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
*Router(config)#**do wr***
Router(config)#do wr
Building configuration...
[OK]

На вкладках FastEthernet можно посмотреть прописанные адреса, маски, а в нижней части команды (рис.36).

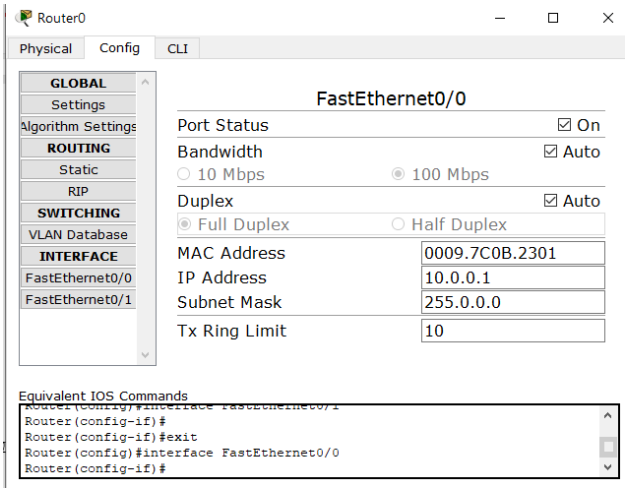


Рис.36 Вкладка роутера Config INTERFACE

Всю последовательность действий в командной строке можно посмотреть с помощью команды **sh run:**

*Router#**sh run***
Building configuration...
Current configuration : 639 bytes
version 12.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption

```
hostname Router
ip dhcp excluded-address 192.168.0.1 192.168.0.10
ip dhcp pool home
 network 192.168.0.0 255.255.255.0
 default-router 192.168.0.1
spanning-tree mode pvst
interface FastEthernet0/0
 ip address 10.0.0.1 255.0.0.0
 duplex auto
 speed auto
interface FastEthernet0/1
 ip address 192.168.0.1 255.255.255.0
 duplex auto
 speed auto
interface Vlan1
 no ip address
 shutdown
ip classless
line con 0
line aux 0
line vty 0 4
login
end
```

Задание для самостоятельной работы

1. Создайте топологию, аналогичную топологии на рис. 29, только к каждому свитчу присоедините не менее трех ПК.
2. Измените имена коммутаторам и роутеру.
3. Обеспечить парольный доступ к привилегированному режиму, используя три возможности формирования паролей (*Enable password Пароль, Service password-encryption, enable secret ПАРОЛЬ***)** и объясните в чем их отличия.
4. Назначьте компьютерам адреса, вручную для левой подсети, согласно варианту 10.0.v.2 - 10.0.v.n (v=1-25). Для правой подсети создайте автоматическое распределение IP адресов с помощью DHCP-сервера: 192.168.v.11 - 192.168.v.n (v=1-25). Нумерация компьютеров для каждого студента уникальна и соответствует номеру студента (v) в списке преподавателя. Например, для варианта 7 (v=7) и компьютера PC1 имеем IP ADDRESS 10.0.7.2, а для PC3 192.168.7.11.
5. Назначьте компьютерам имена, соответствующие их IP адресам, лишние надписи уберите.
6. Поднимите интерфейсы и задайте IP адресацию для роутера в левой и правой подсети.
7. Если сделано всё правильно, то вы сможете пропинговать любой компьютер из любого компьютера – проверьте это.
8. Проверьте действие команд ***sh ip dhcp binding, do wr, sh run*** и объясните их назначение.
9. Запустите процесс симуляции движения пакетов от источника информации к получателю, отфильтруйте протоколы для режима симуляции.
10. Пригласите преподавателя и покажите результат работы.

Лабораторная работа №5 Введение в межсетевую операционную систему IOS компании Cisco

Тема работы: Введение в межсетевую операционную систему IOS компании Cisco.

Цель работы: знакомство с сетевыми устройствами Cisco, конфигурация интерфейсов, настройка IP адресов интерфейсов, применение команды telnet.

Теоретическая часть.

Домашние сети, как правило, соединяют широкий спектр оконечных устройств, включая ПК, ноутбуки, планшетные компьютеры, смартфоны, PlayStation 3, а также многие другие устройства.

Все эти оконечные устройства обычно подключаются к домашнему маршрутизатору. Домашние маршрутизаторы — это фактически четыре устройства в одном:

Маршрутизатор - передает и получает пакеты данных из сети Интернет

Коммутатор - соединяет оконечные устройства с помощью сетевых кабелей

Точка беспроводного доступа - состоит из радиопередатчика, который осуществляет беспроводное соединение оконечных устройств

Устройство межсетевого экрана - защищает исходящий и запрещает входящий трафик.

В крупных корпоративных сетях со значительно большим количеством устройств и объёмным трафиком эти устройства часто функционируют как независимые, автономные устройства, обеспечивающие специализированное обслуживание. Оконечные устройства, такие как ПК и ноутбуки, подключаются к сетевым коммутаторам с помощью проводных соединений. Чтобы отправлять пакеты за пределы локальной сети, сетевые коммутаторы подключаются к маршрутизаторам сети. Беспроводные точки доступа и выделенные устройства обеспечения безопасности, например, межсетевой экран — это другие устройства инфраструктуры, находящиеся в сети.

Оборудование, назначение и возможности каждого устройства значительно отличаются. Но в любом случае функционировать устройствам позволяет именно операционная система.

Операционные системы используются на всех оконечных и сетевых устройствах, подключённых к сети Интернет. Устройства конечных пользователей — это смартфоны, планшетные компьютеры, ПК и ноутбуки. Сетевые или промежуточные устройства — это устройства, используемые для передачи данных по сети, а также коммутаторы, маршрутизаторы, точки беспроводного доступа и межсетевые экраны. Операционную систему на сетевом устройстве называют сетевой операционной системой.

Операционная система сетевого взаимодействия Cisco (IOS) — это общий термин для группы сетевых операционных систем, используемых на сетевых устройствах Cisco. Операционная система Cisco IOS используется в большинстве устройств Cisco, независимо от их типа и размеров.

При первом входе в сетевое устройство пользователь видит командную строку пользовательского режима вида: Switch>.

Команды, доступные на пользовательском уровне являются подмножеством команд, доступных в привилегированном режиме. Эти команды позволяют выводить на экран информацию без смены установок сетевого устройства. Чтобы получить доступ к полному набору команд, необходимо сначала активизировать привилегированный режим. Press ENTER to start.

Switch>
Switch> **enable**
Switch#

Switch# **disable**
Switch>

О переходе в этот режим будет свидетельствовать появление в командной строке приглашения в виде знака #. Из привилегированного уровня можно получать информацию о настройках системы и получить доступ к режиму глобального конфигурирования и других специальных режимов конфигурирования, включая режимы конфигурирования интерфейса, подинтерфейса, линии, сетевого устройства, карты маршрутов и т.п.

Для выхода из системы IOS необходимо набрать на клавиатуре команду *exit* (выход).

Switch> *exit*

Пользовательский режим — это режим просмотра, в котором пользователь может только просматривать определённую информацию о сетевом устройстве, но не может ничего менять. В этом режиме приглашение имеет вид типа ***Switch>***.

Привилегированный режим — поддерживает команды настройки и тестирования, детальную проверку сетевого устройства, манипуляцию с конфигурационными файлами и доступ в режим конфигурирования. В этом режиме приглашение имеет вид типа ***Switch#***.

Режим глобального конфигурирования — реализует мощные однострочные команды, которые решают задачи конфигурирования. В этом режиме приглашение имеет вид типа ***Switch (config) #***.

Команды в любом режиме IOS распознаёт по первым уникальным символам. При нажатии табуляции IOS сам дополнит команду до полного имени. При вводе в командной строке любого режима имени команды и знака вопроса (*?*) на экран выводятся комментарии к команде.

При вводе одного знака результатом будет список всех команд режима. На экран может выводиться много экранов строк, поэтому иногда внизу экрана будет появляться подсказка - More -. Для продолжения следует нажать enter или пробел. Чтобы не просматривать все строки можно нажать Q. Команды режима глобального конфигурирования определяют поведение системы в целом.

Кроме этого, команды режима глобального конфигурирования включают команды перехода в другие режимы конфигурирования, которые используются для создания конфигураций, требующих многострочных команд. Для входа в режим глобального конфигурирования используется команда привилегированного режима **configure**.

При вводе этой команды следует указать источник команд конфигурирования: **terminal** (терминал), **memory** (энергонезависимая память или файл), **network** (сервер tftp (Trivial ftp -упрощённый ftp) в сети). Например

Switch# configure terminal
Switch(config)#(commands)
Switch(config)# exit
Switch#

Команды для активизации частного вида конфигурации должны предваряться командами глобального конфигурирования. Так для конфигурации интерфейса, на возможность которой указывает приглашение Switch(configif)#, сначала вводится глобальная команда для определения типа интерфейса и номера его порта:

Switch# conf t
Switch(config)# interface type port
Switch(config-if)# ***(commands)***
Switch(config-if)# exit
Switch(config)# exit

Для ограничения доступа к системе используются пароли. Команда *line console* устанавливает пароль на вход на терминал консоли:

Switch (config)# line console 0
Switch (config-line)# login

Switch (config-line)# password Cisco
Команда line vty 0 4 устанавливает парольную защиту на вход по протоколу Telnet:
Switch (config)# line vty 0 4
Switch (config-line)# login
Switch (config-line)# password cisco
Команда enable password ограничивает доступ к привилегированному режиму:
Switch#conf t
Switch(config)# enable password пароль
Далее Ctrl-Z
Switch#ex
…
Press RETURN to get started
Switch>en
Password: пароль
Switch#
Здесь пароль *пароль* – последовательность латинских символов.
Для установки на сетевом интерфейсе IP адреса используется команда*:*
Router(config-if)#*ip address* [ip-address] [subnet-mask].

Важно иметь возможность контроля правильности функционирования и состояния сетевого устройства в любой момент времени. Для этого служат команды, представленные в таблице 1.

Таблица 1.

Команда	Описание
show version	Выводит на экран данные о конфигурации аппаратной части системы, версии программного обеспечения, именах и источниках конфигурационных файлов и загруженных образах
show running-conf ig	Показывает содержание активной конфигурации
show interfaces	Показывает данные обо всех интерфейсах на устройстве
show protocols	Выводит данные о протоколах третьего сетевого уровня.

Cisco Discovery Protocol (CDP)

CDP позволяет устройствам обмениваться основной конфигурационной информацией. CDP будет работать без настройки какого-нибудь протокола. По умолчанию, CDP включен на всех интерфейсах.

CDP работает на втором (канальном) уровне модели OSI. Поэтому CDP не является маршрутизируемым 14 протоколом и работает только с непосредственно подключенными устройствами. Протокол CDP связывает физическую среду передачи данных более низкого уровня с протоколами более высокого сетевого уровня. Поэтому устройства, поддерживающие разные протоколы третьего уровня, могут узнавать друг друга.

При запуске устройства протокол CDP запускается автоматически. Поле этого он может автоматически определить соседние устройства, на которых также выполняется протокол CDP. Среди найденных устройств будут не только те, которые работают с протоколом IP. CDP позволяет администраторам иметь доступ к данным о другом сетевом устройстве, к которому есть непосредственное соединение.

Для вывода информации о соседних устройствах, обнаруженных по протоколу CDP, используется семейство команд *show cdp neighbors.* Оно выводит следующие данные по каждому порту и каждому подсоединённому к нему устройству: идентификаторы устройства, список адресов, идентификатор порта, перечень функциональных возможностей, аппаратная платформа устройства.

Команды ping и traceroute.

Для диагностики возможности установления связи в сетях используются протоколы тип запрос-ответ или протокол эхо-пакетов. Результаты роботы такого протокола могут помочь в оценке надёжности пути к другому устройству, величин задержек в целом и между промежуточными устройствами. Для того чтобы такая команда работала, необходимо, чтобы не только локальное сетевое устройство знало, как попасть в пункт назначения, но и чтобы устройство в пункте назначения знало, как добраться до источника.

Команда ***ping*** посылает *ICMP (Internet Control Message Protocol)* эхо-пакеты для верификации соединения. В приведённом ниже примере время прохождения одного эхо-пакета превысило заданное, о чём свидетельствует точка (.) в выведенной информации, а четыре пакета прошли успешно, о чём говорит восклицательный знак (!). Результаты команды *ping* приведены в таблице 2.

Switch> *ping 172.16.101.1*
Type escape sequence to abort.
Sending 5 100-byte ICMP echoes to 172.16.10.1 timeout is 2 seconds:
.!!!!
Success rate is 80 percent, round-trip min/avg/max = 6/6/6

Таблица 2. Результаты команды ping

Символ	Значение
!	Успешный приём эхо-ответа
.	Превышено время ожидания
U	Пункт назначения недосягаем
C	Перегрузка сети
I	Выполнение команды прервано администратором
?	Неизвестный тип пакета
&	Пакет превысил значение параметра времени жизни TTL пакета

Команды ***traceroute*** показывает адреса промежуточных интерфейсов (хопов) на пути пакетов в пункт назначения.

Switch> traceroute 172.16.101.1

Расширенная версия команды ping поддерживается только в привилегированном режиме. Для того, чтобы войти в расширенный режим, необходимо в строке подсказки Extended commands ввести букву "y"(Yes) Команда в режиме диалога опрашивает значения параметров. Важно отметить, что эта команда позволяет, находясь на одном устройстве, проверять связь между сетевыми интерфейсами на других устройствах.

Router# ping
Protocol [ip]:
Target IP address: 2.2.2.2
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address:1.1.1.1
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data [no]:

Data pattern [OxABCD]:
Loose, Strict, Record, Timestamp, Verbose [none]:
Sweep range of sizes [n]:

Команда telnet.

Протокол виртуального терминала *telnet*, входящий в состав протоколов TCP/IP, позволяет установить соединение между сетевым устройством *telnet* клиента и сетевым устройством *telnet* сервера, что обеспечивает возможность работы в режиме виртуального терминала. *Telnet* используется для удалённого управления сетевым устройством либо для проверки связи на уровне приложений. Успешное установление *Telnet*-соединения позволяет вам управлять удалённым устройством так, как будто вы находитесь за его консолью.

Сетевые устройства *Cisco* способны поддерживать одновременно до пяти входных сеансов протокола *Telnet*.

Основные команды сетевого устройства

Чтобы увидеть список всех доступных команд введите «?».

Router>?

Клавишу *Enter* нажимать не надо.

Теперь войдите в привилегированный режим.

Router>enable
Router#

Просмотрите список доступных команд в привилегированном режиме.

Router#?

Перейдём в режим глобальной конфигурации.

Router#config terminal или *conf t*
Router(config)#

Имя хоста сетевого устройства используется для локальной идентификации. Когда вы входите в сетевое устройство, вы видите *Имя хоста* перед символом режима (">" или "#"). Задать имя сетевому устройству *"Router1"* можно, используя следующую команду.

Router(config)#hostname Router1
Router1(config)#

Основные Show команды.

Перейдите в пользовательский режим командой *disable*. Введите команду для просмотра всех доступных *show* команд.

*Router1>**show ?***
arp Arp table
cdp CDP information
class-map Show QoS Class Map
clock Display the system clock
controllers Interface controllers status
crypto Encryption module
flash: display information about flash: file system
frame-relay Frame-Relay information
history Display the session command history
hosts IP domain-name, lookup style, nameservers, and host table
interfaces Interface status and configuration
ip IP information
policy-map Show QoS Policy Map
privilege Show current privilege level
protocols Active network routing protocols
queue Show queue contents

queueing Show queueing configuration
sessions Information about Telnet connections
ssh Status of SSH server connections
tcp Status of TCP connections
terminal Display terminal configuration parameters
users Display information about terminal lines
version System hardware and software status

Например,

Router1>show clock
**1:41:39.618 UTC Mon Mar 1 1993*

Команда ***show version*** используется для получения типа платформы сетевого устройства, версии операционной системы, имени файла образа операционной системы, время работы системы, объём памяти, количество интерфейсов и конфигурационный регистр.

Можно увидеть часы

*Router1>**show clock***

Во флеш-памяти сетевого устройства сохраняется файл-образ операционной системы *Cisco IOS*. В отличие от оперативной памяти, в реальных устройствах флеш память сохраняет файл-образ даже при сбое питания.

*Router1>**show flash***

ИКС сетевого устройства по умолчанию сохраняет 10 последних введенных команд

*Router1>**show history***

Две команды позволят вам вернуться к командам, введённым ранее. Нажмите на стрелку вверх или *<ctrl> P*.

Две команды позволят вам перейти к следующей команде, сохранённой в буфере. Нажмите на стрелку вниз или *<ctrl> N*.

Можно увидеть список хостов и *IP*-Адреса всех их интерфейсов

*Router1>**show hosts.***

Следующая команда выведет детальную информацию о каждом интерфейсе

*Router1>**show interfaces***

Команда выведет информацию о каждой *telnet* сессии.

*Router1>**show sessions***

Команда показывает конфигурационные параметры терминала.

*Router1>**show terminal***

Можно увидеть список всех пользователей, подсоединённых к устройству по терминальным линиям

*Router1>**show users***

Команда показывает состояние контроллеров интерфейсов.

*Router1>**show controllers***

Перейдём в привилегированный режим.

Router1>en

Введите команду для просмотра всех доступных *show* команд.

Router1#show ?

Привилегированный режим включает в себя все show команды пользовательского режима и ряд новых.

Посмотрим активную конфигурацию в памяти сетевого устройства. Необходим привилегированный режим. Активная конфигурация автоматически не сохраняется и будет потеряна в случае сбоя электропитания.

*Router1**#show running-config***

В строке *more,* нажмите на клавишу пробел для просмотра следующей страницы информации.

Следующая команда позволит вам увидеть текущее состояние протоколов третьего уровня.

*Router#**show protocols***

Практическая часть

Построим сеть (рис.1). Далее сконфигурируем интерфейсы, настроим IP адреса и проверим доступность разных сетей из каждого устройства.

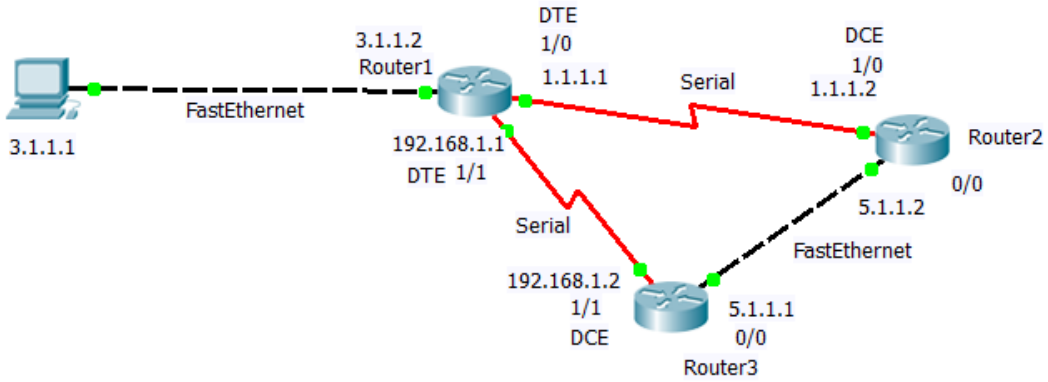


Рис.1 Топология сети

Добавляем три роутера 2621XM (рис.2).

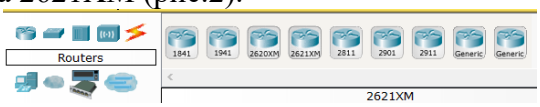


Рис.2

Далее ко всем роутерам подключаем порты: вначале отключаем роутер, далее подключаем порт NM-4A/S, затем включаем роутер (рис.3,4). Это необходимо сделать, чтобы использовать последовательное соединение Serial между роутерами.

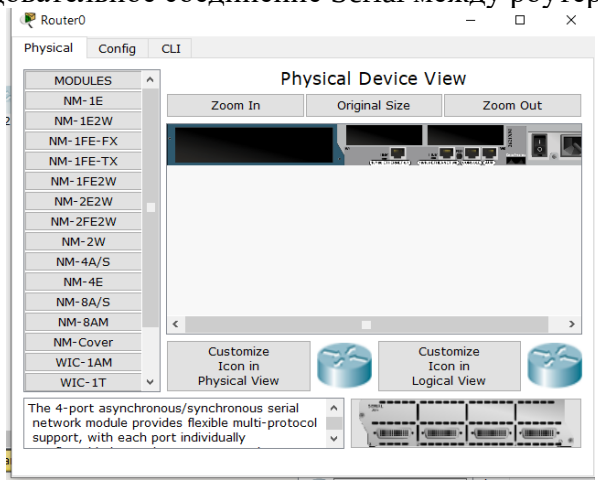


Рис.3

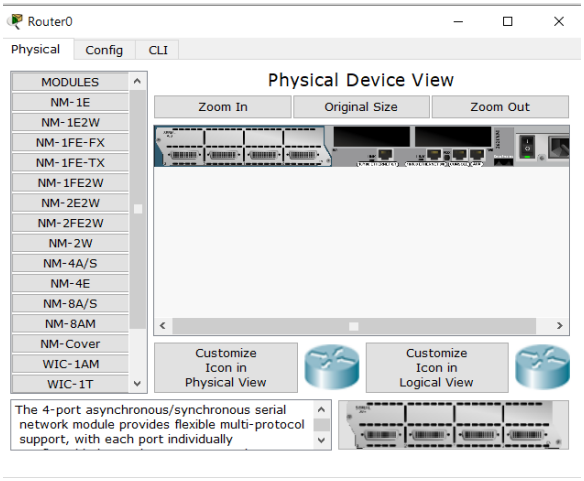


Рис.4

Роутер 1 и роутер 2 соединим последовательным соединением Serial DTE (рис.5).

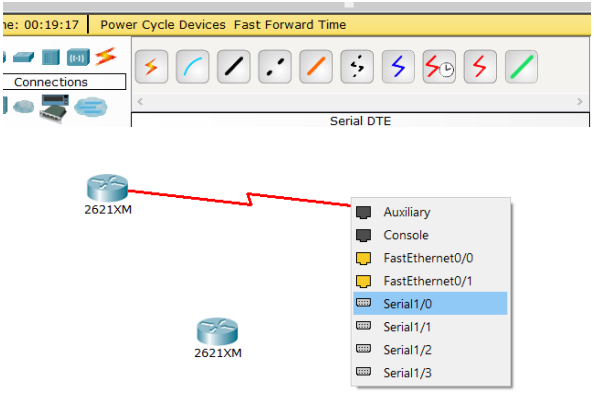


Рис.5

Аналогично соединим роутер 1 и роутер 3 (рис.6).

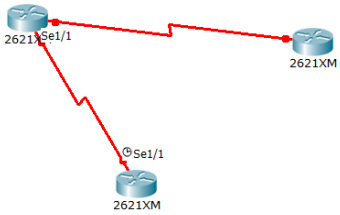


Рис.6

Роутер 2 и роутер 3 соединим кроссовым кабелем (рис.7).

Имеется 2 вида витой пары. Прямой (Straight-Through) и кроссовый (Cross-over). Прямой применяется, когда нужно соединить 2 разных устройства. Например, компьютер и коммутатор. А кроссовый — когда нужно соединить 2 компьютера, 2 коммутатора, компьютер и роутер и т.д. Структурное различие в том, что пары проводов обжимаются по-разному.

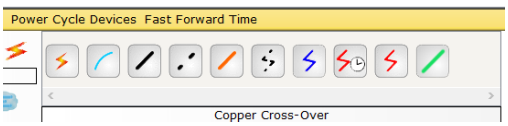


Рис.7

Обратите внимание на интерфейсы и напишите их на топологии, также добавьте названия роутеров, используя кнопку надпись (рис.8)

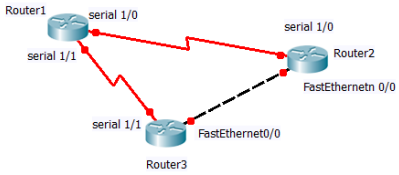


Рис.8

Далее переходим в командную строку и начинаем использовать разные команды для конфигурации сети.

Первоначально необходимо из режима глобальной конфигурации переименовать роутеры.

Заходим на первый роутер, нажимаем *no* при первом предложении системы к диалогу, заходим в режим привилегированный, а затем в режим глобальной конфигурации. Для переименования используем команду *hostname Router1* (рис.9).

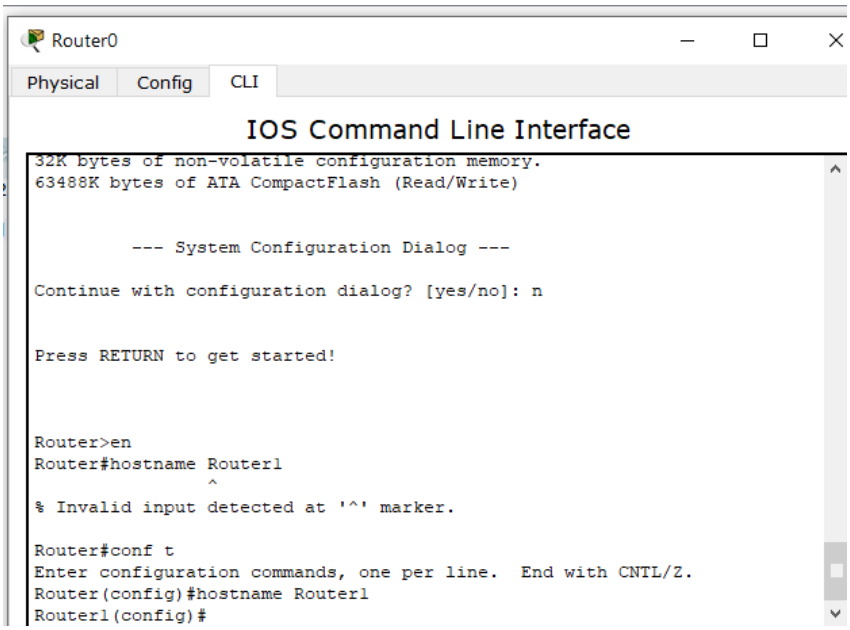


Рис.9

Аналогично переименуем второй роутер.

Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
*Router(config)#**hostname Router2***
Router2(config)#

Далее необходимо поднять интерфейсы. Чтобы поднять последовательные интерфейсы необходимо проверить каким является роутер оконечным (DTE) или устройством связи (DCE).

Перейдём к конфигурации последовательных интерфейсов. Зайдём на *Router1*. Проверим, каким устройством выступает наш маршрутизатор для последовательной линии связи: оконечным устройством *DTE (data terminal equipment)* либо устройством связи *DCE (data circuit)* и выполним команду *show controllers serial 1/0.*

Для Router1 проверим:

Router1#sh
Router1#show con
Router1#show controllers ser
*Router1#**show controllers serial 1/0***

Interface Serial1/0
Hardware is PowerQUICC MPC860
***DTE** V.35 TX and RX clocks detected*
idb at 0x81081AC4, driver data structure at 0x81084AC0
SCC Registers:
General [GSMR]=0x2:0x00000000, Protocol-specific [PSMR]=0x8
Events [SCCE]=0x0000, Mask [SCCM]=0x0000, Status [SCCS]=0x00
…….

Если видим **DTE**, то далее поднимаем интерфейс на роутере 1.
Router1# conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router1(config)#in
Router1(config)#interface s
*Router1(config)#**interface serial 1/0***
Router1(config-if)#no sh
*Router1(config-if)#**no shutdown*** – команда для поднятия интерфейса
Router1(config-if)#
*%LINK-5-CHANGED: Interface Serial1/0, changed state **to up***

То, что интерфейс поднят подтверждают слова *changed state **to up**.*
Задаем адресацию для роутера 1, согласно рис.1.
Router1(config-if)#ip ad
*Router1(config-if)#**ip address 1.1.1.1 255.0.0.0***

Далее аналогично проверим на роутере 2 каким является интерфейс serial 1/0.
Router2#sh con se
Router2#sh con serial 1/0
Interface Serial1/0
Hardware is PowerQUICC MPC860
***DCE** V.35, clock rate 64000*
idb at 0x81081AC4, driver data structure at 0x81084AC0
SCC Registers:
General [GSMR]=0x2:0x00000000, Protocol-specific [PSMR]=0x8
Events [SCCE]=0x0000, Mask [SCCM]=0x0000, Status [SCCS]=0x00
Transmit on Demand [TODR]=0x0, Data Sync [DSR]=0x7E7E
Interrupt Registers:
Config [CICR]=0x00367F80, Pending [CIPR]=0x0000C000
Mask [CIMR]=0x00200000, In-srv [CISR]=0x00000000
Command register [CR]=0x580
Port A [PADIR]=0x1030, [PAPAR]=0xFFFF
[PAODR]=0x0010, [PADAT]=0xCBFF

Если видим - ..... *DCE* ....., то наш маршрутизатор является устройством связи, и он должен задавать частоту синхронизации тактовых импульсов, используемых при передаче данных. Частота берётся из определённого ряда частот.
Router2#en
Router2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router2(config)#int ser1/0
*Router2(config)#**int ser1/0***
Router2(config-if)#cloce rate?

% Unrecognized command
Router2(config-if)#cloc
Router2(config-if)#clock ra
*Router2(config-if)#**clock rate ?***
Speed (bits per second
1200
2400
4800
9600
19200
38400
56000
64000
72000
125000
128000
148000
250000
500000
800000
1000000
1300000
2000000
4000000
<300-4000000> Choose clockrate from list above
*Router2(config-if)#**clock rate 64000***

Далее в этом же режиме конфигурирования интерфейсов поднимаем интерфейс и задаем IP адрес – пишется адрес и через пробел маска.

*Router2(config-if)#**no shutdown***
Router2(config-if)#ip ad
*Router2(config-if)#**ip address 1.1.1.2 255.0.0.0***

Аналогично поднимаем интерфейсы и задаем адресацию для Serial интерфейсов на роутере 1, роутере 2 и роутере 3.

Router1(config)#int ser1/1
Router1(config-if)#ip addr
*Router1(config-if)#**ip address 192.168.1.1 255.255.255.0***

Router3(config)#int ser1/1
Router3(config-if)#ip addr
*Router3(config-if)#**ip address 192.168.1.2 255.255.255.0***

В итоге интерфейсы *Serial* должны загореться зелеными индикаторами (рис.10).

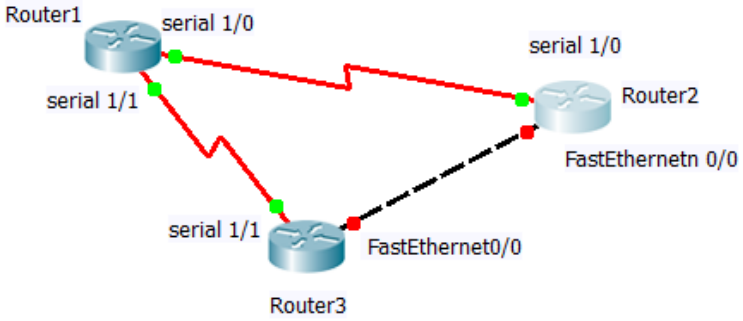


Рис.10

Теперь необходимо поднять интерфейс *FastEthernet* между *Router3* и *Router2*.
Поднимаем *Ethernet* на *Router2*
Router2(config)#int fa
*Router2(config)#**int fastEthernet 0/0***
*Router2(config-if)#**no sh***
Router2(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

Для Router3 выполним аналогичные команды.
Router3>en
Router3#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router3(config)#int fa
*Router3(config)#**int fastEthernet 0/0***
Router3(config-if)#no sh
*Router3(config-if)#**no shutdown***
Router3(config-if)#
*%LINK-5-CHANGED: Interface FastEthernet0/0, **changed state to up***
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up

Далее задаем адресацию для роутера 3 и роутера 2 с интерфейсами *fastEthernet 0/0.*
Router3#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router3(config)#int fa
*Router3(config)#**int fastEthernet 0/0***
Router3(config-if)#ip ad
*Router3(config-if)#**ip address 5.1.1.1 255.0.0.0***

Router2(config)#int fa
*Router2(config)#**int fastEthernet 0/0***
Router2(config-if)#ip ad
*Router2(config-if)#**ip address 5.1.1.2 255.0.0.0***

В итоге все интерфейсы подняты (рис.11).

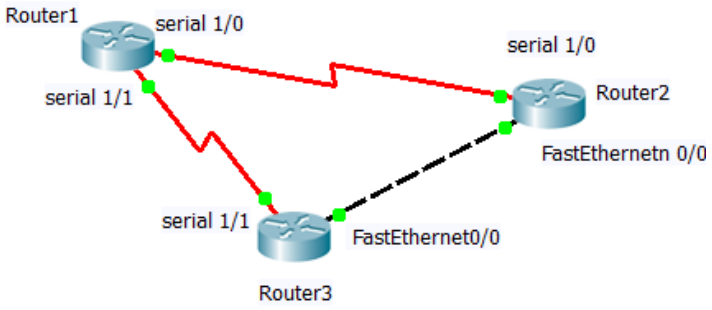


Рис.11

Далее справочными командами можно просмотреть информацию о соседях:
*Router2#**sh cdp neighbors***
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone
Device ID Local Intrfce Holdtme Capability Platform Port ID

Router3	*Fas 0/0*	*131*	*R*	*C2600*	*Fas 0/0*
Router1	*Ser 1/0*	*129*	*R*	*C2600*	*Ser 1/0*

Информацию о состоянии всех интерфейсов можно посмотреть:

*Router2#**sh cdp interface***
FastEthernet0/0 is up, line protocol is up
Sending CDP packets every 60 seconds
Holdtime is 180 seconds
FastEthernet0/1 is administratively down, line protocol is down
Sending CDP packets every 60 seconds
Holdtime is 180 seconds
Serial1/0 is up, line protocol is up
Sending CDP packets every 60 seconds
Holdtime is 180 seconds
Serial1/1 is administratively down, line protocol is down
Sending CDP packets every 60 seconds
Holdtime is 180 seconds
Serial1/2 is administratively down, line protocol is down
Sending CDP packets every 60 seconds
Holdtime is 180 seconds
Serial1/3 is administratively down, line protocol is down
Sending CDP packets every 60 seconds
Holdtime is 180 seconds

Далее добавим к роутерам компьютер и кросс кабелем соединим его с роутером 1, зададим IP адреса для ПК и *FastEthernet0/0* интерфейса роутера 1, согласно рис.1. Далее поднимем интерфейс *FastEthernet0/0* для роутера 1.

В итоге при наведении на роутеры появляется табличка со всеми настройками - для роутера 1 (рис.12).

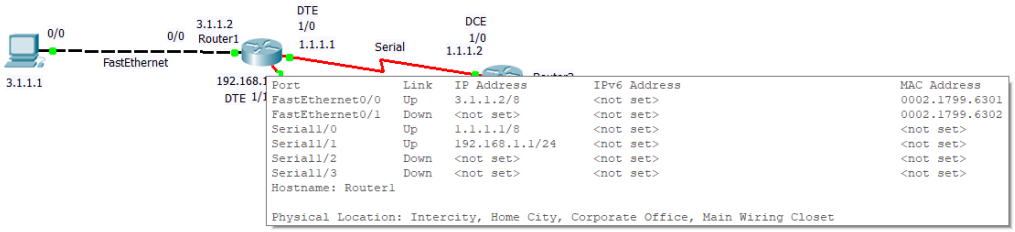


Рис.12

Для роутера 2 появляется табличка со всеми настройками (рис.13).

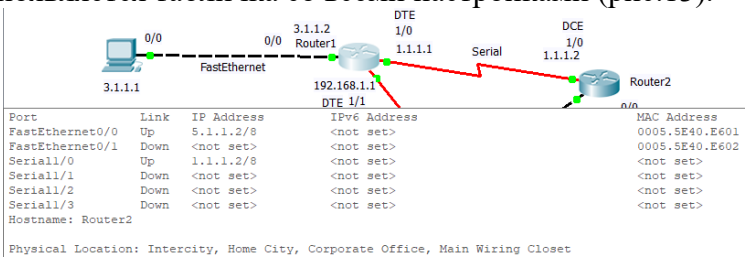


Рис.13

Для роутера 3 появляется табличка со всеми настройками (рис.14).

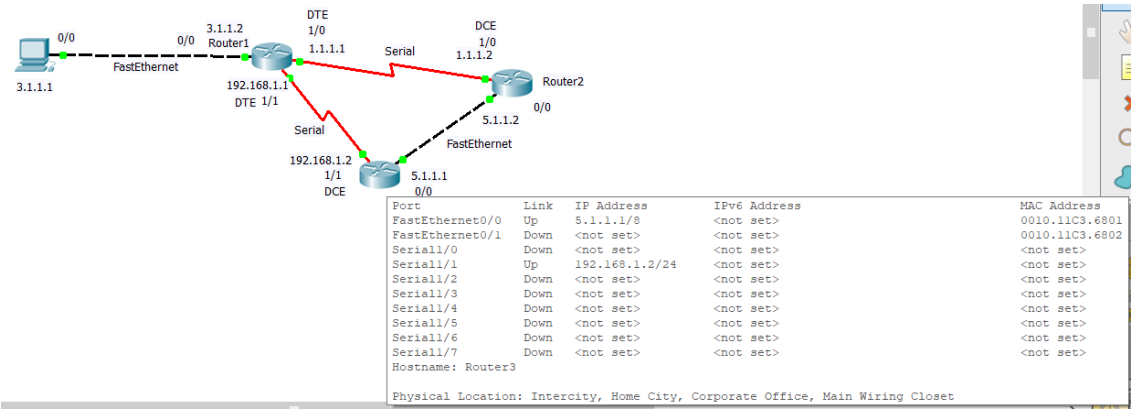


Рис.14

Полную информацию об адресации устройств можно получить с помощью команды.

Router1# ***sh ip interface***

FastEthernet0/0 is up*, line protocol* ***is up*** *(connected)*

Internet address is 3.1.1.2/8
Broadcast address is 255.255.255.255
Address determined by setup command
MTU is 1500 bytes
Helper address is not set
Directed broadcast forwarding is disabled
Outgoing access list is not set
Inbound access list is not set
Proxy ARP is enabled
Security level is default
Split horizon is enabled
ICMP redirects are always sent
ICMP unreachables are always sent
ICMP mask replies are never sent
IP fast switching is disabled
IP fast switching on the same interface is disabled
IP Flow switching is disabled
IP Fast switching turbo vector
IP multicast fast switching is disabled
IP multicast distributed fast switching is disabled
Router Discovery is disabled
IP output packet accounting is disabled
IP access violation accounting is disabled
TCP/IP header compression is disabled
RTP/IP header compression is disabled
Probe proxy name replies are disabled
Policy routing is disabled
Network address translation is disabled
BGP Policy Mapping is disabled
Input features: MCI Check
WCCP Redirect outbound is disabled
WCCP Redirect inbound is disabled
WCCP Redirect exclude is disabled

FastEthernet0/1 is administratively down, line protocol is down (disabled)

Internet protocol processing disabled

Serial1/0 is up, line protocol is up (*connected)*

Internet address is 1.1.1.1/8
Broadcast address is 255.255.255.255
……..

Краткую информацию об адресации устройства можно посмотреть с помощью команд.

*Router1#**sh ip in brief***

Interface	*IP-Address*	*OK? Method Status*	*Protocol*
FastEthernet0/0	*3.1.1.2*	*YES manual up*	*up*
FastEthernet0/1	*unassigned*	*YES unset administratively down*	*down*
Serial1/0	*1.1.1.1*	*YES manual up*	*up*
Serial1/1	*192.168.1.1*	*YES manual up*	*up*
Serial1/2	*unassigned*	*YES unset administratively down*	*down*
Serial1/3	*unassigned*	*YES unset administratively down*	*do*

Информация о всех адресах и подключенных интерфейсах появится после выполнения команды.

*Router1#**sh 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 not set
C 1.0.0.0/8 is directly connected, Serial1/0
C 3.0.0.0/8 is directly connected, FastEthernet0/0
C 192.168.1.0/24 is directly connected, Serial1/1

Аналогично для роутера 2.
Router2>sh 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 not set
C 1.0.0.0/8 is directly connected, Serial1/0
C 5.0.0.0/8 is directly connected, FastEthernet0/0

Аналогично для роутера 3:
Router3>sh 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 not set

C 5.0.0.0/8 is directly connected, FastEthernet0/0
C 192.168.1.0/24 is directly connected, Serial1/1

На каждом устройстве посмотрите вашу активную конфигурацию и убедитесь, что там появились назначенные *IP* адреса.

*Router1#**sh running-config***
Building configuration...
Current configuration : 634 bytes
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
hostname Router1
interface FastEthernet0/0
ip address 3.1.1.2 255.0.0.0
duplex auto
speed auto
interface FastEthernet0/1
no ip address
duplex auto
speed auto
shutdown
interface Serial1/0
ip address 1.1.1.1 255.0.0.0
interface Serial1/1
ip address 192.168.1.1 255.255.255.0
interface Serial1/2
no ip address
shutdown
interface Serial1/3
no ip address
shutdown
ip classless
line con 0
line aux 0
line vty 0 4
login
end

Подключимся к устройству *Router3*. Вы должны успешно пропинговать непосредственно подсоединённый *FaEthernet 0/0* интерфейс на устройстве *Router2*.

Router3>ping 5.1.1.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 5.1.1.2, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/0/0 ms

Router3>ping 5.1.1.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 5.1.1.2, timeout is 2 seconds:

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms

Попробуем пропинговать из роутера 3 интерфейс *Serial 1/1* на устройстве *Router1*.

Router3>ping 192.168.1.1

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/3 ms

Успешно.

Аналогично с роутера 2 успешно пингуются.

Router2>ping 1.1.1.1

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 1.1.1.1, timeout is 2 seconds:

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/3 ms

Router2>ping 5.1.1.1

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 5.1.1.1, timeout is 2 seconds:

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms

С роутера 3 невозможно пропинговать другие сети.

Router3>ping 1.1.1.1

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 1.1.1.1, timeout is 2 seconds:

.....

Success rate is 0 percent (0/5)

Router3>ping 1.1.1.2

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 1.1.1.2, timeout is 2 seconds:

.....

Success rate is 0 percent (0/5)

Неудачи наступили потому, что не настроена на роутерах маршрутизация.

Аналогично с ПК нет доступа к интерфейсам с адресами 1.1.1.1, 1.1.1.2, 5.1.1.2, 192.168.1.1 и т.д. (рис.15).

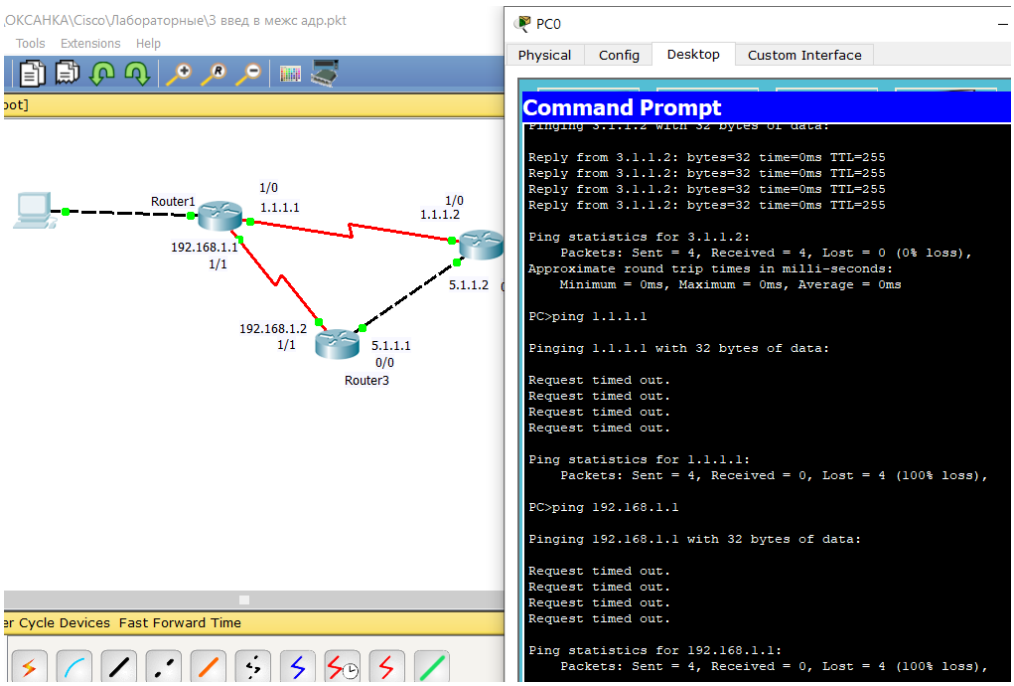


Рис.15

Telnet

Далее воспользуемся командой *telnet*, чтобы получить доступ к устройствам, к которым ранее не было доступа.

Войдите на устройство *Router1*. Нам необходимо, чтобы сетевое устройство принимало *telnet*-сессии и было защищено паролем. Каждая так называемая линия в сетевом устройстве потенциально представляет активную *telnet*-сессию, которую устройство может поддерживать. Наши сетевые устройства поддерживают до 5 линий, назначенные на виртуальные терминалы *vty*. Мы используем все 5 линий.

Router1>en
Router1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router1(config)#line v
Router1(config)#line vty 0 4
Router1(config-line)#login
% Login disabled on line 66, until 'password' is set
% Login disabled on line 67, until 'password' is set
% Login disabled on line 68, until 'password' is set
% Login disabled on line 69, until 'password' is set
% Login disabled on line 70, until 'password' is set
Router1(config-line)#pass
Router1(config-line)#password cisco

Войдите на устройство *Router2* и установим *telnet*-соединение с устройством *Router1*. Для этого мы используем *IP* адрес роутера 1 по их общему интерфейсу. После соединения с роутером 1 в командной строке вместо роутера 2 появляется роутер 1. В результате появилась возможность пинговать те адреса, которые ранее из роутера 2 были недоступны. Чтобы прервать *telnet* сессию надо написать *exit.*

Router2*>telnet 1.1.1.1*
Trying 1.1.1.1 ...Open
User Access Verification
Password:
Router1*>ping 3.1.1.1*
Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 3.1.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms
Router1>ping 192.168.1.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/2 ms
Router1>ping 192.168.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/2/2 ms
Router1>exit
[Connection to 1.1.1.1 closed by foreign host]
Router2>

Контрольные вопросы.

1. Какие есть режимы ввода команд в командной строке?
2. Как переключаться между режимами ввода команд в командной строке?
3. Какую роль играет клавиша табуляции при вводе команд?
4. Как войти в режимы глобальной конфигурации, активизировать частный вид конфигурации и выйти из этих режимов?
5. Как ориентироваться в ранее введенных командах и повторять их?
6. Что такое *CDP*, для чего он служит и как им пользоваться?
7. Какую информацию возвращает команда *ping*?
8. Можно ли находясь на одном устройстве попарно пропинговать все устройства в сети?
9. Для чего служит команда *traceroute*?
10. Для чего служит команда протокол t*elnet*?
11. Как задать имя хоста?
12. Какую информацию можно посмотреть командами *show* в пользовательском режиме?
13. Какую информацию можно посмотреть командами *show* в привилегированном режиме, но нельзя посмотреть в пользовательском режиме?
14. Каким устройством может выступать маршрутизатор для последовательной линии связи?
15. На каком устройстве при последовательном соединении можно устанавливать частоту синхронизации?
16. Как поднять интерфейс и определить его состояние?
17. Как назначить IP адрес на интерфейс и убедиться, что он назначен?
18. Почему могут не проходить пинги между устройствами?
19. Как приостановить и возобновить *telnet*-сессию?
20. Как закрыть *telnet* соединение?

Порядок выполнения и сдачи работы

1. Изучить теоретическую и практическую часть.
2. Сдать преподавателю теорию работы путём ответа на контрольные вопросы.
3. Выполнить практическую часть.
4. Получите вариант и выполните задание для самостоятельной работы
5. Предъявите преподавателю результат выполнения задания для самостоятельной работы.

6. Продемонстрируйте работу *telnet*.
7. Оформите отчёт.
8. Защитите отчёт.

Задание для самостоятельной работы.

1. Получите свой вариант

Таблица 3.

Вариант	i11-i31	i12-i21	i22-i32
1, 9	serial	Serial	serial
2, 10	serial	Serial	ethernet
3, 11	serial	Ethernet	serial
4, 12	serial	Ethernet	ethernet
5, 13	ethernet	Serial	serial
6, 14	ethernet	Serial	ethernet
7, 15	ethernet	Ethernet	serial
8, 16	ethernet	Ethernet	ethernet

Прежде, чем заниматься настройками интерфейсов создайте топологию в программе и на листе бумаги пропишите все интерфейсы, адреса и т.д. – аналогично рис.1.

Выберите подходящие устройства, используя таблицу 3 и создайте топологию, изображённую на рис. 16. Сами назначьте устройствам имена. Поднимите на каждом устройстве используемые интерфейсы. Проверьте их состояния. На каждом устройстве, используя команды *CDP show cdp neighbors*, получите информацию о соседних устройствах.

Назначьте интерфейсам адреса, согласно варианту (v=1-16) из таблицы 5.

Все маски равны 255.255.255.0. Например, для варианта 7 (v=7) имеем адреса из таблицы 4.

Таблица 4.

Устройство	Интерфейс	Адрес
Router1	i11	**7.1.1.2**
Router3	i31	**7.1.1.2**
Router1	i12	**7.1.2.1**
Router2	i21	**7.1.2.2**
Router2	i22	**7.1.3.1**
Router3	i32	**7.1.3.2**

Таблица 5.

Вариант	i11, i31	i12, i21	i22, i32
1	v.1.1.1, v.1.1.2	v.1.2.1, v.1.2.2	v.1.3.1, v.1.3.2
2	v.1.1.1, v.1.1.2	v.1.2.1, v.1.2.2	v.1.3.1, v.1.3.2
3	v.1.1.1, v.1.1.2	v.1.2.1, v.1.2.2	v.1.3.1, v.1.3.2
4	v.1.1.1, v.1.1.2	v.1.2.1, v.1.2.2	v.1.3.1, v.1.3.2
5	v.1.1.1, v.1.1.2	v.1.2.1, v.1.2.2	v.1.3.1, v.1.3.2
6	v.1.1.1, v.1.1.2	v.1.2.1, v.1.2.2	v.1.3.1, v.1.3.2

7	v.1.1.1, v.1.1.2	v.1.2.1, v.1.2.2	v.1.3.1, v.1.3.2
8	v.1.1.1, v.1.1.2	v.1.2.1, v.1.2.2	v.1.3.1, v.1.3.2
9	v.1.1.1, v.1.1.2	v.1.2.1, v.1.2.2	v.1.2.1, v.1.2.2
10	v.1.1.1, v.1.1.2	v.1.2.1, v.1.2.2	v.1.3.1, v.1.3.2
11	v.1.1.1, v.1.1.2	v.1.2.1, v.1.2.2	v.1.3.1, v.1.3.2
12	v.1.1.1, v.1.1.2	v.1.2.1, v.1.2.2	v.1.3.1, v.1.3.2
13	v.1.1.1, v.1.1.2	v.1.2.1, v.1.2.2	v.1.3.1, v.1.3.2
14	v.1.1.1, v.1.1.2	v.1.2.1, v.1.2.2	v.1.3.1, v.1.3.2
15	v.1.1.1, v.1.1.2	v.1.2.1, v.1.2.2	v.1.3.1, v.1.3.2
16	v.1.1.1, v.1.1.2	v.1.2.1, v.1.2.2	v.1.3.1, v.1.3.2

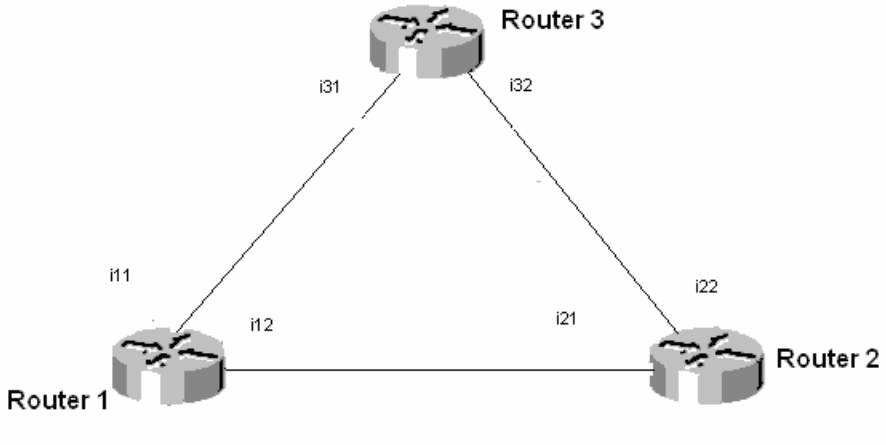


Рис.16 Топология сети.

Проверьте, что адреса назначены. На каждом устройстве выполните команду *show ip interface brief* .

Если сделано всё правильно вы сможете пропинговать из любого компьютера определённые (но не все) адреса интерфейсов других компьютеров.

Настройте на *Router1 Telnet*. Задайте пароль.

Перейдите на Router2. Зайдите по Telnet на Router1. Пропингуйте адреса, которые ранее не были доступны с роутера 2. Выполните команду *show user*. Приостановите сессию.

Лабораторная работа №6 Статическая маршрутизация

Тема работы: Статическая маршрутизация.
Цель работы: маршрутизация, понятие статического маршрута, настройка маршрутизации, таблица маршрутизации.

Теоретическая часть.

ARP (Address Resolution Protocol)

Когда отправитель определил IP адрес приёмника, он смотрит в свою ARP таблицу чтобы узнать MAC адрес приёмника. Если источник обнаруживает, что MAC и IP адреса приёмника присутствуют в ARP таблице, он устанавливает между ними соответствие и использует его в ходе инкапсуляции IP пакетов во фреймы канального уровня. MAC адреса фреймов канального уровня берутся из ARP таблиц. После этого фрейм по физическому каналу отправляется от отправителя к адресату.

Если отправитель имеет IP пакет для получателя с IP-адресом АДР и этот адрес отсутствует в ARP таблице, то отправитель отправляет по сети широковещательный ARP запрос следующего содержания: сообщите MAC адрес сетевого интерфейса с IP-адресом АДР. Запрос принимают все сетевые устройства в сегменте сети, и только устройство, имеющее IP-адрес АДР, реагирует на него, посылая отправителю информацию о MAC адресе своего сетевого интерфейса с IP адресом АДР. Отправитель записывает пару <MAC адрес, IP-адрес АДР> в свою ARP таблицу.

Маршрутизация

Протоколы маршрутизации - это правила, по которым осуществляется обмен информации о путях передачи пакетов между маршрутизаторами. Протоколы характеризуются временем сходимости, потерями и масштабируемостью. В настоящее время используется несколько протоколов маршрутизации. Каждый протокол имеет сильные и слабые стороны.

Одна из главных задач маршрутизатора состоит в определении наилучшего пути к заданному адресату. Маршрутизатор определяет пути (маршруты) к адресатам или из статической конфигурации, введённой администратором, или динамически на основании маршрутной информации, полученной от

других маршрутизаторов. Маршрутизаторы обмениваются маршрутной информацией с помощью протоколов маршрутизации. Маршрутизатор хранит таблицы маршрутов в оперативной памяти. Таблица маршрутов - это список наилучших известных доступных маршрутов. Маршрутизатор использует эту таблицу для принятия решения куда направлять пакет. Для просмотра таблицы маршрутов следует использовать команду ***show ip route***. Даже, если на некотором маршрутизаторе X не задавались никакие команды маршрутизации, тогда он всё равно строит таблицу маршрутов для непосредственно подсоединённых к нему сетей, например:

C 192.168.4.0/24 is directly connected, Ethernet0

10.0.0.0/16 is subnetted, 3 subnets

C 10.3.0.0 is directly connected, Serial0

C 10.4.0.0 is directly connected, Serial1

C 10.5.0.0 is directly connected, Ethernet1

Маршрут на непосредственно подсоединённые сети отображается на интерфейс маршрутизатора, к которому они присоединены. Здесь /24 обозначает маску 255.255. 255.0, а /16 - 255.255.0.0.

Таблица маршрутов отображает сетевые префиксы (адреса сетей) на выходные интерфейсы. Когда X получает пакет, предназначенный для 192.168.4.46, он ищет префикс 192.168.4.0/24 в таблице маршрутов. Согласно таблице, пакет будет направлен на интерфейс Ethernet0. Если X получит пакет для 10.3.21.5, он направит его на Serial0.

Эта таблица показывает четыре маршрута для непосредственно подсоединённых сетей. Они имеют метку C. Маршрутизатор X отбрасывает все пакеты, направляемые к сетям, не указанным в таблице маршрутов. Для направления пакетам к другим адресатам необходимо в таблицу включить дополнительные маршруты. Новые маршруты могут быть добавлены двумя методами:

Статическая маршрутизация – администратор вручную определяет маршруты к сетям назначения.

Динамическая маршрутизация – маршрутизаторы следуют правилам,

определяемым протоколами маршрутизации для обмена информацией о маршрутах и выбора лучшего пути. Статические маршруты не меняются самим маршрутизатором. Динамические маршруты изменяются самим маршрутизатором автоматически при получении информации о смене маршрутов от соседних маршрутизаторов. Статическая маршрутизация потребляет мало вычислительных ресурсов и полезна в сетях, которые не имеют нескольких путей к адресату назначения. Если от маршрутизатора к маршрутизатору есть только один путь, то часто используют статическую маршрутизацию.

Для конфигурации статической маршрутизации в маршрутизаторах Cisco используют две версии команды ip route

Первая версия

ip route АдресСетиНазначения МаскаСетиНазначения Интерфейс

Команда указывает маршрутизатору, что все пакеты, предназначенные для АдресСетиНазначения-МаскаСетиНазначения следует направлять на свой интерфейс Интерфейс. Если интерфейс Интерфейс - типа Ethernet, то физические (MAC) адреса исходящих пакетов будут широковещательными.

Вторая версия

ip route АдресСетиНазначения МаскаСетиНазначения Адрес

Команда указывает маршрутизатору, что все пакеты, предназначенные для АдресСетиНазначения-МаскаСетиНазначения, следует направлять на тот свой интерфейс, из которого достижим IP адрес Адрес. Как правило, Адрес - это адрес следующего хопа по пути к АдресСетиНазначения. Выходной интерфейс и физические адреса исходящих пакетов определяются маршрутизатором по своим ARP таблицам на основании IP адреса Адрес.

Например,

ip route 10.6.0.0 255.255.0.0 Serial1 (1)

ip route 10.7.0.0 255.255.0.0 10.4.0.2 (2)

Первый пример отображает сетевой префикс 10.6.0.0/16 на локальный интерфейс маршрутизатора Serial1. Следующий пример отображает сетевой

префикс 10.7.0.0/16 на IP адрес 10.4.0.2 следующего хопа по пути к 10.7.0.0/16. Обе эти команды добавят статические маршруты в таблицу маршрутизации (метка S):

S 10.6.0.0 via Serial1

S 10.7.0.0 [1/0] via 10.4.0.2

Когда интерфейс падает, все статические маршруты, отображаемые на этот интерфейс, удаляются из таблицы маршрутов. Если маршрутизатор не может больше найти адрес следующего хопа по пути к адресу, указанному в статическом маршруте, то маршрут исключается из таблицы.

Заметим, что для сетей типа Ethernet рекомендуется всегда использовать форму (2) команды ***ip route***. Ethernet интерфейс на маршрутизаторе, как правило, соединён с несколькими Ethernet интерфейсами других устройств в сети. Указание в команде ip route IP адреса позволит маршрутизатору правильно сформировать физический адрес выходного пакета по своим ARP таблицам.

Маршрутизация по умолчанию.

Совсем не обязательно, чтобы каждый маршрутизатор обслуживал маршруты ко всем возможным сетям назначения. Вместо этого маршрутизатор хранит маршрут по умолчанию или шлюз последнего пристанища (last resort). Маршруты по умолчанию используются, когда маршрутизатор не может поставить в соответствие сети назначения строку в таблице маршрутов. Маршрутизатор должен использовать маршрут по умолчанию для отсылки пакетов другому маршрутизатору. Следующий маршрутизатор будет иметь маршрут к этой сети назначения или иметь свой маршрут по умолчанию к третьему маршрутизатору и т.д. В конечном счёте, пакет будет маршрутизирован на маршрутизатор, имеющий маршрут к сети назначения.

Маршрут по умолчанию может быть статически введен администратором или динамически получен из протокола маршрутизации.

Так как все IP адреса принадлежат сети 0.0.0.0 с маской 0.0.0.0, то в простейшем случае надо использовать команду

ip route 0.0.0.0 0.0.0.0 [адрес следующего хопа | выходной интерфейс]

Ручное задание маршрута по умолчанию на каждом маршрутизаторе подходит для простых сетей. В сложных сетях необходимо организовать динамический обмен маршрутами по умолчанию.

Интерфейс петля

На сетевых устройствах можно создавать сетевые интерфейсы, не связанные с реальными каналами для передачи данных и назначать на них IP адреса с масками. Такие интерфейсы называют петлями (loopback). Петли полезны при поэтапном проектировании сетей. Если к какому-то реальному сетевому интерфейсу маршрутизатора в дальнейшем будет подсоединена 32 подсеть, то в начале на маршрутизаторе создаётся *loopback*, настраивается в плане взаимодействия с остальными участками сети и лишь затем заменяется на реальный интерфейс. Интерфейс петля появляется после команды ***interface loopbackN*** или сокращённо int lN, где N целое неотрицательное число – номер петли. Например

Router(conf)>int l0 1.1.1.1 255.0.0.0

Команда trace

Команда **trace** является идеальным способом для выяснения того, куда отправляются данные в сети. Эта команда использует ту же технологию протокола ICMP, что и команда ping, только вместо проверки сквозной связи между отправителем и получателем, она проверяет каждый шаг на пути. Команда trace использует способность маршрутизаторов генерировать сообщения об ошибке при превышении пакетом своего установленного времени жизни (Time To Live, TTL). Эта команда посылает несколько пакетов и выводит на экран данные про время прохождения туда и назад для каждого из них. Преимущество команды trace заключается в том, что она показывает очередной достигнутый маршрутизатор на пути к пункту назначения. Это очень мощное средство для локализации отказов на пути от отправителя к получателю. Варианты ответов утилиты trace представлены в таблице 1.

Таблица 1.

Символ	Значение
!H	Зондирующий пакет был принят маршрутизатором, но не переадресован, что обычно бывает из-за списка доступа
P	Протокол недосягаем
N	Сеть недосягаема
U	Порт недосягаем
*	Превышение границы ожидания

Практическая часть

Построим сеть (рис.1). Далее сконфигурируем интерфейсы, настроим IP адреса и проверим доступность разных сетей из каждого устройства.

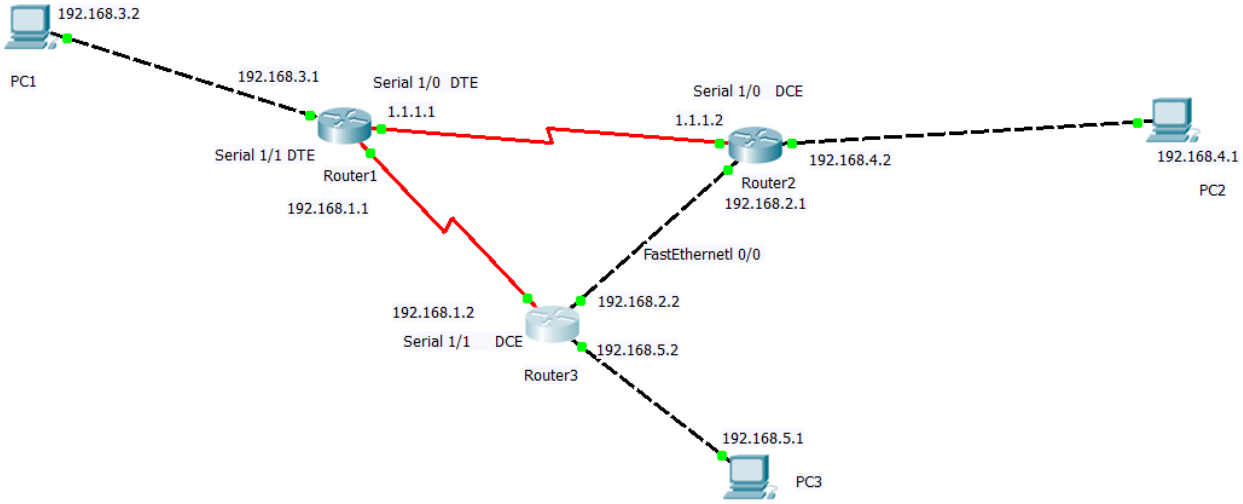


Рис.1 Топология сети

Добавляем три роутера 2621XM.

Далее ко всем роутерам подключаем порты: вначале отключаем роутер, далее подключаем порт NM-4A/S, затем включаем роутер. Это необходимо сделать, чтобы использовать последовательное соединение Serial между роутерами.

Роутер 1 и роутер 2 соединим последовательным соединением Serial DTE.

Аналогично соединим роутер 1 и роутер 3.

Роутер 2 и роутер 3 соединим кроссовым кабелем.

Обратите внимание на интерфейсы и напишите их на топологии, также добавьте названия роутеров, используя кнопку надпись.

Далее переходим в командную строку и начинаем использовать разные команды для конфигурации сети.

Первоначально необходимо из режима глобальной конфигурации переименовать роутеры.

Заходим на первый роутер, нажимаем *no* при первом предложении системы к диалогу, заходим в режим привилегированный, а затем в режим глобальной конфигурации. Для переименования используем команду *hostname Router1*.

Аналогично переименуем второй роутер.

Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
*Router(config)#**hostname Router2***
Router2(config)#

Далее необходимо поднять интерфейсы. Чтобы поднять последовательные интерфейсы необходимо проверить каким является роутер оконечным (DTE) или устройством связи (DCE).

Перейдём к конфигурации последовательных интерфейсов. Зайдём на *Router1*. Проверим, каким устройством выступает наш маршрутизатор для последовательной линии связи: оконечным устройством *DTE (data terminal equipment)* либо устройством связи *DCE (data circuit)* и выполним команду:

*Router1#**show controllers serial 1/0***
Interface Serial1/0
Hardware is PowerQUICC MPC860
***DTE** V.35 TX and RX clocks detected*
idb at 0x81081AC4, driver data structure at 0x81084AC0
SCC Registers:
General [GSMR]=0x2:0x00000000, Protocol-specific [PSMR]=0x8
Events [SCCE]=0x0000, Mask [SCCM]=0x0000, Status [SCCS]=0x00
……..

Если видим **DTE**, то далее поднимаем интерфейс на роутере 1.
*Router1(config)#**interface serial 1/0***
Router1(config-if)#no sh
*Router1(config-if)#**no shutdown*** – команда для поднятия интерфейса
Router1(config-if)#
*%LINK-5-CHANGED: Interface Serial1/0, changed state **to up***

То, что интерфейс поднят подтверждают слова *changed state **to up**.*
Задаем адресацию для роутера 1, согласно рис.1.
Router1(config-if)#ip ad
*Router1(config-if)#**ip address 1.1.1.1 255.0.0.0***

Далее аналогично проверим на роутере 2 каким является интерфейс serial 1/0.
Router2#sh con se
Router2#sh con serial 1/0
Interface Serial1/0
Hardware is PowerQUICC MPC860
***DCE** V.35, clock rate 64000*
idb at 0x81081AC4, driver data structure at 0x81084AC0
SCC Registers:
...

Если видим - ..... *DCE* ....., то наш маршрутизатор является устройством связи, и он должен задавать частоту синхронизации тактовых импульсов, используемых при передаче данных. Частота берётся из определённого ряда частот.

*Router2(config)#**int ser1/0***
*Router2(config-if)#**clock rate 64000***

Далее в этом же режиме конфигурирования интерфейсов поднимаем интерфейс и задаем IP адрес – пишется адрес и через пробел маска.

*Router2(config-if)#**no shutdown***
Router2(config-if)#ip ad
*Router2(config-if)#**ip address 1.1.1.2 255.0.0.0***

Аналогично поднимаем интерфейсы и задаем адресацию для Serial интерфейсов на роутере 1, роутере 2 и роутере 3.

В итоге интерфейсы *Serial* должны загореться зелеными индикаторами.

Теперь необходимо поднять интерфейс *FastEthernet* между *Router3* и *Router2*.
Поднимаем *Ethernet* на *Router2*
Router2(config)#int fa
*Router2(config)#**int fastEthernet 0/0***
*Router2(config-if)#**no sh***
Router2(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

Для Router3 выполним аналогичные команды.

Далее задаем адресацию для роутера 3 и роутера 2 с интерфейсами *fastEthernet 0/0.*
Router3#conf t
Router3(config)#int fa
*Router3(config)#**int fastEthernet 0/0***
Router3(config-if)#ip ad
*Router3(config-if)#**ip address 192.168.2.2 255.255.255.0***

Для *Router2* аналогично.
В итоге все интерфейсы подняты.

Для компьютеров при назначении адресации необходимо заполнить поле Default Gateway (Рис.2), например, для PC1.

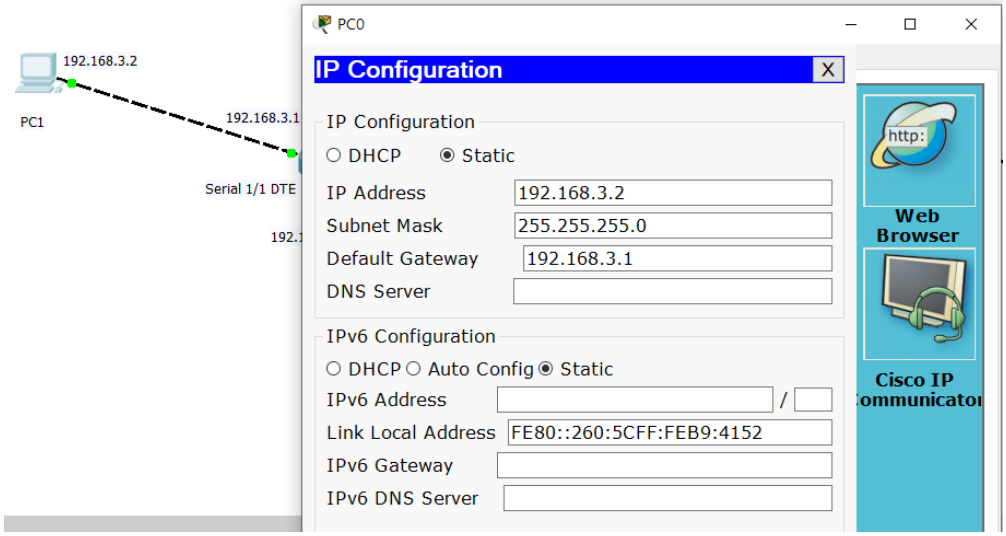


Рис.2

У роутеров посмотрите таблицу ARP.

Router1#sh arp

Protocol Address Age (min) Hardware Addr Type Interface

Internet 192.168.3.1 - 0010.113C.E301 ARPA FastEthernet0/0

Она содержит только одну строку о *MAC* адресе своего *Ethernet* интерфейса с *IP* адресом *192.168.3.1*.

Присоединитесь к маршрутизатору *Router2* и посмотрите его *ARP* таблицу. Она содержит уже две строки.

Router2#sh arp
Protocol Address Age (min) Hardware Addr Type Interface
Internet 192.168.2.1 - 0001.96ED.5001 ARPA FastEthernet0/0
Internet 192.168.4.2 - 0001.96ED.5002 ARPA FastEthernet0/1

Появились дополнительные строки в таблице, т.к. ранее был осуществлен *ping* с роутера 1 на роутер 2 и наоборот.

Статические маршруты

В прошлой работе мы не могли из маршрутизаторов *Router1* и *Router2* пропинговать некоторые интерфейсы из-за отсутствия маршрутизации.

Исправим положение.

Присоединитесь к маршрутизатору *Router2*. Мы не могли пинговать адреса *192.168.3.1* и *192.168.1.2* и т.д. Посмотрите таблицу маршрутов

*Router2# **show ip route**.*

Видим непосредственно присоединённые сети. Нет маршрута к сети *192.168.3.0*. Добавим маршрут к сети *192.168.3.0/24* через адрес *1.1.1.1* ближайшего хопа на пути к этой сети:

Router2>en
Router2#conf t
*Router2(config)#**ip route 192.168.3.0 255.255.255.0 1.1.1.1***

Аналогично настроим маршрутизацию к другим сетям.

*Router2(config)#**ip route 192.168.1.0 255.255.255.0 1.1.1.1***
*Router2(config)#**ip route 192.168.1.0 255.255.255.0 192.168.2.2***
*Router2(config)#**ip route 192.168.5.0 255.255.255.0 192.168.2.2***

Далее посмотрим таблицу маршрутизации.

*Router2#**sh 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 not set

C 1.0.0.0/8 is directly connected, Serial1/0
S 192.168.1.0/24 [1/0] via 1.1.1.1
[1/0] via 192.168.2.2
C 192.168.2.0/24 is directly connected, FastEthernet0/0
S 192.168.3.0/24 [1/0] via 1.1.1.1
C 192.168.4.0/24 is directly connected, FastEthernet0/1

S 192.168.5.0/24 [1/0] via 192.168.2.2

Выполним ping к адресам, которые были недоступны ранее и видим, что все пингуется успешно.

*Router2>**ping 192.168.5.2***
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.5.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/1/5 ms

*Router2>**ping 192.168.4.1***
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.4.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms

Аналогично необходимо настроить маршрутизацию на *Router1* и *Router3*.

Теперь все сетевые интерфейсы в сети пингуются из каждого сетевого устройства. Проверьте это.

Маршрутизация по умолчанию.

Если, например, сетевые устройства *Router5* и *Router4* имеют только по одному выход во внешний мир: через интерфейсы с адресами *10.1.1.1* и *172.16.10.1*, соответственно. Поэтому, можно не определять на какие подсети мы маршрутизируем пакеты и использовать маршрутизацию по умолчанию.

1. Вначале удалим старые маршруты.
Router5(config)#no ip route 172.16.10.0 255.255.255.0 10.1.1.1
Router4(config)#no ip route 10.1.1.0 255.255.255.0 172.16.10.1
2. И назначим маршруты по умолчанию.
Router5(config)#ip route 0.0.0.0 0.0.0.0 10.1.1.1
Router4(config)#ip route 0.0.0.0 0.0.0.0 172.16.10.1

Loopback

Если необходимо определить интерфейс петлю на устройстве *Router4*, то выполнить надо следующую команду:

*Router4(config)#**int loopback 0***
Router4(config-if)#ip address 1.1.1.1 255.255.255.0
Далее надо прописать, например, на устройстве *Router5* маршрут на сеть петли
Router5(conf)# ip route 1.1.1.0 255.255.255.0 172.16.10.2
Присоединимся, например, к устройству *Router6* и пропингуем созданную петлю
Router6#ping 1.1.1.1

Контрольные вопросы

1. Как отправитель узнаёт MAC адрес получателя?

2. Как посмотреть ARP таблицу?

3. Когда в ARP таблице появляются новые строки?

4. Что такое таблица маршрутов?

5. Если администратор не настраивал никаких маршрутов, то что она будет содержать?

6. Чем статическая маршрутизация отличается от динамической?

7. Какие две формы задания статической маршрутизации вы знаете?

8. Как в команде маршрутизации определяется сеть назначения?

9. Почему для сетей типа Ethernet рекомендуется всегда использовать форму (2) команды маршрутизации?

10. Объясните значения полей в командах маршрутизации.

11. Почему в качестве поля Адрес рекомендуют использовать адрес следующего хопа по пути к сети назначения.

12. Когда используется маршрутизация по умолчанию?

13. Когда используют интерфейс петля?

14. Как работает команда трасировки?

Порядок выполнения и сдачи работы

1. Изучить теоретическую и практическую часть.
2. Сдать преподавателю теорию работы путём ответа на контрольные вопросы.
3. Выполнить практическую часть.
4. Получите вариант и выполните задание для самостоятельной работы
5. Предъявите преподавателю результат выполнения задания для самостоятельной работы.
6. Оформите отчёт.
7. Защитите отчёт.

Задание для самостоятельной работы

1. Построить топологию, представленную на рисунке 3. Прежде, чем заниматься настройками интерфейсов создайте топологию в программе и на листе бумаги пропишите все интерфейсы, адреса и т.д. Используйте таблицу 2, для выбора соединений роутеров.

Таблица 2.

Вариант	i11-i31	i12-i21	i22-i32
1, 9	serial	Serial	serial
2, 10	serial	Serial	ethernet
3, 11	serial	Ethernet	serial
4, 12	serial	Ethernet	ethernet
5, 13	ethernet	Serial	serial
6, 14	ethernet	Serial	ethernet
7, 15	ethernet	Ethernet	serial
8, 16	ethernet	Ethernet	ethernet

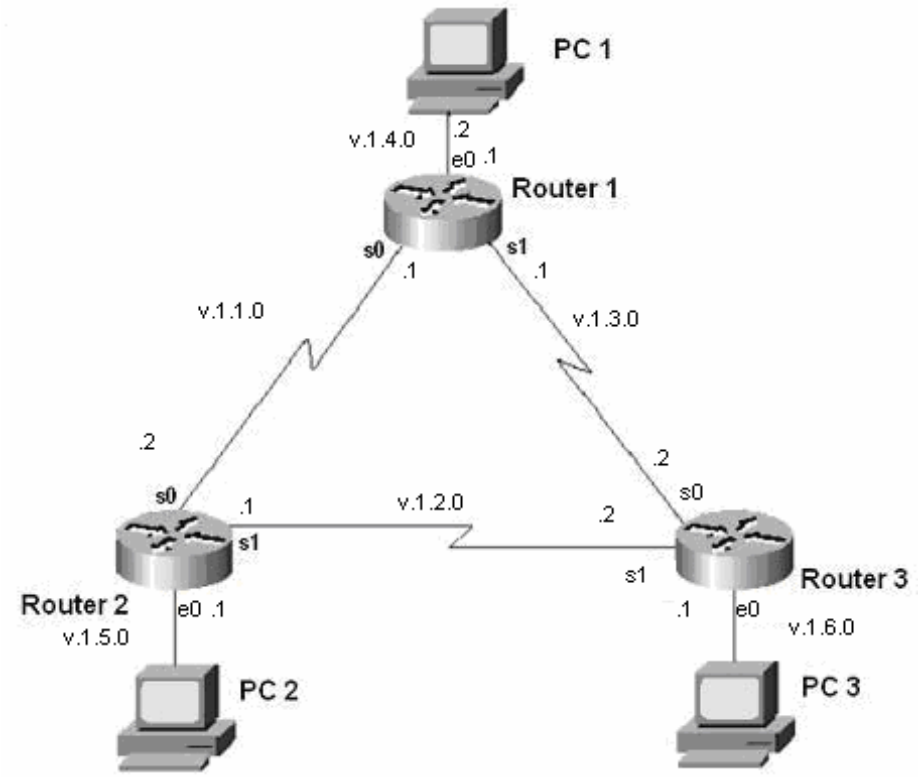


Рис. 3

В нашей сети шесть подсетей. Видно, что каждый маршрутизатор подключён к трём подсетям.

2. На каждом маршрутизаторе поднять используемые интерфейсы и посмотреть соседей командой ***show cdp neighbors***.

3. Назначить интерфейсам сети адреса согласно рисунку 3 и своему варианту, где v – это номер варианта. Все маски 255.255.255.0.

4. Проверьте факт назначения адресов путём выполнения на каждом маршрутизаторе команд ***show running-config*** и ***show ip interface brief***. Для компьютеров используйте команду ***ipconfig*.**

5. Проверьте правильность назначения адресов путём выполнения на

каждом маршрутизаторе команд ***ping*** к непосредственным соседям. Например, на маршрутизаторе Router1 выполните

Router1#ping v.1.1.2

Router1#ping v.1.3.2

Router1#ping v.1.4.2

6. Поставим перед собой задачу связать между собой компьютеры PC1, PC2 и PC3. Для этого осуществим на маршрутизаторах настройку статической маршрутизации. В каждом маршрутизаторе пропишем маршруты на удалённые Ethernet сети.

Всего надо прописать шесть статических маршрутов для каждого роутера.

Например, чтобы из маршрутизатора router1 достичь удалённую Ethernet сеть v.1.5.0/24, пакеты можно направить на IP адрес 1.1.1.2 ближайшего внешнего интерфейса на пути в эту сеть командой ***router1(config)#ip route 1.1.5.0 255.255.255.0 1.1.1.2.***

Задайте остальные пять команд маршрутизации.

7. На каждом маршрутизаторе посмотреть таблицу маршрутизации командой ***show ip route.***

8. На компьютерах выполните команду ***Tracert*** (рис.4).

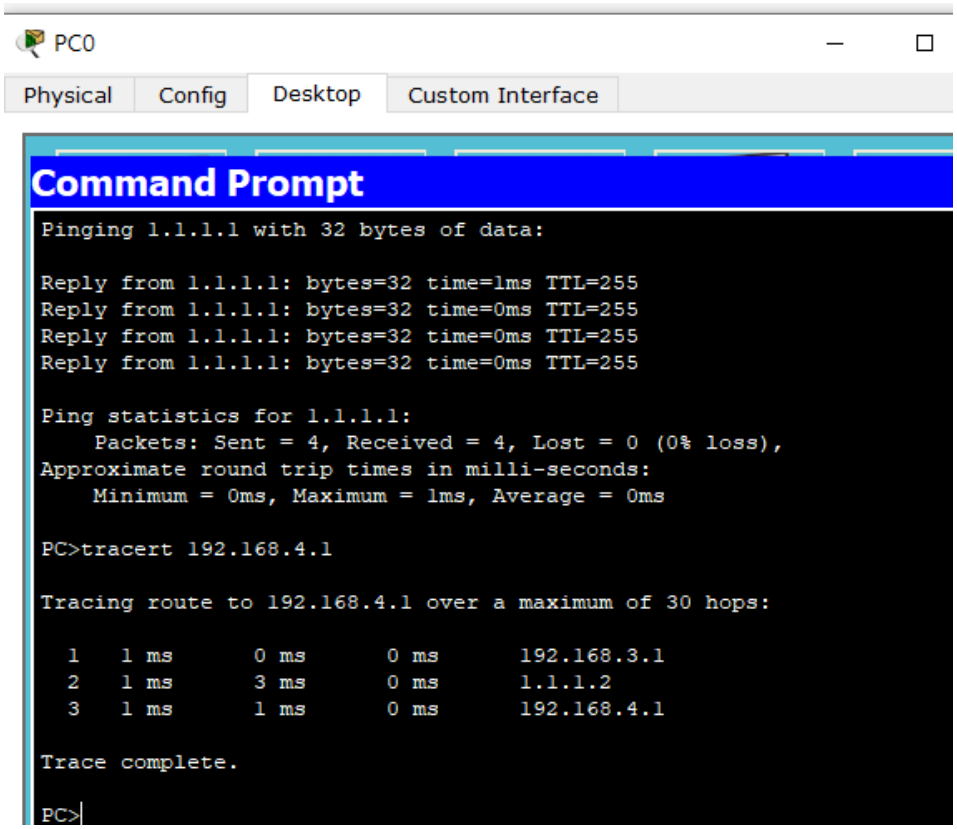

PC0
Physical
Config
Desktop
Custom Interface
Command Prompt
Pinging 1.1.1.1 with 32 bytes of data:
Reply from 1.1.1.1: bytes=32 time=1ms TTL=255
Reply from 1.1.1.1: bytes=32 time=0ms TTL=255
Reply from 1.1.1.1: bytes=32 time=0ms TTL=255
Reply from 1.1.1.1: bytes=32 time=0ms TTL=255
Ping statistics for 1.1.1.1:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 1ms, Average = 0ms
PC>tracert 192.168.4.1
Tracing route to 192.168.4.1 over a maximum of 30 hops:
1 1 ms 0 ms 0 ms 192.168.3.1
2 1 ms 3 ms 0 ms 1.1.1.2
3 1 ms 1 ms 0 ms 192.168.4.1
Trace complete.
PC>

Рис.4

РЕКОМЕНДУЕМАЯ ЛИТЕРАТУРА И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ

а) Список рекомендуемой литературы

основная

1. Олифер Виктор Григорьевич. Компьютерные сети. Принципы, технологии, протоколы: учеб. пособие для вузов по направл. "Информатика и вычисл. техника" и по спец. "Вычисл. машины, комплексы, системы и сети" / Олифер Виктор Григорьевич, Н. Олифер. - 4-е изд. - Санкт-Петербург: Питер, 2013.
2. Сети и телекоммуникации: учебник и практикум для вузов / К. Е. Самуйлов [и др.]; под редакцией К. Е. Самуйлова, И. А. Шалимова, Д. С. Кулябова. — Москва : Издательство Юрайт, 2021. — 363 с. — (Высшее образование). — ISBN 978-5-534-00949-1. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/469090
3. Замятина, О. М. Вычислительные системы, сети и телекоммуникации. Моделирование сетей : учебное пособие для вузов / О. М. Замятина. — Москва : Издательство Юрайт, 2021. — 159 с. — (Высшее образование). — ISBN 978-5-534-00335-2. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/470111

дополнительная

1. Оливер, Ибе Компьютерные сети и службы удаленного доступа / Ибе Оливер; перевод И. В. Синицын. — 2-е изд. — Саратов: Профобразование, 2019. — 335 c. — ISBN 978-5-4488-0054-2. — Текст: электронный // Электронно-библиотечная система IPR BOOKS: [сайт]. — URL: http://www.iprbookshop.ru/87999.html
2. Журнал сетевых решений/LAN// Электронно-библиотечная система IPR BOOKS, М: Открытые системы- 2018.- https://www.iprbookshop.ru/76360.html
3. Бизяев А.А., Сети связи и системы коммутации. Практикум : учеб пособие / Бизяев А.А. - Новосибирск : Изд-во НГТУ, 2016. - 84 с. - ISBN 978-5-7782-2935-8 - Текст : электронный // ЭБС "Консультант студента" : [сайт]. - URL: http://www.studentlibrary.ru/book/ISBN9785778229358.html
4. Маккормик Дж., Девять алгоритмов, которые изменили мир. Остроумные идеи, лежащие в основе современных компьютеров / Дж. Маккормик - М. : ДМК Пресс, 2014. - 236 с. - ISBN 978-5-94074-940-0 - Текст : электронный // ЭБС "Консультант студента" : [сайт]. - URL: http://www.studentlibrary.ru/book/ISBN9785940749400.html
5. Дибров, М. В. Сети и телекоммуникации. Маршрутизация в IP-сетях в 2 ч. Часть 1 : учебник и практикум для вузов / М. В. Дибров. — Москва : Издательство Юрайт, 2021. — 333 с. — (Высшее образование). — ISBN 978-5-9916-9956-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/471236
6. Дибров, М. В. Сети и телекоммуникации. Маршрутизация в IP-сетях в 2 ч. Часть 2 : учебник и практикум для вузов / М. В. Дибров. — Москва : Издательство Юрайт, 2021. — 351 с. — (Высшее образование). — ISBN 978-5-9916-9958-7. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/471908

учебно-методическая

1. **Курилова** О.Л. Межсетевое взаимодействие систем и сетей NGN. Лабораторный практикум : электронный учебный курс / О. Л. Курилова, В. Г. Козловский, В. П. Смолеха. - Ульяновск : УлГУ, 2019. - URL: https://portal.ulsu.ru/course/view.php?id=91890. - Режим доступа: Портал ЭИОС УлГУ. - Текст : электронный
2. **Курилова** О.Л. Методические рекомендации по выполнению лабораторных работ в интерактивном лабораторно-учебном классе телекоммуникационных протоколов и технологий СОТСБИ-NGN для студентов 09.03.02 «Информационные системы и технологии». 11.03.02 Инфокоммуникационные технологии и системы связи». 10.05.01 «Компьютерная

безопасность». 10.05.03 «Информационная безопасность автоматизированных систем». 11.04.02 «Инфокоммуникационные технологии и системы связи» : учебно-методическое пособие. Часть 1 / О. Л. **Курилова**. - Ульяновск : УлГУ, 2022. - 98 с. - Неопубликованный ресурс. - URL: http://lib.ulsu.ru/MegaPro/Download/ MObject/13323. - Режим доступа: ЭБС УлГУ. - Текст : электронный.

б) Электронно-библиотечные системы

1. Электронно-библиотечные системы:

1.1. Цифровой образовательный ресурс IPRsmart : электронно-библиотечная система : сайт / ООО Компания «Ай Пи Ар Медиа». - Саратов, [2023]. – URL: http://www.iprbookshop.ru. – Режим доступа: для зарегистрир. пользователей. - Текст : электронный.

1.2. Образовательная платформа ЮРАЙТ : образовательный ресурс, электронная библиотека : сайт / ООО Электронное издательство «ЮРАЙТ». – Москва, [2023]. - URL: https://urait.ru. – Режим доступа: для зарегистрир. пользователей. - Текст : электронный.

1.3. База данных «Электронная библиотека технического ВУЗа (ЭБС «Консультант студента») : электронно-библиотечная система : сайт / ООО «Политехресурс». – Москва, [2023]. – URL: https://www.studentlibrary.ru/cgi-bin/mb4x. – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

1.4. Консультант врача. Электронная медицинская библиотека : база данных : сайт / ООО «Высшая школа организации и управления здравоохранением-Комплексный медицинский консалтинг». – Москва, [2023]. – URL: https://www.rosmedlib.ru. – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

1.5. Большая медицинская библиотека : электронно-библиотечная система : сайт / ООО «Букап». – Томск, [2023]. – URL: https://www.books-up.ru/ru/library/ . – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

1.6. ЭБС Лань : электронно-библиотечная система : сайт / ООО ЭБС «Лань». – Санкт-Петербург, [2023]. – URL: https://e.lanbook.com. – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

1.7. ЭБС **Znanium.com :** электронно-библиотечная система : сайт / ООО «Знаниум». - Москва, [2023]. - URL: http://znanium.com . – Режим доступа : для зарегистрир. пользователей. - Текст : электронный.

2. КонсультантПлюс [Электронный ресурс]: справочная правовая система. / ООО «Консультант Плюс» - Электрон. дан. - Москва : КонсультантПлюс, [2023].

3. Базы данных периодических изданий:

3.1. eLIBRARY.RU: научная электронная библиотека : сайт / ООО «Научная Электронная Библиотека». – Москва, [2023]. – URL: http://elibrary.ru. – Режим доступа : для авториз. пользователей. – Текст : электронный

3.2. Электронная библиотека «Издательского дома «Гребенников» (Grebinnikon) : электронная библиотека / ООО ИД «Гребенников». – Москва, [2023]. – URL: https://id2.action-media.ru/Personal/Products. – Режим доступа : для авториз. пользователей. – Текст : электронный.

4. Федеральная государственная информационная система «Национальная электронная библиотека» : электронная библиотека : сайт / ФГБУ РГБ. – Москва, [2023]. – URL: https://нэб.рф. – Режим доступа : для пользователей научной библиотеки. – Текст : электронный.

5. Российское образование : федеральный портал / учредитель ФГАУ «ФИЦТО». – URL: http://www.edu.ru. – Текст : электронный.

6. Электронная библиотечная система УлГУ : модуль «Электронная библиотека» АБИС Мега-ПРО / ООО «Дата Экспресс». – URL: http://lib.ulsu.ru/MegaPro/Web. – Режим доступа : для пользователей научной библиотеки. – Текст : электронный.

в) Программное обеспечение

1) Программное обеспечение интерактивного лабораторно-учебного класса телекоммуникационных протоколов и технологий СОТСБИ-NGN.
2) Программы Microsoft Office.
3) Браузеры: Яндекс.Браузер, Google Chrome, Mozilla Firefox, Internet Explorer.
4) Программа моделирования компьютерных сетей Cisco Packet Tracer.