государственное автономное профессиональное образовательное учреждение Чувашской Республики «Межрегиональный центр компетенций – Чебоксарский электромеханический колледж» Министерства образования и молодежной политики Чувашской Республики

СБОРНИК МЕТОДИЧЕСКИХ УКАЗАНИЙ

по выполнению учебной практики в рамках междисциплинарного курса
МДК 02.01 Инфокоммуникационные системы и сети

для специальности СПО 09.02.03 Программирование в компьютерных системах

Автор: Авдиенко Д.В., преподаватель

г. Чебоксары 2017

РЕКОМЕНДОВАНО
Методическим советом
"МЦК-ЧЭМК" Миноборазования
Чувашии

Протокол №____
от "___"_____2017 г.
Председатель Методического совета
_____ О.Б. Кузнецова

Разработаны в соответствии с требованиями Федерального государственного образовательного стандарта по специальности среднего профессионального образования 09.02.03 Программирование в компьютерных системах и на основании Положения об организации самостоятельной работы в колледже и методических рекомендаций об организации самостоятельной работы в условиях реализации ФГОС

РАССМОТРЕНО
на заседании цикловой комиссии
специальности (И)
Протокол №____ от "___" _____2017 г.
Председатель ЦК: _____С.Н.Терентьева

Аннотация

При прохождении учебной практики по данной дисциплине у студентов должны сформироваться навыки разработки и проектирования прикладных программ. Сформироваться представление о роли специальных дисциплин в профессиональной деятельности.

Автор: Авдиенко Д.В.
Рецензенты:

доцент ФГБОУ «ЧГПУ им. И.Я.Яковлева» _____ Е.А. Тенякова

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Методические рекомендации по выполнению практических работ по учебной практики в рамках междисциплинарного курса МДК 02.01 Инфокоммуникационные системы и сети предназначены для обучающихся по специальности 09.02.03 Программирование в компьютерных системах.

Цель методических указаний: оказание помощи обучающимся при выполнении учебной в рамках междисциплинарного курса МДК 02.01 Инфокоммуникационные системы и сети.

Настоящие методические указания содержат работы, которые позволят обучающимся овладеть фундаментальными знаниями, профессиональными умениями и навыками деятельности по специальности, опытом творческой и исследовательской деятельности и направлены на формирование следующих компетенций:

ПРАКТИЧЕСКАЯ РАБОТА № 1

Введение в программу Cisco Packet Tracer (CPT)

Время работы: 2 часа

1. Цель работы: Научится работать с программой Cisco Packet Tracer (CPT)
2. Технические средства

2.1 Оборудование: компьютер

2.2 Программное обеспечение: Cisco Packet Tracer, MS Word.

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.(Рисунок 1.1).

Рисунок 1.1. Логотип программы CPT

Интерфейс программы Cisco Packet Tracer

На Рисунок 1.2 представлен интерфейс (главное окно) программы Cisco Packet Tracer.

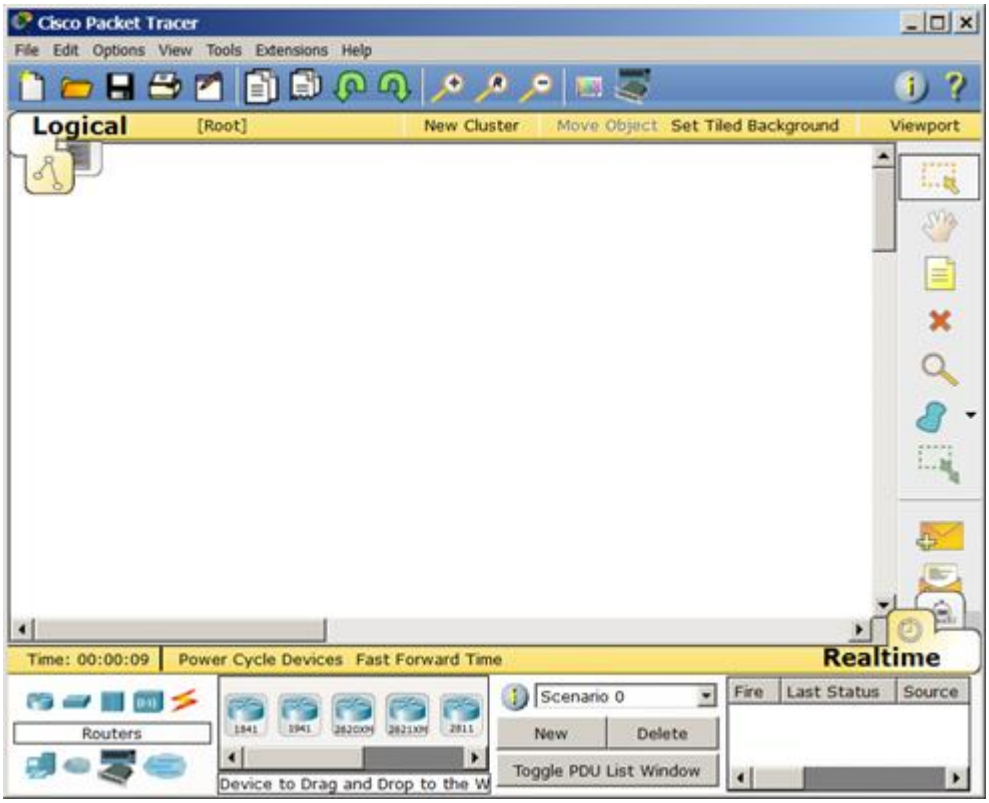


Рисунок 1.2. Интерфейс программы Cisco Packet Tracer (CPT)

Главное меню

Главное меню показано на Рисунок 1.3.

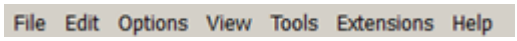


Рисунок 1.3. Главное меню

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 производить локализацию программы на другие языки.

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

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

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

Help (Помощь)–содержит помощь по программе.

Панель инструментов

Панель инструментов приведена на Рисунок 1.4.

Рисунок 1.4. Панель инструментов

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

Оборудование

Снизу, под рабочей областью, расположена панель оборудования. Данная панель содержит в своей левой части типы (классы) устройств, а в правой части – их наименование

(модели). При наведении на каждое из устройств, в прямоугольнике, находящемся в центре между ними будет отображаться его тип. Типы оборудования представлены на Рисунок 1.5.

Рисунок 1.5. 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 вы увидите 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 Рисунок 1.6.

Рисунок 1.6. 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 (Рисунок 1.7).

Рисунок 1.7. 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.

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

Медь 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 Рисунок 1.8 показано графическое меню программы.

Рисунок 1.8. Графическое меню (повернуто)

На этом рисунке 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 Рисунок 1.9.

Рисунок 1.9. 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 (Рисунок 1.10).

Рисунок 1.10. Физическая конфигурация ПК

Для изменения комплектации оборудования необходимо отключить его питание, кликнув мышью на кнопке питания и перетащить мышью нужный модуль в свободный слот, затем включить питание. В качестве примера я добавил в физическую конфигурацию ПК микрофон (PT-MICROPHONE), в результате чего ПК изменил свой значок в программе (Рисунок 1.11).

Рисунок 1.11. Изменение пиктограммы ПК после подключения к нему микрофона

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

Практическая работа 1-1. 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 (Рисунок 1.12).

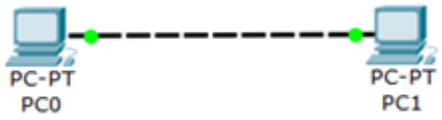


Рисунок 1.12. Сеть из двух ПК

Для решения нашей задачи на вкладке End Devices Ctrl+Alt+V (Конечные устройства) выбираем тип компьютера и переносим его мышью в рабочую область программы (Рисунок 13).

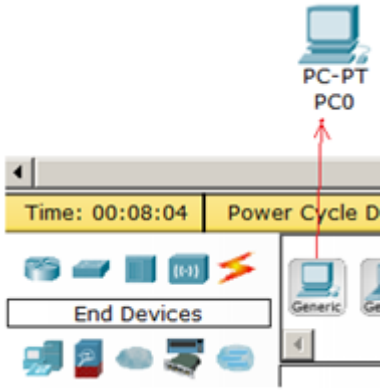


Рисунок 1.13. Устанавливаем в рабочую область программы первый ПК

Компьютеры соединяем посредством медного кроссовера Copper Cross-Over (Перекрестный кабель).

Совет

Если при выборе кроссовера зеленые лампочки не загорятся, то выберите тип соединения Автоматически.

Теперь приступим к настройке левого ПК: щелкаем на нем мышью, переходим на вкладку Ip Configuration (Настройка IP) – Рисунок 1.14.

Рисунок 1.14. Стрелка показывает на кнопку открытия окна IP Configuration

Для первого ПК вводим IP адрес 192.168.1.1 и маску подсети 255.255.255.0, окно закрываем (Рисунок 1.15). Аналогично настраиваем второй ПК на адрес 192.168.1.2 и ту же маску.

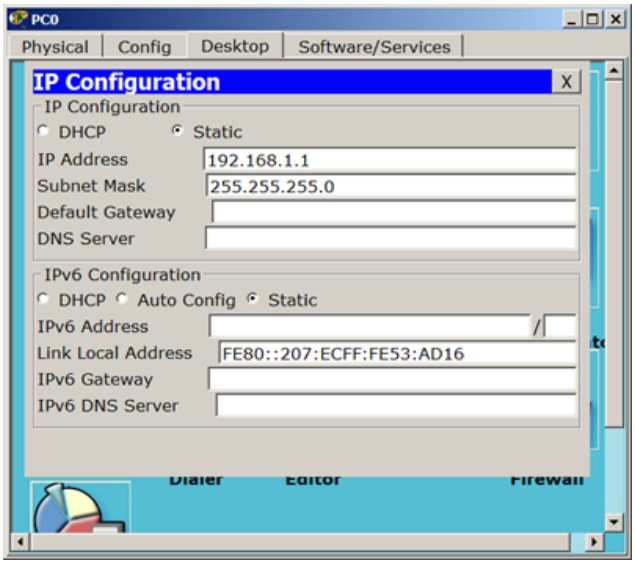


Рисунок 1.15. Окно настройки PC0

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 (Рисунок 1.16).

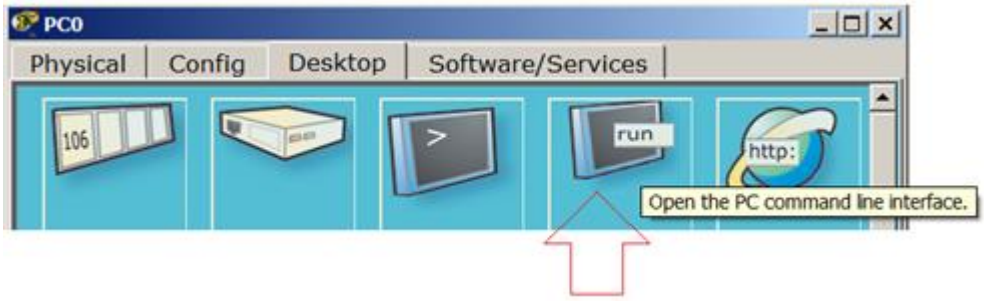


Рисунок 1.16. Кнопка run

Как видно из Рисунок 1.17 связь между ПК присутствует (настроена).

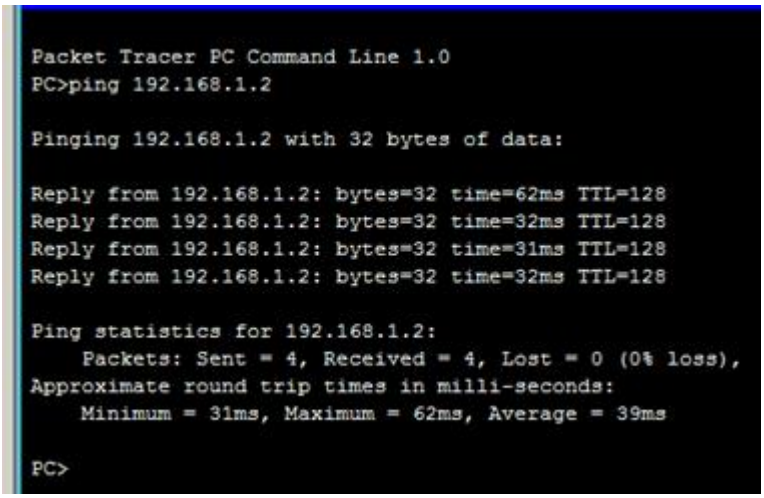


Рисунок 1.17. Пинг прошел успешно

Задание 1

Создайте свою сеть из 2х ПК и настройте ее работу.

3. Оформите отчет

ПРАКТИЧЕСКАЯ РАБОТА № 2.1

Организация Режим симуляции работы сети

Время работы: 2 часа

Цель работы: Научится работать с программой Cisco Packet Tracer (CPT)

Технические средства

2.1 Оборудование: компьютер

2.2 Программное обеспечение: Cisco Packet Tracer, MS Word.

Сформируйте в рабочем пространстве программы сеть из 4х ПК и 2х хабов. Задайте для ПК IP адреса и маску сети 255.255.255.0 (Рисунок 2.1).

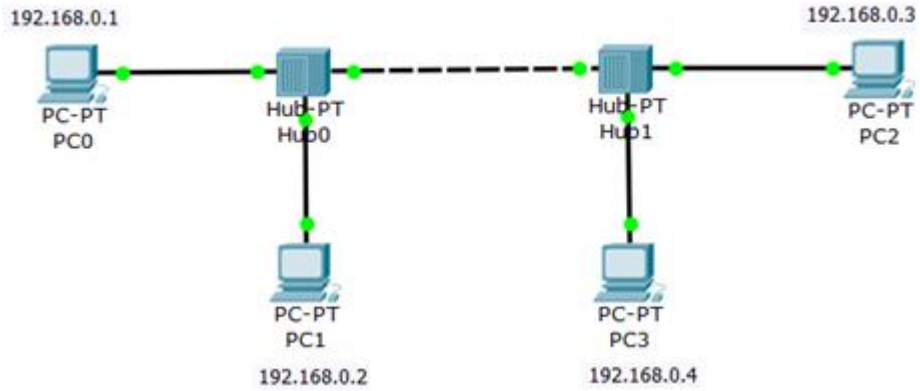


Рисунок 2.1. Все ПК расположены в одной сети

Теперь нужно перейти в режим симуляции комбинацией клавиш Shift+S, или, щелкнув мышью на иконку симуляции в правом нижнем углу рабочего пространства (Рисунок 2.2).

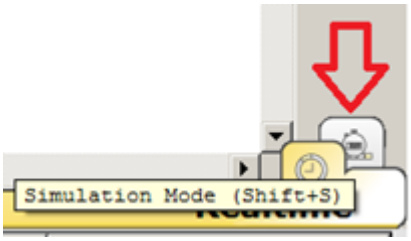


Рисунок 2.2. Кнопка Симуляция

Нажмите на кнопку Edit Filters (Изменить фильтры) и исключите все сетевые протоколы, кроме ICMP (Рисунок 2.3).

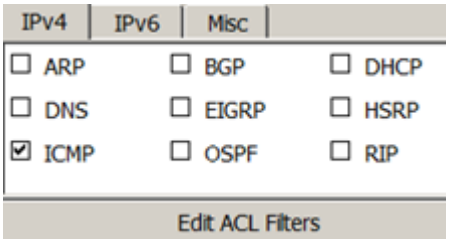


Рисунок 2.3. Флажок ICMP активен

Новый термин

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.

С одного из хостов попробуем пропинговать другой узел. Для этого выбираем далеко расположенные друг от друга узлы, для того, чтобы наглядней увидеть, как будут проходить пакеты по сети в режиме симуляции. Итак, с PC1 пингуем PC2 (Рисунок 2.4).

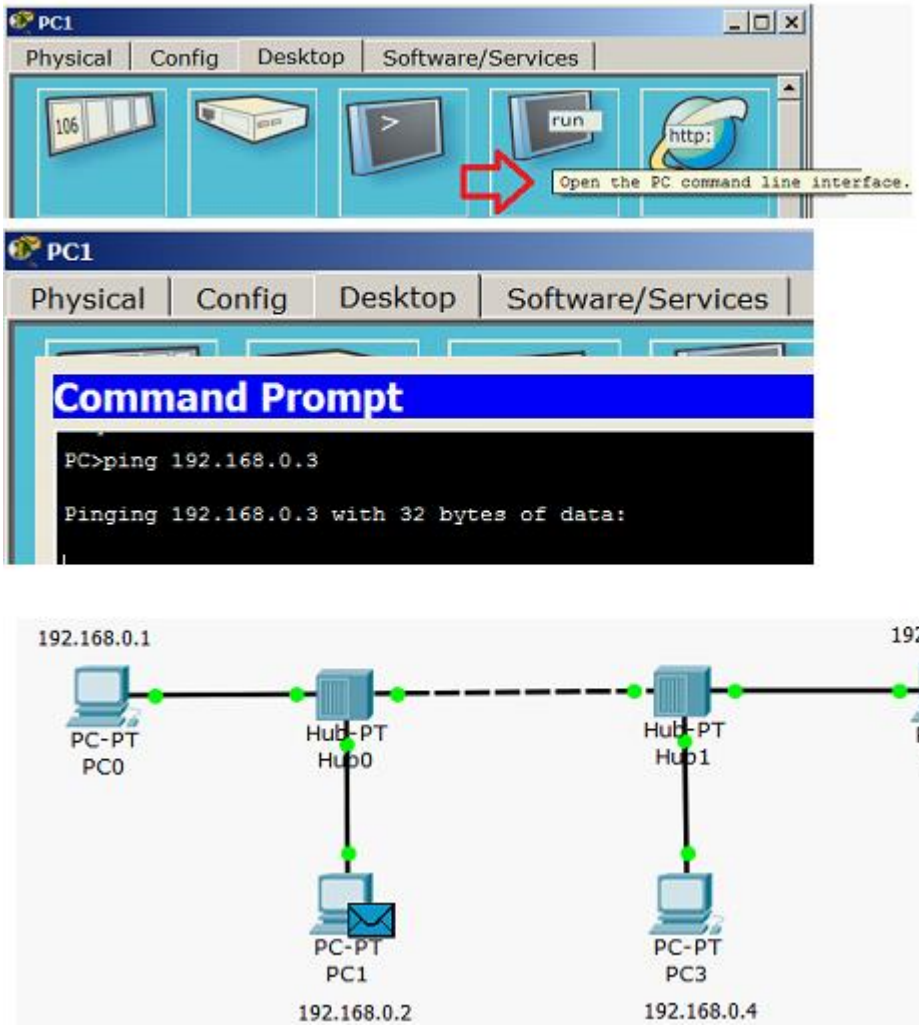


Рисунок 2.4. PC1 пингует PC2 (начало процесса)

Примечание

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

На PC1 образовался пакет (конвертик), который ждёт начала движения его по сети. Запустить продвижение пакет в сеть пошагово можно, нажав на кнопку Capture / Forward (Вперёд) в окне симуляции. Если нажать на кнопку Auto Capture / Play (воспроизведение), то мы увидим весь цикл прохождения пакета по сети. В (Список событий) мы можем видеть успешный результат пинга (Рисунок 2.5).

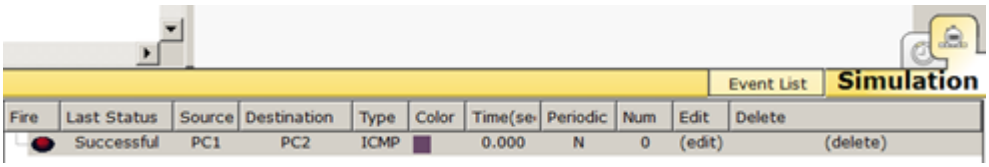


Рисунок 2.5. Связь PC1 и PC2 есть

Модель OSI в Cisco Packet Tracer

Щелчок мышью на конверте покажет нам дополнительную информацию о движении пакета по сети. При этом на первой вкладке мы увидим модель OSI (Рисунок 2.6). На вкладке OSI Model (Модель OSI) представлена информация об уровнях OSI, на которых работает данное сетевое устройство.

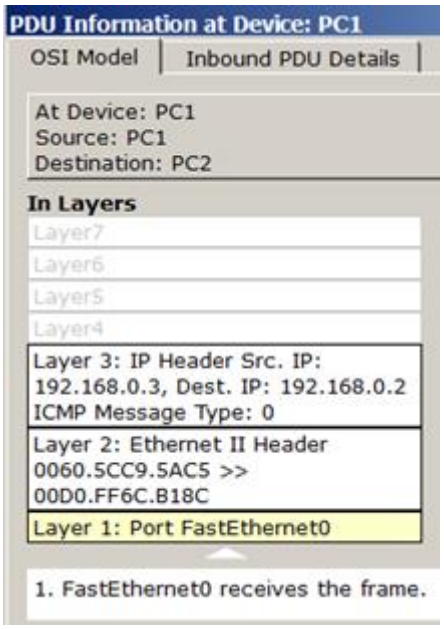


Рисунок 2.6. Мониторинг движения пакета на модели OSI

На другой вкладке можно посмотреть структуру пакета (Рисунок 2.7).

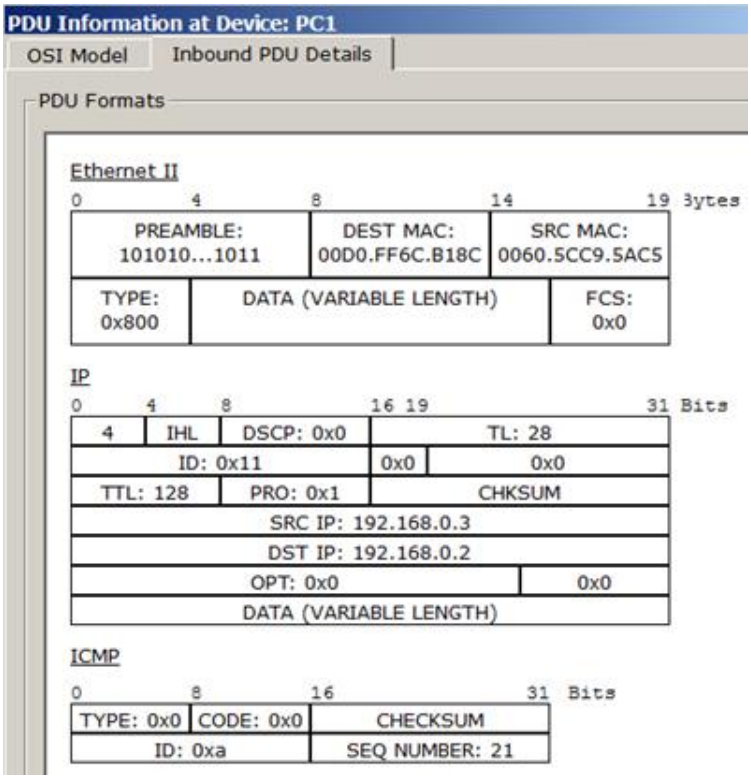


Рисунок 2.7. Структура пакета

В Packet Tracer предусмотрен режим моделирования (Симуляции), в котором показывается, как работает утилита Ping. Чтобы перейти в данный режим, необходимо нажать на значок Simulation Mode (Симуляция) в нижнем правом углу рабочей области или комбинацию клавиш Shift+S. Откроется Simulation Panel (Панель симуляции), в которой будут отображаться все события, связанные с выполнения ping-процесса. Моделирование прекращается либо при завершении ping-процесса, либо при закрытии окна симуляции. В режиме симуляции можно не только отслеживать используемые протоколы, но и видеть, на каком из семи уровней модели OSI данный протокол задействован. В процессе просмотра анимации мы увидели принцип работы хаба. Концентратор (хаб) повторяет пакет на всех портах в надежде, что на одном из них есть получатель информации. Если пакеты каким-то узлам не предназначенные, эти узлы игнорируют пакеты. А когда пакет вернётся отправителю, то мы увидим галочку"принятие пакета". (Рисунок 2.8).

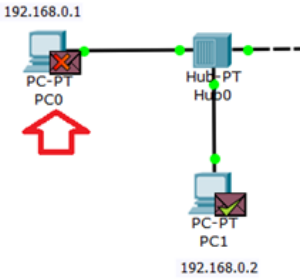


Рисунок 2.8. Значки игнорирования пакетов и подтверждение соединения

Командная строка

Если нажать на кнопку Auto Capture / Play (воспроизведение), то мы увидим весь цикл прохождения пакета по сети (процесс повторится 4 раза) – Рисунок 2.9.

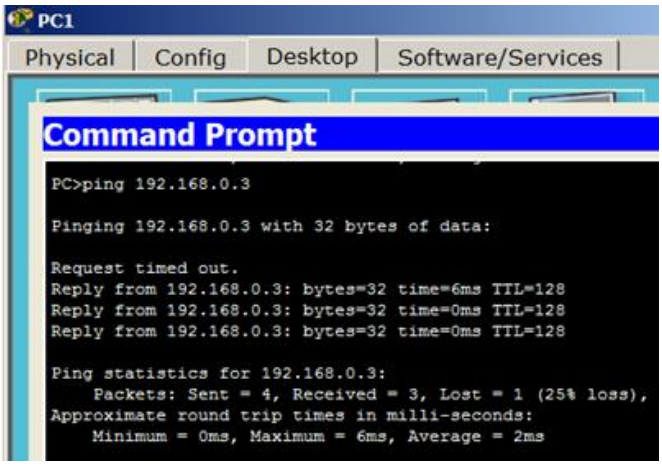


Рисунок 2.9. Пинг от ПК1 до ПК2

Здесь:

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

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

min - минимальное время ответа,

max - максимальное время ответа,

avg - среднее время ответа.

3. Оформите отчет

ПРАКТИЧЕСКАЯ РАБОТА № 2.2

Настройка сетевых параметров ПК в его графическом интерфейсе

Время работы: 2 часа

Цель работы: Научится работать с программой Cisco Packet Tracer (CPT)

Технические средства

2.1 Оборудование: компьютер

2.2 Программное обеспечение: Cisco Packet Tracer, MS Word.

Добавим в сеть еще один ПК – PC4.

Откроем свойства устройства PC4, нажав на его изображение. Для конфигурирования компьютера воспользуемся командой ipconfig из командной строки (Рисунок 2.10).

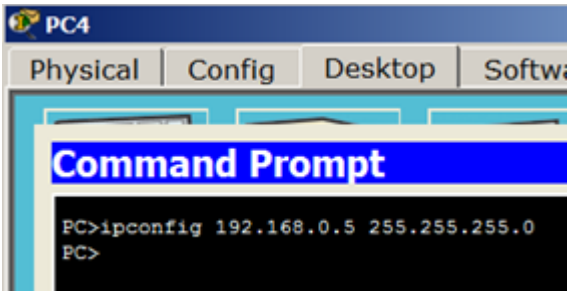


Рисунок 2.10. Назначаем для ПК ip адрес и маску сети

Как вариант, IP адрес и маску сети можно вводить в графическом интерфейсе устройства (Рисунок 2.11).

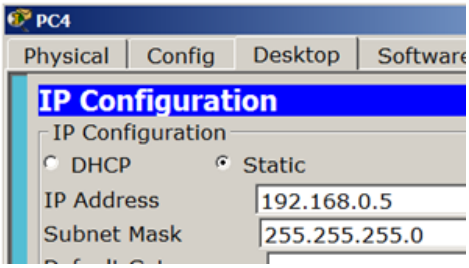


Рисунок 2.11. Второй способ конфигурирования компьютера (настройки узла сети)

На каждом компьютере проверим назначенные нами параметры командой ipconfig (Рисунок 2.12).

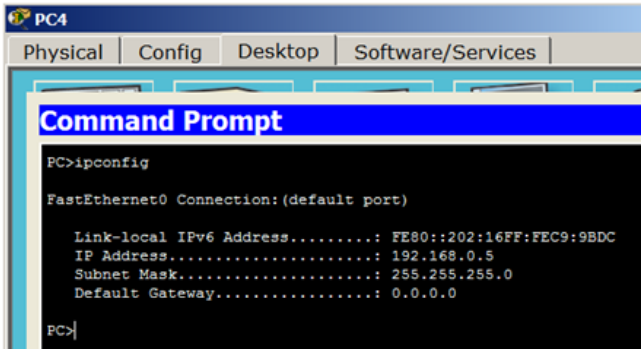


Рисунок 2.12. Проверка конфигурирования ПК3

3. Оформите отчет

ПРАКТИЧЕСКАЯ РАБОТА № 3

Моделирование сети с топологией звезда на базе концентратора

Время работы: 2 часа

1. Цель работы: Научится работать с программой Cisco Packet Tracer (CPT)

2. Технические средства

2.1 Оборудование: компьютер

2.2 Программное обеспечение: Cisco Packet Tracer, MS Word.

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.

В данном работе построим с помощью программного симулятора Packet Tracer построим сеть с топологией Звезда на базе концентратора (Рисунок 3.1) и изучим ряд новых приемов работы в этой программе.

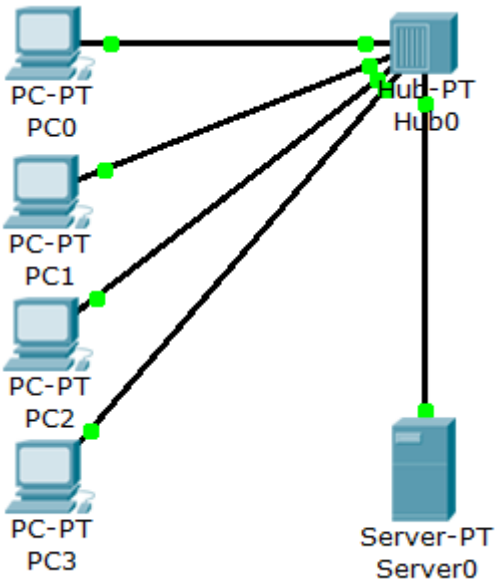


Рисунок 3.1. Моделирование сети с топологией звезда на базе концентратора

В рабочей области компонуем узлы сети

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. 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-a, 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 Config (Конфигурация)- Interface (Интерфейс)- FastEthetnet0. В группе параметров IP Configuration (Настройка IP) должен быть активирован переключатель Static (Статический) в поле IP Address необходимо ввести IP-адрес компьютера, маска появится автоматически. Port status (Состояние порта) – On (Вкл).

Инструмент создания заметок Place Note

Используя инструмент создания заметок Place Note (клавиша N), подписываем все IP устройств, а вверху рабочей области создаем заголовок нашего проекта "Изучение топологии звезда" - Рисунок 3.2.

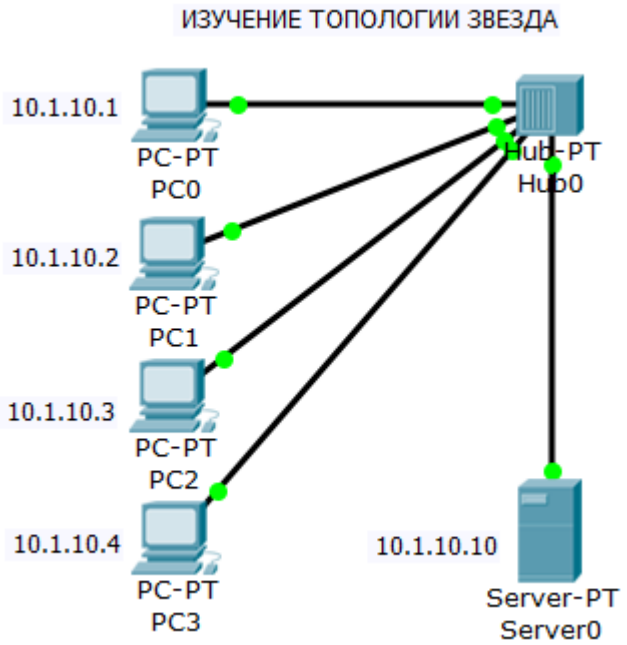


Рисунок 3.2. Используем инструмент Place Note (Заметка)

Совет

IP адреса следует скопировать из окна Config (Конфигурация). При этом активируйте 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) - Рисунок 3.3.

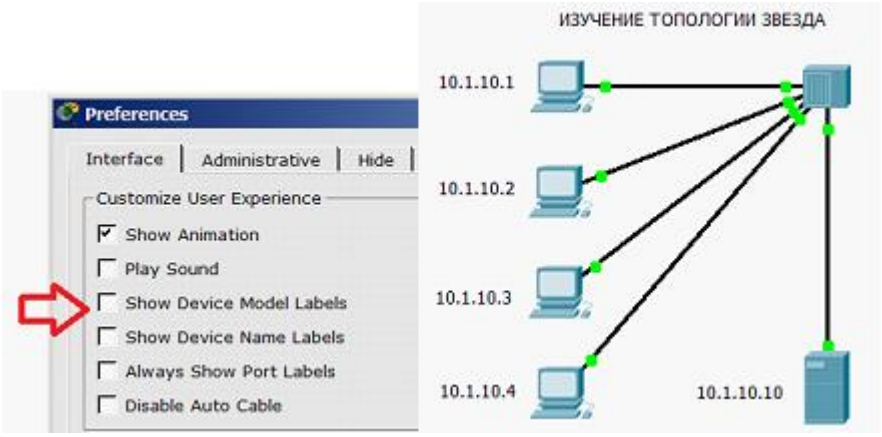


Рисунок 3.3. Дезактивируем флажок Show device model labels

Для проверки работоспособности сети отправим с компьютера на другой ПК тестовый сигнал ping и 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.

Далее окно Event list (Список событий) закрываем (Рисунок 3.4).

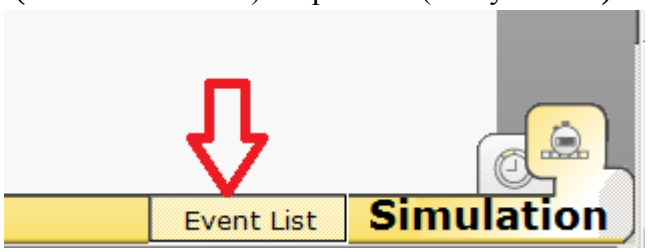
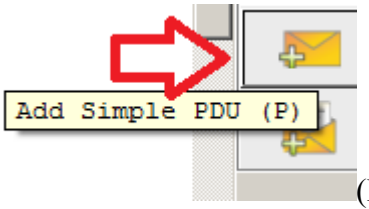


Рисунок 3.4. Кнопка Event list (Список событий)

В правой части окна, в графическом меню выбираем



(Простой PDU) и щелчками мыши, устанавливаем его на ПК - выбираем 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 – Рисунок 3.5

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

Рисунок 3.5. Успешное прохождение пакетов по сети

Новый термин

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

Полезные приемы работы в CPT

Предположим, что вам нужно спроектировать и настроить следующую сеть (Рисунок 3.6). Рассмотрим, как можно ускорить и упростить этот процесс.

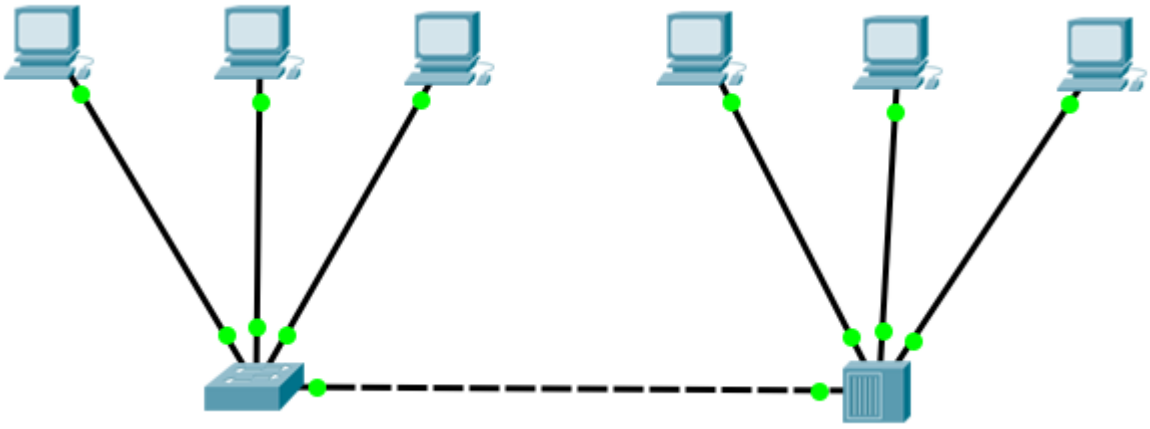


Рисунок 3.6. Постановка задачи

Поместите в рабочую область первый ПК (это будет PC) и настройте его (Рисунок 3.7).

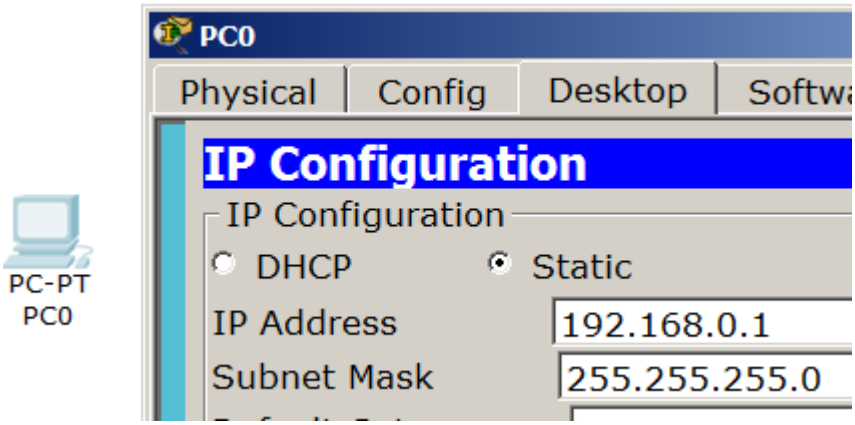


Рисунок 3.7. Настраиваем PC0

Удерживая клавишу Ctrl скопируйте этот ПК несколько раз и настройте остальные адреса ПК, меняя только последнюю цифру IP адреса (Рисунок 3.8).

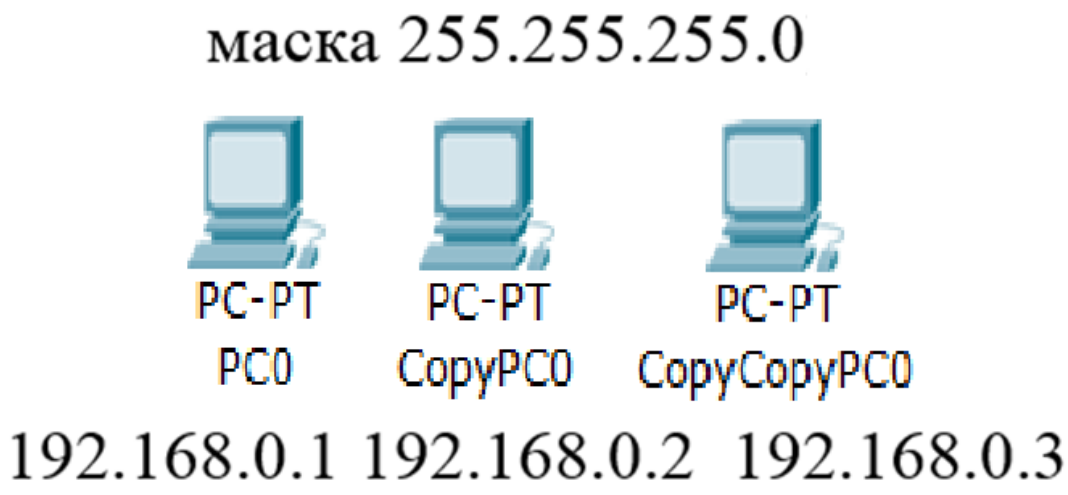


Рисунок 3.8. Быстрое создание и настройка трех ПК

Далее скопируйте, удерживая Ctrl сразу три ПК и настройте их также, меняя только последнюю цифру IP адреса (Рисунок 3.9).

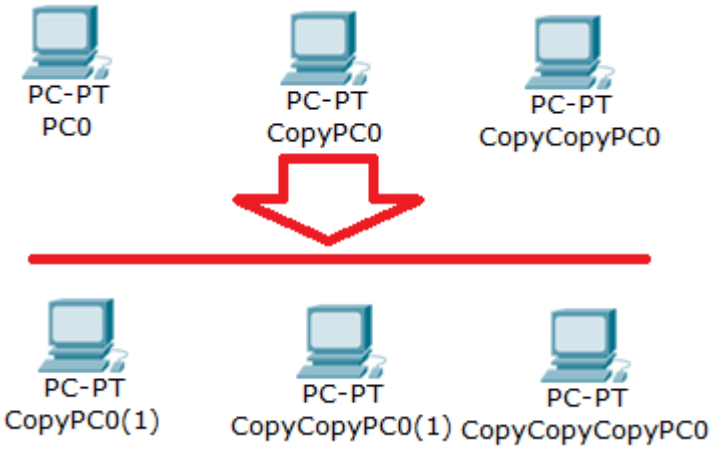


Рисунок 3.9. Копируем все три ПК сразу

Добавление свитча и хаб делаем традиционно, а подключение кабеля - автоматическое.

3.Оформите отчет

ПРАКТИЧЕСКАЯ РАБОТА № 4.1

Моделирование сети с топологией звезда на базе коммутатора

Время работы: 2 часа

1.Цель работы: Научится работать с программой Cisco Packet Tracer (CPT)

2.Технические средства

2.1 Оборудование: компьютер

2.2 Программное обеспечение: Cisco Packet Tracer, MS Word.

Сначала немного теории. Hub работает на 1м уровне модели OSI и отправляет информацию во все порты, кроме порта – источника. Switch работает на 2м уровне OSI и отправляет информацию только в порт назначения за счет использования таблицы MAC адресов хостов. В сетях IP существует 3 основных способа передачи данных: Unicast, Broadcast, Multicast.

Unicast (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 (Рисунок 4.1).

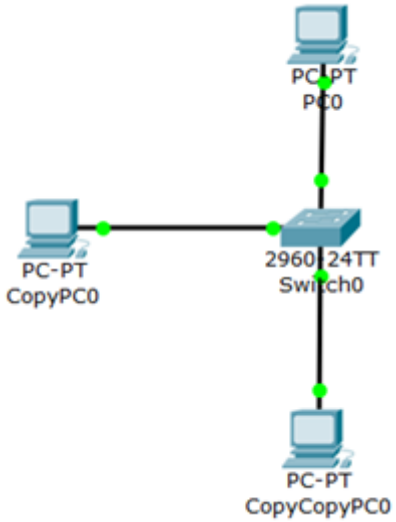


Рисунок 4.1. Звезда на базе коммутатора модели 2960

На вкладке Physical вы можете посмотреть вид коммутатора, имеющего 24 порта Fast Ethernet и 2 порта Gigabit Ethernet (Рисунок 4.2).

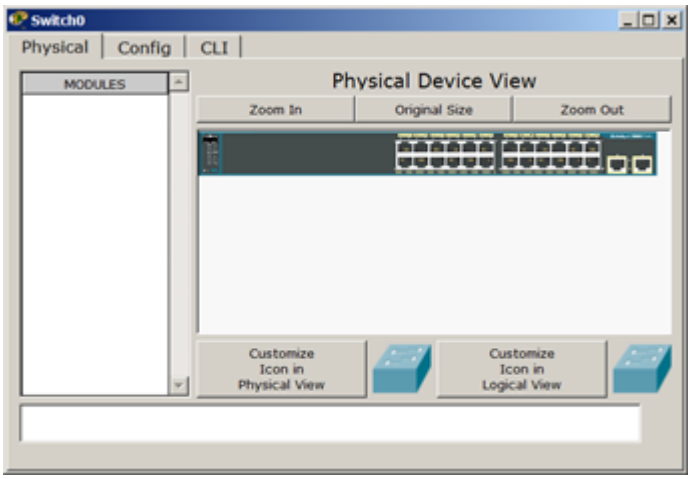
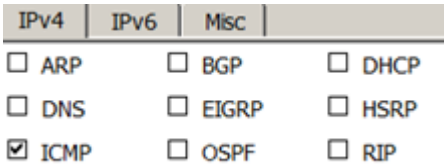


Рисунок 4.2. Физический внешний вид коммутатора модели 2960



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

Задание 4.1

Произведите проектирование локальной сети из хаба, коммутатора и 4х ПК

Сеть, которую необходимо спроектировать представлена на Рисунок 4.3.

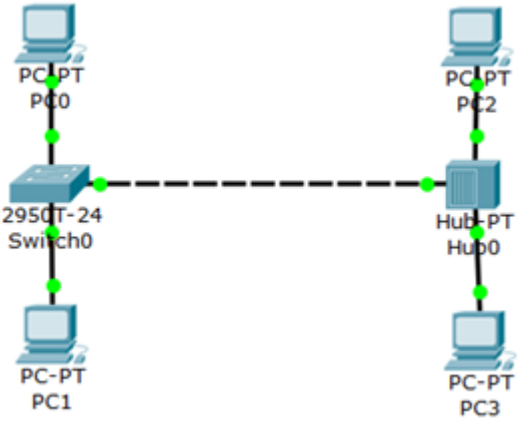


Рисунок 4.3. Проектируемая сеть

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

Примечание

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.

3.Оформите отчет

ПРАКТИЧЕСКАЯ РАБОТА № 4.2

Исследование качества передачи трафика по сети

Время работы: 2 часа

1.Цель работы: Научится работать с программой Cisco Packet Tracer (CPT)

2.Технические средства

2.1 Оборудование: компьютер

2.2 Программное обеспечение: Cisco Packet Tracer, MS Word.

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 (Рисунок 4.4).

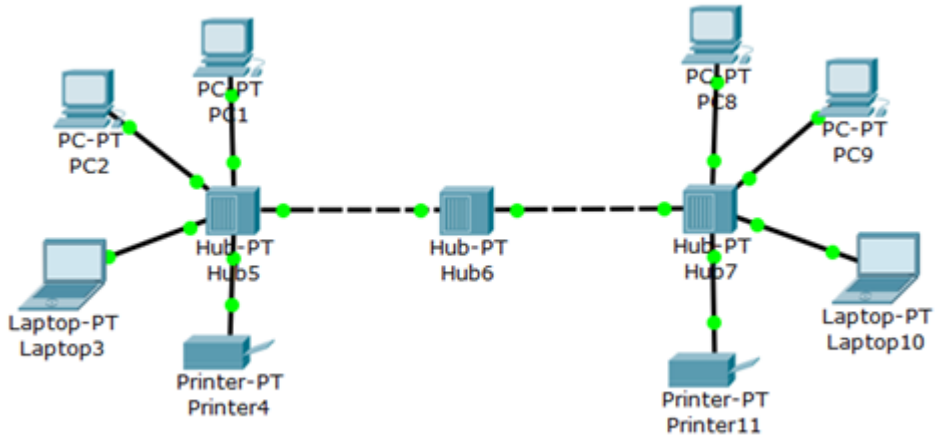


Рисунок 4.4. Топология сети для нашей работы

Первое знакомство с Traffic Generator

В окне управления PC1 во вкладке Desktop выберите приложение Traffic Generator и задайте настройки, как на Рисунок 4.5 для передачи трафика от PC1 на PC8. Для ясности я рядом с английской версией окна разместил тот же текст в русской версии программы CPT.

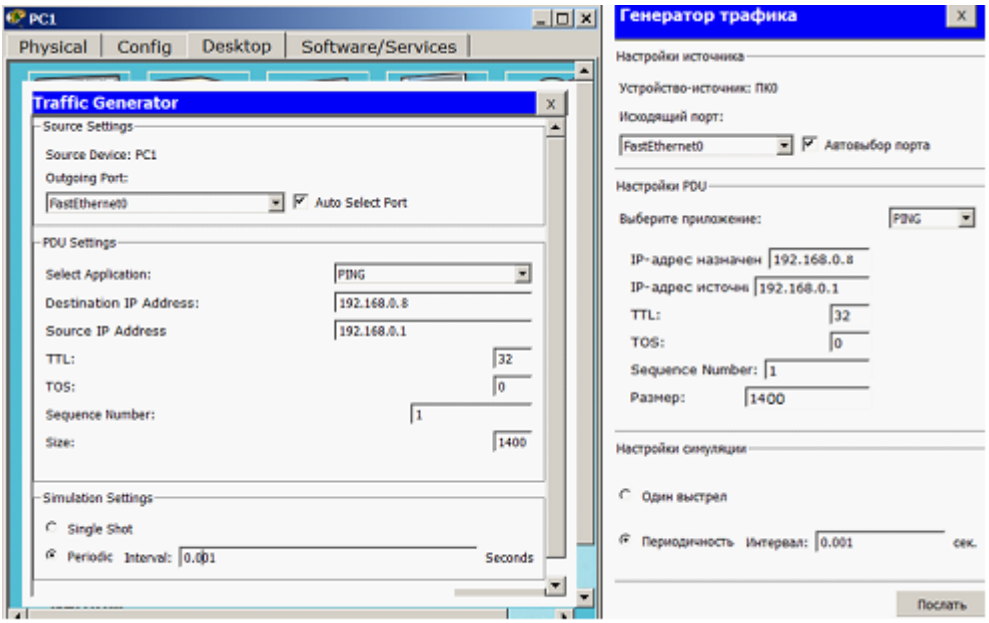


Рисунок 4.5. Настройка генератора трафика (Вариант трафика от PC1 до PC8)

Итак, при помощи протокола ICMP мы сформировали трафик между компьютерами PC1 с адресом 192.168.0.1 и PC8 с адресом 192.168.0.8. 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: 192.168.0.8 (адресполучателя);

Source IP Address: 192.168.0.1 (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: 0.3 Seconds (период повторения пакетов)

Внимание

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

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

Новый термин

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 PC8 при помощи команды ping –n 200 192.168.0.8и будем оценивать качество работы сети по числу потерянных пакетов. Параметр "–n" позволяет задать количество передаваемых эхо-запросов (у нас их 200) – Рисунок 4.6.

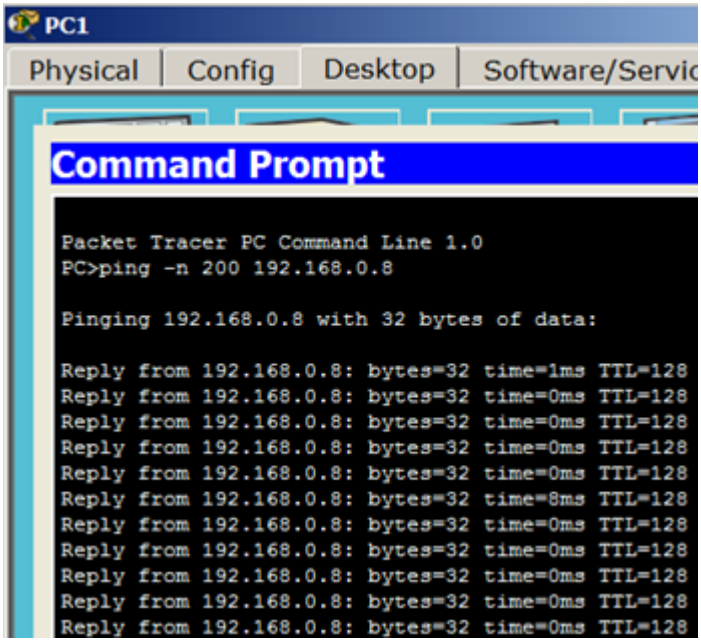


Рисунок 4.6. Отправляем 200 пакетов на PC8

Одновременно с пингом, нагрузите сеть, включив генератор трафика на компьютере PC2 (узел назначения – PC8, размер поля данных–2500 байт, период повторения передачи - 0,1 сек. – Рисунок 4.7.

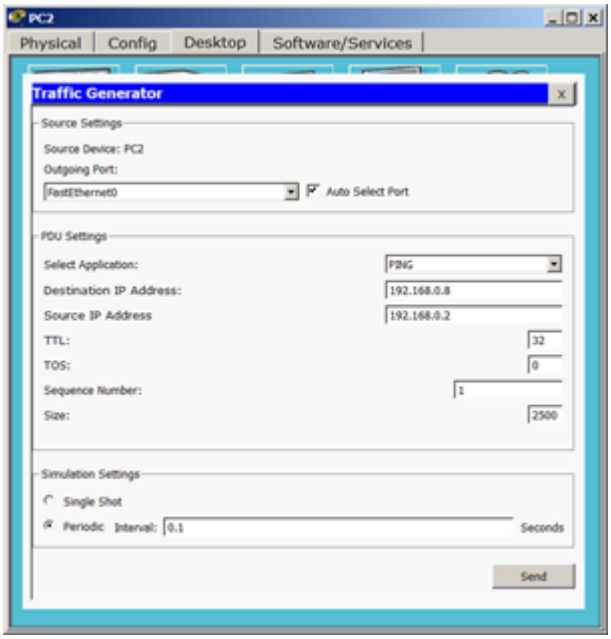


Рисунок 4.7. Увеличиваем нагрузку на сеть

Для оценки качества работы сети - зафиксируйте число потерянных пакетов (Рисунок 4.8).

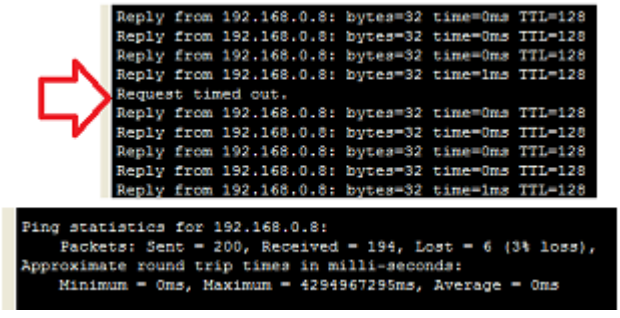


Рисунок 4.8. Потеряно 6 пакетов

Примечание

Как вариант можно было бы загрузить сеть путем организации еще одного потока трафика между какими-либо узлами сети, например, включив генератор трафика еще на ноутбуке PC3.

В заключение этой части нашей работы остановите 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 (Рисунок 4.9). Немного подождите и убедитесь, что сеть находится в рабочем состоянии - все маркеры портов не красные, а зеленые.

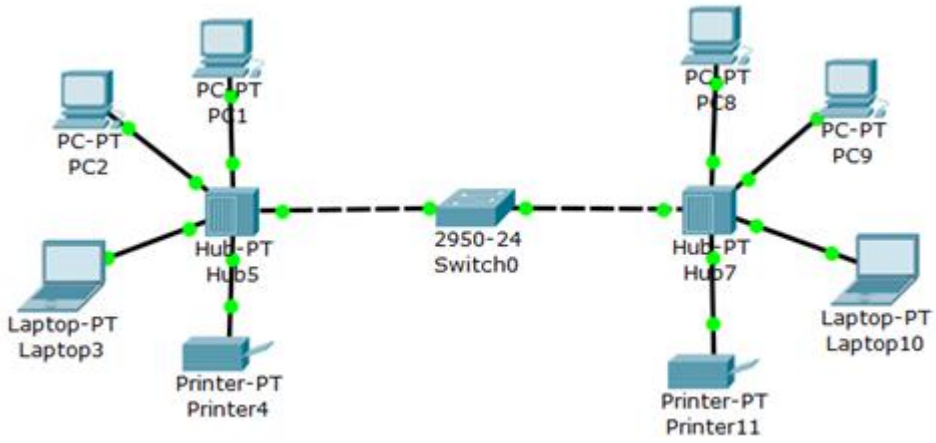


Рисунок 4.9. Топология сети при замене центрального концентратора на коммутатор

Снова задайте поток пакетов между PC1 и PC8 при помощи команды ping –n 200 192.168.0.8и включите Traffic Generator на PC2. Проследите работу нового варианта сети. Убедитесь, что за счет снижения паразитного трафика качество работы сети стало выше (

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

Рисунок 4.10).


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


Рисунок 4.10. Потерян 1 пакет

Задание 2

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

3.Оформите отчет

ПРАКТИЧЕСКАЯ РАБОТА № 5.1

Исследование качества передачи трафика по сети

Время работы: 2 часа

1.Цель работы: Научится работать с программой Cisco Packet Tracer (CPT)

2.Технические средства

2.1 Оборудование: компьютер

2.2 Программное обеспечение: Cisco Packet Tracer, MS Word.

Консоль

Большинство сетевых устройств компании CISCO допускают конфигурирование. Для этого администратор сети должен подключиться к устройству через прямое кабельное (консольное) подключение (Рисунок 5.1).

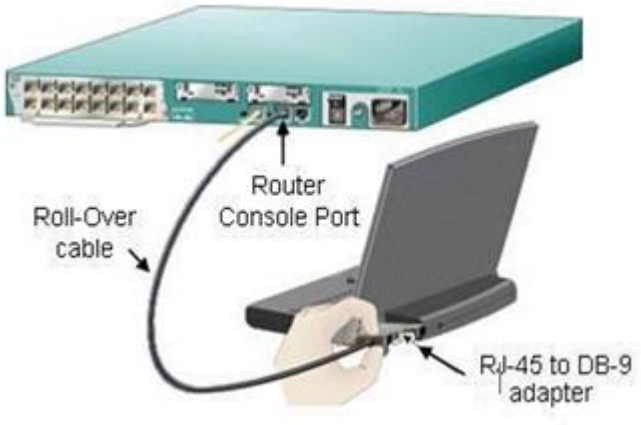


Рисунок 5.1. Консольное подключение к сетевому устройству

Итак, программирование устройств CISCO чаще всего производят через консольный порт RJ-45. На Рисунок 5.2 и Рисунок 5.3 приведены фотографии консольных разъёмов на маршрутизаторе и 2 варианта консольного кабеля.

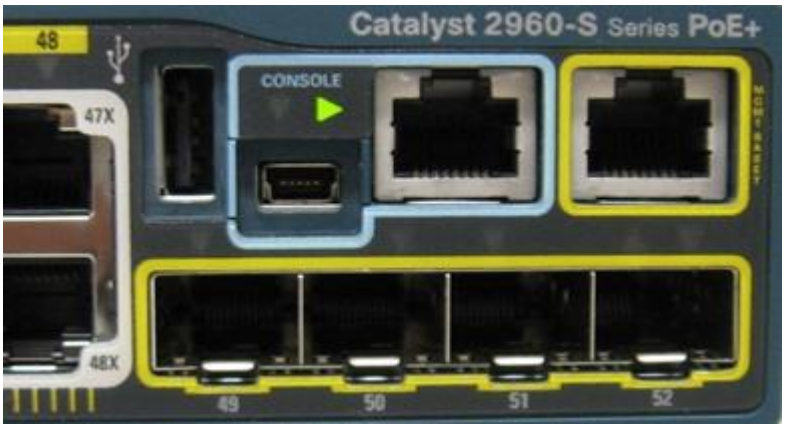


Рисунок 5.2. Синим цветом показаны разъёмы под управляющий (консольный) кабель

Рисунок 5.3. Варианты консольных кабелей

Примечание

Классический консольный кабель имеет разъем DB9 для подключения к COM-порту компьютера и разъем RG-45 для подключения к консольному порту маршрутизатора. Сейчас Cisco активно продвигает новые маршрутизаторы серий 28xx, 38xx и т.д. В них предусмотрена возможность конфигурирования через USB-интерфейс (используются обычные USB-кабели).

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

Режимы работы с устройством при использовании CLI

Командная строка представляет собой место, куда пользователь вводит символы, формирующие управляющее воздействие. Работа с командной строкой осуществляется в нескольких режимах (таблица 5.1).

Таблица 5.1. 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

Несколько слов о виде 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 привилегированном режиме. 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 режиме 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.

ПРАКТИЧЕСКАЯ РАБОТА № 5.1.1

Знакомство с командами Cisco IOS

Время работы: 2 часа

1.Цель работы: Научится работать с программой Cisco Packet Tracer (CPT)

2.Технические средства

2.1 Оборудование: компьютер

2.2 Программное обеспечение: Cisco Packet Tracer, MS Word.

В Cisco Packet Tracer интерфейс командной строки для устройств доступен в окне настроек параметров сетевого устройства на вкладке "CLI". Это окно имитирует прямое кабельное (консольное) подключение к сетевому устройству. Работа с командной строкой (CLI) для настройки (программирования) сетевого производится с помощью команд операционной системы Cisco IOS (Рисунок 5.4).

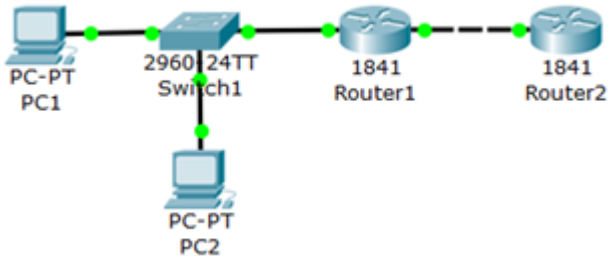


Рисунок 5.4. Сеть для выполнения команд ОС CiscoIOS

Выше мы говорили о режимах командного интерфейса – пользовательском, привилегированном и глобального конфигурация. Проделайте все команды входа и выхода в эти режимы для Router1. При входе в сетевое устройство Router1 и нажатии на клавишу Enter командная строка имеет вид как на Рисунок 5.5. Выход из пользовательского режима – logout.

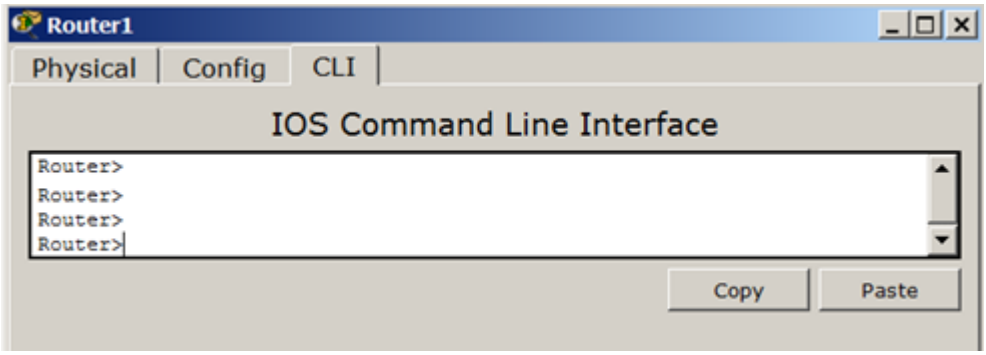


Рисунок 5.5. Вид командной строки в пользовательском режиме

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

Примечание

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

Режим глобального конфигурирования — реализует мощные однострочные команды, которые решают задачи конфигурирования. Для входа в режим глобального конфигурирования используется команда привилегированного режима configure terminal. Выход командой exit или end.

Установка пароля на вход в привилегированный режим

Пароль доступа позволяет вам контролировать доступ в привилегированный режим от неопытных пользователей и злоумышленников. Напомним, что только в привилегированном режиме можно вносить конфигурационные изменения. На Router1 установите пароль доступа в этот режим как "parol" командой Router1(config)#enable password parol, затем выйдите из привилегированного режима сетевого устройства, то есть перейдите в пользовательский режим. Попытайтесь снова зайти в привилегированный режим. Как видите, без ввода пароля это теперь невозможно (Рисунок 5.6).

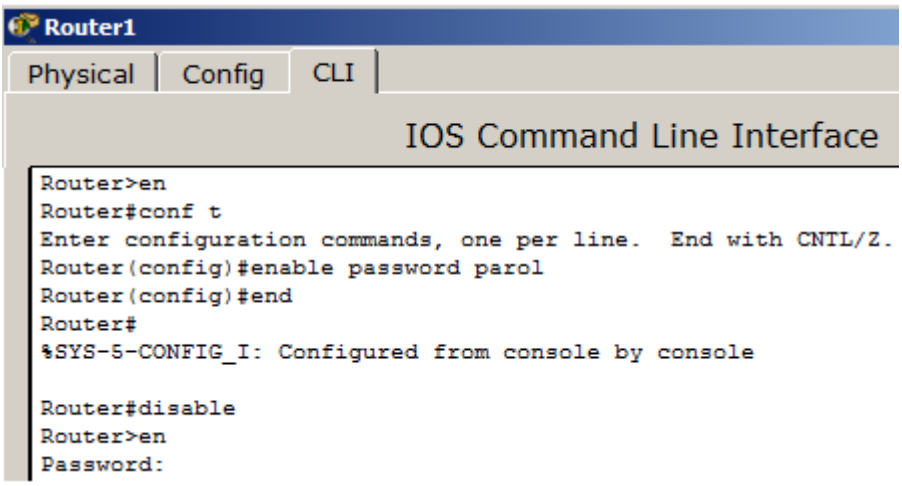


Рисунок 5.6. Установка пароля на вход в привилегированный режим

Для изменения пароля введем новый пароль привилегированного режима (Рисунок 5.7).

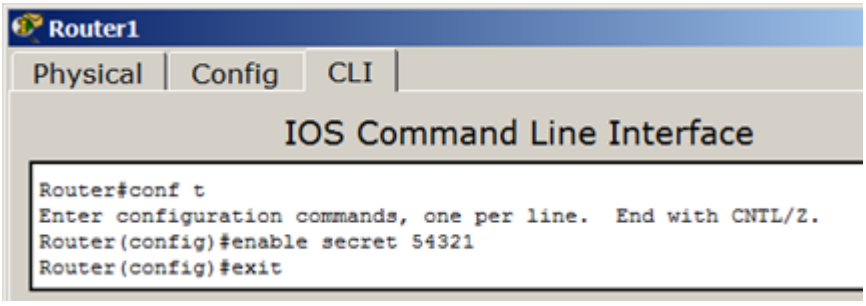


Рисунок 5.7. Был пароль 12345, стал пароль 54321

Для сброса пароля можно произвести перезагрузку роутера (Рисунок 5.8).

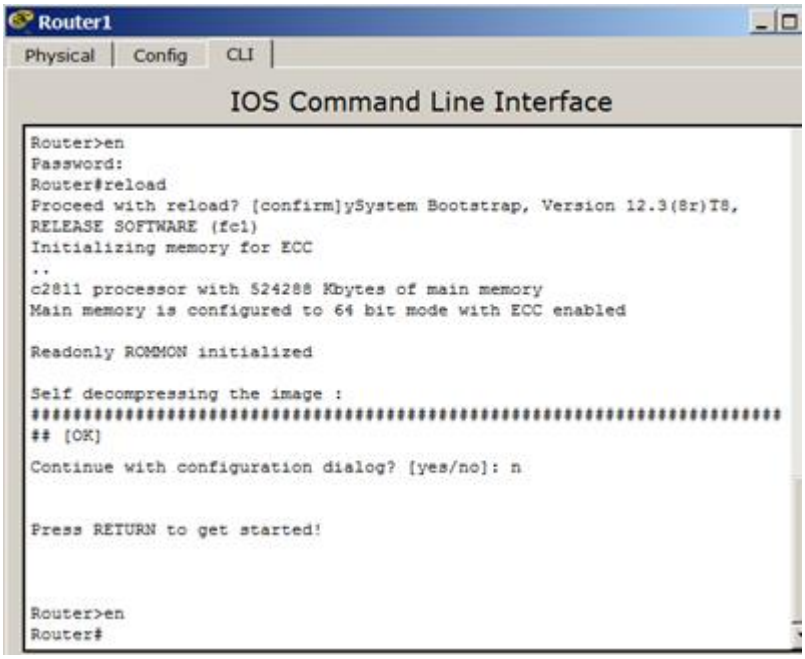


Рисунок 5.8. Перезагрузка R1 командой reload

Советы при работе с CLI

Все команды в консоли можно сокращать, но, важно, чтобы сокращение однозначно указывало на команду. Используйте клавишу Tab и знак вопроса (?). По нажатию Tab сокращенная команда дописывается до полной, а знак вопроса (?), следующий за командой, выводит список дальнейших возможностей и небольшую справку по ним. Можно перейти к следующей команде, сохранённой в буфере. Для этого нажмите на Стрелку вниз или Ctrl + N. Можно вернуться к командам, введённым ранее. Нажмите на Стрелку вверх или Ctrl + P (Рисунок 5.9).

Рисунок 5.9. Стрелки Вверх или Вниз на клавиатуре позволяют листать ранее использованные вами команды

Активная конфигурация автоматически не сохраняется и будет потеряна в случае сбоя электропитания. Чтобы сохранить настройки роутера используйте команду write memory (Рисунок 5.10).

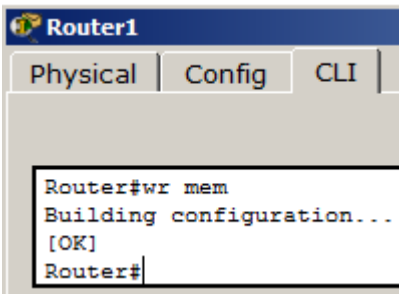


Рисунок 5.10. Сохранение текущей конфигурации R1

Задание 5.1

Схема сети показана на Рисунок 5.11.

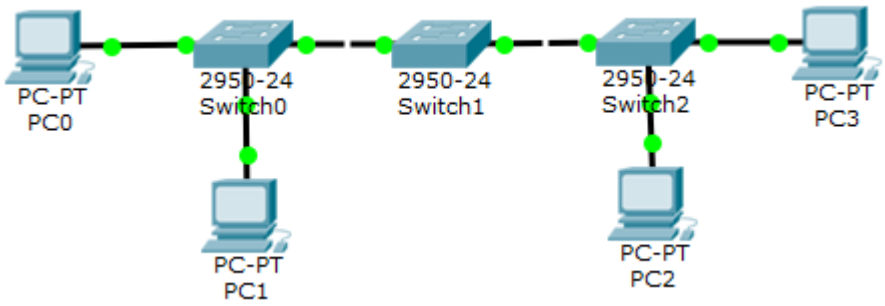


Рисунок 5.11. Схема сети

Нужно:

Построить такую сеть

Изменить имя коммутаторов Cisco;

Обеспечить парольный доступ к привилегированному режиму на коммутаторах;

Задать ip-адреса и маски коммутаторам (172.16.1.11/24, 172.16.1.12/24, 172.16.1.13/24);

Задать ip-адреса и маски сетей персональным компьютерам. (172.16.1.1/24, 172.16.1.2/24, 172.16.1.3/24, 172.16.1.4/24);

Убедиться в достижимости всех объектов сети по протоколу IP;

Переключившись в "Режим симуляции" и рассмотреть и пояснить процесс обмена данными по протоколу ICMP между устройствами (выполнив команду Ping с одного компьютера на другой).

Виртуальные локальные сети VLAN

VLAN (Virtual Local Area Network) — виртуальная локальная компьютерная сеть из группы хостов с общим набором требований. VLAN позволяют хостам группироваться или дистанцироваться между собой. Устройства, в пределах одной VLAN могут общаться, а узлы, находящиеся в разных VLAN'ах, невидимы друг для друга.

ПРАКТИЧЕСКАЯ РАБОТА № 5.1.2

VLAN с одним коммутатором

Время работы: 2 часа

1.Цель работы: Научится работать с программой Cisco Packet Tracer (CPT)

2.Технические средства

2.1 Оборудование: компьютер

2.2 Программное обеспечение: Cisco Packet Tracer, MS Word.

Для рисования ПК выбираем в конечных устройства настольный компьютер и, удерживая Ctrl, (так быстрее) нажмите 1 раз на ПК а затем рисуйте нужное кол-во ПК, щелкая мышкой (Рисунок 5.12). Этим приемом вы сможете за один раз нарисовать сразу 4 ПК.

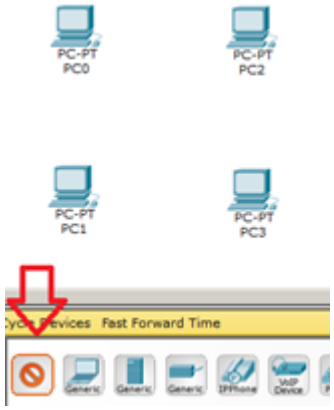


Рисунок 5.12. Выбор устройств, удерживая Ctrl

Устанавливаем коммутатор и, удерживая Ctrl, создаем подключение прямым кабелем, выбирая порты коммутатора. После инициализации портов все лампы загорятся зеленым. На схему будет две подсети (Рисунок 5.13) .

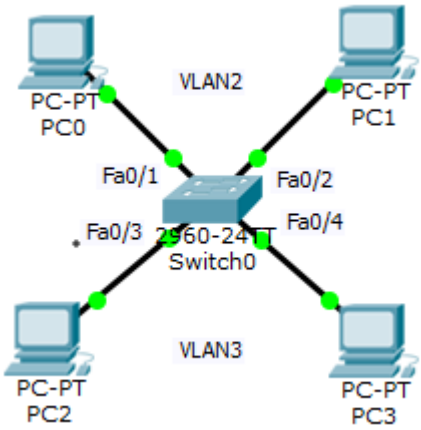


Рисунок 5.13. Две подсети: VLAN2 и VLAN3

Примечание

Имя VLAN1 используется по умолчанию, его лучше в нашем примере не использовать.

На коммутаторе набираем команду en и входим в привилегированный режим. Затем набираем команду conf t для входа в режим глобального конфигурирования. Если подвести курсор мыши к портам коммутатора, то вы увидите какие порты в каком сегменте задействованы. Для VLAN3 – это Fa0/3 и Fa0/4 (предположим, что это будет бухгалтерия -

buh) и для VLAN2 – это Fa0/1 и Fa0/2 (предположим, что это будет склад – sklad). Сначала будем конфигурировать второй сегмент сети VLAN2 (sklad) – Рисунок 5.14.

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

Рисунок 5.14. VLAN2 получает имя sklad

В виртуальной сети VLAN2 настраиваем порты коммутатора Fa0/1 и Fa0/2 как access порты, т.е. порты для подключения пользователей (Рисунок 5.15).

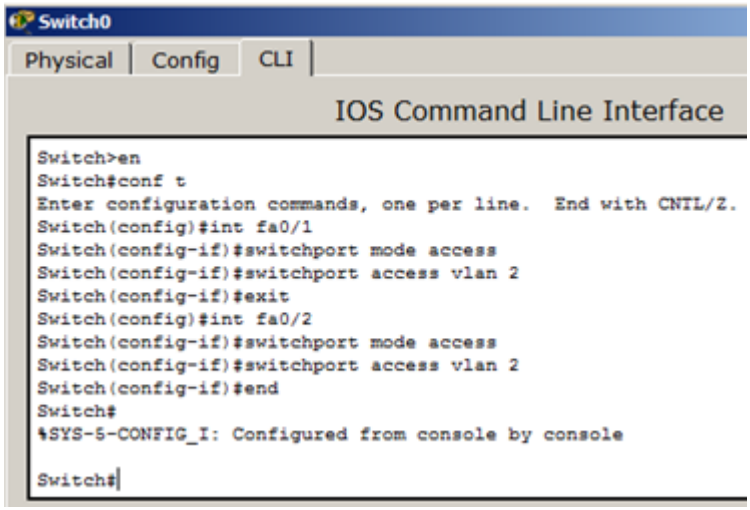


Рисунок 5.15. Указываем порты коммутатора для подключения пользователей

Теперь командой show vlan можно проверить результат (Рисунок 5.16).

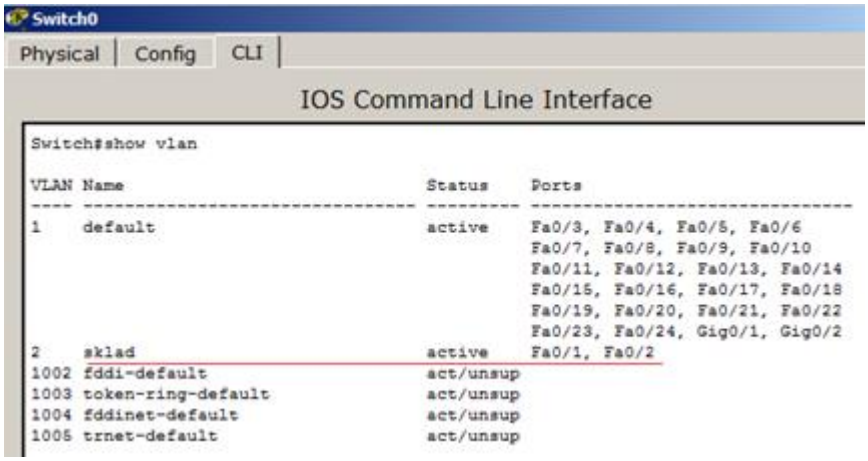


Рисунок 5.16. Подсеть VLAN2 склад настроена

Далее работаем с VLAN3 (Рисунок 5.17).

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

Рисунок 5.17. VLAN3 получает имя buh

В виртуальной сети VLAN3 настраиваем порты коммутатора Fa0/3 и Fa0/4 как access порты, т.е. порты для подключения пользователей, затем командой show vlan можно проверить и убедиться, что мы создали в сети 2 сегмента на разные порты коммутатора (Рисунок 5.18).

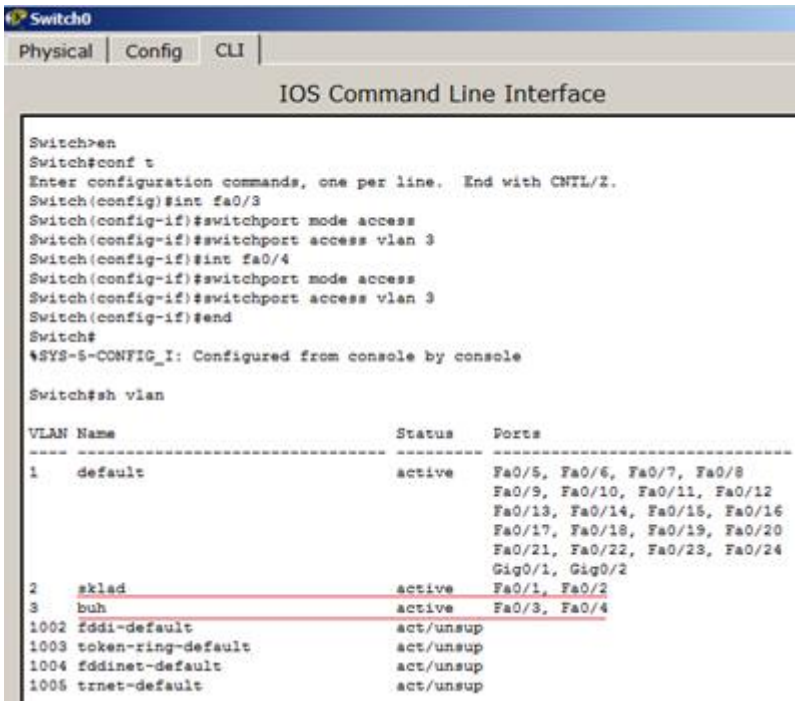


Рисунок 5.18. Мы настроили VLAN2 и VLAN3

Настраиваем IP адреса компьютеров – для VLAN2 из сети 192.168.2.0, а для VLAN3 из сети 192.168.3.0 (Рисунок 5.19).

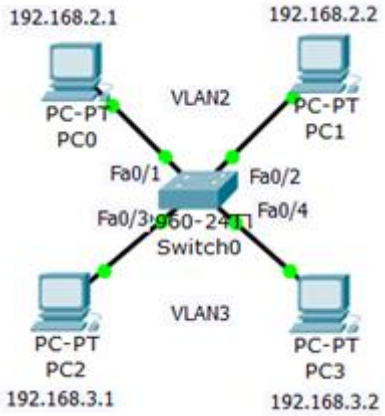


Рисунок 5.19. Настраиваем IP адреса компьютеров

Проверяем связь ПК в пределах VLAN и отсутствие связи между VLAN2 и VLAN3 (Рисунок 5.20).

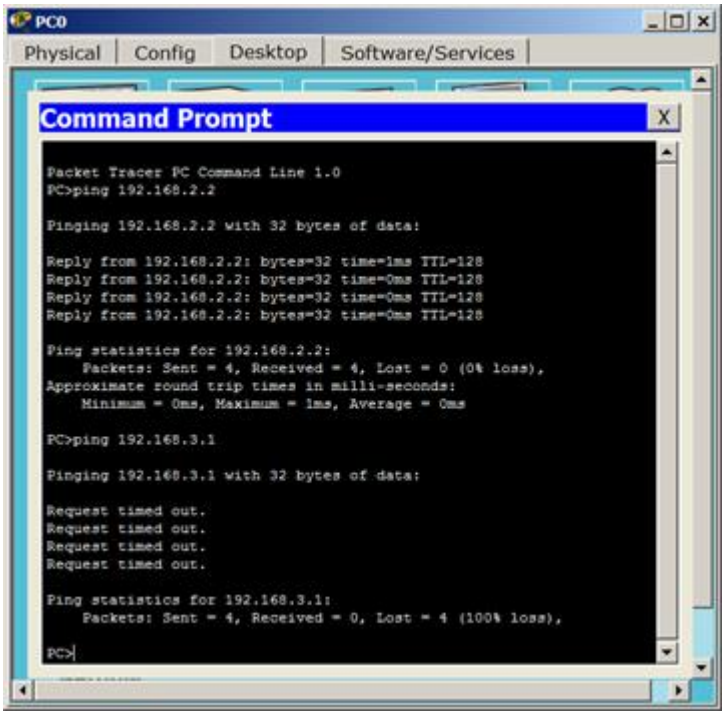


Рисунок 5.20. Все работает так, как было задумано

Итак, на компьютере ПК0 мы убедились, что компьютер в своем сегменте видит ПК, а в другом сегменте – нет.

ПРАКТИЧЕСКАЯ РАБОТА № 5.2.1

Настройка виртуальной сети на коммутаторе 2960

Время работы: 2 часа

1.Цель работы: Научится работать с программой Cisco Packet Tracer (CPT)

2.Технические средства

2.1 Оборудование: компьютер

2.2 Программное обеспечение: Cisco Packet Tracer, MS Word.

В данной работе рассматривается настройка VLAN на коммутаторе фирмы Cisco в программе CPT. Мы уже делали подобную работу. Но здесь мы не только закрепим пройденное, но и узнаем ряд новых команд Cisco IOS.

Создайте сеть, топология которой представлена на Рисунок 5.21.

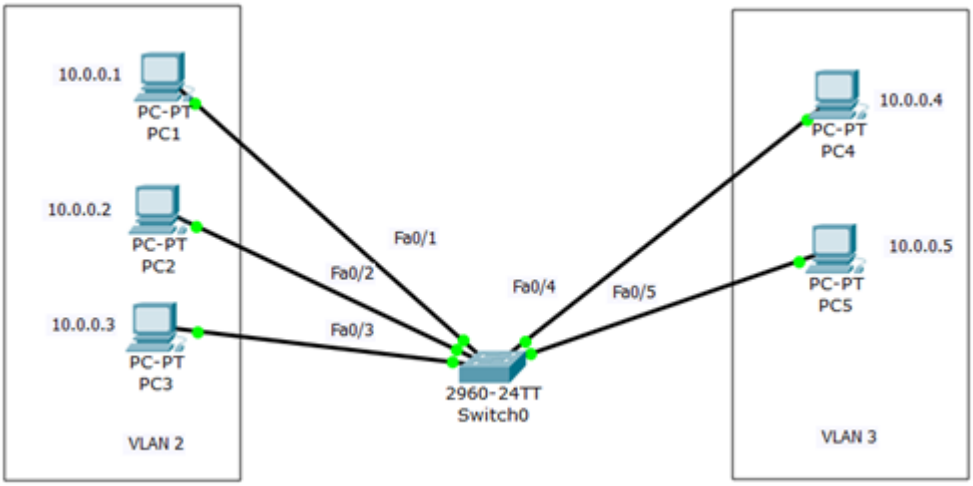


Рисунок 5.21. Схема сети с одним коммутатором

Задача данной работы является создание 2х независимых групп компьютеров: ПК1-ПК3 должны быть доступны только друг для друга, а вторая независимая группа - компьютеры ПК4 и ПК5.

Настройка коммутатора

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

Switch>en

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

Switch#conf t

Теперь вводим команду VLAN 2. Данной командой вы создадите на коммутатореVLANс номером 2. Указатель ввода Switch (config)# изменится на Switch (config-vlan)# это свидетельствует о том, что вы конфигурируете уже не весь коммутатор в целом, а только отдельныйVLAN, в данном случаеVLANномер 2 (Рисунок 5.22).

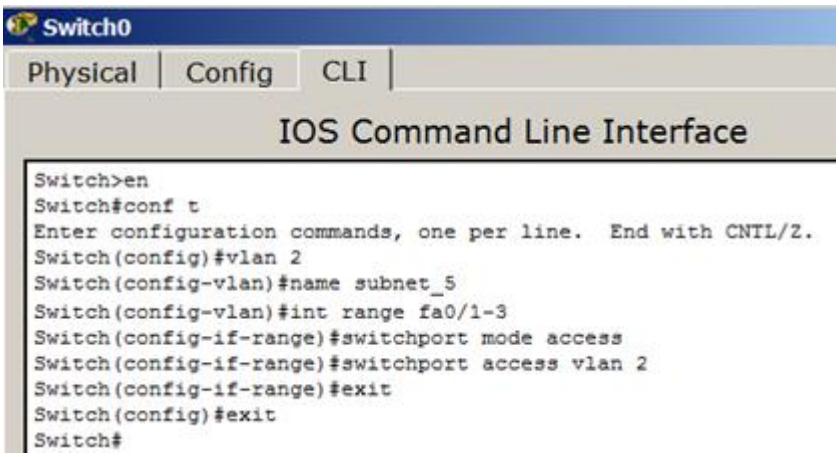


Рисунок 5.22. Листинг команд для формирования VLAN2

Примечание

Командой VLAN2, мы создаем на коммутаторе новый VLAN с номером 2. Команда name subnet_5 присваивает имя subnet_5 виртуальной сети номер 2. Выполняя команду interface range fast Ethernet 0/1-3 мы переходим к конфигурированию интерфейсов fastEthernet 0/1, fastEthernet 0/2 и fastEthernet 0/3 коммутатора. Слово range в данной команде, указывает на то, что мы будем конфигурировать не один порт, а диапазон портов. Команда switch port mode access конфигурирует выбранный порт коммутатора, как порт доступа (access порт). Команда switch port access vlan 2 указывает, что данный порт является портом доступа для VLAN номер 2.

Выйдите из режима конфигурирования, дважды набрав команду exit и просмотрите результат конфигурирования (Рисунок 5.23), выполнив команду sh vl br. Как видим, на коммутаторе появился VLAN с номером 2 и именем subnet_5, портами доступа которого являются fastEthernet 0/1, fastEthernet 0/2 и fastEthernet 0/3.

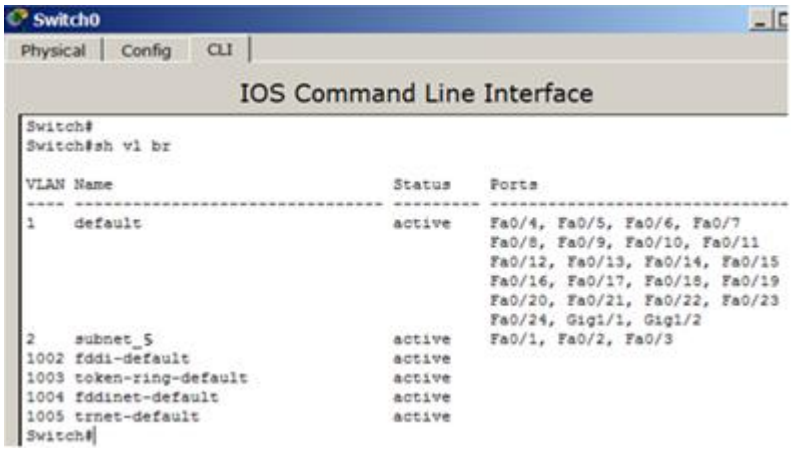


Рисунок 5.23. Просмотр информации о VLAN на коммутаторе

Примечание

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

Далее аналогичным образом создадим VLAN 3 с именем subnet_6 и сделаем его портами доступа интерфейсы fastEthernet 0/4 и fastEthernet 0/5. Результат показан на Рисунок 5.24.

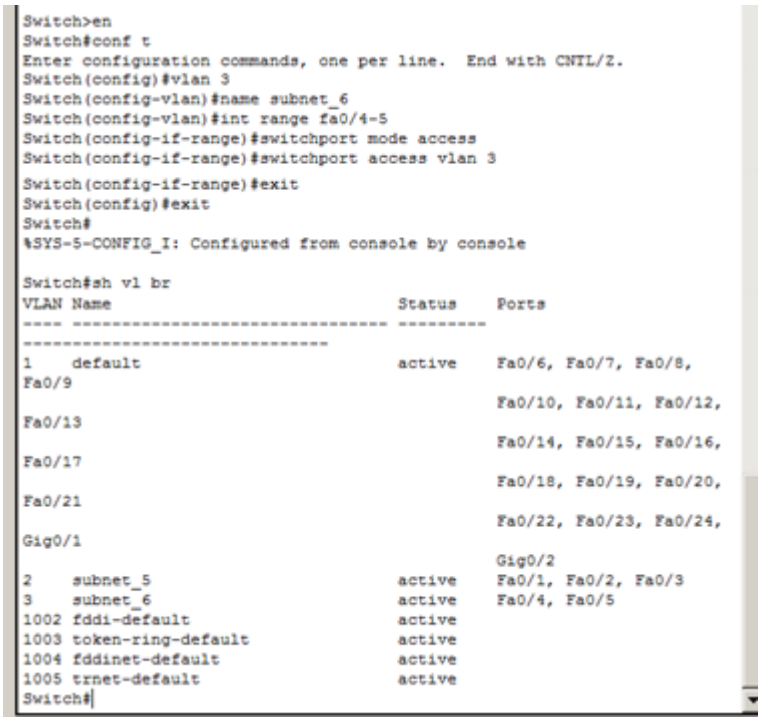


Рисунок 5.24. Результат – настройка на коммутатореVLAN2 и VLAN3

Проверка результатов работы

Сеть настроена и нужно ее протестировать. Результат положителен, если в пределах своей VLAN компьютеры доступны, а компьютеры из разных VLAN не доступны (Рисунок 5.25). У нас все пять компьютеров находя в одной сети 10.0.0.0/8, но они находятся в разных виртуальных локальных сетях.

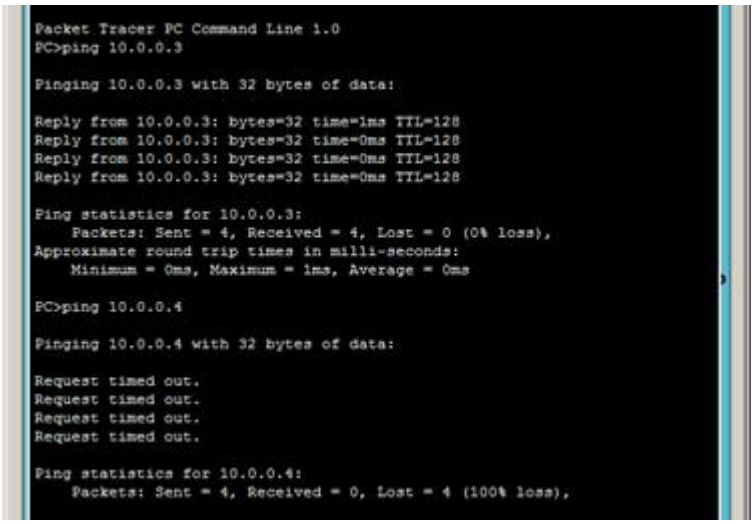


Рисунок 5.25. Пинг с PC1 на PC3 и PC4

ПРАКТИЧЕСКАЯ РАБОТА № 5.2.2

VLAN с двумя коммутаторами. Разделяемый общий канал (транк)

Время работы: 2 часа

1.Цель работы: Научится работать с программой Cisco Packet Tracer (CPT)

2.Технические средства

2.1 Оборудование: компьютер

2.2 Программное обеспечение: Cisco Packet Tracer, MS Word.

На практике часто возникает задача разделения устройств, подключенных к одному или нескольким коммутаторам на несколько непересекающихся локальных сетей. В случае, если используется только один коммутатор, то эта задача решается путем конфигурирования портов коммутатора, указав каждому порту к какой локальной сети он относится. Если же используется несколько коммутаторов (Рисунок 5.26), то необходимо между коммутаторами помимо данных передавать информацию к какой локальной сети относится кадр. Для этого был разработан стандарт 802.1Q.

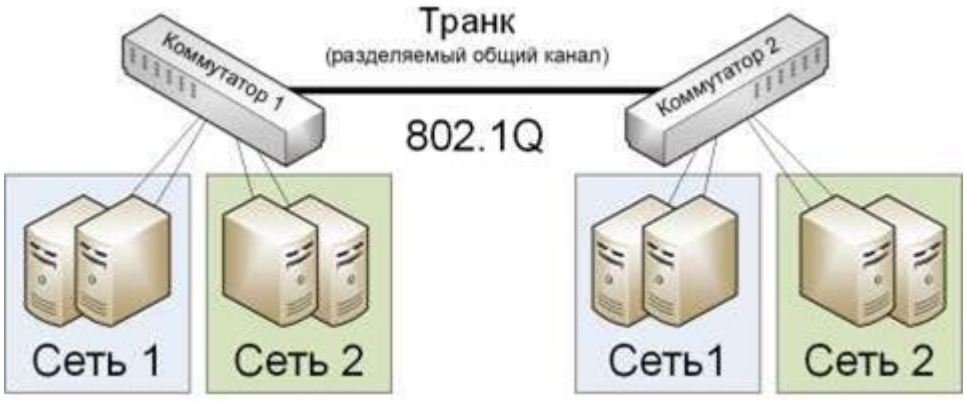


Рисунок 5.26. Виртуальные локальные сети (VLAN) с использованием двух коммутаторов

От теории перейдем к практике и произведем дублирование нашей сети (той, которая была показана ранее на Рисунок 5.21). Для этого выделим всю сеть инструментом Select (Выделить), и, удерживая клавишу Ctrl, перетащим на новое место в рабочей области программы. Так мы произведем копирование (Рисунок 5.27).

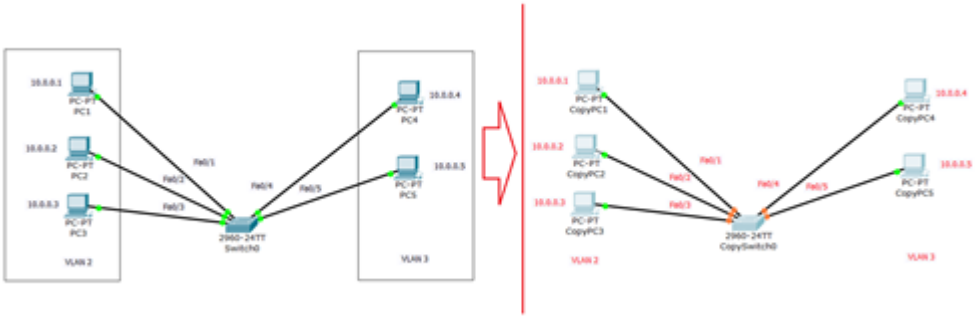


Рисунок 5.27. Дублируем сеть с одним коммутатором

Соединим коммутаторы перекрестным кабелем (кроссом) через самые производительные порты – Gigabit Ethernet (Рисунок 5.28).

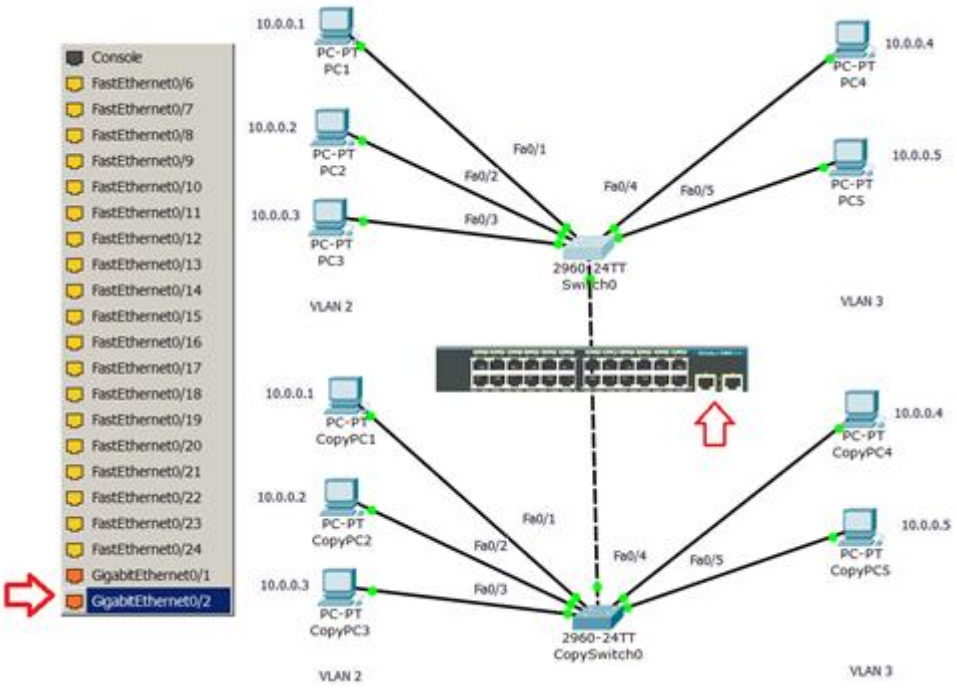


Рисунок 5.28. Соединяем коммутаторы через Gigabit Ethernet порты

Теперь поправим настройки на дубликате исходной сети (Рисунок 5.29).

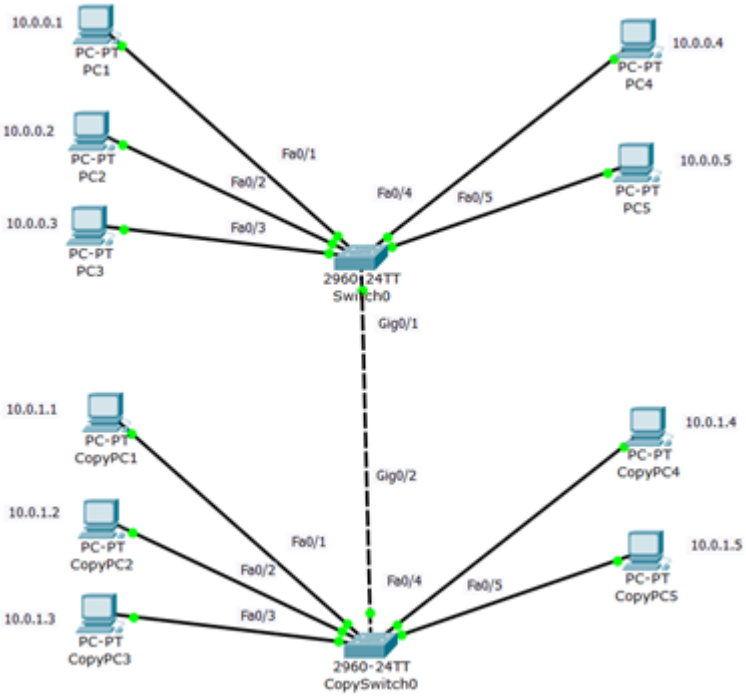


Рисунок 5.29. Настраиваем сеть-дубликат

Укажем новый вариант подсетей VLAN2 и VLAN3, а также выделим trunk (транк) связь коммутаторов (Рисунок 5.30).

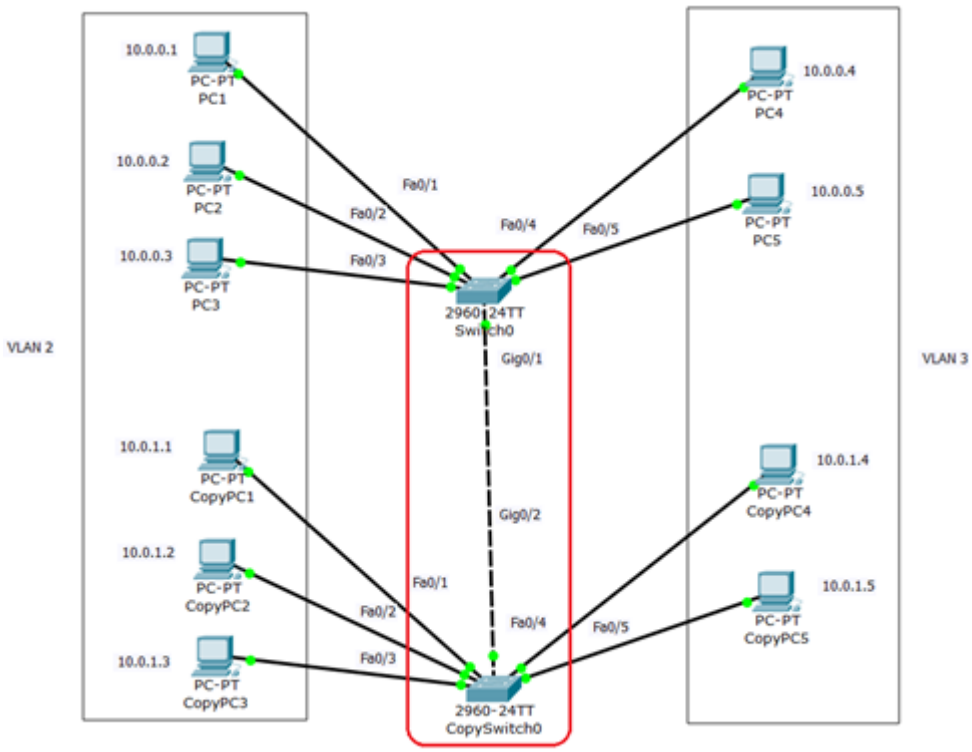


Рисунок 5.30. В сети обозначаем подсети VLAN2 и VLAN3

Настраиваем транк порт Gig0/1

При настройке Gig0/1 на коммутаторе Switch0 мы меняем состояние порта и указываем vlan 2 и 3 для работы с ним (Рисунок 5.31).

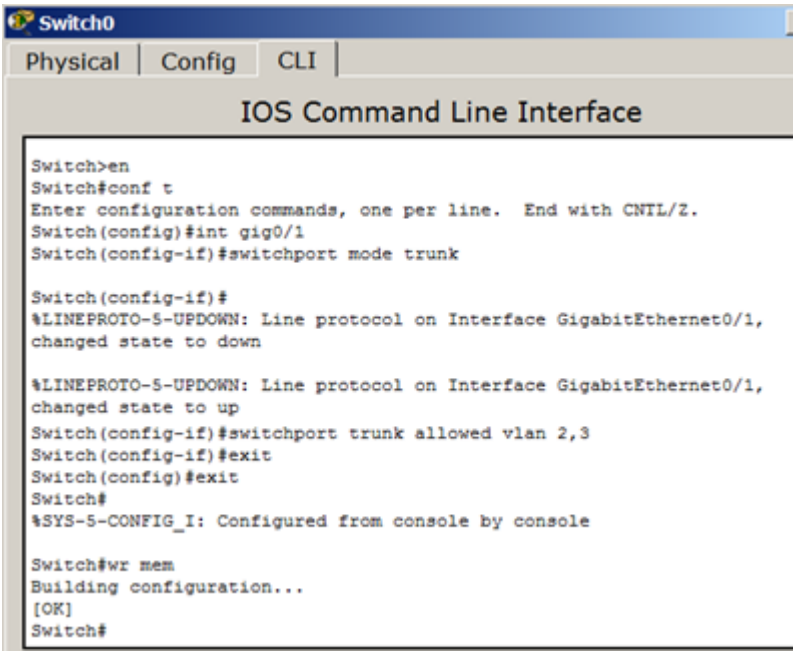


Рисунок 5.31. Настраиваем транк порт Gig0/1 на коммутаторе Switch0

Настраиваем транк порт Gig0/2

Транк порт Gig0/2 на коммутаторе CopySwitch0 настраиваем аналогично (Рисунок 5.32).

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

Switch#end
```

Рисунок 5.32. Настраиваем trunk порт Gig0/2 на коммутаторе CopySwitch0

Диагностика результатов работы

Проверяем пинг с PC1 в разные vlan (Рисунок 5.33).Все отлично: в пределах своей vlan ПК доступны, а между ПК разных vlan связи нет.

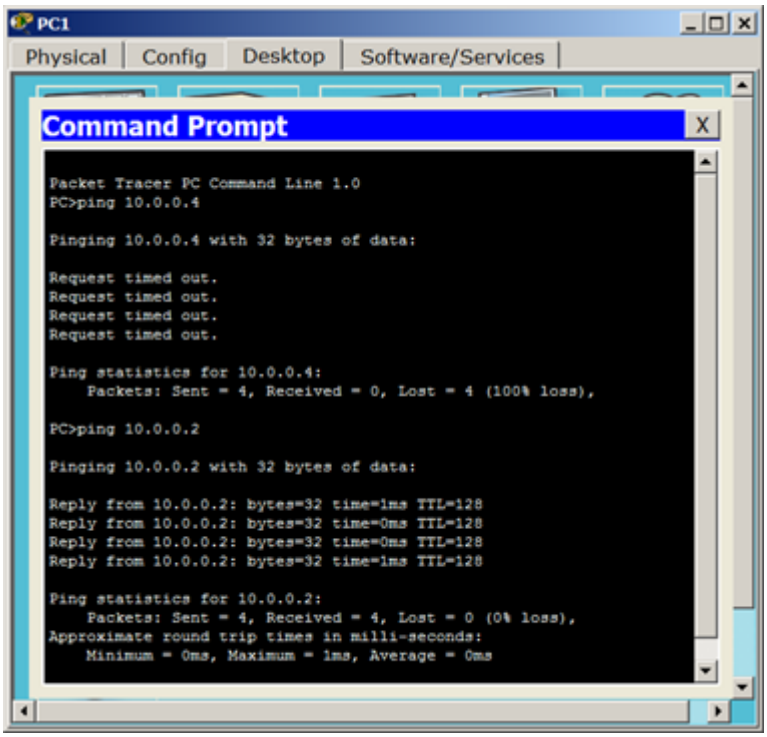


Рисунок 5.33. Пинг с PC1 в разные vlan

ПРАКТИЧЕСКАЯ РАБОТА № 5.3

Настройка виртуальной сети из двух свитчей и четырех ПК.

Время работы: 2 часа

1.Цель работы: Научится работать с программой Cisco Packet Tracer (CPT)

2.Технические средства

2.1 Оборудование: компьютер

2.2 Программное обеспечение: Cisco Packet Tracer, MS Word.

Ниже мы рассмотрим как настроить VLAN из двух свитчей и четырех ПК.

Создайте сеть, топология которой представлена на Рисунок 5.34. Пока в сети 10.0.0.0 нет разделения на VLAN - все компьютеры доступны между собой.

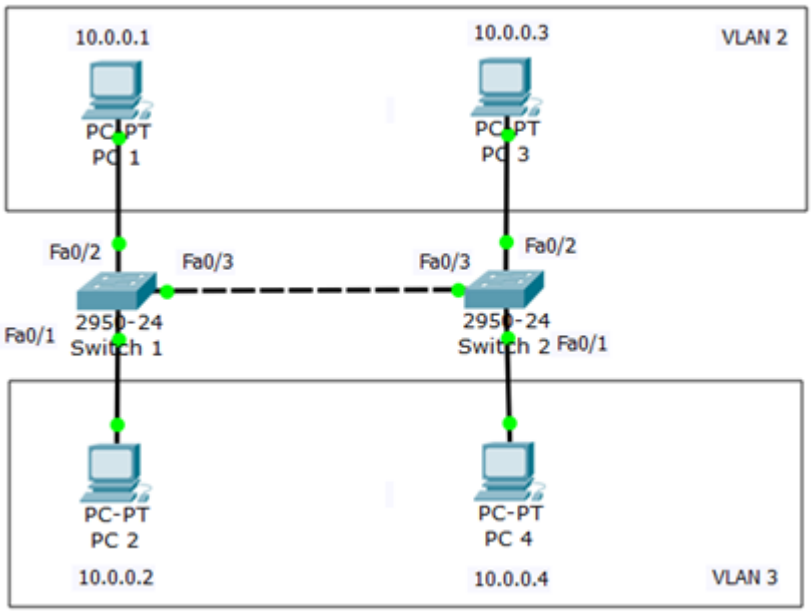


Рисунок 5.34. Схема сети

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

Настройка VLAN 2 и VLAN3

Перейдите к настройке коммутатора Switch1. Откройте его консоль. В открывшемся окне перейдите на вкладку CLI, войдите в привилегированный режим и настройте VLAN 2 и VLAN3. Затем просмотрите информацию о существующих на коммутаторе VLAN-ах командой: Switch1#sh vl br (Рисунок 5.35).

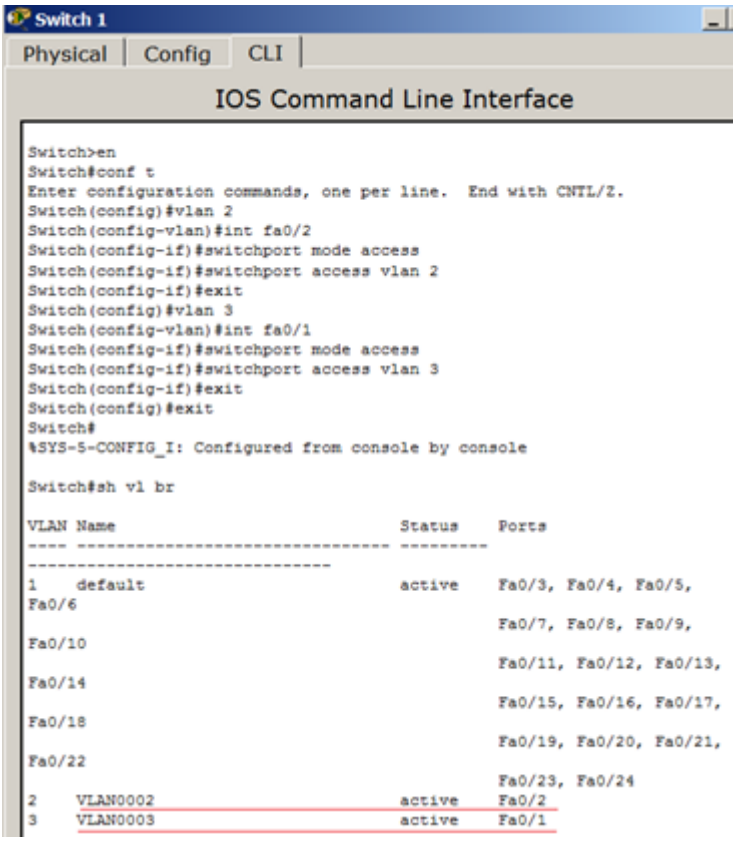


Рисунок 5.35. Конфигурация Switch1

Аналогичным образом сконфигурируйте Switch2, исходя из того, что по условиям задачи у нас Fa0/2 расположен в Vlan2, а Fa0/1 находится в Vlan 3 (это не всегда так). Результат конфигурирования S2 показан на Рисунок 5.36.

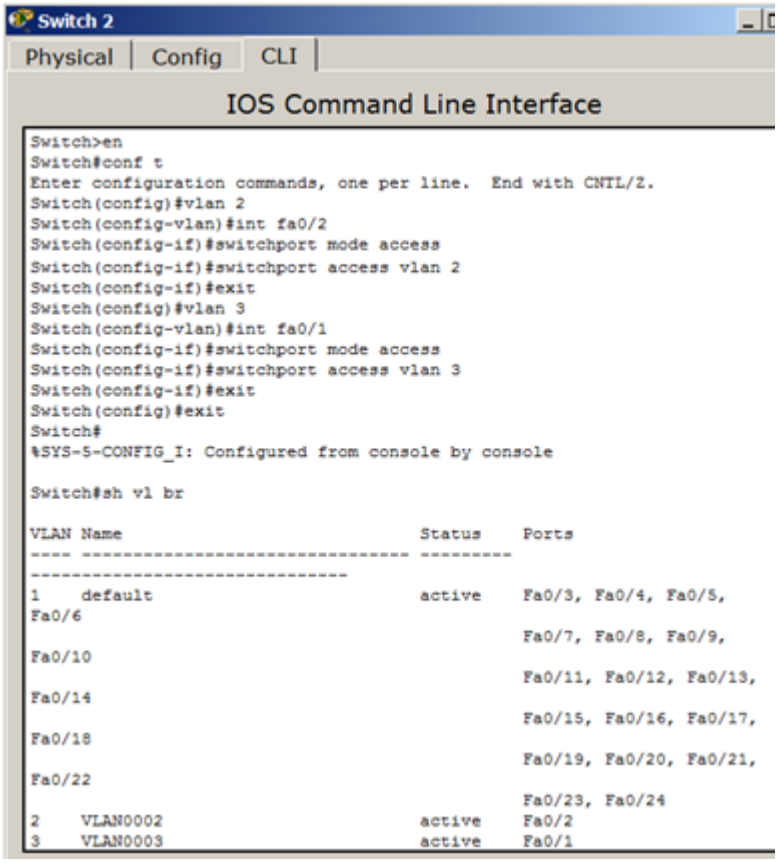


Рисунок 5.36. Конфигурация Switch2

Итак, подсети Vlan 2 принадлежат порты коммутаторов Fa0/2, а Vlan 3 принадлежат порты коммутаторов Fa0/1. Поскольку в данный момент нет обмена информации о виланах, то все компьютеры разобщены (Рисунок 5.37).

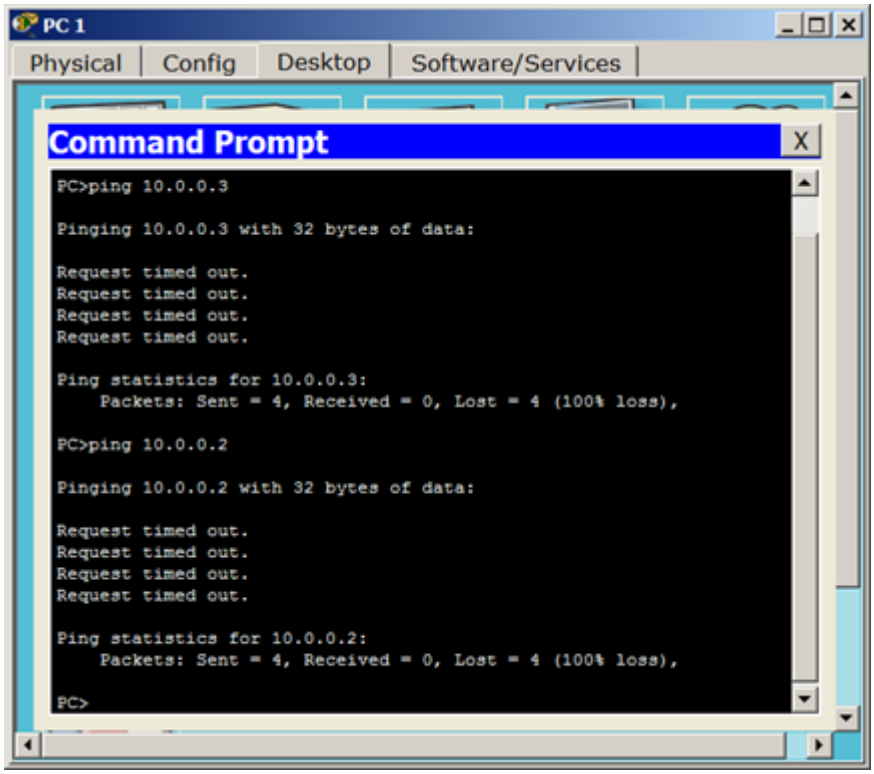


Рисунок 5.37. Связей между ПК нет

Настройка связи коммутаторов через транковый порт

Теперь организуем магистраль обмена между коммутаторами. Для этого настроим третий порт Fa0/3 на каждом коммутаторе как транковый. Войдите в консоль коммутатора Switch1 и задайте транковый порт (Рисунок 5.38).

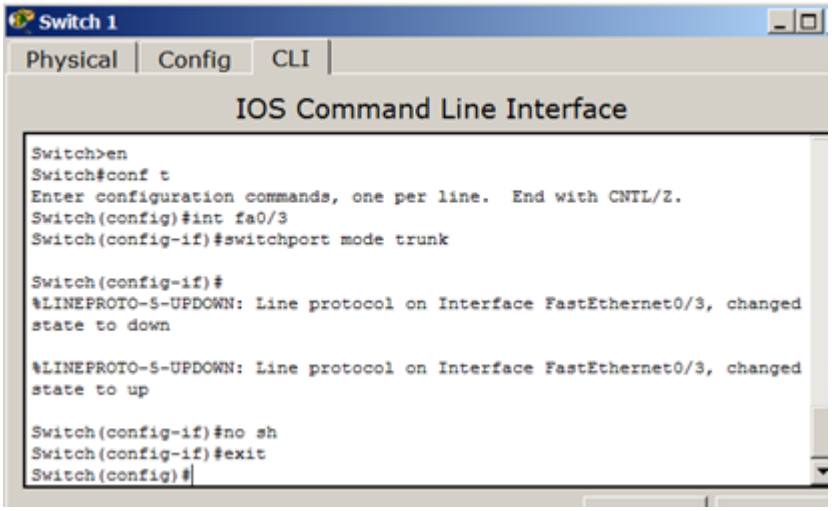


Рисунок 5.38. Настраиваем транковый порт на S1

Откройте конфигурацию коммутатораS1 на интерфейсе FastEthernet 0/3 и убедитесь, что порт транковый (Рисунок 5.39).

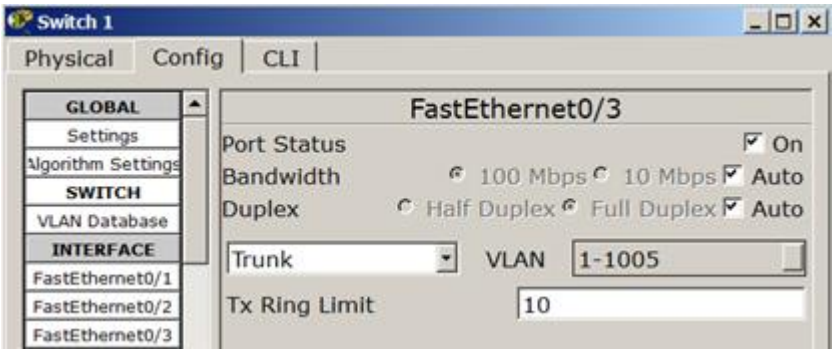


Рисунок 5.39. Конфигурация интерфейса FastEthernet0/3 на Switch1

На коммутаторе Switch2 интерфейс FastEthernet 0/3 автоматически настроится как транковый (Рисунок 5.40).

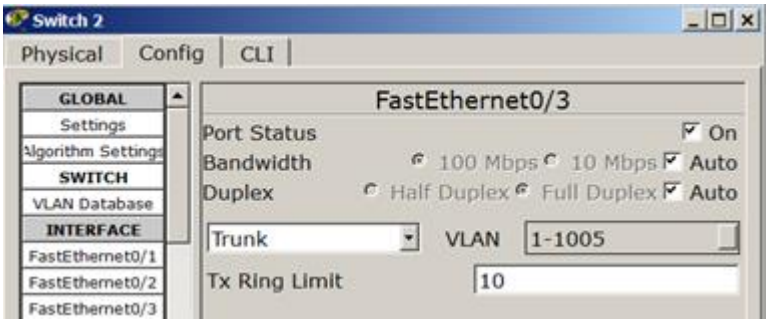


Рисунок 5.40. Конфигурация интерфейса FastEthernet0/3 на Switch2

Теперь компьютеры, входящие в один виллан должны пинговаться, а компьютеры в разных виллах будут взаимно недоступны (Рисунок 5.41).

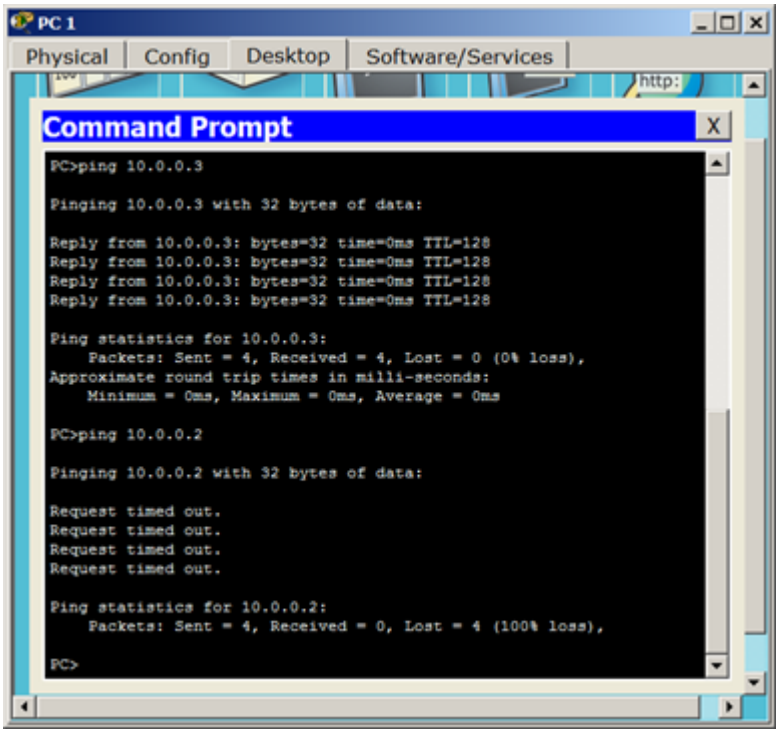


Рисунок 5.41. Проверка связи PC1 с ПК в VLAN 2 и VLAN 3

ПРАКТИЧЕСКАЯ РАБОТА № 6.1

Настраиваем WEB сервер

Время работы: 2 часа

1. Цель работы: Научится работать с программой Cisco Packet Tracer (CPT)

2. Технические средства

2.1 Оборудование: компьютер

2.2 Программное обеспечение: Cisco Packet Tracer, MS Word.

Как правило, сервер отдает в сеть свои ресурсы, а клиент эти ресурсы использует. Также, на серверах устанавливаются специализированное программное и аппаратное обеспечение. На одном компьютере может работать одновременно несколько программ-серверов. Сервисы серверов часто определяют их название:

Cisco HTTP (WEB) сервер – позволяет создавать простейшие веб-странички и проверять прохождение пакетов на 80-ый порт сервера. Эти серверы предоставляют доступ к веб-страницам и сопутствующим ресурсам, например, картинкам.

DHCP сервер – позволяет организовывать пулы сетевых настроек для автоматического конфигурирования сетевых интерфейсов. Dynamic Host Configuration Protocol обеспечивает автоматическое распределение IP-адресов между компьютерами в сети. Такая технология широко применяется в локальных сетях с общим выходом в Интернет.

DNS сервер – позволяет организовать службу разрешения доменных имён.Функция DNS-сервера заключается в преобразовании доменных имен серверов в IP-адреса.

Cisco EMAIL – почтовый сервер, для проверки почтовых правил. Электронное письмо нельзя послать непосредственно получателю – сначала оно попадает на сервер, на котором зарегистрирована учетная запись отправителя. Тот, в свою очередь, отправляет "посылку" серверу получателя, с которого последний и забирает сообщение.

FTP – файловый сервер. В его задачи входит хранение файлов и обеспечение доступа к ним клиентских ПК, например, по протоколу FTP. Ресурсы файл-сервера могут быть либо открыты для всех компьютеров в сети, либо защищены системой идентификации и правами доступа.

Итак, эмулятор сетевой среды Cisco Packet Tracer позволяет проводить настройку таких сетевых сервисов, как: HTTP, DHCP, DNS, EMAIL, FTP и ряда других в составе сервера сети. Рассмотрим настойку некоторых из них.

Топология для наших исследований приведена на Рисунок 6.1.

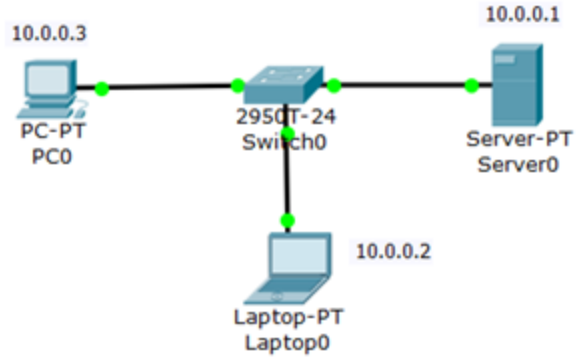


Рисунок 6.1. Схема сети

Создаем WEB-документ на сервере

Для создания HTTP-сервера открываем на сервере вкладку HTTP и редактируем первую страницу сайта с названием index.html. Включаем службу HTTP переключателем On (Рисунок 6.2).

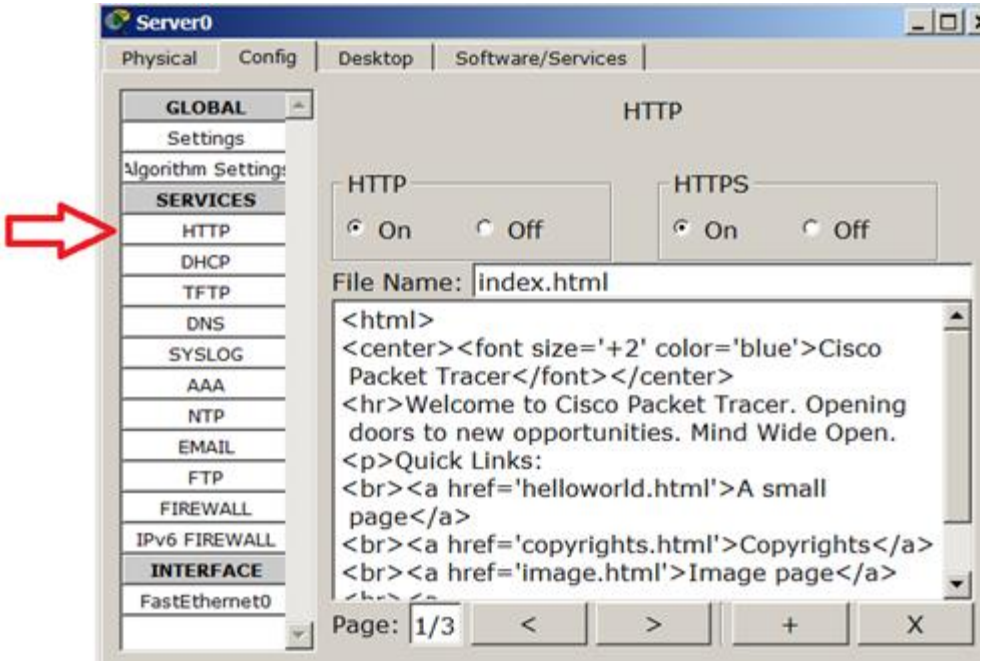


Рисунок 6.2. Вкладка Config, служба сервера HTTP

Примечание

В этом окне можно добавить новую страницу кнопкой + или удалить текущую кнопкой X. Переключение между несколькими страницами осуществляется кнопками < | >.

В окнеhtmlкода создаем текст первой страницы сайта index.html. Вариант 1 (Рисунок 6.3).

```
<html>
<body>
<h1>Welcome to WEB-Server CISCO!</h1>
<p>Server working: <font color="red"><b>OK!</b></font></p>
</body>
</html>
```

Рисунок 6.3. Текст web-страницы, вариант 1

Либо вариант 2 (Рисунок 6.4).

```
<html>
<center><font size='+2' color='blue'>Welcome to Cisco Packet Tracer HTML Server! </font></center>
<body>
Hello!<br/>I am OK!
</body>
</html>
```

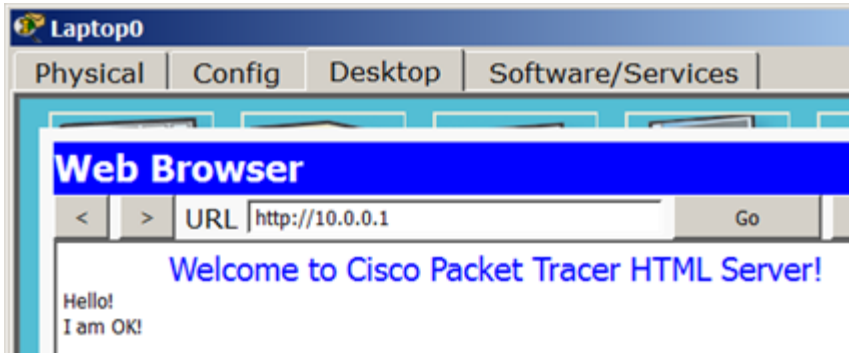


Рисунок 6.4. Текст web-страницы, вариант 2

Совет

Текст можно переносить в это окно через буфер обмена. Он может быть только на английском языке

Для того, чтобы проверить работоспособность нашего сервера, открываем клиентскую машину (10.0.0.2 или 10.0.0.3) и на вкладке Desktop (Рабочий стол) запускаем приложение Web Browser. После чего набираем адрес нашего WEB-сервера 10.0.0.1 и нажимаем на кнопку GO. Убеждаемся, что наш веб-сервер работает.

ПРАКТИЧЕСКАЯ РАБОТА № 6.2

Настройка сетевых сервисов DNS, DHCP и Web

Время работы: 2 часа

1. Цель работы: Научится работать с программой Cisco Packet Tracer (CPT)

2. Технические средства

2.1 Оборудование: компьютер

2.2 Программное обеспечение: Cisco Packet Tracer, MS Word.

Создайте схему сети, представленную на Рисунок 6.5.

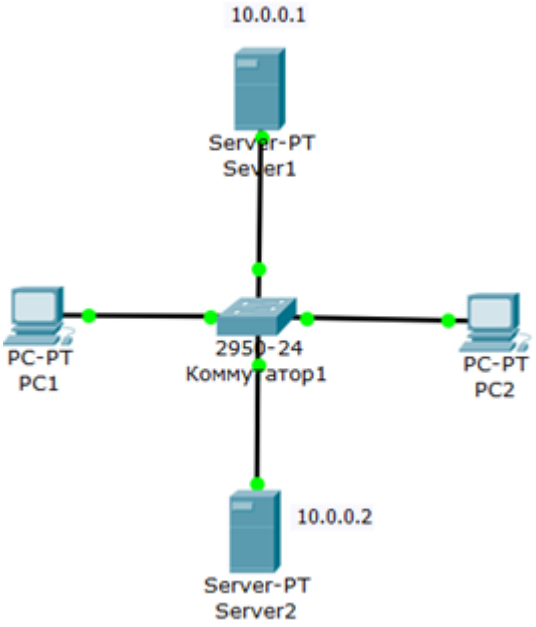


Рисунок 6.5. Схема сети

Наша задача состоит в том, чтобы настроить Server1 как DNS и Web-сервер, а Server2 как DHCP сервер. Напомню, что работа DNS-сервера заключается в преобразовании доменных имен серверовв IP-адреса. DHCP сервер позволяет организовывать пулы для автоматического конфигурирования сетевых интерфейсов, то есть, обеспечивает автоматическое распределение IP-адресов между компьютерами в сети. Иначе говоря, в нашем случае компьютеры получают IP-адреса благодаря сервису DHCP Server2 и открывают, например, сайт на Server1.

Настраиваем IP адреса серверов и DHCP на ПК

Войдите в конфигурацию PC1 и PC2 и установите настройку IP через DHCP сервер Рисунок 6.6.

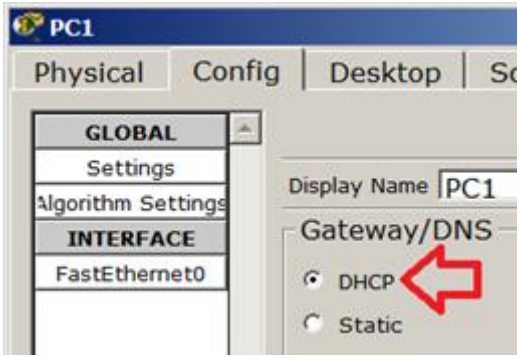


Рисунок 6.6. Настройка IPна PC1

Задайте в конфигурации серверов настройки IP: Server1 – 10.0.0.1 (Рисунок 6.7), Server2 – 10.0.0.2 (Рисунок 6.8). Маска подсети установится автоматически как 255.0.0.0.

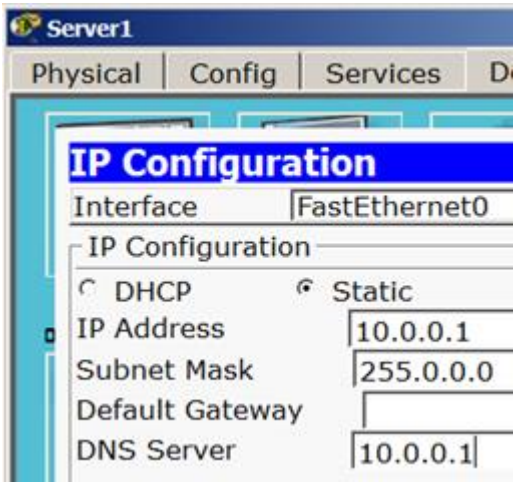


Рисунок 6.7.

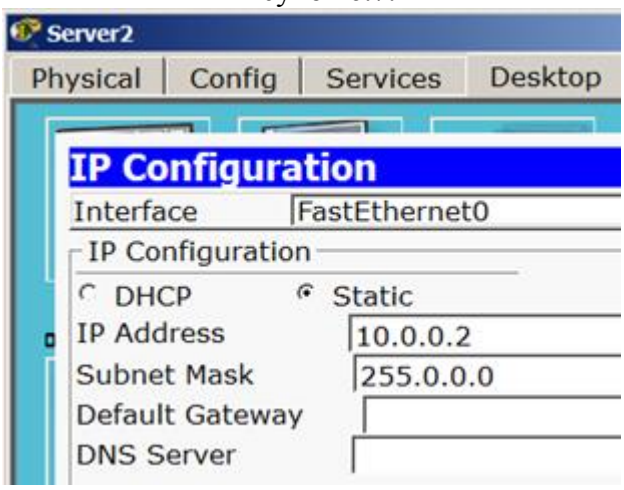


Рисунок 6.8.

Настройка служб DNS и HTTP на Server1

В конфигурации Server1 войдите на вкладку DNS и задайте две ресурсные записи (Resource Records) в прямой зоне DNS.

Новый термин

Зона DNS — часть дерева доменных имен (включая ресурсные записи), размещаемая как единое целое на сервере доменных имен (DNS-сервере). В зоне прямого просмотра на запрос доменного имени идет ответ в виде IP адреса. В зоне обратного просмотра по IP мы узнаем доменное имя ПК.

Сначала в ресурсной записи типа A Record свяжите доменное имя компьютера server1.yandex.ru с его IP адресом 10.0.0.1 и нажмите на кнопку Add (добавить) и активируйте переключатель On – Рисунок 6.9.

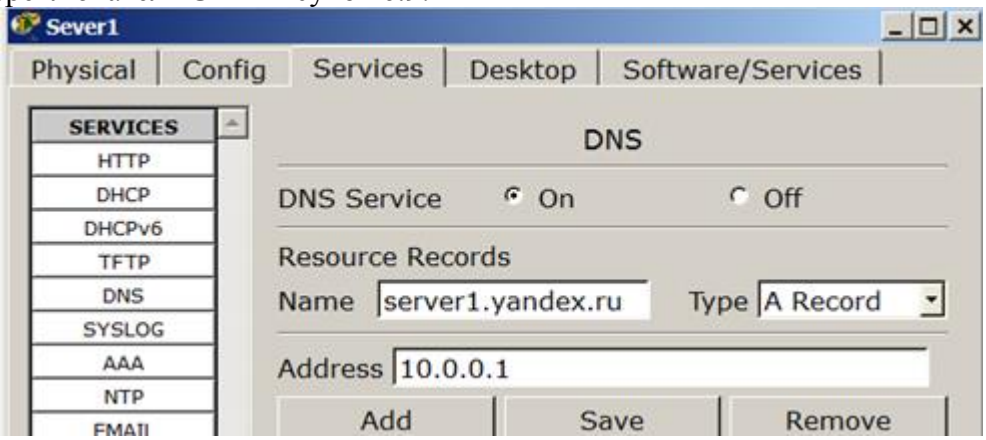


Рисунок 6.9. Ввод ресурсной записи типа A Record

Далее в ресурсной записи типа CNAME свяжите название сайта с сервером и нажмите на кнопку Add (добавить) – Рисунок 6.10.

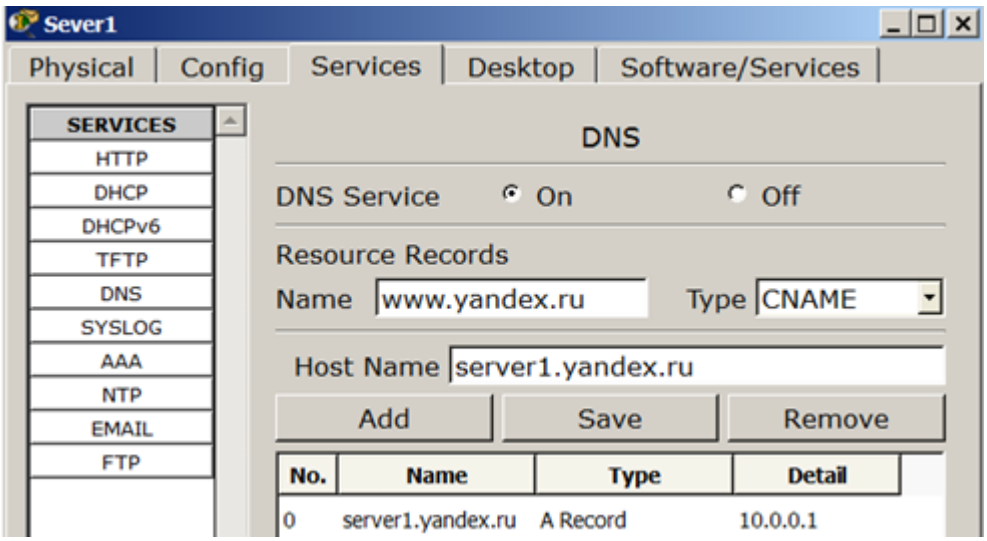


Рисунок 6.10. Ввод ресурсной записи типа CNAME

В результате должно получиться следующее (Рисунок 6.11).

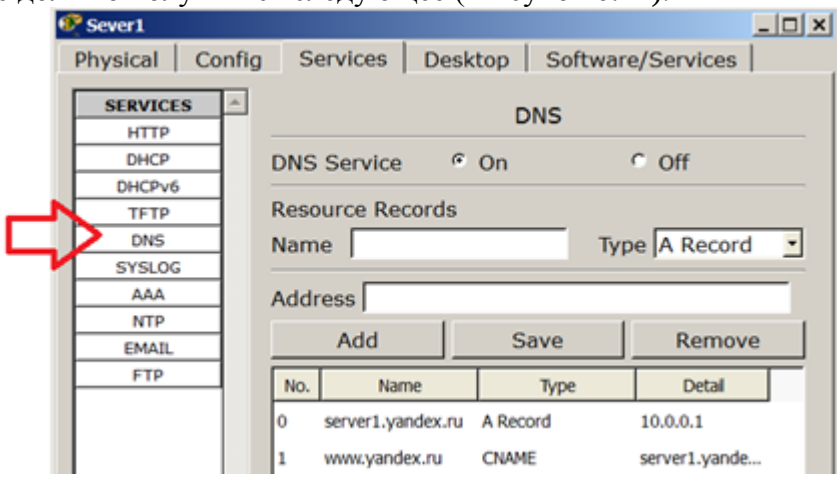


Рисунок 6.11. Служба DNS в прямой зоне

Теперь настроим службу HTTP. В конфигурации Server1 войдите на вкладку HTTP и создайте стартовую страницу сайта (Рисунок 6.12).

```
<html>
<center><font size='+2' color='green'>Web Server</font></center>
www.yandex.ru
<p>
Hello!<br/>I am Server1
</html>
```

Рисунок 6.12. Стартовая страница сайта

Включите командную строку на Server1 и проверьте работу службы DNS. Для проверки правильности работы прямой зоны DNS сервера введите команду SERVER>nslookup . Если все правильно настроено, то вы получите отклик на запрос с указанием доменного имени DNS сервера в сети и его IP адреса (Рисунок 6.13).

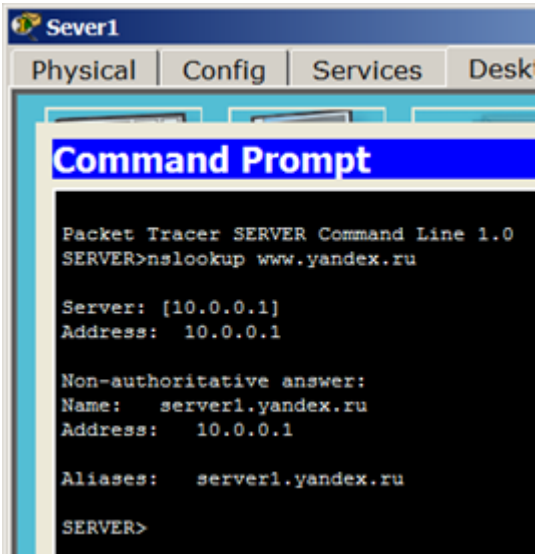


Рисунок 6.13. Служба DNSв прямой зоне DNSна Server1 настроена правильно

Примечание

Команда nslookup служит для определения ip-адреса по доменному имени (и наоборот).

Настройка службы DHCP на Server2

Войдите в конфигурацию Server2 и на вкладке DHCP настройте службу DHCP. Для этого наберите новые значения пула, установите переключатель On и нажмите на кнопку Save (Сохранить) - Рисунок 6.14.

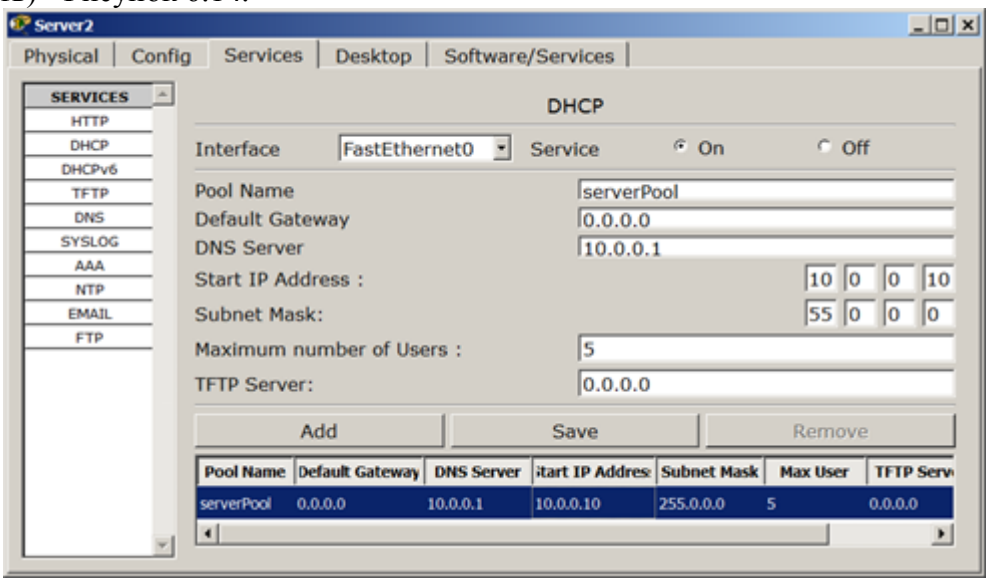


Рисунок 6.14. Настройка DHCPсервера.

Проверка работы клиентов

Войдите в конфигурации хоста PC1и PC2 и в командной строке сконфигурируйте протокол TCP/IP. Для этого командой PC> ipconfig /release сбросьте (очистите) старые параметры IP адреса (Рисунок 6.15).

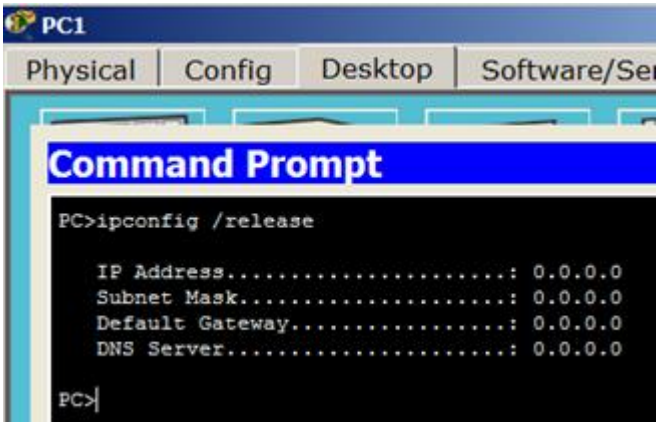


Рисунок 6.15. Удаление конфигурации IP-адресов для всех адаптеров

Примечание

Команда ipconfig /release отправляет сообщение DHCP RELEASE серверу DHCP для освобождения текущей конфигурации DHCP и удаления конфигурации IP-адресов для всех адаптеров (если адаптер не задан). Этот ключ отключает протокол TCP/IP для адаптеров, настроенных для автоматического получения IP-адресов.

Теперь командой PC> ipconfig /renew получите новые параметры от DHCP сервера (Рисунок 6.16).

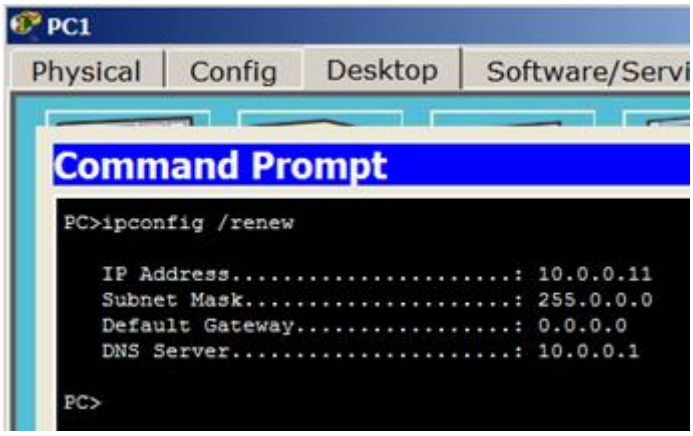


Рисунок 6.16. Конфигурация протокол TCP/IP клиента от DHCP сервера

Аналогично поступите для PC2 (Рисунок 6.17).

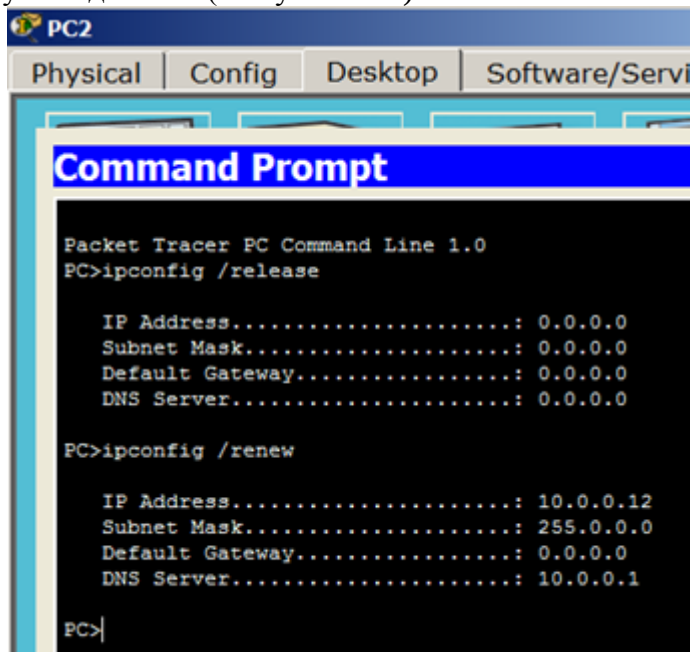


Рисунок 6.17. PC2 получил IP адрес от DHCP сервера Server2

Осталось проверить работу WEB сервера Server1 и открыть сайт в браузере на PC1 или PC2 (Рисунок 6.18).

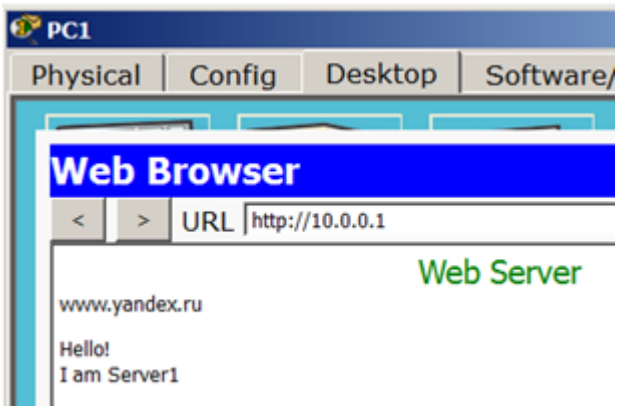


Рисунок 6.18. Проверка работы службы HTTP на Server1

ПРАКТИЧЕСКАЯ РАБОТА № 6.3

Конфигурирование DHCP сервера на маршрутизаторе

Время работы: 2 часа

1. Цель работы: Научится работать с программой Cisco Packet Tracer (CPT)
2. Технические средства

2.1 Оборудование: компьютер

2.2 Программное обеспечение: Cisco Packet Tracer, MS Word.

Примеры работы маршрутизатора в роли DHCP сервера

Маршрутизация (routing) – процесс определения маршрута следования информации в сетях связи. Задача маршрутизации состоит в определении последовательности транзитных узлов для передачи пакета от источника до адресата. Определение маршрута следования и продвижение IP-пакетов выполняют специализированные сетевые устройства – маршрутизаторы. Каждый маршрутизатор имеет от двух и более сетевых интерфейсов, к которым подключены: локальные сети либо маршрутизаторы соседних сетей.

Новый термин

Маршрутизатор (router, роутер) – сетевое устройство третьего уровня модели OSI, обладающее как минимум двумя сетевыми интерфейсами, которые находятся в разных сетях. Маршрутизатор может иметь интерфейсы: для работы по медному кабелю, оптическому кабелю, так и по беспроводным "линиям" связи.

Выбор маршрута маршрутизатор осуществляет на основе таблицы маршрутизации. Таблицы маршрутизации содержат информацию о сетях, и интерфейсов, через которые осуществляется подключение непосредственно, а также содержатся сведения о маршрутах или путях, по которым маршрутизатор связывается с удаленными сетями, не подключенными к нему напрямую. Эти маршруты могут назначаться администратором статически или определяться динамически при помощи программного протокола маршрутизации. Таблица маршрутизации содержит набор правил – записей, состоящих из определенных полей. Каждое правило содержит следующие основные поля-компоненты:

- адрес IP-сети получателя,
- маску,
- адрес следующего узла, которому следует передавать пакеты,
- административное расстояние — степень доверия к источнику маршрута,
- метрику - некоторый вес - стоимость маршрута,
- интерфейс, через который будут продвигаться данные.

Пример таблицы маршрутизации:

```
192.168.64.0/16 [110/49] via 192.168.1.2, 00:34:34, FastEthernet0/0.1

где 192.168.64.0/16 – сеть назначения,
    110/- административное расстояние
    /49 – метрика маршрута,
    192.168.1.2 – адрес следующего маршрутизатора, которому следует
                  передавать пакеты для сети 192.168.64.0/16,
    00:34:34 – время, в течение которого был известен этот маршрут,
    FastEthernet0/0.1 – интерфейс маршрутизатора, через который можно
                  достичь «соседа» 192.168.1.2.
```

Протокол DHCP представляет собой стандартный протокол, который позволяет серверу динамически присваивать клиентам IP-адреса и сведения о конфигурации. Идея работы DHCP сервиса такова: на ПК заданы настройки получения ip адреса автоматически. После включения и загрузки каждый ПК отправляет широковещательный запрос в своей сети с вопросом "Есть здесь DHCP сервер - мне нужен ip адрес?". Данный запрос получают все компьютере в подсети, но ответит на этот запрос только DHCP сервер, который отправит компьютеру свободный ip адрес из пула, а также маску и адрес шлюза по умолчанию. Компьютер получает параметры от DHCP сервера и применяет их. После перезагрузки ПК

снова отправляет широковещательный запрос и может получить другой ip адрес (первый свободный который найдется в пуле адресов на DHCP сервере).

Маршрутизатор можно сконфигурировать как DHCP сервер. Иначе говоря, вы можете программировать интерфейс маршрутизатора на раздачу настроек для хостов.Системный администратор настраивает на сервере DHCP параметры, которые передаются клиенту. Как правило, сервер DHCP предоставляет клиентам по меньшей мере: IP-адрес, маску подсети и основной шлюз. Однако предоставляются и дополнительные сведения, такие, например, как адрес сервера DNS.

Схема сети приведена на Рисунок 6.19. С помощью настроек ПК, представленных на рисунке, мы указываем хосту, что он должен получатьIP адрес, адрес основного шлюза и адрес DNS сервера от DHCP сервера.

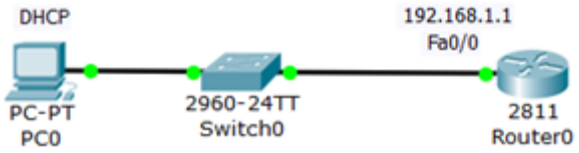


Рисунок 6.19. Схема сети

Произведем настройку R0:

Router (config)#ip dhcp pool TST создаем пул IP адресов для DHCP сервера с именем TST

Router (dhcp-config)#network 192.168.1.0 255.255.255.0 указываем из какой сети мы будем раздавать IP адреса (первый параметр - адрес данной сети, а второй параметр ее маска)

Router (dhcp-config)#default-router 192.168.1.1 указываем адрес основного шлюза, который будет рассылать в сообщениях DHCP

Router (dhcp-config)#dns-server 5.5.5.5 указываем адрес DNS сервера, который так же будет рассылаться хостам в сообщениях DHCP

Router (dhcp-config)#exit

Router (config)#ip dhcp excluded-address 192.168.1.1 этот хост исключен из пула, то есть, ни один из хостов сети не получит от DHCP сервера этот адрес.

Полный листинг этих команд приведен на Рисунок 6.20.

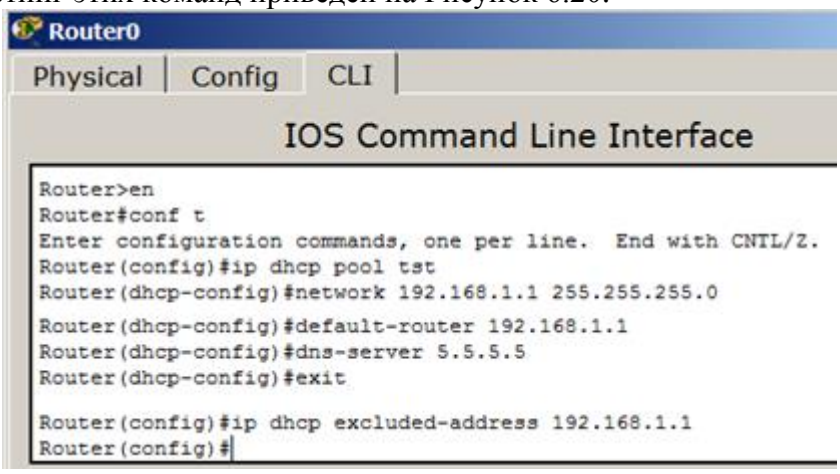


Рисунок 6.20. Команды для конфигурирования R0

Проверим результат получения динамических параметров для PC0 (Рисунок 6.21).

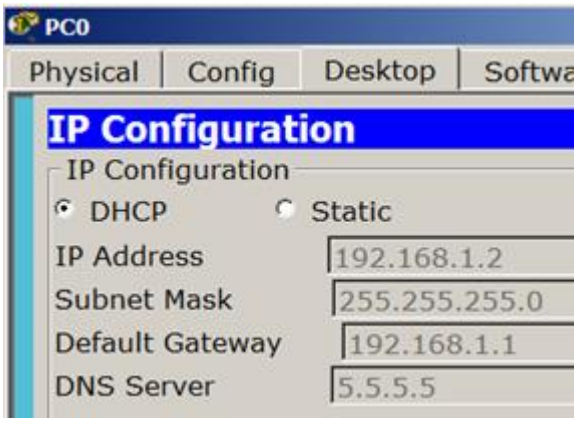


Рисунок 6.21. DHCP работает

Проверим работоспособность DHCP сервера на хосте PC0 командой ipconfig /all (Рисунок 6.22).

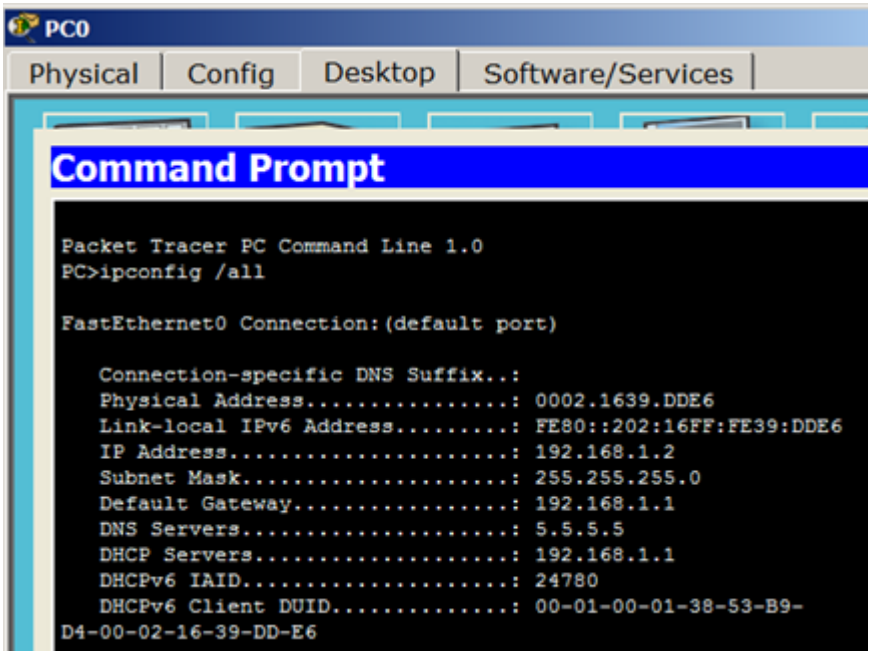


Рисунок 6.22. Хост получил настройки от DHCP сервера

Хост успешно получил IP адрес, адрес шлюза и адрес DNS сервера от DHCP сервера R0.

ПРАКТИЧЕСКАЯ РАБОТА № 6.4

Настройки интерфейса маршрутизатора в качестве DHCP клиента

Время работы: 2 часа

1. Цель работы: Научится работать с программой Cisco Packet Tracer (CPT)

2. Технические средства

2.1 Оборудование: компьютер

2.2 Программное обеспечение: Cisco Packet Tracer, MS Word.

Схема сети показана на Рисунок 6.23.

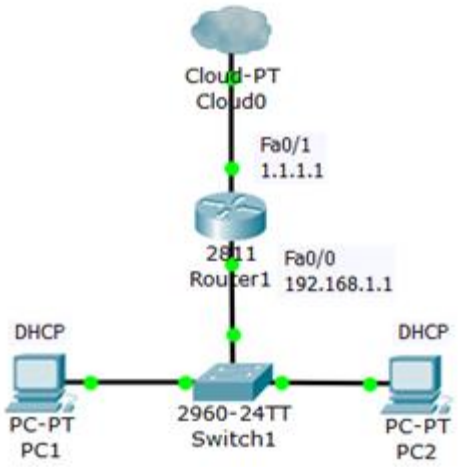


Рисунок 6.23. Схема сети

Конфигурируем интерфейс Fa0/0 для R1 (Рисунок 6.24).

Рисунок 6.24. Конфигурируем интерфейс маршрутизатора

Наблюдаем результат (Рисунок 6.25).

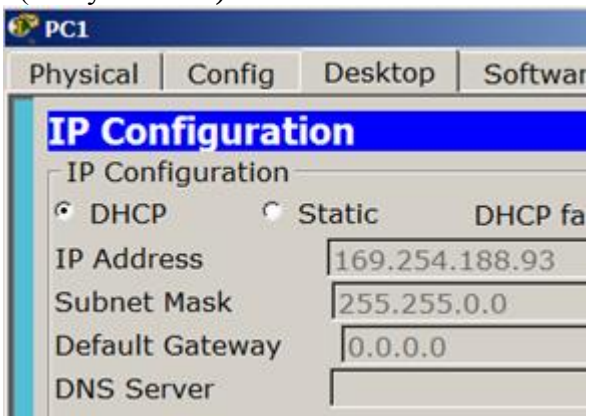


Рисунок 6.25. DHCP не работает

После настройки интерфейса роутера на получение настроек по DHCP, DHCP клиент на PC1 перестал получать IP-адрес – IP из диапазона 169.254.x.x/16 назначается автоматически самим ПК при проблемах с получением адреса по DHCP. Интерфейс роутера IP-адрес так же не получит т.к. в данной подсети нет DHCP серверов.

ПРАКТИЧЕСКАЯ РАБОТА № 6.5

DHCP сервис на маршрутизаторе 2811

Время работы: 2 часа

1. Цель работы: Научится работать с программой Cisco Packet Tracer (CPT)

2. Технические средства

2.1 Оборудование: компьютер

2.2 Программное обеспечение: Cisco Packet Tracer, MS Word.

В этом примере мы будем конфигурировать маршрутизатор 2811, а именно, настраивать на нем DHCP сервер, который будет выдавать по DHCP адреса из сети 192.168.1.0 (Рисунок 6.26). PC1 и PC2 буду получать настройки динамически, а для сервера желательно иметь постоянный адрес, т.е., когда он задан статически.

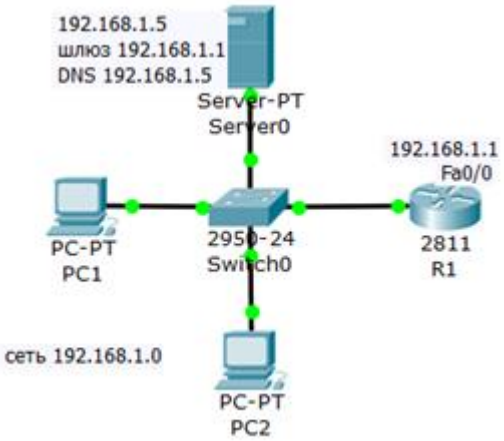


Рисунок 6.26. Схема сети

Примечание

Как устройство с постоянным адресом здесь можно включить еще и принтер.

Резервируем 10 адресов

R1 (config)#ip dhcp excluded-address 192.168.1.1 192.168.1.10

Примечание

Этой командой мы обязали маршрутизатор R1 не выдавать адреса с 192.168.1.1 по 192.168.1.10 потому, что адрес 192.168.1.1 будет использоваться самим маршрутизатором как шлюз, а остальные адреса мы зарезервируем под различные хосты этой сети.

Таким образом, первый DHCP адрес, который выдаст R1 равен 192.168.1.11.

Создаем пул адресов, которые будут выдаваться из сети 192.168.1.0

R1 (config)#ip dhcp pool POOL1

R1 (dhcp-config)#network 192.168.1.0 255.255.255.0

R1 (dhcp-config)#default-router 192.168.1.1

R1 (dhcp-config)#domain-name my-domain.com

R1 (dhcp-config)#dns-server 192.168.1.5

Примечание

Согласно этим настройкам выдавать адреса из сети 192.168.1.0 (кроме тех, что мы исключили) будет маршрутизатор R1 через шлюз 192.168.1.1.

Настраиваем интерфейс маршрутизатора

R1 (config)#interfacefa0/0

R1 (config-if)#ip address 192.168.1.1 255.255.255.0

R1 (config-if)#no shutdown

R1 (config-if)#exit

R1(config)#exit

R1#

Примечание

Команда no shut (сокращение от no shutdown) используется для того, чтобы бы интерфейс был активным. Обратная команда – shut, выключит интерфейс.

Проверка результата

Теперь оба ПК получили настройки и командой R1#show ip dhcp binding можно посмотреть на список выданных роутером адресов (Рисунок 6.27).

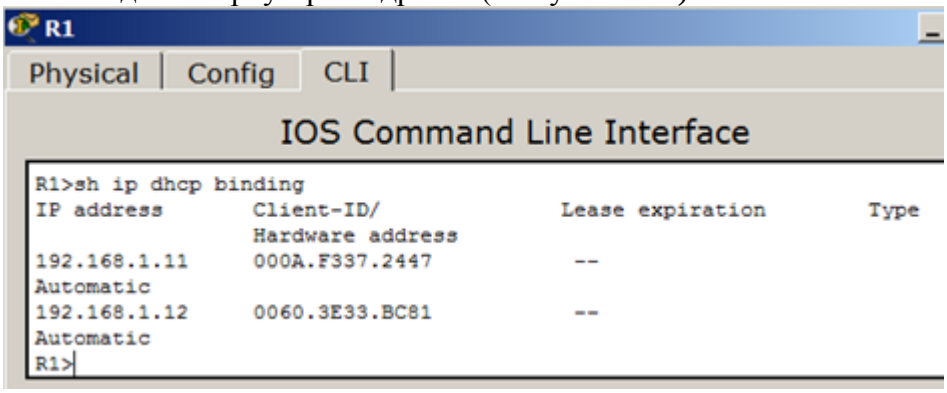


Рисунок 6.27. Адреса выдаются автоматически, начиная с адреса 192.168.1.11

Итак, мы видим, что протокол DHCP позволяет производить автоматическую настройку сети на всех компьютерах (Рисунок 6.28).

Рисунок 6.28. PC1 и PC2 получают IP адреса от DHCP сервера

ПРАКТИЧЕСКАЯ РАБОТА № 7.1

Настраиваем связь двух сетей через маршрутизатор

Время работы: 2 часа

1. Цель работы: Научится работать с программой Cisco Packet Tracer (CPT)

2. Технические средства

2.1 Оборудование: компьютер

2.2 Программное обеспечение: Cisco Packet Tracer, MS Word.

Таблица маршрутизации может составляться двумя способами: статично и динамично. В случае статической маршрутизации записи в таблице вводятся и изменяются вручную. Такой способ требует вмешательства администратора каждый раз, когда происходят изменения в топологии сети. С другой стороны, он является наиболее стабильным и требующим минимума аппаратных ресурсов маршрутизатора для обслуживания таблицы. При динамической маршрутизации записи в таблице обновляются автоматически при помощи одного или нескольких протоколов маршрутизации — RIP, OSPF, IGRP, EIGRP и др. Кроме того, маршрутизатор строит таблицу оптимальных путей к сетям назначения на основе различных критериев (метрик), таких, как: количества промежуточных узлов, пропускной способности каналов, задержки передачи данных и т. п. Динамическая маршрутизация оказывает дополнительную нагрузку на устройства, а высокая нестабильность сети может приводить к ситуациям, когда маршрутизаторы не успевают синхронизировать свои таблицы, что приводит к противоречивым сведениям о топологии сети в различных её частях и потере передаваемых данных.

Новый термин

Статическая маршрутизация — вид маршрутизации, при котором информация о маршрутах заносится в таблицы маршрутизации каждого маршрутизатора вручную администратором сети. Отсюда сразу же вытекает ряд недостатков. Прежде всего это очень плохая масштабируемость сетей, так как при добавлении N+1 сети потребуется сделать 2*(N+1) записей о маршрутах. Но, при использовании статических записей процессору маршрутизатора не требуется производить никаких расчетов, связанных с определением маршрутов – это плюс.

Статическая маршрутизация успешно используется при организации работы компьютерных сетей небольшого размера (1-2 маршрутизатора), в силу легкости конфигурации и отсутствии дополнительной нагрузки на сеть в виде широковещательного служебного трафика, характерного для динамических протоколов маршрутизации. Также статическая маршрутизация используется на компьютерах внутри сети. В таком случае обычно задается маршрут шлюза по умолчанию.

Построим такую сеть (Рисунок 7.1).

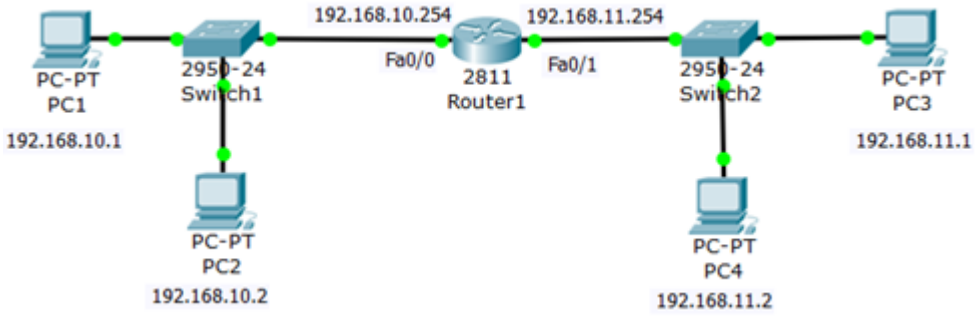


Рисунок 7.1. Постановка задачи

Наша цель – настроить связь двух сетей через маршрутизатор (роутер).

Шаг 1. Настройка ПК

Настраиваем компьютеры подсети 192.168.10.0 (Рисунок 7.2).

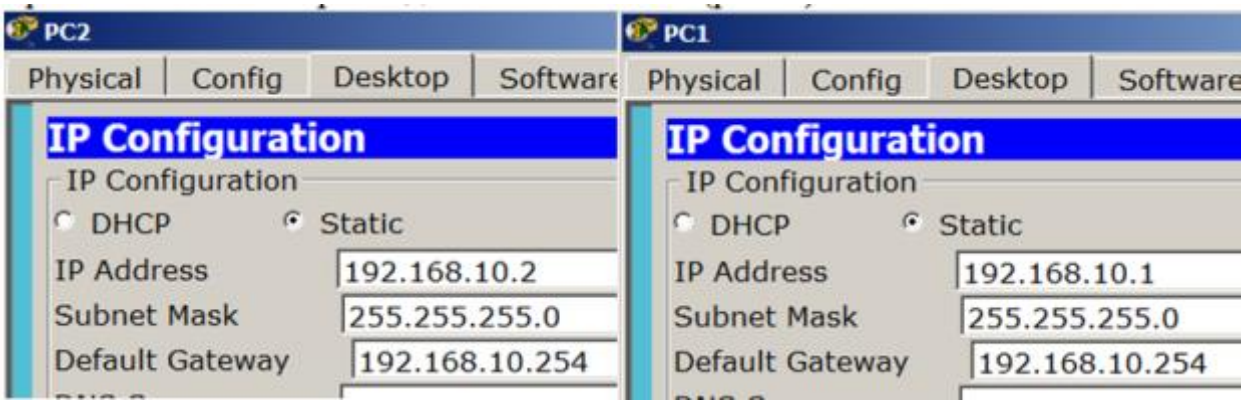


Рисунок 7.2. Настраиваем компьютеры подсети 192.168.10.0

Настраиваем компьютеры подсети 192.168.11.0 (Рисунок 7.3).

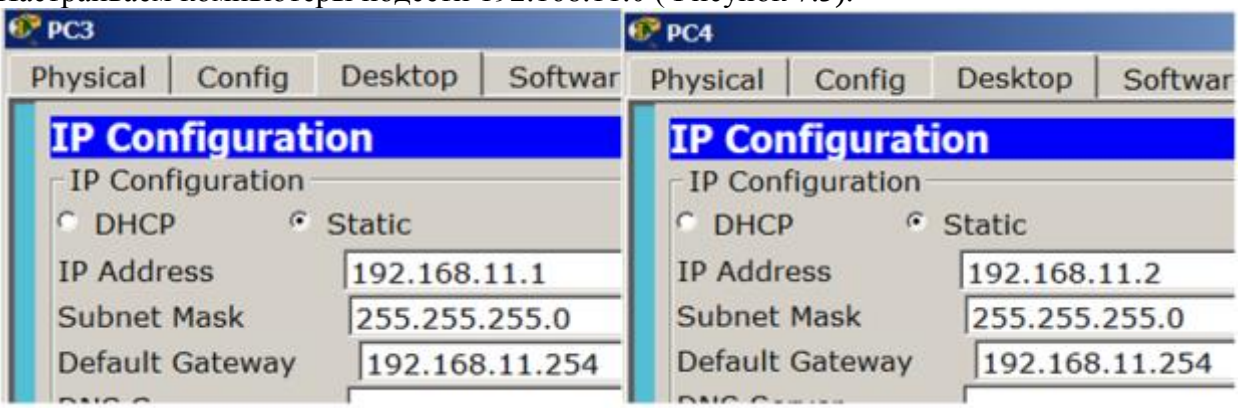


Рисунок 7.3. Настраиваем компьютеры подсети 192.168.11.0

Шаг 2. Настройка роутера (маршрутизатора)

Настраиваем роутер (маршрутизатор)как шлюз 192.168.10.254 для первой сети на интерфейсе Fa0/0 (Рисунок 7.4).

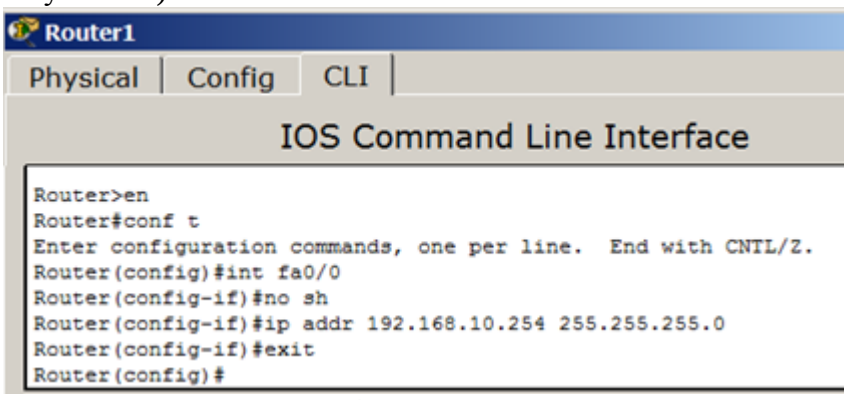


Рисунок 7.4. Окно ввода команд

Примечание

Здесь описаны следующие команды: привилегированный режим, режим конфигурирования, заходим на интерфейс, включаем этот интерфейс, задаем IPадрес и маску порта, выходим.

Аналогично настраиваем роутер как шлюз 192.168.11.254 для второй сети на интерфейсе Fa0/1 (Рисунок 7.5).

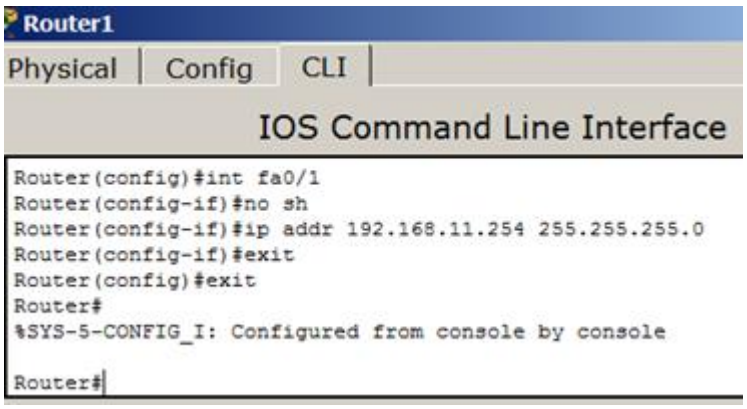


Рисунок 7.5. Настраиваем R1как шлюз 192.168.11.254 для второй сети

Шаг 3. Проверка связи сетей

Проверяем таблицу маршрутизации командой show ip route (Рисунок 7.6).

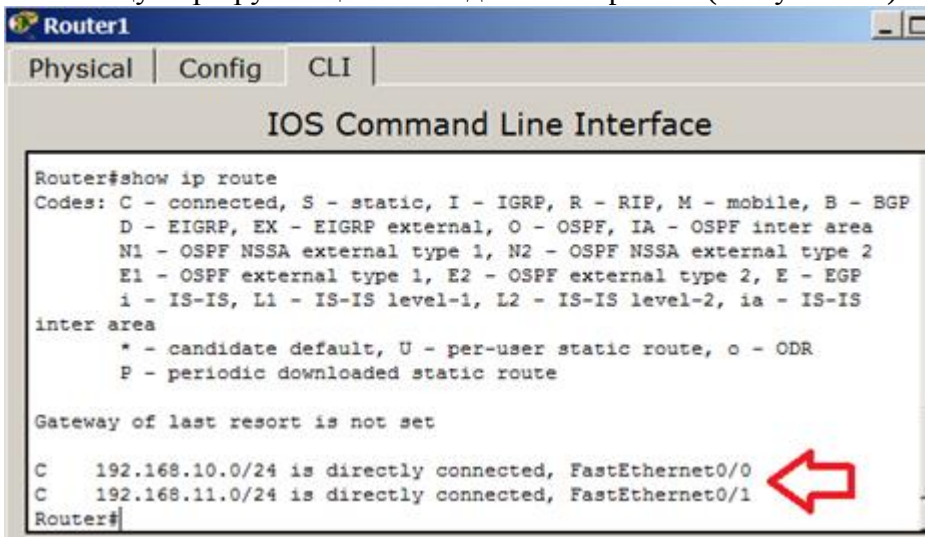


Рисунок 7.6. Проверяем таблицу маршрутизации роутера R1

У нас роутер обслуживает две сети. Проверяем связь роутера и ПК (Рисунок 7.7).

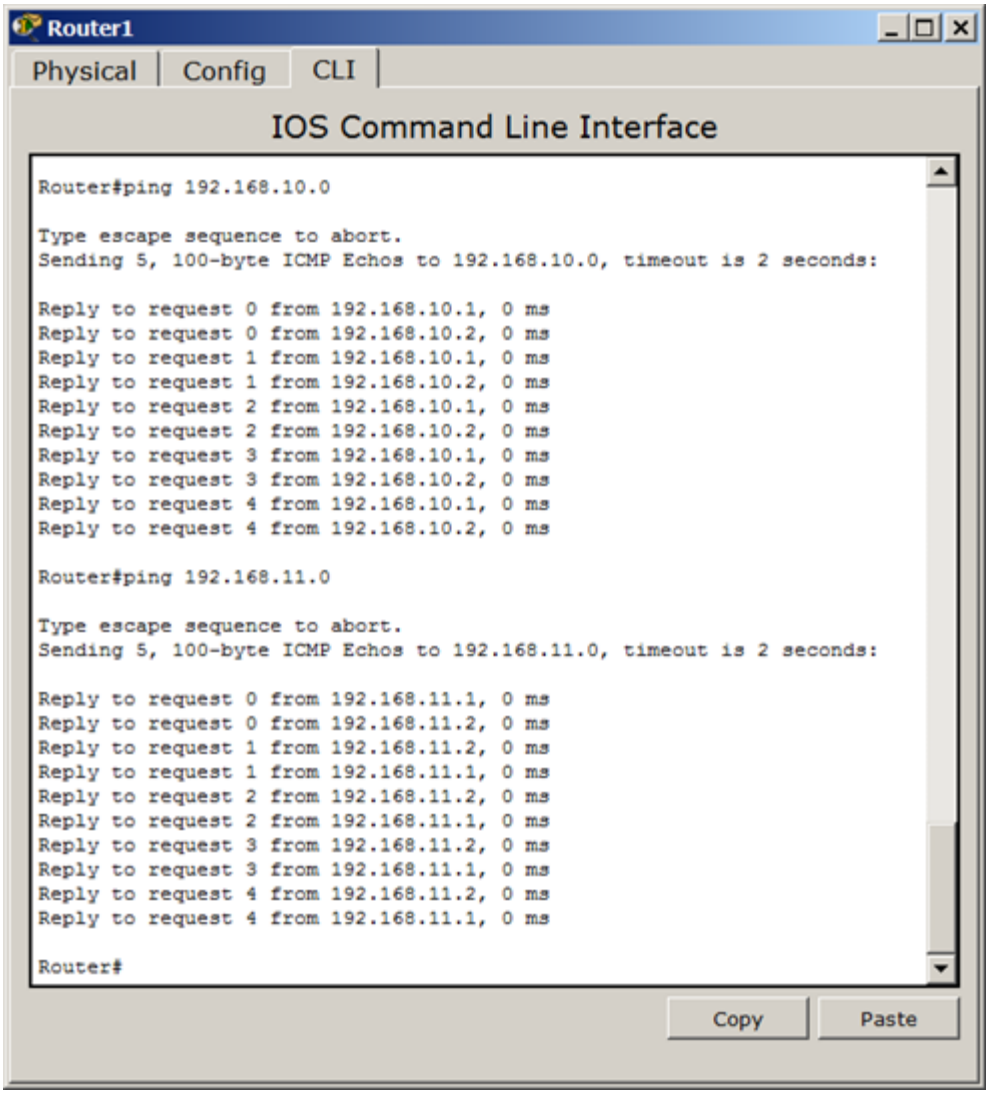


Рисунок 7.7. Связь роутера со всеми ПК есть

Проверяем связь роутера с подсетями (Рисунок 7.8).

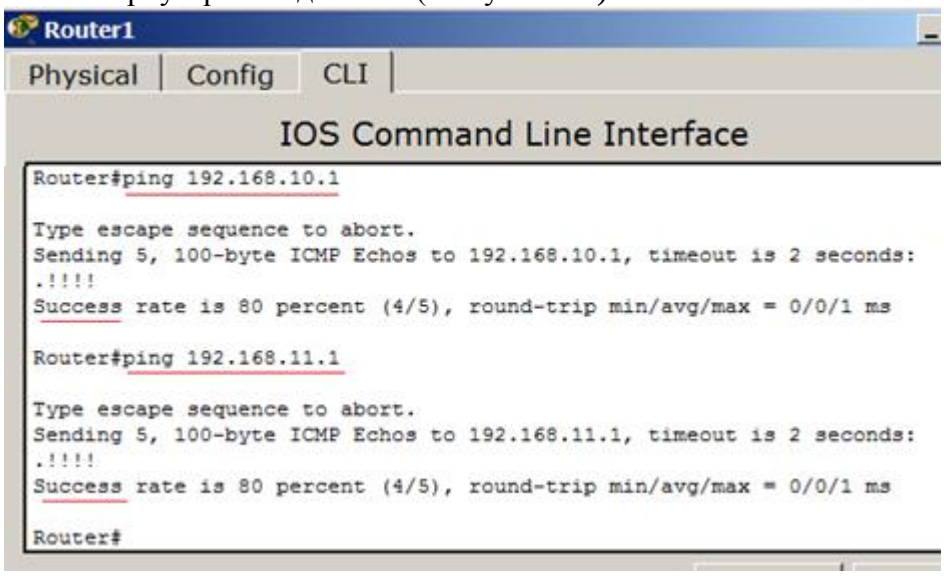


Рисунок 7.8. Проверяем связь роутера с подсетями

Примечание

Команда ping посылает ICMP эхо-пакеты для верификациисоединения. В приведённом выше 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 (!).

Проверим также связь ПК из разных сетей между собой (Рисунок 7.9).

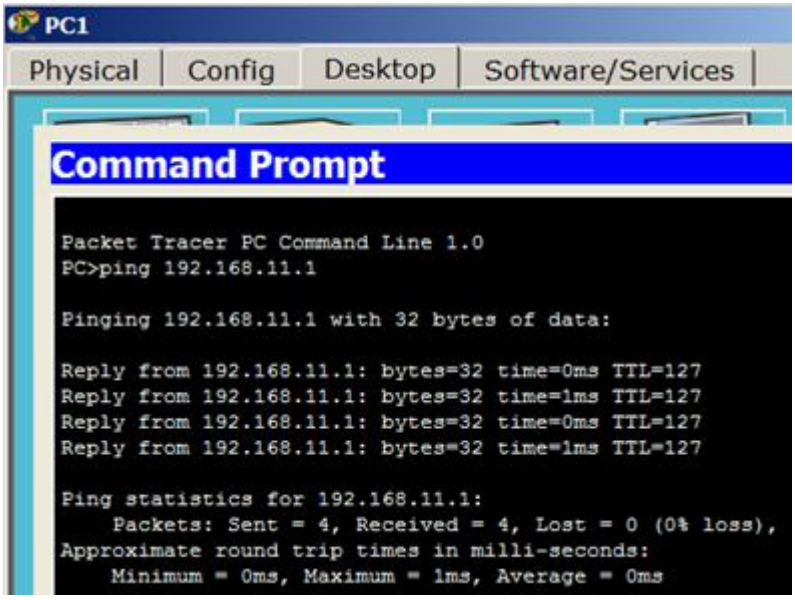


Рисунок 7.9. Проверка связи PC1иPC3

Примечание

Как выглядит порт маршрутизатора физически показано на Рисунок 7.10. Как видите, в него вставляется кабель с разъемом RJ-45.

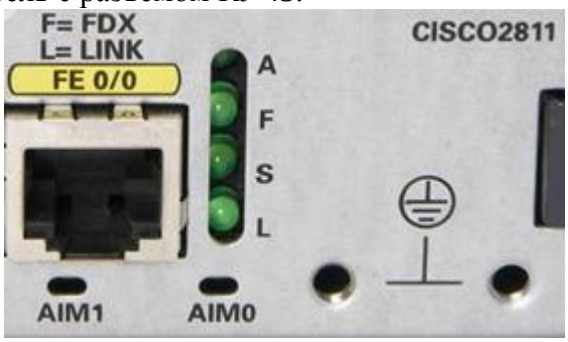


Рисунок 7.10. Ethernetport 0/0 маршрутизатора CISCO 2811

Задание 1. Настройка статической маршрутизации на оборудовании Cisco

Схема сети показана на Рисунок 7.11.

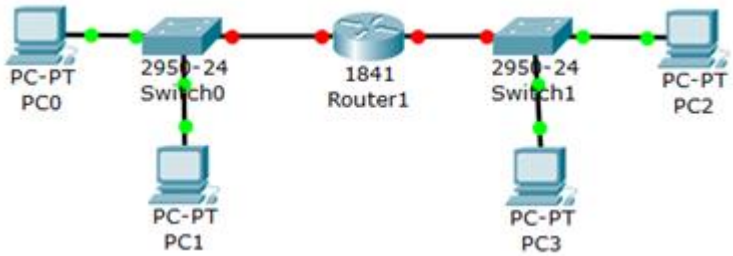


Рисунок 7.11. Схема сети

Студент должен:

1. Выполнить весь пример по настройке связи двух сетей
2. Покажите преподавателю Шаг 1. Настройку ПК
3. Покажите преподавателю Шаг 2. Настройку роутера (маршрутизатора)
4. Покажите преподавателю Шаг 3. Проверку связи сетей
5. Какой протокол следит за тем, чтобы в сети не было повторения IP адресов? (ARP)
6. Как шлюз по умолчанию для узлов сети связан с портами маршрутизатора?

В процессе выполнения задания необходимо:

1. Задать IP адреса сетевым интерфейсам маршрутизаторов, интерфейсам управления коммутаторов и сетевым интерфейсам локальных компьютеров;

2. Установить связь на физическом и канальном уровнях между соседними маршрутизаторами по последовательному сетевому интерфейсу;
3. Добиться возможности пересылки данных по протоколу IP между соседними объектами сети (C1-S1, C1-R1, S1-R1, R1-R2, R2-S2, R2-C2, и т.д.);
4. Настроить на маршрутизаторе R2 статические маршруты к сетям локальных компьютеров C1, C3
5. Настроить на маршрутизаторах R1, R3 маршруты "по умолчанию" к сетям локальных компьютеров C2-C3 и C1-C2 соответственно;
6. Добиться возможности пересылки данных по протоколу IP между любыми объектами сети (ping);
7. Переключившись в "Режим симуляции" рассмотреть и пояснить процесс обмена данными по протоколу ICMP между устройствами (выполнив команду Ping с одного компьютера на другой), пояснить роль протокола ARP в этом процессе.

ПРАКТИЧЕСКАЯ РАБОТА № 7.2

Настройка трех сетей с WEB сервером. Понятие маршрута по умолчанию

Время работы: 2 часа

1. Цель работы: Научится работать с программой Cisco Packet Tracer (CPT)

2. Технические средства

2.1 Оборудование: компьютер

2.2 Программное обеспечение: Cisco Packet Tracer, MS Word.

Специальные термины и понятия

Маршрутизатором (шлюзом), называется узел сети с несколькими IP-интерфейсами (содержащими свой MAC-адрес и IP-адрес), подключенными к разным IP-сетям, осуществляющий на основе решения задачи маршрутизации перенаправление дейтаграмм из одной сети в другую для доставки от отправителя к получателю. Как уже отмечалось, динамическая маршрутизация — это процесс протокола маршрутизации, определяющий взаимодействие устройства с соседними маршрутизаторами. Маршрутизатор будет обновлять сведения о каждой подключенной к нему сети. Если в сети произойдет изменение, протокол динамической маршрутизации автоматически информирует об изменении все маршрутизаторы. Если же используется статическая маршрутизация, обновить таблицы маршрутизации на всех устройствах придется системному администратору. Статическая маршрутизация позволяет сократить объем таблиц маршрутизации в конечных узлах и маршрутизаторах за счет использования в качестве номера сети назначения так называемого маршрута по умолчанию – default (0.0.0.0), который обычно занимает в таблице маршрутизации последнюю строку. Если в таблице маршрутизации есть такая запись, то все пакеты с номерами сетей, которые отсутствуют в таблице маршрутизации, передаются маршрутизатору, указанному в строке default.

Новый термин

Шлюз по умолчанию (defaultgateway) - адрес маршрутизатора, на который отправляется трафик для которого не нашлось отдельных записей в таблице маршрутизации. Для устройств, подключенных к одному маршрутизатору (как правило, это рабочие станции) использование шлюза по умолчанию — единственная форма маршрутизации.

Доступность компьютера проверяется при помощи посылки контрольного диагностического сообщения по протоколу ICMP (Internet Control Message Protocol), по которому любая оконечная станция должна выдать эхо-ответ узлу, отправившему такое сообщение. В сетях на основе TCP/IP для проверки соединений обычно используется утилита ping. Эта программа отправляет запросы (ICMP Echo-Request) протокола ICMP узлу сети с указанным IP-адресом. Получив этот запрос, исследуемый узел должен послать пакет с ответом (ICMP Echo-Reply). Первый узел фиксирует поступающие ответы. Время между отправкой запроса и получением ответа (RTT, от англ. Round Trip Time) позволяет определять двусторонние задержки (RTT) по маршруту и частоту потери пакетов, то есть косвенно определить загруженность каналов передачи данных и промежуточных устройств. Метрика — числовой коэффициент, влияющий на выбор маршрута в компьютерных сетях. Как правило, определяется количеством "хопов" (ретрансляционных переходов) до сети назначения или параметрами канала связи. Чем метрика меньше, тем маршрут приоритетнее. Петля маршрутизации — явление, возникающее, когда маршрутизатор отсылает пакет на неверный адрес назначения. Получивший такой пакет маршрутизатор возвращает его обратно. Таким образом получается петля. Для борьбы с подобными петлями в TCP/IP предусмотрен механизм TTL. Протоколы маршрутизации так же предлагают свои способы борьбы с петлями.

Схема у нас будет следующая:два коммутатора 2950-24, два ПК в сети 192.168.10.0 с маской 255.255.255.0. Сервер и компьютер в сети 192.168.20.0 с маской 255.255.255.0. Сеть между маршрутизаторами (марки 1841) 192.168.1.0 с маской 255.255.255.252. Компьютеры из сети 192.168.10.0 должны достучаться к DNScерверу в сети 192.168.20.0 (Рисунок 7.12).

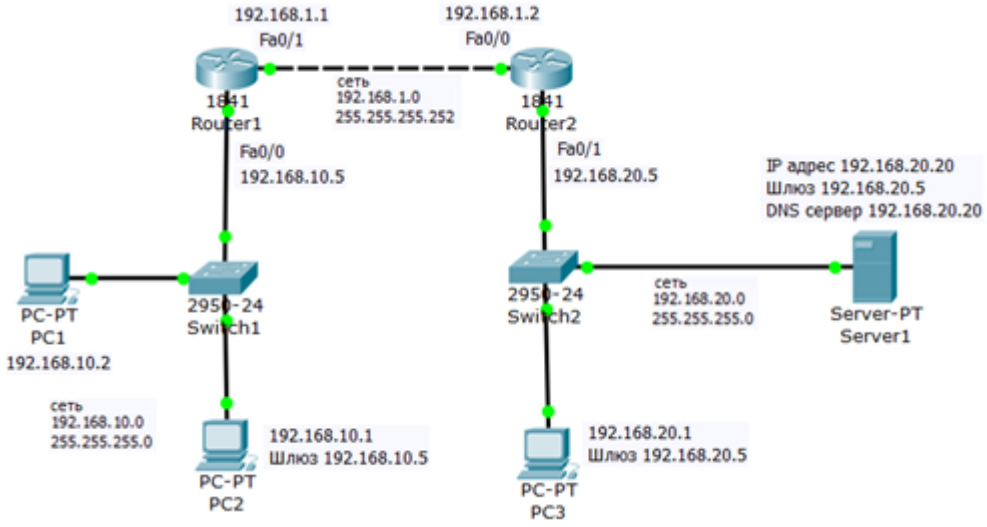


Рисунок 7.12. Постановка задачи

Сеть у нас не сложная, ПК в ней немного, поэтому будем использовать не динамическую, а статическую маршрутизацию.

Настройки сетевых интерфейсов роутеров

Будем настраивать связь роутеров через порты Fa0/1для R1 и Fa0/0 для R2. Настраиваем Router1 исходя из постановки задачи о том, что сеть между маршрутизаторами192.168.1.0 с маской 255.255.255.252. Поэтому порту Fa0/1 присвоим IP адрес 192.168.1.1 (Рисунок 7.13).

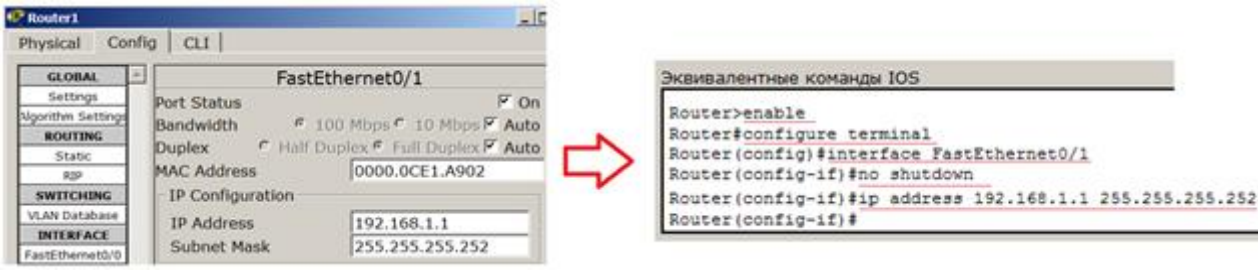


Рисунок 7.13. Настраиваем порт 0/1для маршрутизатораR1

Важно

При конфигурировании через webинтерфейс обязательно установите флажок On (Вкл.), что эквивалентно команде nosh.

Примечание

Как вариант, все параметры маршрутизатор можно настроить из командной строки на вкладке CLI следующими командами: enable (включаем привилегированный режим), config terminal (входим в режим конфигурации), interface fastethernet0/1 (настраиваем интерфейс 100 мб Ethernet 0/1), ip address 192.168.1.1 255.255.255.252 (прописываем ip адрес интерфейса и маску сети маршрутизатора), no shutdown (включаем интерфейс - по умолчанию все выключено), exit (выходим из режима конфигурирования интерфейса), end (закончили редактирование), write (сохранили конфигурацию).

Аналогично настраиваем Router2 исходя из постановки задачи о том, что сеть между маршрутизаторами192.168.1.0 с маской 255.255.255.252. Порту Fa0/0 присвоим IP адрес 192.168.1.2 (Рисунок 7.14).

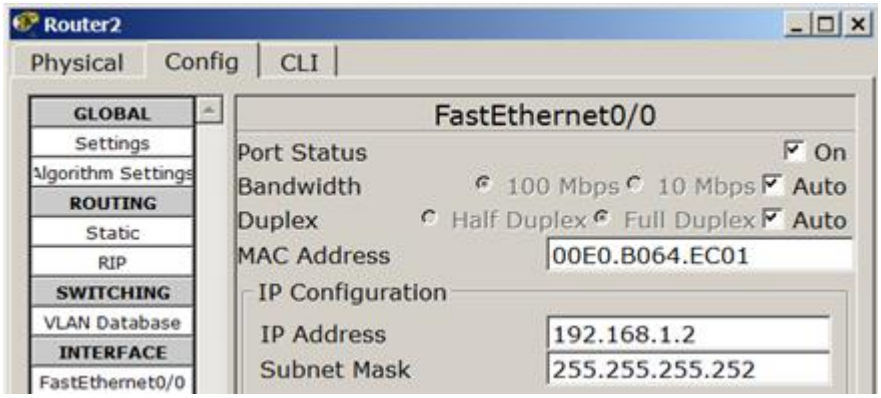


Рисунок 7.14. Конфигурируем R2

Примечание

При конфигурировании роутера из командной строки можно использовать сокращенную форму записи команд: en (включаем расширенный режим). conf t (входим в режим конфигурации). int fa0/0 (настраиваем интерфейс 100 мб. Ethernet 0/0). Ip addr192.168.1.2 255.255.255.252 (прописываем ip адрес интерфейса и маску сети). No shut (включаем интерфейс - по умолчанию он выключен). exit (выходим из режима конфигурирования интерфейса). end (заканчиваем редактирование). wr (сохраняем конфигурацию).

В итоге после настройки маршрутизаторов на портах загораются зеленые маркеры, то есть, связь между ними есть. Сеть между маршрутизаторами работает, но маршрутизации пока нет, то есть, из одной сети в другую попасть нельзя.

Настройка связи маршрутизаторов с подсетями (настройка шлюзов)

Настроим порт Fa0/0 маршрутизатора R1 на работу с сетью 192.168.10.0 (Рисунок 7.15).

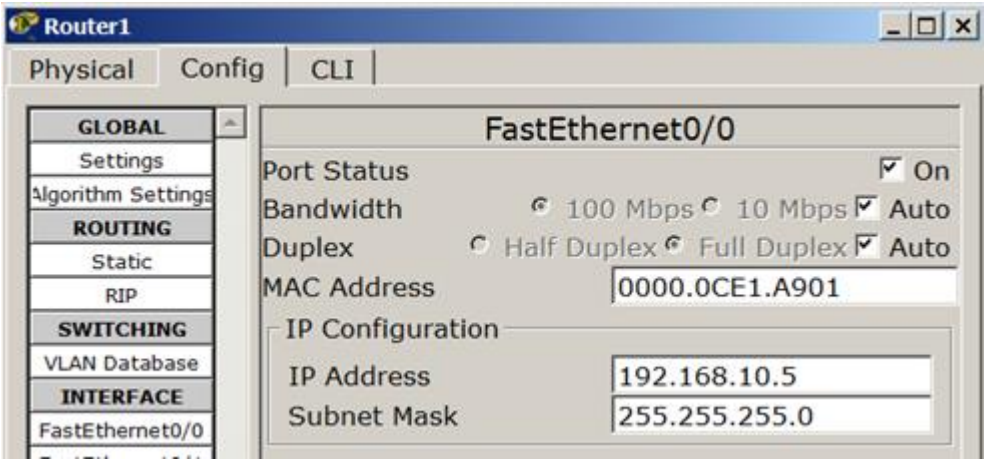


Рисунок 7.15. Настроим портFa0/0 маршрутизатораR1 на работу с сетью 192.168.10.0

Аналогично порт Fa0/1 маршрутизатора R2 настроим на работу с сетью 192.168.20.0 (Рисунок 7.16).

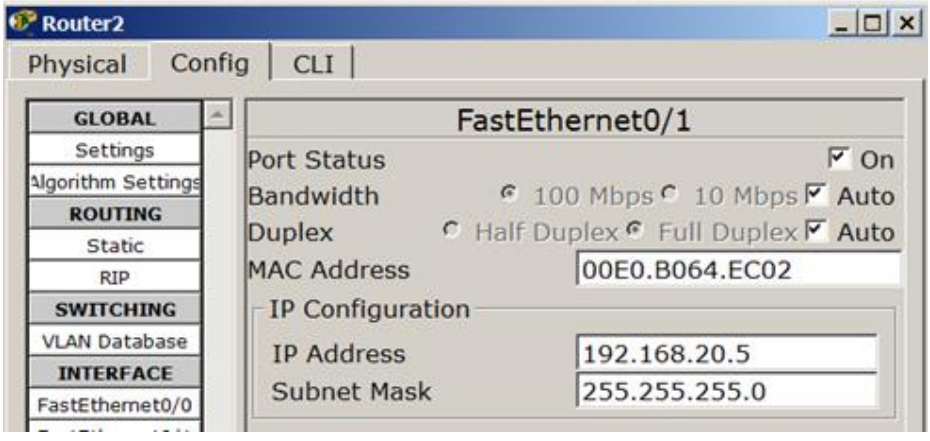


Рисунок 7.16. Порт Fa0/1 маршрутизатораR2 настроим на работу с сетью 192.168.20.0

Как теперь видно по маркерам – сеть поднялась (Up), то есть все индикаторы горят зеленым цветом.

Настройка PC1 и PC2

Продолжим работу и настроим компьютеры в сети 192.168.10.0, то есть, нужно задать IP компьютеров, маску сети и основной шлюз. По исходным условиям задачи у нас слева пара компьютеров в сети 192.168.10.0 с маской 255.255.255.0 (Рисунок 7.17).

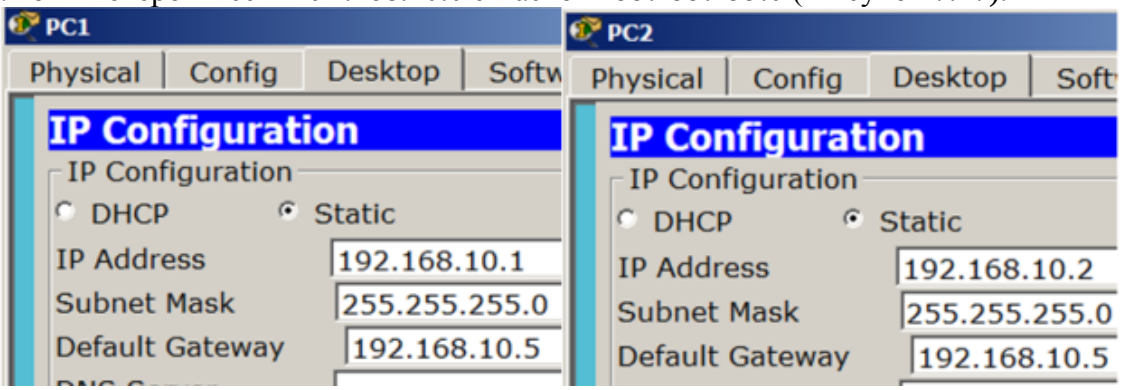


Рисунок 7.17. Настраиваем PC1 и PC2

Новый термин

Основной шлюз (Default Gateway) – это адрес, куда компьютер отправляет пакет, если не знает, куда его отправить. Например, при попытке узла Б отправить данные узлу А. в отсутствие конкретного адреса к узлу А, узел Б направляет трафик TCP/IP, предназначенный для узла А, своему основному шлюзу.

Настройка сервера и PC3

Далее нужно настроитьPC3 и сервер в сети 192.168.20.0 (Рисунок 7.18 и Рисунок 7.19).

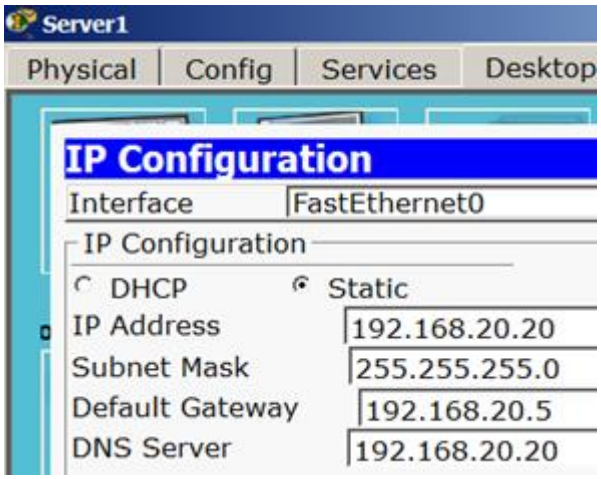


Рисунок 7.18. Настройка сервера

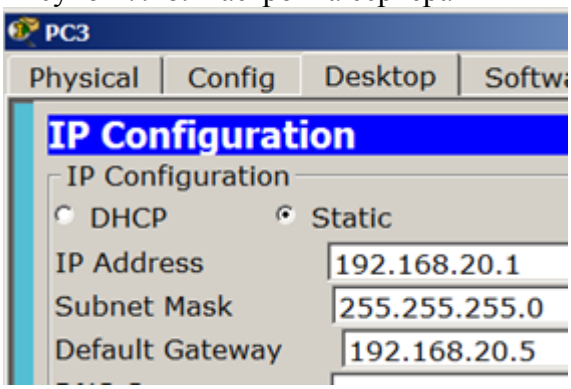


Рисунок 7.19. НастраиваемPC2

Настройка маршрутизации на маршрутизаторах (маршрута по умолчанию)

Можете пропинговать сети и убедиться в том, что ситуация такая: запросы из сети …10.0 в сеть…20.0 проходят, а ответов – нет. Поэтому надо прописать на маршрутизаторах маршруты по умолчанию. Вспомним, что порту Fa0/1 мы присвоили IP адрес 192.168.1.1, а порту Fa0/0 – адрес 192.168.1.2. Поэтому на маршрутизаторе R1 для порта Fa0/1 с IP адресом 192.168.1.1 следует выполнить такие команды (Рисунок 7.20).

Рисунок 7.20. Прописываем маршрут по умолчанию на R1

Примечание

Запись означает, что все запросы, для которых не прописаны маршруты, R1 посылает на 192.168.1.2, то есть, на R2.

Для R2 поступаем аналогично (Рисунок 7.21).

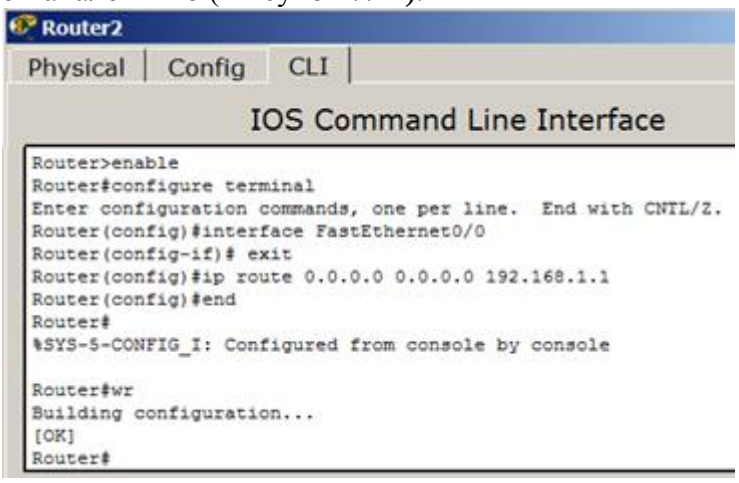


Рисунок 7.21. Прописываем маршрут по умолчанию на R2

Примечание

Запись означает, что все запросы, для которых не прописаны маршруты, R2 отправляет на 192.168.1.1, то есть, на R1.

Проверяем работу сети

После настройки роутеров можно протестировать сеть, для этого нужно пропинговать компьютерами из одной сети — компьютеры из другой сети (Рисунок 7.22).

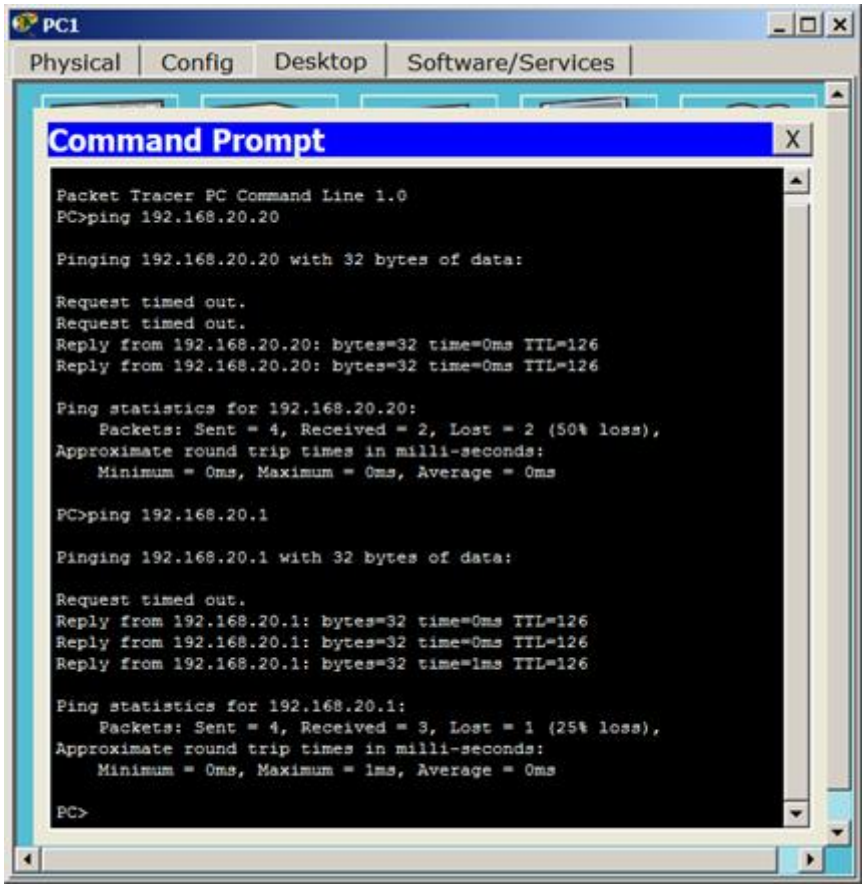


Рисунок 7.22. Связь не идеальная, но есть

Чтобы убедиться наверняка, давайте посмотрим, как идут пакеты по узлам сети и для этого воспользуемся командой tracert 192.168.20.20 (Рисунок 7.23).

Примечание

Tracert — команда, предназначенная для определения маршрутов следования данных в сетях TCP/IP.

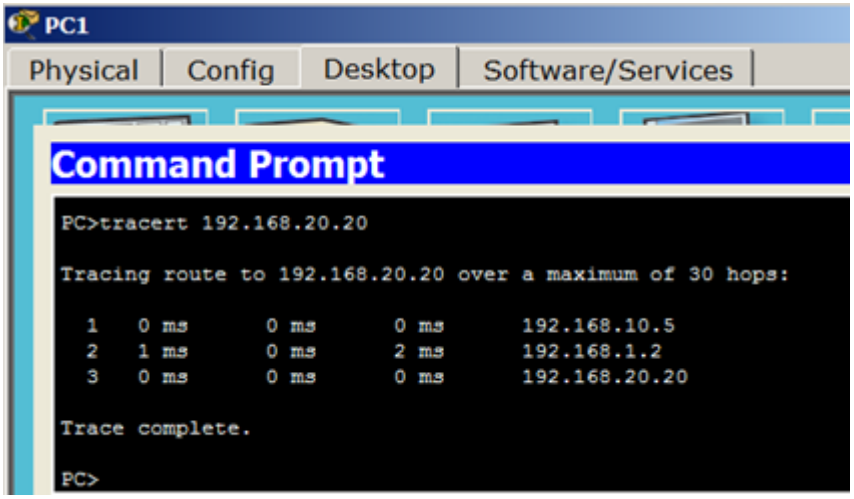


Рисунок 7.23. Наблюдаем как идут пакеты между сегментами сети от PC1 на сервер

Как видно из скриншота пакеты сначала уходят на адрес 192.168.10.5 (R1– порт Fa0/0), далее на адрес 192.168.1.2 (R2 – порт Fa0/0), а дальше приходит на сервер 192.168.20.20 — все верно!

Примечание

Web страниц на сервере мы не создавали, но они там существуют изначально, по умолчанию. Запустите Web Browser и убедитесь в этом самостоятельно (Рисунок 7.24).

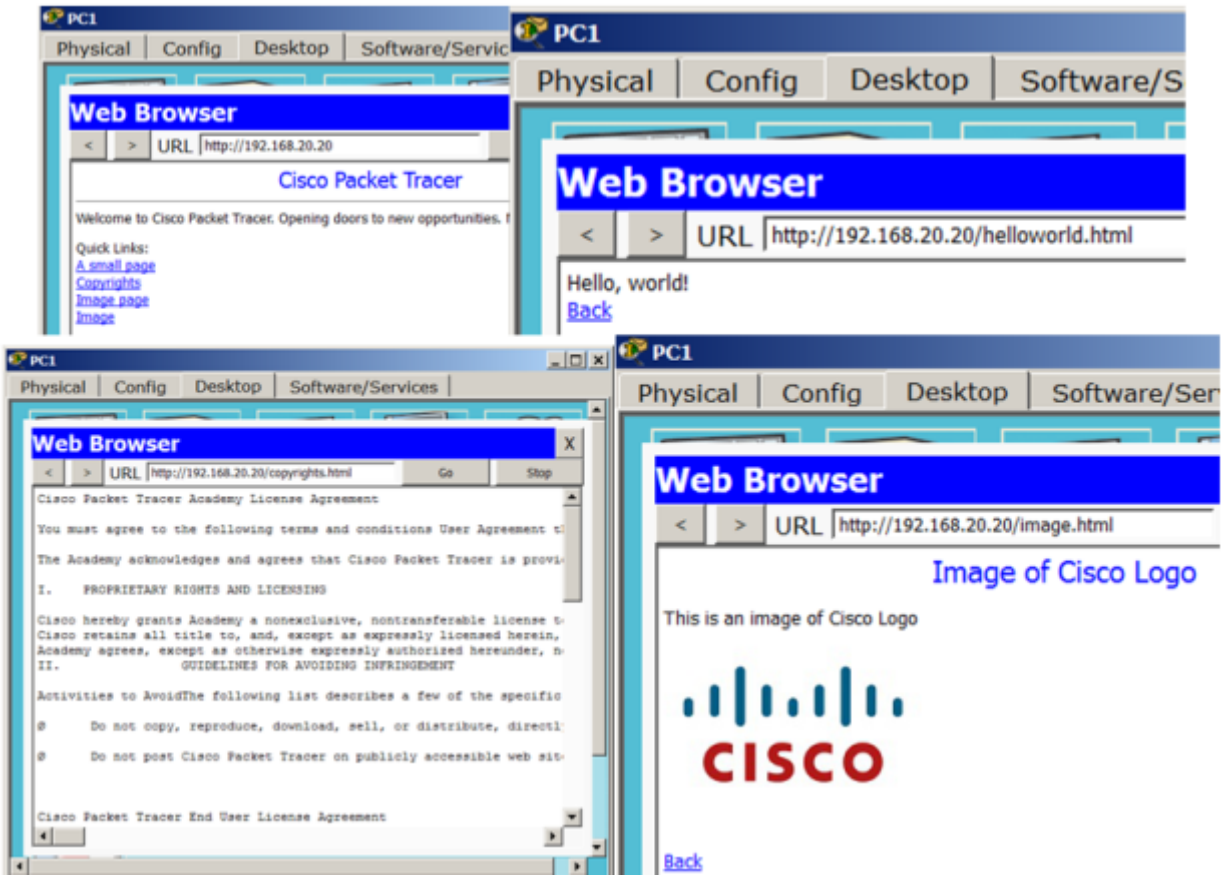


Рисунок 7.24. На сервере работает служба HTTP

Описанная выше и полностью настроенной сеть (файл task-7-2.pkt) прилагается.

ПРАКТИЧЕСКАЯ РАБОТА № 7.3

Сеть на двух маршрутизаторах

Время работы: 2 часа

1. Цель работы: Научится работать с программой Cisco Packet Tracer (CPT)

2. Технические средства

2.1 Оборудование: компьютер

2.2 Программное обеспечение: Cisco Packet Tracer, MS Word.

Далее мы изучим статическую маршрутизацию в локальных сетях, рассмотрев этот вопрос на двух практических примерах.

Схема сети для настройки статической маршрутизации приведена на Рисунок 7.25.

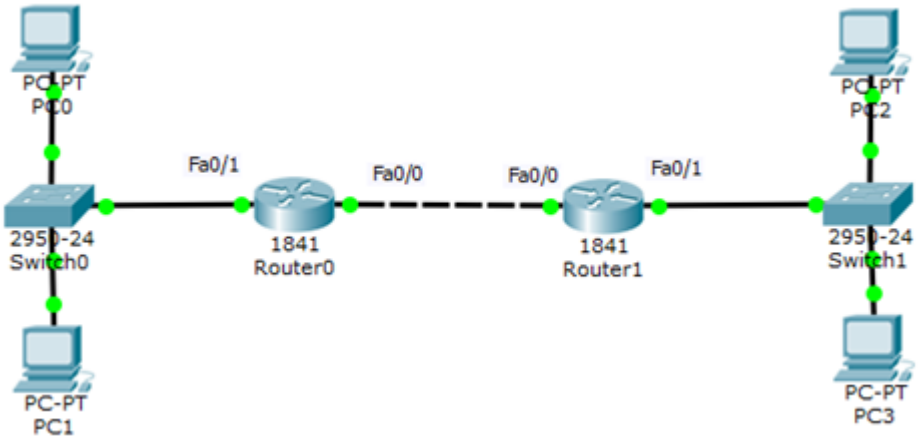


Рисунок 7.25. Схема сети

Если сейчас командой show ip route посмотреть таблицу маршрутизации на R0 и R1, то увидим следующее (Рисунок 7.26 и Рисунок 7.27).

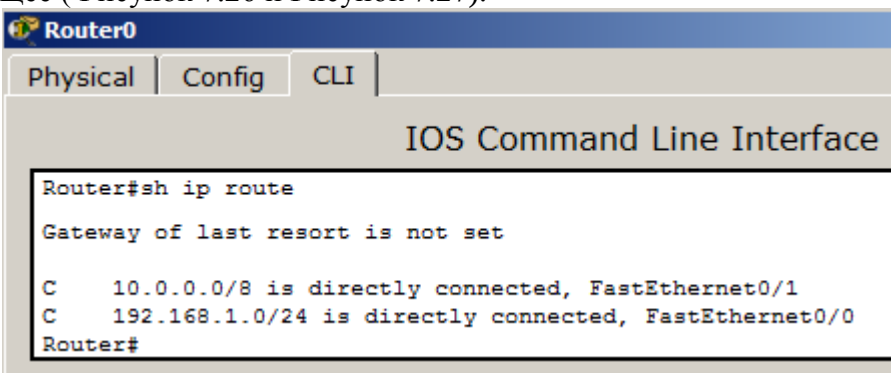


Рисунок 7.26. Таблица маршрутизации на 1-ммаршрутизаторе

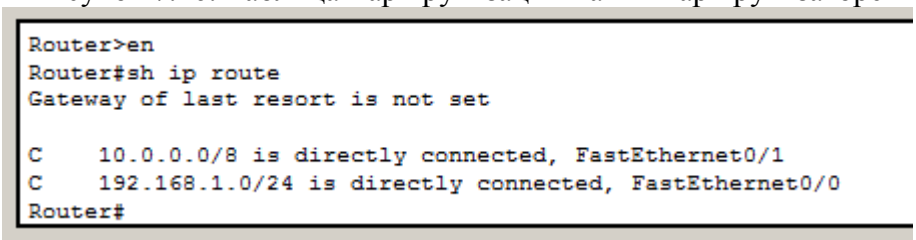


Рисунок 7.27. Таблица маршрутизации на 2-ммаршрутизаторе

Мы видим, что в данный момент в нашей таблице есть только сети, подключенные напрямую. R0 не знает сеть 10.1.2.0, а R1 не знает сеть 10.1.1.0. Поэтому, чтобы настроить маршрутизацию, следует добавим эти маршруты в таблицы маршрутизаторов:

R0 (config)#ip route 10.1.2.0 255.255.255.0 192.168.1.2

R1 (config)#ip route 10.1.1.0 255.255.255.0 192.168.1.1

Теперь снова выведем таблицы маршрутизации наших устройств (Рисунок 7.28).

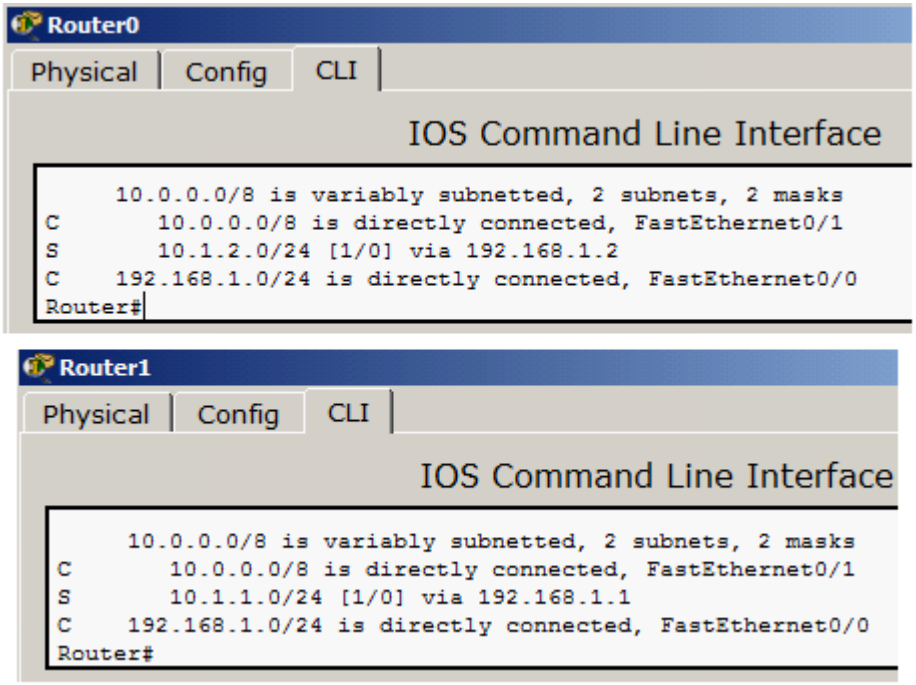


Рисунок 7.28. Маршрутизация настроена

Теперь 1-й маршрутизатор знает, что пакеты, направляемые в подсеть 10.1.2.0 можно переслать маршрутизатору с ip адресом 192.168.1.2, а 2-й маршрутизатор знает, что пакеты, направляемые в подсеть 10.1.1.0 можно переслать маршрутизатору с ip адресом 192.168.1.1. Проверяем связь ПК из разных сетей (Рисунок 7.29).

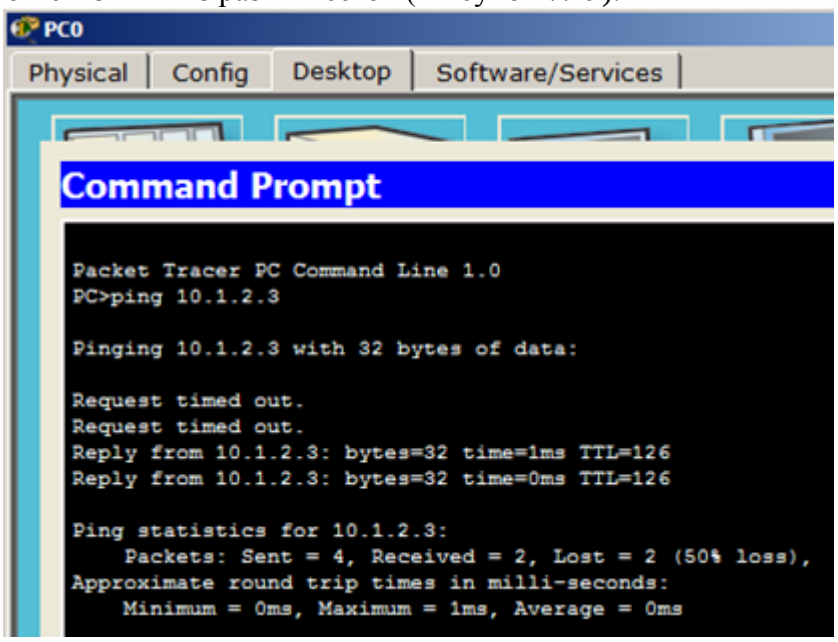


Рисунок 7.29. Статическая маршрутизация настроена – PC0 может общаться с PC3

Статическая маршрутизация для пяти сетей и роутеров с тремя портами

В этом примере мы соберем и настроим следующую схему сети (Рисунок 7.30).

Схема сети

На данной схеме имеется пять сетей: 192.168.1.0, 172.20.20.0, 192.168.100.0, 10.10.10.0 и 192.168.2.0. В качестве шлюза по умолчанию у каждого компьютера указан интерфейс маршрутизатора, к которому он подключен. Маска у всех ПК одна - 255.255.255.0. Маска маршрутизаторов для каждого порта своя: Fa0/0 -255.255.255.0, Fa0/1 - 255.255.0.0, Fa1/0 - 255.255.255.252.

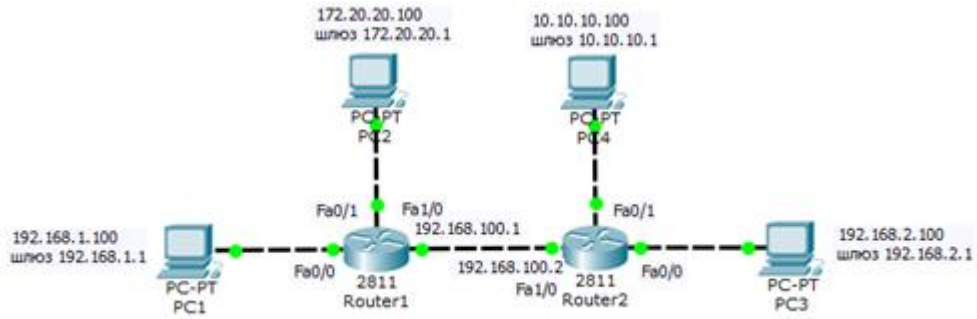


Рисунок 7.30. Связь сетей посредством маршрутизаторов

Далее соединим маршрутизаторы между собой нам потребуется добавить к маршрутизатору интерфейсную плату NM-1FE-TX (NM – Network module, 1FE – содержит один порт FastEthernet, TX – поддерживает 10/100MBase-TX). Чтобы это сделать перейдите к окну конфигурации маршрутизатора0, выключите его, щелкнув на кнопке питания. После этого перетяните интерфейсную плату NM-1FE-TX в разъем маршрутизатора (Рисунок 7.31). После того как карта добавлена, еще раз щелкните по тумблеру маршрутизатора, чтобы включить его. Повторите аналогичные действия со вторым маршрутизатором.

Рисунок 7.31. Вставляем интерфейсную плату в маршрутизатор

Постановка задачи

Нам требуется произвести необходимые настройки для того, чтобы все ПК могли общаться друг с другом, то есть, необходимо обеспечить доступность компьютеров из разных сетей между собой.

Настройка маршрутизации (маршрута по умолчанию)

В настоящий момент если мы отправим с компьютера PC1 с IP адресом 192.168.1.100 пакет на интерфейс Fa1/0 с IP адресом 192.168.100.2 маршрутизатора R2, то ICMP пакет слева дойдет до этого маршрутизатора, но при отправке ICMP пакетов в обратном направлении с адреса 192.168.100.2 на адрес 192.168.1.100 возникнет проблема. Дело в том, что маршрутизатор R2 не имеет в своей таблице маршрутизации информации о сети 172.20.20.0, так как шлюз по умолчанию мы еще не прописывали и маршрутизатор R2 не знает, куда отправлять ответы на запрос. В небольших сетях самым простым способом настроить маршрутизацию, является добавление маршрута по умолчанию. Для того чтобы это сделать выполните на маршрутизаторе R1 в режиме конфигурирования следующие команды (Рисунок 7.32).

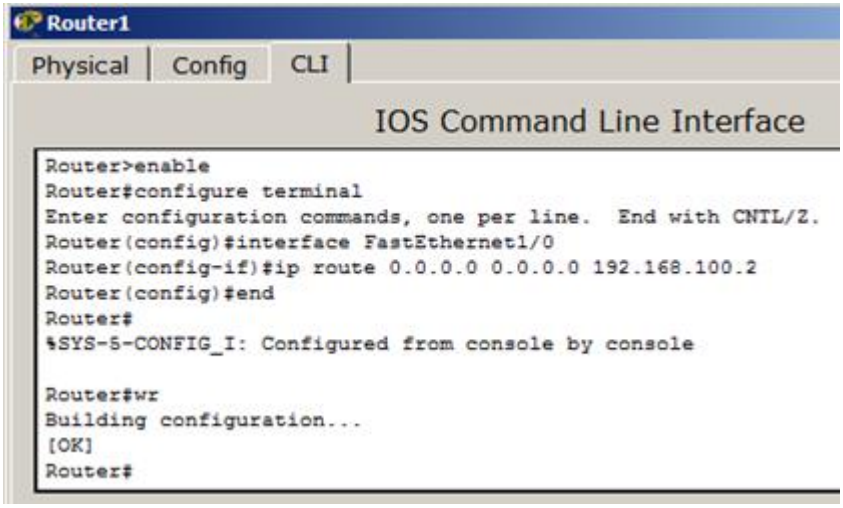


Рисунок 7.32. Настройка маршрута по умолчанию на R1

Примечание

В этих командах первая группа цифр 0.0.0.0 обозначают IP адрес сети назначения, следующая группа цифр 0.0.0.0 обозначает её маску, а последние цифры – 192.168.100.2 это IP адрес интерфейса, на который необходимо передать пакеты, чтобы попасть в данную сеть. Если мы указываем в качестве адреса сети 0.0.0.0 с маской 0.0.0.0, то данный маршрут становится маршрутом по умолчанию, и все пакеты, адреса назначения которых, прямо не указаны в таблице маршрутизации будут отправлены на него.

На правом маршрутизаторе R2 поступаем аналогично (Рисунок 7.33).

Рисунок 7.33. Настройка маршрута по умолчанию на R2

Отправим с компьютера PC1 с IP адресом 192.168.1.100 пакет на интерфейс Fa1/0 с IP адресом 192.168.100.2 маршрутизатора R2 и посмотрим, что изменилось (Рисунок 7.34).

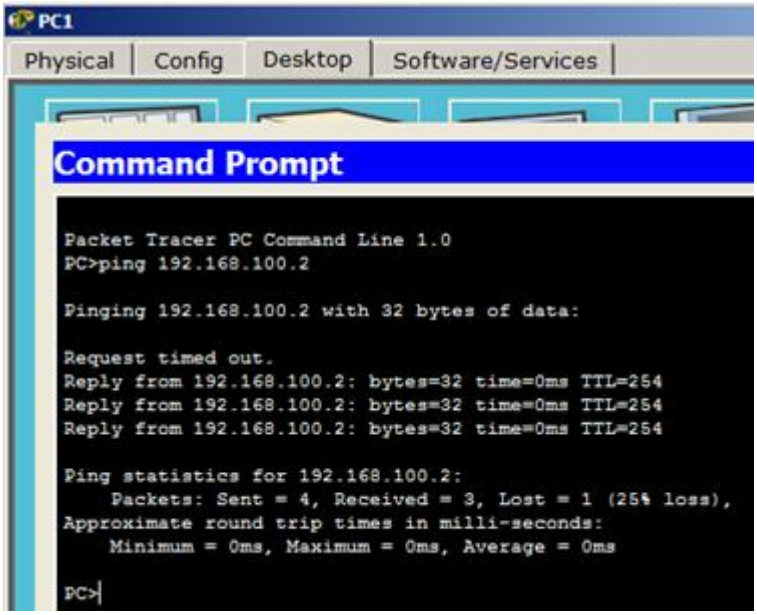


Рисунок 7.34. С компьютера PC1 с IP адресом 192.168.1.100 успешно пингуем интерфейс Fa1/0 с IP адресом 192.168.100.2 маршрутизатора R2

Резюме

Допустим, мы хотим пропинговать с компьютера PC1 с адресом 192.168.1.100 (из левой сети) компьютер PC4 с IP адресом 10.10.10.100 (из правой сети). В качестве шлюза по умолчанию на компьютере с адресом 192.168.1.100 установлен адрес 192.168.1.1интерфейса Fa0/0 маршрутизатора R1.

Сначала компьютер будет искать в свой таблице маршрутизации адрес 10.10.10.100, а после того, как он его не найдет, ICMP пакеты будут отправлены на адрес по умолчанию, то есть на интерфейс маршрутизатора R1 с адресом 192.168.1.1 (порт Fa0/0). Получив пакет, маршрутизатор R1 просмотрит адрес его назначения – 10.10.10.100 и также попытается обнаружить его в свой таблице маршрутизации. Когда он не обнаружит и его, пакет будет отправлен на интерфейс Fa1/0, с адресом 192.168.100.2 маршрутизатора R2.

Маршрутизатор R2 попробует обнаружить в свой таблице маршрутизации маршрут к адресу 10.10.10.100. Когда это не увенчается успехом, маршрутизатор будет искать маршрут к сети 10.0.0.0. Информация о данной сети содержится в таблице маршрутизации, и маршрутизатор знает, что для того чтобы попасть в данную сеть необходимо отправить пакеты на интерфейс FastEthernet0/1, непосредственно к которому подключена данная сеть.

Так как в нашем примере вся сеть 10.0.0.0, представляет из себя всего 1 компьютер, то пакеты сразу же попадают в место назначения, то есть, на компьютер с IP адресом 10.10.10.100. При отсылке ответных ICMP пакетов, все происходит аналогичным образом. Однако, не всегда можно обойтись указанием только маршрутов по умолчанию. В более сложных сетевых конфигурациях может потребоваться прописывать маршрут для каждой из сетей в отдельности. Это будет непросто. Поэтому в больших сетях обычно используют не статическую, а динамическую маршрутизацию.

ПРАКТИЧЕСКАЯ РАБОТА № 8.1

Настройка протокола RIP версии 2 для сети из шести устройств

Время работы: 2 часа

1. Цель работы: Научится работать с программой Cisco Packet Tracer (CPT)

2. Технические средства

2.1 Оборудование: компьютер

2.2 Программное обеспечение: Cisco Packet Tracer, MS Word.

Маршрутизация - процесс определения в сети наилучшего пути, по которому пакет может достигнуть адресата. Динамическая маршрутизация может быть осуществлена с использованием одного и более протоколов (RIP v2, OSPF и др.).

Новый термин

Динамическая маршрутизация — вид маршрутизации, при котором таблица маршрутизации заполняется и обновляется автоматически при помощи одного или нескольких протоколов маршрутизации (RIP, OSPF, EIGRP, BGP).

Каждый протокол маршрутизации использует свою систему оценки маршрутов (метрику). Маршрут к сетям назначения строится на основе таких критериев как

- количество ретрансляционных переходов
- пропускная способность канала связи
- задержки передачи данных
- и др.

Маршрутизаторы обмениваются друг с другом информацией о маршрутах с помощью служебных пакетов по протоколу UDP. Такой обмен информации увеличивает наличие дополнительного трафика в сети и нагрузку на эту сеть. Возможна также ситуация, при которой таблицы маршрутизации на роутерах не успевают согласоваться между собой, что может повлечь появление ошибочных маршрутов и потерю данных.

Протоколы маршрутизации делятся на три типа:

- Дистанционно векторные протоколы (RIP)
- Протоколы с отслеживанием состояния каналов (OSPF)
- Смешанные протоколы (EIGRP)
- И др.

Протокол RIP

RIP — протокол дистанционно-векторной маршрутизации, использующий для нахождения оптимального пути алгоритм Беллмана-Форда. Алгоритм маршрутизации RIP-один из самых простых протоколов маршрутизации. Каждые 30 секунд он передает в сеть свою таблицу маршрутизации. Основное отличие протоколов в том, что RIPv2 (в отличие от RIPv1) может работать по мультикасту, то есть, рассылаясь на мультикаст адрес. Максимальное количество "хопов" (шагов до места назначения), разрешенное в RIP1, равно 15 (метрика 15). Ограничение в 15 хопов не дает применять RIP в больших сетях, поэтому протокол наиболее распространен в небольших компьютерных сетях. Вторая версия протокола — протокол RIP2 была разработана в 1994 году и является улучшенной версией первого. В этом протоколе повышена безопасность за счет введения дополнительной маршрутной информации. Принцип дистанционно-векторного протокола: каждый маршрутизатор, использующий протокол RIP периодически широковещательно рассылает своим соседям специальный пакет-вектор, содержащий расстояния (измеряются в метрике) от данного маршрутизатора до всех известных ему сетей. Маршрутизатор получивший такой вектор, наращивает компоненты вектора на величину расстояния от себя до данного соседа и дополняет вектор информацией об известных непосредственно ему самому сетях или сетях, о которых ему сообщили другие маршрутизаторы. Дополненный вектор маршрутизатор рассылает всем своим соседям. Маршрутизатор выбирает из нескольких альтернативных маршрутов маршрут с наименьшим значением метрики, а маршрутизатор, передавший информацию о таком маршруте помечается как следующий (next hop). Протокол непригоден для работы в больших сетях, так как засоряет сеть интенсивным трафиком, а узлы сети оперируют только векторами-расстояний, не имея точной

информации о состоянии каналов и топологии сети. Сегодня даже в небольших сетях протокол вытесняется превосходящими его по возможностям протоколами EIGRP и OSPF.

Наша задача – настроить маршрутизацию на схеме, представленной на Рисунок 8.1.

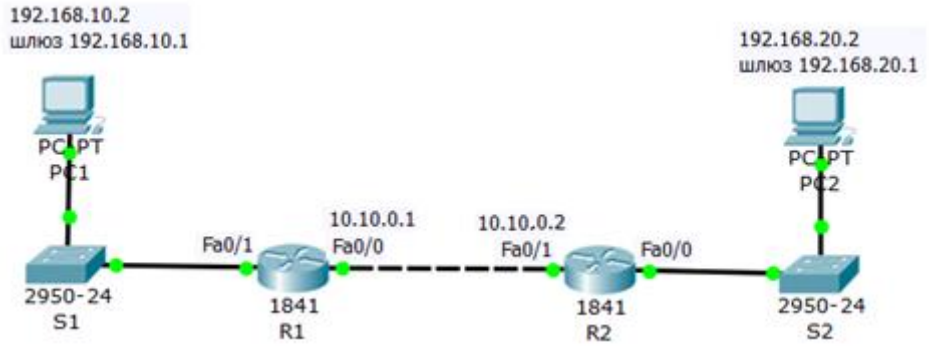


Рисунок 8.1. Схема сети

Примечание

При настройке сети не забывайте включать порты.

Настройка протокола RIP на маршрутизаторе R1

Войдите в конфигурации в консоль роутера и выполните следующие настройки (Рисунок 8.2).

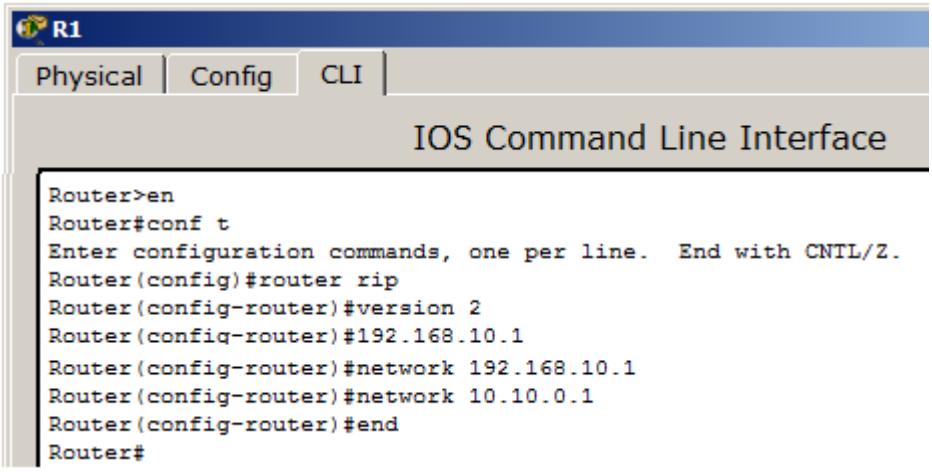


Рисунок 8.2. Настройка протокола RIPv2 на маршрутизаторе Router1

Примечание

Router(config)#router rip (Вход в режим конфигурирования протокола RIP). Router(config-router)#network 192.168.10.1 (Подключение клиентской сети к роутеру со стороны коммутатора S1). Router(config-router)#network 192.168.20.1 (Подключение второй сети, то есть сети между роутерами). Router(config-router)#version 2 (Задание использования второй версии протокол RIP).

Настройка протокола RIP на маршрутизаторе R2

Войдите в конфигурации роутера 2 и выполните следующие настройки (Рисунок 8.3).

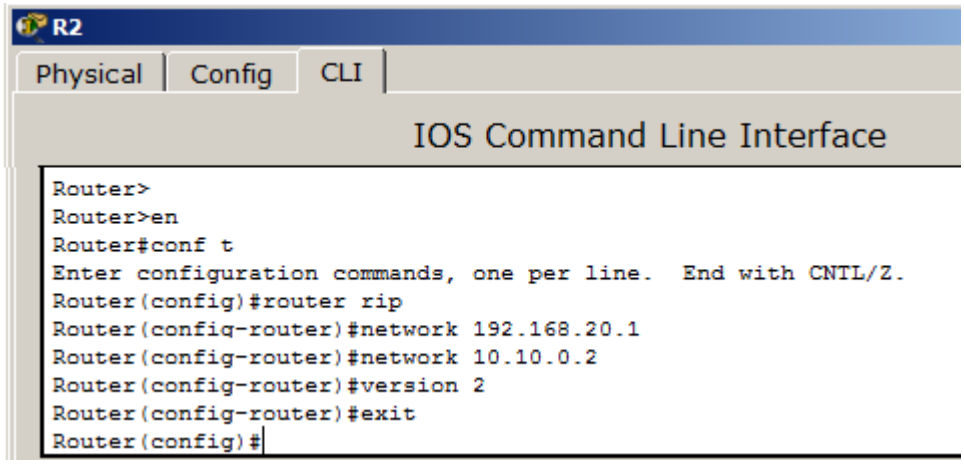


Рисунок 8.3. Настройка протокола RIPv2 на маршрутизаторе R2

Проверяем настройки коммутаторов и протокола RIP

Давайте посмотрим настройки протокола RIPv2 на маршрутизаторах R1 и R2 (Рисунок 8.4).

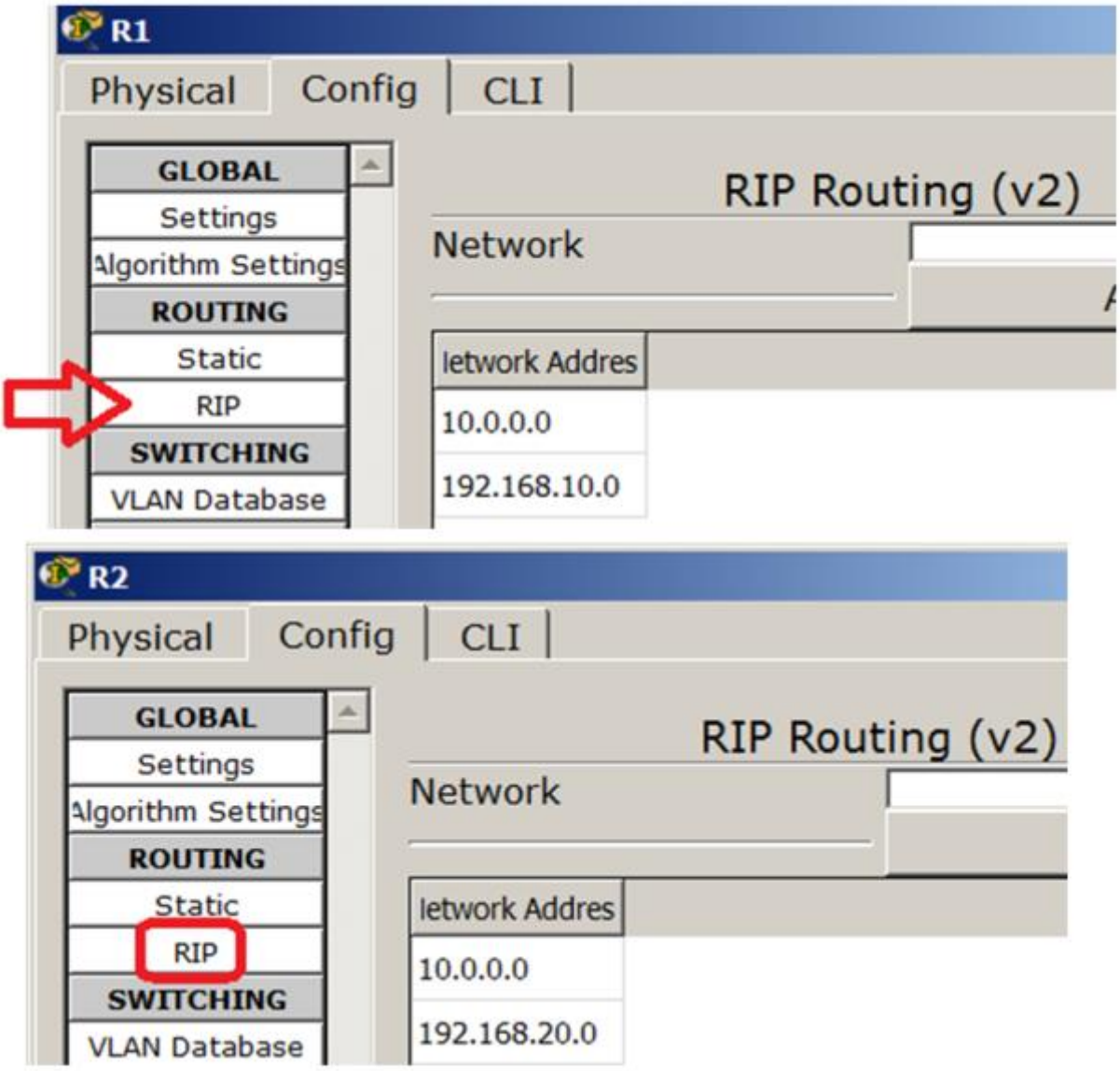


Рисунок 8.4. Настройки маршрутизаторов R1 и R2

Чтобы убедиться в том, что маршрутизаторы действительно правильно сконфигурированы и работают корректно, просмотрите таблицу RIP роутеров, используя команду: Router#show ip route rip (Рисунок 8.5 и Рисунок 8.6).

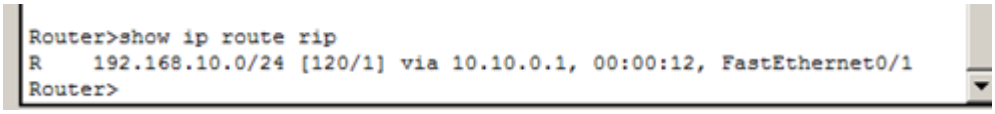


Рисунок 8.5. Таблица маршрутизации R1

Данная таблица показывает, что к сети 192.168.10.0 есть только один маршрут: через R1(сеть 10.10.0.1).

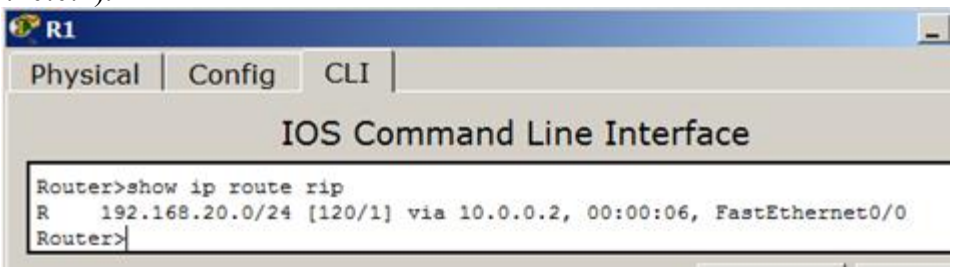


Рисунок 8.6. Таблицы маршрутизации R2

Данная таблица показывает, что к сети 192.168.20.0 есть только один маршрут: через R2 (сеть 10.10.0.2).

Проверка связи между PC1 и PC2

Проверим, что маршрутизация производится верно (Рисунок 8.7).

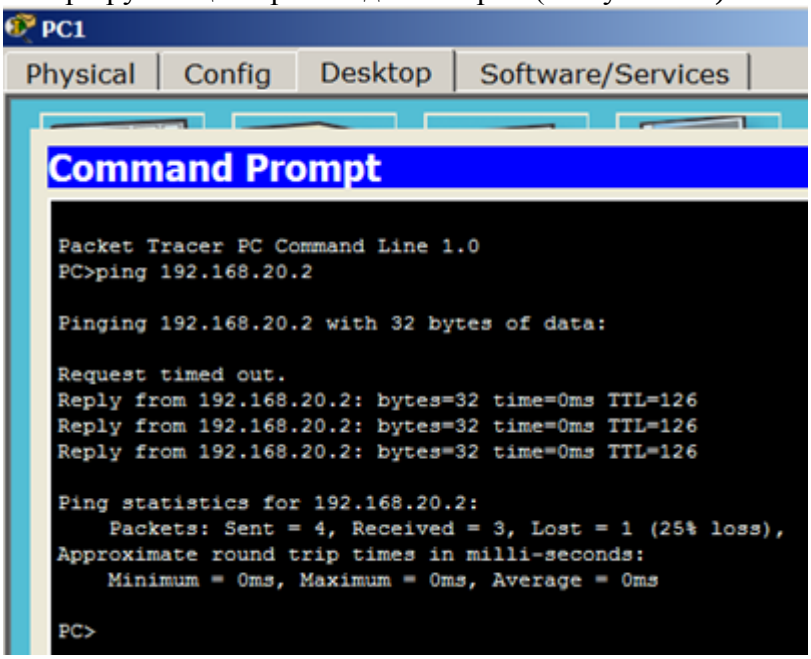


Рисунок 8.7. Пинг с PC1 на PC2

ПРАКТИЧЕСКАЯ РАБОТА № 8.2

Конфигурирование протокола RIP версии 2 для сети из четырех устройств

Время работы: 2 часа

1. Цель работы: Научится работать с программой Cisco Packet Tracer (CPT)

2. Технические средства

2.1 Оборудование: компьютер

2.2 Программное обеспечение: Cisco Packet Tracer, MS Word.

На Рисунок 8.8 представлена сеть, на примере которой мы сконфигурируем протокол маршрутизации RIP v2.

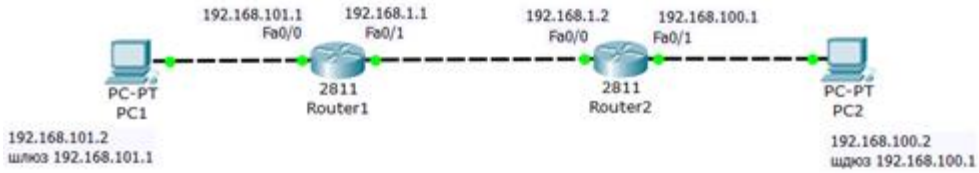


Рисунок 8.8. Сеть для конфигурации протоколов маршрутизации

Сначала сконфигурируем R1 (Рисунок 8.9).

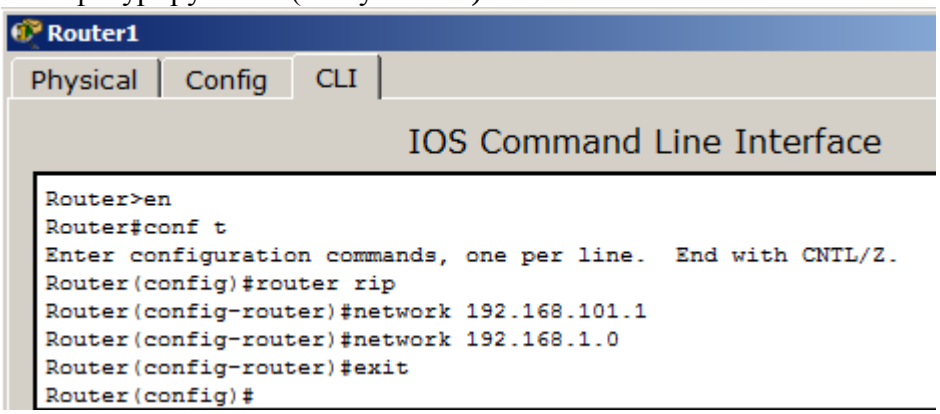


Рисунок 8.9. Настройка RIP на R1

Смотрим результат на вкладке Config (Рисунок 8.10).

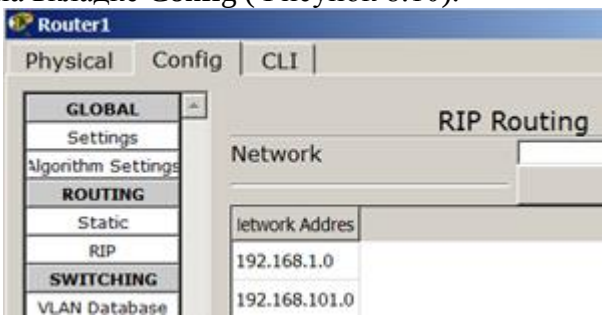


Рисунок 8.10. Окно R1,вкладка Config

Конфигурируем R2 (Рисунок 8.11).

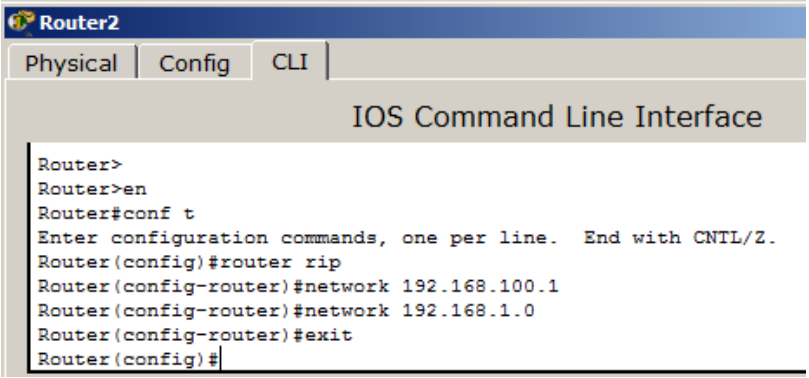


Рисунок 8.11. Настройка RIP на R2

Наблюдаем результат (Рисунок 8.12).

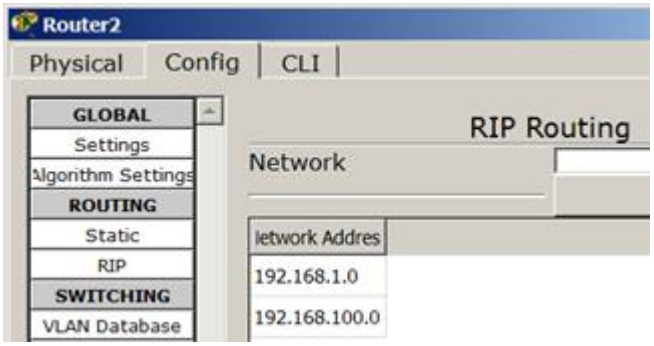


Рисунок 8.12. Окно R2, вкладка Config

Проверяем доступность ПК из разных сетей (Рисунок 8.13).

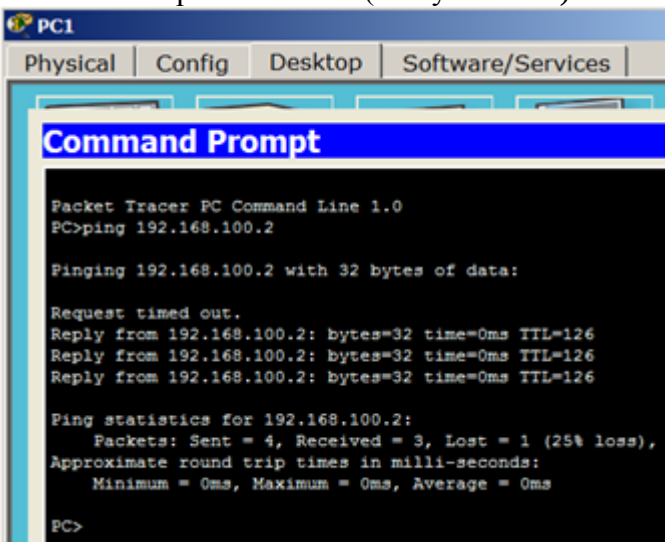


Рисунок 8.13. Результат маршрутизации по протоколу RIP

ПРАКТИЧЕСКАЯ РАБОТА № 8.3

Конфигурирование протокола EIGRP

Время работы: 2 часа

1. Цель работы: Научится работать с программой Cisco Packet Tracer (CPT)
2. Технические средства

2.1 Оборудование: компьютер

2.2 Программное обеспечение: Cisco Packet Tracer, MS Word.

Протокол маршрутизации EIGRP

Протокол EIGRP более прост в реализации и менее требователен к вычислительным ресурсам маршрутизатора, чем протокол OSPF. Также EIGRP имеет более продвинутый алгоритм вычисления метрики. В формуле вычисления метрики есть возможность учитывать загруженность и надежность интерфейсов на пути пакета. Недостатком протокола EIGRP является его ограниченность в его использовании только на оборудовании компании Cisco.

Схема сети изображена на Рисунок 8.14.

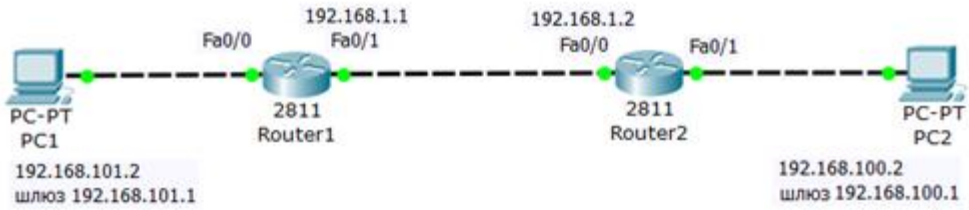


Рисунок 8.14. Схема для конфигурации протокола EIGRP

Настройка протокола EIGRP очень похожа на настройку протокола RIP.

Программирование R1

Конфигурируем R1 (Рисунок 8.15).

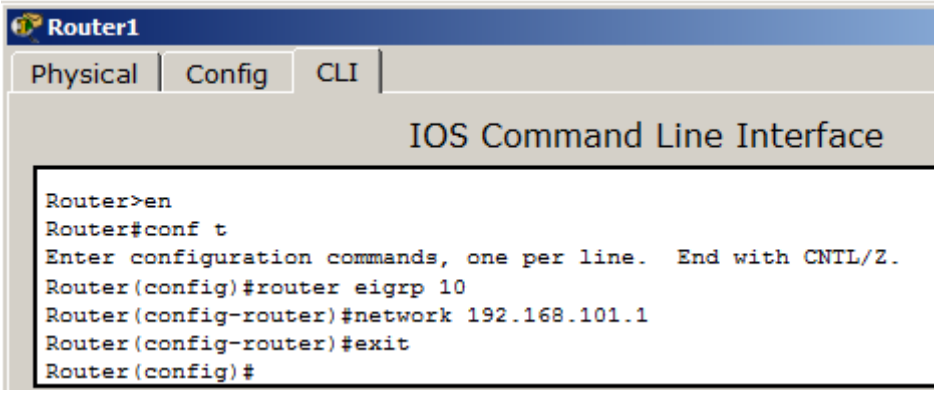


Рисунок 8.15. Конфигурирование R1

Программирование R2

Конфигурируем R2 (Рисунок 8.16).

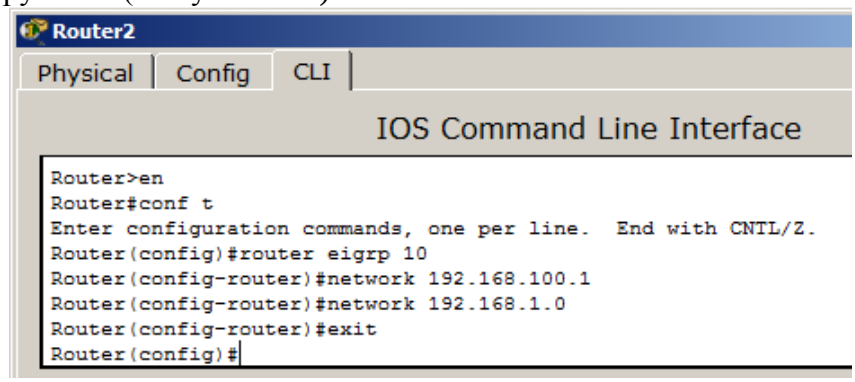


Рисунок 8.16. Конфигурирование R2

Проверка работы сети

Проверяем работу маршрутизаторов (Рисунок 8.17).

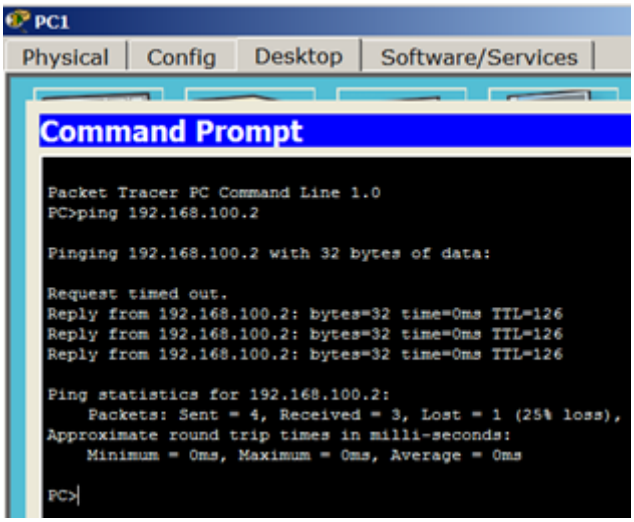


Рисунок 8.17. Результат проверки работоспособности сети

ПРАКТИЧЕСКАЯ РАБОТА № 8.4

Конфигурирования протокола OSPF для 4-х устройств

Время работы: 2 часа

1. Цель работы: Научится работать с программой Cisco Packet Tracer (CPT)

2. Технические средства

2.1 Оборудование: компьютер

2.2 Программное обеспечение: Cisco Packet Tracer, MS Word.

Протокол OSPF

Алгоритм работы протокола динамической маршрутизации OSPF основан на использовании всеми маршрутизаторами единой базы данных, описывающей, с какими сетями связан каждый маршрутизатор. Описывая каждую связь, маршрутизаторы связывают с ней метрику – значение, характеризующее "качество" канала связи. Это позволяет маршрутизаторам OSPF (в отличие от RIP, где все каналы равнозначны) учитывать реальную пропускную способность канала и выявлять наилучшие маршруты. Важной особенностью протокола OSPF является то, что используется групповая, а не широковещательная рассылка (как в RIP), то есть, нагрузка каналов меньше.

OSPF (Open Shortest Path First) — протокол динамической маршрутизации, основанный на технологии отслеживания состояния канала link-state (LSA). Основан на алгоритме для поиска кратчайшего пути. Отслеживание состояния канала требует отправки объявлений о состоянии канала (LSA) на активные интерфейсы всех доступных маршрутизаторов зоны. В этих объявлениях содержится описание всех каналов маршрутизатора и стоимость каждого канала. LSA сообщения отправляются, только если произошли какие-либо изменения в сети, но раз в 30 минут LSA сообщения отправляются в принудительном порядке. Протокол реализует деление автономной системы на зоны (areas). Использование зон позволяет снизить нагрузку на сеть и процессоры маршрутизаторов и уменьшить размер таблиц маршрутизации.

Описание работы протокола:

Все маршрутизаторы обмениваются специальными Hello-пакетами через все интерфейсы, на которых активирован протокол OSPF. Таким образом, определяются маршрутизаторы-соседи, разделяющие общий канал передачи данных. В дальнейшем hello-пакеты посылаются с интервалом раз в 30 секунд. Маршрутизаторы пытаются перейти в состояние соседства со своими соседями. Переход в данное состояние определяется типом маршрутизаторов и типом сети, по которой происходит обмен hello-пакетами, по зонному признаку. Пара маршрутизаторов в состоянии соседства синхронизирует между собой базу данных состояния каналов. Каждый маршрутизатор посылает объявление о состоянии канала своим соседям, а каждый получивший такое объявление записывает информацию в базу данных состояния каналов и рассылает копию объявления другим своим соседям. При рассылке объявлений по зоне, все маршрутизаторы строят идентичную базу данных состояния каналов. Каждый маршрутизатор использует алгоритм SPF для вычисления графа (дерева кратчайшего пути) без петель. Каждый маршрутизатор строит собственную маршрутизацию, основываясь на построенном дереве кратчайшего пути.

Прямая и обратная маска

В оборудовании Cisco иногда приходится использовать обратную маску, то есть не привычную нам 255.255.255.0 (Subnet mask — прямая маска), а 0.0.0.255 (Wildcard mask — обратная маска). Обратная маска используется в листах допуска (access list) и при описании сетей в протоколе OSPF. Прямая маска используется во всех остальных случаях. Отличие масок заключается также в том, что прямая маска оперирует сетями, а обратная — хостами. С помощью обратной маски вы можете, например, выделить во всех подсетях хосты с конкретным адресом и разрешить им доступ в Интернет. Так, как чаше всего в локальных сетях используют адреса типа 192.168.1.0 с маской 255.255.255.0, то самая распространенная Wildcard mask (шаблонная маска или обратная маска, или инверсная маска) - маска 0.0.0.255.

Новый термин

Шаблонная маска (wildcard mask) — маска, указывающая на количество хостов сети. Является дополнением для маски подсети. Вычисляется по формуле для каждого из октетов маски подсети как 255-маска_подсети. Например, для сети 192.168.1.0 и маской подсети 255.255.255.242 шаблонная маска будет выглядеть как 0.0.0.13. Шаблонная маска используется в настройке некоторых протоколов маршрутизации, а также является удобным параметром ограничений в списках доступа.

Расчёт Wildcard mask

Существует связь, между обратной и прямой маской: в сумме эти маски по каждому разряду должны составлять 255.

Пусть наша сеть 192.168.32.0 /28. Рассчитает wildcard mask: префикс /28 это 255.255.255.240 или 11111111.11111111.11111111.11110000.

Для wildcard mask нам нужны только нули, то есть, 11110000 переводим в десятичное число и считаем: 128/64/32/16/8/4/2/1 это будет 8+4+2+1=15, т.е. наша wildcard mask будет равна 0.0.0.15.

Самостоятельно

Дана прямая маска 255.255.255.248. Выполните расчет и докажите, что обратная равна 0.0.0.7.

Соберите схему, изображенную на Рисунок 8.18.

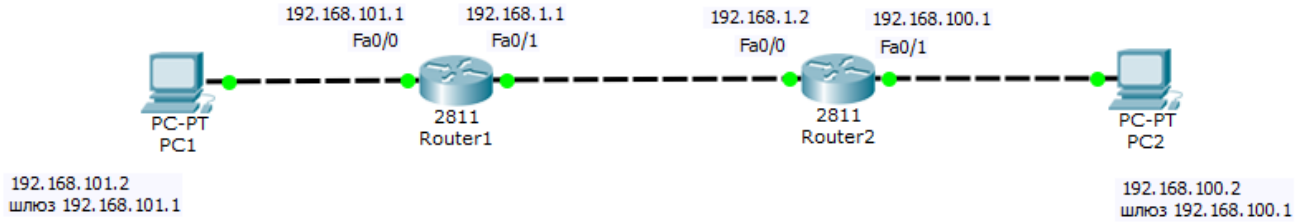


Рисунок 8.18. Схема для конфигурации протокола OSPF

Настройка роутеров

Выполним конфигурирование R1 (Рисунок 8.19).

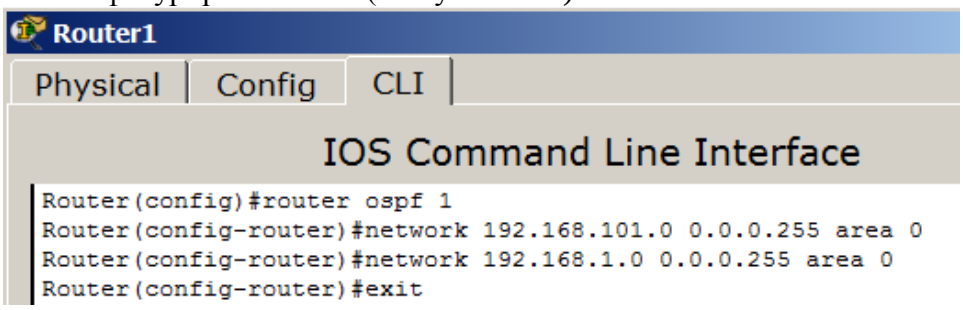


Рисунок 8.19. Настройка R1

Теперь выполним настройки R2 (Рисунок 8.20).

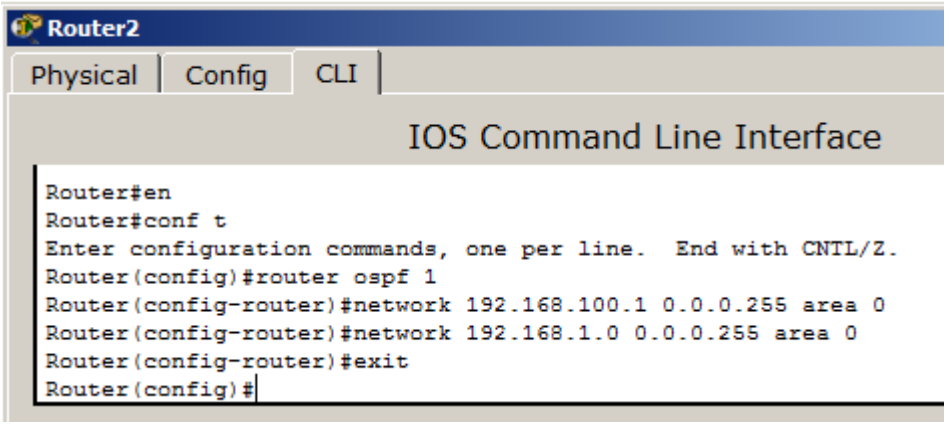


Рисунок 8.20. Настройка R2

Совет

Если вам потребуется в CPT сбросить настройки роутера, то следует выключить его тумблер питания, а затем снова включить.

Проверка результата

Для проверки маршрутизации пропингуем ПК из разных сетей (Рисунок 8.21).

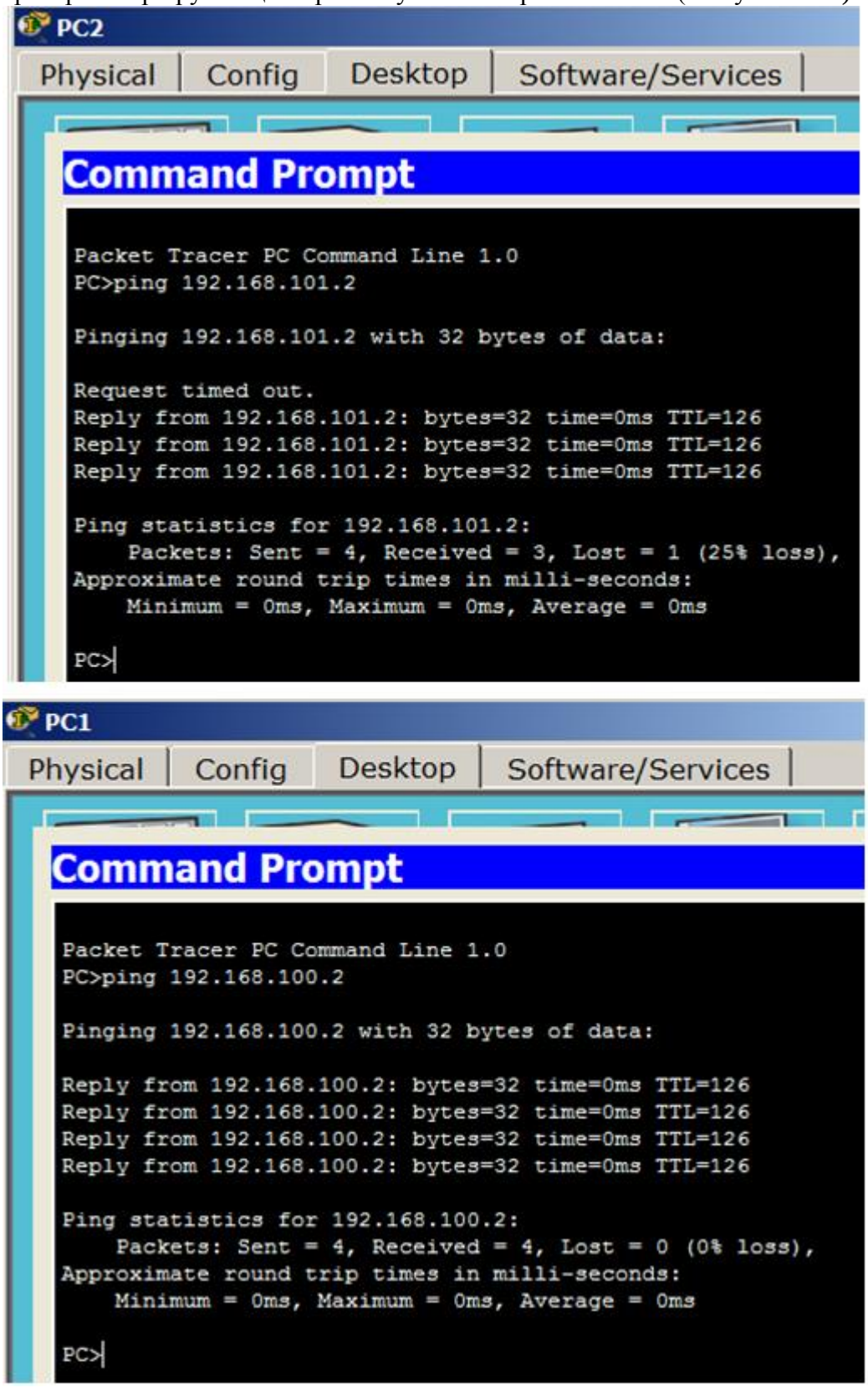


Рисунок 8.21. Результат проверки работоспособности OSPF

.

ПРАКТИЧЕСКАЯ РАБОТА № 8.5

Настройка маршрутизации по протоколу OSPF для 6 устройств

Время работы: 2 часа

1. Цель работы: Научится работать с программой Cisco Packet Tracer (CPT)

2. Технические средства

2.1 Оборудование: компьютер

2.2 Программное обеспечение: Cisco Packet Tracer, MS Word.

Постройте следующую схему (Рисунок 8.22).

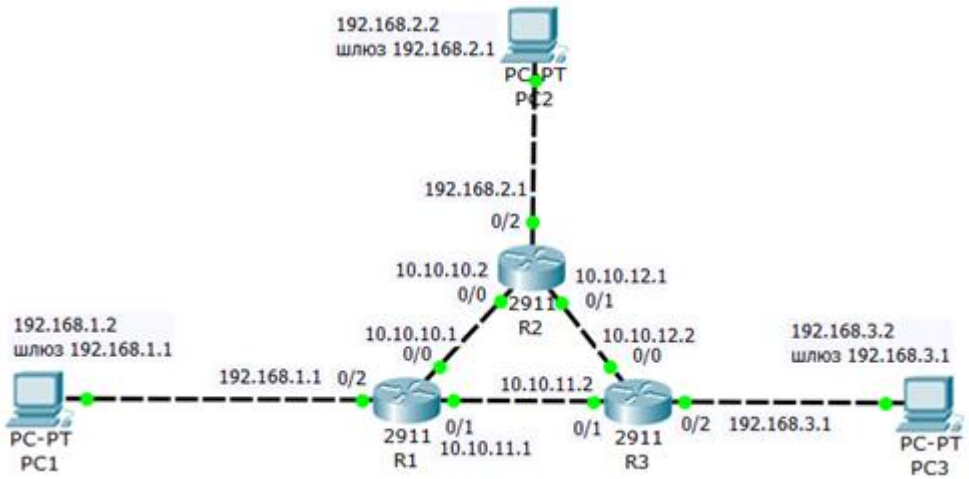


Рисунок 8.22. Начальная схема сети для нашей работы

Цель работы – настроить маршрутизацию в данной сети по протоколу OSPF.

Настроим loopback интерфейс на R1

На R1 настроим программный loopback интерфейс — алгоритм, который направляет полученный сигнал (или данные) обратно отправителю (Рисунок 8.23).

Примечание

IPv4-адрес, назначенный loopback-интерфейсу, может быть необходим для процессов маршрутизатора, в которых используется IPv4-адрес интерфейса в целях идентификации. Один из таких процессов — алгоритм кратчайшего пути (OSPF). При включении интерфейса loopback для идентификации маршрутизатор будет использовать всегда доступный адрес интерфейса loopback, а не IP-адрес, назначенный физическому порту, работа которого может быть нарушена. На маршрутизаторе можно активировать несколько интерфейсов loopback. IPv4-адрес для каждого интерфейса loopback должен быть уникальным и не должен быть задействован другим интерфейсом.

Рисунок 8.23. Настраиваем интерфейс loopback на R1

Настраиваем протокол OSPF на R1

Включаем OSPF на R1, все маршрутизаторы должны быть в одной зоне area 0 (Рисунок 8.24).

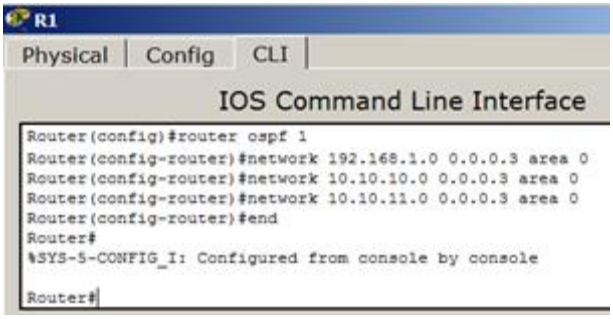


Рисунок 8.24. Включаем протокол OSPF на R1

Подводим курсор мыши к R1 и наблюдаем результат наших настроек (Рисунок 8.25).

Port	Link	VLAN	IP Address
GigabitEthernet0/0	Up	--	10.10.10.1/30
GigabitEthernet0/1	Up	--	10.10.11.1/30
GigabitEthernet0/2	Up	--	192.168.1.1/24
Loopback0	Up	--	192.168.100.1/32

Рисунок 8.25. Маршрутизатор R1 настроен

Примечание

Обратите внимание, что физически порта 192.168.100.1 нет, он существует только логически (программно).

Настроим loopback интерфейс на R2

На R2 настроим программный loopback интерфейс по аналогии с R1 (Рисунок 8.26).

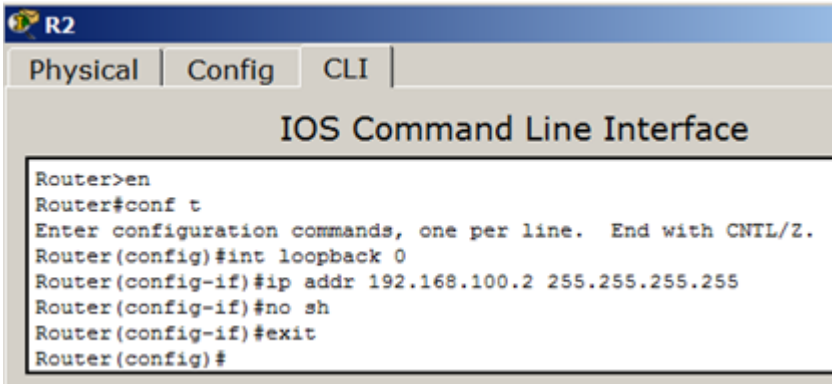


Рисунок 8.26. Настраиваем логический интерфейс loopback на R2

Настраиваем OSPF на R2

Включаем протокол OSPF на R2, все маршрутизаторы должны быть в одной зоне area 0 (Рисунок 8.27).

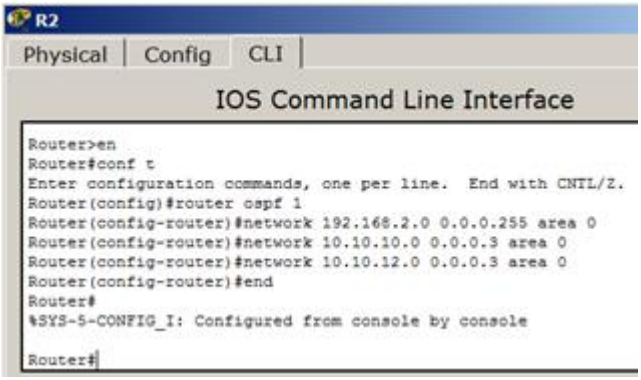


Рисунок 8.27. Включаем протокол OSPF на R2

Подводим курсор мыши к R2 и наблюдаем результат наших настроек (Рисунок 8.28).

Port	Link	VLAN	IP Address
GigabitEthernet0/0	Up	--	10.10.10.2/30
GigabitEthernet0/1	Up	--	10.10.12.1/30
GigabitEthernet0/2	Up	--	192.168.2.1/24
Loopback0	Up	--	192.168.100.2/32

Рисунок 8.28. Маршрутизатор R2 настроен

Настраиваем loopback интерфейс на R3

Делаем все аналогично (Рисунок 8.29).

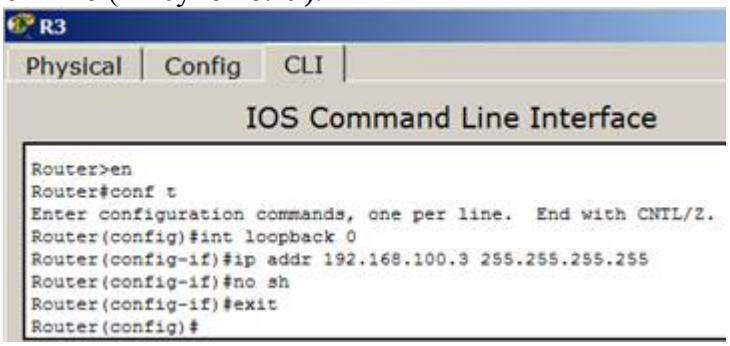


Рисунок 8.29. Настраиваем логический интерфейс loopback на R3

Настраиваем протокол OSPF на R3

Здесь делаем все, как раньше (Рисунок 8.30).

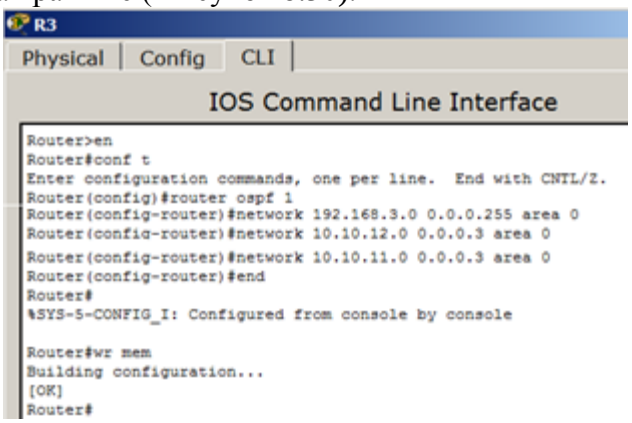


Рисунок 8.30. Включаем протокол OSPF на R2

Проверяем результат (Рисунок 8.31).

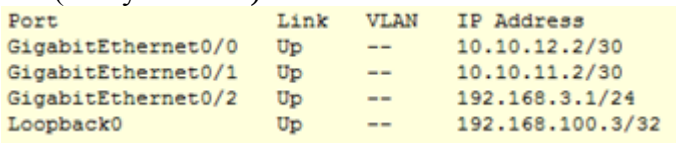


Рисунок 8.31. Маршрутизатор R3 настроен

Проверяем работу сети

Убеждаемся, что роутер R3 видит R2 и R1 (Рисунок 8.32).

Рисунок 8.32. Роутер R3 видит своих соседей

Теперь посмотрим таблицу маршрутизации для R3 (Рисунок 8.33).

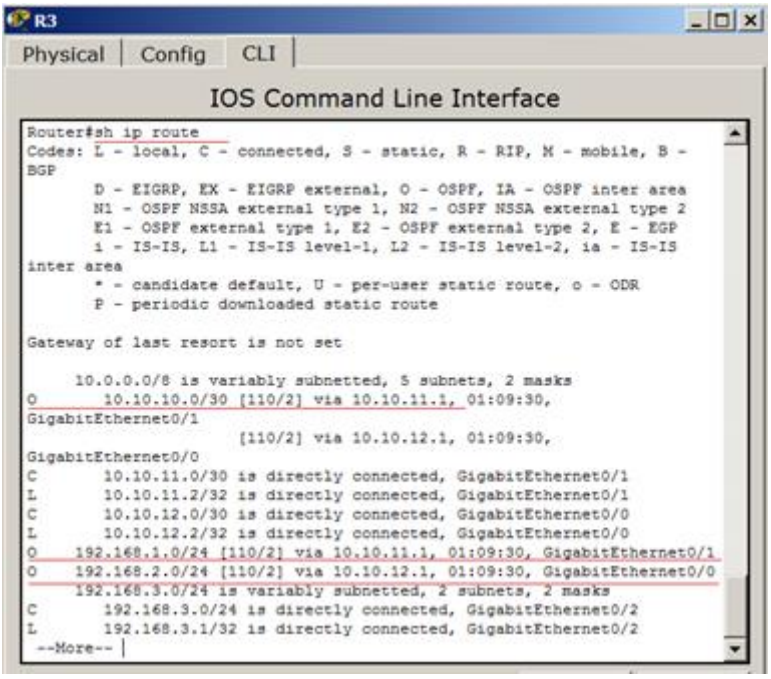


Рисунок 8.33. Таблица маршрутизации для R3

Примечание

В этой таблице запись с буквой "O" говорит о том, что данный маршрут прописан протоколом OSPF. Мы видим, что сеть 192.168.1.0 доступна для R3 через адрес 10.10.11.1 (это порт gig0/1 маршрутизатора R1). Аналогично, сеть 192.168.2.0 доступна для R3 через адрес 10.10.12.1 (это порт gig0/1 маршрутизатора R2).

Теперь проверяем доступность разных сетей (Рисунок 8.34).

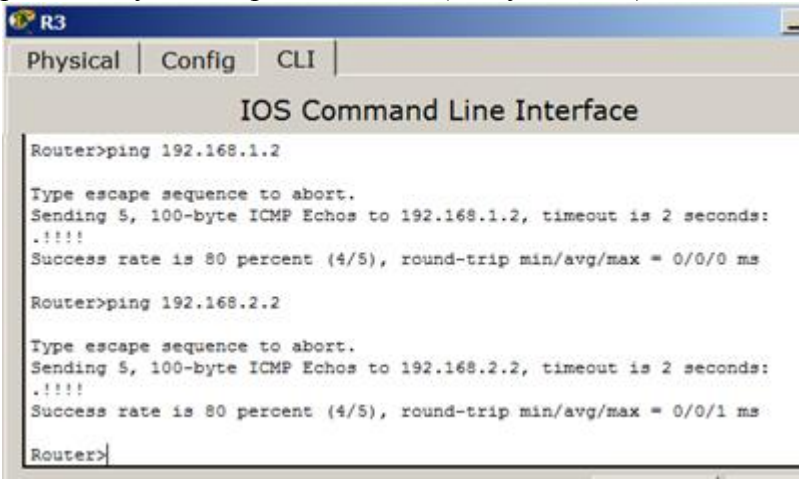


Рисунок 8.34. Сети 192.168.1.0 и 192.168.2.0 доступны

ПРАКТИЧЕСКАЯ РАБОТА № 9.1

Создание стандартного списка доступа

Время работы: 2 часа

1. Цель работы: Научится работать с программой Cisco Packet Tracer (CPT)

2. Технические средства

2.1 Оборудование: компьютер

2.2 Программное обеспечение: Cisco Packet Tracer, MS Word.

Списки доступа (access-lists) используются в целом ряде случаев и являются механизмом задания условий, которые роутер проверяет перед выполнением каких-либо действий. Маршрутизатор проверяет каждый пакет и на основании вышеперечисленных критериев, указанных в ACL определяет, что нужно сделать с пакетом, пропустить или отбросить. Типичными критериями являются адреса отправителя и получателя пакета, тип протокола. Каждый критерий в списке доступа записывается отдельной строкой. Список доступа в целом представляет собой набор строк с критериями, имеющих один и тот же номер (или имя). Порядок задания критериев в списке существенен. Проверка пакета на соответствие списку производится последовательным применением критериев из данного списка (в том порядке, в котором они были введены). Пакет, который не соответствует ни одному из введенных критериев будет отвергнут. Для каждого протокола на интерфейс может быть назначен только один список доступа. Как пример ниже приведена таблица списка управления доступом по умолчанию:

№ правила	Подсеть	Конечная точка	Разрешить или запретить
100	0.0.0.0/0	3389	Разрешить

Без ACL - по умолчанию при создании конечной точки ей все разрешено.

Разрешить - при добавлении одного или нескольких диапазонов "разрешения" все остальные диапазоны по умолчанию запрещаются. Только пакеты из разрешенного диапазона IP-адресов смогут достичь конечной точки виртуальной машины.

Запретить - при добавлении одного или нескольких диапазонов "запретить" все другие диапазоны трафика по умолчанию разрешаются.

Сочетание разрешения и запрета - можно использовать сочетание правил "разрешить" и "запретить", чтобы указать вложенный разрешенный или запрещенный диапазон IP-адресов.

Рассмотрим два примера стандартных списков:

access-list 1 permithost 10.0.0.10 - разрешаем прохождение трафика от узла 10.0.0.10.

access-list 2 deny 10.0.1.0 0.0.0.255 - запрещаем прохождение пакетов из подсети 10.0.1.0/24.

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

На Рисунок 9.1 показаны две подсети: 192.168.0.0 и 10.0.0.0.

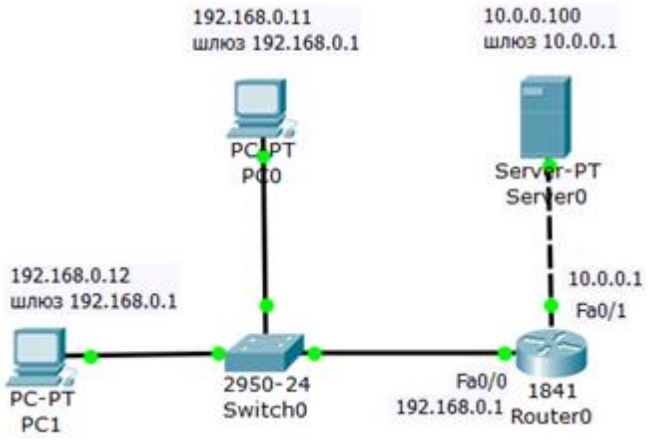


Рисунок 9.1. Схема сети

Постановка задачи

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

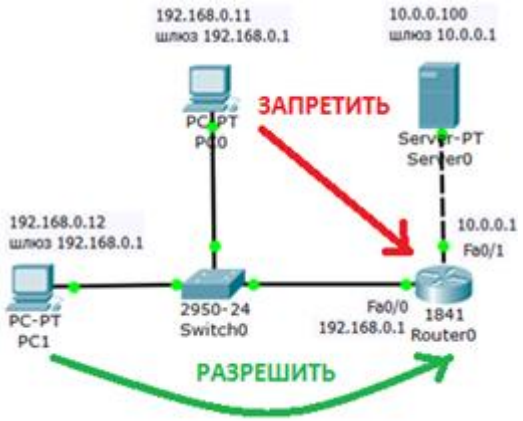


Рисунок 9.2. Постановка задачи

Соберем данную схему и настроим ее. Настройку PC0 и PC1 выполните самостоятельно.

Настройка R0

Интерфейс 0/0 маршрутизатора1841 настроим на адрес 192.168.0.1 и включим следующими командами:

Router>en

Router#conf t

Router (config)#int fa0/0

Router (config-if)#ip addr 192.168.0.1 255.255.255.0

Router (config-if)#no shut

Router (config-if)#exit

Второй интерфейс маршрутизатора (порт 0/1) настроим на адресом 10.0.0.1 и так же включим:

Router (config)#intfa0/1

Router (config-if)#ip addr 10.0.0.1 255.255.255.0

Router (config-if)#no shut

Настройка сервера

Настройки сервера приведены на Рисунок 9.3.

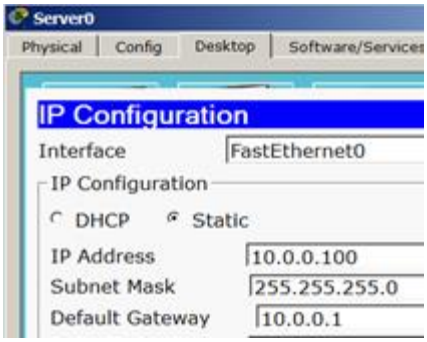


Рисунок 9.3. Конфигурирование S0

Диагностика сети

Проверяем связь ПК из разных сетей (Рисунок 9.4).

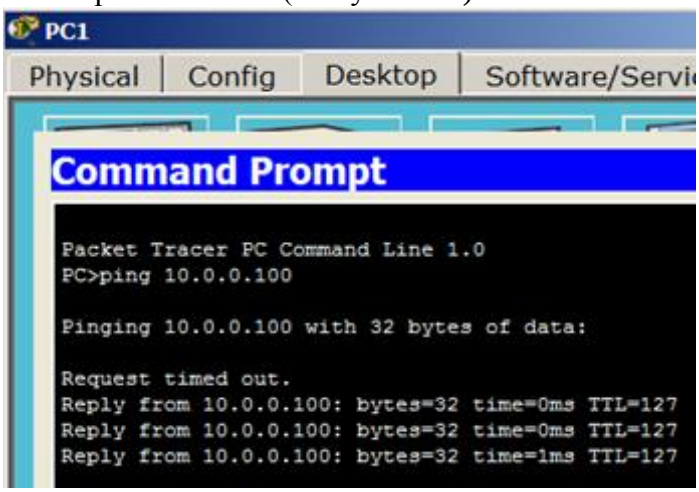


Рисунок 9.4. ПК из разных сетей могут общаться

Приступаем к решению задачи

Правило запрета и разрешения доступа будем составлять с использованием стандартных списков доступа (ACL). Пока не задан список доступа на интерфейсе всё разрешено (permit). Но, стоит создать список, сразу действует механизм "Всё, что не разрешено, то запрещено". Поэтому нет необходимости что-то запрещать (deny) – указываем что разрешено, а "остальным – запретить" подразумевается автоматически. По условиям задачи нам нужно на R0 пропустить пакеты с узла 192.168.0.12 на сервер (Рисунок 9.5).

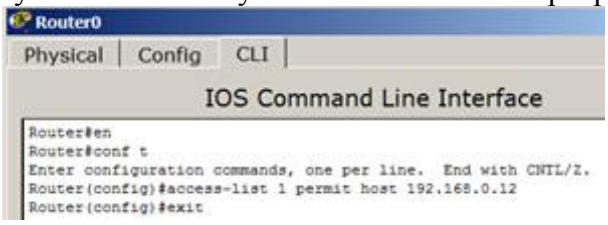


Рисунок 9.5. Создаем на R0 разрешающий ACL

Применяется данное правило на интерфейс в зависимости от направления (PC1 расположен со стороны порта Fa0/0) – Рисунок 9.6. Эта настройка означает, что список доступа (правило с номером 1) будет действовать на интерфейсе fa0/0 на входящем (in) от PC1 направлении.

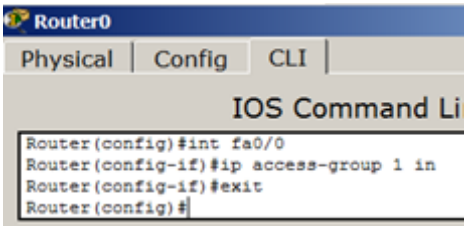


Рисунок 9.6. Применяем правило к порту Fa0/0

Примечание

Входящий трафик (in) — этот тот, который приходит на интерфейс извне. Исходящий (out) — тот, который отправляется с интерфейса вовне. Список доступа вы можете применить либо на входящий трафик, тогда неугодные пакеты не будут даже попадать на маршрутизатор и соответственно, дальше в сеть, либо на исходящий, тогда пакеты приходят на маршрутизатор, обрабатываются им, доходят до целевого интерфейса и только на нём обрабатываются. Как правило, списки применяют на входящий трафик (in).

Проверяем связь ПК с сервером (Рисунок 9.7 и Рисунок 9.8).

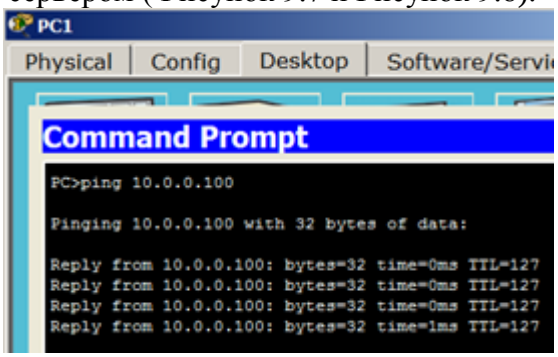


Рисунок 9.7. Для PC1 сервер доступен

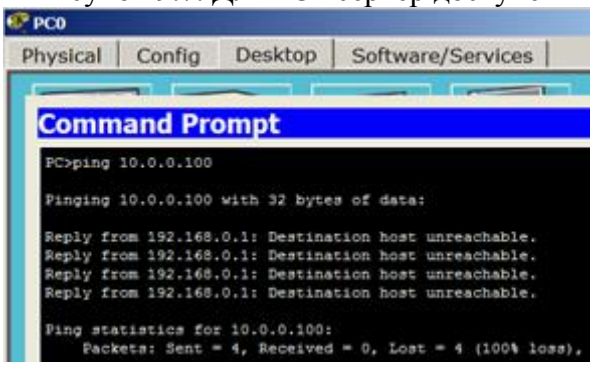


Рисунок 9.8. Для PC0 сервер не доступен

Давайте посмотрим ACL (Рисунок 9.9).

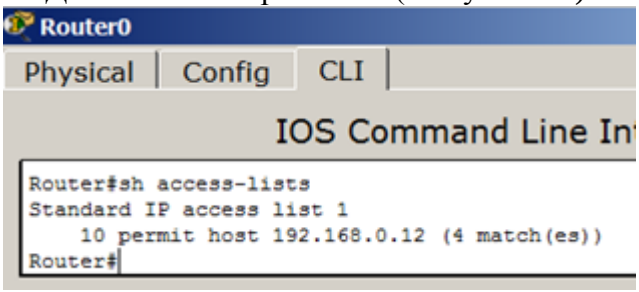


Рисунок 9.9. Узел 192.168.0.12 разрешен

Примечание

Теперь, предположим, нужно добавить новый узел, например, PC2 с адресом 192.168.0.13 в раздел "разрешённых". Пишем команду Router (config)#access-list 1 permit host 192.168.0.13. Теперь адреса 192.168.0.12 и 192.168.0.13 могут общаться с сервером, в 192.168.0.11 – нет. А для отмены какого-либо правила – повторяем его с приставкой "no". Тогда это правило исключается из конфигурации. Например, если выполнить команду Router (config-if)#no ip access-group 1 in, то ACL будет отменен и снова все ПК могут пинговать сервер.

ПРАКТИЧЕСКАЯ РАБОТА № 9.2

Расширенные списки доступа ACL

Время работы: 2 часа

1. Цель работы: Научится работать с программой Cisco Packet Tracer (CPT)
2. Технические средства

2.1 Оборудование: компьютер

2.2 Программное обеспечение: Cisco Packet Tracer, MS Word.

Расширенные списки доступа ACL

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

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

Соберите схему сети, показанную на Рисунок 9.10.

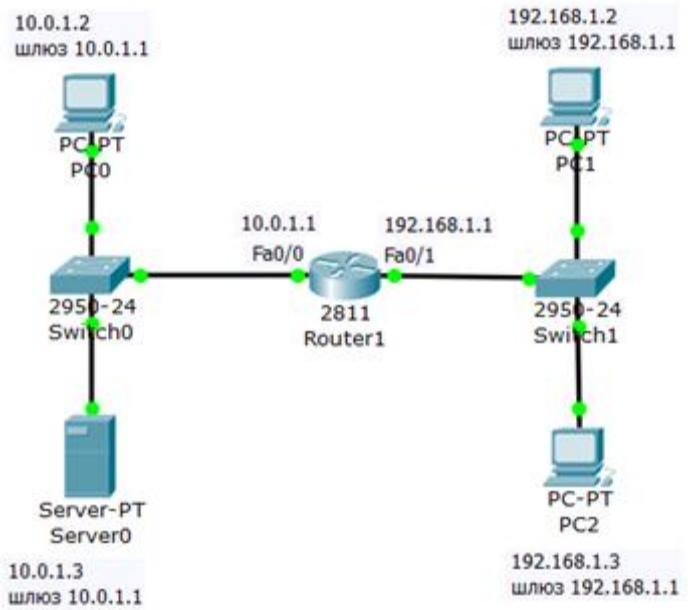


Рисунок 9.10. Схема сети

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

Создаем расширенные списки доступа и запрещаем FTP трафик

Постановка задачи графически изображена на Рисунок 9.11.

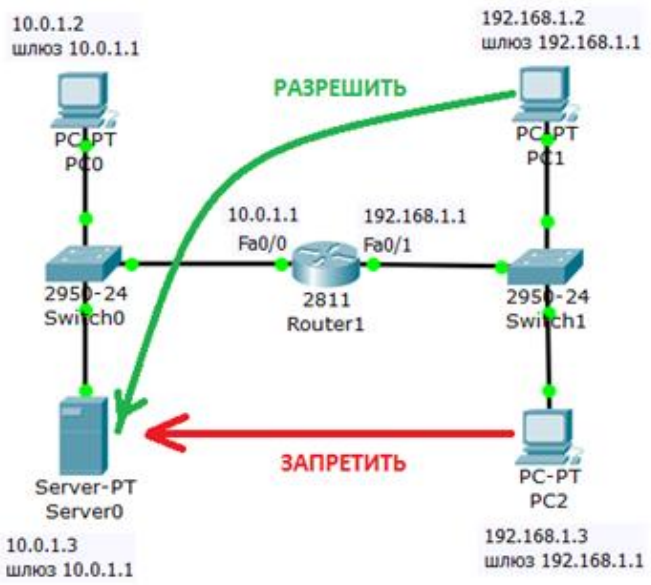


Рисунок 9.11. Стрелками показана цель нашей работы

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

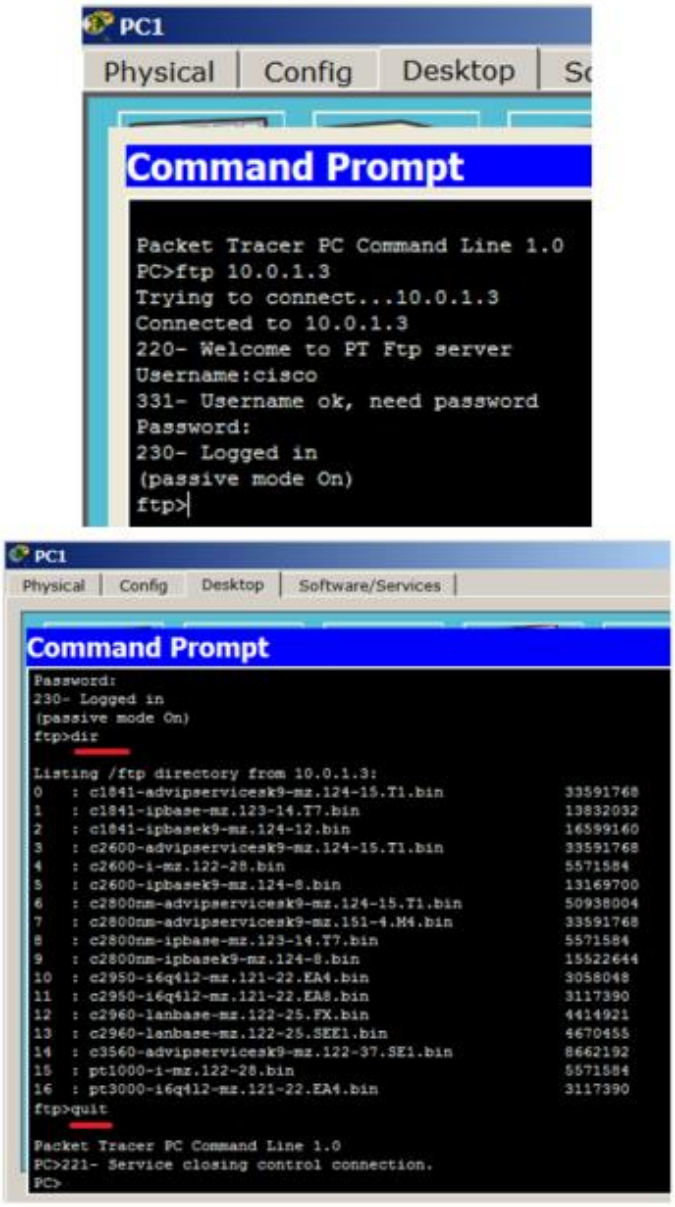


Рисунок 9.12. FTPсервер доступен

Примечание

При наборе пароля на экране ничего не отображается.

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

```
Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#ip access-list extended 101
Router(config-ext-nacl)#permit tcp 192.168.1.2 0.0.0.0 10.0.1.3 0.0.0.0 eq 21
Router(config-ext-nacl)#permit tcp 192.168.1.2 0.0.0.0 10.0.1.3 0.0.0.0 eq 20
Router(config-ext-nacl)#deny tcp 192.168.1.3 0.0.0.0 10.0.1.3 0.0.0.0 eq 21
Router(config-ext-nacl)#deny tcp 192.168.1.3 0.0.0.0. 10.0.1.3 0.0.0.0 eq 20
Router(config-ext-nacl)#deny tcp 192.168.1.3 0.0.0.0 10.0.1.3 0.0.0.0 eq 20
Router(config-ext-nacl)#
```

Рисунок 9.13. Составляем расширенные списки доступа

Совет

Набирайте команды аккуратно и внимательно: даже один лишний пробел может привести к ошибке при выполнении команды.

А теперь применяем наш список с номером 101 на вход (in) Fa0/1 потому, что трафик входит на этот порт роутера со стороны сети 192.168.1.0 (Рисунок 9.14).

```
Router(config-ext-nacl)#int fa0/1
Router(config-if)#ip access-group 101 in
Router(config-if)#exit
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console

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

Рисунок 9.14. Применяем правило с номером 101 к порту 0/1 роутера

Проверяем связь сервера с PC2 (Рисунок 9.15).

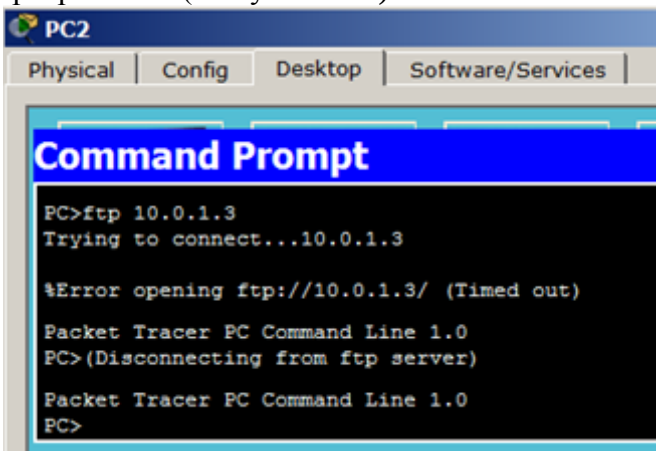


Рисунок 9.15. Для PC2 FTP сервер не доступен

Проверяем связь сервера с PC1 (Рисунок 9.16).

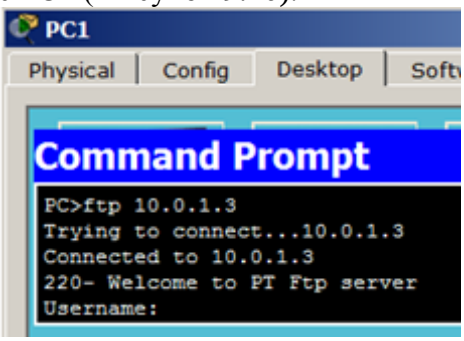


Рисунок 9.16. Для PC1 FTP сервер доступен

ПРАКТИЧЕСКАЯ РАБОТА № 9.3

Статическая трансляция адресов NAT

ремя работы: 2 часа

1. Цель работы: Научится работать с программой Cisco Packet Tracer (CPT)

2. Технические средства

2.1 Оборудование: компьютер

2.2 Программное обеспечение: Cisco Packet Tracer, MS Word.

Настройка статического NAT

NAT (Network Address Translation) — трансляция сетевых адресов, технология, которая позволяет преобразовывать (изменять) IP адреса и порты в сетевых пакетах. NAT используется чаще всего для осуществления доступа устройств из локальной сети предприятия в Интернет, либо наоборот для доступа из Интернет на какой-либо ресурс внутри сети. Локальная сеть предприятия строится на частных IP адресах:

10.0.0.0 — 10.255.255.255 (10.0.0.0/255.0.0.0 (/8))

172.16.0.0 — 172.31.255.255 (172.16.0.0/255.240.0.0 (/12))

192.168.0.0 — 192.168.255.255 (192.168.0.0/255.255.0.0 (/16))

Эти адреса не маршрутизируются в Интернете, и провайдеры должны отбрасывать пакеты с такими IP адресами отправителей или получателей. Для преобразования частных адресов в Глобальные (маршрутизируемые в Интернете) применяют NAT.

Новый термин

NAT — технология трансляции сетевых адресов, т.е. подмены адресов (или портов) в заголовке IP-пакета. Другими словами, пакет, проходя через маршрутизатор, может поменять свой адрес источника и/или назначения. Подобный механизм служит для обеспечения доступа из LAN, где используются частные IP-адреса, в Internet, где используются глобальные IP-адреса.

Существует три вида трансляции Static NAT, Dynamic NAT, Overloading (PAT).

Static NAT (статический NAT) осуществляет преобразование IP адреса один к одному, то есть сопоставляется один адрес из внутренней сети с одним адресом из внешней сети. Иными словами, при прохождении через маршрутизатор, адрес(а) меняются на строго заданный адрес, один-к-одному (Например, 10.1.1.5 всегда заменяется на 11.1.1.5 и обратно). Запись о такой трансляции хранится неограниченно долго, пока есть соответствующая строчка в конфигурации роутера.

Dynamic NAT (динамический NAT) производит преобразование внутреннего адреса/ов в один из группы внешних адресов. То есть, перед использованием динамической трансляции, нужно задать nat-пул внешних адресов. В этом случае при прохождении через маршрутизатор, новый адрес выбирается динамически из некоторого диапазона адресов, называемого пулом (pool). Запись о трансляции хранится некоторое время, чтобы ответные пакеты могли быть доставлены адресату. Если в течение некоторого времени трафик по этой трансляции отсутствует, трансляция удаляется и адрес возвращается в пул. Если требуется создать трансляцию, а свободных адресов в пуле нет, то пакет отбрасывается. Иными словами, хорошо бы, чтобы число внутренних адресов было ненамного больше числа адресов в пуле, иначе высока вероятность проблем с выходом в WAN.

- Overloading(или PAT) позволяет преобразовывать несколько внутренних адресов в один внешний. Для осуществления такой трансляции используются порты, поэтому такой NAT называют PAT (Port Address Translation). С помощью PAT можно преобразовывать внутренние адреса во внешний адрес, заданный через пул или через адрес на внешнем интерфейсе.

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

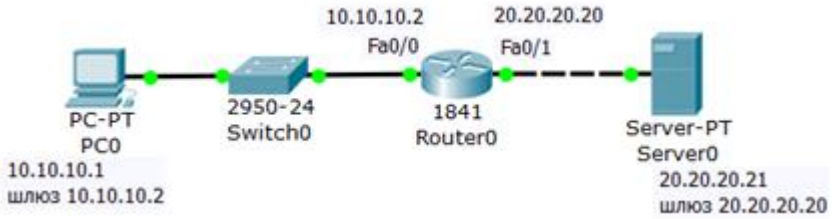


Рисунок 9.17. Схема сети

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

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

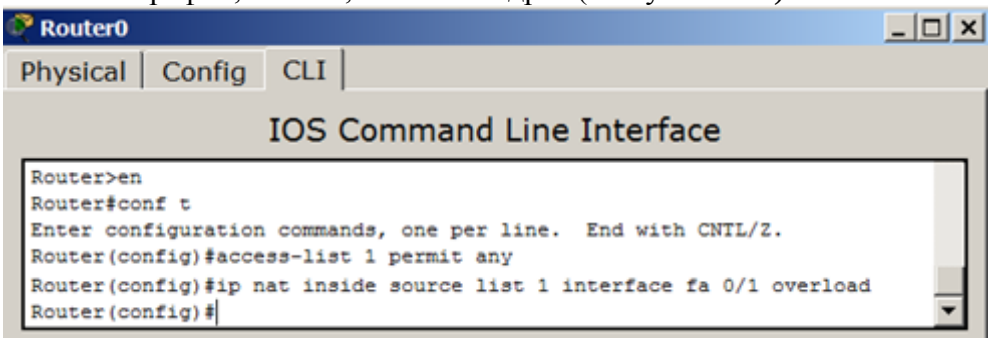


Рисунок 9.18. Составляем лист допуска

Создаём правило трансляции

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

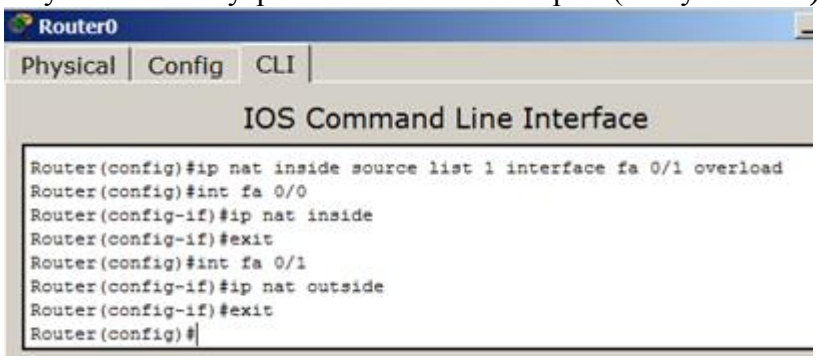


Рисунок 9.19. Для R0 назначаем внутренний и внешний порты

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

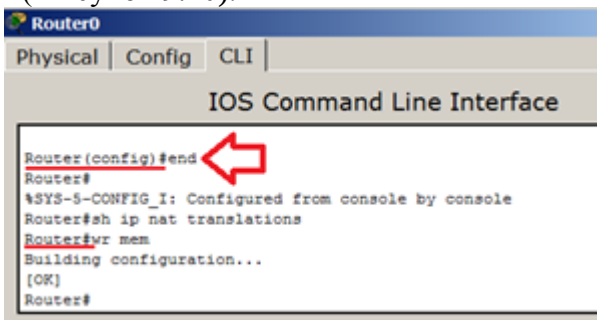


Рисунок 9.20. Сохраняем настройки в ОЗУ

Проверяем работу сети (просмотр состояния таблицы NAT)

С PC0 пингуем провайдера и убеждаемся, что PC1 и сервер могут общаться (Рисунок 9.21).

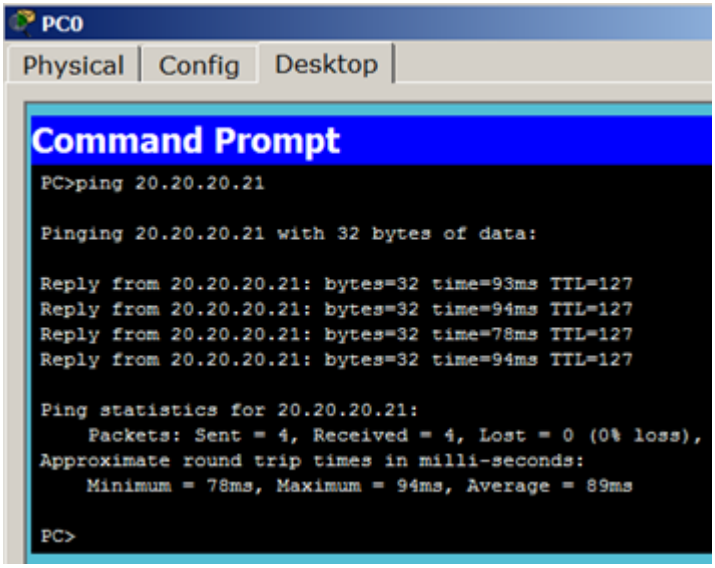


Рисунок 9.21. Из внутренней сети пингуем внешнюю сеть

Для просмотра состояния таблицы NAT, одновременно с пингом используйте команду Router#sh ip nat translations (я запустил пинг с машины 10.10.10.1, т.е., с PC1 на адрес 20.20.20.21, т.е., на S0) – Рисунок 9.22.

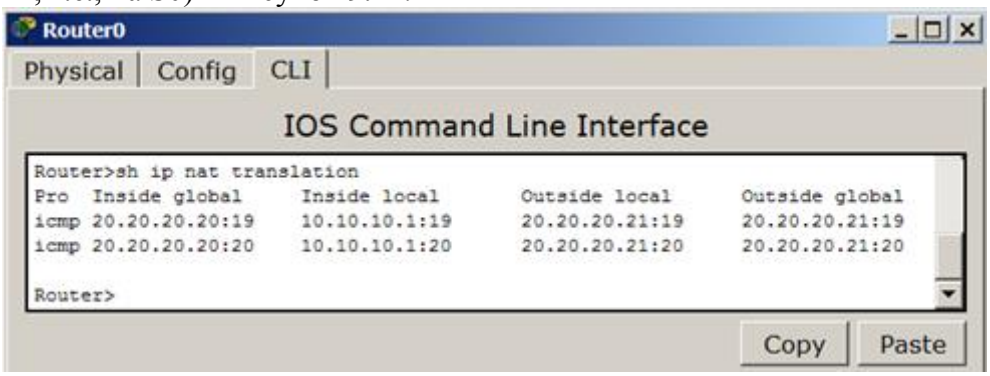


Рисунок 9.22. Вовремя пинга просматриваем состояние таблицы NAT

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

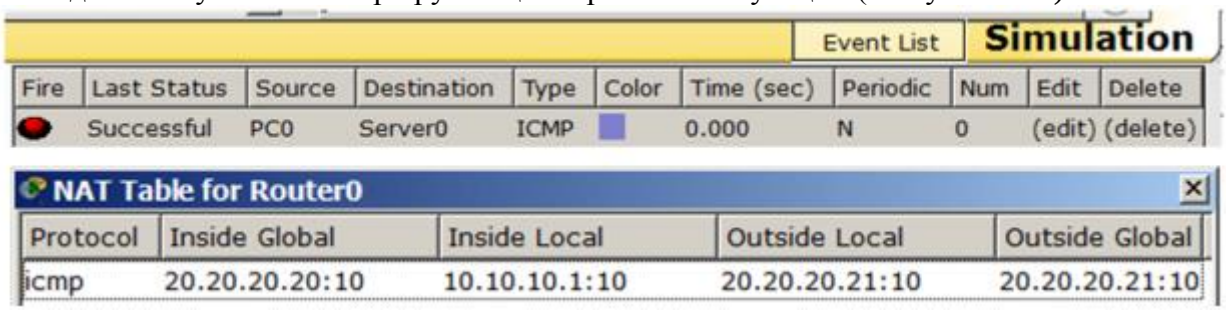


Рисунок 9.23. Связь PC0 и S0 работает

Задание

Если в схему добавить PC1 (Рисунок 9.24), то будет ли работать статический NAT между ним и S0?

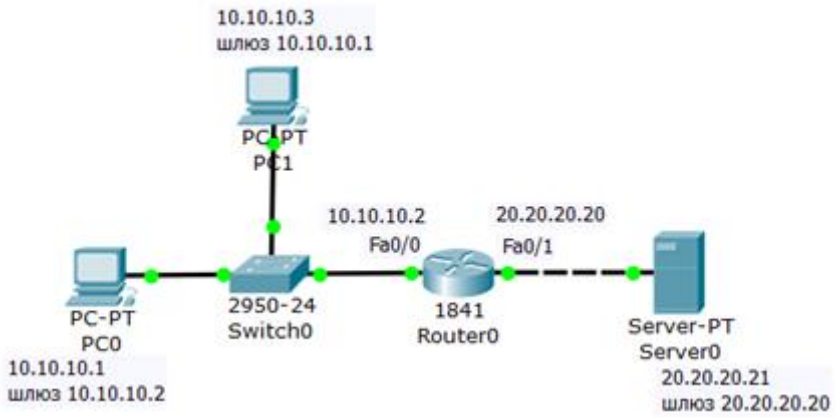


Рисунок 9.24. Задание для самостоятельной работы

ПРАКТИЧЕСКАЯ РАБОТА № 9.4

Настройка статического NAT

ремя работы: 2 часа

1. Цель работы: Научится работать с программой Cisco Packet Tracer (CPT)

2. Технические средства

2.1 Оборудование: компьютер

2.2 Программное обеспечение: Cisco Packet Tracer, MS Word.

Статический NAT - сопоставляет один NAT inside (внутренний=частный локальный ip-адрес) с одним NAT outside (глобальным=публичным внешним ip-адресом) – Рисунок 9.25. Здесь ISP (Internet Service Provider) - поставщик Интернет-услуг (Интернет-провайдер).

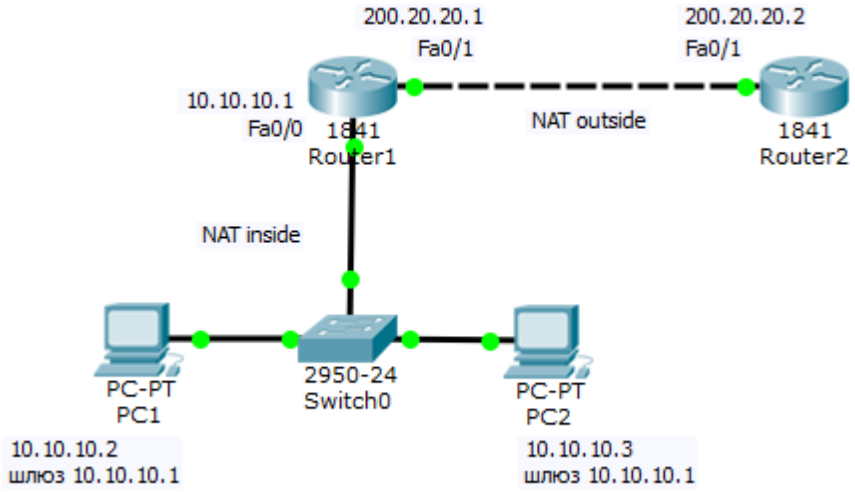


Рисунок 9.25. Схема сети

Алгоритм настройки R1

Ниже приведена последовательность команд конфигурирования маршрутизатора R1 по шагам.

Шаг 1. Настройка дефолта на R1

R1(config)# ip route 0.0.0.0 0.0.0.0 200.20.20.2

Шаг 2. Настройка внутреннего интерфейса в отношение NAT

R1(config)# interface fastethernet 0/0

R1(config-if)# ip nat inside

Шаг 3. Настройка внешнего интерфейса в отношение NAT

R1(config)# interface fastethernet 0/1

R1(config-if)# ip nat outside

Шаг 4. Настройка сопоставления ip-адресов.

R1(config)# ip nat inside source static 10.10.10.2 200.10.21.5

В результате этой команды ip-адресу 200.10.21.5 всегда будет соответствовать внутренний ip-адрес 10.10.10.2, т.е. если мы будем обращаться к адресу 200.10.21.5 то отвечать будет PC1.

Полный листинг команд приведен на Рисунок 9.26.

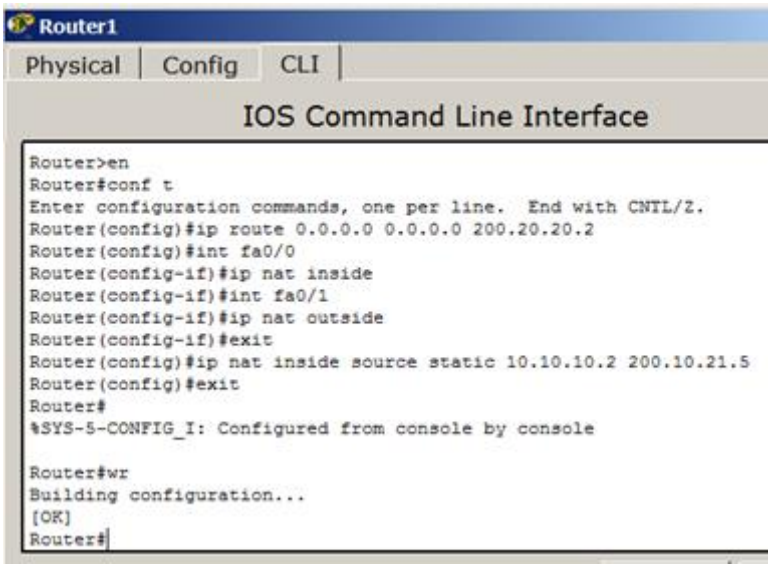


Рисунок 9.26. Полный листинг команд по настройке R1

Команды для проверки работы NAT

Проверим связь PC1 и R2 (Рисунок 9.27).

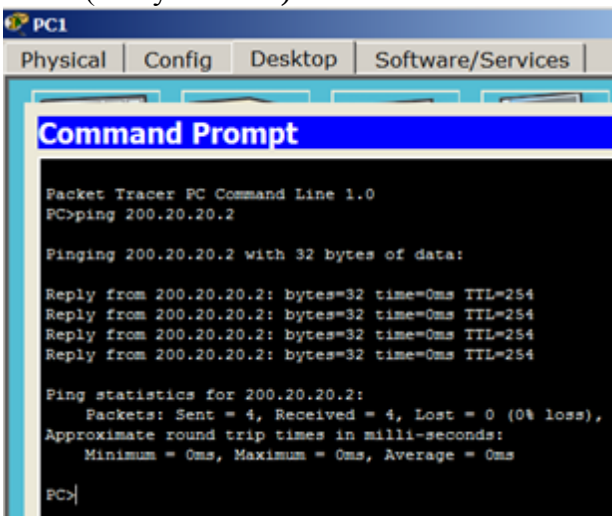


Рисунок 9.27. PC1 видит R2

Проверим, что R1 видит соседние сети (Рисунок 9.28).

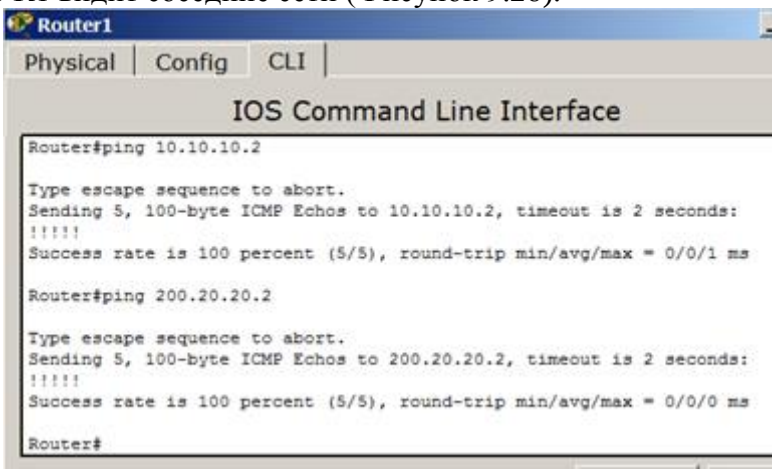


Рисунок 9.28. R1 видит PC1 и R2

Проверим механизм работы статического NAT: команда show ip nat translations выводит активные преобразования, а команда show ip nat statistics выводит статистику по NAT преобразованиям (Рисунок 9.29).

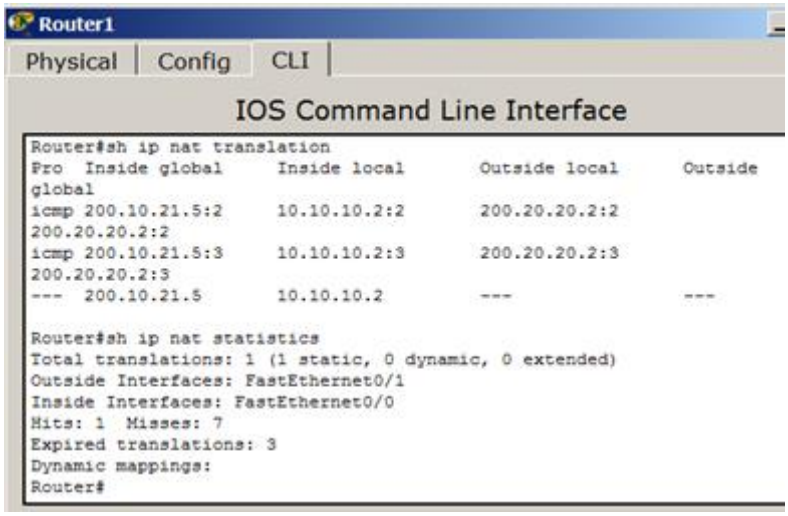


Рисунок 9.29. Проверка механизма работы статического NAT

Из иллюстрации видим, что глобальному ip-адресу 200.10.21.5 соответствует локальный ip-адрес 10.10.10.2,а также, какой интерфейс является внешним, а какой - внутренним.

ПРАКТИЧЕСКАЯ РАБОТА № 9.5

Динамическая трансляция адресов. Настройка динамического NAT

Время работы: 2 часа

1. Цель работы: Научится работать с программой Cisco Packet Tracer (CPT)

2. Технические средства

2.1 Оборудование: компьютер

2.2 Программное обеспечение: Cisco Packet Tracer, MS Word.

Динамический NAT - использует пул доступных глобальных (публичных) ip-адресов и назначает их внутренним локальным (частным) адресам. Схема для нашей работы приведена на Рисунок 9.30.

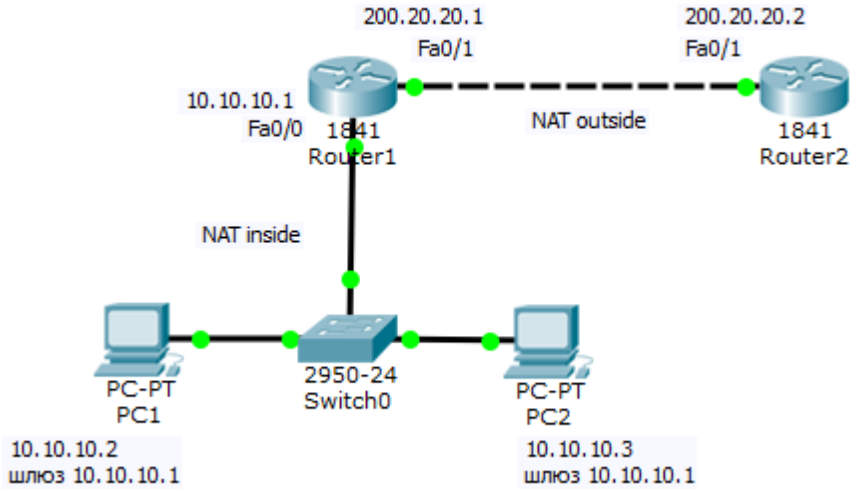


Рисунок 9.30. Схема сети

Шаг 1. Настройка на R1 списка доступа, соответствующего адресам LAN

R1 (config)# access-list 1 permit 10.10.10.0 0.0.0.255

Здесь 0.0.0.225 – обратная (инверсная) маска для адреса 10.10.10.0.

Шаг 2. Настройка пула адресов

R1 (config)# ip nat pool white-address 200.20.20.1 200.20.20.30 netmask 255.255.255.0

Шаг 3. Настройка трансляции

R1 (config)# ip nat inside source list 1 pool white-address

Шаг 4. Настройка внутреннего интерфейса в отношение NAT

R1 (config)# interface fastethernet 0/0

R1 (config-if)# ip nat inside

Шаг 5. Настройка внешнего интерфейса в отношение NAT

R1 (config)# interface fastethernet 0/1

R1 (config-if)# ip nat outside

Ниже дан полный листинг команд по настройке R1 (Рисунок 9.31).

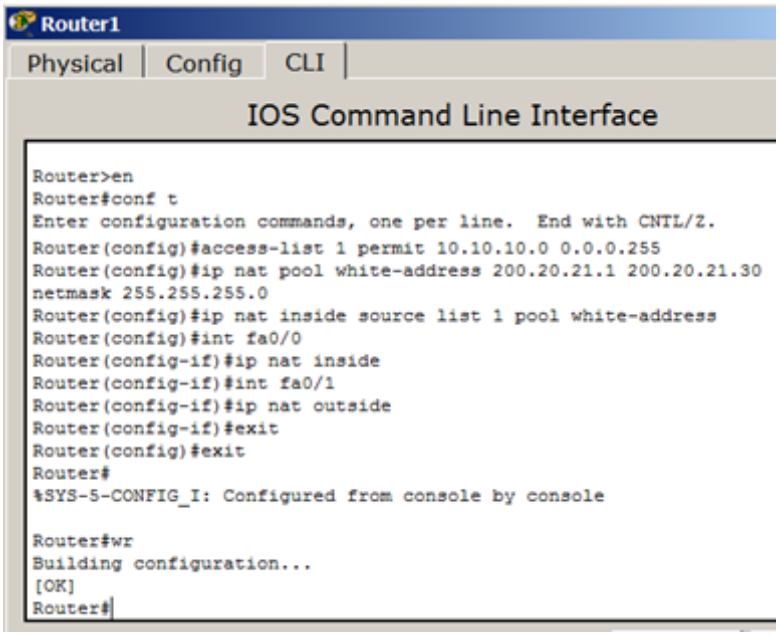


Рисунок 9.31. Полный листинг команд по конфигурированию R1

Команды для проверки работы динамического NAT

Проверим связь PC1 и R2 (Рисунок 9.32).

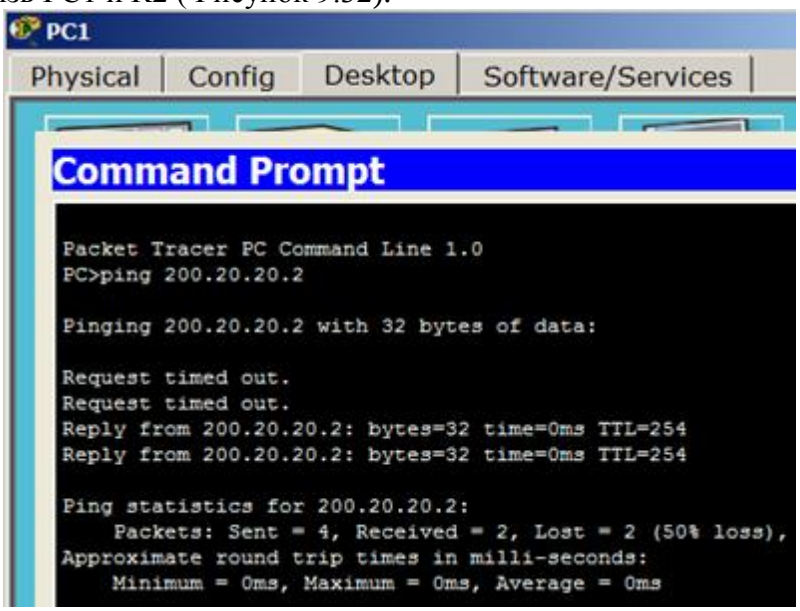


Рисунок 9.32. PC1 видит R2

Проверим, что R1 видит соседние сети (Рисунок 9.33).

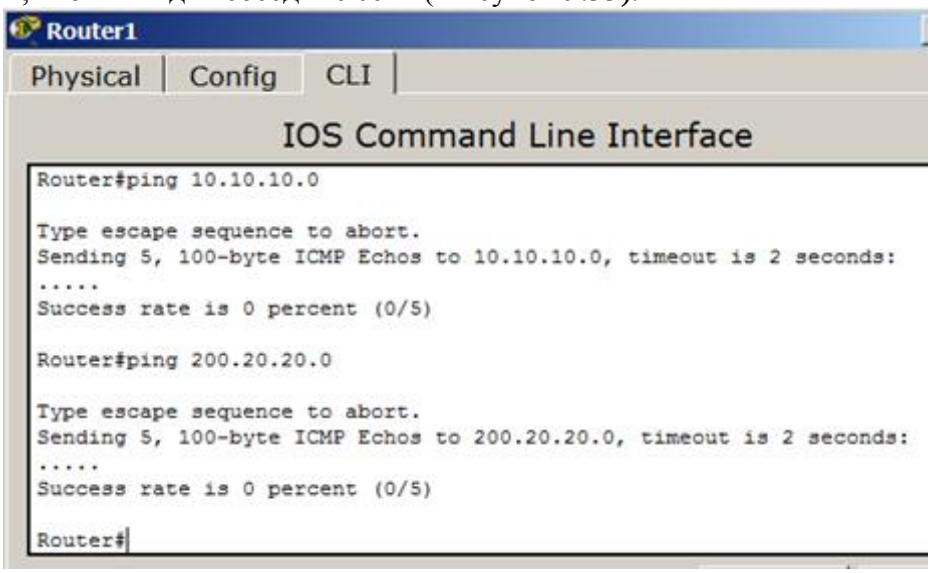


Рисунок 9.33. R1 видит подсети 10.10.10.0 и 200.20.20.0

Проверим механизм работы динамического NAT: для этого выполним одновременно (параллельно) команды ping и show ip nat translations (Рисунок 9.34).

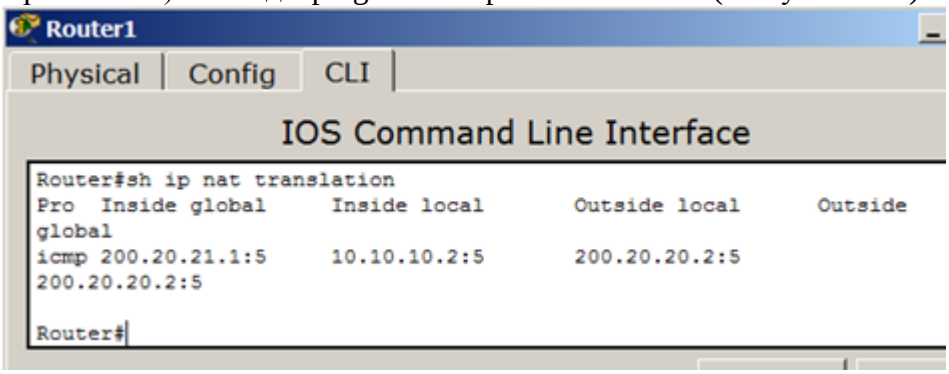


Рисунок 9.34. Адреса: глобальный, внутренний, внешний

Командой show ip nat statistics выведем статистику по NAT преобразованиям (Рисунок 9.35).

Рисунок 9.35. Статистика работы динамического NAT

Из иллюстрации видим, что локальным адресам соответствует пул внешних адресов от 200.20.20.1 до 20.20.20.30.

ПРАКТИЧЕСКАЯ РАБОТА № 9.6

Динамический NAT Overload: настройка PAT (маскарадинг)

Время работы: 2 часа

1. Цель работы: Научится работать с программой Cisco Packet Tracer (CPT)

2. Технические средства

2.1 Оборудование: компьютер

2.2 Программное обеспечение: Cisco Packet Tracer, MS Word.

PAT (Port Address Translation) - отображает несколько локальных (частных) ip-адресов в глобальный ip-адрес, используя различные порты (Рисунок 9.36).

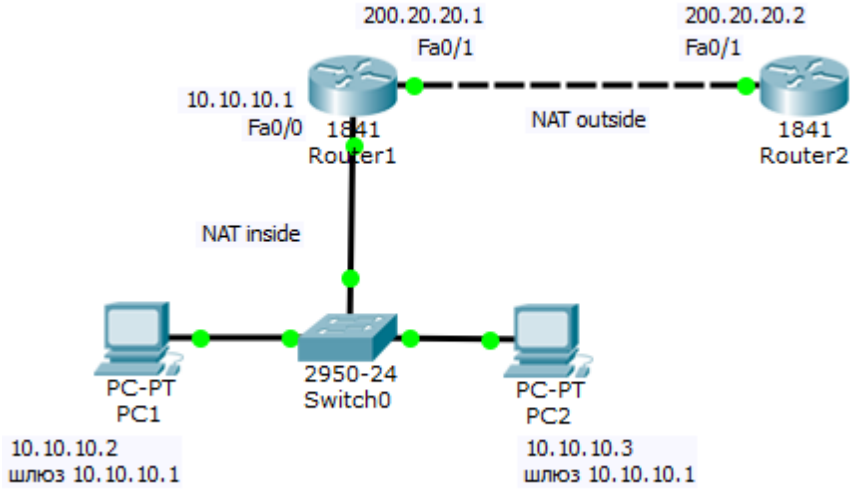


Рисунок 9.36. Схема сети на настройки трансляции адресов PAT

Рассмотрим алгоритм нашей работы по шагам.

Шаг 1. Настройка списка доступа, соответствующего внутренним частным адресам

R1(config)# access-list 1 permit 10.10.10.0 0.0.0.255

Шаг 2. Настройка трансляции

R1(config)# ip nat inside source list 1 interface fastethernet 0/1 overload

Шаг 3. Настройка внутреннего интерфейса в отношение NAT

R1(config)# interface fastethernet 0/0

R1(config-if)# ip nat inside

Шаг 4. Настройка NAT на интерфейсе

R1(config)# interface fastethernet 0/1

R1(config-if)# ip nat outside

Ниже дан полный листинг команд по конфигурированию R1 (Рисунок 9.37).

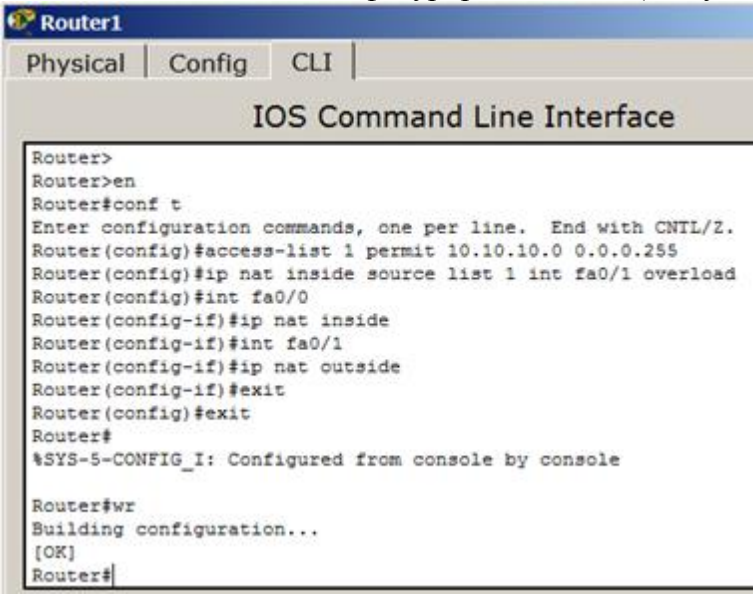


Рисунок 9.37. Листинг команд по конфигурированию R1

Команды для проверки работы маскарадинга (PAT)

Проверим связь PC1 и R2 (Рисунок 9.38).

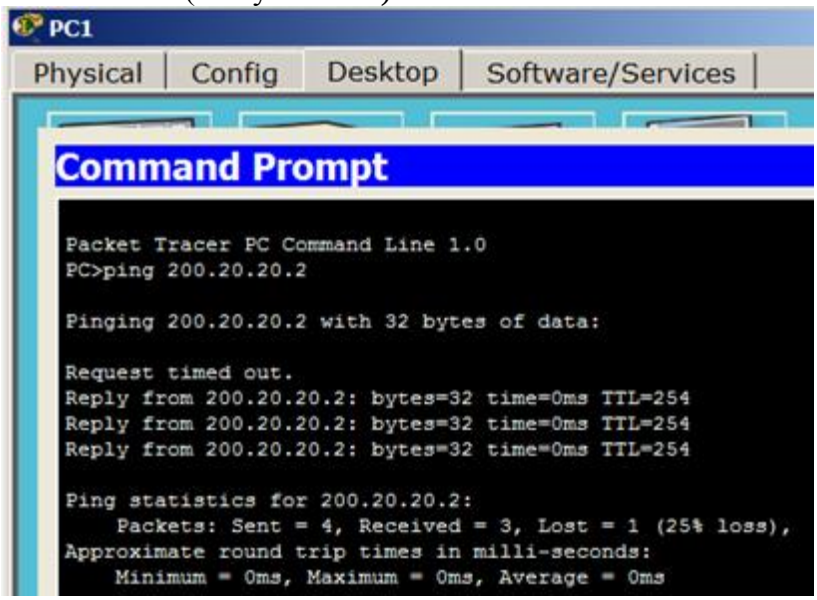


Рисунок 9.38. PC1 видит R2

Проверим, что R1 видит соседние сети (Рисунок 9.39).

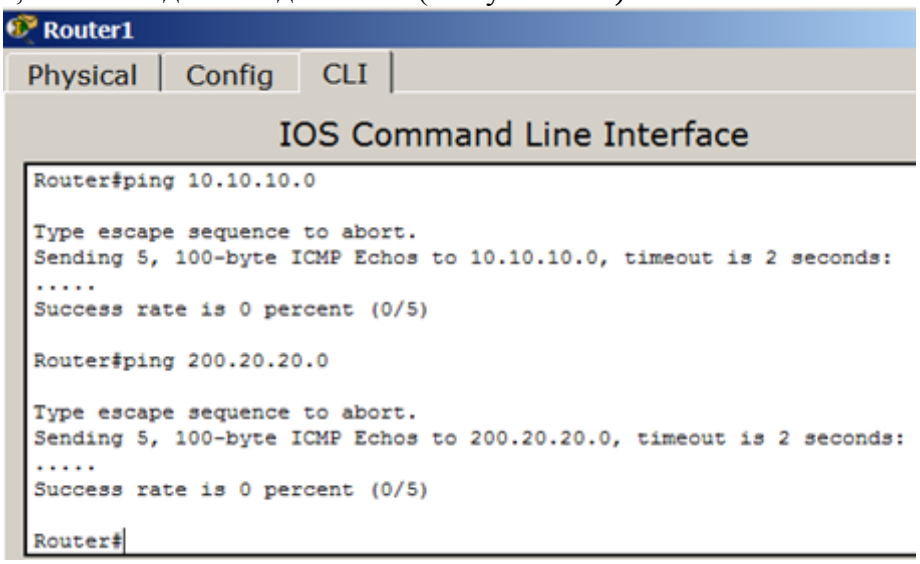


Рисунок 9.39. R1 видит подсети 10.10.10.0 и 200.20.20.0

Проверим механизм работы динамического NAT: для этого выполним одновременно (параллельно) команды ping и show ip nat translations (Рисунок 9.40).

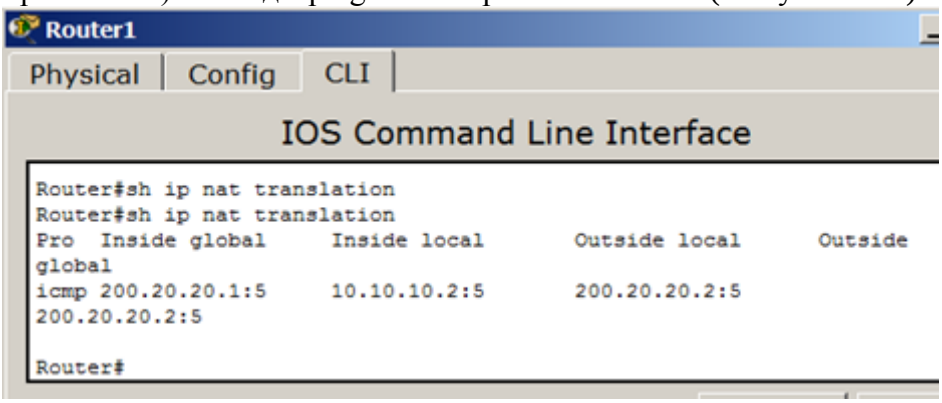


Рисунок 9.40. Адреса: глобальный, внутренний, внешний

Проверим работу сети в режиме симуляции (Рисунок 9.41).

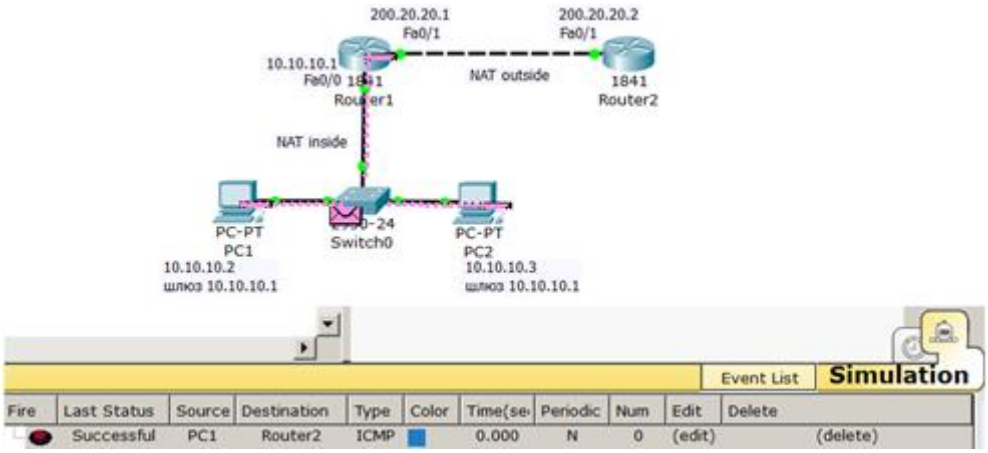


Рисунок 9.41. PAT работает, PC1 и R2 отправляют и получают пакеты Successful

ПРАКТИЧЕСКАЯ РАБОТА № 10.1

Создание новой беспроводной сети

Время работы: 2 часа

1. Цель работы: Научится работать с программой Cisco Packet Tracer (CPT)

2. Технические средства

2.1 Оборудование: компьютер

2.2 Программное обеспечение: Cisco Packet Tracer, MS Word.

Беспроводная сеть WEP

Создание новой беспроводной сети начинается непосредственно с конфигурации точки доступа - беспроводного маршрутизатора (роутера) подключения к ней компьютеров и другого беспроводного оборудования. Классический способ настройки такой: вначале производится подключение к точке доступа оборудования, а затем нужно задать вручную имя беспроводной сети и ключ безопасности. В этой лекции и далее мы рассмотрим различные варианты беспроводных сетей и способы их настройки в программе CPT. Ключ безопасности беспроводной сети - уникальный код (пароль), который закрывает доступ к вашей сети. При этом важен не столько сам ключ, сколько тип шифрования. Дело в том, что вся информация, которая протекает между роутером и ПК шифруется. И если вы ввели неправильный ключ, то ваше устройство просто не сможет раскодировать ее. Это сделано для повышения безопасности. Стоит отметить, что на сегодняшний день существует три типа шифрования Wi-Fi подключений: WPA. WPA2. WEP.

Новый термин

WEP (Wired Equivalent Privacy) — алгоритм для обеспечения безопасности сетей Wi-Fi. Используется для обеспечения защиты, передаваемых данных

Схема для работы показана на Рисунок 10.1.

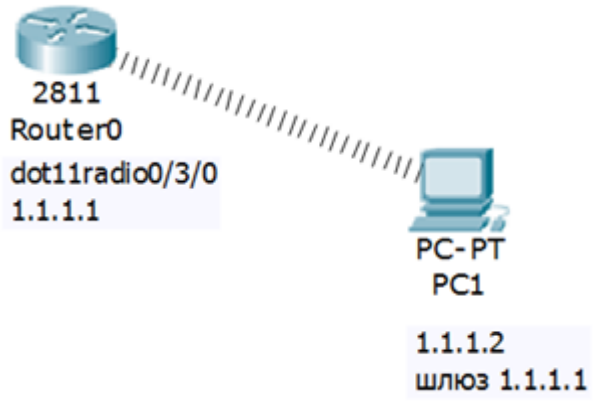


Рисунок 10.1. Схема сети

Оснастим маршрутизатор радиоточкой доступа HWIC-AP-AG-B (Рисунок 10.2).

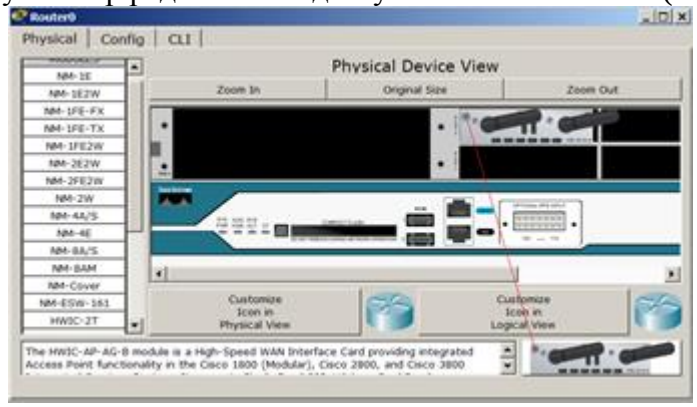


Рисунок 10.2. Радиоточка доступа HWIC-AP-AG-B

Вставим в ПК беспроводный адаптер WMP300N. Для этого сначала выключим ПК и уберем из него модуль PT-HOST-NM-1CFE (Рисунок 10.3).

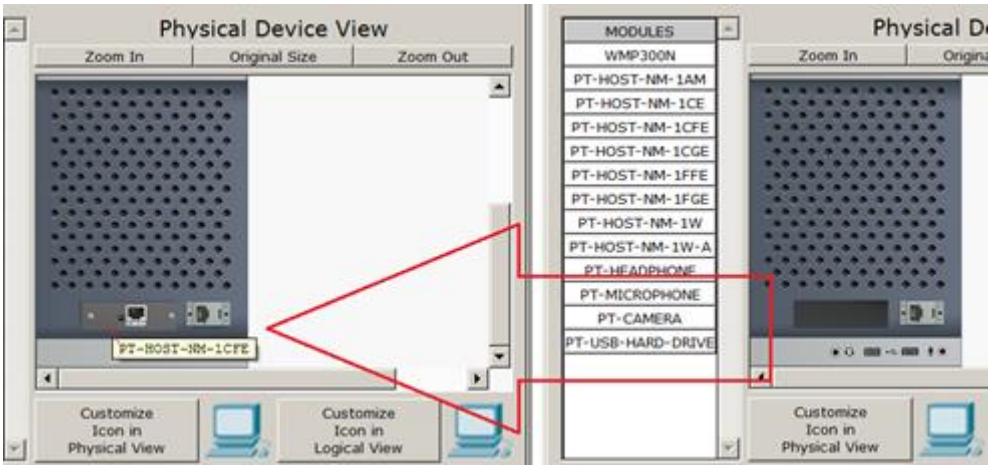


Рисунок 10.3. Удаляем модуль PT-HOST-NM-1CFE

Вставляем беспроводный адаптер WMP300N (Рисунок 10.4).

Рисунок 10.4. Оснащаем ПК беспроводным адаптером

Реальный вид беспроводного адаптера WMP300N приведен на Рисунок 10.5.

Рисунок 10.5. Беспроводный адаптер WMP300N

Настроим беспроводный адаптер на PC1 (Рисунок 10.6).

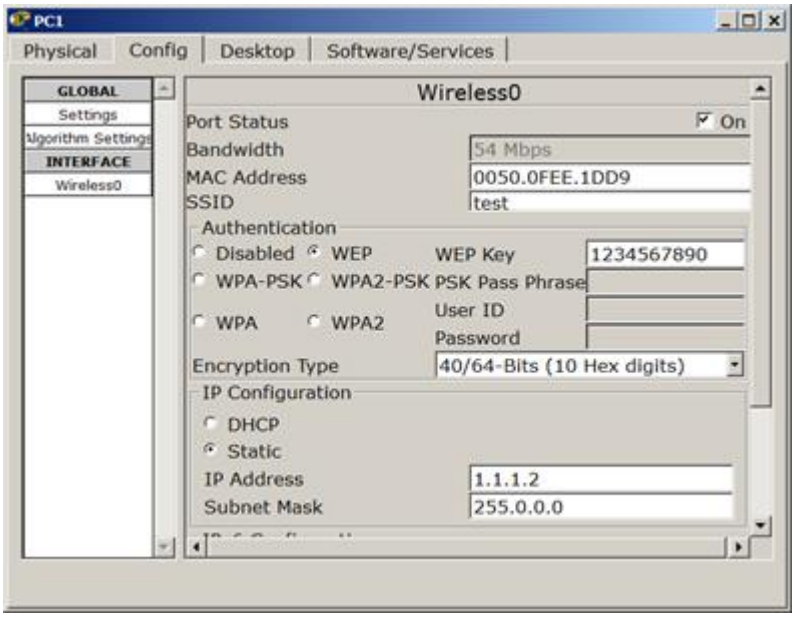


Рисунок 10.6. Настройка беспроводного адаптера

Проверим результат (Рисунок 10.7 и Рисунок 10.8).

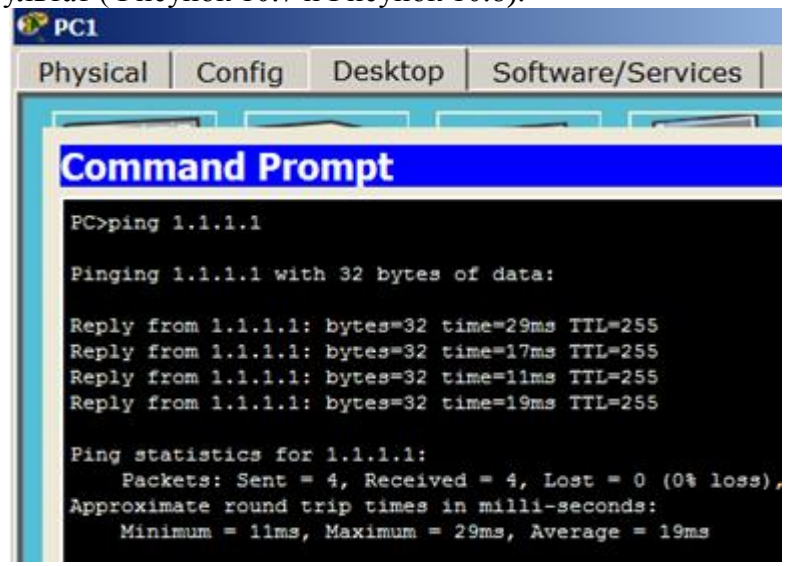


Рисунок 10.7. Проверка связи ПК и маршрутизатора

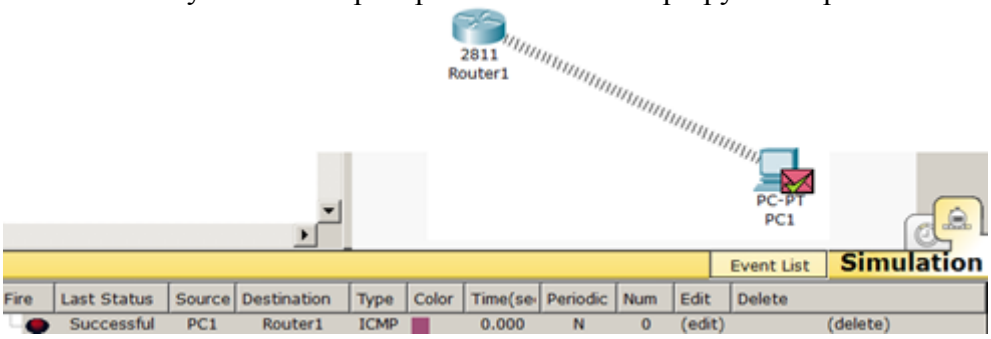


Рисунок 10.8. Проверка связи ПК и маршрутизатора в режиме симуляции

ПРАКТИЧЕСКАЯ РАБОТА № 10.2

Настройка беспроводной сети WPA

Время работы: 2 часа

1. Цель работы: Научится работать с программой Cisco Packet Tracer (CPT)

2. Технические средства

2.1 Оборудование: компьютер

2.2 Программное обеспечение: Cisco Packet Tracer, MS Word.

Беспроводная сеть WPA

Типы шифрования сети WPA и WPA2 требуют от абонентов введение уникального пароля. Без него вы просто не сможете выполнить подключение. После проверки введенного ключа все данные, которые передаются между участниками сети, шифруются. Современные роутеры поддерживают обе технологии. Но, WPA2 все же предоставляет более высокую защиту. Поэтому по возможности следует выбирать именно его.

Новый термин

WPA (Wi-Fi Protected Access) — представляет собой технологию защиты беспроводной Wi-Fi сети. Плюсами WPA являются усиленная безопасность данных и ужесточённый контроль доступа к беспроводным сетям, а также - совместимость между множеством беспроводных устройств как на аппаратном уровне, так и на программном.

Рассмотрим сеть, изображенную на Рисунок 10.9.

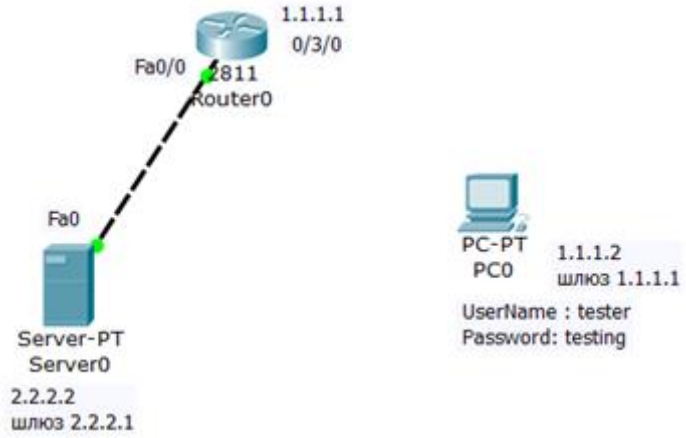


Рисунок 10.9. Схема сети

Здесь для нас ничего нового, кроме настроек адаптера ПК (Рисунок 10.10).

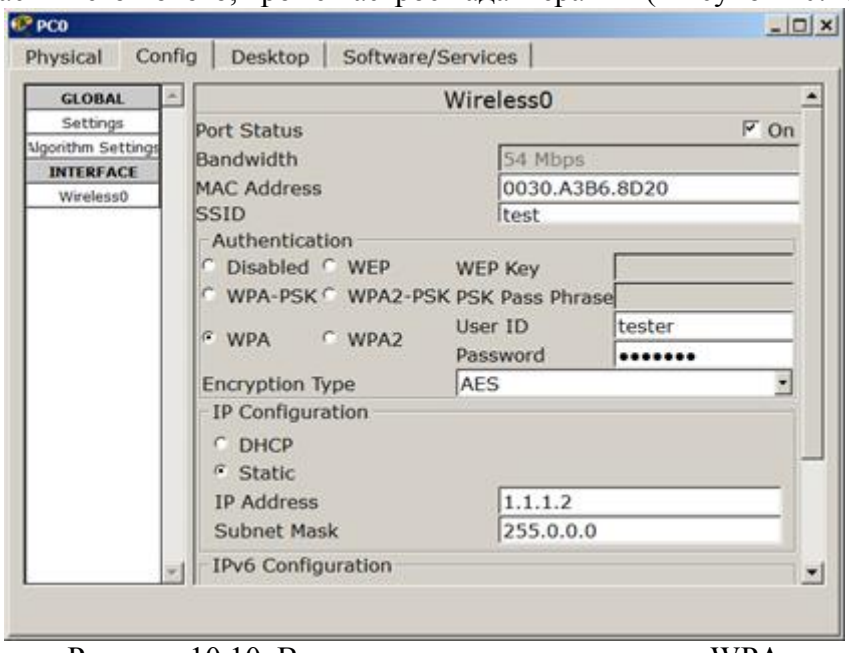


Рисунок 10.10. Включаем технологию защиты WPA

Теперь зайдем в маршрутизатор (Рисунок 10.11) и, чтобы включить беспроводную связь, наберем логин и пароль (Рисунок 10.12).

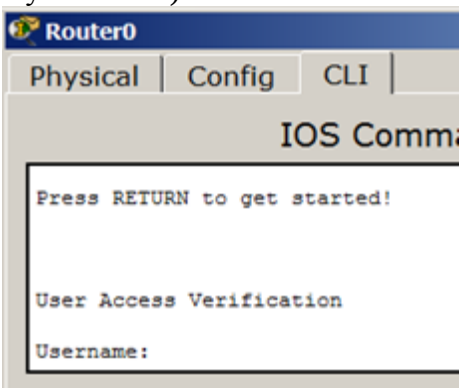


Рисунок 10.11. Роутер требует провести аутентификацию

UserName : tester
Password: testing

Рисунок 10.12. Логин и пароль для связи беспроводных устройств

После проведения аутентификации связь будет установлена (Рисунок 10.13).

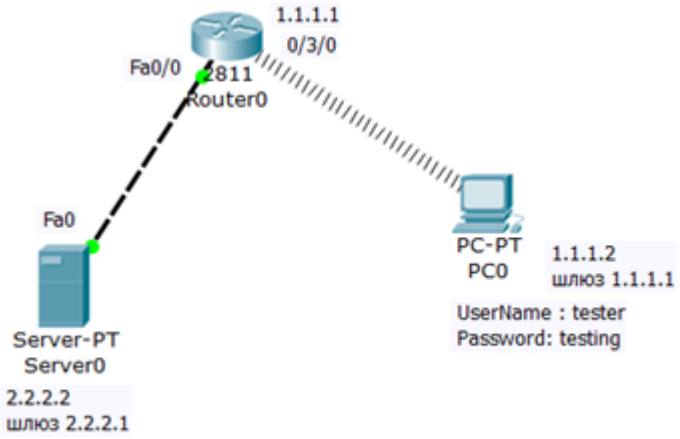


Рисунок 10.13. Беспроводная связь работает

ПРАКТИЧЕСКАЯ РАБОТА № 10.3

Беспроводная сеть с точкой доступа

Время работы: 2 часа

1. Цель работы: Научится работать с программой Cisco Packet Tracer (CPT)
2. Технические средства

2.1 Оборудование: компьютер

2.2 Программное обеспечение: Cisco Packet Tracer, MS Word.

Беспроводная сеть с точкой доступа

Ниже мы рассмотрим два примера настройки беспроводных WI-FI сетей.

Соберите схему сети, представленную на Рисунок 10.14.

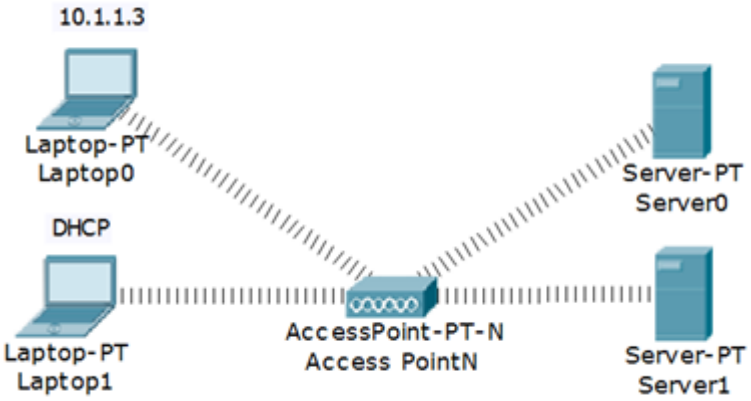


Рисунок 10.14. Схема сети

Новый термин

Точка доступа в английской терминологии – Wireless Access Point.

Рассмотрим настройки точки доступа, они соответствуют настройкам по умолчанию (Рисунок 10.15).

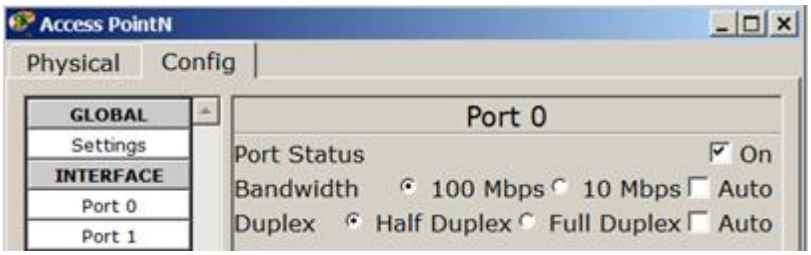


Рисунок 10.15. Настройки точки доступа

Статическая настройка ноутбука (Рисунок 10.16).

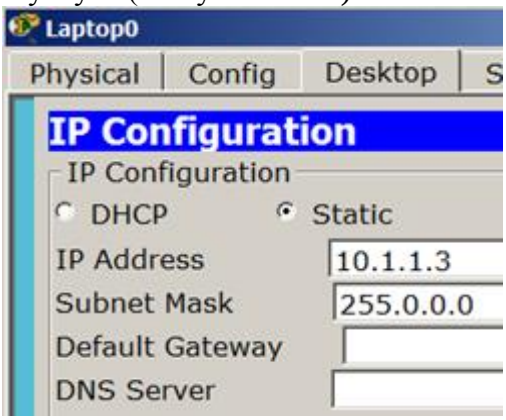


Рисунок 10.16. Задаем IPадрес для L0

Динамическая настройка ноутбука (Рисунок 10.17).

Рисунок 10.17. Включаем переключатель DHCP для L1

Настройка серверов (Рисунок 10.18).

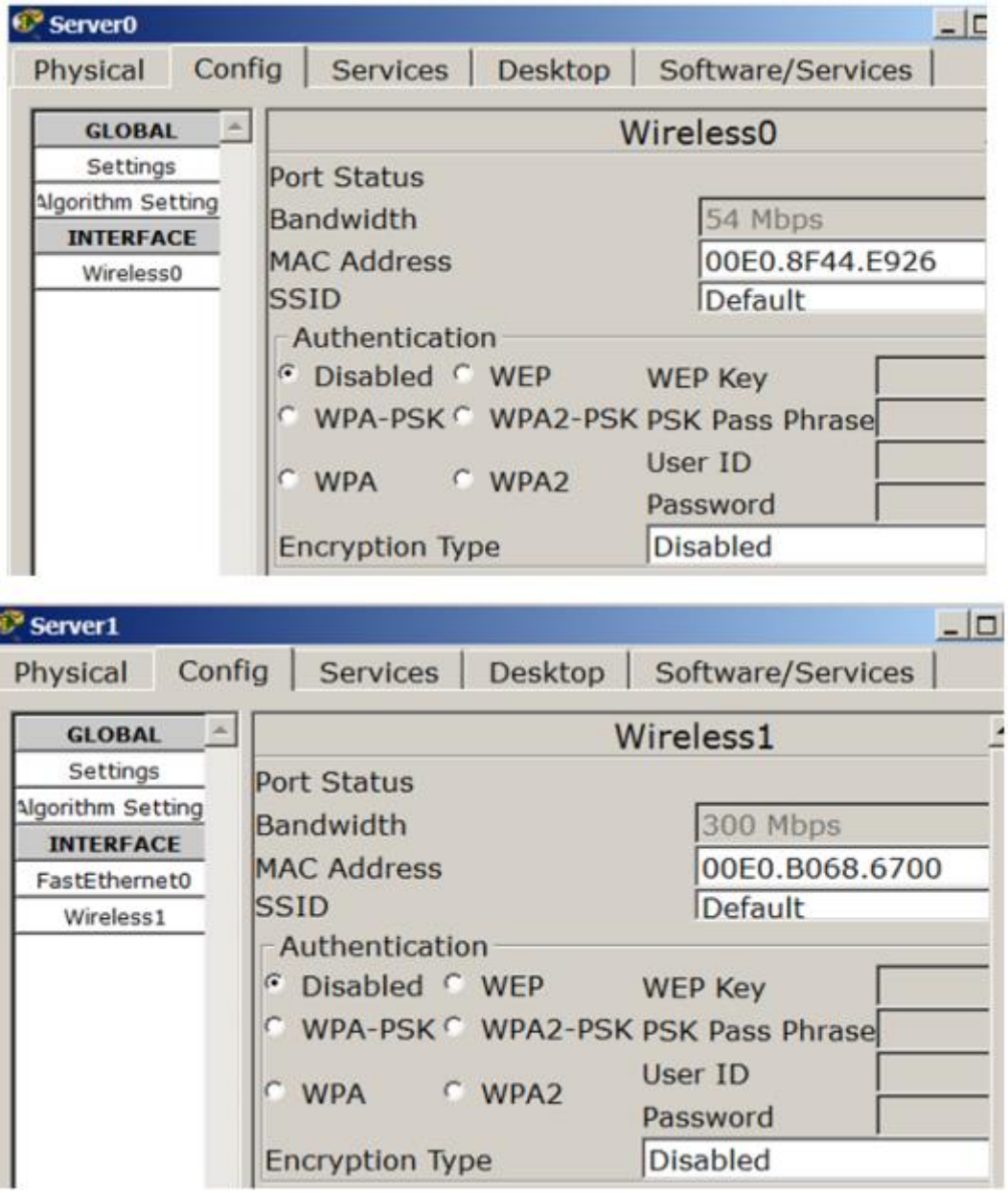


Рисунок 10.18. Сервера настроены по умолчанию

Точку доступа POINT N можете заменить на POINT 0, при этом настройки хостов можно не менять (Рисунок 10.19).

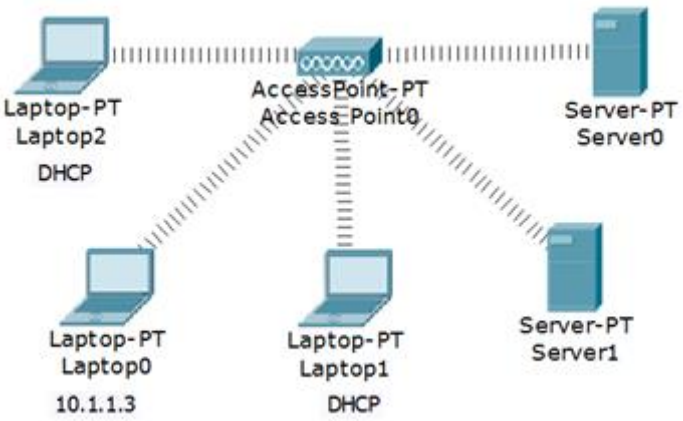


Рисунок 10.19. Беспроводная связь установлена

ПРАКТИЧЕСКАЯ РАБОТА № 10.4

Беспроводная сеть между офисами

Время работы: 2 часа

1. Цель работы: Научится работать с программой Cisco Packet Tracer (CPT)

2. Технические средства

2.1 Оборудование: компьютер

2.2 Программное обеспечение: Cisco Packet Tracer, MS Word.

Настроим следующую беспроводную сеть (Рисунок 10.20).

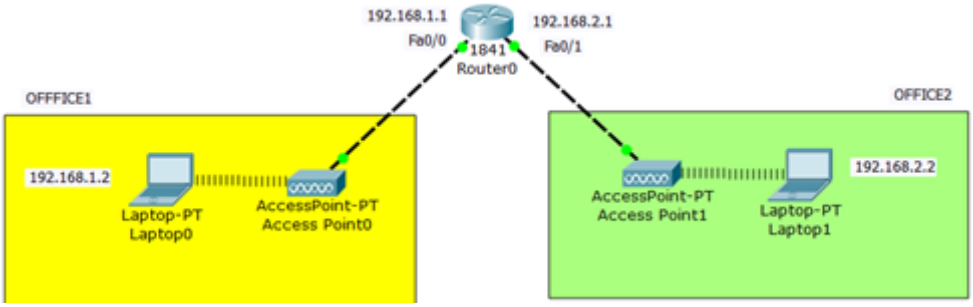


Рисунок 10.20. WI-FI сеть между офисами

Снабжаем ноутбука wi-fi адаптерами WPC300N. Настройки обоих ноутбуков аналогичны (Рисунок 10.21).

Рисунок 10.21. Настройки ноутбуков

Примечание

Каждая беспроводная локальная сеть использует уникальное сетевое имя для идентификации сети. Это имя также называется идентификатором обслуживания сети - SSID. Когда вы будете устанавливать адаптер Wi-Fi, нужно будет указать SSID. Если вы хотите подключиться к существующей беспроводной сети, вы должны использовать имя этой сети. Имя может иметь длину до 32 символов и содержать буквы и цифры.

Помимо SSID на ноутбуках настраивается шлюз (Рисунок 10.22).

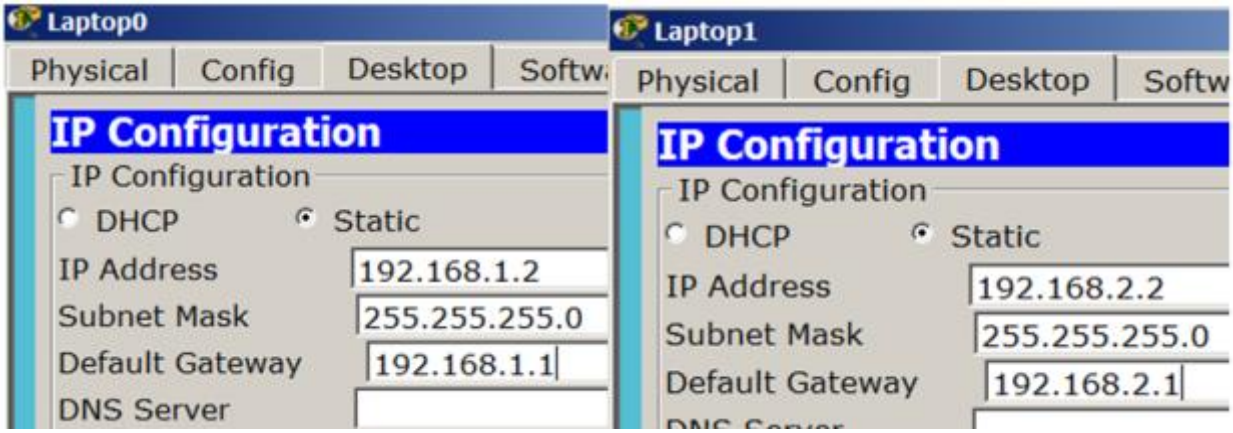


Рисунок 10.22. На L0 и L1 указываем адрес шлюза

SSID задаем на обеих точках доступа (Рисунок 10.23).

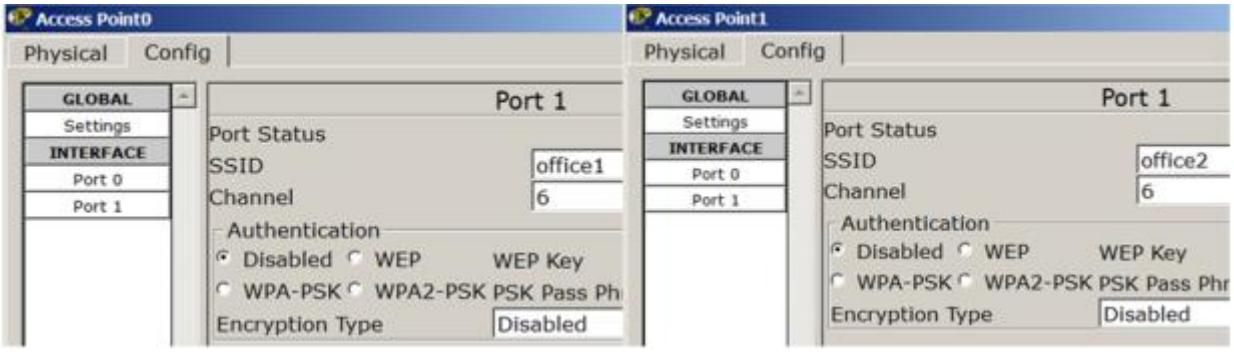


Рисунок 10.23. Задаем SSIDна точках доступа

Проверяем связь ПК из разных офисов (Рисунок 10.24).

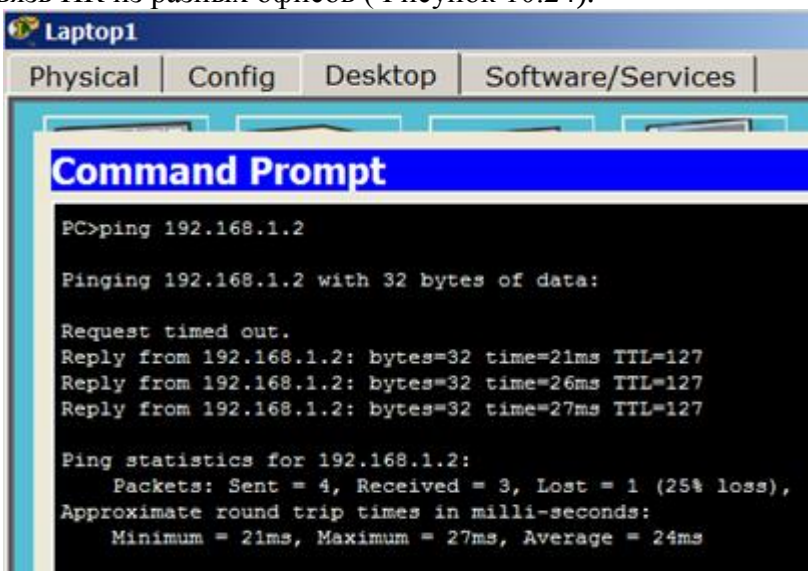


Рисунок 10.24. Связь L1 и L0 присутствует

ПРАКТИЧЕСКАЯ РАБОТА № 10.5

Настройка коммутируемого WI-FI соединения

Время работы: 2 часа

1. Цель работы: Научится работать с программой Cisco Packet Tracer (CPT)

2. Технические средства

2.1 Оборудование: компьютер

2.2 Программное обеспечение: Cisco Packet Tracer, MS Word.

Настройка коммутируемого WI-FI соединения

В этой лекции мы рассмотрим два примера работы с wi-fi сетью.

Соберем и настроим сеть, изображенную на Рисунок 10.25.

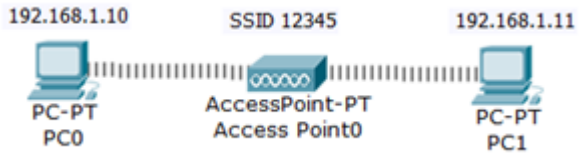


Рисунок 10.25. WI-FI сеть

Сначала зададим имя сети (SSID) на точке доступа (Рисунок 10.26).

Рисунок 10.26. Задаем SSID на точке доступа

В оба ПК вставляем беспроводной адаптер Linksys-WPM-300N (Рисунок 10.27).

Рисунок 10.27. Адаптер Linksys-WPM-300N вставлен в PC0

Устанавливаем связь точки доступа и PC0, для этого нажимаем на кнопку PC Wireless (Рисунок 10.28).

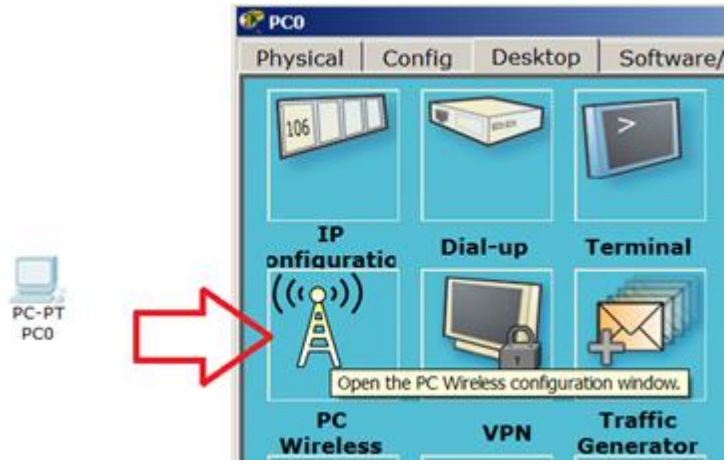


Рисунок 10.28. Нажимаем на кнопку PCWireless

Теперь открываем вкладку Connect и нажимаем на кнопку Connect (Рисунок 10.29).

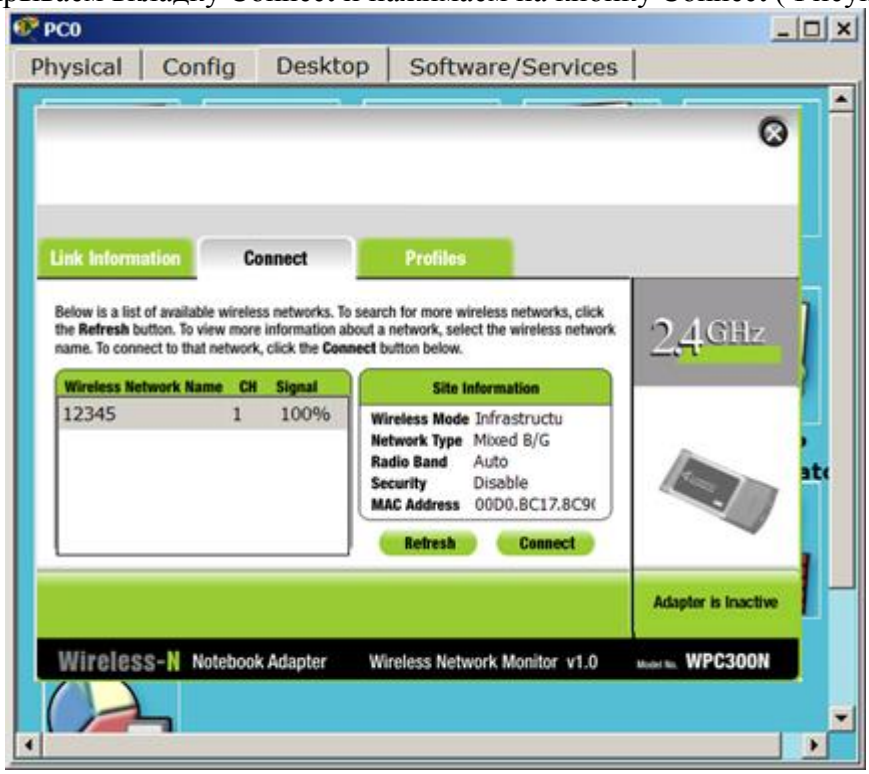


Рисунок 10.29. Нажимаем на кнопку Connectи окно закрываем

В результате у нас получается динамическая связь PC0 и Access Point-PT (Рисунок 10.30).

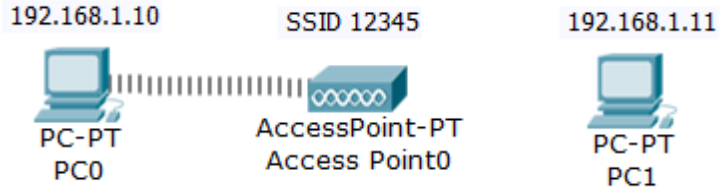


Рисунок 10.30. Динамическая связь точки доступа и беспроводного адаптера

Меняем динамический адрес на статический (Рисунок 10.31).

Рисунок 10.31. Меняем динамический адрес на статический

Теперь аналогично настраиваем PC1 и проверяем связь между ПК (Рисунок 10.32).

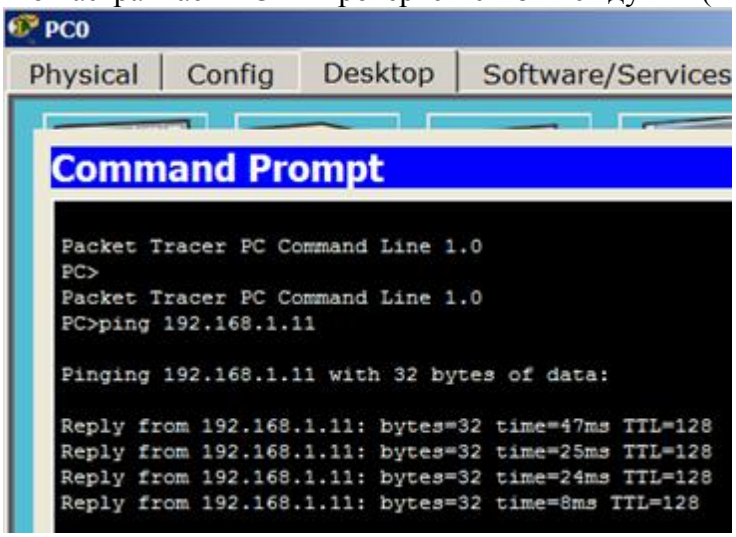


Рисунок 10.32. Связь между ПК отличная

ПРАКТИЧЕСКАЯ РАБОТА № 10.6

Беспроводная связь в Packet Tracer с беспроводным роутером

Время работы: 2 часа

1. Цель работы: Научится работать с программой Cisco Packet Tracer (CPT)

2. Технические средства

2.1 Оборудование: компьютер

2.2 Программное обеспечение: Cisco Packet Tracer, MS Word.

На Рисунок 10.33 приведена схема сети с беспроводным роутером.

Рисунок 10.33. Схема сети с беспроводным роутером

Если мы снабдим оба ПК беспроводным модулем,то в данной сети мы можем наблюдать появление WIFI связи (Рисунок 10.34).

Рисунок 10.34. Мы можем наблюдать появление WIFIсвязи

Зайдем на роутер и посмотрим на его IP address. Как видим, включен DHCP service и роутер получает IP адрес автоматически (Рисунок 10.35).

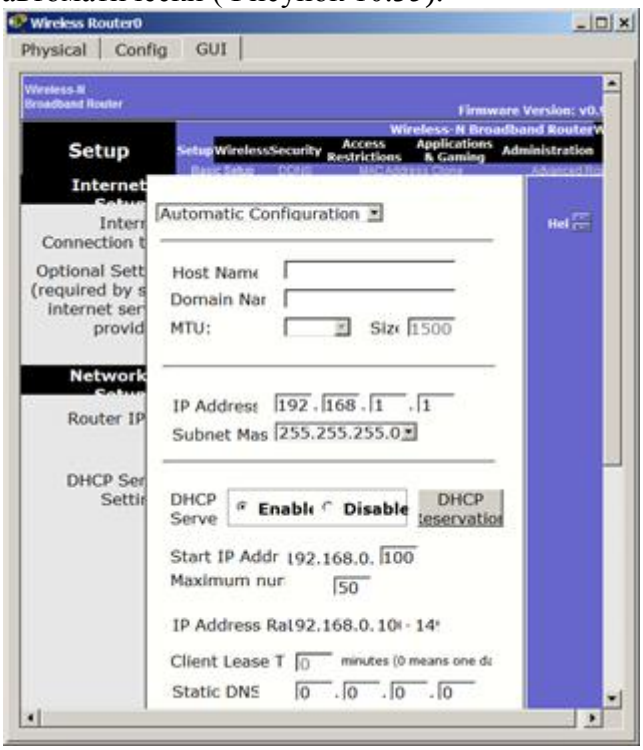


Рисунок 10.35. Автоматическое конфигурирование роутера

Теперь на вкладке Config настроим аутентификацию роутера (Рисунок 10.36).

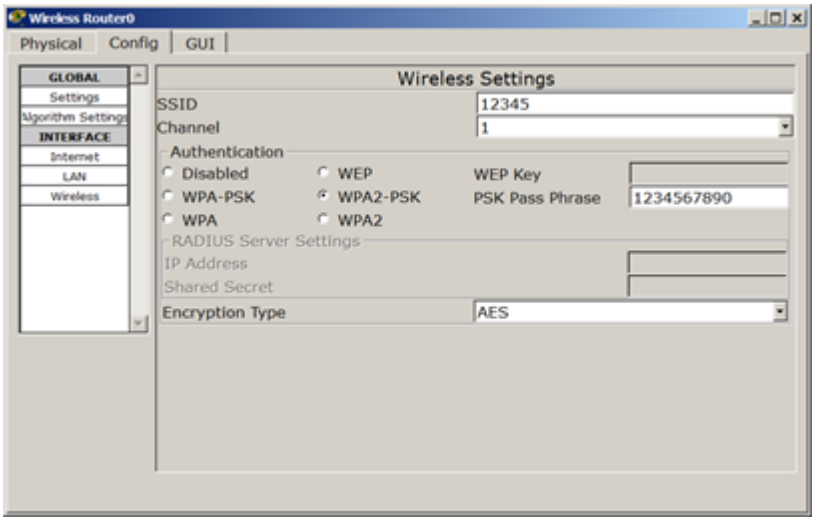


Рисунок 10.36. Вводим SSIDи WPA2-PSK

Теперь для PC0 заходим в меню PCWireless (Рисунок 10.37).

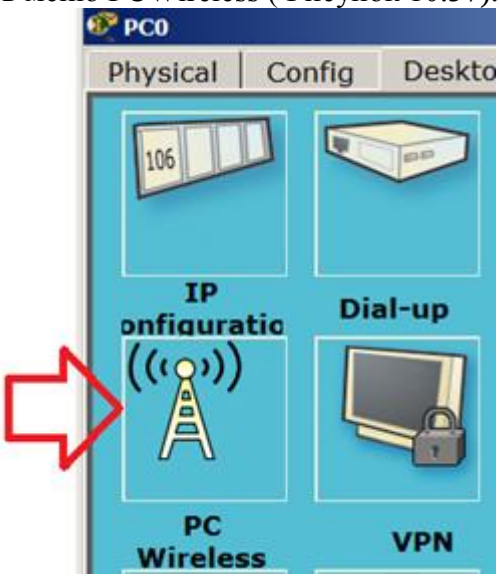


Рисунок 10.37. Заходим в меню PCWireless

Устанавливаем соединение PC0 и роутера (Рисунок 10.38).

Рисунок 10.38. На вкладке Connect нажимаем на кнопку Connect

Для аутентификации необходим WPA2-PSK пароль, т.е. 1234567890 (Рисунок 10.39).

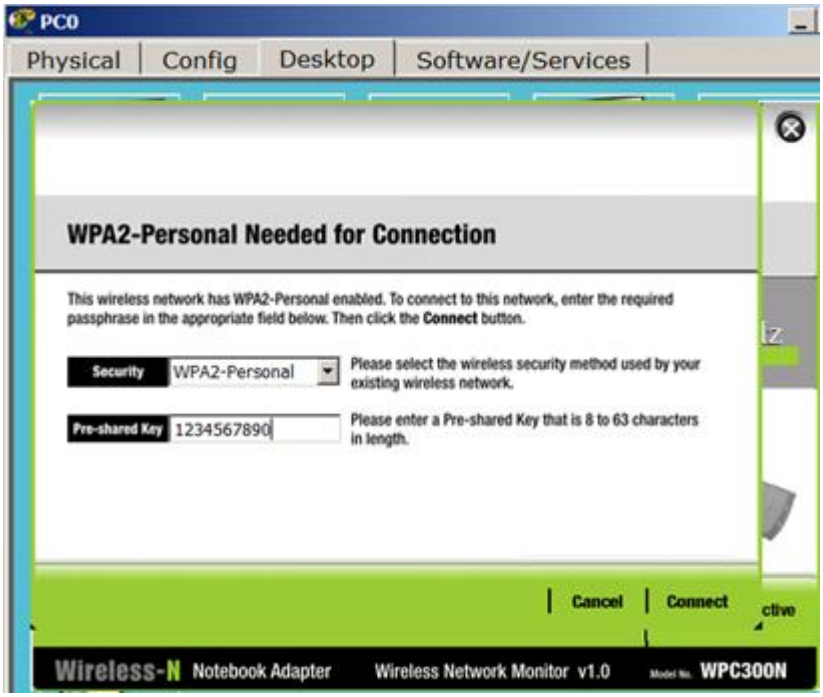


Рисунок 10.39. Вводим пароль и нажимаем на кнопку Connect

Примечание

Протокол безопасности WPA2-PSK - упрощенный вариант WPA2. Технологии защиты беспроводных сетей WPA2 является самой лучшей на сегодняшний день. Но, из соображений совместимости на маршрутизаторах можно встретить ее вариант WPA2-PSK.

Итак, мы предъявили наш "пропуск" на вход пользователя в сеть и связь устройств установлена (Рисунок 10.40).

Рисунок 10.40. Связь PC0 и роутера настроена

Теперь вводим пароль на PC1 (Рисунок 10.41).

Рисунок 10.41. Появилась связь роутера и PC1

Узнаем динамический IP адрес для PC1

```
Port         Link   IP Address
Wireless0    Up     192.168.0.101/24

Gateway: 192.168.0.1
DNS Server:  <not set>
Line Number:  <not set>
```

и пингуем его с PC0 (Рисунок 10.42).

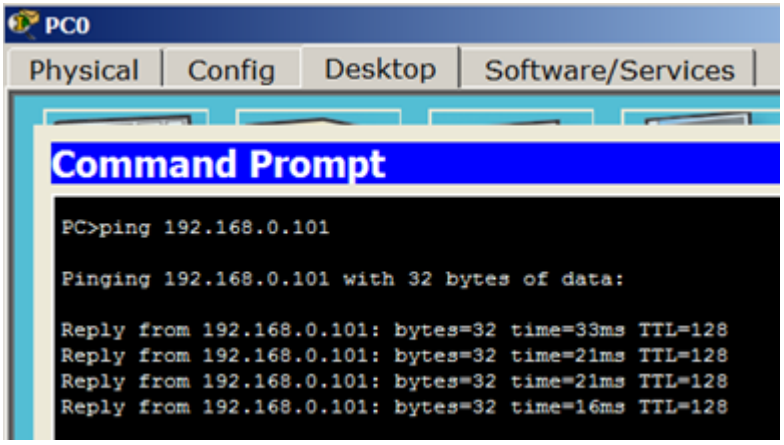


Рисунок 10.42. Связь между PC0 и PC1 есть

ПРАКТИЧЕСКАЯ РАБОТА № 11.1

Строим сеть из двух ПК и коммутатора в NetEmul

Время работы: 2 часа

1. Цель работы: Научится работать с программой Cisco Packet Tracer (CPT)

2. Технические средства

2.1 Оборудование: компьютер

2.2 Программное обеспечение: NetEmul,Oracle VM Virtual Box, MS Word.

Программа-конкурент и аналог CPT для изучения компьютерных сетей - NetEmul

Бесплатная программа NetEmul была создана в учебных целях и служит для визуализации работы компьютерных сетей, для облегчения понимания, происходящих в ней процессов. Программа одинаково хорошо работает во всех версиях ОС, начиная с Windows XP и Windows 7. Программа не привязана к конкретному оборудованию Cisco или D-Link и имеет русификацию интерфейса.

Интерфейс программы

Для начала установим программу, запустим и русифицируем ее командой Сервис-Настройки (Рисунок 11.1).

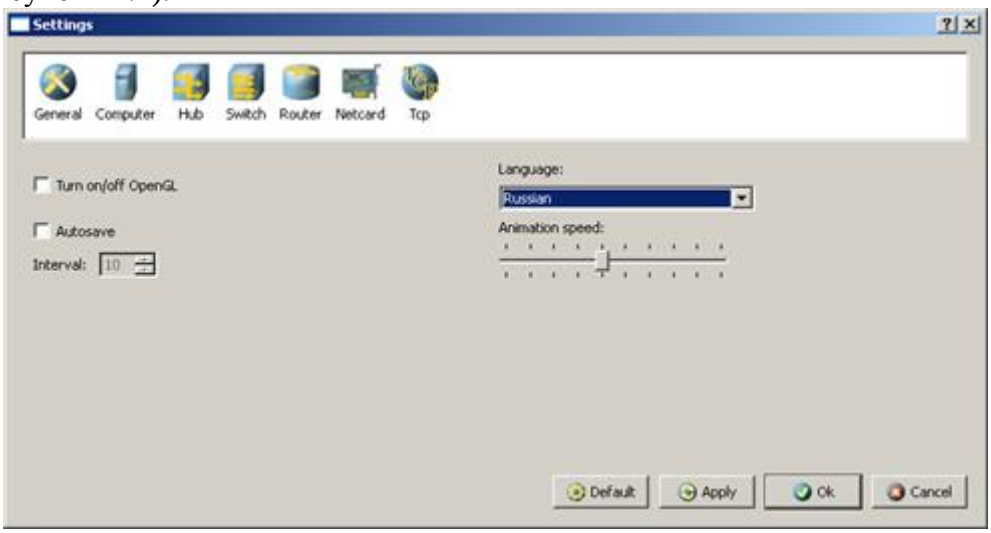


Рисунок 11.1. Русифицируем интерфейс программы

В главном окне программы все элементы размещаются на рабочей области (на Сцене). На всей свободной области сцены, размеченной сеткой можно ставить устройства, при этом они не должны пересекаться. На Панели устройств размещены все необходимые для построения сети инструменты, а также кнопка отправки сообщений и Запустить/Остановить. На Панели параметров расположены свойства объектов. Для выделенного объекта появляются только те свойства, которые характерны для него (Рисунок 11.2).

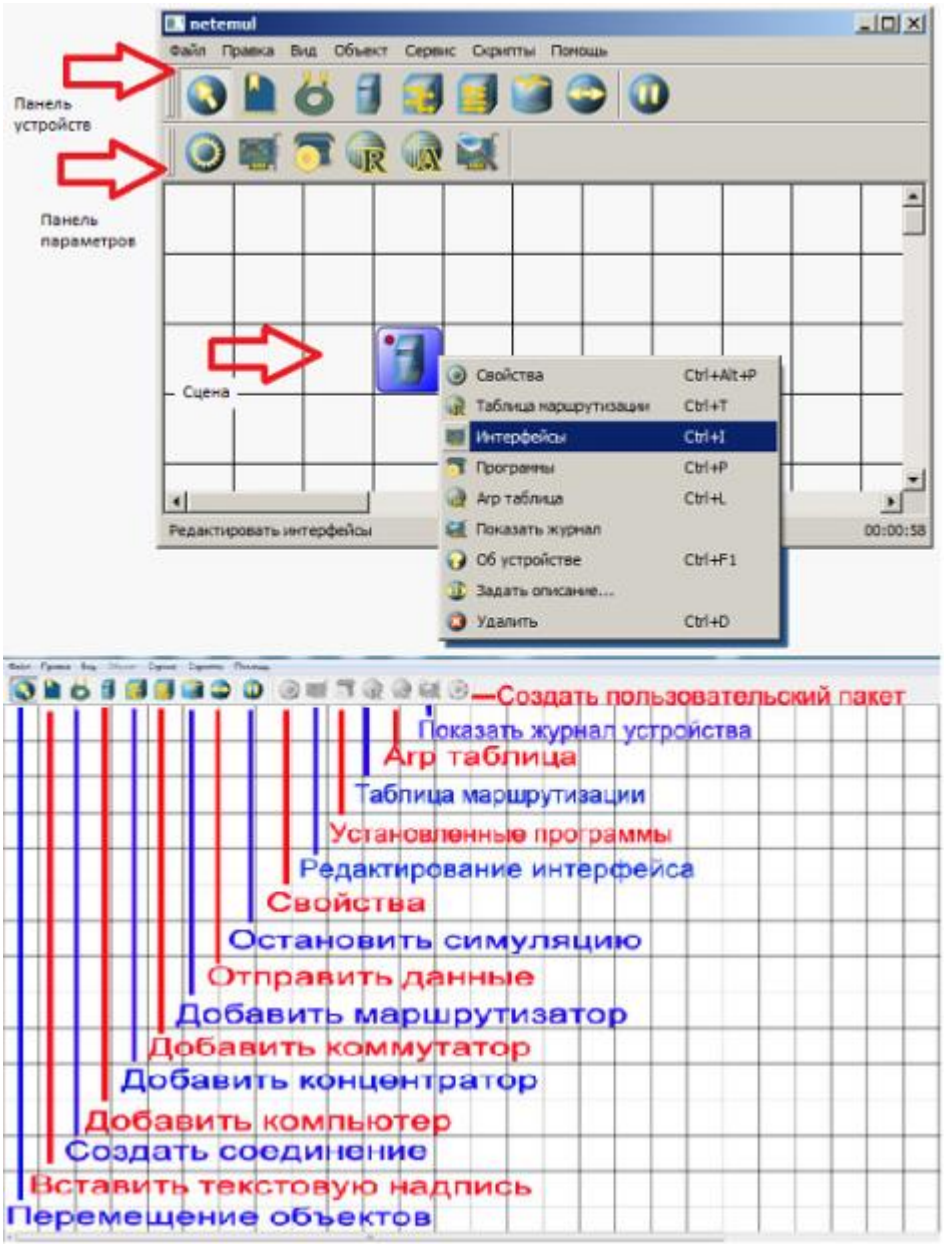


Рисунок 11.2. Интерфейс программы NetEmul

Для начального знакомства с программой давайте построим простейшую локальную сеть и посмотрим, как она работает. Для этого выполните команду Файл-Новый и нарисуйте схему сети как на Рисунок 11.3.

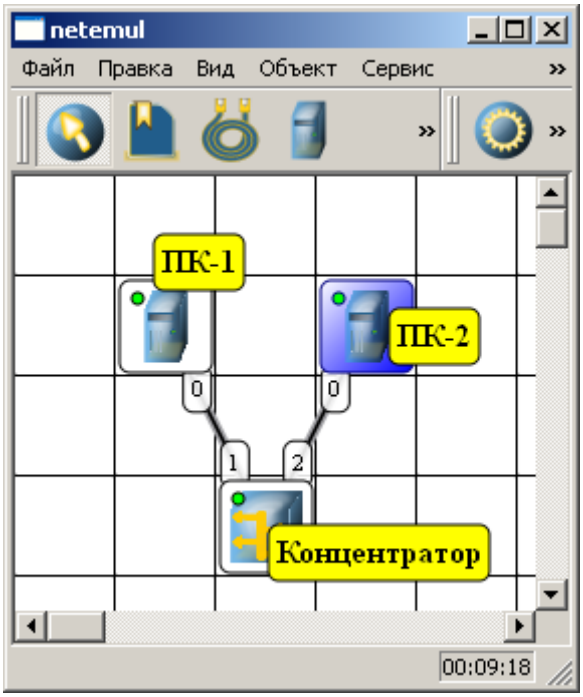


Рисунок 11.3. Схема из двух ПК и концентратора

После рисования двух ПК и концентратора создадим их соединение (Рисунок 11.4).

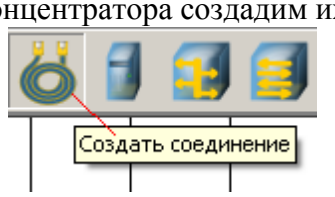


Рисунок 11.4. Инструмент создания соединений сетевых устройств

В процессе рисования связей между устройствами вам потребуется выбрать соединяемые интерфейсы и нажать на кнопку Соединить (Рисунок 11.5 и Рисунок 11.6).

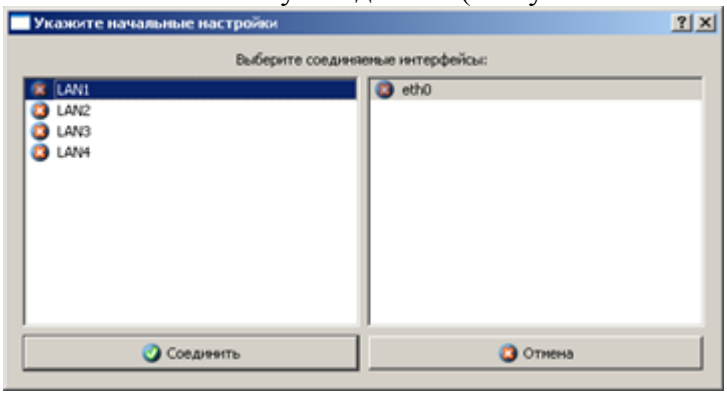


Рисунок 11.5. Выбор начальных настроек соединения

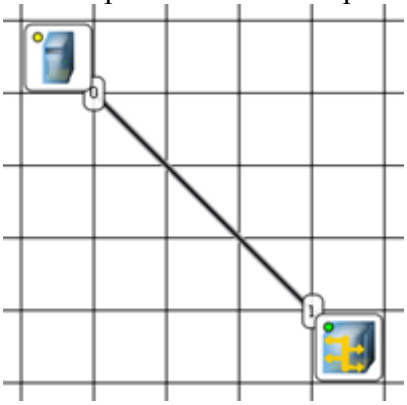


Рисунок 11.6. Соединение устройств произведено

Теперь настроим интерфейс (сетевую карту) на наших ПК ее – Рисунок 11.7 и Рисунок 11.8. Чтобы появилось подобное меню следует щелкнуть правой кнопкой мыши по ПК.

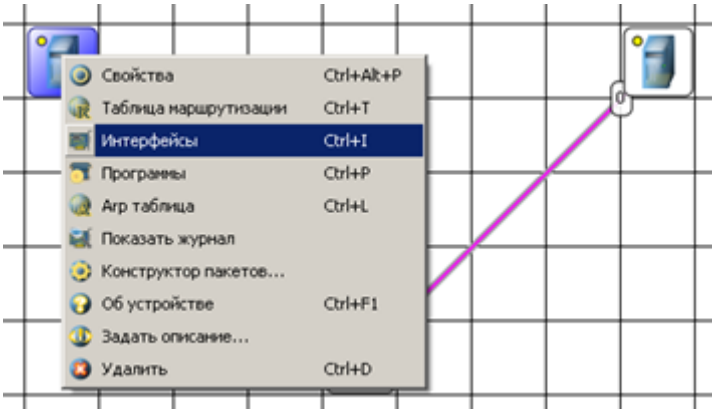


Рисунок 11.7. Добавляем интерфейс

В меню выбираем строчку Интерфейсы и задаем IP адрес и маску ПК. Обратите внимание: после того, как вы напишете 192.168.0.1 маска появляется автоматически. После нажатия на кнопки Применить и ОК – появляется анимация движущихся по сети пакетов информации. Для второго ПК адрес будет 192.168.0.2.

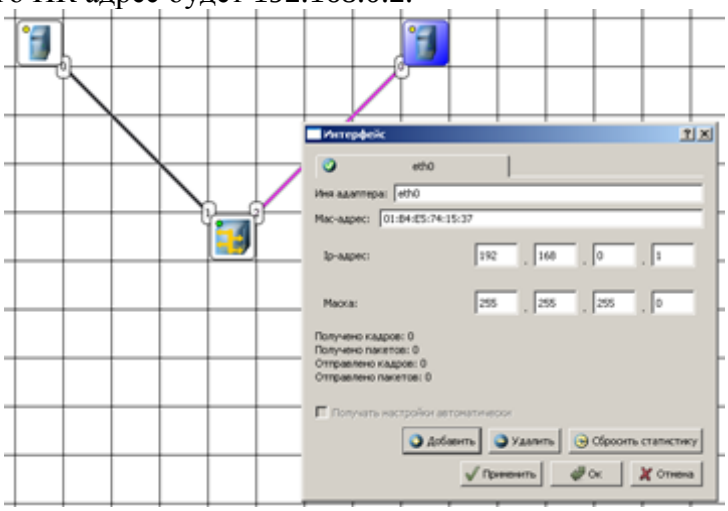


Рисунок 11.8. Вводим IPадрес и маску сети

Все - сеть создана и настроена. Отравляем данные по протоколу TCP (Рисунок 11.9).

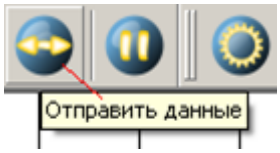


Рисунок 11.9. Кнопка Отправить данные

Для этого щелкаем мышью сначала по одному ПК, а затем – по другому ПК. Выбираем протокол и размер пакета (Рисунок 11.10).

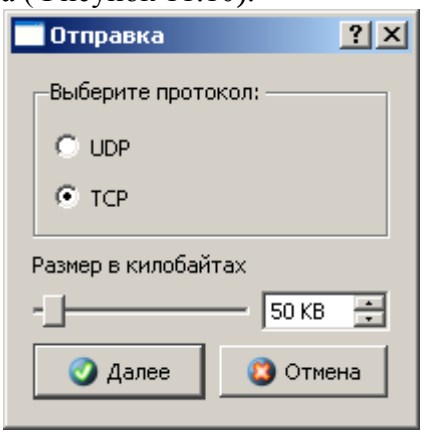


Рисунок 11.10. Выбор протокола

Если вы где-то ошиблись, то появиться соответствующее сообщение, а если все верно – то произойдет анимация движущихся по сети пакетов (Рисунок 11.11).

Рисунок 11.11. Движение пакетов по сети

Подписать устройства на схеме можно инструментом Вставить текстовую надпись (Рисунок 11.12).

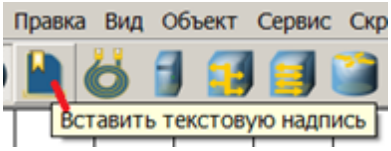


Рисунок 11.12. Инструмент Вставить текстовую надпись

Примечание

По умолчанию каждый ПК имеет одну сетевую карту, но их может быть и несколько. Для того, чтобы добавить для ПК адаптер нужно щелкнуть на нем правой кнопкой мыши и выбрать пункт меню Интерфейсы. В результате откроется следующее диалоговое окно (Рисунок 11.13).

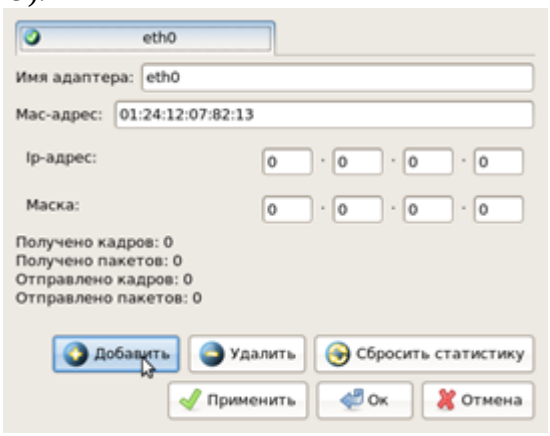


Рисунок 11.13. Диалоговое окно работы с сетевым интерфейсом ПК

Нажимаем на кнопку Добавить, выбираем тип нового адаптера, нажимаем OK, и у нас есть еще один интерфейс. В качестве примера на Рисунок 11.14 изображен ПК, имеющий три сетевых карты.

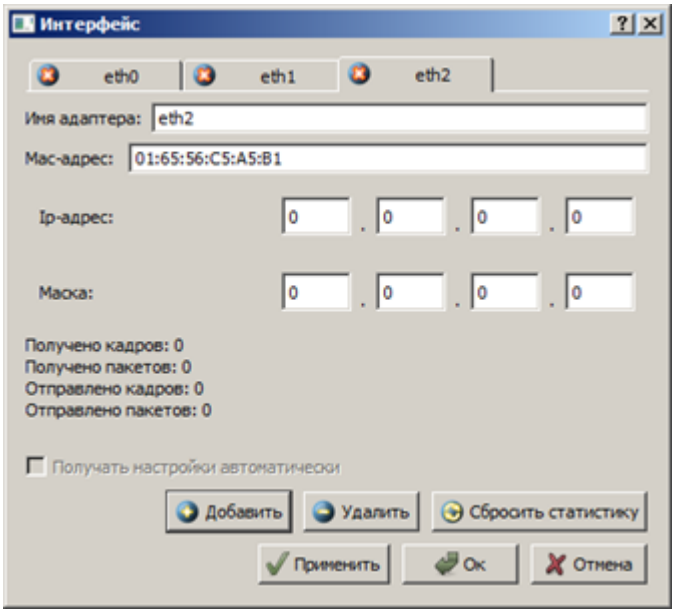


Рисунок 11.14. В этом ПК установлены адаптеры eth0-eth2

Примечание

Каждый сетевой интерфейс (адаптер) имеет свой собственный mac-адрес. В программе NetEmul в строке "Мас-адрес" можно задать новый адрес, но по умолчанию, при создании интерфейса, ему автоматически присваивается этот уникальный номер.

ПРАКТИЧЕСКАЯ РАБОТА № 11.2

Собираем сеть из двух ПК и свитча. Изучаем таблицу коммутации

Время работы: 2 часа

1. Цель работы: Научится работать с программой Cisco Packet Tracer (CPT)

2. Технические средства

2.1 Оборудование: компьютер

2.2 Программное обеспечение: NetEmul,Oracle VM Virtual Box, MS Word.

Постройте схему, показанную на Рисунок 11.15 и настройте ее работу. Отправьте пакет с одного ПК на другой и просмотрите таблицу коммутации свитча.

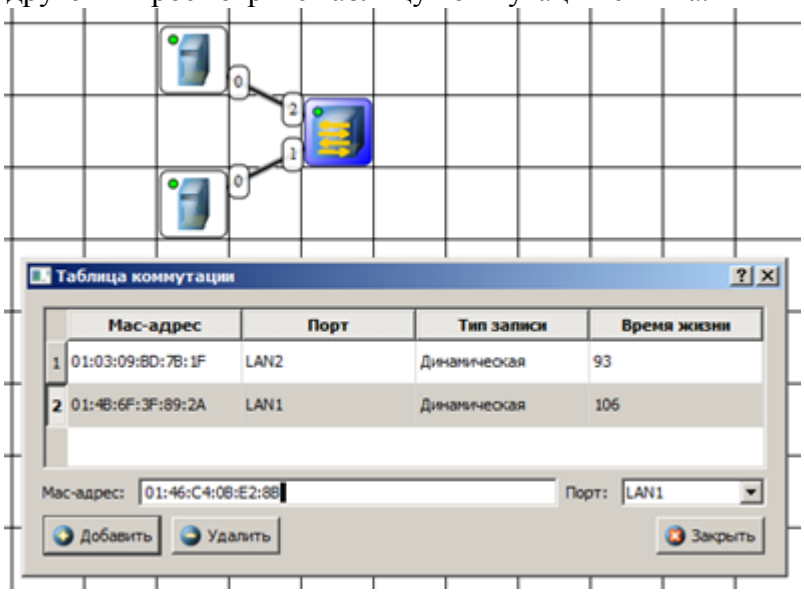


Рисунок 11.15. Схема сети по топологии звезда построена

На схеме:

- красный индикатор означает, что устройство не подключено;
- желтый - устройство подключено, но не настроено;
- зеленый - знак того, что устройство подключено, настроено и готово к работе.

Таблица коммутации устройств вызывается щелчком правой кнопки мыши на коммутаторе (Рисунок 11.16).

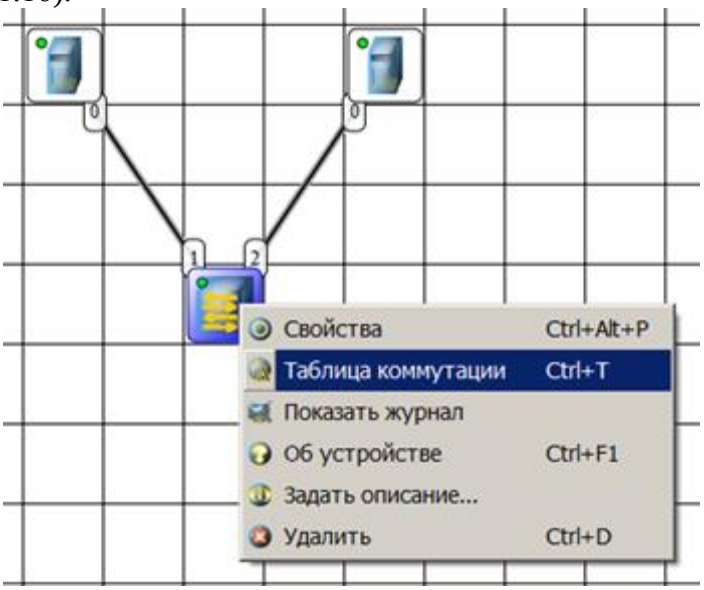


Рисунок 11.16. Комбинация клавиш Ctrl+T вызывает Таблицу коммутации

ПРАКТИЧЕСКАЯ РАБОТА № 11.3

Изучаем в NetEmul сеть из двух подсетей и маршрутизатора

Время работы: 2 часа

1. Цель работы: Научится работать с программой Cisco Packet Tracer (CPT)

2. Технические средства

2.1 Оборудование: компьютер

2.2 Программное обеспечение: NetEmul,Oracle VM Virtual Box, MS Word.

Постройте новую сеть (Рисунок 11.17). Разобьем нашу сеть на 2 подсети. Допустим, у нас есть пул адресов сети. Разобьем его на 2 части: 192.168.0.1-192.168.0.254 (для подсети слева) и 192.168.1.1-192.168.1.254(для подсети справа) с маской 255.255.255.0.

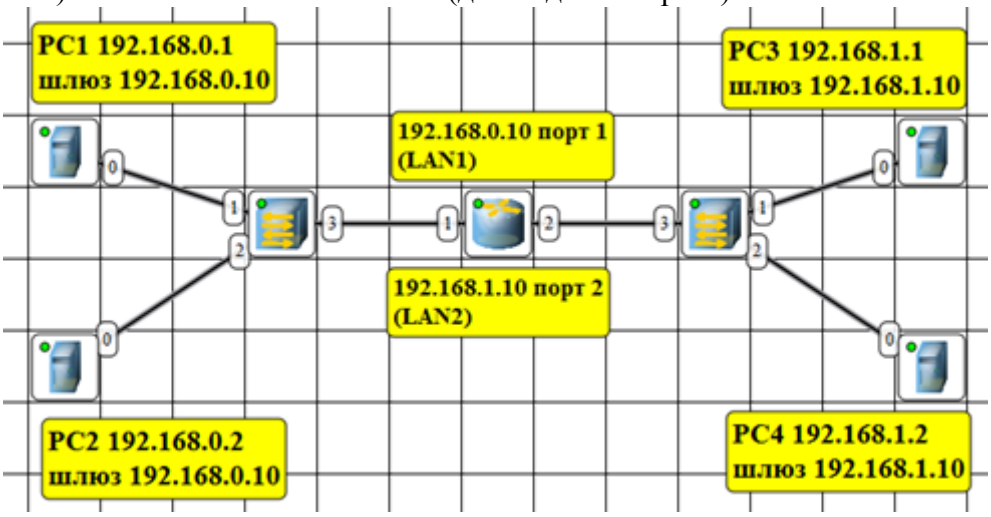


Рисунок 11.17. Вариант сети из двух подсетей на коммутаторах, соединенных маршрутизатором

Примечание

Обратите внимание на то, что число портов у коммутатора можно задавать. У нас на рисунке коммутатор четырехпортовый (Рисунок 11.18).

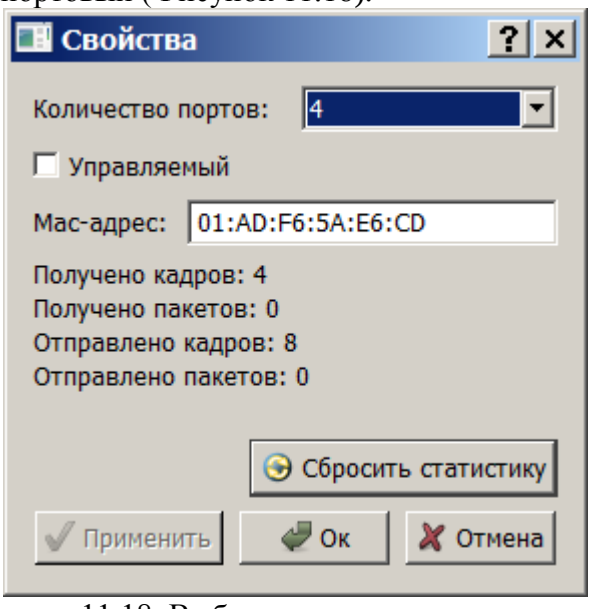


Рисунок 11.18. Выбор числа портов коммутатора

Настройка компьютеров

Для настройки ip-адреса интерфейса ПК и маски подсети из меню правой кнопки мыши открываем окно Интерфейсы и выставляем ip-адреса в соответствии со схемой сети и маску подсети 255.255.255.0. После нажатия на кнопку "Применить" и "ОК", мы можем наблюдать,как индикатор поменял цвет с желтого на зеленый и от нашего устройства, которому сейчас дали адрес, побежал кадр Arp-протокола. Это нужно для того, чтобы выявить, нет ли в нашей сети повторения адресов.

Новый термин

ARP (Протокол определения адреса) — протокол в компьютерных сетях, предназначенный для определения MAC-адреса по известному IP-адресу. Иными словами, ARP представляет собой сетевой протокол, предназначенный для преобразования IP-адресов в MAC-адреса в сетях TCP/IP, что выполняется путем поиска в ARP-таблице. Ниже приведен пример простейшей ARP-таблицы:

IP-адрес	Ethernet-адрес
192.168.0.1	08:00:34:00:2F:C3
192.168.0.2	08:00:5A:71:A7:72
192.168.0.3	08:00:10:98:AC:24

В поле "Описание" из меню правой кнопки мыши необходимозадать имя каждому компьютеру. Оно в дальнейшем будет всплывать в подсказке при наведении мыши на устройство, а также при открытии журнала для устройства заголовок будет содержать именно это описание (Рисунок 11.19).

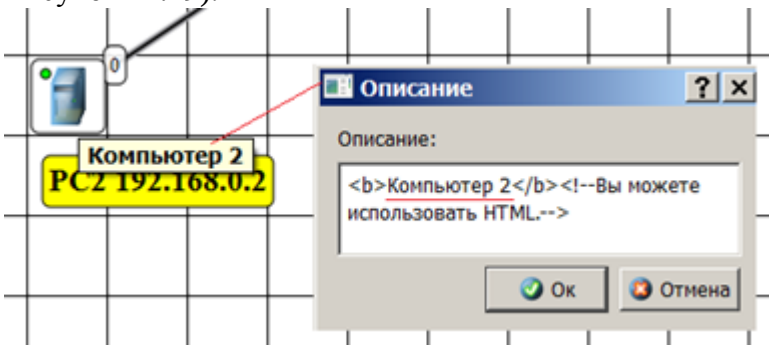


Рисунок 11.19. Пример задания описания устройства

Настройка маршрутизатора

Пока послать сообщения из одной такой подсети в другую мы не можем. Необходимо дать IP адреса каждому интерфейсу маршрутизатора, а на конечных узлах (то есть, на всех ПК) установить шлюзы по умолчанию. В подсети слева настроим 1й порт маршрутизатора LAN1 на адрес 192.168.1.10 (Рисунок 11.20).

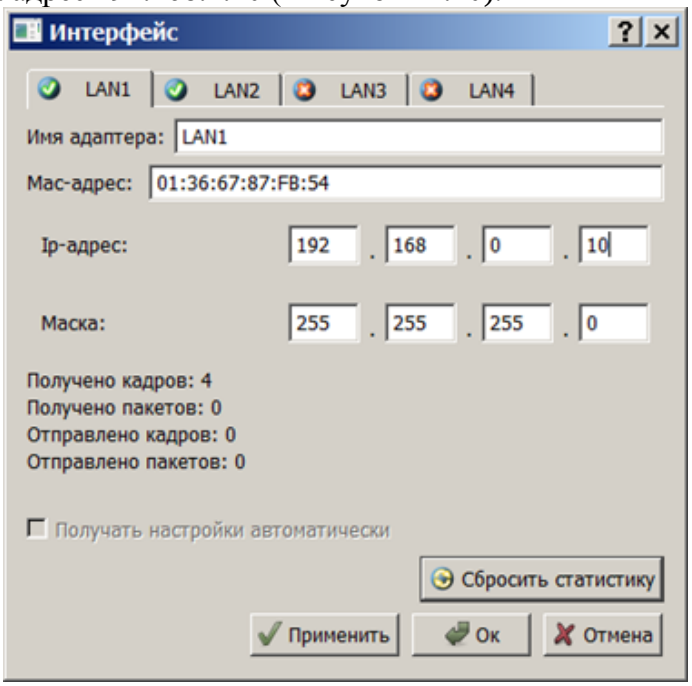


Рисунок 11.20. Настраиваем порт 1 (LAN1) маршрутизатора

Теперь у всех ПК слева в свойствах должен быть шлюз 192.168.0.10. (Рисунок 11.21). Установите флажок Включить маршрутизацию.

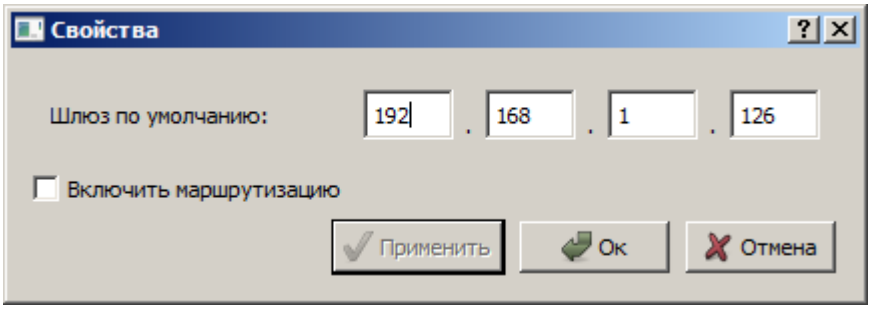


Рисунок 11.21. Настройка шлюза по умолчанию для узлов левой подсети

Аналогично настраиваем порт 2 (LAN2) – Рисунок 11.22.

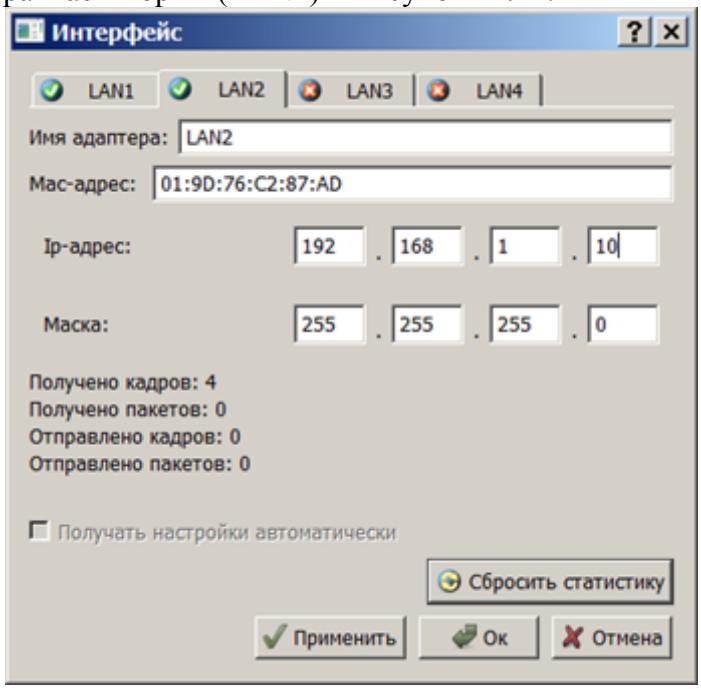


Рисунок 11.22. Настраиваем порт 2 (LAN 2) маршрутизатора

Настраиваем шлюз по умолчанию для узлов правой сети (Рисунок 11.23).

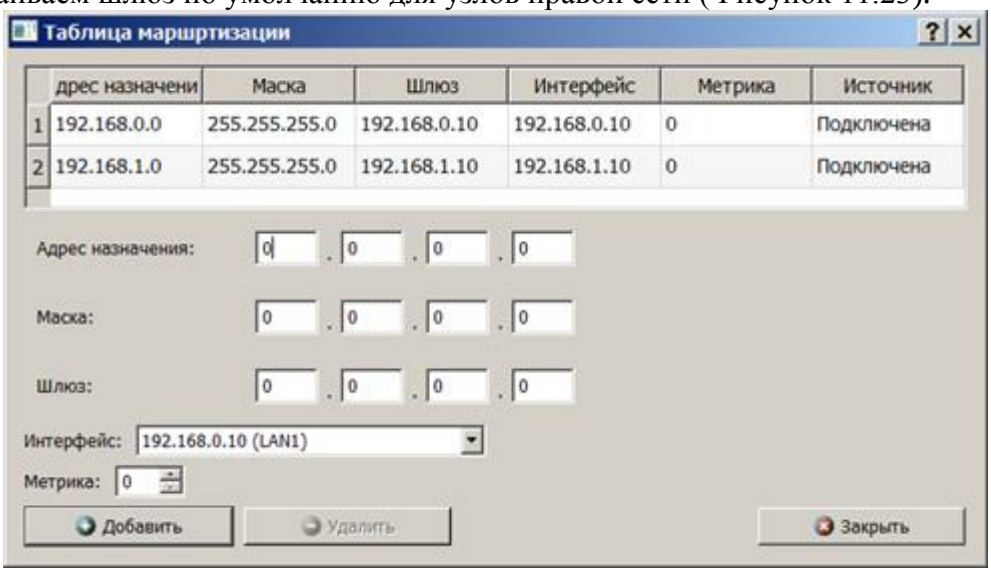


Рисунок 11.23. Настройка шлюза по умолчанию для узлов правой подсети

Шлюзы мы задали и теперь у нас полностью рабочая сеть. Давайте рассмотрим свойства ее объектов.

Наблюдаем свойства маршрутизатора

В таблице маршрутизации видим 2 записи, которые соответствуют нашим подсетям (Рисунок 11.24).

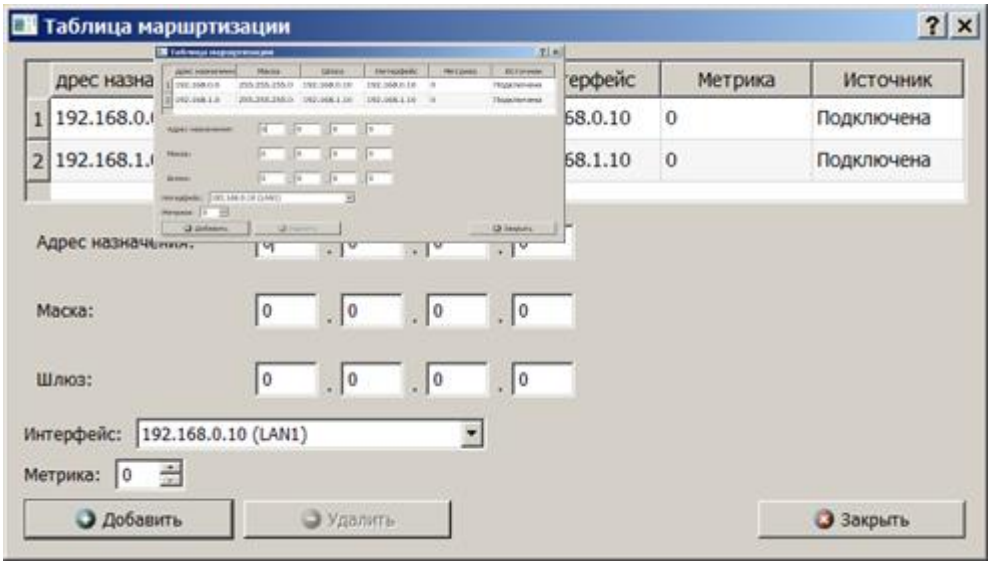


Рисунок 11.24. Таблица маршрутизации маршрутизатора

Тестирование сети

Давайте проверим, насколько правильно функционирует сеть. Для того, чтобы

отправить пакеты, выберите на панели инструментов значок . Мы отправим данные из одной сети в другую. Далее нажимаем на кнопку Отправка и наблюдаем бегущие по сети кадры (Рисунок 11.25).

Рисунок 11.25. Показан ПК, получающий данные

У каждого сетевого устройства в контекстном меню есть пункт "Показать журнал". В процессе отправки пакетов можно открыть этот журнал и увидеть информацию о пакете, пришедшем (или отправленном), и его содержимое – Рисунок 11.26 и Рисунок 11.27.

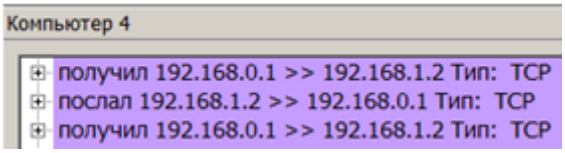


Рисунок 11.26. Часть журнала событий PC4

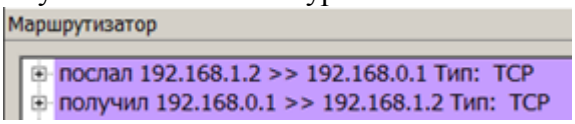


Рисунок 11.27. Часть журнала событий на маршрутизаторе

ПРАКТИЧЕСКАЯ РАБОТА № 11.4

GNS3

Время работы: 2 часа

1. Цель работы: Научится работать с программой Cisco Packet Tracer (CPT)

2. Технические средства

2.1 Оборудование: компьютер

2.2 Программное обеспечение: GNS3, MS Word.

Что такое GNS3? Основные настройки программы

Еще одной альтернативой Cisco Packet Tracer является бесплатная программа GNS3 –Графический Симулятор Сети. GNS3 позволяет моделировать работу реальных сетей, что крайне важно для обучения сетевого персонала. Фактически вы получаете имитацию полноценной компьютерной сети с дорогостоящим оборудованием – на вашем домашнем ПК. С установкой эмулятора GNS3 справиться даже школьник – все шаги по установке программы на ПК можно принять по-умолчанию (Рисунок 11.28).

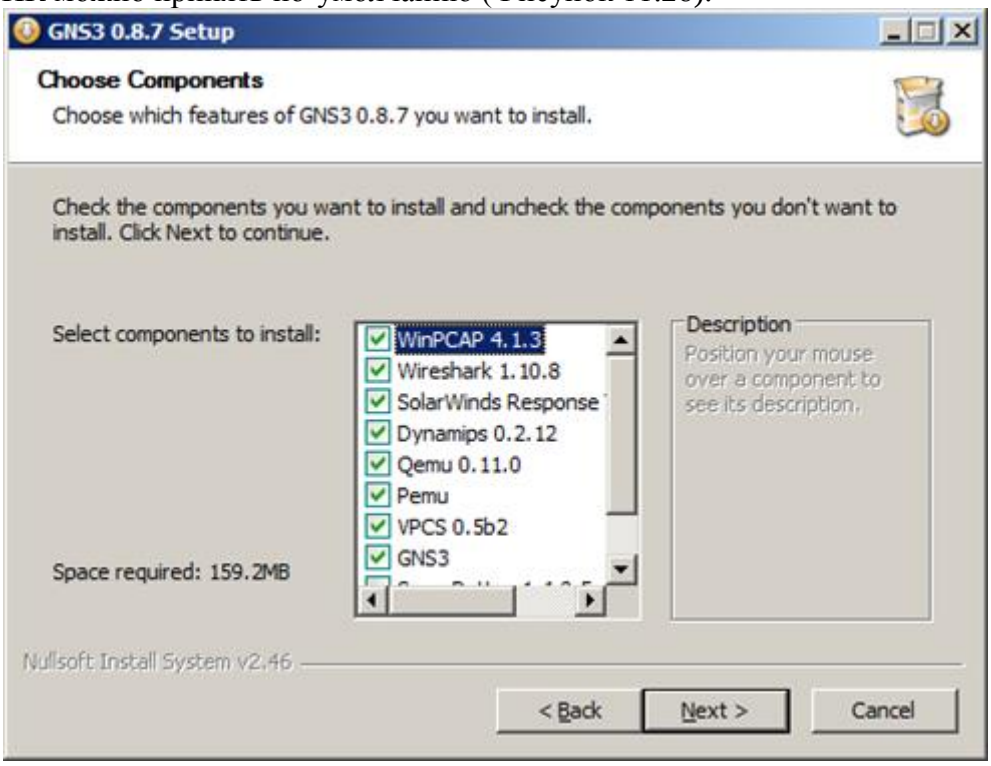


Рисунок 11.28. Соглашаемся с установкой всех по-умолчанию

После первого запуска программы вам будет предложено выполнить три шага (Рисунок 11.29)

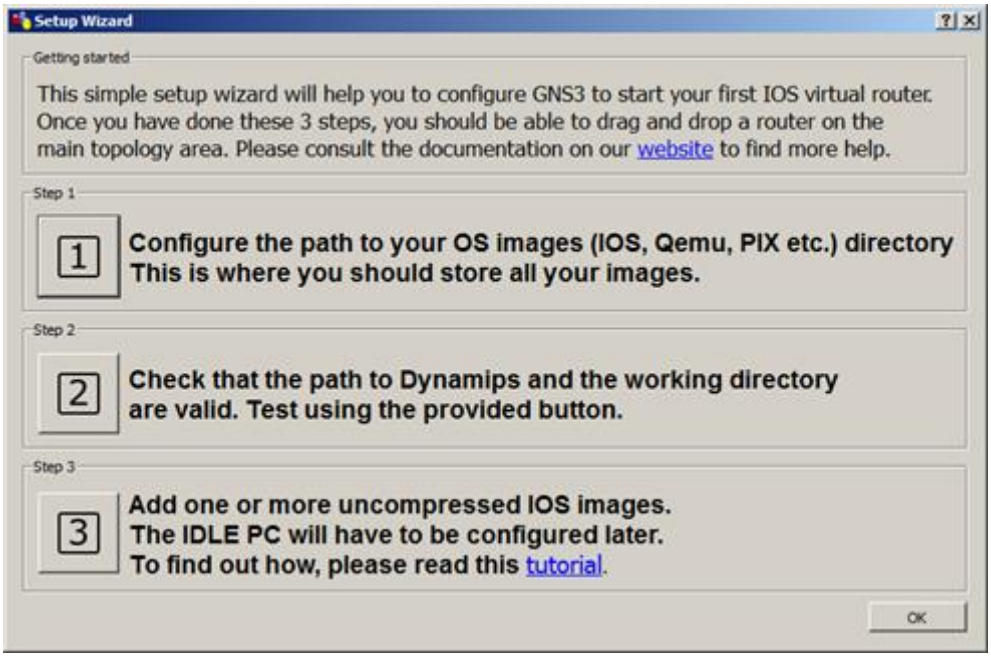


Рисунок 11.29. Окно Мастера при первом запуске программы

Здесь предлагается:

- Сконфигурировать рабочие директории ОС
- Проверить работу Динамипса
- Выделить директорию под IOS-ы устройств, добавить распакованные образы, а значение IDLE PC можно будет рассчитать позднее.

Примечание

По поводу Dynamips замечу, что это программное обеспечение организует виртуализацию маршрутизаторов.

Как видим, при установке CPT проблем меньше, поскольку GNS3 - программа для симуляции сложных компьютерных сетей.

Теперь выполним команду Edit-Preferences и перейдем на вкладку Динамипса – Рисунок 11.30. Здесь имеет смысл создать отдельную директорию, в которой и будут храниться – образы, конфигурации и прочее. Я задал путь C:\Users\vova\TEST.

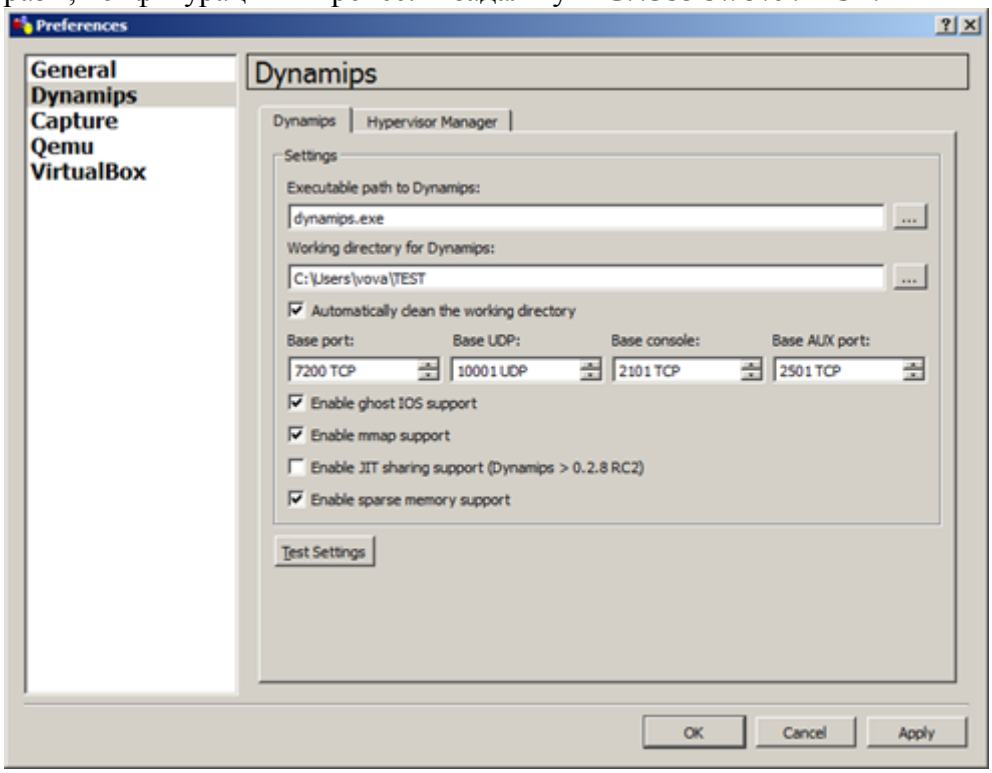


Рисунок 11.30. Окно Preferences

Теперь нужно скачать из Сети образы ios'а для GNS3 и установить их. Выполняем команду Edit-IOS images and hypervisors – Рисунок 11.31. На этом рисунке стрелка указывает кнопку для поиска образа, а кнопка Save сохраняет выбранные вами образы оборудования Cisco в программе.

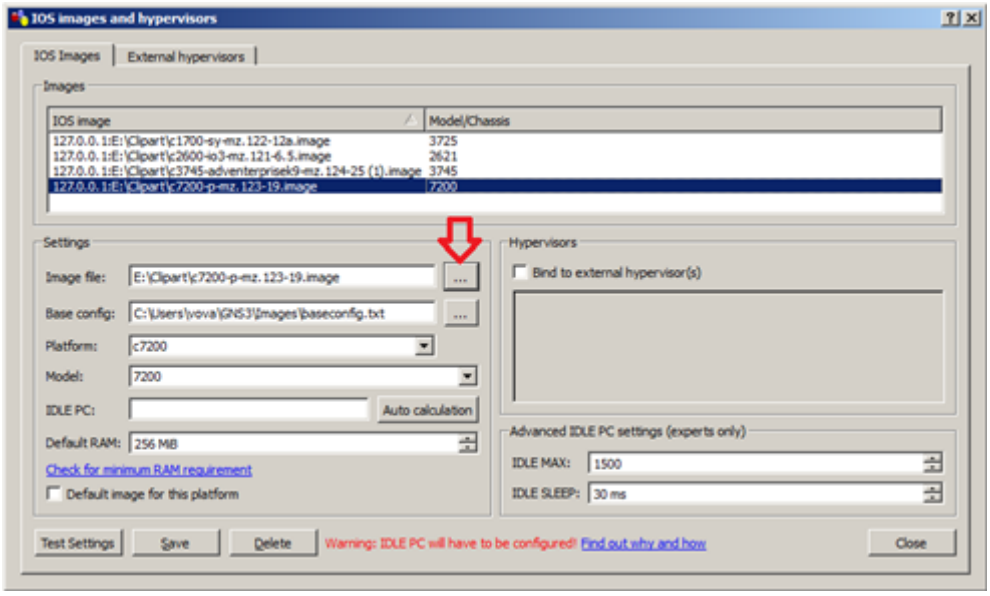


Рисунок 11.31. Добавляем образы для работы в программе

Основные настройки выполнены – можно начинать работать (Рисунок 11.32).

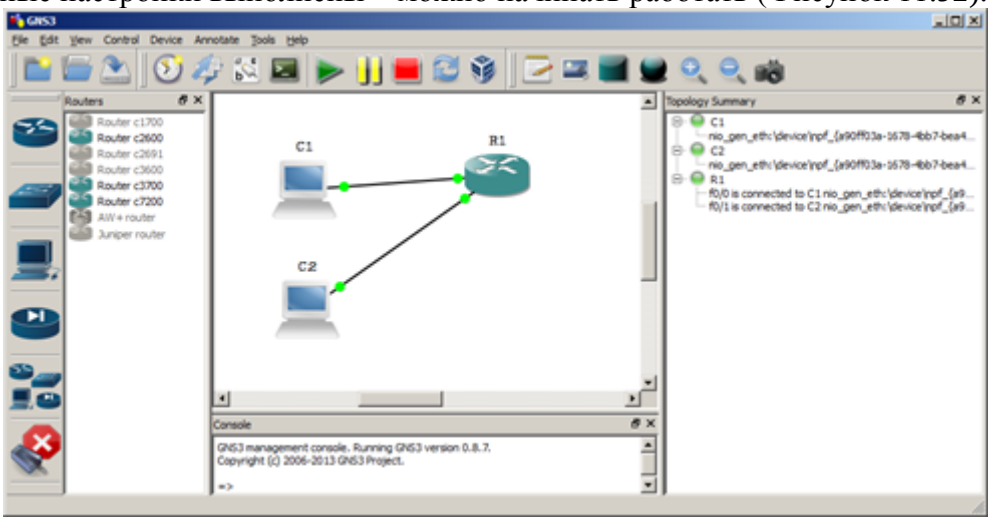


Рисунок 11.32. Первые шаги в программе GNS3

Совет

При желании командой Edit-Preferences с переходом на вкладку General можно русифицировать программу (Рисунок 11.33).

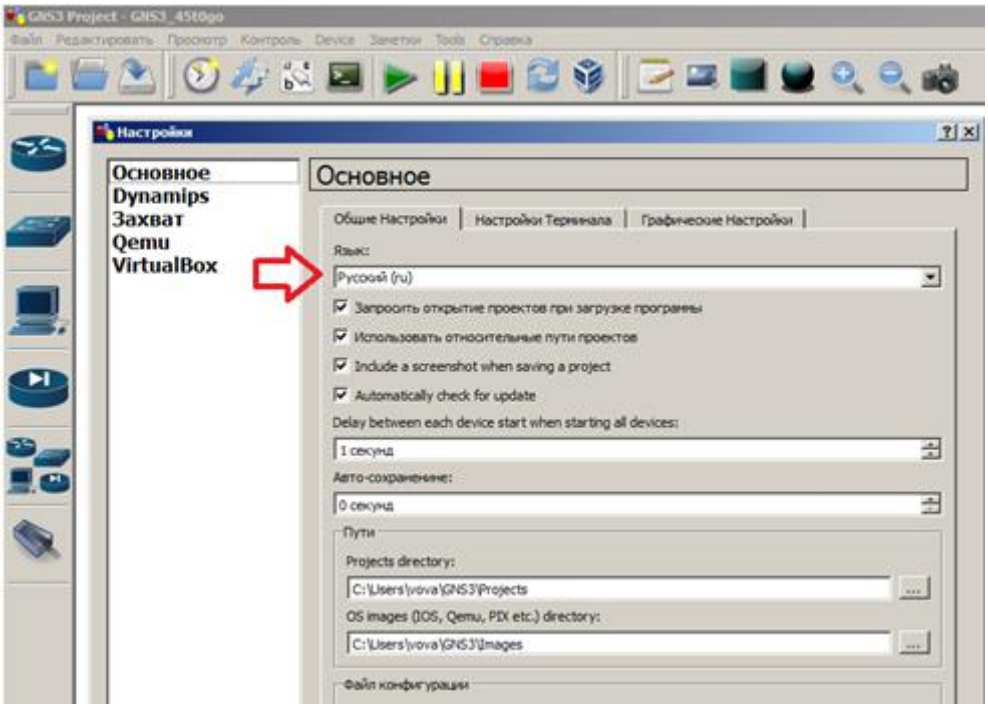


Рисунок 11.33. Интерфейс программы русифицирован

ЗАКЛЮЧЕНИЕ

В ходе выполнения практических работ по учебной практики в рамках междисциплинарного курса МДК 02.01 Инфокоммуникационные системы и сети, обучающиеся овладевают фундаментальными знаниями, профессиональными умениями и навыками деятельности по специальности, опытом творческой и исследовательской деятельности.

ЛИТЕРАТУРА

1 Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы: учебник для вузов. 3-е издание. – СПб: Питер, 2015.

2 Сетевые операционные системы Н. А. Олифер, В. Г. Олифер. – СПб: Питер, 2016.

Приложение А – Требования к отчету

1 Титульный лист

Титульный лист является первой страницей документа, служит источником информации, необходимой для обработки и поиска документа. Приложение Б

2 Содержание

Содержание включает наименование всех практических работ с указанием номеров страниц, с которых начинаются. Слово «СОДЕРЖАНИЕ» записывают в виде заголовка (симметрично тексту) прописными буквами. Наименования, включенные в содержание, записывают строчными буквами, начиная с прописной буквы. Рамка 1 в Приложении В.

3 Общие требования

Изложение текста и оформление документа выполняют в соответствии с требованиями настоящего стандарта. Страницы текста, иллюстрации и таблицы должны соответствовать формату А4.

Шрифт - Times New Roman, 14 кегль. Цвет шрифта – черный. Полужирный шрифт не применяется. В таблицах с большим объемом текста допускается шрифт - Times New Roman, 12 кегль, Междустрочный интервал основного текста – 1,5. Абзацный отступ 1,25 от текста. Цвет шрифта – черный.

Текст документа следует печатать, соблюдая следующие размеры полей: правое – 10 мм, верхнее – 15 мм, и нижнее – 30 мм, левое – 25 мм.

Каждая практическая работа начинается с нового листа. Рамка 2 приложение В, должна присутствовать на каждой странице.

Если заголовок состоит из двух предложений, его разделяют точкой. Переносы слов в заголовках не допускаются.

Иллюстрации (следует располагать в документе непосредственно после текста, в котором они упоминаются впервые или на следующей странице. На все иллюстрации должны быть даны ссылки в документе. Иллюстрации, за исключением иллюстрации приложений, следует размещать посередине листа, нумеровать арабскими цифрами в пределах раздела.

Номер иллюстрации состоит из номера раздела и порядкового номера иллюстрации, разделенных точкой. Например: Рисунок 4.1.

Иллюстрация, слово «Рисунок» и его наименование располагают посередине строки.

4 Требования к оформлению практической работы

Заголовок должен соответствовать номеру выполняемой практической работы. В отчете должно присутствовать название практической работы, цель, программное обеспечение, код программы и результат.

Приложение Б - Титульный лист

государственное автономное профессиональное образовательное учреждение Чувашской Республики «Межрегиональный центр компетенций – Чебоксарский электромеханический колледж» Министерства образования и молодежной политики Чувашской Республики

Дисциплина _____

ОТЧЕТ

по учебной практике

_____

_____

ПР.ПР1-15.15.01.02.ОТ

Выполнил студент ____курса, группы _____

_____
(Фамилия И. О.)

_____
(подпись) (чч.мм.гггг)

Преподаватель _____
(Фамилия И. О.)

Зачтено _____
(чч.мм.гггг)

Подпись _____ _____
(подпись) (расшифровка подписи)

2017

Приложение В – РАМКИ

					НОМЕР ДОКУМЕНТА			
Изм.	Лист	№ докум.	Подпись	Дата				
Разраб.		Ф.И.О.			Название работы	Лит.	Лист	Листов
Провер.		Ф.И.О.					3	
Реценз.		Ф.И.О.				МЦК-ЧЭМК		
Н. Контр.		Ф.И.О.						
Утверд.		Ф.И.О.						

					НОМЕР ДОКУМЕНТА	Лист
Изм.	Лист	№ докум.	Подпись	Дата		