МИНИСТЕРСТВО ВЫСШЕГО ОБРАЗОВАНИЯ, НАУКИ И ИННОВАЦИЙ РЕСПУБЛИКИ УЗБЕКИСТАН

«ТАШКЕНТСКИЙ ИНСТИТУТ ИНЖЕНЕРОВ ИРРИГАЦИИ И МЕХАНИЗАЦИИ СЕЛЬСКОГО ХОЗЯЙСТВА» НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ

Э.О.БОЗОРОВ, М.М.ИСМАИЛОВ, М.Ш.АБДУЛЛАЕВ

ОСНОВЫ НАДЕЖНОСТИ И БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ

УЧЕБНОЕ ПОСОБИЕ

Ташкент 2024

UDC: 004.056

Э.О.Бозоров, М.М.Исмаилов, М.Ш.Абдуллаев. Основы информационных технологий и информационной безопасности: Учебное пособие / – Т.: Республика Узбекистан, 2024. – 135 ст.

В данном учебном пособии предусмотрены практические занятия по «Основам информационных технологий и информационной безопасности», работе с сетевыми симуляторами и процессами обмена информацией между двумя и более компьютерами с использованием локального симулятора «Cisco Packet Tracer» а формирование навыков проектирования глобальных сетей и настройки параметров безопасности является основной целью. При этом на каждой «Практической работе» студентам даются задания, которые они должны выполнить самостоятельно.

Методическое указание предназначено для студентов всех очных курсов бакалавриата «60610200 – Информационные системы и технологии».

UDC: 004.056

Р е ц е н з е н т ы :

Рахматов А.Ю. - доцент кафедры «Электроснабжение и возобновляемые источники энергии» Национального исследовательского университета «Ташкентский институт инженеров ирригации и механизации сельского хозяйства», кандидат технических наук.

Уринов Ш.Р. - Профессор кафедры “Экономика и компютерного инжиниринга” института ISFT “International School of Finance Technology and Science”, д.т.н. (DSc), профессор.

Введение

Информационные системы играют важную роль в поддержке принятия решений, операций и коммуникации в современных организациях. Обеспечение надежности и безопасности этих систем имеет решающее значение для обеспечения их эффективности, целостности и устойчивости к таким рискам, как системные сбои, кибератаки и несанкционированный доступ.

Надежность информационных систем означает способность информационной системы безошибочно и непрерывно выполнять свои задачи. Надежные системы сокращают время простоя информационных систем и поддерживают целостность данных. Ключевые факторы, влияющие на надежность: 1. Архитектура системы. Хорошо спроектированная архитектура предотвращает возникновение узких мест и сбоев системы. 2. Резервирование: системы резервного копирования, механизмы балансировки нагрузки и отказоустойчивости. 3. Мониторинг и обслуживание: регулярная диагностика, обновления и профилактический ремонт. 4. Масштабируемость. Системы предназначены для обработки растущих рабочих нагрузок без ущерба для производительности.

Безопасность информационных систем включает защиту конфиденциальности, целостности и доступности информационных систем от угроз. Основные принципы безопасности: 1. Конфиденциальность: обеспечение доступа к информации только авторизованным пользователям. 2. Целостность: защита данных от несанкционированной модификации. 3. Доступность: обеспечение доступности информации и ресурсов авторизованным пользователям при необходимости.

Данное образовательное пособие по информационной безопасности полностью охватывает основные аспекты использования информационных технологий, а также методы и средства обеспечения информационной безопасности.

Информационная безопасность защищает все формы цифровой и физической информации. Кибербезопасность защищает все формы цифровых данных, включая компьютеры, портативные устройства, облако и сети, и может рассматриваться как часть информационной безопасности.

Особое внимание уделяется защите информации от различных угроз, таких как кибератаки, утечка данных, социальная инженерия и другие виды киберпреступлений.

Данное учебное пособие предназначено для студентов и преподавателей, интересующихся информатикой и информационной безопасностью, изучающих области информационных систем и технологий.

Практическая работа № 1

Сетевое оборудование и монтаж.

Цель работы: ознакомиться с основными компонентами сетевого устройства, их назначением и характеристиками. Получить представление о стандартах проектирования и установки кабельной системы. Научиться подключать отдельный персональный компьютер к локальной сети (LAN), изучить топологию и разработать навыки организации LAN для малого отдела. Освоить простейшие методы работы в сетевой среде и команды операционной системы, используемые для этого.

1. Сетевое оборудование.

Для эффективной работы предприятий компьютеры, телефоны и периферийные устройства объединяются в единую сеть. Это позволяет обмениваться данными, пользоваться принтерами и доступом в Интернет. Эффективность подключения, включая скорость и стабильность, в значительной степени определяется характеристиками сетевого оборудования.

Оборудование делится на пассивное и активное. Пассивные устройства обязаны соответствовать установленным стандартам, тогда как активные устройства должны обеспечивать функционирование сети на различных скоростях и поддерживать ключевые сетевые протоколы и стандарты.

При проектировании кабельной структуры важно обеспечить соответствие всех её элементов установленным стандартам. Основные стандарты для кабельных систем включают:

• Международный стандарт ISO/IEC 11801 'Generic Cabling for Customer Premises' (доступен на www.iso.ch, www.iec.ch).

• Европейский стандарт EN 50173 'Information Technology – Generic Cabling Systems'.

• Американский стандарт ANSI/TIA/EIA 568-B 'Commercial Building Telecommunication Cabling Standard' (информация доступна на www.tiaonline.org, www.eia.org).

Стандарты устанавливают требования к параметрам среды передачи, коннекторам, линиям и каналам, включая максимально допустимую длину, топологию и характеристики функциональных компонентов системы.

1.2. Структурированная кабельная система (СКС).

Данная иерархическая кабельная система предназначена для передачи электрических или оптических сигналов внутри здания. Она разделена на структурные подсистемы и включает в себя такие компоненты, как кабели, коннекторы, панели, шкафы и сопутствующее оборудование.

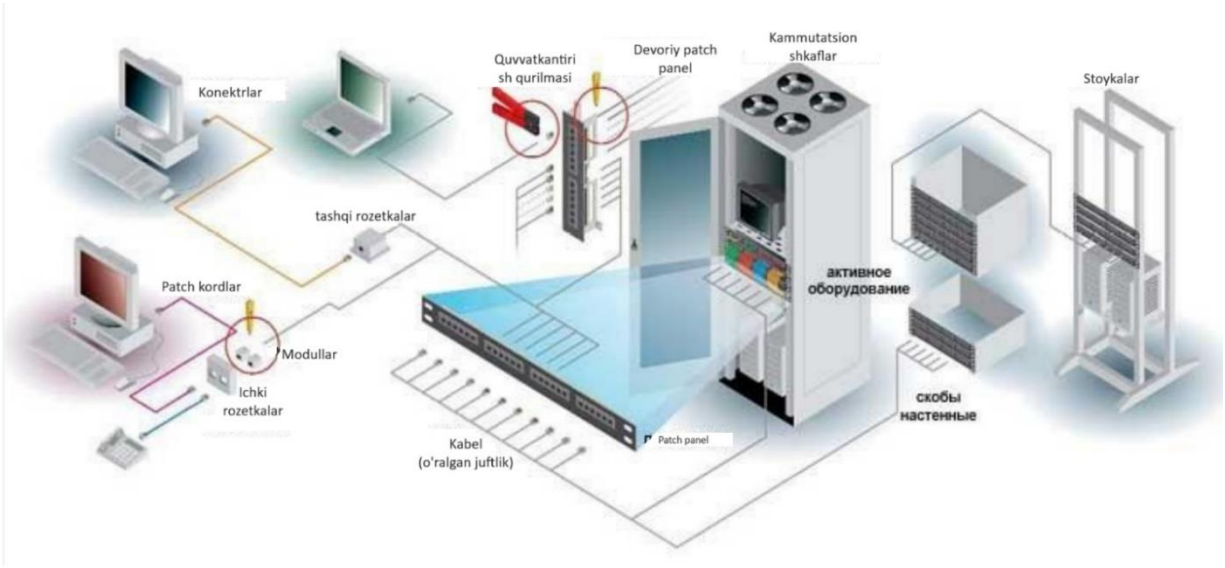


Рисунок - 1.1. Иерархическая кабельная среда в малой сети.

СКС объединяет удобство использования, качество и надежность передачи данных. Она построена таким образом, что каждый интерфейс (или точка подключения) предоставляет доступ ко всем ресурсам сети. Кабели проложены от компьютера до распределительных пунктов и подключены через основные линии топологии.

1.2.1. Пассивное сетевое оборудование.

Оборудование, которое не требует потребления электроэнергии, называется пассивным. К пассивным элементам относятся розетки, кабели, разъемы, патч-панели и другие компоненты. Ключевыми элементами этого типа оборудования являются электрические кабели и разъемы, которые на них установлены.

1.2.1.1. Силовой кабель и вилка.

При установке кабельных систем часто применяется неэкранированная витая пара пятой категории (UTP 5 «cat»). Этот кабель состоит из нескольких пар медных проводов, которые покрыты пластиковым оболочкой. Каждая пара проводов скручена, что снижает взаимные помехи. Изоляция проводов окрашена в различные цвета, включая:

- бело-зеленый;
- зеленый;
- бело-оранжевый;
- оранжевый;
- бело-синий;
- синий;
- бело-коричневый;
- коричневый.

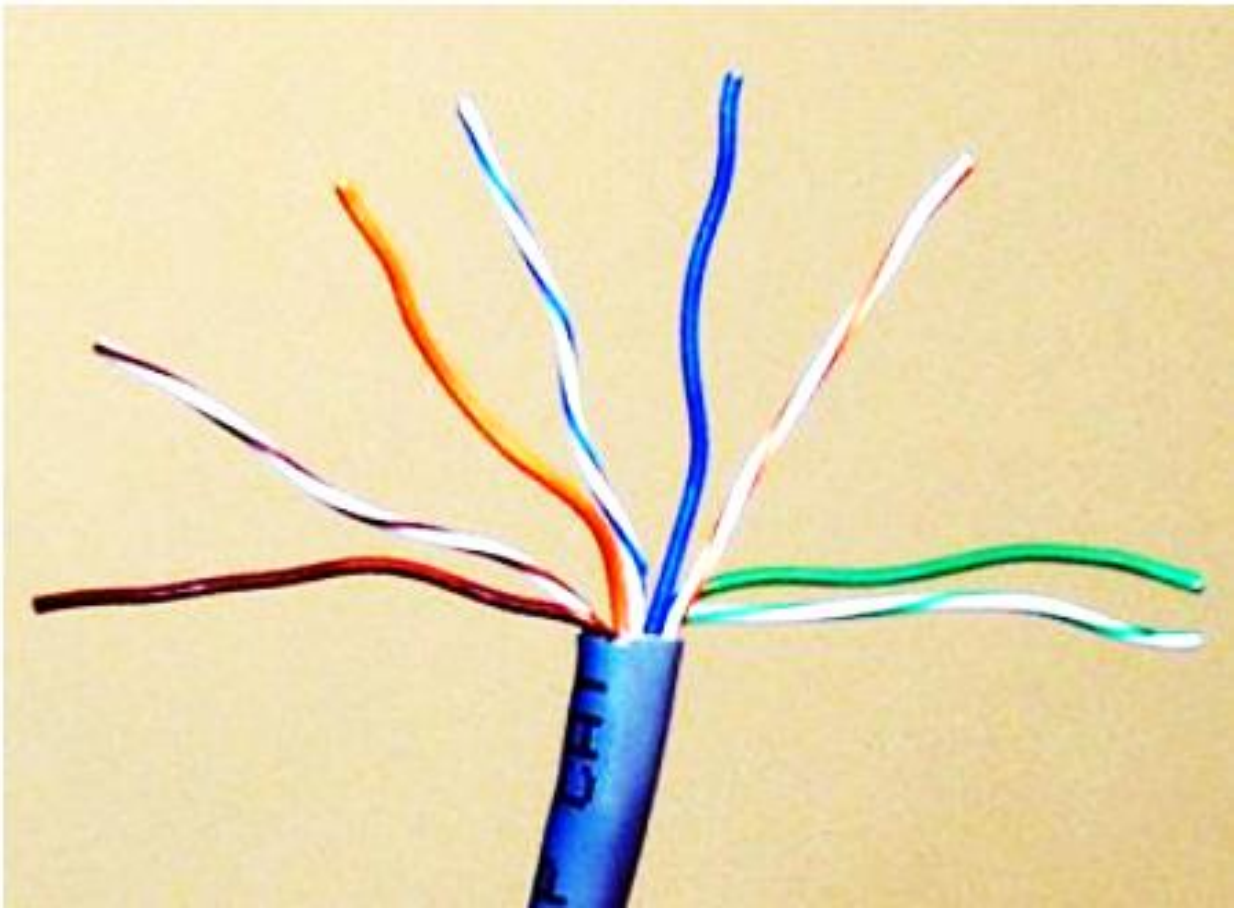


Рисунок - 1.2. Неэкранированный витой парный кабель.

Провода одного цвета формируют 4 пары следующим образом:

- Пара 1: бело-зеленый и зеленый;
- Пара 2: бело-оранжевый и оранжевый;
- Пара 3: бело-синий и синий;
- Пара 4: бело-коричневый и коричневый.

Для подключения витой пары применяются разъемы RJ-45, которые монтируются на концах кабеля. Разъем RJ-45 имеет восемь контактов и фиксируется на кабеле с помощью специального инструмента.

1.2.1.2.Коммутационная панель (кросс-панель, патч-панель)

Это панель, оснащенная несколькими разъемами на передней части и контактами на задней стороне для надежного подключения к кабелям.

Основные характеристики кросс-панелей включают:

- метод монтажа (на стену или на стойку);
- количество портов (обычно от 12 до 48);
- категория (3, 5e, 6);
- экранированные и неэкранированные.

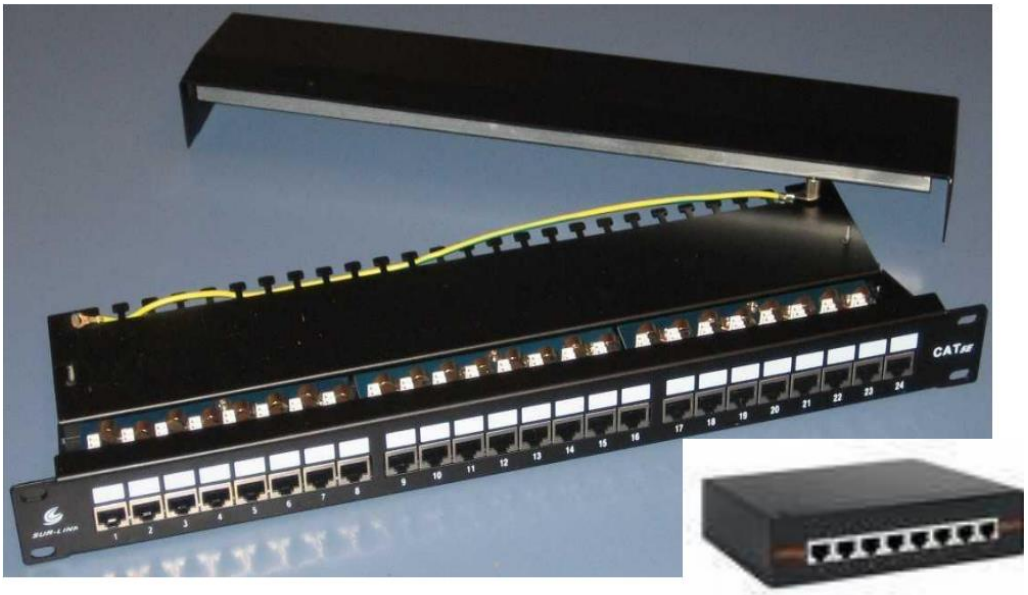


Рисунок - 1.3. Кросс-панель для крепления на стену и в стойку.

Панели могут использоваться двумя способами:

В первом варианте патч-панель служит точкой соединения между портами активного сетевого оборудования (АСО) и портами рабочих станций через кабели горизонтальной подсистемы СКС. Соединение осуществляется от панели к портам АСО с помощью патч-кордов.

Во втором варианте используются так называемые двойные патч-панели: одна из них подключается к портам АСО, а другая — к портам рабочих станций. Связь между панелями осуществляется через патч-корды.

1.2.1.3. Коммутационный кабель (патч-корд).

Коммутационный кабель, также известный как патч-корд (от англ. patching cord — соединительный шнур), представляет собой электрический кабель, предназначенный для соединения одного электронного устройства с другим.

Рисунок - 1.4. Коммутационный кабель.

Коммутационный кабель, или патч-корд, может иметь различную длину и быть оснащен разъемами (коннекторами) как на одном, так и на обоих концах.

Патч-корды классифицируются по нескольким типам: телефонные (RJ11 и RJ12), компьютерные (RJ45), а также для межсоединений 110-го типа. Они могут быть неэкранированными (UTP) или экранированными (STP), а также обычными или перекрестными.

Патч-корды применяются для различных задач, таких как подключение персонального компьютера к розетке, соединение двух патч-панелей и другие аналогичные цели.

Основное отличие патч-корда от внутреннего кабеля заключается в том, что патч-корд использует многожильный провод, в то время как внутренний кабель обычно имеет цельный провод. Это приводит к снижению передающих характеристик патч-корда, но повышает его гибкость и уменьшает минимально допустимый радиус изгиба.

Патч-корды используются для подключения персональных компьютеров к розеткам, соединения двух патч-панелей, а также для других задач, требующих гибкого соединения оборудования.

Основное отличие коммутационного шнура от внутреннего кабеля состоит в использовании многожильного провода вместо цельного. Хотя это приводит к снижению передающих характеристик, оно увеличивает гибкость шнура и уменьшает минимально допустимый радиус изгиба.

1.2.1.4. Телефонные и компьютерные розетки.

Они представляют собой важный элемент системы кабельной связи (СКС) и имеют пластиковый корпус с встроенными разъемами для телефонов (RJ12) или компьютеров (RJ45).

Патч-корды подключаются к розеткам с фронтальной стороны, в то время как на задней стороне розеток расположены контакты, которые обеспечивают надежное соединение с кабелями и электрическое соединение с разъемами.

Телефонные и компьютерные розетки служат для подключения терминальных устройств, таких как телефонные аппараты и сетевые карты компьютеров, к локальным телефонным и компьютерным сетям через патч-корды.

1.2.2. Активное сетевое оборудование.

Активное сетевое оборудование охватывает такие устройства, как сетевые адаптеры, хабы, коммутаторы, маршрутизаторы, серверы печати и другие компоненты сети.

1.2.2.1. Сетевые адаптеры.

Для подключения к LAN компьютеру необходим сетевой адаптер. Этот адаптер должен иметь драйвер, который обеспечит его корректное функционирование с операционной системой Windows. Для проверки совместимости сетевого адаптера с Windows OS следует ознакомиться со списком совместимости оборудования (HCL), размещённым на сайте

Microsoft по адресу http://www.microsoft.com/hcl/. В данном списке указаны адаптеры, которые прошли тестирование на совместимость с данной операционной системой.

Хотя это не является обязательным, использование одинаковых сетевых карт при создании LAN может упростить настройку сети. Все сетевые карты выполняют основную функцию — соединение компьютеров в сеть. Тем не менее, более дорогие модели могут обладать дополнительными функциями и технологиями, которые отсутствуют у более простых и дешёвых карт.

Риснуок - 1.5. Устройство сетевой карты.

BootRom - это специализированный чип, обеспечивающий возможность загрузки компьютера через сеть. При правильно настроенной системе компьютер может функционировать без жесткого диска. Опция сетевой загрузки настраивается через BIOS компьютеров, которые поддерживают эту функцию. В более недорогих сетевых картах чип BootRom либо отсутствует, либо присутствует только разъем для него без самого чипа.

Wake-on-LAN (WOL) - это функция, которая позволяет удаленно включать компьютер через сеть. Для использования WOL компьютер должен быть оснащен блоком питания ATX. В BIOS необходимо активировать опцию включения компьютера по запросу с сетевого порта, к которому подключена сетевая карта (обычно PCI). Если сетевая карта подключается через разъем WOL на материнской плате, потребуется использовать трехжильный кабель. Если сетевая карта встроена в материнскую плату, последний шаг обычно не требуется.

1.2.2.2. Хабы и коммутаторы.

Вы можете подключить компьютеры с помощью хаба или коммутатора. Хотя на первый взгляд они кажутся идентичными, на самом деле между ними существуют значительные различия.

Hub. Когда пакет данных поступает на хаб из сетевой карты, хаб лишь разделяет и усиливает сигнал, чтобы все устройства в сети могли его получить. Однако только та сетевая карта, к которой адресован пакет, будет его принимать. В результате, при одновременной активности нескольких пользователей скорость сети заметно падает. Сегодня большинство компаний прекратили производство хабов и переключились на более эффективные коммутаторы (Switch), которые лучше управляют сетевыми потоками и повышают общую производительность сети.

Рисунок - 1.6. Сетевой коммутатор.

Switch (коммутатор). В отличие от хаба, коммутатор (Switch) анализирует информацию о том, откуда и куда направляется пакет данных, и подключает только те устройства, которые участвуют в передаче этого пакета, оставляя другие каналы свободными. Это делает коммутатор более эффективным, особенно в сетях с большим числом пользователей, поскольку он значительно увеличивает скорость передачи данных. Внешне коммутатор почти не отличается от хаба.

1.2.2.3. Сервер печати.

Сервер печати — это устройство, которое подключается к локальной сети и к принтеру с интерфейсом LPT или USB (включая персональный компьютер), обеспечивая возможность централизованного управления печатью.

Рисунок - 1.7. Сервер печати HP JetDirect 620N.

1.3. Установка кабельной системы и подключение сетевого борудования.

1.3.1. Правила установки кабельной системы

Основные правила для установки кабельной системы включают:

- Избегайте растяжения кабеля во время монтажа.
- Радиус изгиба кабеля должен составлять не менее 10 диаметров кабеля.
- Удаляйте оболочку кабеля только на необходимую длину для установки.
- Сохраняйте целостность витых пар кабеля как можно ближе к месту установки, чтобы минимизировать взаимные помехи. Не перекручивайте витые пары, которые потеряли скрутку при установке, так как это может ухудшить производительность.
- LAN-кабели следует размещать вдали от электрических проводов (220 В), люминесцентных ламп, силовых трансформаторов и других источников сильных электромагнитных полей, чтобы избежать шумов и ухудшения качества передачи сигнала.

1.3.2. Установка разъема RJ-45.

Монтаж разъёма RJ-45 осуществляется путём обжима с использованием специального инструмента в соответствии со стандартами T568A или T568B.

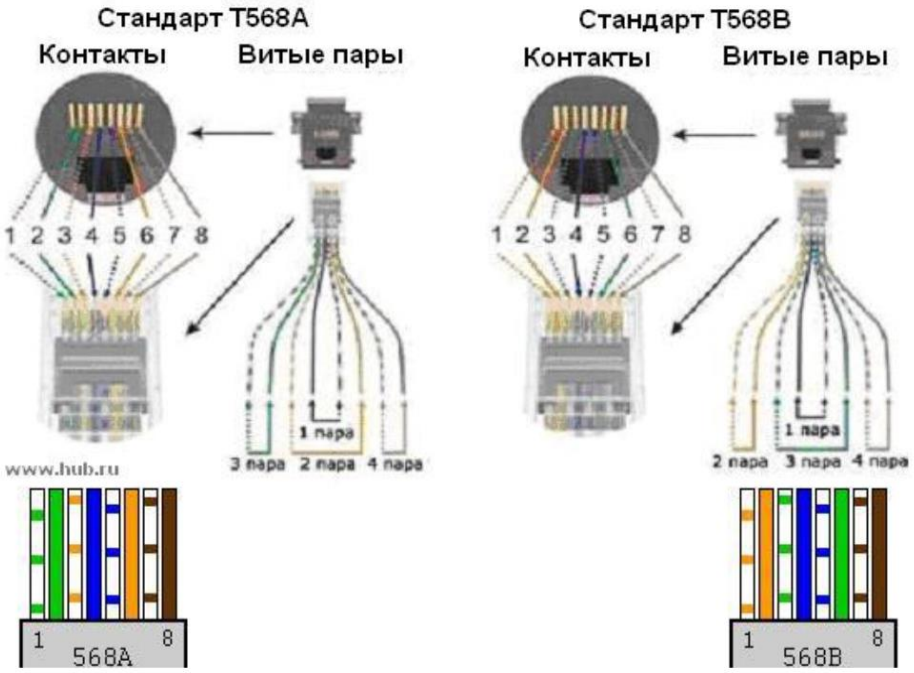


Рисунок - 1.8. Стандарты подключения RJ-45.

Способы установки определяются типом подключения, и выделяют два основных варианта:

- Компьютер подключается к сетевому порту или свитчу с помощью кабеля, выполненного по стандарту T568B.
- Для соединения между коммутаторами или узловыми точками, например «hub - hub», «switch - switch» или «hub - switch», используется кабель с перекрестной (Crossover) либо прямой (Uplink) разводкой. Один конец кабеля выполнен по стандарту T568A, а другой — по стандарту T568B. Подробную информацию о способе обрезки кабеля можно найти в приложении.

1.3.3. Подключение сетевого оборудования.

Коммутаторы и хабы подключаются к локальной сети схожим способом. При использовании нескольких коммутаторов они соединяются между собой посредством UTP-кабеля с перекрестной разводкой (T568A и T568B). Длина такого кабеля должна быть не менее 0,5 метра.

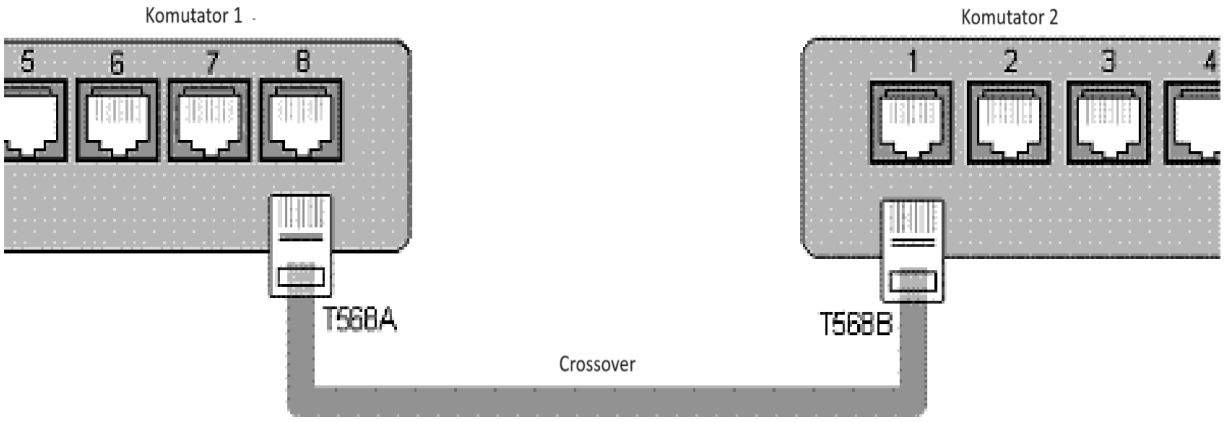


Рисунок - 1.9. Для подключения коммутаторов используется кабель с перекрёстной проводкой в соответствии с комбинацией стандартов T568A и T568B.

Многие модели коммутаторов оснащены дополнительным портом «Uplink», который совмещён с одним из стандартных портов и имеет перекрёстную проводку по стандарту T568A. Этот порт позволяет подключить второй коммутатор с помощью обычного кабеля (T568B - T568B).

Рисунок - 1.10. Использование порта «Uplink» для подключения кабеля T568B - T568B.

На диаграмме представлено применение дополнительного порта «Uplink», который соединён с портом №8. В результате, порт №8 следует оставлять незанятым.

Современные коммутаторы оснащены функцией автоматического определения типа кабеля. Каждый порт коммутатора способен самостоятельно идентифицировать стандарт подключенного кабеля и выбрать соответствующий режим работы. Эта функция значительно упрощает работу сетевого администратора.

Чтобы подключить компьютер к локальной сети (LAN), выполните следующие шаги:

- Установите сетевой адаптер, поддерживающий технологию Ethernet.
- Подключите компьютер к сетевому оборудованию с помощью сетевого кабеля.

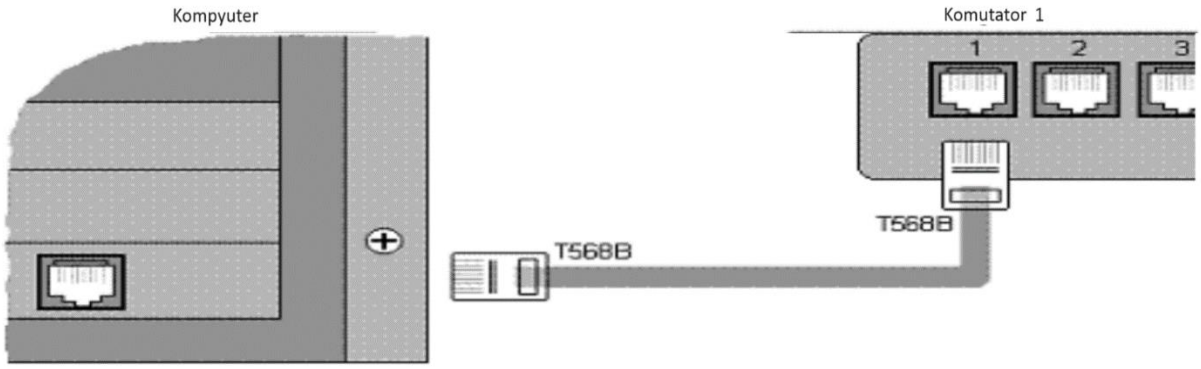


Рисунок - 1.11. Соединение компьютера с коммутатором LAN при помощи кабеля стандарта T568B с обоих концов.

Чтобы соединить два персональных компьютера, используя только сетевые адаптеры, применяйте кабель с перекрестной проводкой (Uplink или Crossover), соответствующий стандартам T568A или T568B.

Приложение 1. Обрезка кабеля в локальных сетях

В этом разделе мы рассмотрим практические методы работы с кабелями, их обрезку и подключение.

П.1.1. Обрезка коаксиальных кабелей.

Для обрезки коаксиальных кабельных разъемов рекомендуется использовать специальные инструменты:

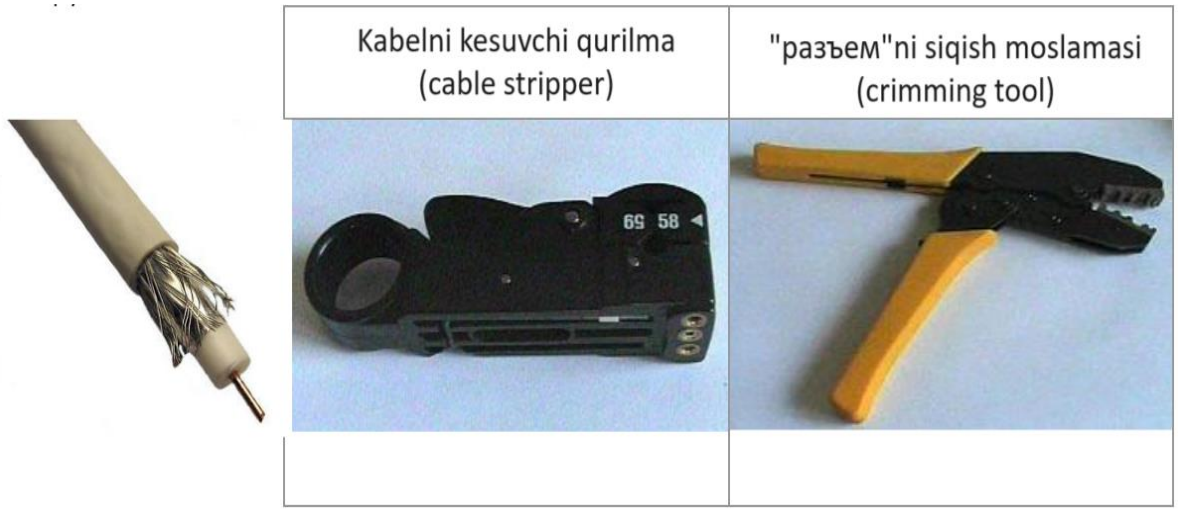


Рисунок - 1.12. Коаксиальный кабель и специальные инструменты, используемые для его обрезки.

Комплект компрессионных разъемов BNC включает следующие компоненты:

- центральный контакт;
- корпус разъема;
- фиксирующая трубка.

Рисунок - 1.13. BNC приемник сигнала.

Процесс установки разъема начинается с обрезки кабеля. Для этого следуйте следующим шагам:

- Лезвие, предназначенное для обрезки внутренней изоляции, должно быть настроено так, чтобы оно доходило почти до центрального проводника, но не за его пределы.
- Среднее лезвие должно аккуратно разрезать плетение и слегка надрезать внутреннюю изоляцию, избегая повреждения проводов.
- Лезвие для обрезки внешней изоляции должно проходить полностью через изоляцию. После этого лучше вручную удалить оставшуюся часть изоляции по обрезанному кольцу.

Затем разъем обжимается на кабель с использованием обжимного инструмента в следующей последовательности:

- **Вставка центрального контакта**: Сначала вставьте центральный контакт разъема на центральный проводник обрезанного кабеля таким образом, чтобы контакт плотно прилегал к внутренней изоляции кабеля. Если контакт не достигает внутренней изоляции, возможно, потребуется немного укоротить центральный проводник кабеля, чтобы обеспечить правильное положение контакта.
- Далее центральный контакт, который закреплен на кабеле, помещается в обжимной инструмент. При этом фланец, предназначенный для обжатия центральных контактов, должен упираться во внутреннюю часть обжимного гнезда, после чего производится обжим.
- После этого на кабель устанавливается фиксирующая трубка.
- Затем, используя, к примеру, отвертку, слегка подталкиваются оплетенные проводники и помещаются в корпус разъема.
- Переместите трубку вперед к корпусу разъема, убедившись, что она надежно прижимает оплетенные проводники. Важно, чтобы центральный контакт был на уровне с краем корпуса разъема. Для достижения этого можно

поставить край корпуса на твердую поверхность и аккуратно протолкнуть кабель вниз до тех пор, пока не будет достигнут нужный результат.

- Далее аккуратно поместите фиксирующую трубку в обжимной инструмент. Сначала слегка нажмите на трубку, чтобы убедиться, что между ней и корпусом разъема нет зазора. Затем выполните основной обжим с необходимым усилием для активации обжимного флажка. Если длина трубки превышает ширину обжимных губок, повторите обжим, смещая инструмент вдоль трубки. В некоторых случаях полезно провести повторный обжим с поворотом на 60 или 120 градусов, если края трубки остаются неровными после первого обжима.

П.1.2. Обрезка витой пары.

Для обрезки витых пар применяется специальное устройство, оснащенное тремя рабочими зонами, каждая из которых выполняет свою функцию:

- Зона, находящаяся ближе всего к рукояткам устройства, предназначена для обрезки витых проводников.
- В центральной части устройства расположено гнездо для обжатия разъема.
- В верхней части устройства расположена область для снятия внешней изоляции витой пары. Внутренняя изоляция проводников не удаляется, поскольку её удаление происходит при контакте с разъемом.

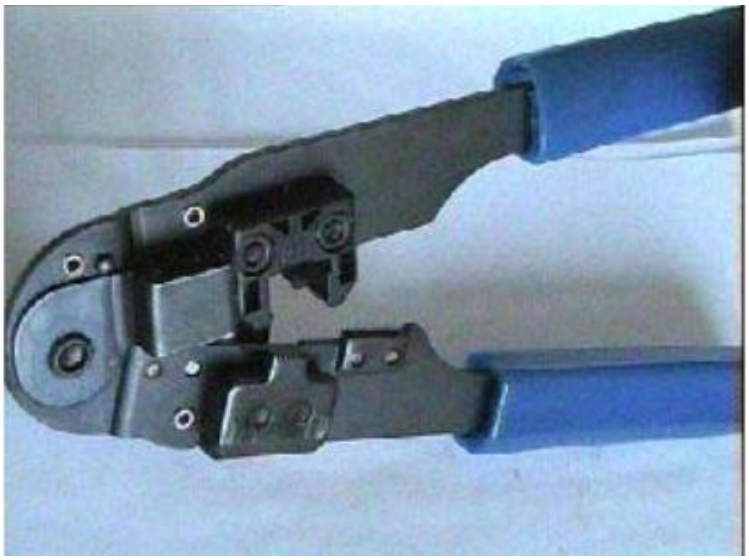


Рисунок - 1.14. Инструмент для обрезки и обжатия витых пар кабелей.

Последовательность операций при обрезке разъема витой пары следующая:

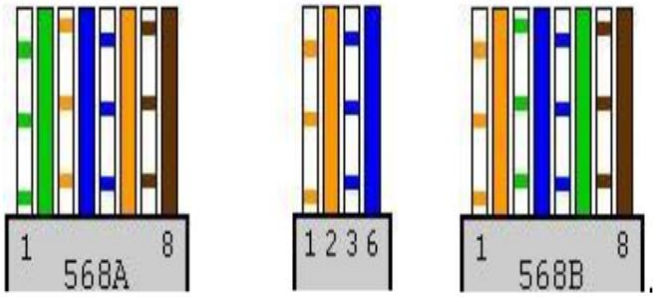
1. Сначала удалите внешнюю изоляцию кабеля.

Для удаления изоляции с плоского кабеля и достижения необходимой глубины зачистки для разъема прижмите кабель к выступу на инструменте, обеспечивающему его выравнивание. Закрепите кабель с помощью зажима и снимите изоляцию.

Процесс зачистки круглых кабелей с витой парой более сложен. Рекомендуется сначала сделать небольшой надрез внешней оболочки, после чего аккуратно повернуть кабель в месте надреза и вручную удалить изоляцию вдоль этой линии.

2. После зачистки провода витой пары выравниваются в одну плоскость в соответствии с заданным порядком. Затем все провода обрезаются до одинаковой длины и снова выравниваются.

Стандарт EIA/TIA-568B определяет порядок подключения проводов в разъемах RJ-45. В рисунке показаны номера контактов для кабелей с восьмижильной и четырехжильной витой парой.



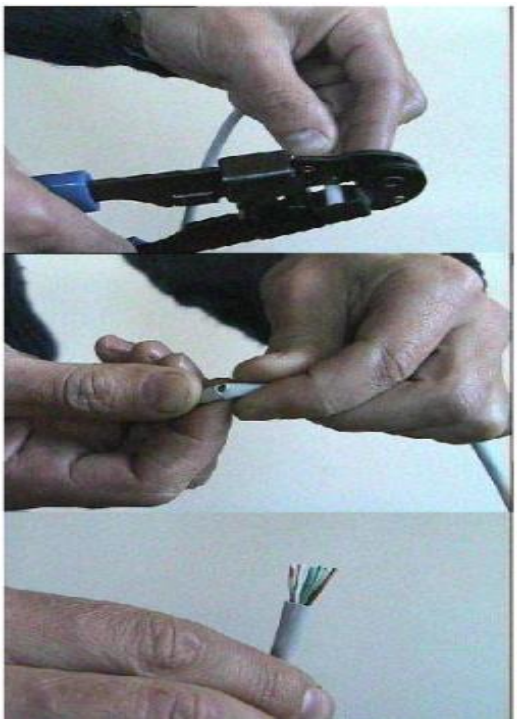


Рисунок - 1.15. Отделение защитной части витой пары кабеля.

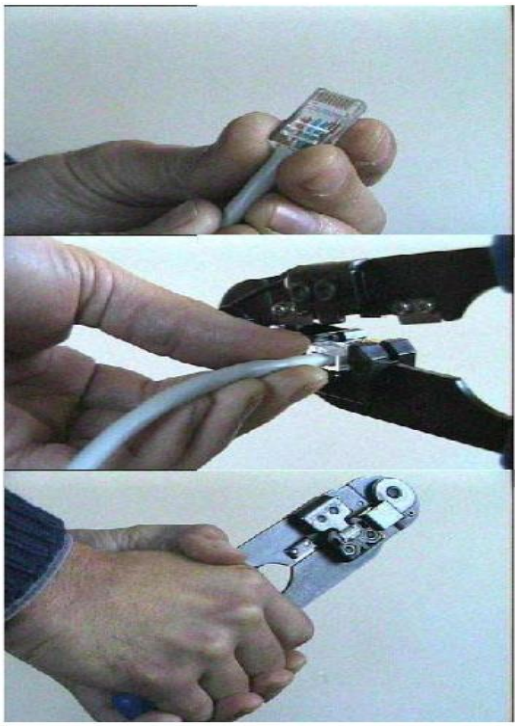


Рисунок - 1.16. Разделение витых пар кабеля по цветовой последовательности и подключение к разъему (RJ-45).

3. Проводники помещаются в разъем и обжимаются. По возможности рекомендуется использовать разъемы без вставки, поскольку процесс размещения проводников в таких разъемах является более простым.

3a. Если разъем не имеет вставки, проводники аккуратно вставляются в корпус разъема до достижения его конца. После этого разъем помещается в гнездо обжимного инструмента и обжимается до полного закрытия.

3b. Если разъем имеет вставку, сначала она надевается на витые проводники.

Вставка имеет форму спичечного коробка с отверстиями на одной из сторон, соответствующими количеству проводников в витой паре.

Вставка надевается на проводники таким образом, чтобы разъемы были ориентированы в сторону корпуса разъема.

После установки вставки проводники снова обрезаются, чтобы их концы совпадали с краем вставки.

Чтобы закрепить вставку в этом положении и предотвратить её перемещение, полезно слегка согнуть проводники с противоположной стороны пальцами.

Затем вставка с проводниками помещается в корпус разъема до тех пор, пока она не станет на место и не совпадет с концом разъема. После этого разъем обжимается так же, как и разъем без вставки.

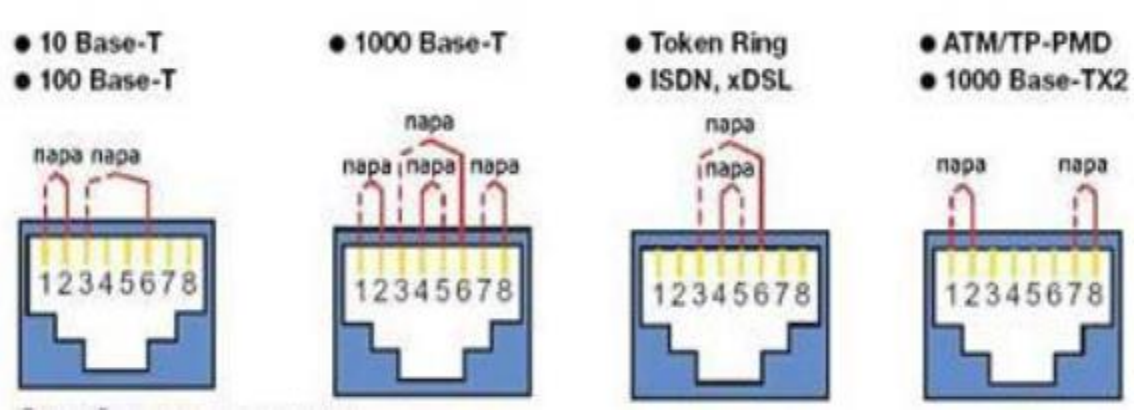


Рисунок - 1.17. Подключение проводов к разъему (RJ-45) для различных протоколов.

Многие считают, что этот этап установки сети является самым сложным из-за большого количества проводов, которые легко запутать, необходимости приобретения специального обжимного инструмента и других нюансов. На самом деле, это достаточно просто. Для обжима витой пары вам понадобятся специальные клещи и разъемы RJ-45.

После обжима кабелей подключите их к разъемам сетевой карты с одной стороны и к коммутатору с другой. Затем останется только настроить сеть на компьютерах.

Следует отметить, что многие сети начинались таким образом: коридоры и офисы заполнялись кусками кабелей, и если кабели не подписаны, то в сети с 10 компьютерами это может стать настоящим кошмаром для

обслуживающего персонала. В этом случае наилучшим решением будет использование СКС (структурированной кабельной системы).

Контрольные вопросы:

1. На какие два больших класса делится всё сетевое оборудование и чем они отличаются друг от друга?
2. Что такое структурированная кабельная система и из чего она состоит?
3. Какие элементы относятся к классу пассивного сетевого оборудования?
4. Какие типы кабельных средств могут использоваться для передачи данных в локальной сети (LAN)?
5. Что определяют стандарты T568A и T568B?
6. Почему в витых парных кабелях отдельные проводники скручены вместе? Сколько витых пар содержат кабели категории 5e и категории 6?
7. В чем разница между UTP и STP? Какие различия в их использовании?
8. Что такое RJ11, RJ12 и RJ45, чем они отличаются и каковы области их применения?
9. Какова цель патч-кабеля и чем он отличается от внутреннего прокладочного кабеля?
10. Какие общие черты и различия между патч-панелями и розетками?
11. Для каких целей используются хабы и коммутаторы?
12. Укажите основные различия в работе хабов и коммутаторов.
13. Какие различия между подключением одного персонального компьютера к сетевой карте другого персонального компьютера и его подключением к LAN-коммутатору?
14. Какие основные ограничения следует учитывать при прокладке LAN-кабелей?
15. Для чего и как используются патч-панели?
16. Что означает аббревиатура WOL и какую технологию она поддерживает?
17. Какую функцию сетевого адаптера поддерживает чип BootRom?
18. Что определяют основные стандарты кабельных систем?
19. Какие параметры относятся к основным характеристикам кросс-панелей?
20. Для каких целей используется порт «Uplink» в коммутаторах?
21. Укажите последовательность операций при установке разъема RJ-45.
22. Какой кабель и почему используется для подключения ПК к сетевой розетке?

Практическая работа № 2

Работа с командным интерфейсом коммутаторов Cisco и начальная настройка. Проектирование и создание локальной сети (LAN) в Cisco Packet Tracer

Цель работы: Изучение проектирования и создания локальной сети (LAN) с использованием программы Cisco Packet Tracer.

LAN (локальная вычислительная сеть) — это группа устройств, которые обеспечивают связь между подключенными к сети устройствами.

Проще говоря, локальная сеть (LAN) представляет собой группу компьютеров и других устройств, соединенных между собой в одном месте, обычно в одном здании, например, в офисе или доме. Далее мы рассмотрим это более подробно.

Что такое LAN ?

Из названия «локальная сеть» можно понять две вещи: устройства в сети подключены друг к другу и находятся в ограниченном локальном пространстве. Этот локальный аспект определяет локальную сеть и отличает её от других типов сетей, таких как глобальные сети (WAN) и городские сети (MAN).

LAN обычно ограничены небольшой областью, как одно здание, хотя это не обязательно. Область может варьироваться от вашего дома или малого бизнеса с несколькими устройствами до гораздо большей территории, например, целого офисного здания с сотнями или тысячами устройств.

Однако, вне зависимости от размера, основной характеристикой локальной сети является то, что она объединяет устройства, расположенные в одной ограниченной области.

Преимущества использования локальной сети аналогичны преимуществам подключения любых устройств к сети. Эти устройства могут совместно использовать одно интернет-соединение, обмениваться файлами, печатать на общих принтерах и выполнять другие функции.

В крупных локальных сетях часто можно найти специализированные серверы, которые предоставляют услуги, такие как глобальные каталоги пользователей, электронная почта и доступ к различным ресурсам компании.

В обычной домашней или малой офисной сети вы найдете модем, обеспечивающий доступ в интернет и выполняющий роль основного брандмауэра для защиты от внешних угроз. Также будет маршрутизатор, который делит интернет-соединение между различными устройствами и

соединяет их друг с другом, а также точку доступа Wi-Fi, позволяющую устройствам подключаться к сети беспроводным способом.

Иногда все эти функции могут быть объединены в одном устройстве. Например, многие интернет-провайдеры предлагают комбинированные устройства, которые совмещают функции модема, маршрутизатора и точки беспроводного доступа. Также можно встретить устройства, называемые коммутаторами, которые позволяют разделить одно Ethernet-подключение на несколько точек подключения.

В крупных локальных сетях используются те же сетевые устройства, но в большем масштабе, как по количеству устройств, так и по эффективности их работы. Например, профессиональные маршрутизаторы и коммутаторы могут управлять большим количеством одновременных подключений, обеспечивать более надежную безопасность и мониторинг, а также предлагать расширенные возможности настройки. Профессиональные точки доступа Wi-Fi позволяют управлять множеством устройств из одного интерфейса и обеспечивать более эффективное управление доступом.

Что такое коммутатор (switch)?

Сетевой коммутатор (или switch) — это устройство, предназначенное для соединения нескольких узлов в пределах одного сегмента сети. В отличие от концентратора (hub), который передает трафик от одного подключенного устройства ко всем остальным, коммутатор направляет данные только непосредственно к получателю. Исключение составляют широковещательные пакеты (с MAC-адресом FF:FF:FF:FF:FF), которые отправляются всем узлам в сети. Это улучшает производительность и безопасность сети, устраняя необходимость в обработке данных, не предназначенных для остальных устройств сети, и снижая риск их перехвата.

Процесс работы коммутатора

Коммутатор хранит в своей памяти таблицу, которая отображает соответствие между MAC-адресами хостов и портами коммутатора. Эта таблица сохраняется в ассоциативной памяти. При первом включении коммутатора таблица пуста, и устройство находится в режиме обучения. В этом режиме данные, поступающие на один порт, передаются на все остальные порты коммутатора. При этом коммутатор анализирует кадры, определяет MAC-адрес отправителя и записывает его в таблицу. В дальнейшем, если коммутатор получает кадр, предназначенный для хоста с MAC-адресом, уже записанным в таблице, этот кадр передается только через порт, указанный в таблице. Если MAC-адрес назначения отсутствует в таблице, кадр отправляется на все порты. Со временем коммутатор создает

полную таблицу для всех своих портов, что позволяет локализовать трафик. Также стоит отметить, что каждый порт коммутатора обеспечивает низкую задержку и высокую скорость передачи данных.

Обычно при проектировании сети с использованием коммутаторов несколько коллизионных доменов локальной сети соединяются друг с другом. В реальной жизни этажи здания, в котором создается сеть, обычно функционируют как коллизионные домены. Обычно их больше двух, что делает управление трафиком более эффективным по сравнению с мостами, которые являются предшественниками коммутаторов. Коммутаторы могут поддерживать избыточные связи между узлами сети.

Коммутаторы могут управлять трафиком на основе протокола канального уровня модели OSI (2-й уровень), что позволяет управлять MAC-адресами подключенных устройств и даже обеспечивать преобразование пакетов между различными стандартами (например, от Ethernet к FDDI и наоборот). Эти возможности особенно ярко выражены в коммутаторах уровня 3, которые по своим возможностям приближаются к маршрутизаторам.

Коммутатор позволяет маршрутизировать пакеты между несколькими сегментами сети. Это обучающее устройство работает по аналогичной технологии. В отличие от мостов, некоторые коммутаторы не буферизируют все входящие пакеты. Это происходит только в случае необходимости согласования скорости передачи или когда адрес назначения отсутствует в таблице адресов, или когда порт, на который нужно направить пакет, занят, и пакеты пересылаются быстро.

Коммутатор анализирует только адрес назначения в заголовке пакета и, проверив таблицу адресов, сразу (с задержкой около 30-40 микросекунд) направляет пакет на соответствующий порт. Таким образом, заголовок пакета может быть передан через выходной порт даже до того, как весь пакет полностью пройдет через входной порт. К сожалению, стандартные коммутаторы работают по алгоритму «старения адресов». Это означает, что если в течение определенного времени не поступает обращений к этому адресу, он удаляется из таблицы адресов.

Коммутаторы поддерживают полнодуплексное соединение при подключении друг к другу. В этом режиме данные передаются и принимаются одновременно, что невозможно в обычных Ethernet-сетях. Это удваивает скорость передачи данных и позволяет достичь высокой производительности при подключении нескольких коммутаторов.

Характеристики и типы коммутаторов

Коммутаторы бывают управляемыми и неуправляемыми (самыми простыми). Более сложные коммутаторы позволяют управлять коммутацией на сетевом (третьем) уровне модели OSI и часто обозначаются как Layer 3 Switch или просто L3. Управление такими коммутаторами может осуществляться через веб-интерфейс, протокол SNMP, RMON (протокол, разработанный Cisco) и другие средства.

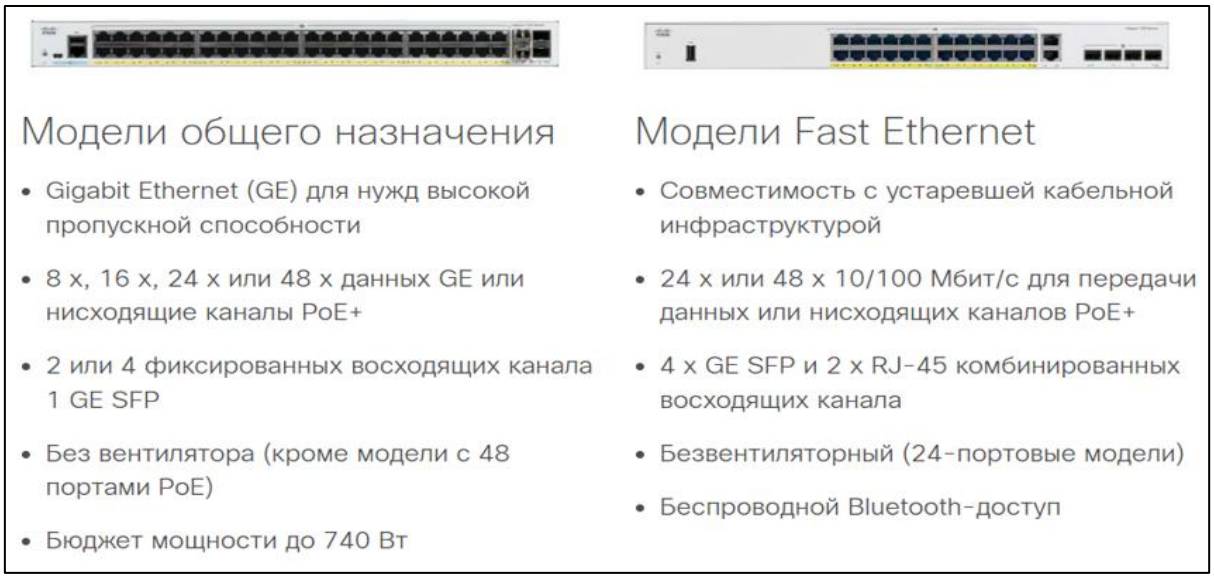


Рисунок - 2.1. Cisco коммутаторы и их характеристики.

Многие управляемые коммутаторы предоставляют дополнительные функции, такие как VLAN, QoS, агрегация и зеркалирование. Сложные коммутаторы можно объединить в одно логическое устройство для увеличения количества портов. Например, можно объединить четыре коммутатора по 24 порта каждый и получить логический коммутатор с 90 портами (4 * 24 - 6) или 96 портами, если используются специальные порты для стекирования.

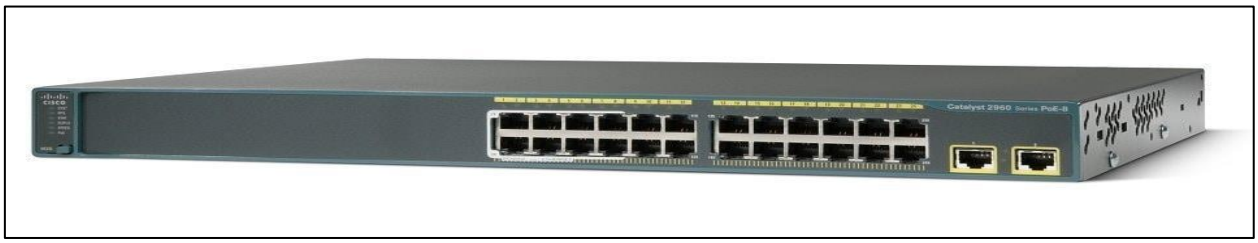


Рисунок - 2.2. Cisco коммутатор Catalyst 2960.

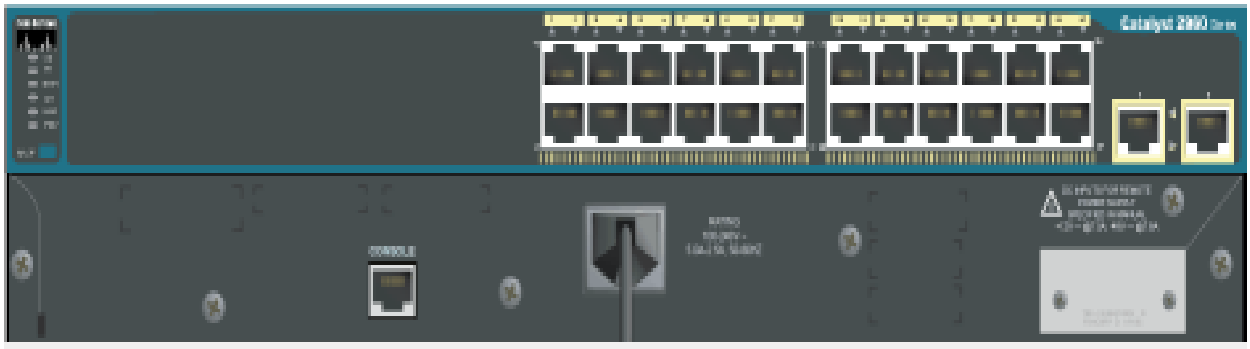


Рисунок - 2.3. Задняя панель коммутатора Cisco Catalyst 2960 в Cisco Packet Tracer.

Практическая часть работы:

Откройте Cisco Packet Tracer. В нижней левой панели откройте список оборудования и терминальных устройств. Выберите компьютер и создайте два персональных компьютера на рабочей области.

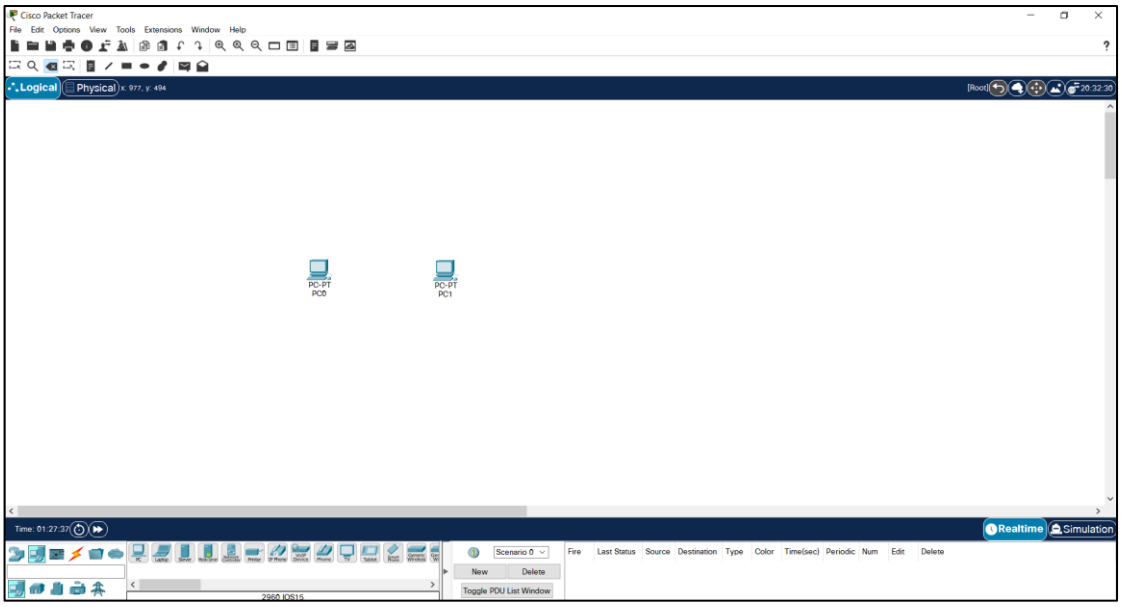


Рисунок - 2.4. Рабочая область Cisco Packet Tracer.

Затем настройте IP-адрес и маску подсети на обоих персональных компьютерах. После этого мы подключим их друг к другу.

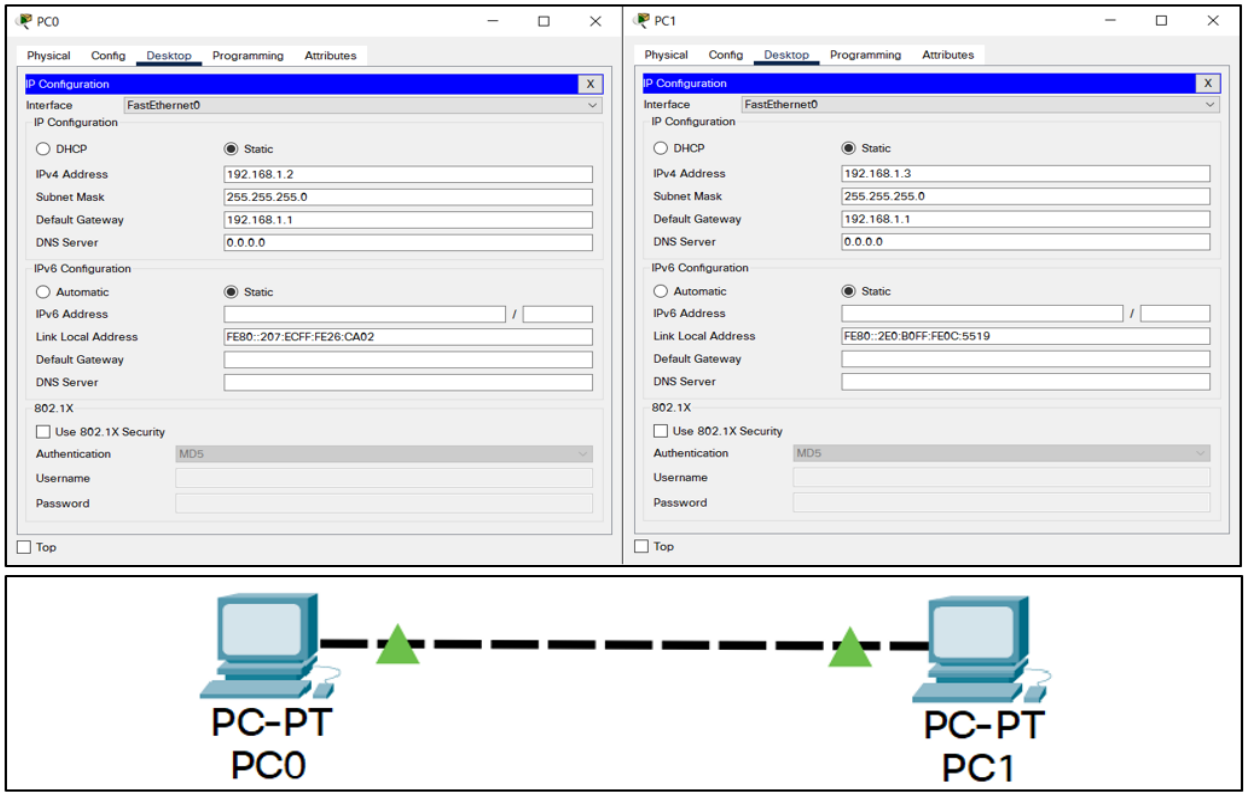


Рисунок - 2.5. Настройка IP-адресов на компьютерах и их подключение друг к другу.

Проверка соединения с помощью команды ping. Если оборудование настроено правильно, то не будет потерянных пакетов (Lost = 0) или будет потеряно менее 50% (иногда пакеты могут теряться при передаче).

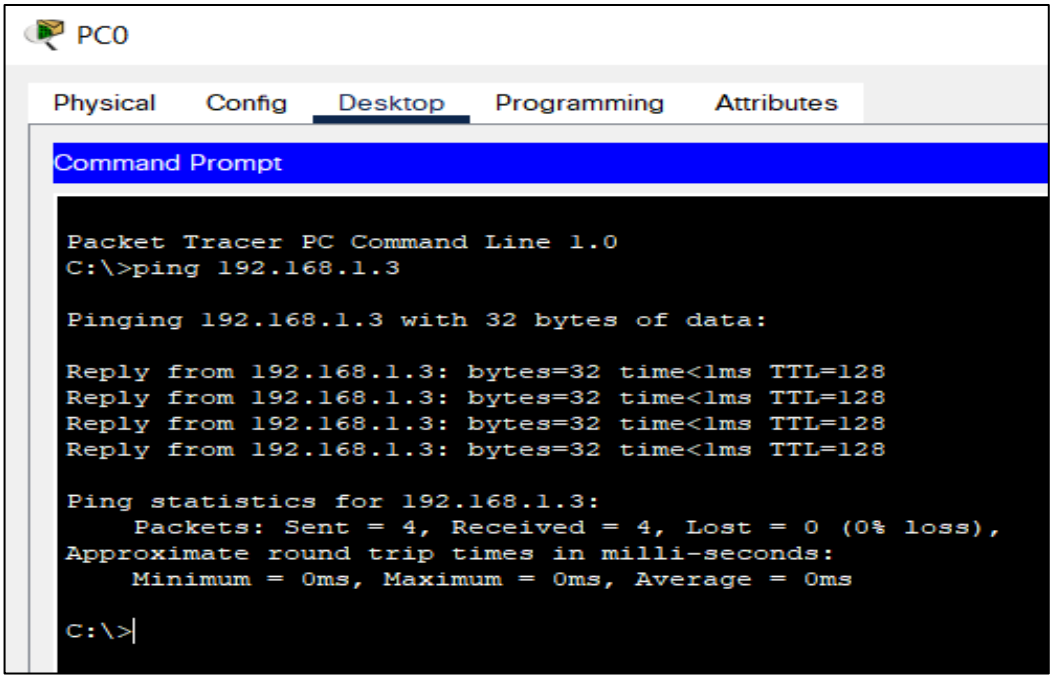


Рисунок - 2.6. PC0 с Ping PC1.

Далее, на той же панели оборудования перейдите в раздел сетевого оборудования и выберите коммтатор модели Cisco Catalyst 2960. Перетащите

его на рабочую область. Ранее подключенные друг к другу персональные компьютеры подключите к коммутатору, а также добавьте еще один коммутатор.

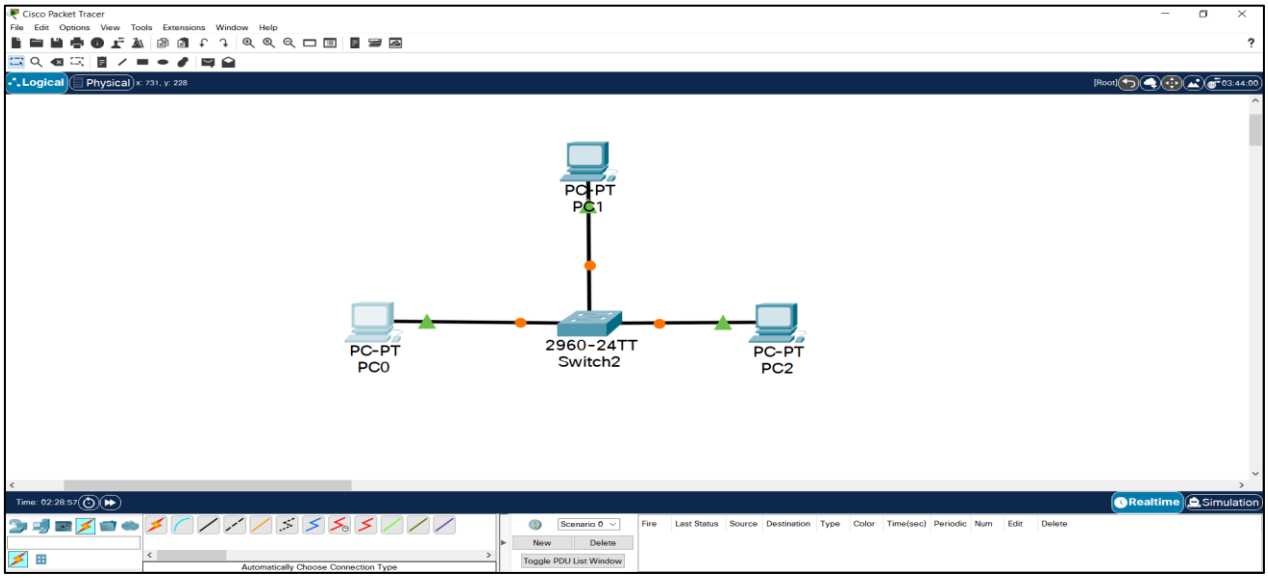


Рисунок - 2.7. Сеть, состоящая из 3 персональных компьютеров, подключенных через коммутатор.

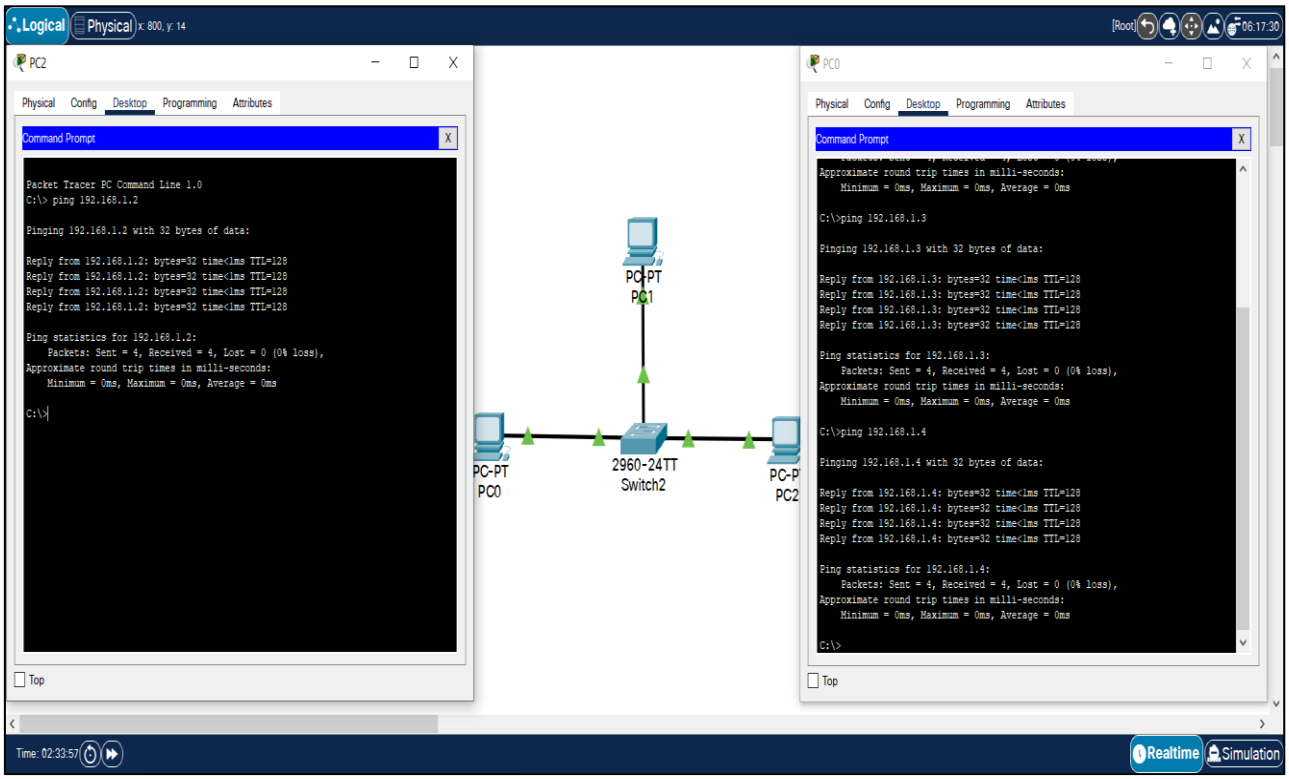


Рисунок - 2.8. Мы ждем активации портов (вместо оранжевой точки загорятся зеленые треугольники) и пингуем завершенное оборудование.

```
C:\>ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:
        Reply from 192.168.1.3: bytes=32 time<1ms TTL=128
        Reply from 192.168.1.3: bytes=32 time<1ms TTL=128
        Reply from 192.168.1.3: bytes=32 time<1ms TTL=128
        Reply from 192.168.1.3: bytes=32 time<1ms TTL=128
Ping statistics for 192.168.1.3:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>ping 192.168.1.4

Pinging 192.168.1.4 with 32 bytes of data:
        Reply from 192.168.1.4: bytes=32 time<1ms TTL=128
        Reply from 192.168.1.4: bytes=32 time<1ms TTL=128
        Reply from 192.168.1.4: bytes=32 time<1ms TTL=128
        Reply from 192.168.1.4: bytes=32 time<1ms TTL=128
Ping statistics for 192.168.1.4:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Задание для выполнения:

- Создайте сеть, состоящую из N компьютеров (Таблица 3.1), подключенных через коммутатор.
- Введите IP-адреса для компьютеров, выбираемых из таблицы с вариантами.
- Подготовьте сеть для следующих лабораторных работ.

Таблица - 2.1

Варианты выполнения работы

Вариант	N	IP адрес	Вариант	N	IP адрес
1	3	190.118.1. …	16	3	141.168.1. …
2	4	180.128.1. …	17	4	131.178.1. …
3	5	170.138.1. …	18	5	121.188.1. …
4	6	160.148.1. …	19	6	111.198.1. …
5	7	150.158.1. …	20	7	102.108.1. …
6	8	140.168.1. …	21	8	192.118.1. …
7	9	130.178.1. …	22	9	182.128.1. …
8	8	120.188.1. …	23	8	172.138.1. …
9	7	110.198.1. …	24	7	162.148.1. …
10	6	101.108.1. …	25	6	152.158.1. …
11	5	191.118.1. …	26	5	142.168.1. …
12	4	181.128.1. …	27	4	132.178.1. …
13	3	171.138.1. …	28	3	122.188.1. …
14	4	161.148.1. …	29	4	112.198.1. …
15	5	151.158.1. …	30	5	103.108.1. …

Контрольные вопросы:

1. Что такое LAN?
2. Что такое коммутатор?
3. Опишите, как работает коммутатор.
4. Типы коммутаторов.
5. Опишите коммутатор Cisco Catalyst 2960.

Практическое задание № 3

Проектирование компьютерной сети для предприятий и организаций.

Цель задания: Изучение основ построения корпоративных компьютерных сетей, разработка требований к сети и исследование технологий и протоколов, используемых в корпоративной сети.

Теоретическая информация

Принципы проектирования корпоративной компьютерной сети включают:

1. Архитектура сети: Процесс проектирования и разработки компьютерной сети называется архитектурой сети. Понятие архитектуры включает в себя физические компоненты сети, их функциональные объекты, конфигурацию, принципы и порядок работы, а также используемые протоколы связи. Архитектура сети также включает услуги, предоставляемые через сеть, их подробные описания, а также расчет и структуру платежей за предоставляемые услуги. Существует два наиболее распространенных типа архитектуры сети: равноправная (peer-to-peer) и клиент-серверная. Взаимосвязь компьютерных сетей в глобальном масштабе образует Интернет. Архитектура Интернета характеризуется использованием протоколов (TCP/IP), а не определенной модели или типа аппаратных соединений. Каждая сеть, созданная с использованием конкретной технологии, имеет свою архитектуру, например, OSI, TCP/IP, общедоступные телефонные сети, мобильные сети и другие.

2. Проектирование и создание локальной корпоративной сети: Процесс проектирования корпоративной сети включает объединение локальных сетей различных подразделений компании и создание материально-технической базы для дальнейшего планирования, организации и управления основной деятельностью предприятия.

3. Создание корпоративной сети: Основано на последовательной и развитой архитектуре данных, платформ и приложений, обеспечивающих обмен информацией между пользователями.

4. Хранение и защита данных: Функционирующая корпоративная сеть также включает разработку средств для хранения и защиты баз данных.

5. LAN (Local Area Network): Локальная вычислительная сеть, обеспечивающая стабильный обмен необходимой информацией и управление правами доступа пользователей.

6. СКС (Структурированная кабельная система): Телекоммуникационная инфраструктура – набор всех компьютерных устройств компании, между которыми осуществляется обмен данными в режиме реального времени.

Эти принципы лежат в основе процесса проектирования и создания корпоративной сети.

Процесс создания сети в симуляторе Cisco Packet Tracer

Шаг 1: запустите Cisco Packet Tracer и создайте новый пустой проект. Запустите Packet Tracer на вашем компьютере или ноутбуке. Дважды щелкните на значок Packet Tracer на рабочем столе или перейдите в каталог, содержащий исполняемый файл Packet Tracer, и запустите его. Packet Tracer должен открыться с пустым стандартным рабочим пространством логической топологии, как показано на рисунке.

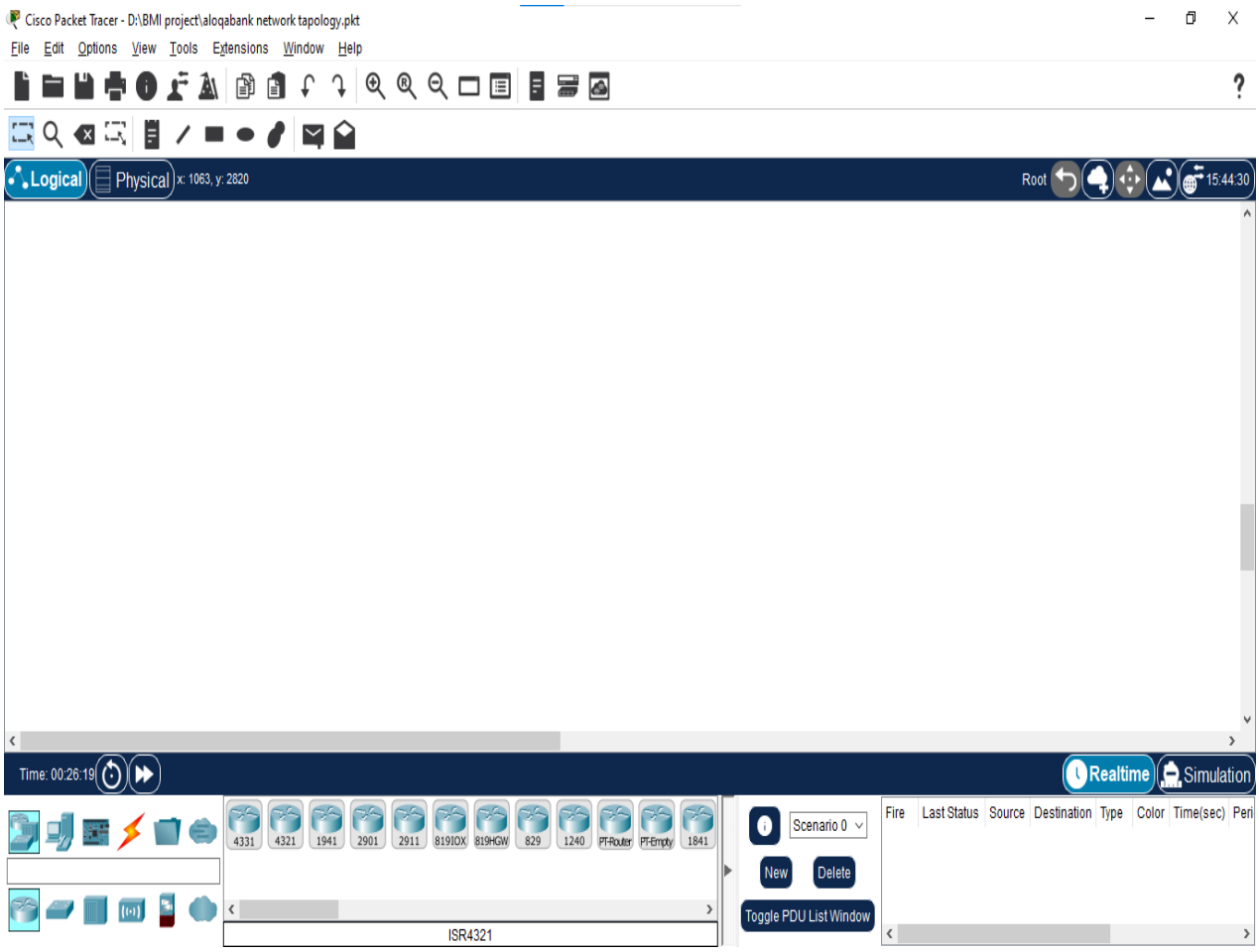


Рисунок - 3.1. Интерфейс нового приложения.

Шаг - 2: Создайте топологию. Добавьте сетевые устройства на рабочую область.

Используя окно выбора устройства, добавьте сетевые устройства на рабочую область, как показано на диаграмме топологии. Чтобы разместить устройство на рабочей области, сначала выберите тип устройства в окне выбора типа устройства. Затем нажмите на необходимую модель устройства в

окне «Выбор конкретного устройства». Наконец, нажмите на место на рабочей области, где вы хотите разместить устройство. Если вы хотите отменить свой выбор, нажмите на значок отмены для данного устройства. Также можно выбрать устройство в окне «Выбор конкретного устройства» и перетащить его на рабочую область.

Шаг 3: Добавьте сетевые устройства на рабочую область.

Используя окно выбора устройства, добавьте сетевые устройства на рабочую область, как показано на диаграмме топологии. Чтобы разместить устройство на рабочей области, сначала выберите тип устройства в окне выбора типа устройства. Затем нажмите на необходимую модель устройства в окне «Выбор конкретного устройства».

Шаг 4: Измените отображаемые имена сетевых устройств.

Чтобы изменить отображаемые имена сетевых устройств, нажмите на значок устройства в логической рабочей области Packet Tracer, затем нажмите на вкладку Config в окне конфигурации устройства. Введите новое имя устройства в поле «Display Name», как показано на рисунке ниже.

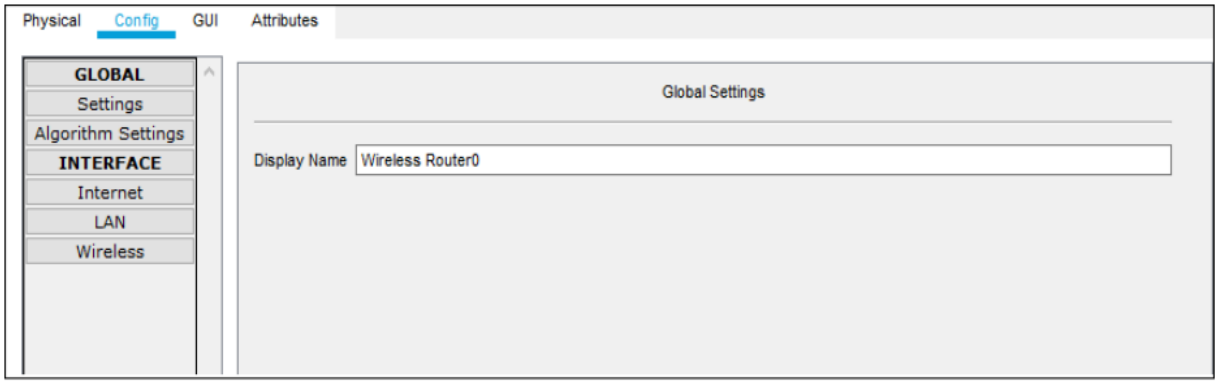


Рисунок - 3.2. Меню конфигурации.

Шаг 5: Добавление физического кабеля между устройствами на рабочем столе Используя окно выбора устройства, добавьте физический кабель между устройствами на рабочей области, как показано на диаграмме топологии.

Чтобы подключить компьютер к беспроводному маршрутизатору, потребуется прямой медный кабель. В окне выбора устройства выберите прямой медный кабель и подключите его к порту FastEthernet0 на персональном компьютере и к порту Ethernet 1 на беспроводном маршрутизаторе. Для подключения беспроводного маршрутизатора к кабельному модему также потребуется прямой медный кабель. В окне выбора устройства выберите прямой медный кабель и подключите его к порту Internet на беспроводном маршрутизаторе и к порту 1 на кабельном модеме. Для подключения кабельного модема к интернет-облаку потребуется коаксиальный кабель. В окне выбора устройства выберите коаксиальный

кабель и подключите его к порту Port 0 на кабельном модеме и к коаксиальному интерфейсу интернет-облака.

Общий вид сетевой топологии

(VLANS и используемые устройства)

VLANs	Network Devices used
"Plastic cards & International cards" department	5 phones, 5 computers, 2 printers, 1 Access Point
"Credit" department	6 phones, 6 computers, 3 printers, 1 Access Point
Cash Desk	3 phones, 3 computers, 1 printers, 1 Access Point
Call Center	10 phones, 10 computers, 5 printers, 1 Access Point
International Relations & Marketing	7 phones, 7 computers, 2 printers, 1 Access Point
Accounting	7 phones, 7 computers, 7 printers, 1 Access Point

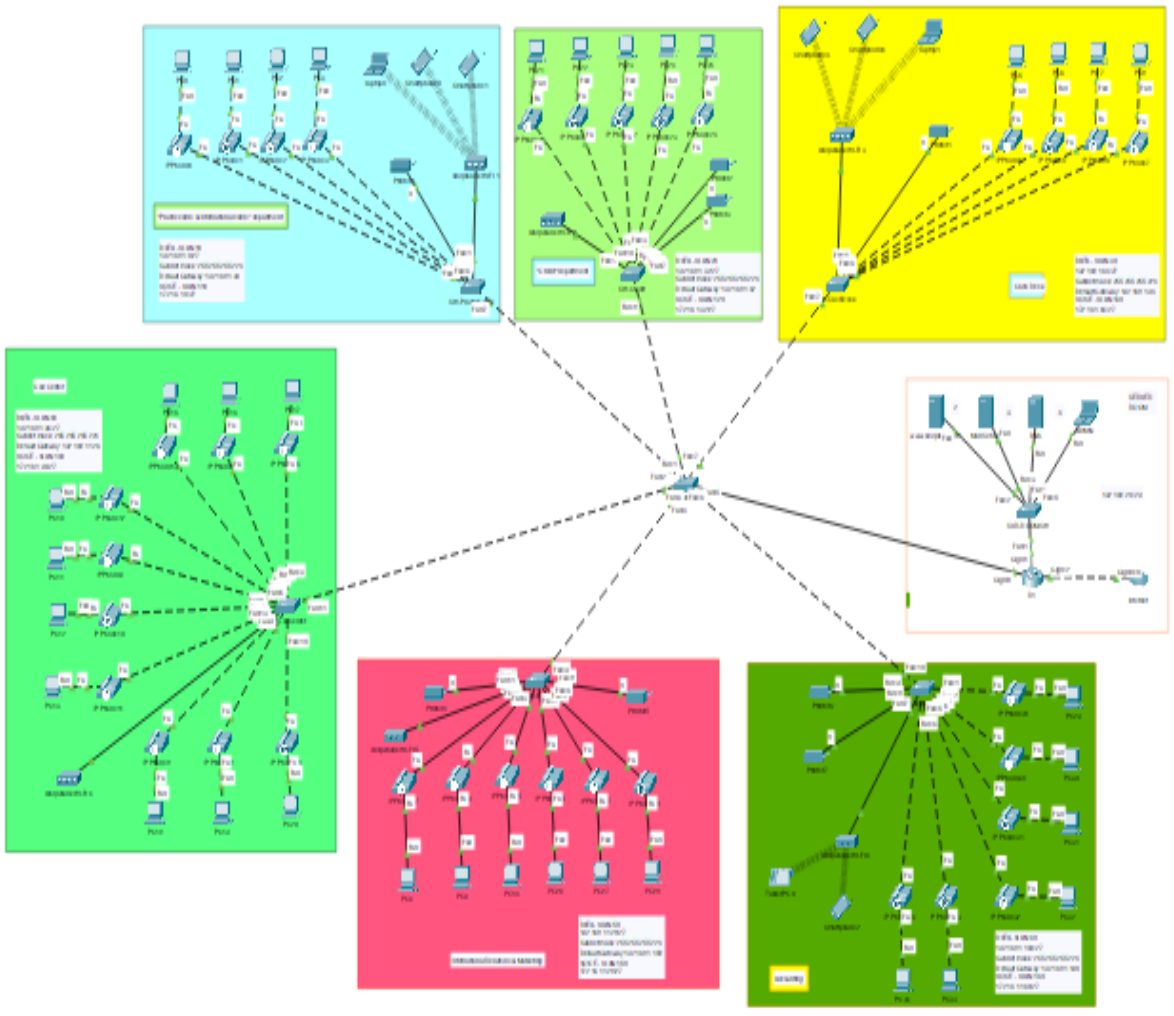


Рисунок - 3.3. Конечное состояние сетевой топологии.

Команды, используемые на распределительном коммутаторе для создания VLAN:

```
Switch>enable
Switch#conf
Switch#conFigure t
Switch#conFigure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#
Switch(config)#vlan 10
Switch(config-vlan)#vlan 20
Switch(config-vlan)#vlan 30
Switch(config-vlan)#vlan 40
Switch(config-vlan)#vlan 50
Switch(config-vlan)#vlan 60
Switch(config-vlan)#do wr
Switch(config-vlan)#exit
Switch(config)#interface range fast
Switch(config)#interface range fastEthernet 0/1-7
Switch(config-if-range)#switchport mode trunk
```

Команды, используемые на коммутаторах доступа для создания VLAN:

```
Switch>enable
Switch#conf
Switch#conFigure t
Switch#conFigure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface range FastEthernet0/1-24
Switch(config-if-range)#switchport access vlan 10
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport voice vlan 110
```

Настройка SSH:

```
en
conf t
hostname
enable password cisco
line console 0
password cisco
login
exit
banner motd ##RUXSATSIZ KIRISH TA'QIQLANADI!!!##
service password-encryption
no ip domain lookup
do wr
username cisco password cisco
ip domain name cisco.net
crypto key generate rsa general-keys modulus 1024
line vty 0 15
login local
transport input ssh
exit
do wr
```

Настройка Cisco ROAS (Router on A Stick - позволяет подключить все VLAN через один физический интерфейс. Физический интерфейс разделяется на логические интерфейсы (называемые подинтерфейсами) по одному для каждой VLAN).

```
R1(config)#int Gi0/0
R1(config-if)#no shutdown
R1(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state
to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/0, changed state to up
R1(config-if)#int Gi0/0.1
R1(config-subif)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0.1, changed
state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/0.1, changed state to up
R1(config-subif)#encapsulation dot1q 3
```

```
R1(config-subif)#ip address 10.0.3.1 255.255.255.0
R1(config-subif)#int Gi0/0.2
R1(config-subif)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0.2, changed
state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/0.2, changed state to up
R1(config-subif)#encapsulation dot1q 10
R1(config-subif)#ip address 10.0.10.1 255.255.255.0
R1(config-subif)#int Gi0/0.3
R1(config-subif)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0.3, changed
state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/0.3, changed state to up
R1(config-subif)#encapsulation dot1q 5
R1(config-subif)#ip address 10.0.5.1 255.255.255.0
```

Контрольные вопросы:

1. Какова основная цель корпоративной сети?
2. Как должна быть структурирована корпоративная сеть?
3. Какие устройства используются в сети?
4. Какое программное обеспечение используется в сети?
5. Как обеспечивается безопасность сети?
6. Какие средства используются для контроля работы сети?
7. С помощью каких инструментов проверяется эффективность сети?
8. Какие протоколы обмена информацией используются в сети?
9. Какие данные хранятся в сети и как к ним можно получить доступ?
10. Какая система технического обслуживания сети существует?
11. Каковы возможности расширения сети?
12. Какие проблемы могут возникнуть в процессе построения сети?
13. Какие технические характеристики имеет сеть?
14. Какие производственные характеристики имеет сеть?
15. Каковы экономические характеристики сети?
16. Какая база данных используется в сети?
17. Как обеспечивается информационная безопасность сети?
18. Каковы возможности хранения данных и доступа к ним в сети?
19. Какие данные хранятся в сети и как к ним можно получить доступ?
20. Какие данные хранятся в сети и как к ним можно получить доступ?

Пракческая работа № 4

Подключение корпоративных сетей предприятия через интернет с использованием VPN-туннелей и создание возможности удаленного доступа к сети с помощью мобильных устройств.

Цель работы: Изучение принципов работы VPN, создание и запуск VPN-сетей, исследование подключения корпоративных сетей предприятия через VPN-туннели.

VPN (Virtual Private Network) – это технология, позволяющая создать собственную частную сеть поверх существующей. С помощью VPN вы можете обеспечить безопасность данных, передаваемых через интернет. Например, если кто-то хочет следить за вами или доступ к нужному веб-сайту заблокирован в вашей стране, вы можете использовать интернет через подключение к VPN.

Если ваш компьютер или смартфон не подключен к VPN, ваши данные могут попасть в руки хакеров. В современном мире информация о вашем финансовом состоянии и другие личные данные должны быть хорошо защищены.

По мере развития интернета не только крупные компании, но и обычные пользователи начинают использовать VPN. С VPN можно подключиться к различным странам.

Если вы не знаете, как установить VPN, на YouTube есть множество видео, подробно объясняющих, какие приложения загружать. В интернете также есть множество статей о VPN. Однако будьте осторожны при скачивании бесплатных VPN. Бесплатные VPN могут защитить вас от посторонних, но существует риск, что они могут продать ваши конфиденциальные данные другим после получения доступа. Бесплатные VPN не полностью оптимизированы для защиты личной жизни.

Крупные международные компании используют VPN не только для защиты своих данных от кражи, но и для защиты от вирусов и вредоносных программ.

VPN можно использовать и для удаленного доступа к домашней сети. Существует два типа VPN:

1. Удаленный доступ к внутренней сети.
2. Доступ к заблокированным сайтам..

Удаленный доступ к внутренней сети. Например, вы можете установить VPN у себя дома и заполнить пользовательские данные для доступа к нему из другого места. Таким образом, посещаемые вами веб-сайты

будут видеть IP-адрес вашей домашней сети вместо вашего реального IP-адреса.

Доступ к заблокированным сайтам. В вашем регионе некоторые сайты могут быть заблокированы. Но с помощью VPN вы можете подключиться к сети другого региона и получить доступ к нужному сайту.

Сети в разных уголках мира могут быть соединены друг с другом через две или более частных сетей, и все это будет работать как одна виртуальная частная сеть в интернете.

Таким образом, если кто-то хочет шпионить за вами, он может легко перехватить пакеты данных из сети. VPN же предоставляет вам возможность использовать скрытую сеть внутри большой сети. Все ваши данные будут зашифрованы, чтобы никто не мог вас идентифицировать. У VPN есть и слабые стороны.

Слабая сторона VPN заключается в отсутствии упрощенных процедур для обеспечения качества обслуживания в интернете.

Вы также можете установить VPN на смартфонах Android. Это создаст возможность прямого доступа к вашей личной корпоративной сети с устройства Android, а администратор VPN-сети сможет управлять вашим устройством, следить за данными на смартфоне.

Для предотвращения таких проблем мы рекомендуем использовать платные VPN-сервисы с лицензией, которые гарантируют конфиденциальность ваших личных данных, когда возникает необходимость в использовании VPN.

Порядок выполнения работы

1. В симуляторе Cisco Packet Tracer сначала создадим следующую топологию и выполним соответствующие подключения.

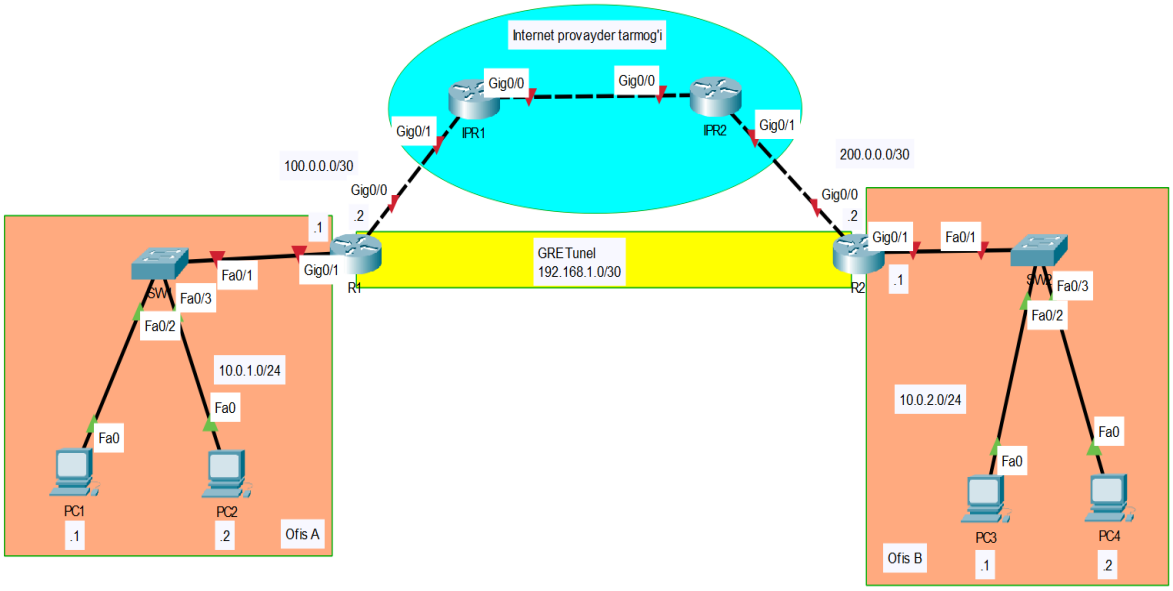


Рисунок - 4.1. Топология, созданная в симуляторе Cisco Packet Tracer.

2. На следующем этапе установим указанные IP-адреса на компьютеры, коммутаторы и маршрутизаторы в топологии.

3. Затем создадим GRE-туннели между маршрутизаторами R1 и R2 для формирования виртуальной частной сети. Для этого введем следующие команды на интерфейсе G0/0 маршрутизатора R1:

```
Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface tunnel 0
Router(config-if)#
%LINK-5-CHANGED: Interface Tunnel0, changed state to up

Router(config-if)#tunnel source g0/0
Router(config-if)#tunnel destination 200.0.0.2
Router(config-if)#ip address 192.168.1.1 255.255.255.252

Router(config-if)#do sh ip int br
Interface IP-Address OK? Method Status Protocol
GigabitEthernet0/0 unassigned YES unset administratively down down
GigabitEthernet0/1 unassigned YES unset administratively down down
GigabitEthernet0/2 unassigned YES unset administratively down down
Tunnel0 192.168.1.1 YES manual up down
Vlan1 unassigned YES unset administratively down down
```

Подобным образом, введем следующие команды на интерфейсе G0/0 маршрутизатора R2:

```
Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface tunnel 0

Router(config-if)#
%LINK-5-CHANGED: Interface Tunnel0, changed state to up

Router(config-if)#tunnel source g0/0
Router(config-if)#tunnel destination 100.0.0.2
Router(config-if)#ip address 192.168.1.2 255.255.255.252
Router(config-if)#do sh ip int br

Interface IP-Address OK? Method Status Protocol
GigabitEthernet0/0 unassigned YES unset administratively down down
GigabitEthernet0/1 unassigned YES unset administratively down down
GigabitEthernet0/2 unassigned YES unset administratively down down
Tunnel0 192.168.1.2 YES manual up down
Vlan1 unassigned YES unset administratively down down
```

4. На следующем этапе настроим «default route» для маршрутизаторов R1 и R2:

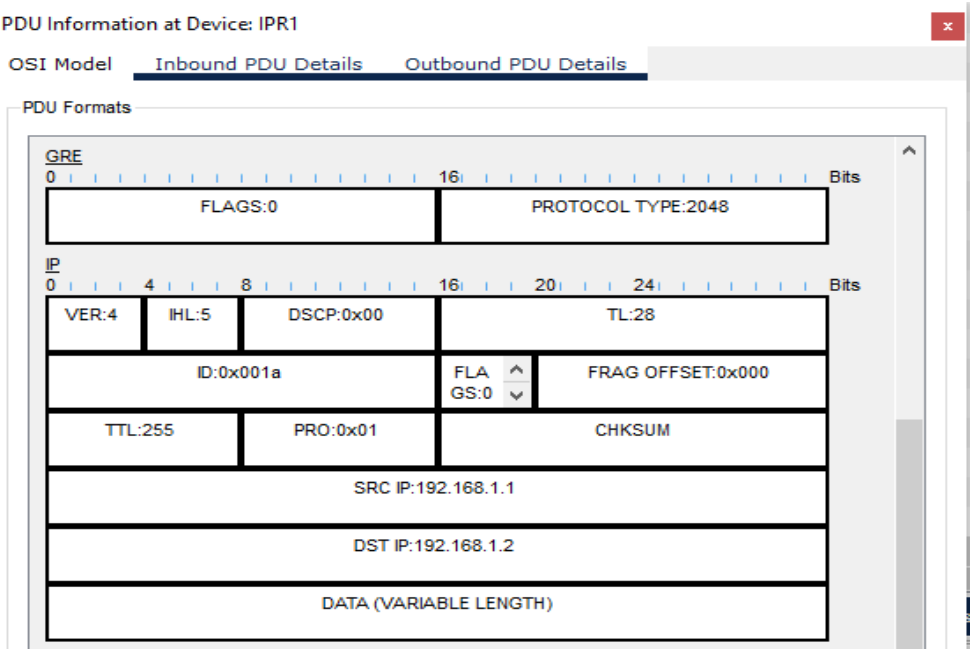
```
Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#ip route 0.0.0.0 0.0.0.0 200.0.0.1
Router(config)#
Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# ip route 0.0.0.0 0.0.0.0 100.0.0.1
Router(config)#
```

5. Теперь для проверки связи между R1 и R2 выполните команду ping от R1 к R2 и наоборот через виртуальную частную сеть.

```
Router(config)#do ping 192.168.1.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.2, timeout is 2
seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max =
0/0/1 ms
```

В режиме симуляции, наблюдая за движением пакетов и анализируя их содержимое, можно увидеть, что пакеты проходят от R1 к R2 через виртуальную частную сеть.



Контрольные вопросы:

1. Что такое VPN?
2. Как работает VPN?

3. Для чего нужен VPN?
4. Какова структура VPN?
5. Как обеспечивается безопасность VPN?
6. Как осуществляется подключение к интернету через VPN?
7. Кто может отслеживать интернет-трафик через VPN?
8. Законно ли использование VPN?
9. Какие риски связаны с использованием VPN?
10. Как использование VPN влияет на скорость интернета?
11. Как использование VPN обеспечивает анонимность?
12. Как использование VPN помогает обходить гео-блокировки?
13. Как использование VPN помогает загружать торренты?
14. Как использование VPN повышает безопасность Wi-Fi?
15. Как использование VPN помогает скрыть IP-адрес??

Пратическая работа № 5

Создание резервных баз данных и системы с использованием облачных технологий.

Цель работы: Изучение методов и средств резервного копирования баз данных и компьютерных систем с использованием облачных вычислений (cloud computing), а также механизмов их реализации.

Теоретический материал

Облачные технологии, или технологии облачных вычислений, — это технологии предоставления компьютерных ресурсов через интернет. Эти технологии позволяют пользователям хранить, обрабатывать и получать доступ к данным из любого места и в любое время.

Облачные технологии предоставляют серверы, хранилища, приложения, сети и другие IT-ресурсы в виде услуг через интернет. Эти технологии помогают пользователям быстро сократить время и затраты, связанные с приобретением, установкой и управлением необходимыми ресурсами.

Облачные технологии подразделяются на три типа:

1. Инфраструктура как услуга (IaaS) предоставляет пользователям виртуальные серверы и сетевую инфраструктуру.

2. Платформа как услуга (PaaS) предлагает платформы, необходимые для разработки, тестирования и управления приложениями.

3. Программное обеспечение как услуга (SaaS) представляет собой программы, предоставляемые через интернет. Пользователи могут получить к ним доступ через браузер и использовать их онлайн.

Облачные технологии помогают бизнесу расти, повышать гибкость и эффективность. Эти технологии стали одним из основных способов предоставления IT-услуг.

Облачное резервное копирование, также известное как онлайн-резервное копирование или удаленное резервное копирование, — это стратегия отправки физической или виртуальной копии файла или базы данных на вторичное, внешнее местоположение для сохранения в случае отказа оборудования, сбоя сайта или ошибки пользователя. Резервные серверы и системы хранения данных обычно размещаются третьей стороной или провайдером SaaS, который взимает периодическую плату в зависимости от используемого пространства для хранения, пропускной способности передачи данных, количества пользователей, числа серверов и других факторов.

Реализация облачного резервного копирования помогает защитить данные организации, обеспечить непрерывность бизнеса и соблюдать нормативные требования без увеличения нагрузки на IT-персонал. Экономия труда может быть значительной и может компенсировать некоторые дополнительные затраты, связанные с облачным резервным копированием, такие как плата за передачу данных.

Многие облачные подписки работают на ежемесячной или ежегодной основе. Если изначально онлайн-резервное копирование использовалось преимущественно потребителями и домашними офисами, то сейчас оно широко применяется как малыми, так и крупными предприятиями для резервного копирования различных типов данных. Для крупных компаний облачное резервное копирование может служить дополнительной формой резервного копирования.

Использование облачного резервного копирования и подходы

Приложение для резервного копирования в центре обработки данных организации создает копии данных и сохраняет их в различных средах или других системах хранения для удобного восстановления в случае необходимости. Хотя существует несколько вариантов и подходов к резервному копированию за пределами сайта, облачное резервное копирование часто служит внешним решением для многих организаций. В компании может быть собственный сервер за пределами сайта, если она имеет собственную облачную службу, но если компания использует провайдера услуг для управления средой облачного резервного копирования и регулярно оплачивает счета за хранение резервных копий, метод оплаты и услуги будут аналогичны.

Существуют различные подходы к облачному резервному копированию, которые легко интегрируются в существующие услуги, защищающие текущие данные организации. К видам облачного резервного копирования относятся:

1. Прямое резервное копирование в общедоступное облако:

- Один из способов хранения рабочих нагрузок организации - это репликация ресурсов в общедоступное облако. Этот метод включает запись данных напрямую в облачных провайдеров, таких как AWS, Google Cloud или Microsoft Azure. Организация использует свое собственное программное обеспечение для резервного копирования для создания копии данных, которая затем отправляется в облачное хранилище. Облачная служба хранения обеспечивает назначение и сохранность данных, но не предоставляет специальное приложение для резервного копирования. В этом сценарии важно, чтобы программное обеспечение для резервного копирования взаимодействовало с облачной службой хранения. Кроме того, с опциями

общедоступного облака IT-специалисты должны рассмотреть дополнительные меры защиты данных, такие как шифрование данных и управление идентификацией и доступом.

2. Резервное копирование у провайдера услуг:

- В этом сценарии организация записывает данные в облачную службу или провайдера SaaS, предлагающего резервные услуги в управляемом центре обработки данных. Программное обеспечение для резервного копирования, которое организация использует для отправки своих данных в службу, может быть предоставлено как часть услуги или служба может поддерживать коммерчески доступные специализированные приложения для резервного копирования.

3. Резервное копирование из облака в облако (C2C):

- Эти услуги являются одними из новейших предложений в области облачного резервного копирования. Они специализируются на создании резервных копий данных, уже существующих в облаке, таких как данные, созданные с помощью приложения SaaS, или данные, хранящиеся в облачной службе резервного копирования. Как следует из названия, служба C2C резервного копирования перемещает данные из одного облака в другое. Служба резервного копирования из облака в облако обычно включает программное обеспечение, которое управляет этим процессом.

4. Использование онлайн-систем облачного резервного копирования:

- Существуют также аппаратные альтернативы, которые облегчают резервное копирование данных в облачную службу резервного копирования. Эти устройства представляют собой универсальные резервные машины, включающие сервер резервного копирования, программное обеспечение для резервного копирования и объем диска. Оборудование обычно plug-and-play и большинство из них обеспечивают бесшовную интеграцию с одной или несколькими облачными службами резервного копирования или облачными провайдерами. Перечень поставщиков, предлагающих резервные устройства с облачными интерфейсами, включает Quantum, Unitrends, Arcserve, Rubrik, Cohesity, Dell EMC, StorageCraft и Asigra. Эти устройства обычно хранят самую последнюю резервную копию локально, что позволяет выполнять любые необходимые восстановления с локальной резервной копии, экономя время и затраты на передачу данных.

Принципы сбора информации

Облачные резервные копии обычно строятся вокруг клиентского программного приложения, которое работает по расписанию, определенному уровнем обслуживания и требованиями клиента. Например, если клиент заключил договор на ежедневное резервное копирование, программа будет

каждые 24 часа собирать, сжимать, шифровать данные и передавать их на серверы облачного провайдера. Чтобы уменьшить объем потребляемой пропускной способности и время, необходимое для передачи файлов, провайдер может предложить инкрементное резервное копирование после первоначального полного резервного копирования.

Облачные резервные копии часто включают программное и аппаратное обеспечение, необходимое для защиты данных организации, включая приложения Microsoft Exchange и SQL Server. Независимо от того, использует ли клиент свое собственное программное обеспечение для резервного копирования или программное обеспечение, предоставляемое облачной резервной службой, организация будет использовать это программное обеспечение для восстановления резервных данных. Восстановление может быть выполнено по файлам, по объему или путем полного восстановления всей резервной копии. Восстановление файлов по одному обычно является предпочтительным методом, поскольку оно позволяет быстро восстановить потерянные или поврежденные файлы без необходимости восстанавливать целые объемы, что может занять больше времени и увеличить риск.

Если объем восстанавливаемых данных очень велик, облачная резервная служба может отправить данные на полный массив хранения, к которому клиент может подключиться для восстановления своих данных. Это, по сути, обратный процесс начального копирования. Восстановление большого объема данных через сеть может занять неприемлемо много времени в зависимости от целевого времени восстановления (RTO) организации.

Ключевой особенностью восстановления облачных резервных копий является то, что оно может быть выполнено с практически любого компьютера и из любого места. Например, организация может восстановить свои данные напрямую на другой площадке или на сайт восстановления после аварии, если ее основной центр обработки данных недоступен.

Виды резервного копирования

В дополнение к различным подходам к облачному резервному копированию существует несколько методов резервного копирования, которые также необходимо рассмотреть. Хотя облачные провайдеры резервного копирования предоставляют клиентам возможность выбрать метод резервного копирования, который наилучшим образом соответствует их потребностям и приложениям, важно понимать различия между тремя основными типами.

Полные резервные копии копируют весь набор данных каждый раз при запуске резервного копирования. В результате они обеспечивают самый высокий уровень защиты. Однако большинство организаций не могут часто

выполнять полное резервное копирование, так как оно требует много времени и занимает значительный объем хранения данных.

Инкрементные резервные копии создают резервные копии только тех данных, которые были изменены или обновлены после последнего инкрементного или полного резервного копирования. Этот метод экономит время и место для хранения, но может усложнить полное восстановление, так как если какой-либо инкрементный файл будет потерян или поврежден, полное восстановление станет невозможным. Инкрементное облачное резервное копирование является распространенной формой, так как оно использует меньше ресурсов.

Дифференциальные резервные копии похожи на инкрементные, поскольку включают только измененные данные. Однако дифференциальные резервные копии создают резервные копии данных, измененных с момента последнего полного резервного копирования, а не с момента последнего инкрементного резервного копирования. Этот метод решает проблему сложного восстановления, которая может возникнуть с инкрементными резервными копиями.

Лучшие практики

Хотя стратегии, технологии и провайдеры облачного резервного копирования могут сильно различаться, существуют общепризнанные лучшие практики для их реализации в корпоративной среде. Вот несколько рекомендаций:

1. Понимание всех аспектов соглашения об уровне обслуживания (SLA) облачного провайдера:

- Узнайте все детали касательно резервного копирования и защиты данных, расположения офисов поставщика и того, как будут накапливаться расходы со временем. Понимайте ограничения ответственности провайдера и как получить помощь и исправление в случае необходимости.

2. Не полагайтесь на один метод или средство хранения данных:

- Методология резервного копирования 3-2-1 остаётся центральной политикой для корпоративных резервных копий.

3. Проверка стратегий резервного копирования и контрольных списков восстановления данных:

- Убедитесь, что они достаточны для чрезвычайных ситуаций. Подтверждайте резервные копии и периодически проверяйте процессы восстановления, чтобы удостовериться в достаточной квалификации технологий и персонала.

4. Регулярный мониторинг облачных резервных копий администраторами:

- Убедитесь, что процессы проходят успешно и не нарушены.

5. Выбор места для восстановления данных, которое легко доступно и не перезаписывает существующие данные:

- Определите, какие данные или файлы нужно резервировать, основываясь на их важности для бизнес-операций.

6. Использование метаданных для быстрой идентификации и восстановления определённых файлов:

- Применяйте метаданные правильно, чтобы обеспечить оперативное размещение и восстановление файлов.

7. Использование личного шифрования для данных, которые должны оставаться конфиденциальными:

- Рассмотрите возможность использования личного шифрования для защиты конфиденциальной информации.

8. Использование политики хранения данных и методов управления данными:

- Резервируйте только необходимые данные, особенно в облаке, где накапливаются повторяющиеся расходы.

Следование этим рекомендациям поможет обеспечить надёжную защиту данных и эффективное использование ресурсов при облачном резервном копировании.

Услуги, предоставляющие возможность облачного резервного копирования

Подходы к онлайн-резервному копированию разнообразны, поэтому организация должна тщательно рассмотреть SLA, ценовые планы и долгосрочные затраты перед выбором провайдера. Примеры вариантов облачных резервных копий у поставщиков включают:

- Acronis. Этот поставщик предлагает Cyber Backup, гибридное облачное резервное копирование как услугу. Acronis Cyber Backup защищает виртуальные, физические и облачные среды и включает бизнес-модель с оплатой по мере использования.

- Arcserve. С приобретением Zetta Arcserve расширил своё предложение единой защиты данных (UDP). Продукт Arcserve UDP Cloud Direct включает прямое резервное копирование и восстановление в облаке. Облачная защита ориентирована на средний рынок.

- Asigra. Пионер в области облачных резервных копий, Cloud Backup от Asigra имеет встроенные антивирусные движки, предотвращающие заражение резервных копий вредоносным ПО.

- Backblaze. Этот поставщик предлагает облачное резервное копирование для личных и бизнес-пользователей, а также облачное

хранилище. Backblaze хранит данные на открытой платформе Storage Pods и в облачной файловой системе Backblaze Vault. Доступ к резервным копиям данных можно получить через мобильные устройства и веб-браузеры на компьютерах. Восстановления загружаются через SSL.

- Carbonite. Продавая свои услуги частным лицам, малым и средним предприятиям и корпорациям, компания предлагает резервное копирование документов, электронной почты, музыки, фотографий и настроек для пользователей Windows и Mac. В марте 2018 года Carbonite приобрела конкурента Mozy у Dell EMC и включила его услуги в свои предложения. В 2019 году Carbonite приобрела поставщика кибербезопасности Webroot, а затем была куплена компанией по управлению контентом OpenText.

- CrashPlan. Этот поставщик предлагает варианты резервного копирования для малого бизнеса и корпоративных клиентов. Он поддерживает полное резервное копирование дисков на локальные диски и защищает сетевые диски Linux и macOS.

- Druva. Этот облачный поставщик резервного копирования имеет три основных предложения. Druva inSync предназначен для корпоративного уровня и ориентирован на конечные точки, создавая резервные копии данных на физическом и общедоступном облачном хранилище. Druva для гибридных рабочих нагрузок используется для резервного копирования и восстановления данных на распределенных физических и виртуальных серверах в облаке. В 2018 году Druva приобрела CloudRanger для защиты данных AWS.

- IDrive. Предназначенный для потребителей и малого бизнеса, IDrive включает снимки данных, сервис синхронизации и гибридную защиту данных.

- Microsoft Azure Backup. Эта служба автоматически отправляет резервные копии в облако Azure. Azure Site Recovery автоматизирует репликацию для резервного копирования частной Windows-инфраструктуры.

- Rubrik. Специализируясь на сильной безопасности и быстром восстановлении, Rubrik предлагает платформу управления данными для гибридных и многоклаудных сред.

- SpiderOak One Backup. Это предложение гибридного облачного резервного копирования для SMB защищает неограниченное количество устройств, включая внешние устройства, и предлагает до 5 ТБ хранилища.

- Unitrends. Этот поставщик позволяет клиентам создавать резервные копии в личном облаке на неограниченный срок с помощью Forever Cloud и предлагает несколько вариантов DRaaS для восстановления.

- Veeam Software. Veeam предоставляет облачное резервное копирование через свой продукт Cloud Connect. Поставщики услуг могут

сотрудничать с Veeam для создания целей резервного копирования и восстановления в облаке.

- Veritas NetBackup. Veritas обеспечивает единую защиту данных для физических, виртуальных и многоклаудных сред, которые могут управляться из одного окна.

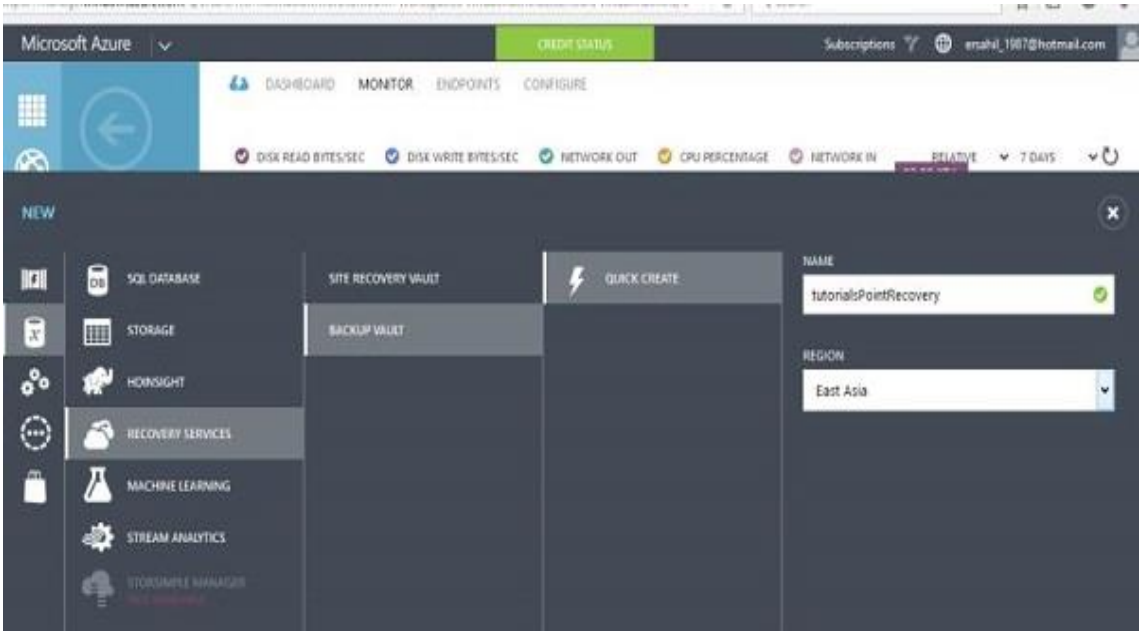
Практическая часть

Резервная копия Microsoft Azure может использоваться для резервного копирования локальных данных в облаке. Данные хранятся в зашифрованном виде. В следующих разделах подробно описано, как это сделать с помощью Microsoft Azure. В этом процессе мы сначала создадим хранилище для резервных копий, где будут храниться наши данные, а затем рассмотрим, как можно выполнять резервное копирование данных с нашего локального компьютера. Установленный на компьютере агент резервного копирования сначала шифрует данные, а затем отправляет их через сеть в хранилище Microsoft Azure. Ваши данные полностью защищены и находятся в безопасности.

Создание хранилища резервных копий

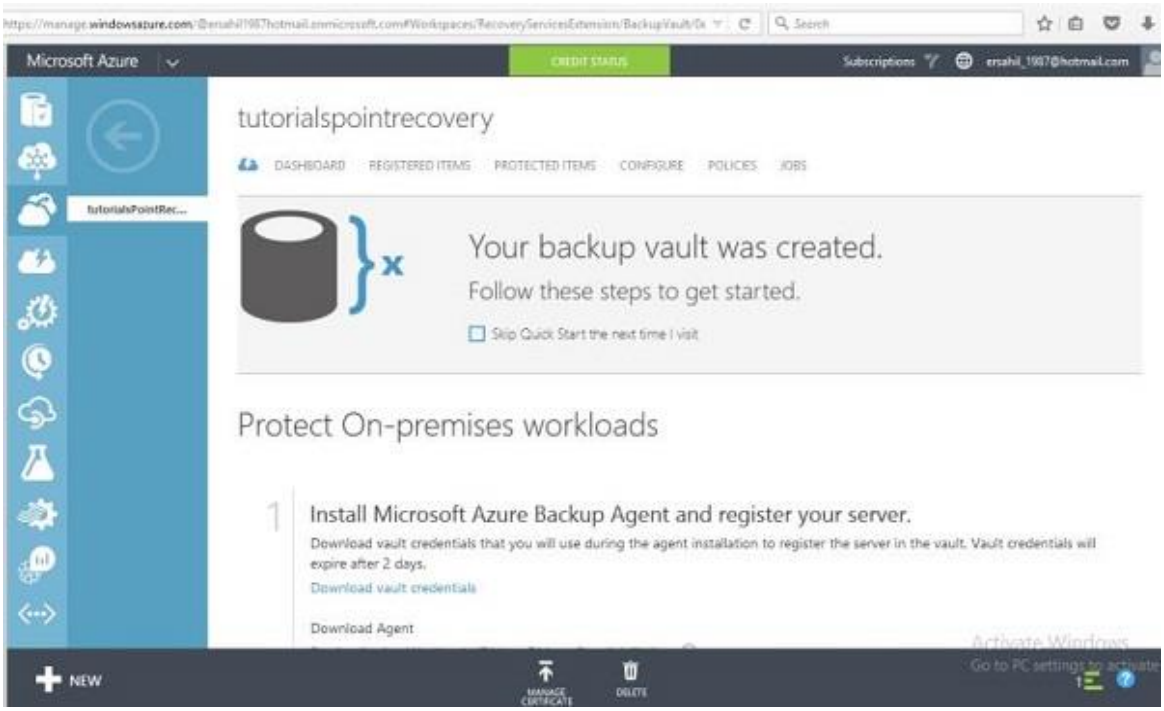
Шаг 1 - Войдите в ваш портал управления.

Шаг 2 - В правом нижнем углу выберите Новый → Службы данных → Службы восстановления → Хранилище резервных копий → Быстрое создание.



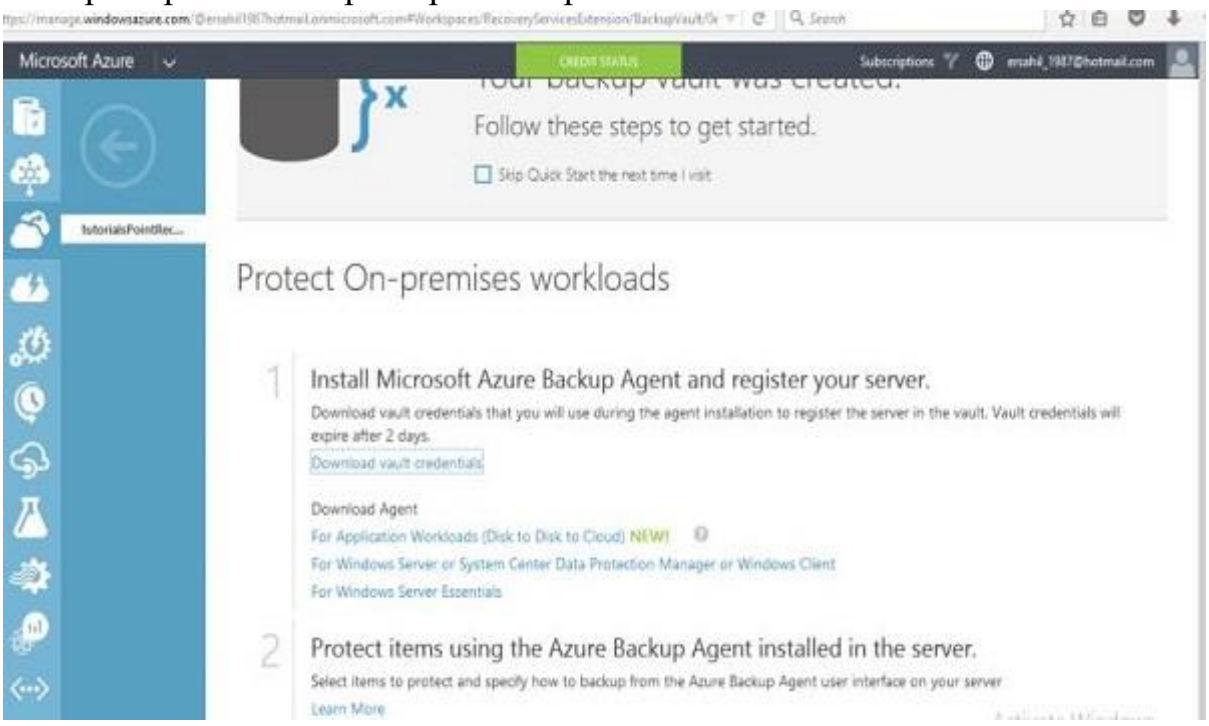
Шаг 3 - Введите имя хранилища и выберите регион. Хранилище будет создано и отображено в вашем портале управления.

Шаг 4 - Выберите созданное хранилище и нажмите кнопку «Скачать учетные данные», как показано на рисунке ниже.

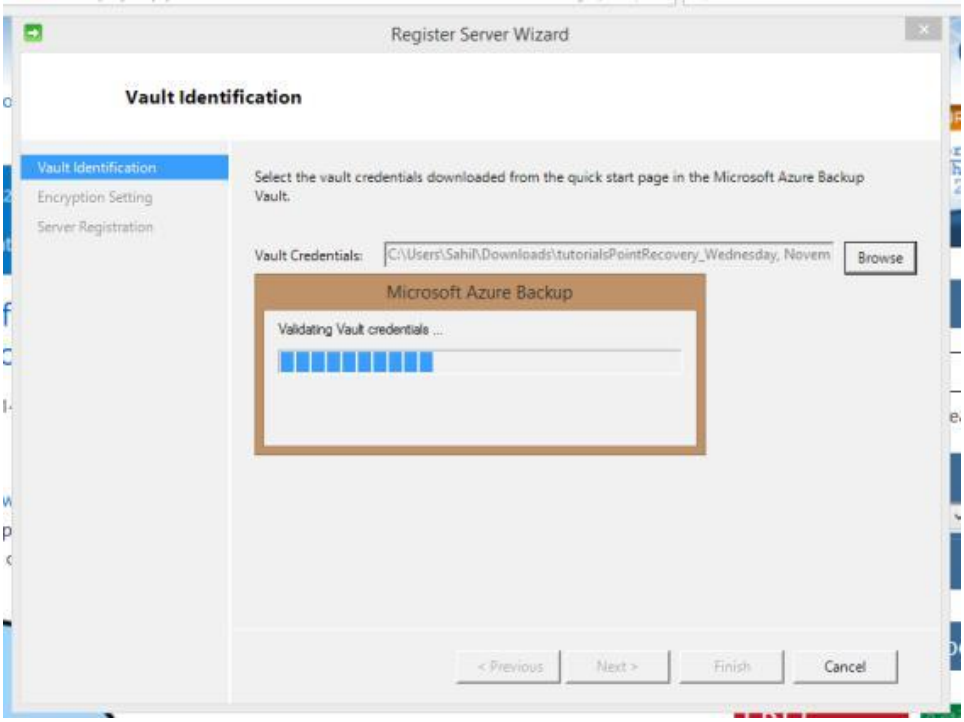


Шаг 5 - Это сохранит файл учетных данных на вашем компьютере.

Шаг 6 - Теперь прокрутите эту же страницу вниз в Microsoft Azure, и вы увидите три варианта под «Скачать агент». Выберите подходящий вариант. В этом примере мы выберем третий вариант из списка..



Шаг 7 - Настройки агента будут сохранены на вашем компьютере. Вам нужно будет следовать инструкциям для его установки. Процесс установки очень простой**.**

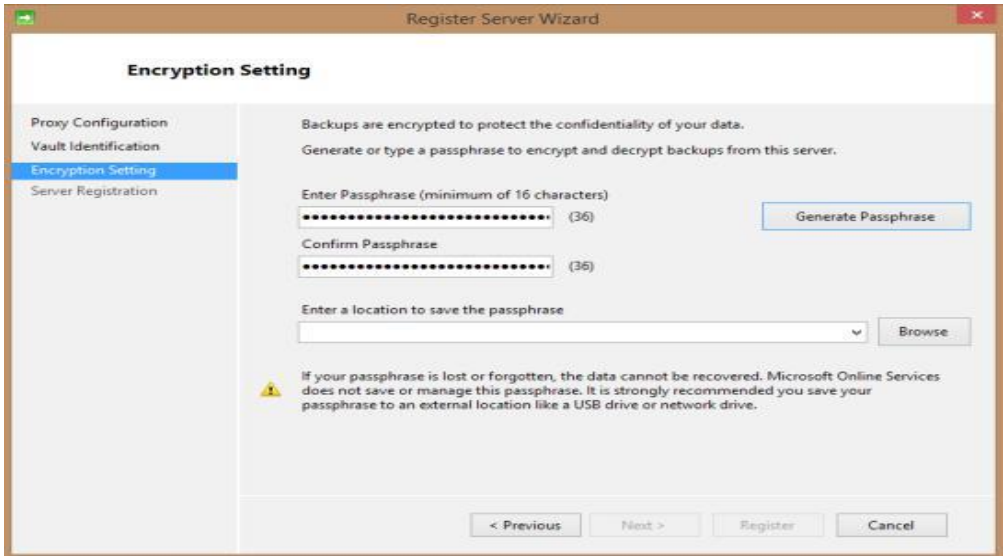


Шаг 8 - В конце установки вы увидите кнопку «Перейти к регистрации» в нижней части всплывающего окна. Нажмите эту кнопку, и появится следующий экран.

Шаг 9 - Первый шаг — это идентификация хранилища. Обзор файла учетных данных, сохраненного на вашем компьютере на последнем этапе.

Шаг 10 - Следующий шаг в мастере регистрации — выбор настроек шифрования. Вы можете ввести собственный пароль или позволить системе создать его. Здесь выберите «Создать пароль».

Шаг 11 - Укажите место для сохранения пароля. Очень важно сохранить этот файл пароля в безопасном месте, так как вы не сможете восстановить резервные копии без него.

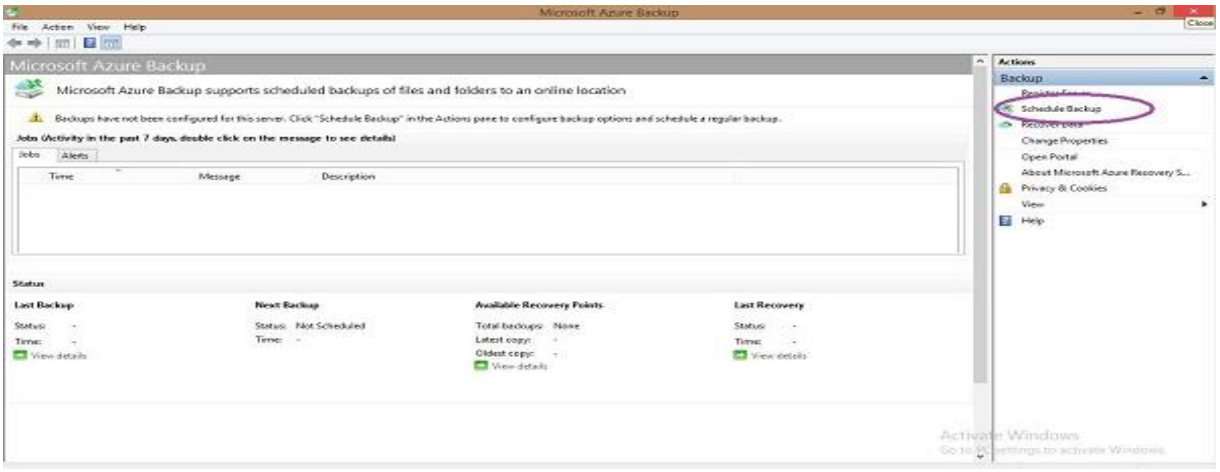


Шаг 12 - Нажмите кнопку «Далее», и файл будет сохранен в выбранном вами месте.

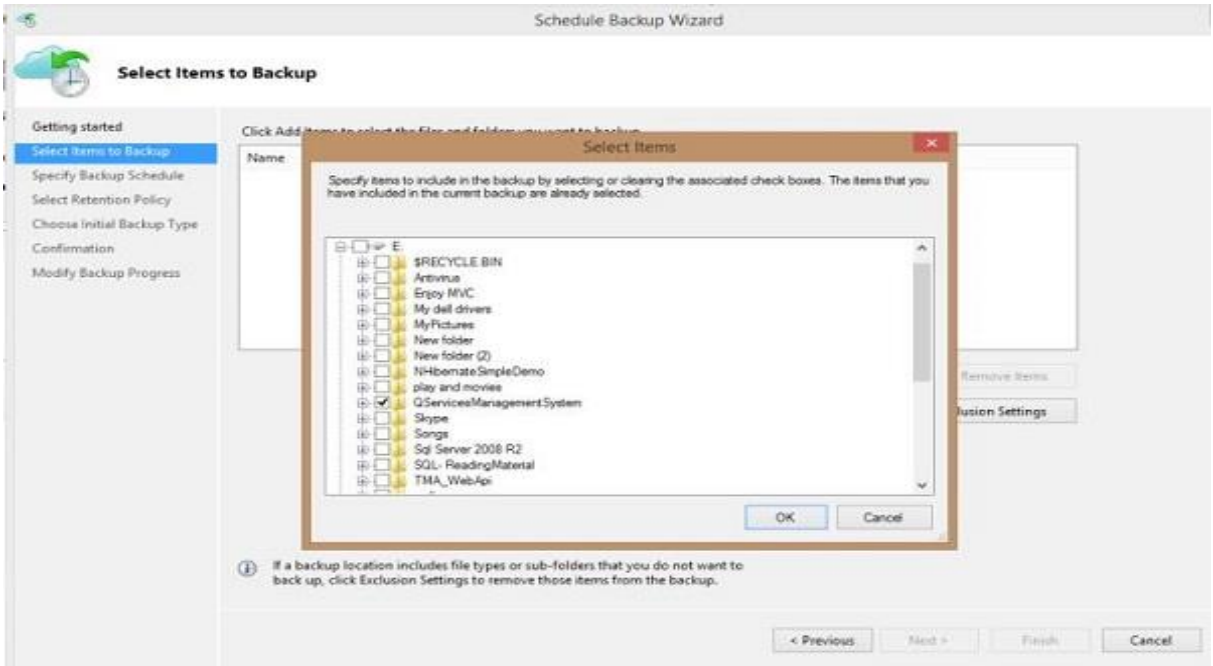
Планирование резервного копирования

После завершения процесса, описанного в предыдущем разделе, вы увидите следующее приложение, работающее на вашем компьютере, которое было установлено на предыдущем этапе. Вы выберете папку данных с вашего компьютера, которую хотите резервировать в Azure, и установите частоту резервного копирования.

Шаг 1 - Нажмите кнопку «Планировать резервное копирование» на правой панели.

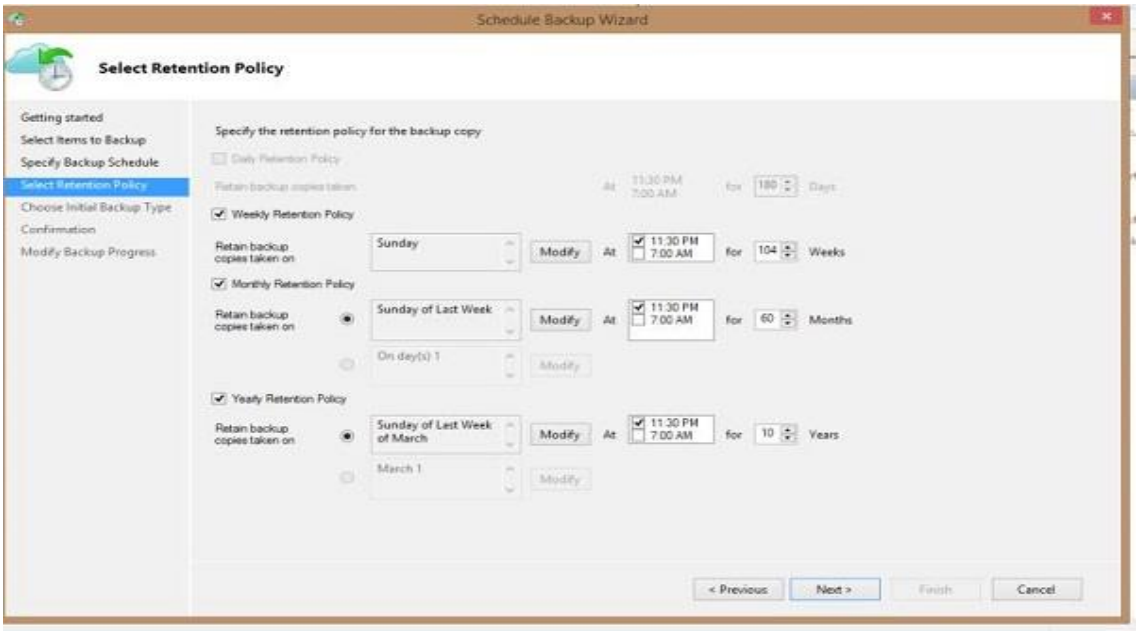


В этом примере выберите папку данных с именем «QServicesManagementSystem».

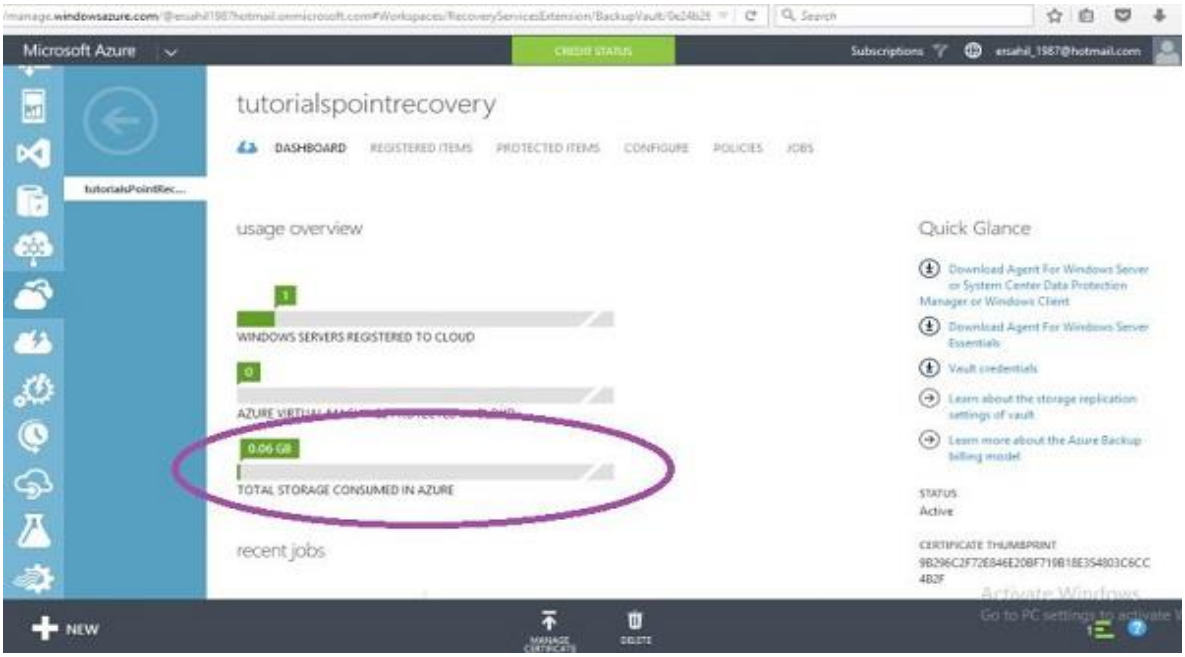


Следуйте пошаговым инструкциям на экране, они очень понятны. Вам разрешено создавать до 3 резервных копий, вы можете выбрать дневную или недельную частоту.

Шаг 2 – На следующем этапе выберите, как долго вы хотите хранить резервную копию в вашем онлайн-хранилище. Настройте это в соответствии с вашими потребностями.

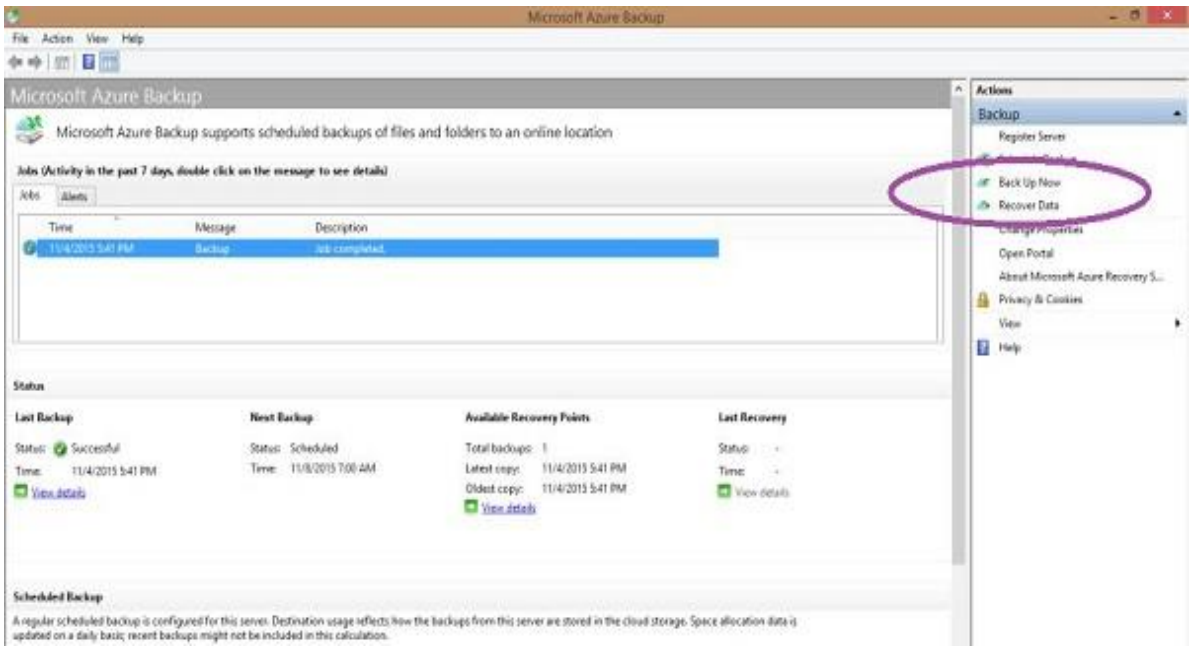


Шаг 3 - На левой панели агента резервного копирования выберите «Сделать резервную копию сейчас». Это сразу сохранит копию ваших данных. Затем вы можете выбрать хранилище резервных копий и перейти к его панели управления, чтобы увидеть его в управленческом портале.



На следующем изображении в разделе «Задания» вы можете увидеть один элемент, так как данные были сохранены с помощью опции «сделать резервную копию сейчас». Этот раздел показывает все действия в задаче резервного копирования. Подробности расписания резервного копирования отображаются в разделе «Состояние».

Шаг 4 - В агенте резервного копирования выберите «Восстановить данные» и следуйте инструкциям системы для восстановления данных.



Контрольные вопросы:

1. Что такое облачное резервное копирование?
2. Каковы основные характеристики облачного резервного копирования?
3. Какие коммерческие операции можно проводить с использованием облачных услуг?
4. Какие меры предприняты для обеспечения безопасности при использовании облачных услуг?
5. В каком порядке можно внедрять облачные услуги?
6. Что такое гибридные облака? Как они работают?
7. Какова экономическая структура использования облачных услуг?
8. Что означают IaaS, PaaS и SaaS? Какие типы облачных услуг они представляют?
9. Как обеспечивается поддержка облачных услуг?
10. Что такое бессерверные вычисления (serverless computing)? Каковы их преимущества?
11. Какие системы используются в облачном резервном копировании?
12. Как данные хранятся с использованием облачных услуг?
13. Как защищаются правовые аспекты безопасности при использовании облачных услуг?
14. Как внедряются изменения в облачные услуги?
15. Какие последние обновления происходят в области облачного резервного копирования?

Практическая работа № 6

Использование технологии PoE.

Цель работы: Знакомство с технологией PoE (Power over Ethernet – передача питания через Ethernet), исследование принципа ее работы и видов.

Теоретический материал

Технология PoE (Power over Ethernet) представляет собой систему, позволяющую передавать электрическую мощность вместе с потоком данных через витую пару Ethernet кабеля (UTP или STPЭто позволяет подключать к сети устройства, такие как беспроводные точки доступа (WAP), IP-камеры и VoIP-телефоны, одновременно обеспечивая их как передачей данных, так и достаточной электрической мощностью по одному кабелю.

Технология Power over Ethernet (PoE) поддерживает ряд протоколов сети Ethernet. Эта технология позволяет передавать мощность и данные по Ethernet-кабелю одновременно.

Технология PoE работает с следующими протоколами сети Ethernet:

- 10BASE-T: Этот протокол сети Ethernet работает на скорости 10 Мбит/с.

- 100BASE-TX: Этот протокол сети Ethernet работает на скорости 100 Мбит/с.

- 1000BASE-T и выше: Эти протоколы сети Ethernet работают на скоростях Gigabit Ethernet и выше.

Существует несколько общих методов передачи мощности через Ethernet-кабель. Три из них стандартизированы Институтом инженеров по электротехнике и электронике (IEEE) с 2003 года в рамках стандарта IEEE 802.3.

Они включают:

1. Тип A: Использует две из четырех пар сигнальных проводов обычного кабеля Cat 5 для передачи данных в 10BASE-T и 100BASE-TX.

2. Тип B: Разделяет провода для передачи данных и мощности в 10BASE-T/100BASE-TX, что облегчает устранение неисправностей.

3. 4PPoE: Использует все четыре пары витых проводов параллельно, увеличивая доступную мощность.

Тип A передает мощность по тем же проводам, что и данные, для вариантов Ethernet со скоростью 10 и 100 Мбит/с. Это похоже на технику фантомного питания, широко используемую для питания конденсаторных

микрофонов. Мощность передается по проводам данных за счет подачи общего напряжения на каждую пару. Поскольку витая пара Ethernet использует дифференциальные сигналы, это не мешает передаче данных. Общее напряжение легко извлекается с помощью центрального отвода стандартного Ethernet импульсного трансформатора. В Gigabit Ethernet и на более высоких скоростях мощность передается как по парам A, так и по парам B, поскольку для передачи данных на таких скоростях используются все четыре пары.

4PPoE обеспечивает подачу мощности через все четыре пары витых проводов. Это позволяет передавать большую мощность, что подходит для таких устройств, как панорамные камеры с функцией наклона и увеличения (PTZ), высокопроизводительные точки доступа (WAP) и даже для зарядки батарей ноутбуков.

Первоначальный стандарт PoE IEEE 802.3af-2003 обеспечивает до 15,4 Вт постоянной мощности (минимум 44 В постоянного тока и 350 мА) на каждый порт. Поскольку часть мощности теряется в кабеле, гарантируется, что на подключенное устройство поступит не менее 12,95 Вт.

Стандарт PoE IEEE 802.3at-2009, также известный как PoE+ или PoE Plus, предоставляет до 25,5 Вт мощности для устройств второго типа. Этот стандарт запрещает использовать все четыре пары для подачи мощности на подключенные устройства. Оба этих стандарта включены в издание IEEE 802.3-2012.

Стандарт IEEE 802.3bt-2018, который также известен как PoE++ или 4PPoE, расширяет возможности по подаче мощности по сравнению с 802.3at. Этот стандарт вводит два дополнительных типа мощности: до 51 Вт (тип 3) и до 71,3 Вт (тип 4). Каждая пара витых проводов должна поддерживать ток до 600 мА (тип 3) или 960 мА (тип 4). Стандарт также поддерживает 2.5GBASE-T, 5GBASE-T и 10GBASE-T. Эти улучшения открывают новые возможности для применения и способствуют более широкому использованию высокопроизводительных беспроводных точек доступа и камер наблюдения.

Стандарт IEEE 802.3bu-2016 ввел передачу мощности через данные линии (PoDL) для стандартов одномаршрутной передачи данных 100BASE-T1 и 1000BASE-T1, предназначенных для автомобильных и промышленных приложений. В двухпроводных или четырехпроводных стандартах на каждый провод пары подается одинаковое напряжение, поэтому внутри каждой пары нет разницы в напряжении, представляющего данные. В одномаршрутной

передаче данных через Ethernet мощность передается параллельно с данными. Изначально PoDL определил десять классов мощности (PD) в диапазоне от 0,5 до 50 Вт. Позже PoDL был расширен для поддержки 10BASE-T1, 2.5GBASE-T1, 5GBASE-T1 и 10GBASE-T1, и к 2021 году включает в себя 15 классов мощности с дополнительными промежуточными уровнями напряжения и мощности.

Применение

Рисунок - 6.1. Устройства работающие по технологии PoE.

1. **Беспроводные точки доступа (WAP)**:

Эти устройства обеспечивают беспроводную связь и могут быть установлены в местах, где нет доступа к источникам питания, что упрощает их установку и расширяет зону покрытия Wi-Fi.

2. **IP-камеры видеонаблюдения**:

IP-камеры могут получать питание и передавать видео по одному кабелю, что облегчает их установку в труднодоступных местах и уменьшает затраты на прокладку дополнительных кабелей.

3. **VoIP-телефоны**:

IP-телефоны получают питание и данные через Ethernet-кабель, что уменьшает количество проводов на рабочем месте и упрощает их установку и перемещение.

4. **Информационные табло и цифровые вывески**:

Эти устройства могут быть установлены в любом месте с доступом к Ethernet, что упрощает их использование в коммерческих и общественных местах для отображения информации.

5. **Системы безопасности и контроля доступа**:

Считыватели карт, камеры, контроллеры дверей и другие устройства безопасности могут получать питание через PoE, что упрощает их установку и обслуживание.

6. **Сетевые коммутаторы с поддержкой PoE**:

Эти коммутаторы обеспечивают питание PoE для подключенных к ним устройств, таких как IP-камеры и точки доступа, что устраняет необходимость в отдельных блоках питания для каждого устройства.

7. **Умные домофоны и системы контроля доступа**:

Эти устройства могут получать питание и передавать данные по одному кабелю, что упрощает их интеграцию в системы безопасности зданий.

8. **Медиаконвертеры**:

Устройства, преобразующие медные сигналы в оптические и обратно, могут использовать PoE для получения питания, что упрощает их установку и использование.

9. **Умные датчики и устройства IoT**:

Различные датчики и устройства Интернета вещей (IoT) могут получать питание через PoE, что облегчает их установку и управление в умных зданиях и промышленных средах.

Технология PoE позволяет значительно упростить процесс установки и уменьшить количество проводов, обеспечивая гибкость размещения устройств и снижение затрат на прокладку кабелей и обслуживание оборудования.

Преимущества технологии Power over Ethernet (PoE):

- Снижение затрат на установку: Возможность одновременной передачи питания и данных по одному кабелю уменьшает затраты на установку PoE-систем. Кроме того, для установки PoE-систем не требуется квалифицированный электрик.

- Безопасность: PoE-системы очень безопасны. Источники питания (PSE) подают питание только при обнаружении PoE-устройств.

- Гибкость: PoE-технология обеспечивает большую гибкость при установке сетевых устройств. Устройства можно устанавливать в наиболее удобных местах, не зависимо от розеток.

- Масштабируемость: PoE-технология позволяет легко расширять сеть, добавляя или удаляя устройства без прерывания работы сети.

- Сбор данных: PoE-технология удобна для сбора данных.

- Снижение требований к источникам питания: Уменьшает количество источников питания, требуемых для каждого установленного устройства, что экономит деньги.

Эти преимущества упрощают установку и управление сетевыми устройствами с использованием технологии PoE.

Недостатки технологии Power over Ethernet (PoE):

- Ограниченная выходная мощность: В зависимости от стандарта PoE, количество передаваемой энергии может быть ограничено, что недостаточно для некоторых устройств с высоким энергопотреблением.

- Ограничение расстояния: PoE ограничено максимальной длиной Ethernet-кабеля, которая обычно составляет 100 метров (328 футов).

- Поддержка нескольких устройств одновременно: Если один PoE-источник питания или коммутатор подключены к нескольким устройствам, проблемы с одним из этих устройств могут привести к отказу всех подключенных устройств.

- Проблемы с подачей питания: Современные PoE-источники питания могут сталкиваться с проблемами подачи питания. Например, они могут обеспечивать достаточную мощность для стандартных панорамных, наклонных и зум-камер, но недостаточны для устройств с высоким энергопотреблением, таких как сетевые PTZ-камеры.

Эти недостатки требуют осторожного использования технологии PoE.

Стандарты технологии Power over Ethernet (PoE):

- IEEE 802.3af: Этот стандарт был утвержден в 2003 году и определяет требования к проводам для передачи питания или данных.

- IEEE 802.3at (PoE+ или Type 2): Этот стандарт был утвержден в 2009 году и увеличивает мощность до 30 Вт.

- IEEE 802.3bt (4PPoE Type 3 и Type 4): Этот стандарт был утвержден в 2018 году и увеличивает мощность до 60 Вт (Type 3) и 90 Вт (Type 4).

Каждый новый стандарт обеспечивает совместимость и гибкость с предыдущими стандартами и определяет минимальное количество мощности, подаваемой на порт. Этот минимальный показатель учитывает потерю мощности по длине кабеля, что ограничивает максимальную длину до 100 метров (328 футов). С увеличением мощности требования к кабелям также повышаются, и кабель категории 5 остается минимальным требованием для PoE Type 3 (60 Вт) и Type 4 (90 Вт).

Требования к выполнению практической работы:

1. Сначала в симуляторе «Cisco Packet Tracer» создадим простую топологию с поддерживающими технологию PoE WAP и IP-телефоном. После добавления IP-телефона и WAP к коммутатору Cisco третьего уровня на рабочее пространство, мы подключим все устройства кабелями.

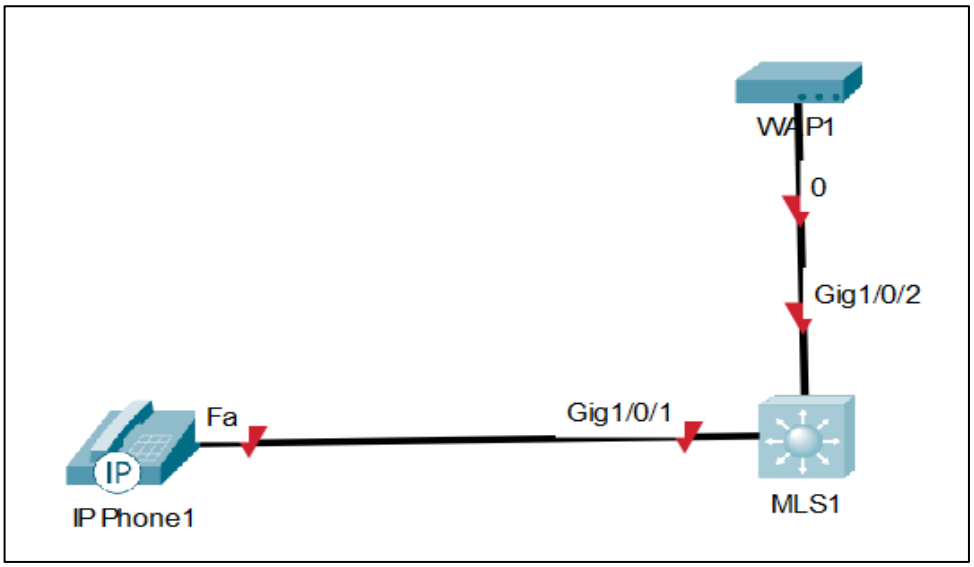


Рисунок - 6.2. Построение сети.

2. Затем один раз щелкните левой кнопкой мыши на “MLS1”, перейдите в открывшемся окне на вкладку “Physical”. Там в списке дополнительных модулей “MLS1” выберите источник питания “AC-POWER-SUPPLY”, удерживая левую кнопку мыши, подключите его к коммутатору.

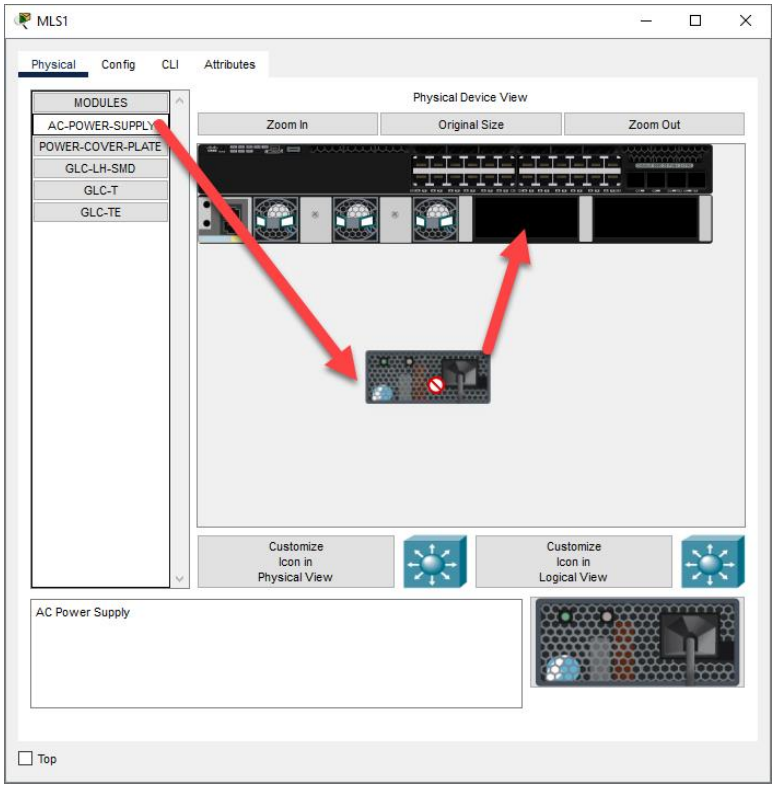


Рисунок - 6.3. Установка блока питания.

3. Чтобы открыть командную строку CLI, дважды щелкните по коммутатору. Введите «No» для пропуска первоначальной установки и нажмите Enter.

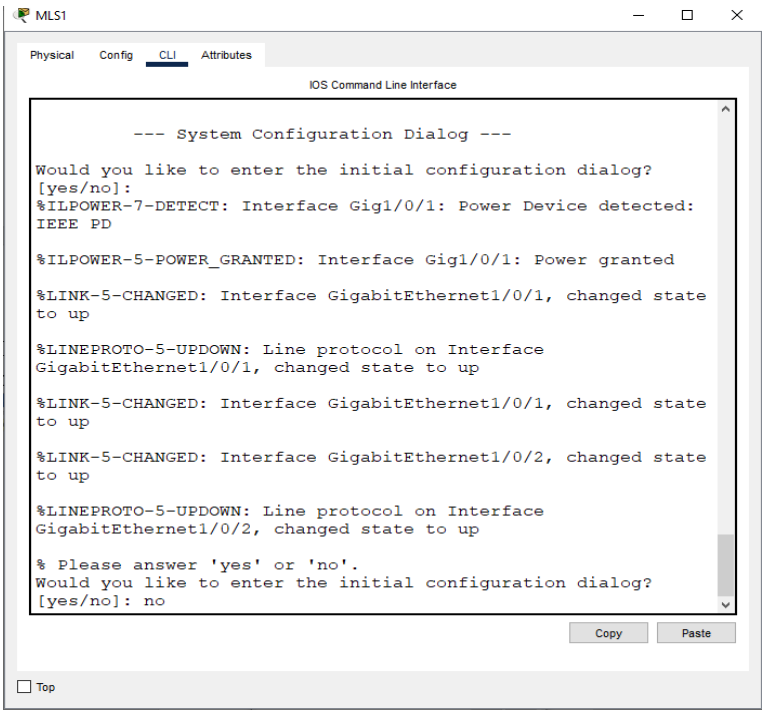


Рисунок - 6.4. Настройка устройства.

4. На следующем этапе мы вводим команду show power inline, чтобы просмотреть настройки питания коммутатора, и получаем следующий результат:

```
Switch>en
Switch#show power
Switch#show power inline
Available:390.0(w) Used:10.0(w) Remaining:380.0(w)
Interface Admin Oper PowerDevice Class Max
 (Watts)
--------- ------ ---------- ------- ------------------ ----- ----
Gig1/0/1 autoon10.0 Switch 79603 30.0
Gig1/0/2 autooff 0.0 n/a n/a30.0
Gig1/0/3 autooff 0.0 n/a n/a30.0
Gig1/0/4 autooff 0.0 n/a n/a30.0
Gig1/0/5 autooff 0.0 n/a n/a30.0
Gig1/0/6 autooff 0.0 n/a n/a30.0
Gig1/0/7 autooff 0.0 n/a n/a30.0
Gig1/0/8 autooff 0.0 n/a n/a30.0
Gig1/0/9 autooff 0.0 n/a n/a30.0
Gig1/0/10 autooff 0.0 n/a n/a30.0
Gig1/0/11 autooff 0.0 n/a n/a30.0
Gig1/0/12 autooff 0.0 n/a n/a30.0
Gig1/0/13 autooff 0.0 n/a n/a30.0
Gig1/0/14 autooff 0.0 n/a n/a30.0
Gig1/0/15 autooff 0.0 n/a n/a30.0
Gig1/0/16 autooff 0.0 n/a n/a30.0
Gig1/0/17 autooff 0.0 n/a n/a30.0
Gig1/0/18 autooff 0.0 n/a n/a30.0
Gig1/0/19 autooff 0.0 n/a n/a30.0
Gig1/0/20 autooff 0.0 n/a n/a30.0
Gig1/0/21 autooff 0.0 n/a n/a30.0
Gig1/0/22 autooff 0.0 n/a n/a30.0
Gig1/0/23 autooff 0.0 n/a n/a30.0
Gig1/0/24 autooff 0.0 n/a n/a30.0
```

Результат показывает, что каждый порт коммутатора может обеспечивать максимальную мощность 30 Вт, а общая мощность составляет 390 Вт.

Контрольные вопросы:

1. Что такое технология PoE?
2. Как работает технология PoE?
3. Какие устройства поддерживает технология PoE?
4. Какие преимущества дает технология PoE?
5. Какие недостатки у технологии PoE?
6. На каких стандартах основана технология PoE?
7. Что такое PoE+?
8. В чем разница между PoE+ и UPOE?
9. Когда был утвержден стандарт IEEE 802.3at PoE+?
10. Какие сетевые устройства поддерживает технология PoE?
11. Какие производители используют технологию PoE?
12. В каких сферах используется технология PoE?
13. Какие проблемы безопасности связаны с технологией PoE?
14. Какие технические характеристики имеет технология PoE?
15. С какими сетевыми стандартами работает технология PoE?
16. С какими сетевыми протоколами работает технология PoE?
17. В каких сетевых топологиях работает технология PoE?
18. Каким сетевым устройствам подходит технология PoE?
19. Каким сетевым устройствам не подходит технология PoE?
20. Какое энергопотребление требуется для поддержки различных сетевых устройств с технологией PoE?

Практическая работа № 7

Управление потоком трафика в сети.

Цель работы: Изучение методов и средств управления трафиком в компьютерных сетях, знакомство с существующими прикладными программами. Под управлением сетевым трафиком понимается процесс «захвата» (capture) и анализа сетевого трафика, а также направление трафика на оптимальные ресурсы на основе приоритетов. Основными компонентами, которые необходимо контролировать для улучшения управления сетью, являются производительность сети, трафик и безопасность. Инструменты управления сетевым трафиком используют методы мониторинга ширины сети и ее производительности, отслеживания шаблонов трафика для выявления и предотвращения препятствий, анализа безопасности сети и оптимизации для обеспечения оптимальной работы сети. Это помогает максимизировать производительность и безопасность сети за счет предотвращения перегрузок и угроз.

Сетевые инструменты управления трафиком обладают рядом преимуществ:

- *Устранение сбоев:* возможность видеть данные о производительности сети в реальном времени помогает выявлять и предотвращать потенциальные проблемы и сбои до их возникновения.

- *Быстрое и эффективное решение проблем: о*бнаружение препятствий в сети и других проблем, включая нерегулярные изменения в движении трафика и конфигурации, в реальном времени облегчает решение проблем.

- *Управление изменениями в сети:* помогает адаптироваться к росту и изменениям в сети, отслеживать аномальные колебания или угрозы, прогнозировать движение трафика и планировать требования для соответствия сетевым потребностям.

- *Обнаружение угроз безопасности:* анализ поведения сети позволяет различать необходимые уровни безопасности, помогая выявлять угрозы безопасности, включая серьезные инциденты, такие как атаки нулевого дня.

Инструмент управления сетевым трафиком:

Большинство инструментов управления сетевым трафиком в реальном времени включают функции мониторинга и оптимизации пропускной способности, однако их решения на этом не заканчиваются. Одним из самых важных аспектов управления сетевым трафиком, который почти всегда остается без внимания, является безопасность сети и анализ поведения. Отсутствие мощного решения по безопасности в дополнение к средству мониторинга сетевого трафика может оставить вашу сеть уязвимой для атак.

Идеальный инструмент для управления сетевым трафиком должен:

- Обеспечивать реальное время наблюдения за сетью;
- Анализировать поведенческие шаблоны и активно управлять трафиком;
- Обеспечивать быструю и эффективную диагностику и устранение проблем;
- Защищать вашу сеть от атак нулевого дня, внутренних угроз и неизвестных червей.

Управление сетевым трафиком в реальном времени с помощью NetFlow Analyzer

Контроль и управление сетевым трафиком крайне важны для максимальной эффективности вашей сети; полноценное решение для управления сетевым трафиком, такое как NetFlow Analyzer, значительно упрощает понимание того, что происходит в вашей сети. NetFlow Analyzer не только обеспечивает приоритетность приложений, важных для вашего бизнеса, и предотвращает перегрузку канала, но и предлагает множество других преимуществ, включая защиту вашей сети от сбоев, помощь в более быстром устранении и исправлении проблем, предвидение и предотвращение потенциальных узких мест, управление развитием вашей сети, более эффективное выявление угроз безопасности и, в конечном итоге, повышение рентабельности инвестиций (ROI).

Мониторинг сетевого трафика от начала до конца:

Причины сбоев или перегрузок в вашей сети могут быть различными, включая человеческие ошибки и угрозы безопасности. Визуализация сетевого трафика в реальном времени необходима для проактивного мониторинга и выявления любых проблем, которые могут повлиять на производительность сети. NetFlow Analyzer предоставляет вам полную информацию о вашей сети с помощью более 50 настраиваемых отчетов и графиков. Он отображает различные показатели, такие как использование полосы пропускания для каждого устройства и приложения, ведущие пользователи и сеансы, задержки и джиттер, давая вам ясную картину происходящего в вашей сети. NetFlow Analyzer также помогает устанавливать пороговые уведомления на основе объема, скорости и использования, информируя вас через электронную почту, SMS, SNMP-ловушки или систему заявок службы поддержки.

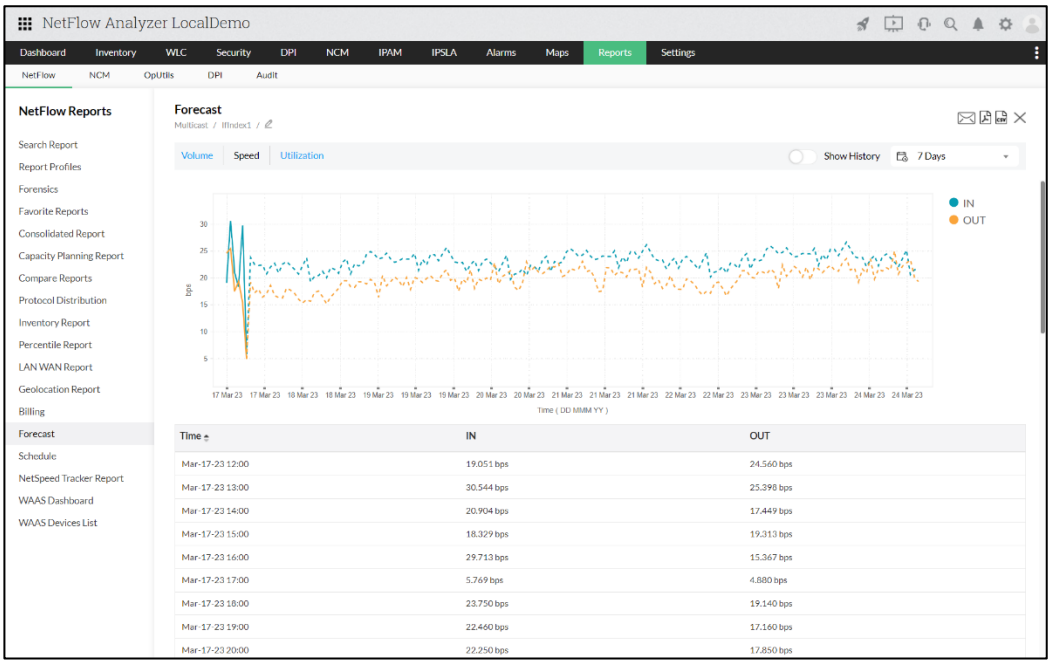


Рисунок - 7.1. Прогнозирование использования трафика с помощью NetFlow Analyzer.

Многие IT-администраторы хотят иметь инструмент управления сетевым трафиком, который способен предсказывать препятствия и другие неисправности, а также решать проблемы, связанные с работой сети, до того, как они возникнут. NetFlow Analyzer использует методы, такие как автокорреляция, декомпозиция сезонных трендов и регрессия, для прогнозирования тенденций использования пропускной способности. С помощью функции планирования ёмкости он предоставляет целостный обзор тенденций активности трафика и использования пропускной способности за выбранный интервал времени, а также помогает в планировании требований к пропускной способности и принятии обоснованных решений по обнаружению любых аномалий в росте трафика.

Формирование трафика для лучшей системы управления сетевым трафиком:

Управление сетевым трафиком включает в себя ограничение пропускной способности для определенных приложений и пользователей, приоритизацию трафика и приложений, а также обеспечение максимальной или минимальной пропускной способности для всех пользователей. Формирование трафика — это метод управления, который значительно ограничивает использование пропускной способности для несущественных приложений и пользователей. Для обеспечения оптимальной работы важных задач и приложений этот метод может задерживать определенные потоки или пакеты.

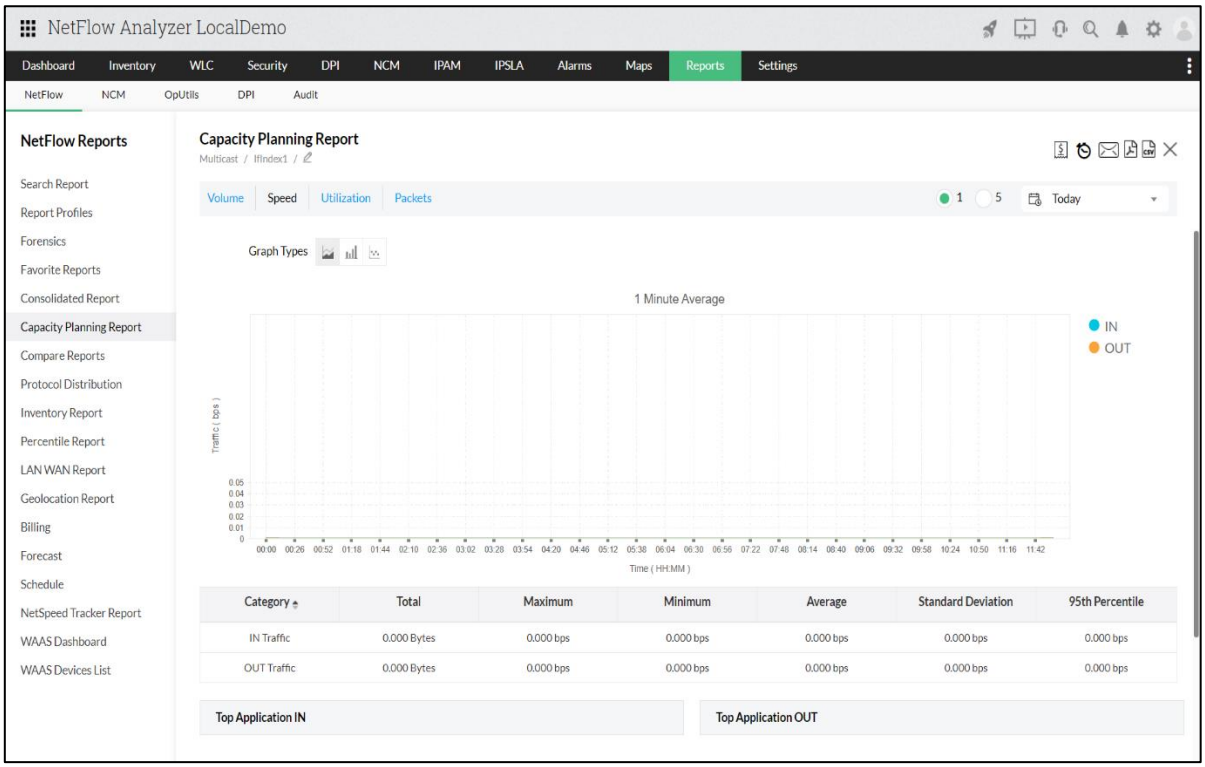


Рисунок - 7.2. Планирование пропускной способности сети.

NetFlow Analyzer использует различные методы управления трафиком, такие как списки управления доступом (ACL) и политики обслуживания, чтобы помочь вам переопределить политики качества обслуживания. Это помогает обеспечить хорошую работу сети, ограничивая или блокируя несущественные IP-адреса и приложения, потребляющие пропускную способность. Система Cisco CBQoS в NetFlow Analyzer позволяет вам просматривать образцы трафика на основе классов, что помогает проверять ваши политики и их эффективность.

Анализ сетевой безопасности и поведения

Для обеспечения сетевой безопасности не всегда легко или возможно иметь инструменты для обнаружения атак, помимо нескольких брандмауэров. Модуль продвинутого анализа безопасности NetFlow Analyzer представляет собой инструмент для анализа и обнаружения аномалий на основе потоков, который помогает выявить атаки или угрозы, превышающие возможности брандмауэра. Он предоставляет практическую разведку для обнаружения широкого спектра внутренних и внешних угроз и атак, таких как ботнеты, распределенные атаки отказа в обслуживании, нулевые дни и сканеры, которые могут повлиять на общую производительность сети или остановить её.

NetFlow Analyzer отслеживает каждый поток данных, чтобы защитить вашу сеть до того, как угроза станет атакой, и представляет эту информацию в одном удобном виде.

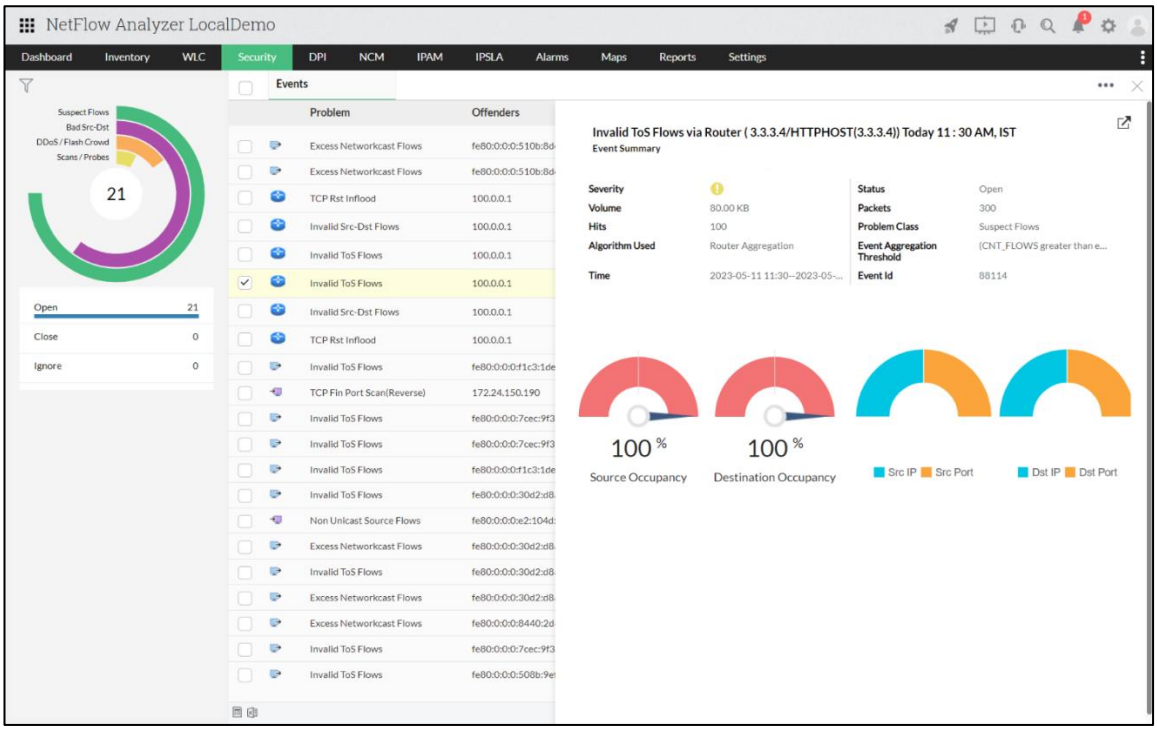


Рисунок - 7.3. Возможности безопасности NetFlow Analyzer.

Вот перевод на русский:

NetFlow Analyzer — это надежная и расширяемая платформа, предлагающая мониторинг пропускной способности и единственный анализ трафика.»

Установка «NetFlow Analyzer»:

1. Для установки NetFlow Analyzer на компьютер с Windows необходимо скачать его EXE-установочный файл по следующей ссылке:

https://www.manageengine.com/products/netflow/

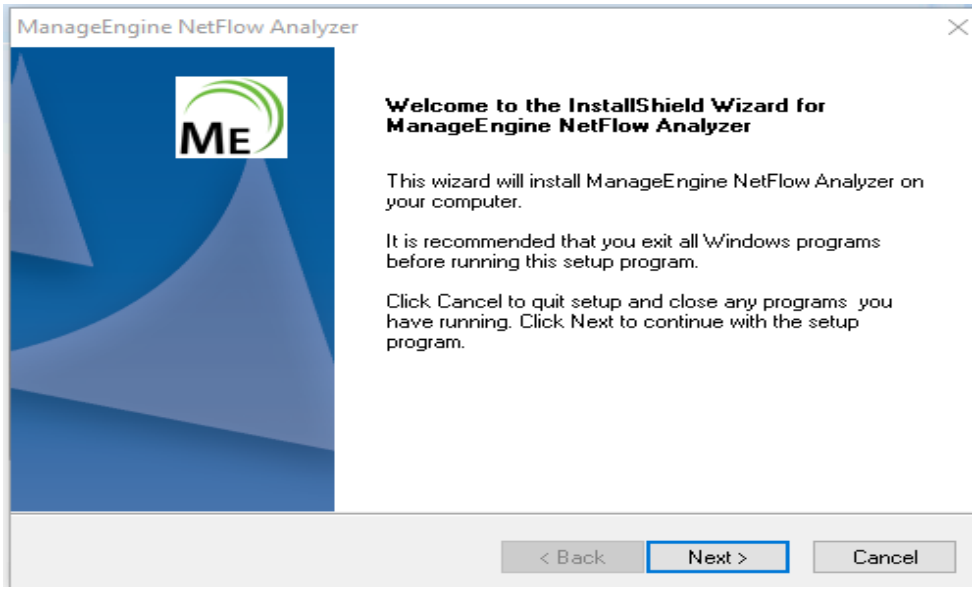


Рисунок - 7.4. Процесс установки.

2. После загрузки дважды щелкните правой кнопкой мыши на установочный файл и следуйте инструкциям, нажимая кнопки «Далее» для завершения установки программы.

3. После завершения установки программа NetFlow Analyzer автоматически запустится в виде веб-приложения в браузере. При первом запуске потребуется ввести логин и пароль для доступа к системе. По умолчанию логин и пароль установлены как admin/admin.

Основные возможности NetFlow Analyzer:

1. Мониторинг пропускной способности: Позволяет отслеживать и анализировать использование сетевой пропускной способности в реальном времени.

2. Анализ трафика: Предоставляет детализированные отчеты и графики о сетевом трафике, включая источники, назначения и типы данных.

3. Управление трафиком: Позволяет устанавливать приоритеты и ограничивать пропускную способность для определенных приложений или пользователей.

4. Оповещения и уведомления: Настраивает уведомления для предупреждения о сетевых проблемах, аномалиях и нарушениях.

5. Исторический анализ: Предоставляет исторические данные о трафике, что позволяет выявлять тенденции и аномалии.

6. Обнаружение и предотвращение угроз: Идентифицирует потенциальные угрозы, такие как ботнеты и DDoS-атаки, и помогает предотвратить их.

7. Отчеты и визуализация: Генерирует подробные отчеты и визуализации для анализа производительности и состояния сети.

8. Поддержка нескольких протоколов: Работает с различными сетевыми протоколами и стандартами для получения данных о трафике.

Этот программный продукт облегчает администраторам сети анализ пропускной способности и трафика, а также позволяет оптимизировать использование пропускной способности, проводить сетевое форенсическое расследование, анализировать сетевой трафик и мониторить сетевые потоки.

Контрольные вопросы:

1. Что такое управление сетевым трафиком?
2. Почему управление сетевым трафиком необходимо?
3. Как осуществляется управление сетевым трафиком?
4. Какие программы существуют для управления сетевым трафиком?
5. Какие оборудования необходимы для управления сетевым трафиком?
6. Как управление сетевым трафиком помогает устранить сетевые проблемы?
7. Как управление сетевым трафиком влияет на безопасность сети?
8. Как управление сетевым трафиком влияет на скорость работы сети?
9. Как управление сетевым трафиком обеспечивает надежную работу сети?
10. Как управление сетевым трафиком помогает администратору сети?
11. Как управление сетевым трафиком повышает эффективность сети?
12. Как управление сетевым трафиком влияет на использование ресурсов сети?
13. Как управление сетевым трафиком контролирует загрузку сети?
14. Как управление сетевым трафиком оптимизирует загрузку сети?
15. Какие методы существуют для расчета загрузки сети при управлении сетевым трафиком?

Практическая работа № 8

Настройка статической маршрутизации в программе Cisco Packet Tracer.

Цель работы: Овладение навыками работы со статической маршрутизацией через маршрутизатор.

Теоретическая часть

Существует два способа создания таблицы маршрутизации: статический и динамический. При статической маршрутизации записи в таблицу добавляются и изменяются вручную. Этот метод требует вмешательства администратора каждый раз, когда в сети происходят изменения. С другой стороны, он наиболее стабильный и требует минимальных ресурсов маршрутизатора для хранения таблицы. В динамической маршрутизации записи в таблице автоматически обновляются с помощью различных протоколов маршрутизации, таких как RIP, OSPF, IGRP, EIGRP и других. Кроме того, маршрутизатор строит оптимальные маршруты к целевым сетям, учитывая различные критерии (метрики), такие как промежуточные узлы, пропускная способность канала, задержка передачи данных и другие.

Статическая маршрутизация — это метод маршрутизации, при котором сетевой администратор вручную вводит информацию о маршрутах в таблицы маршрутизации каждого маршрутизатора. Это приводит к ряду недостатков. Во-первых, плохой масштабируемости сетей, так как при добавлении n+1 сетей необходимо ввести 2*(n+1) записей маршрутов. Однако одним из основных преимуществ статических записей является то, что процессору маршрутизатора не требуется выполнять вычисления для определения маршрутов.

Статическая маршрутизация успешно применяется в небольших компьютерных сетях (с 1-2 маршрутизаторами) благодаря простоте конфигурации и отсутствию дополнительной нагрузки от маршрутизационного трафика, как в случае с динамическими протоколами маршрутизации. Также она используется на отдельных компьютерах внутри сети, где часто указывается стандартный шлюз по умолчанию.

Маршрутизатор (или шлюз) — это сетевой узел с несколькими IP-интерфейсами, подключенными к различным IP-сетям, и имеющий как свой MAC-адрес, так и IP-адрес. В зависимости от задачи маршрутизации маршрутизатор перенаправляет дейтаграммы от отправителя к получателю между различными сетями. Как уже упоминалось, динамическая маршрутизация — это процесс, в котором протокол маршрутизации определяет, как устройство взаимодействует с соседними маршрутизаторами.

Маршрутизатор обновляет информацию о каждой сети, к которой он подключен. Если в сети происходят изменения, протокол динамической маршрутизации автоматически сообщает обо всех изменениях всем маршрутизаторам. Если вы используете статическую маршрутизацию, системный администратор должен обновить таблицы маршрутизации на всех устройствах вручную. **Статическая маршрутизация** уменьшает размер таблицы маршрутизации маршрутизаторов, где конечный маршрут обычно имеет стандартный маршрут (default) с адресом 0.0.0.0. Если в таблице маршрутизатора имеется такая запись, то пакеты, адрес которых не представлен в таблице маршрутизации, будут направлены на маршрутизатор, указанный в стандартной строке.

Стандартный шлюз (default gateway) — это адрес маршрутизатора, на который отправляется трафик, для которого нет отдельных записей в таблице маршрутизации. Использование стандартного шлюза для устройств, подключенных к тому же маршрутизатору (обычно рабочие станции), является единственным способом маршрутизации.

Наличие компьютера проверяется с помощью ICMP (Internet Control Message Protocol) управляющего сообщения, через которое любая конечная станция должна ответить на сообщение, отправленное узлом. В TCP/IP сетях программа ping обычно используется для проверки соединений. Эта программа отправляет ICMP Echo-Request на указанный IP-адрес хоста. После получения такого запроса проверяемый узел должен отправить ответный пакет (ICMP Echo-Reply). Первый узел записывает полученные ответы. Время между отправкой запроса и получением ответа (RTT, Round Trip Time) позволяет определить двухстороннюю задержку маршрута и частоту потерь пакетов, то есть косвенно оценить загрузку каналов передачи данных и промежуточных устройств.

Метрика — это числовой коэффициент, который влияет на выбор маршрута в компьютерных сетях. Обычно она определяется количеством «хопов» (пересылок) до целевой сети или параметрами канала связи. Чем меньше метрика, тем приоритетнее маршрут.

Цикл маршрутизации (Routing loop) — это ситуация, когда маршрутизатор отправляет пакет по неправильному адресу, и этот пакет возвращается к исходному маршрутизатору. Таким образом, образуется цикл. Для борьбы с такими циклами TCP/IP использует механизм TTL. Протоколы маршрутизации также предлагают свои методы работы с циклами.

Порядок выполенения практической работы

Рассмотрим настройку подключения двух сетей через маршрутизатор (рисунок 8.1).

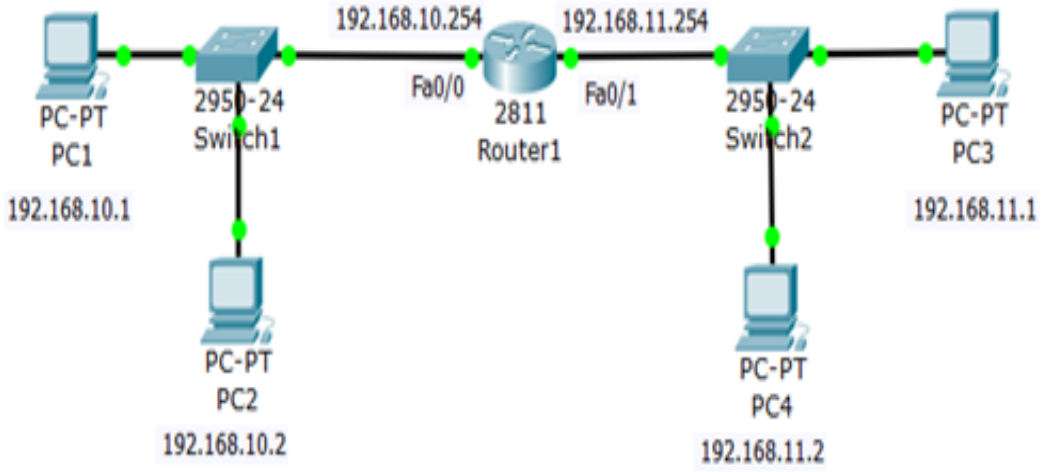


Рисунок - 8.1. Формулировка задачи.

Формулировка задачи

Наша цель — настроить подключение двух сетей через маршрутизатор.

Шаг 1. Настройка компьютеров, мы настроим компьютеры в сети 192.168.10.0 (см. рисунок 8.2).

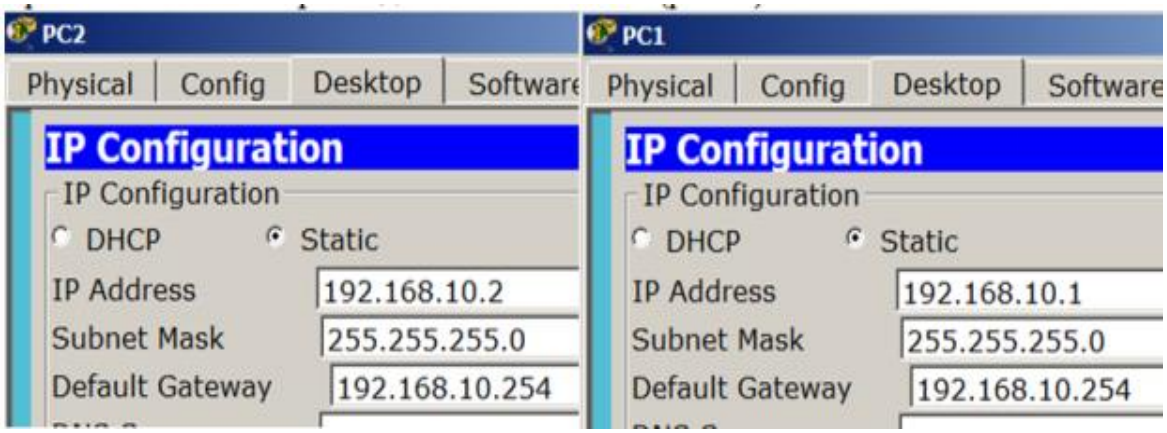


Рисунок - 8.2. Настройка компьютеров в сети 192.168.10.0.

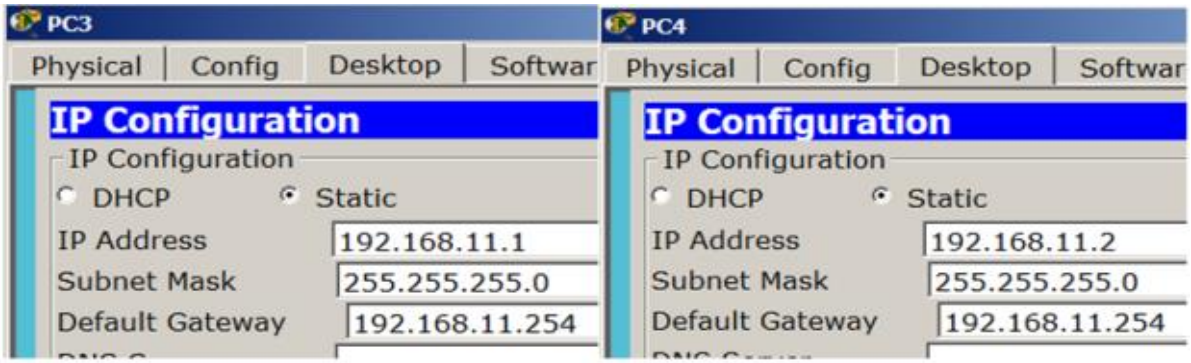


Рисунок – 8.3. Настройка компьютеров в сети 192.168.11.0.

Шаг 2. Настройка маршрутизатора

Мы настраиваем маршрутизатор как шлюз 192.168.10.254 для первой сети на интерфейсе Fa0/0 (см. рисунок 8.4).

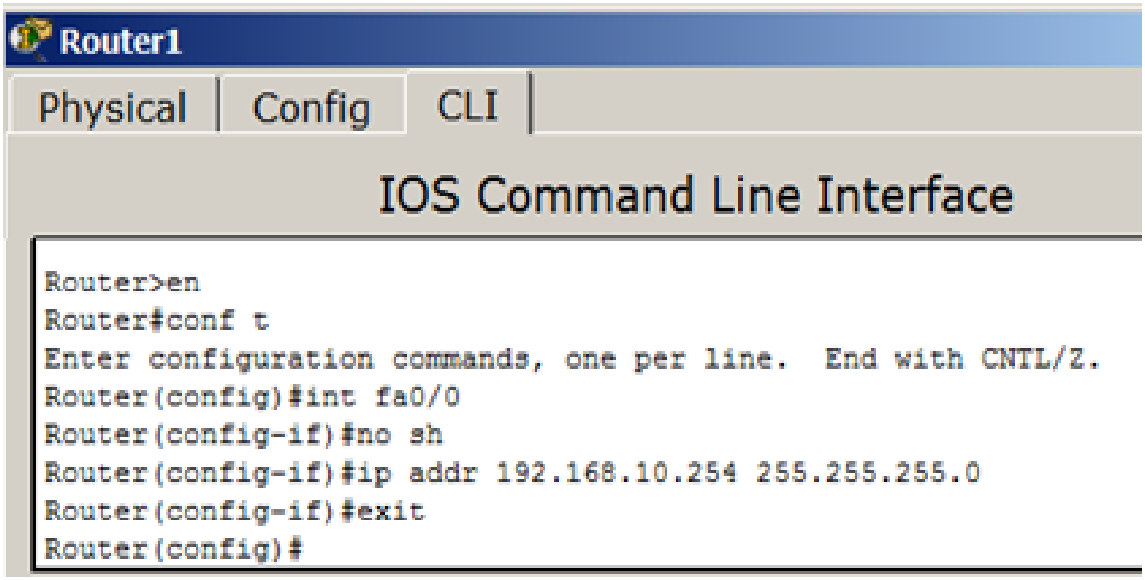


Рисунок - 8.4. Окно ввода команд.

Здесь описаны следующие команды: режим привилегий, режим конфигурации, вход в интерфейс, активация этого интерфейса, установка IP-адреса и маски подсети, выход из режима. Аналогичным образом мы настраиваем маршрутизатор в качестве шлюза 192.168.11.254 для второго сети на интерфейсе Fa0/1 (см рисунок 8.5).

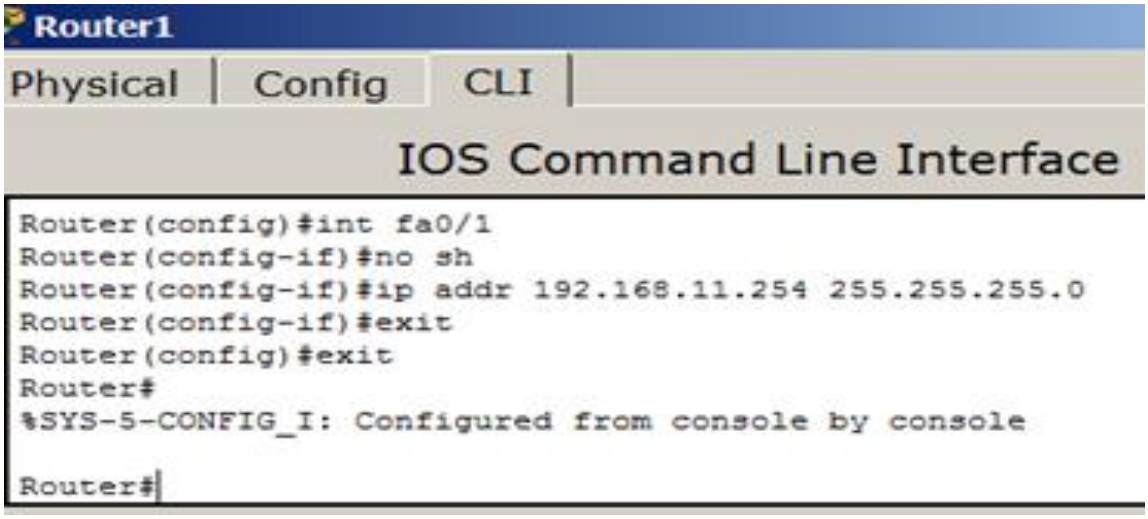


Рисунок - 8.5. Настройка R1 в качестве шлюза 192.168.11.254 для второго сети.

Шаг - 3 Проверка соединения сети

Проверяем таблицу маршрутизации маршрутизатора с помощью команды `show ip route` (см. рисунок 8.6).

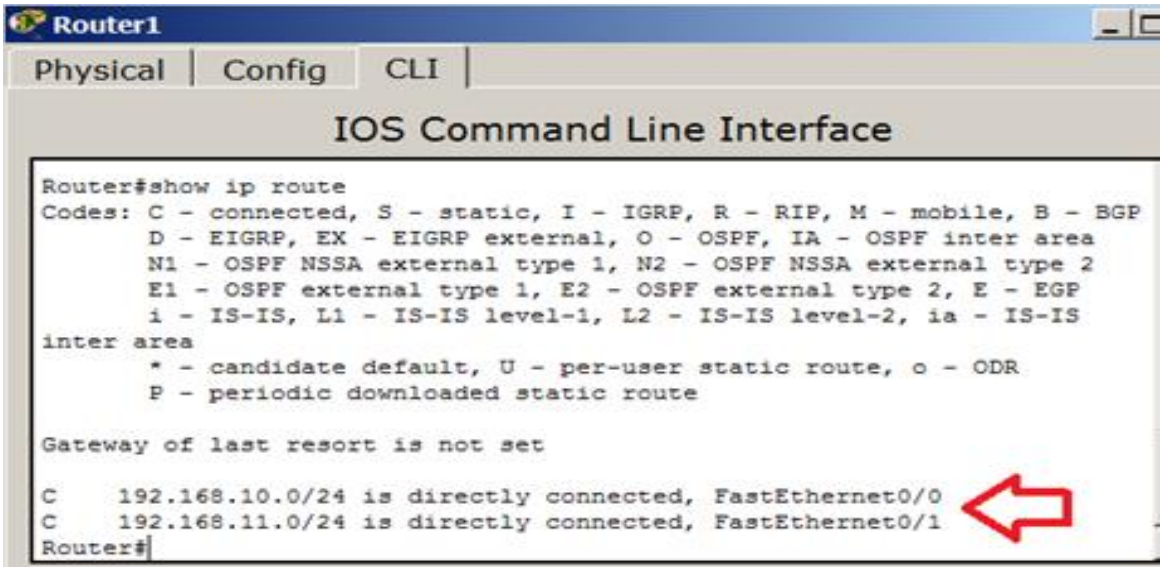


Рисунок 8.6. Проверка таблицы маршрутизации маршрутизатора R1.

Наш маршрутизатор обслуживает две сети. Проверим связь между маршрутизатором и компьютером (см рис. 8.7).

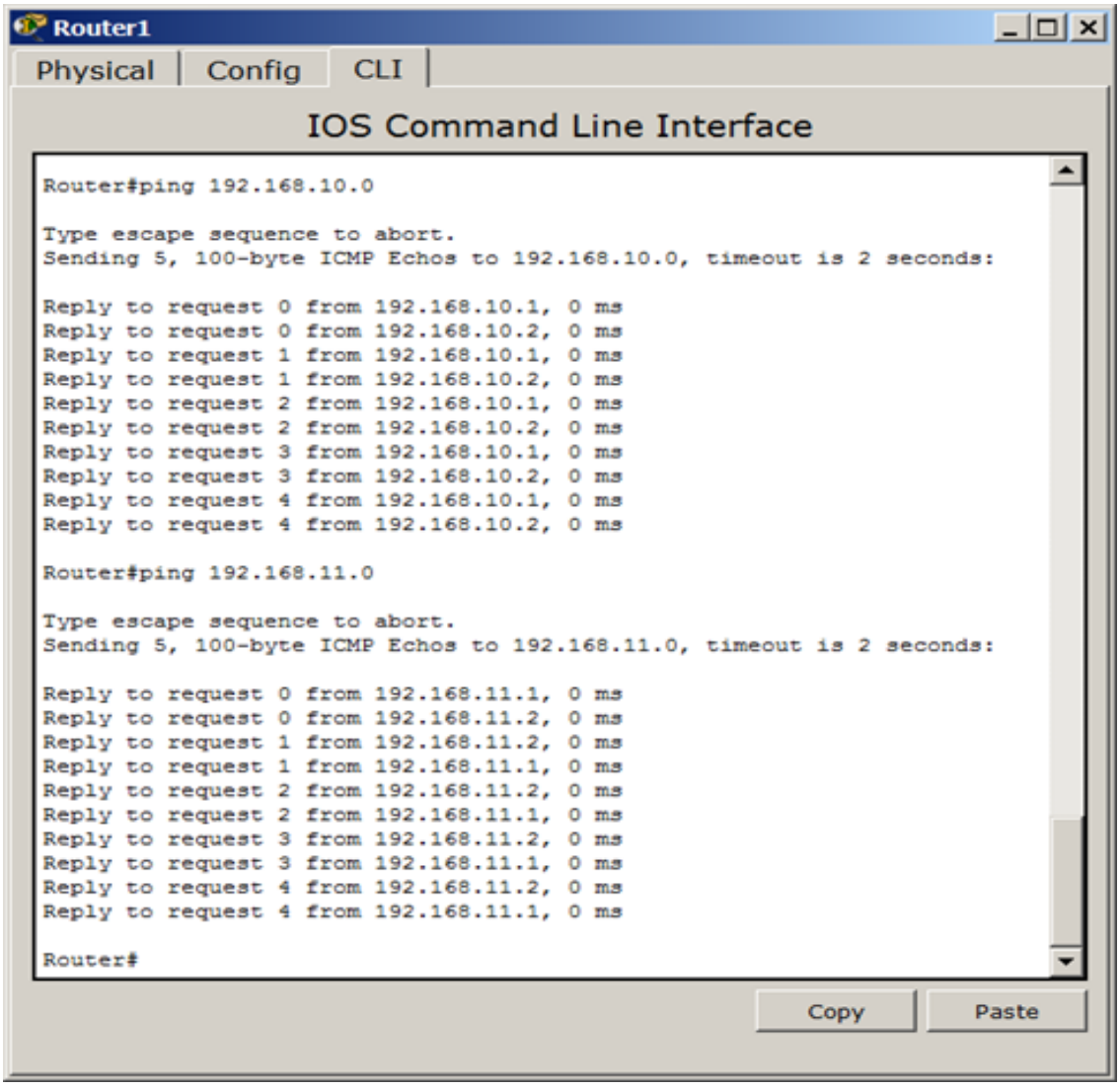


Рисунок. 8.7. Маршрутизатор имеет связь со всеми персональными компьютерами.

Проверяем подключение маршрутизатора к подсети (см рис. 8.8).

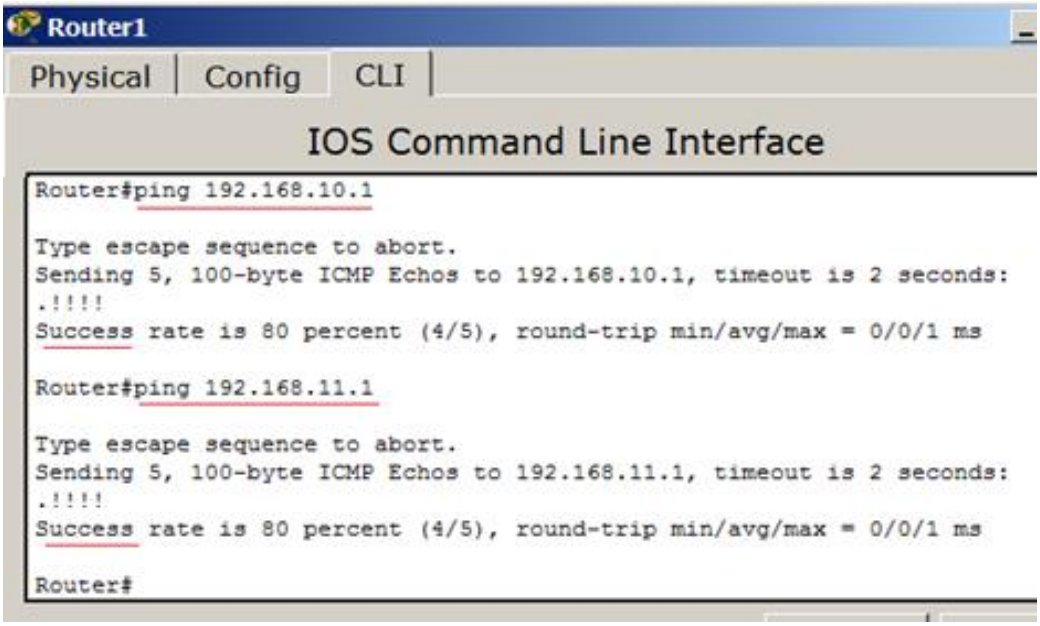


Рисунок - 8.8. Проверка подключения маршрутизатора к подсетям.

Команда Ping отправляет запрос ICMP (эхо-пакет) для проверки подключения. В приведенном выше примере один из запросов превысил установленное время транзита, что указано в строке времени. Также проверим связь между персональными компьютерами из разных сетей (рис. 8.9).

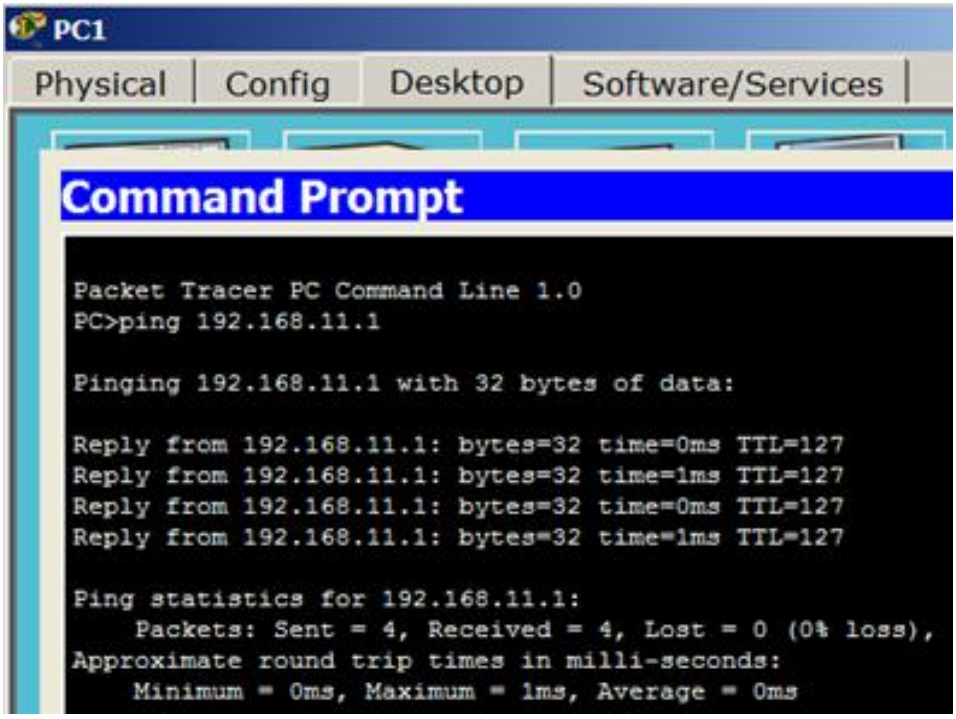


Рисунок - 8.9. Проверка связи между ПК1 и ПК3.

На рисунке - 8.10. Порт маршрутизатора. Как вы видите, к нему подключен кабель RJ-45.

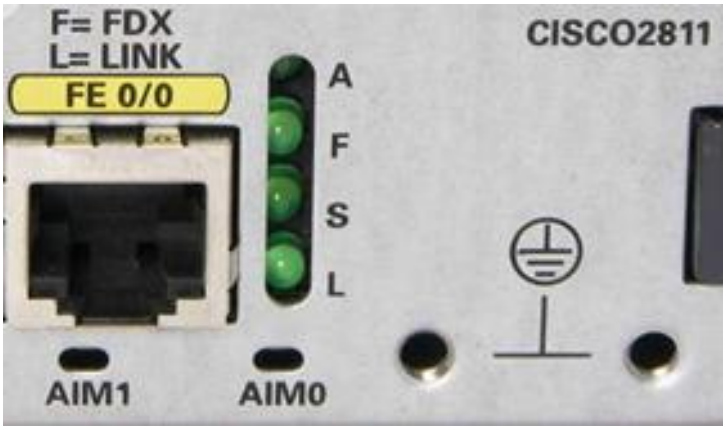


Рисунок - 8.10. Ethernet-порт 0/0 маршрутизатора CISCO 2811.

Задание по практической работе

Задание - 1. Настройка статической маршрутизации на устройствах Cisco

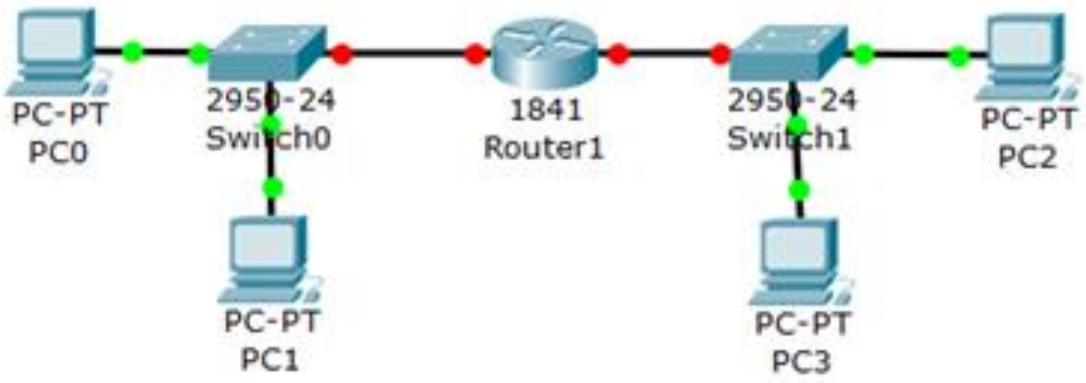


Рисунок - 8.11. Схема сети.

Выполните все примеры по установлению связи между двумя сетями, приведённые на рисунке 8.11:

1. Настройте компьютер
2. Настройте маршрутизатор
3. Проверьте сетевое соединение
4. Определите, какой протокол обеспечивает уникальные IP-адреса в сети
5. Покажите, как узлы сети связаны с портами маршрутизатора в качестве шлюза по умолчанию.

В процессе выполнения задания необходимо сделать следующее:

1. Назначить IP-адреса на сетевые интерфейсы маршрутизаторов, управляющие интерфейсы коммутаторов и сетевые интерфейсы локальных компьютеров.
2. Установить физическое и канальное соединение между соседними маршрутизаторами через последовательный сетевой интерфейс.

3. Обеспечить возможность передачи данных по протоколу IP между соседними сетевыми объектами (C1-S1, C1-R1, S1-R1, R1-R2, R2-S2, R2-C2 и другими).

4. Настроить статические маршруты к сетям локальных компьютеров C1 и C3 на маршрутизаторе R2.

5. Настроить «стандартные» маршруты к сетям локальных компьютеров C2-C3 и C1-C2 соответственно на маршрутизаторах R1 и R3.

6. Обеспечить возможность передачи данных по протоколу IP между любыми сетевыми объектами (ping).

7. Перейти в «режим симуляции», просмотреть и объяснить процесс обмена данными между устройствами с использованием протокола ICMP (выполнив команду ping с одного компьютера на другой), объяснить роль протокола ARP в этом процессе.

Задание - 2 Настройка трех сетей с WEB-сервером. Понятие стандартного маршрута.

Мы будем работать со схемой, состоящей из следующих устройств:

- два коммутатора 2950-24, два компьютера 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 (модель 1841) с маской 255.255.255.252 и сетью 192.168.1.0.

- Компьютеры в сети 192.168.10.0 должны иметь доступ к DNS-серверу в сети 192.168.20.0 (рисунок 8.12).

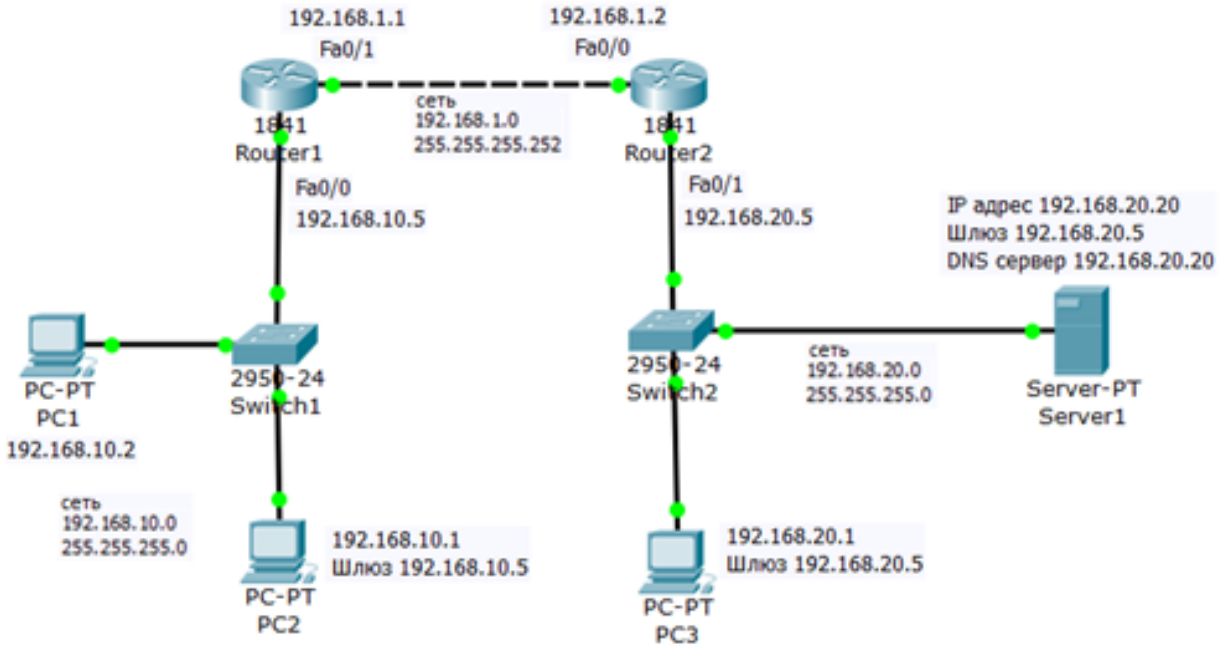


Рисунок - 8.12. Проект сети.

Наша сеть несложная, в ней нет большого количества компьютеров, поэтому мы будем использовать статическую маршрутизацию, а не динамическую.

Настройка сетевого интерфейса для маршрутизаторов

Мы настроим подключение маршрутизаторов через порты Fa0 / 1 для R1 и Fa0 / 0 для R2. Настроим Router1 на основе постановки задачи в сети 192.168.1.0 с маской 255.255.255.252. Поэтому мы присваиваем IP-адрес 192.168.1.1 порту Fa 0/1 (рис. 8.13).

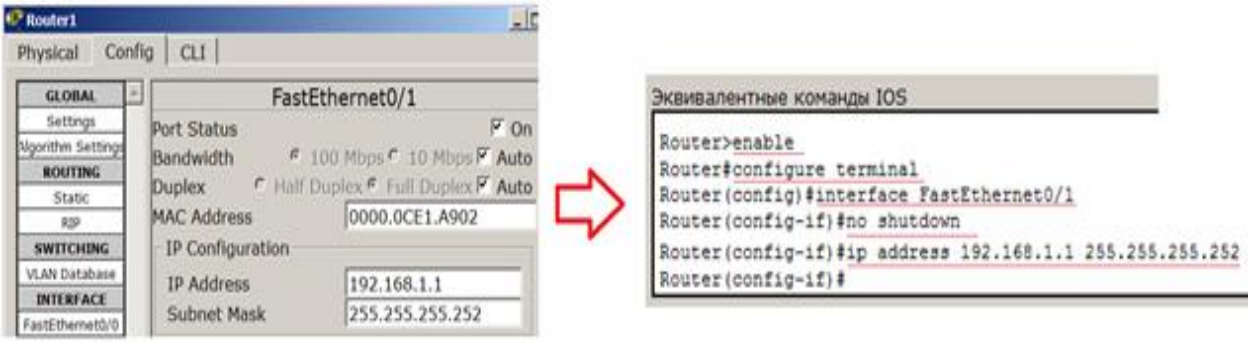


Рисунок - 8.13. Окно настройки порта 0/1 для маршрутизатора R1.

При настройке через веб-интерфейс убедитесь, что установлен **флажок On** в поле, эквивалентном команде no shutdown.

Альтернативно, все параметры маршрутизатора можно настроить через командную строку на вкладке CLI с помощью следующих команд: enable (включение привилегированного режима), **config terminal** (вход в режим конфигурации), **interface** fastethernet0/1 (настройка интерфейса 100mb Ethernet 0/1), **ip address** 192.168.1.1 255.255.255.252 (установка IP-адреса интерфейса и маски сети маршрутизатора), **no shutdown** (включение интерфейса - по умолчанию все выключено), **exit** (выход из режима настройки интерфейса), end (завершение редактирования), **write** (сохранение конфигурации).

Точно так же мы настраиваем Router2 на основе задачи с сетью между маршрутизаторами 192.168.1.0 с маской 255.255.255.252. IP-адрес 192.168.1.2 назначается порту Fa0/0 (рисунок 8.14).

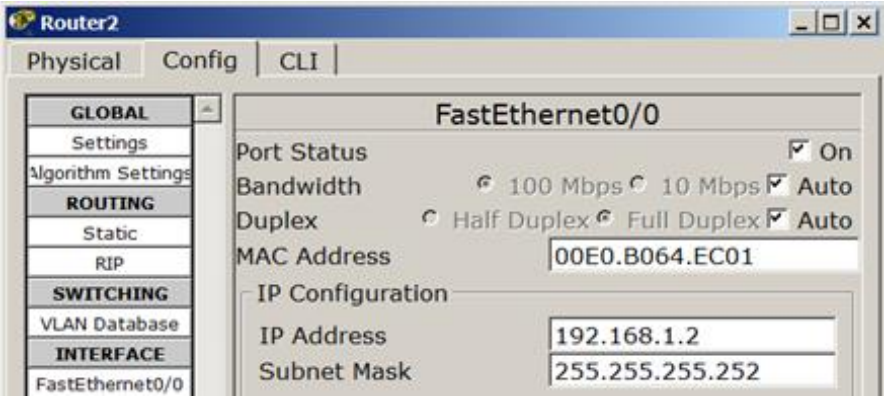


Рисунок - 8.14. Окно настройки R2.

При настройке маршрутизатора с командной строки вы можете использовать сокращенные команды: en (включить привилегированный режим). **conf t** (войти в режим конфигурации). **int fa0/0** (настроить интерфейс Ethernet 0/0 на 100 Мб). **IP addr** 192.168.1.2 255.255.255.252 (ввести IP-адрес интерфейса и маску сети). **No shut** (включить интерфейс - по умолчанию он выключен). **exit** (выйти из режима настройки интерфейса). **end** (завершить редактирование). **wr** (сохранить конфигурацию). В результате, после настройки маршрутизаторов, индикаторы портов загорятся зелеными, что означает наличие связи между ними. Сеть между маршрутизаторами работает, но маршрутизация пока не настроена, то есть переход из одной сети в другую невозможен.

Настройка соединения маршрутизаторов с подсетью

Настроим порт Fa0/0 маршрутизатора R1 для работы с сетью 192.168.10.0 (рис. 8.15).

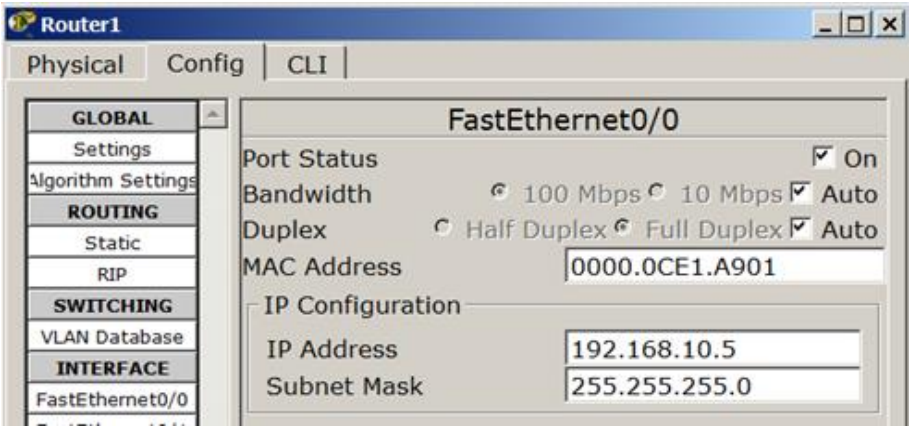


Рисунок - 8.15. Окно настройки порта Fa0 / 0 маршрутизатора R1 для работы с сетью 192.168.10.0.

Аналогичным образом настроим порт Fa0 / 1 маршрутизатора R2 для работы с сетью 192.168.20.0 (рис. 8.16).

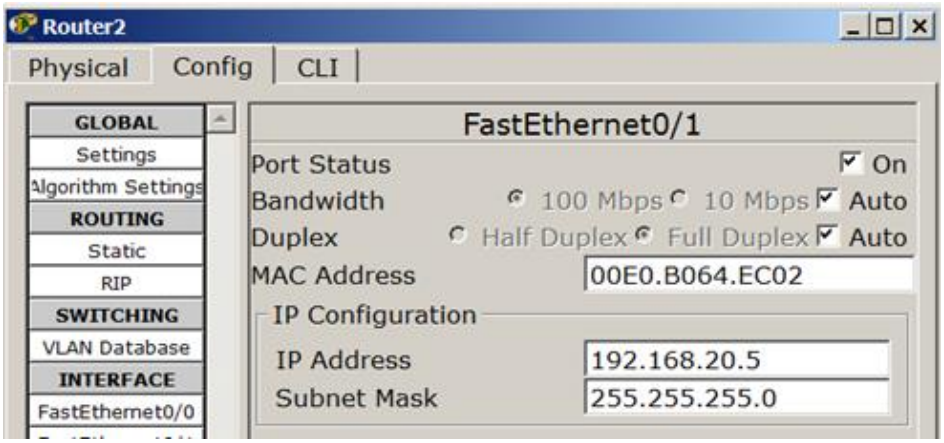


Рисунок - 8.16. Окно настройки порта Fa0 / 1 маршрутизатора R2 для работы с сетью 192.168.20.0.

Судя по маркерам, сеть поднята (Up), то есть все индикаторы зеленого цвета.

Настройка PC1 и PC2

Продолжаем настройку и работу компьютеров в сети 192.168.10.0, то есть необходимо установить IP, сетевую маску и шлюз по умолчанию для компьютеров. Согласно начальным условиям задачи, у нас есть пара компьютеров в сети 192.168.10.0 с маской 255.255.255.0 на левой стороне (рисунок 8.17).

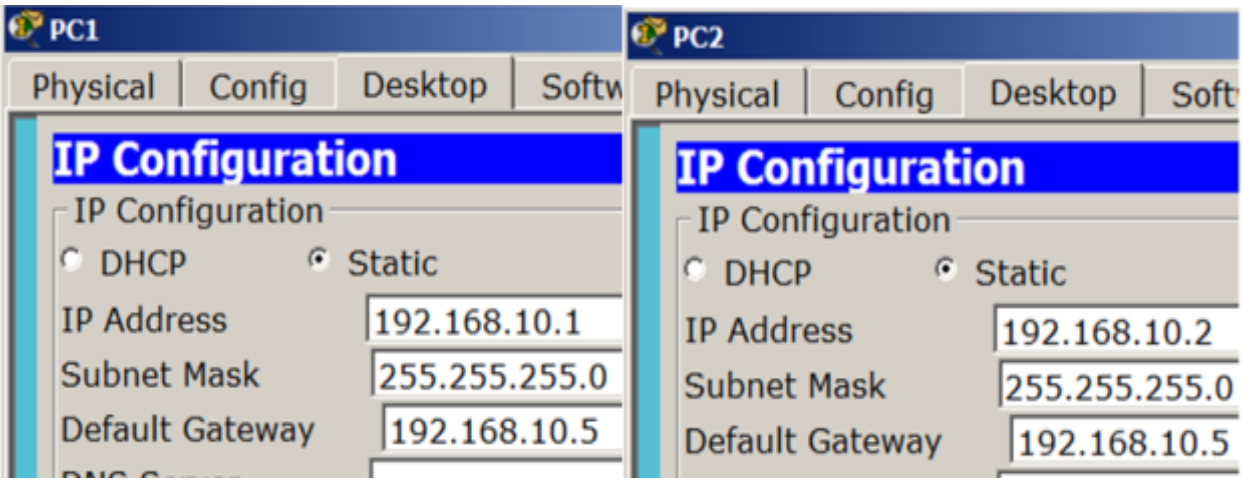


Рисунок 8.17. Окно настройки PC1 и PC2.

Стандартный шлюз (Default Gateway) — это адрес, на который компьютер отправляет пакет, если он не знает, куда его отправить. Например, когда хост B пытается отправить данные хосту A без точного адреса назначения для хоста A, он направляет TCP/IP трафик, предназначенный для хоста B, на стандартный шлюз.

Настройка сервера и ПК3

Затем необходимо настроить ПК3 и сервер в сети 192.168.20.0 (рисунки 8.18 и 8.19).

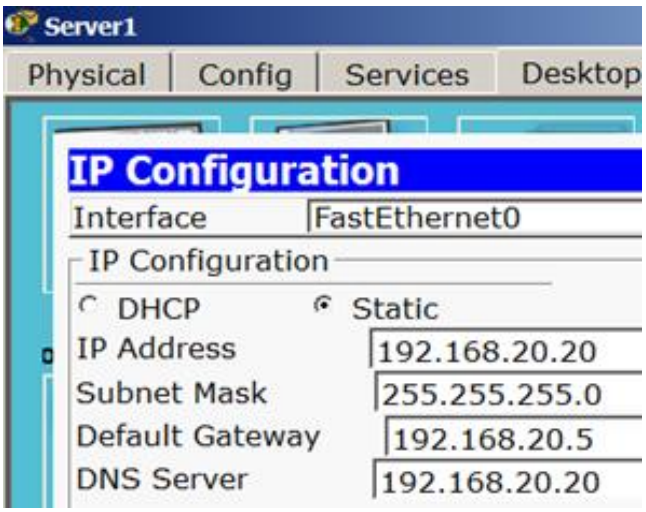


Рисунок - 8.18. Окно настройки сервера.

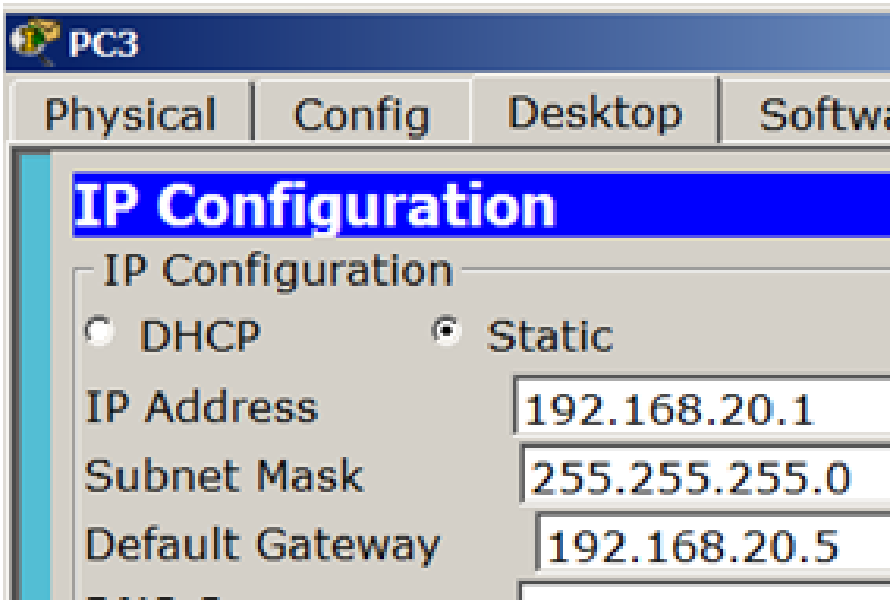


Рисунок - 8.19. Окно настройки ПК2.

Настройка маршрута на маршрутизаторах (статический маршрут)

Вы можете отправить пинг на сети и убедиться, что ситуация следующая: запросы из сети 10.0 отправляются в сеть 20.0, но ответов нет. Поэтому вам нужно зарегистрировать статические маршруты на маршрутизаторах. Напомним, что мы назначили IP-адрес 192.168.1.1 порту Fa0 / 1 и 192.168.1.2 порту Fa0 / 0. Поэтому для порта Fa0 / 1 с IP-адресом 192.168.1.1 на маршрутизаторе R1 вам нужно выполнить следующие команды (рис. 8.20).

Рисунок - 8.20. Окно регистрации стандартного маршрута на маршрутизаторе R1.

Запись означает, что все запросы, которым не назначены маршруты, будут отправлены маршрутизатором R1 на IP-адрес 192.168.1.2, то есть на маршрутизатор R2. Для R2 мы сделаем то же самое (см рис. 8.21).

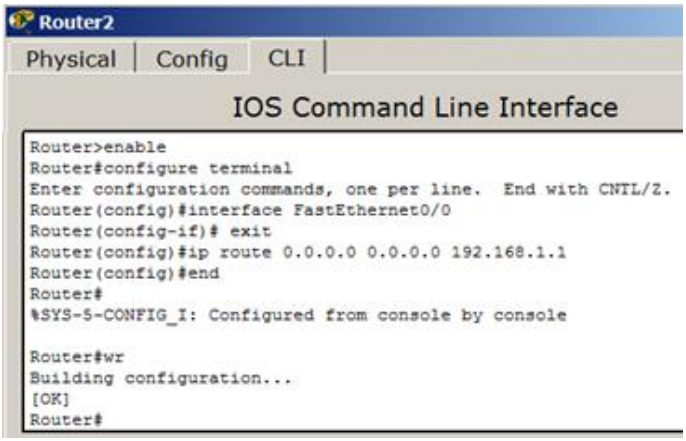


Рисунок - 8.21. Окно регистрации стандартного маршрута на R2.

Запись означает, что все запросы, для которых не зарегистрированы маршруты, будут отправлены R2 на 192.168.1.1, то есть на R1.

Проверка работы сети

После настройки маршрутизаторов можно протестировать сеть, для этого нужно отправить ping с компьютеров одной сети на компьютеры другой сети - (см рис 8.22).

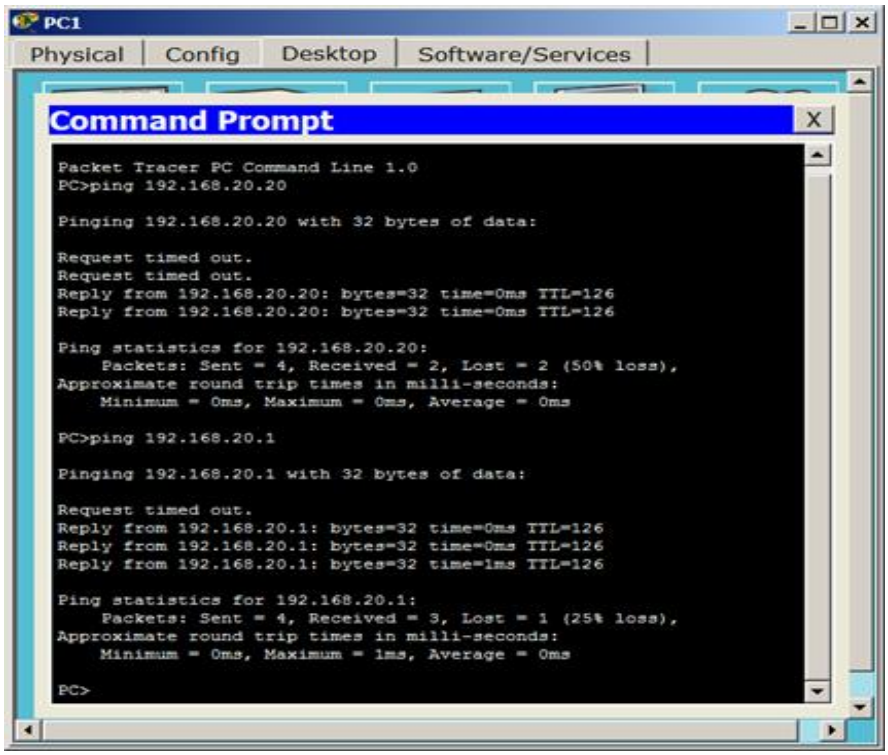


Рисунок - 8.22. Окно проверки связи.

Для проверки, как пакеты проходят от одного хоста к другому, используем команду **tracert 192.168.20.20** (см рис 8.23).

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

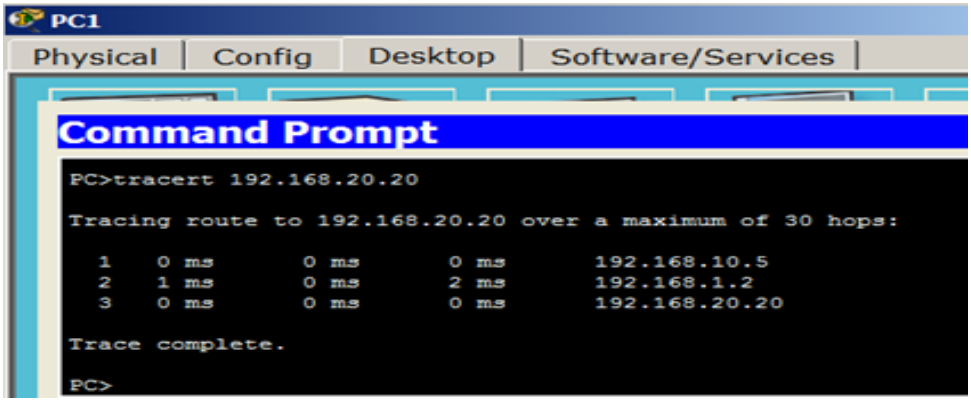


Рисунок - 8.23. Окно наблюдения за прохождением пакетов от компьютерного сегмента к серверу.

Как видно из скриншота, пакеты сначала проходят через 192.168.10.5 (порт R1 - Fa0/0), затем через 192.168.1.2 (порт R2 - Fa0/0), и наконец достигают сервера 192.168.20.20 - всё правильно!

Мы не создавали веб-страницы на сервере, но они были там по умолчанию. Запустите веб-браузер и убедитесь в этом сами (см рис 8.24).

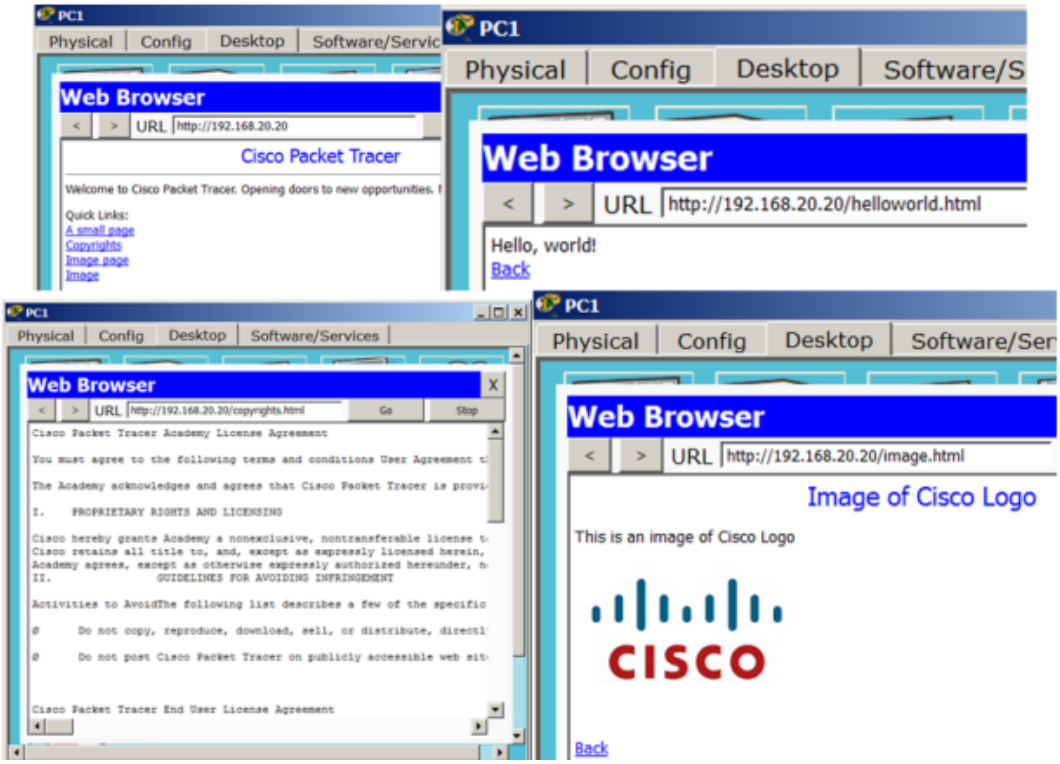


Рисунок - 8.24. Окно сервера с работающим HTTP-сервисом.

Задание 3. Создание сети на двух маршрутизаторах

В этом задании мы изучим статическую маршрутизацию в локальных сетях на двух практических примерах. Схема сети для настройки статической маршрутизации приведена на рисунке 8.25.

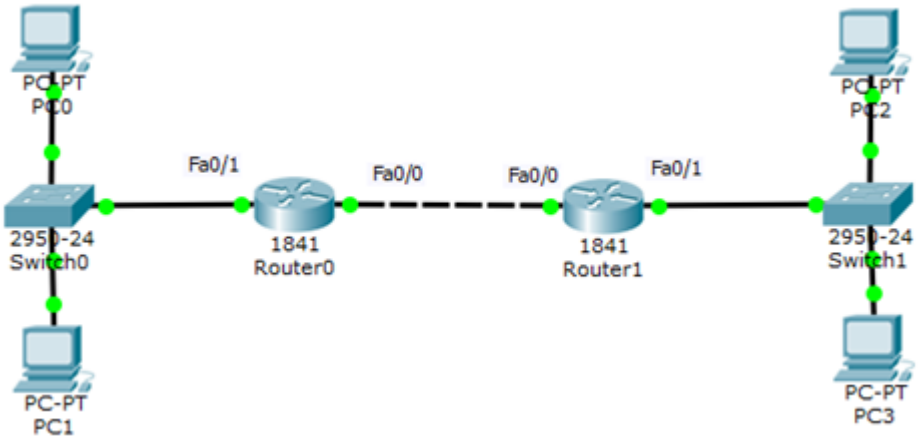


Рисунок - 8.25. Проект сети.

Если мы теперь используем команду **show ip route** для просмотра таблицы маршрутизации для R0 и R1, мы увидим следующее (см. рис. 8.26 и 8.27).

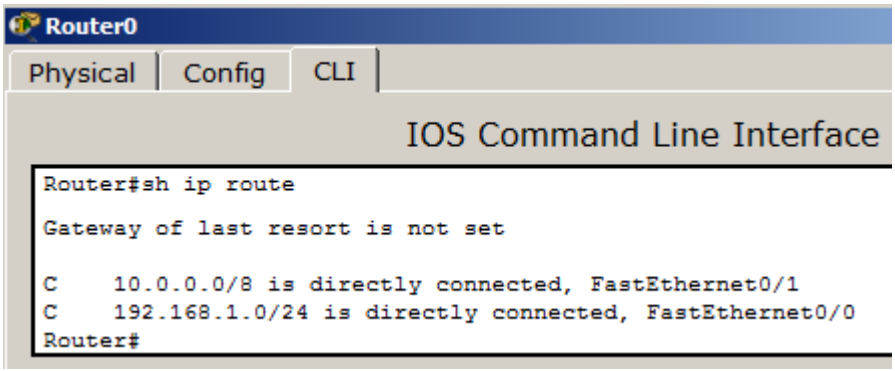


Рисунок - 8.26. Окно таблицы маршрутов для маршрутизатора 1.

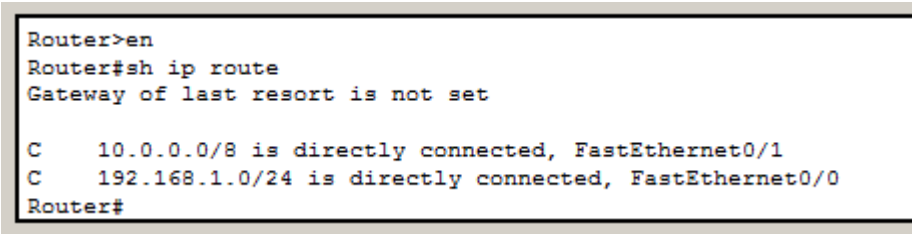


Рисунок - 8.27. Окно таблицы маршрутизации для 2-го маршрутизатора.

На данный момент мы видим, что в нашей таблице есть только напрямую подключенные сети. R0 не знает о сети 10.1.2.0, а R1 не знает о сети 10.1.1.0. Поэтому для настройки маршрутизации добавьте 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 мы снова отображаем таблицы маршрутизации наших устройств (рис. 8.28).

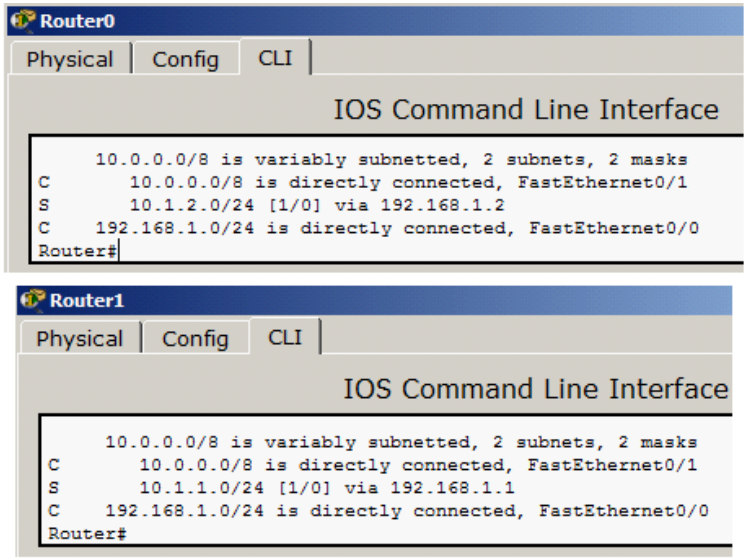


Рисунок - 8.28. Окно с настроенным маршрутом.

Теперь маршрутизатор 1 знает, что пакеты, направленные к подсети 10.1.2.0, можно передавать маршрутизатору с IP-адресом 192.168.1.2, а маршрутизатор 2 знает, что пакеты, направленные к подсети 10.1.1.0, можно отправлять маршрутизатору с IP-адресом 192.168.1.1. Проверим подключение ПК из различных сетей (см рис. 8.29).

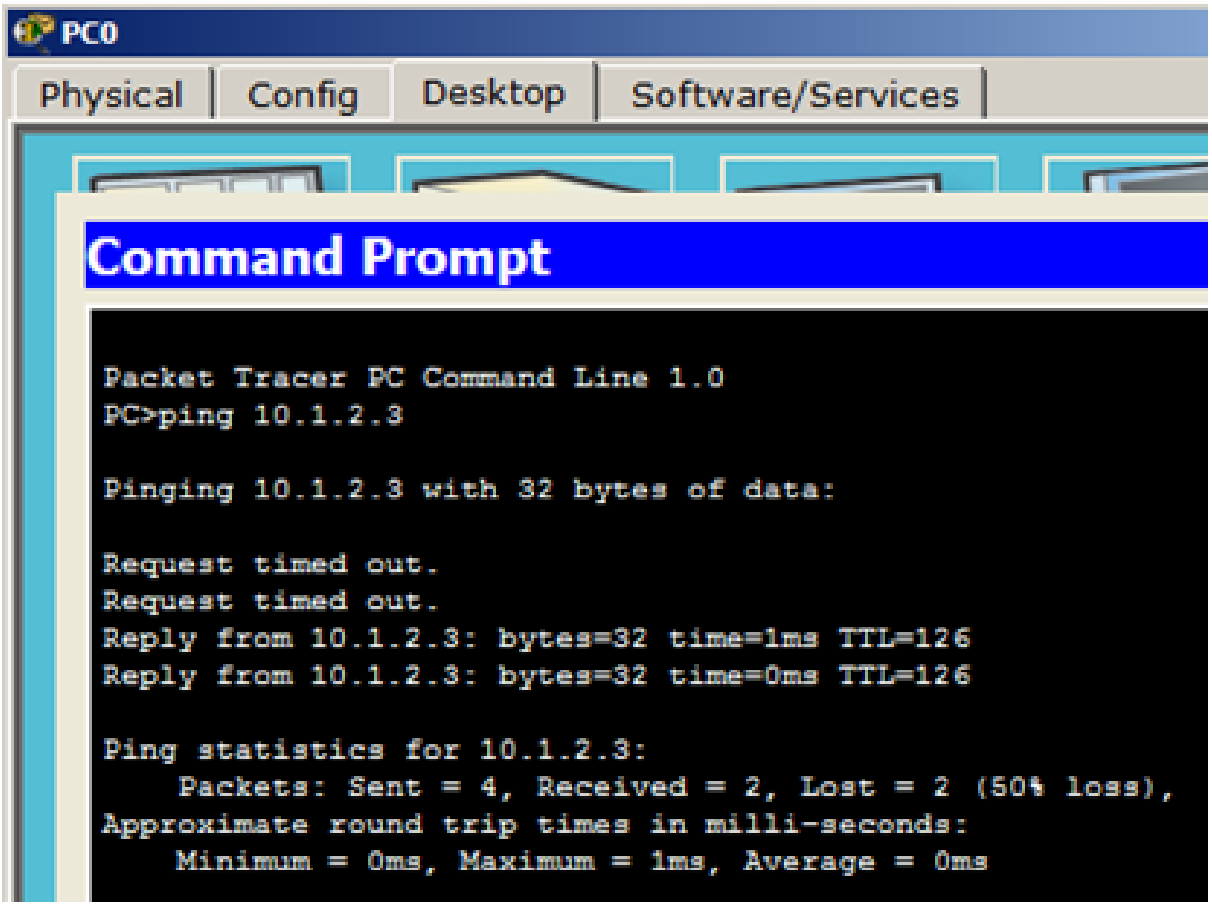


Рисунок - 8.29. Статическая маршрутизация настроена - окно проверки связи PC0 с PC3.

Статическая маршрутизация для пяти сетей и маршрутизатора с тремя портами

В этом примере мы создадим и настроим следующую сетевую схему (рисунок 8.30).

Сетевая схема

В этой схеме существует пять сетей: 192.168.1.0, 172.20.20.0, 192.168.100.0, 10.10.10.0 и 192.168.2.0. Каждый компьютер имеет в качестве шлюза по умолчанию интерфейс подключенного маршрутизатора. У всех компьютеров одинаковая маска - 255.255.255.0. Для каждого порта маршрутизатора используется разная маска: Fa0/0 - 255.255.255.0, Fa0/1 - 255.255.0.0, Fa1/0 - 255.255.255.252.

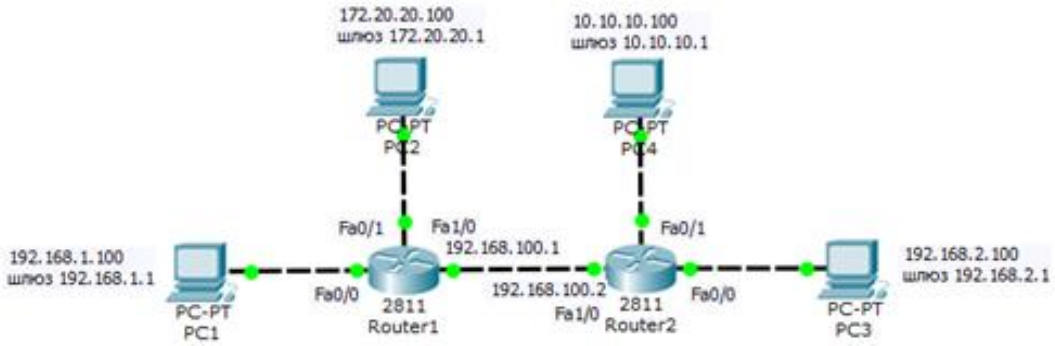


Рисунок - 8.30. Соединение сетей через маршрутизаторы.

Затем подключите маршрутизаторы друг к другу, для этого добавьте карту интерфейса NM-1FE-TX к маршрутизатору (NM - сетевой модуль, 1FE - включает один порт FastEthernet, TX - поддерживает 10 / 100MBase-TX). Для этого откройте окно конфигурации маршрутизатора0, нажмите кнопку питания, чтобы выключить его. После этого перетащите интерфейсную плату NM-1FE-TX в разъем маршрутизатора (рисунок 8.31). После добавления карты снова нажмите кнопку питания маршрутизатора, чтобы включить его. Повторите те же действия для второго маршрутизатора.

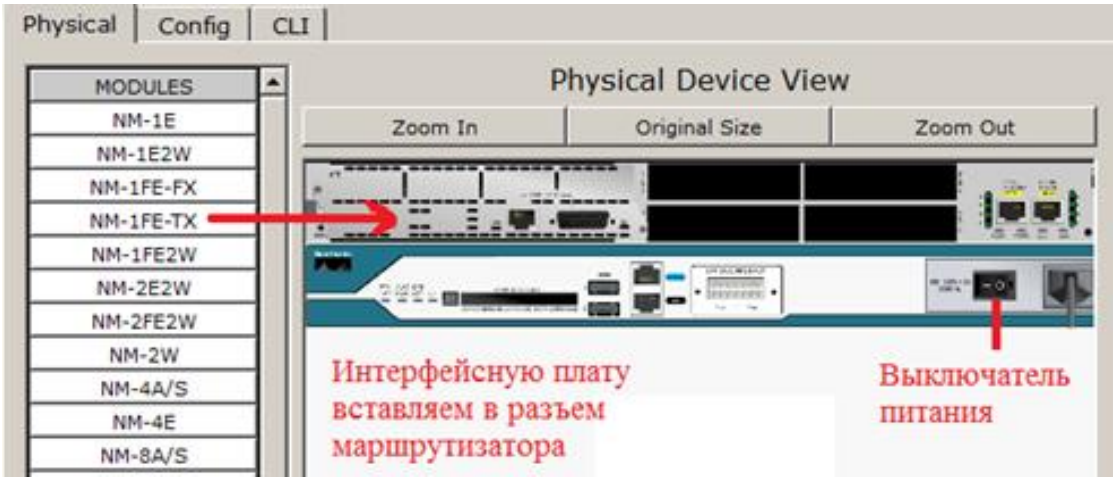


Рисунок - 8.31. Окно вставки интерфейсной платы в маршрутизатор.

Постановка задачи

Мы должны настроить необходимые параметры, чтобы все персональные компьютеры могли подключаться друг к другу, то есть обеспечить наличие компьютеров из различных сетей.

Настройка маршрутизатора (стандартный маршрут)

В данный момент, если мы отправим пакет с IP-адресом 192.168.1.100 с ПК1 на интерфейс Fa1/0 маршрутизатора R2 с IP-адресом 192.168.100.2, ICMP пакет достигнет этого маршрутизатора слева, но при отправке ICMP пакетов в обратном направлении от 192.168.100.2 до 192.168.1.100 возникнет проблема. Дело в том, что маршрутизатор R2 не имеет информации о сети 172.20.20.0 в своей таблице маршрутизации, так как мы еще не зарегистрировали стандартный шлюз, и маршрутизатор R2 не знает, куда отправить ответы на запросы. Самый простой способ настроить маршрутизацию между подсетями - добавить стандартный маршрут. Для этого в режиме конфигурации на маршрутизаторе R1 выполните следующие команды (см рис. 8.32).

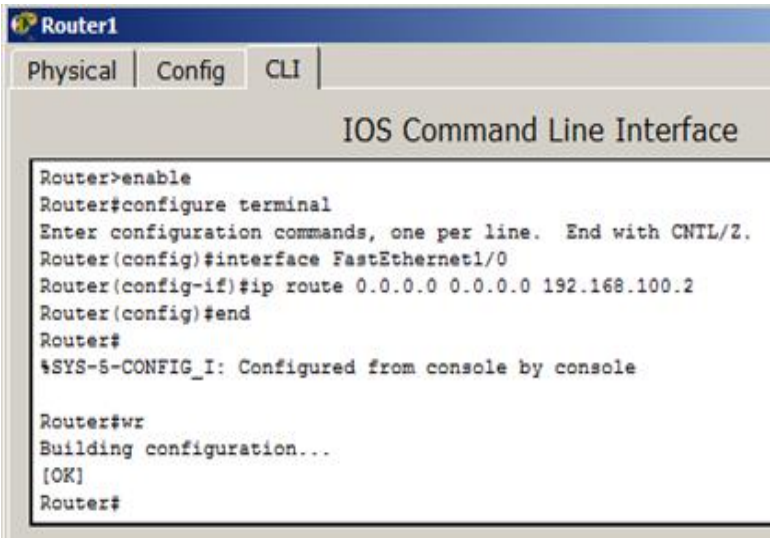


Рисунок - 8.32. Окно настройки стандартного маршрута на R1.

В этих командах первая группа цифр 0.0.0.0 обозначает IP-адрес целевой сети, следующая группа цифр 0.0.0.0 обозначает её маску, а последние цифры — 192.168.100.2 — это IP-адрес интерфейса, на который необходимо отправлять пакеты для доступа к этой сети. Если мы укажем 0.0.0.0 в качестве IP-адреса сети с маской 0.0.0.0, то этот маршрут станет маршрутом по умолчанию, и все пакеты, адреса которых не указаны напрямую в таблице маршрутов, будут отправляться на него.

На правом маршрутизаторе R2 мы поступаем аналогичным образом (см рис. 8.33).

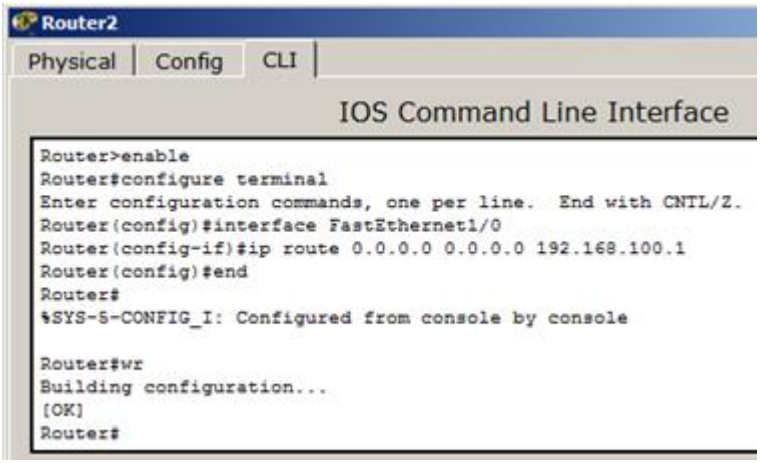


Рисунок - 8.33. Окно установки стандартного маршрута на R2.

Отправим пакет с IP-адресом 192.168.1.100 с PC1 на интерфейс Fa1/0 маршрутизатора R2 с IP-адресом 192.168.100.2 и посмотрим, что изменилось (см рис. 8.34)

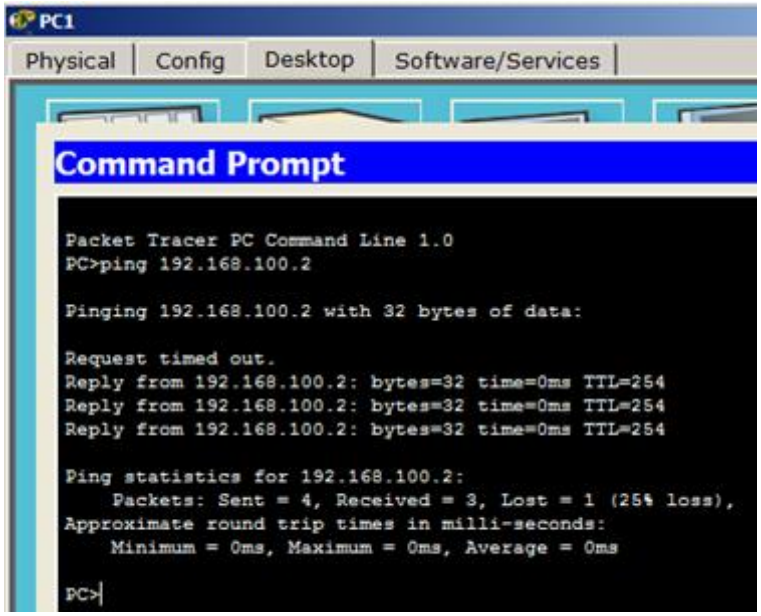


Рисунок - 8.34. Окно проверки интерфейса Fa1/0 маршрутизатора R2 с IP-адресом 192.168.100.2 от компьютера PC1 с IP-адресом 192.168.1.100.

Практическая работаimiz В итоге можно сказать, что если мы хотим выполнить ping от компьютера PC1 с IP-адресом 192.168.1.100 (левая сеть) до компьютера PC4 с IP-адресом 10.10.10.100 (правая сеть), то на компьютере с адресом 192.168.1.100 будет указан шлюз по умолчанию - это интерфейс Fa0/0 маршрутизатора R1 с адресом 192.168.1.1. Сначала компьютер проверит адрес 10.10.10.100 в таблице маршрутизации и, не найдя его, отправит ICMP пакеты на шлюз по умолчанию, то есть на интерфейс маршрутизатора R1 с адресом 192.168.1.1 (порт Fa0/0). Получив пакет, R1 проверяет адрес 10.10.10.100 и также пытается найти его в своей таблице маршрутизации. Не найдя его, он отправляет пакет на интерфейс Fa1/0, к маршрутизатору R2 с адресом

192.168.100.2. Маршрутизатор R2 также попытается найти маршрут до 10.10.10.100 в своей таблице маршрутизации. Если это не удастся, он проверит маршрут до сети 10.0.0.0. Информация об этой сети будет найдена в таблице маршрутизации, и маршрутизатор будет знать, что пакеты следует отправлять непосредственно на интерфейс FastEthernet0/1, который подключен к этой сети. В нашем примере вся сеть 10.0.0.0 состоит из одного компьютера, поэтому пакеты сразу попадут к своему адресу, то есть к компьютеру с IP-адресом 10.10.10.100. При отправке ответных ICMP пакетов все будет происходить аналогично. Однако, не всегда удается настроить маршрутизацию только с использованием маршрутов по умолчанию. В более сложных конфигурациях сети может потребоваться отдельная запись маршрутов для каждой сети. Это будет нелегко. Поэтому в больших сетях обычно используется динамическая, а не статическая маршрутизация.

Контрольные вопросы:

1. Сколько способов создания таблицы маршрутизации существует?
2. Что такое статическая маршрутизация?
3. Каковы преимущества статической маршрутизации?
4. Какие различия между статической и динамической маршрутизацией?
5. Что такое шлюз по умолчанию (default gateway)?
6. Что такое ICMP?
7. Что такое маршрутизационная петля (Routing loop)?
8. Какие команды используются для настройки маршрутизатора?
9. Что такое команда tracert?

Практическая работа № 9

Настройка динамической маршрутизации в программе Cisco Packet Tracer.

Цель работы: Изучение навыков динамической маршрутизации с использованием протоколов RIP и EIGRP.

Теоретическая часть

Маршрутизация — это процесс нахождения наилучшего пути в сети для доставки пакета к его пункту назначения. Динамическая маршрутизация осуществляется с помощью одного или нескольких протоколов, таких как RIP v2, OSPF и другие.

Динамическая маршрутизация — это метод, при котором таблица маршрутизации автоматически заполняется и обновляется с помощью одного или нескольких маршрутизационных протоколов, таких как RIP, OSPF, EIGRP и BGP.

Каждый маршрутизационный протокол применяет систему оценки маршрутов (метрики). Выбор маршрута к определённым сетям основывается на следующих критериях:

- количество пересылок (хопов),
- пропускная способность канала связи,
- задержка при передаче данных.

Маршрутизаторы обмениваются информацией о маршрутах через служебные пакеты по протоколу UDP. Этот обмен создает дополнительный трафик и увеличивает нагрузку на сеть. Кроме того, маршрутизаторы могут не успевать синхронизировать свои таблицы маршрутизации, что может привести к появлению некорректных маршрутов и потере данных.

Маршрутизационные протоколы делятся на три типа:

- Протоколы дистанционно-векторной маршрутизации (RIP),
- Протоколы отслеживания состояния каналов (OSPF),
- Гибридные протоколы (EIGRP).

Протокол RIP

RIP (Routing Information Protocol) — это протокол дистанционно-векторной маршрутизации, который использует алгоритм Беллмана-Форда для нахождения оптимального пути. RIP является одним из самых простых маршрутизационных протоколов, поскольку передает таблицу маршрутизации в сеть каждые 30 секунд. Основное различие между RIPv2 и RIPv1 заключается в том, что RIPv2 поддерживает мультикаст, то есть может отправлять данные на мультикаст-адрес. Максимальное количество хопов

(пересылок) в RIPv1 составляет 15, что ограничивает использование RIP в больших сетях. Поэтому этот протокол часто используется в небольших компьютерных сетях. Вторая версия протокола, RIP2, была разработана в 1994 году и представляет собой улучшенную версию первой. Она повышает безопасность, добавляя дополнительные данные маршрутизации.

Принцип работы дистанционно-векторного протокола заключается в следующем: каждый маршрутизатор, использующий протокол RIP, периодически отправляет всем своим соседям специальный векторный пакет, который содержит информацию о расстоянии до всех сетей, известных этому маршрутизатору (в измерении метрики). Получив такой вектор, маршрутизатор увеличивает значения компонентов на расстояние до соседнего маршрутизатора и добавляет данные о сетях, которые ему известны напрямую или через другие маршрутизаторы. Затем маршрутизатор отправляет обновленный вектор всем своим соседям. При наличии нескольких альтернативных маршрутов маршрутизатор выбирает маршрут с наименьшим значением метрики. Маршрутизатор, передавший информацию об этом маршруте, обозначается как следующий переход (next hop).

Протокол RIP не подходит для крупных сетей, так как он генерирует значительный объем трафика и увеличивает нагрузку на сеть. Узлы сети работают только с векторами расстояний, не имея точной информации о состоянии каналов и топологии сети. В настоящее время, даже в небольших сетях, RIP часто заменяют более продвинутые протоколы, такие как EIGRP и OSPF.

Порядок выполнения работы

Настройка версии RIPv2 для сети с шестью устройствами

Наша задача - настройка маршрутизации по схеме, показанной на рисунке 9.1

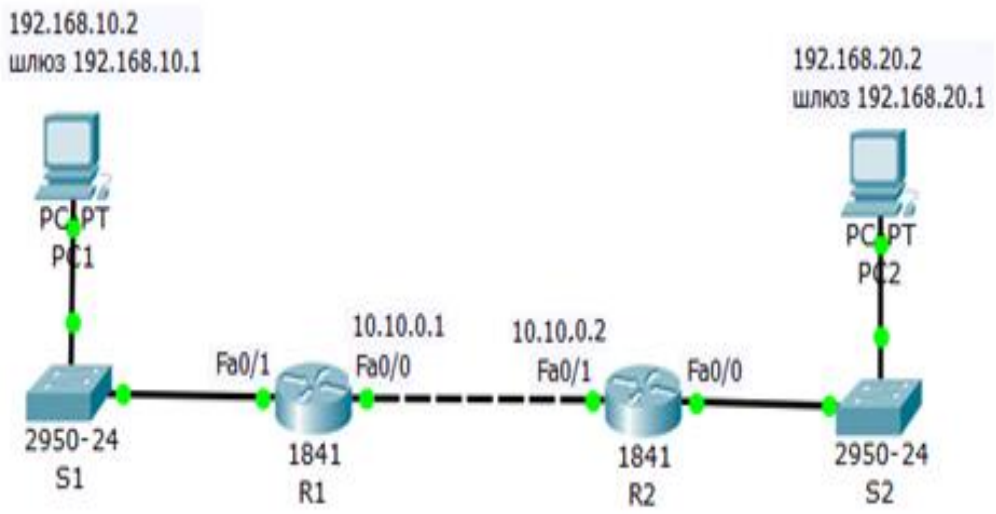


Рисунок - 9.1. Проект сети.

Не забудьте включить порты при настройке сети.

Настройка маршрутизационного протокола RIP на маршрутизаторе R1

Войдите в консоль маршрутизатора и выполните следующие настройки (см рис 9.2).

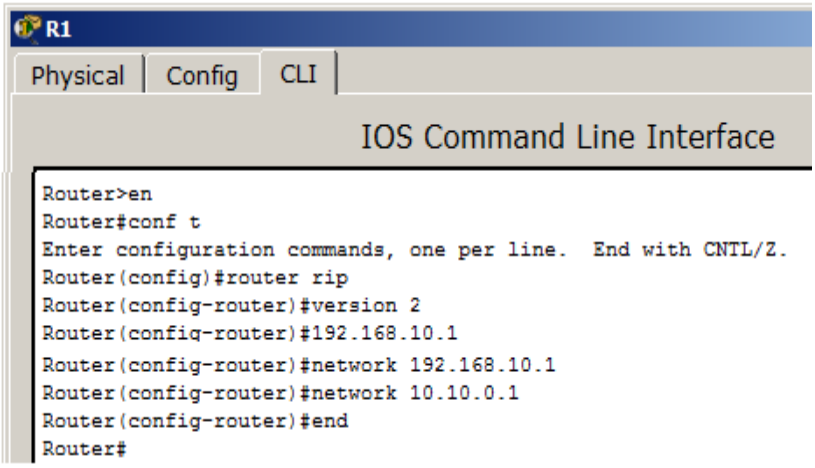


Рисунок - 9.2. Окно настройки протокола RIPv2 на маршрутизаторе Router1.

Router (config) #router rip (вход в режим конфигурации маршрутизатора RIP).

Router (config-router) #network 192.168.10.1 (подключение клиентской сети через коммутатор S1).

Router (config-router) #network 192.168.20.1 (подключение второй сети, то есть сети между маршрутизаторами).

Router (config-router) #version 2 (установка использования второй версии протокола RIP).

Настройка протокола RIP на маршрутизаторе R2

Войдите в консоль второго маршрутизатора и выполните следующие настройки (см рис 9.3).

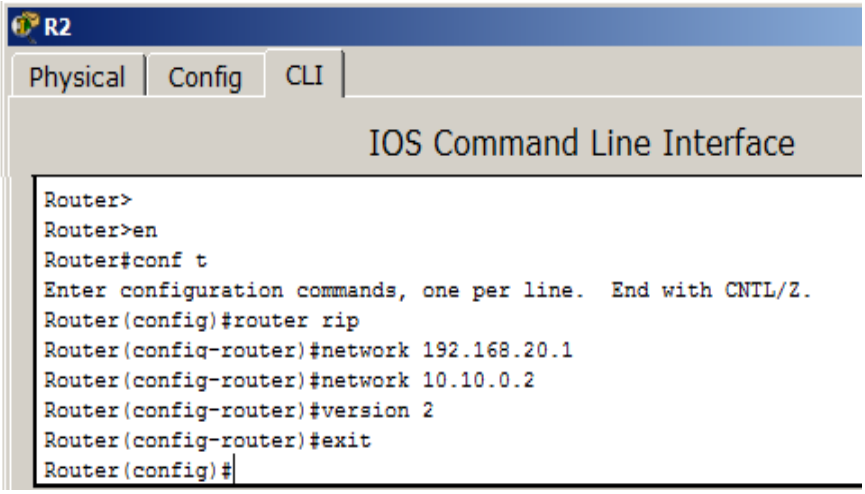


Рисунок - 9.3. Настройка протокола RIPv2 на маршрутизаторе R2.

Проверка настроек коммутатора и протокола RIP

Рассмотрим настройки протокола RIPv2 на маршрутизаторах R1 и R2 (Рисунок 9.4).

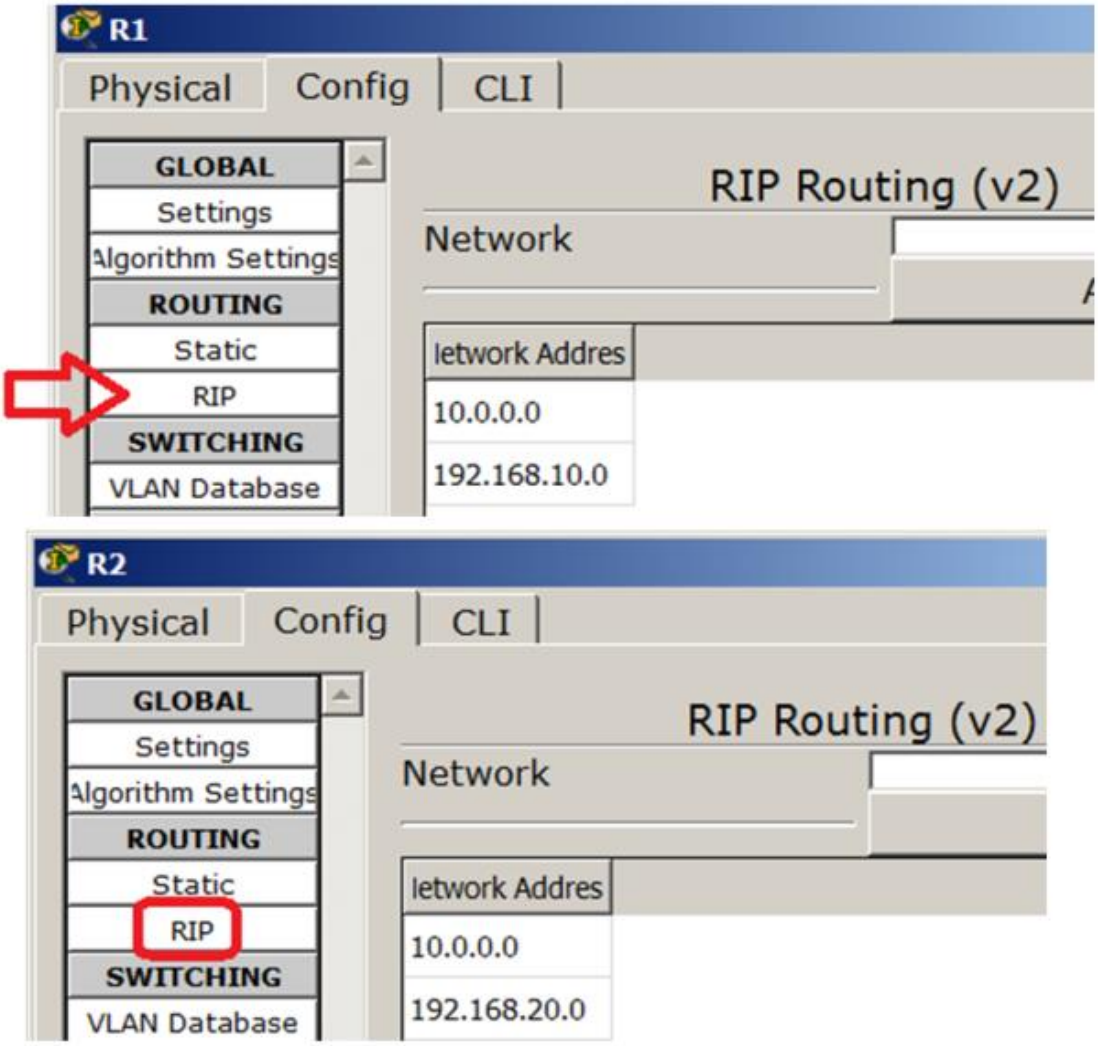


Рисунок - 9.4. Окно настроек маршрутизаторов R1 и R2.

Чтобы убедиться, что маршрутизаторы действительно правильно настроены и работают корректно, просмотрите таблицу маршрутизации RIP с помощью следующей команды:

Router # show ip route rip (Рисунок 9.5 и Рисунок 9.6).

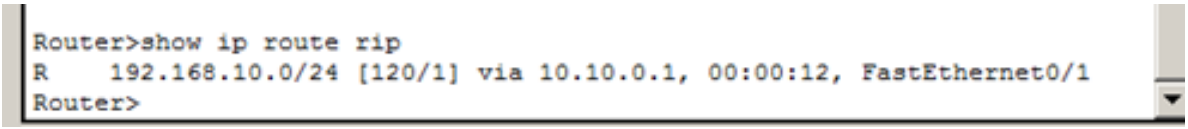


Рисунок - 9.5. Окно таблицы маршрутизации на R1.

Эта таблица показывает, что до сети 192.168.10.0 существует только один маршрут: через R1 (сеть 10.10.0.1).

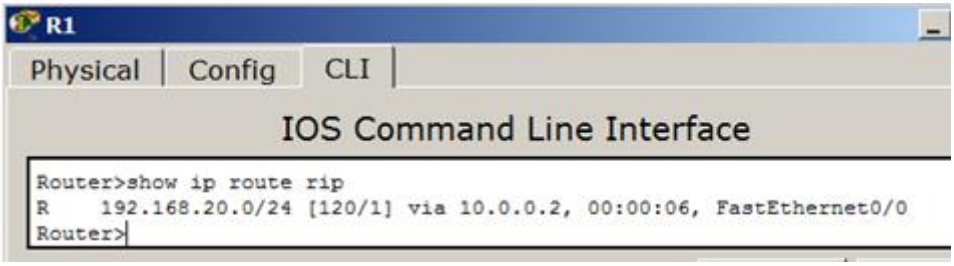


Рисунок 9.6. Окно таблицы маршрутизации на R2.

Эта таблица показывает, что для сети 192.168.20.0 существует только один маршрут: через R2 (сеть 10.10.0.2).

Проверка связи между PC1 и PC2

Проверим правильность выполнения маршрутизации (Рисунок 9.7).

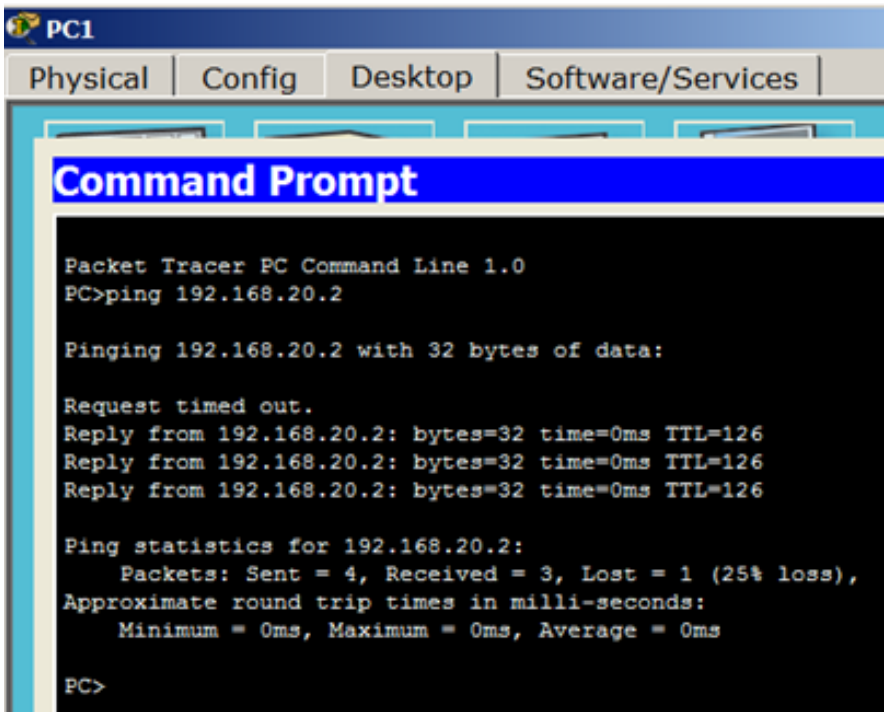


Рисунок 9.7. Окно ping от PC1 к PC2.

Задания по выполнению работы

1-е Задание. Настройка версии RIP 2 для сети с четырьмя устройствами

На рисунке 9.8 показана сеть, которую мы будем использовать для настройки маршрутизационного протокола RIPv2.

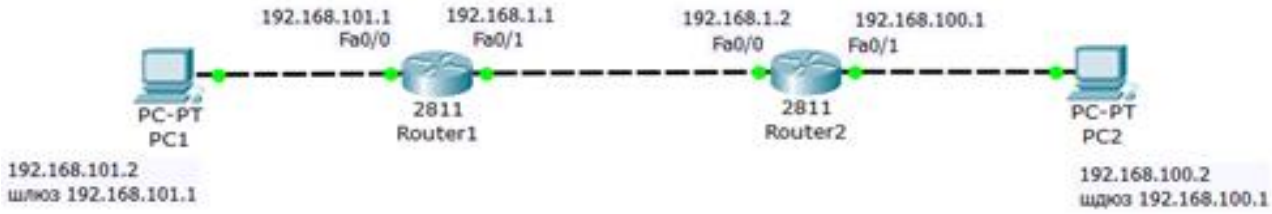


Рисунок - 9.8. Проект сети для настройки маршрутизационных протоколов.

Сначала настроим R1 (Рисунок 9.9).

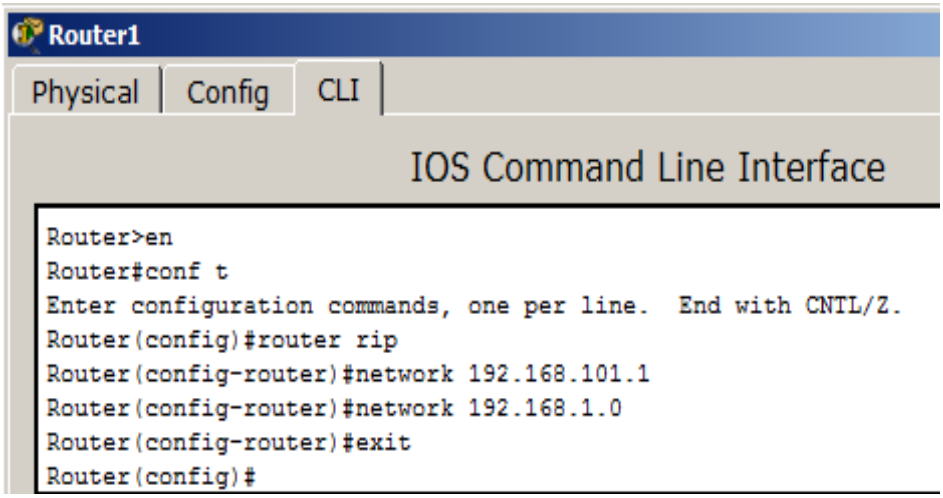


Рисунок - 9.9. Окно настройки протокола RIP на маршрутизаторе R1.

Рассмотрим результат на вкладке Config (Рисунок 9.10).

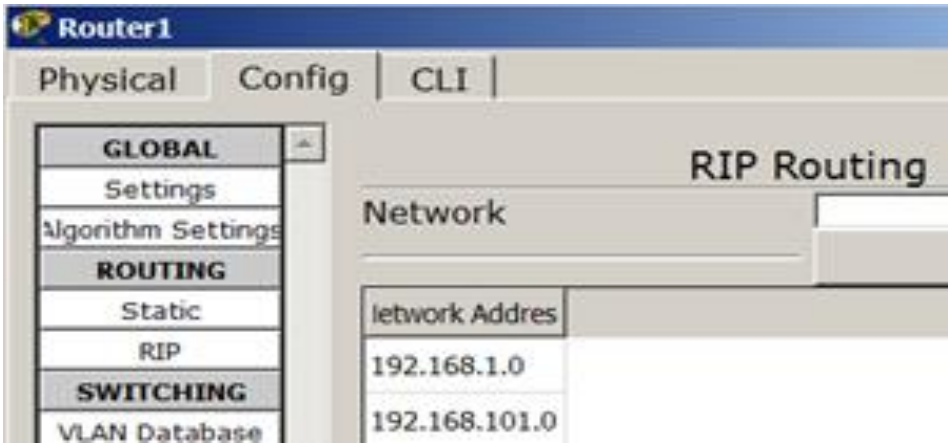


Рисунок - 9.10. Окно маршрутизатора R1, вкладка Config.

Настроим маршрутизацию на R2 (Рисунок 9.11).

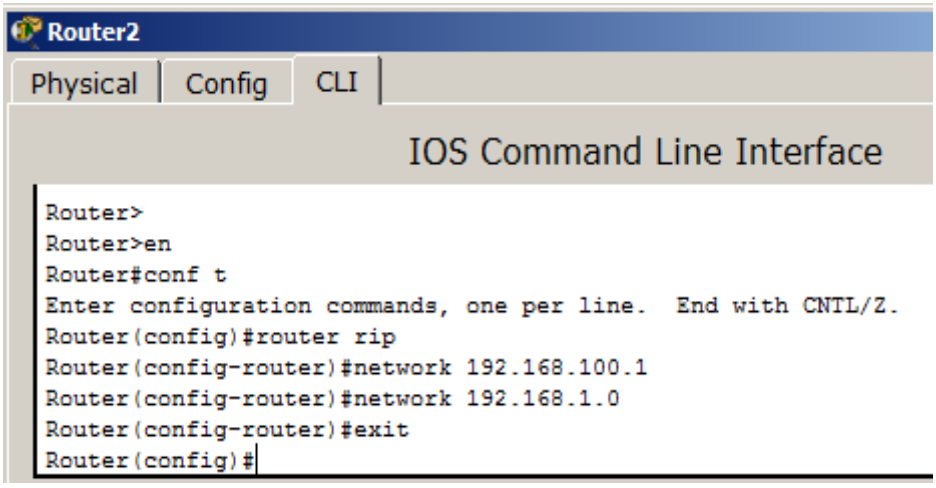


Рисунок - 9.11. Окно настройки протокола RIP на маршрутизаторе R2.

Рассмотрим результат (Рисунок 9.12).

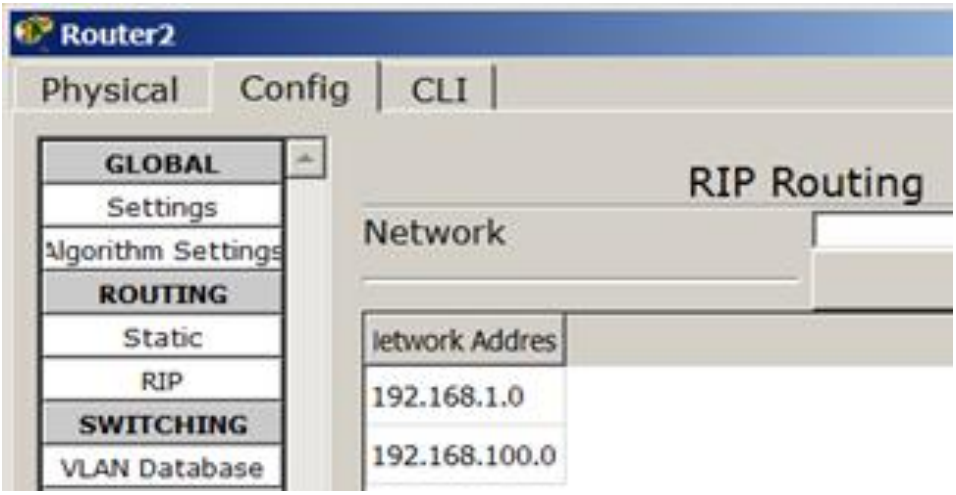
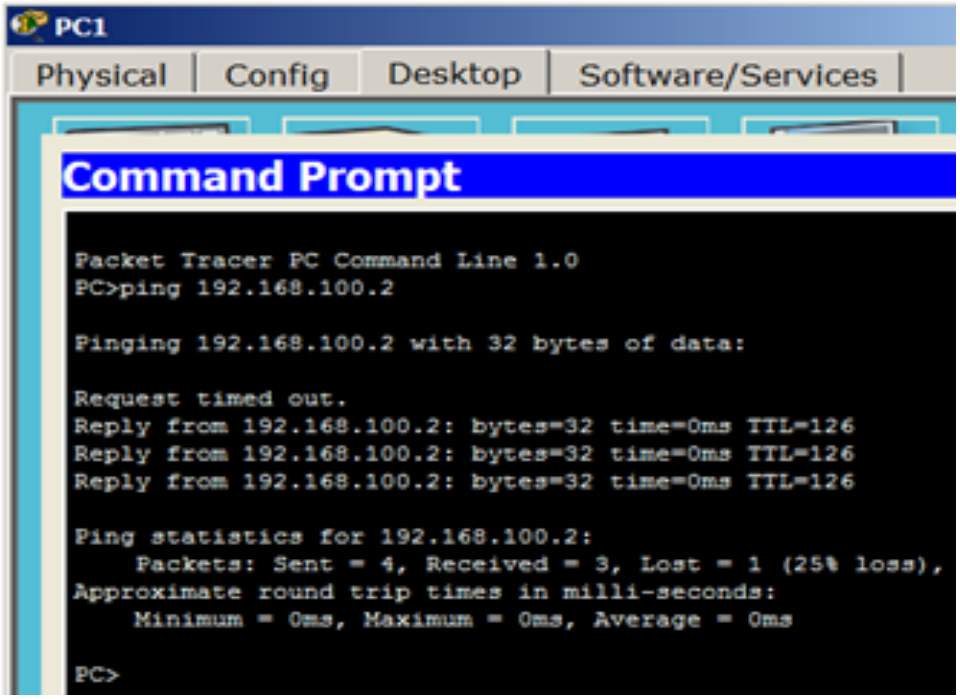


Рисунок - 9.12. Окно маршрутизатора R2, вкладка Config.

Проверим доступность персональных компьютеров из разных сетей (Рисунок 9.13).



9.13-rasm. RIP protokolini yo‘naltirish natijasi oynasi.

Протокол маршрутизации EIGRP

Протокол EIGRP проще внедрить и требует меньше вычислительных ресурсов маршрутизатора по сравнению с OSPF. В EIGRP более развит алгоритм расчета метрики, который позволяет учитывать загрузку и надежность интерфейсов на пути пакета. Однако недостатком EIGRP является его ограниченное использование только на оборудовании Cisco.

2-е Задание. Настройка протокола EIGRP

Схема сети представлена на рисунке 9.14..

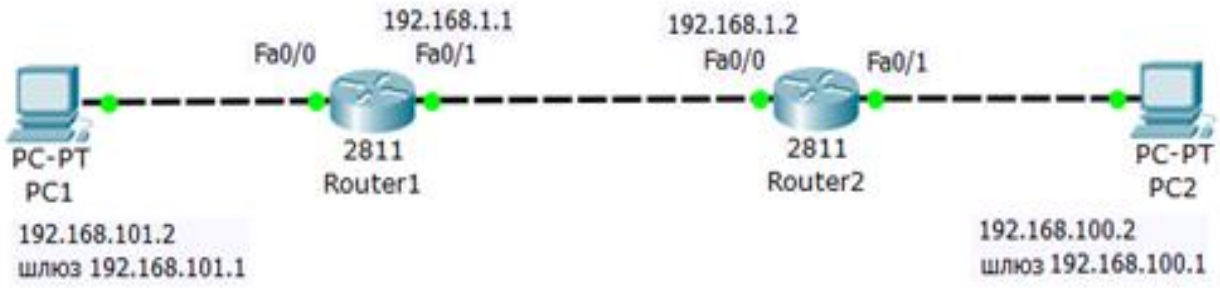


Рисунок 9.14. Проект конфигурации EIGRP.

Настройка EIGRP очень похожа на настройку RIP.

Программирование маршрутизатора R1

Настроим R1 (Рисунок 9.15).

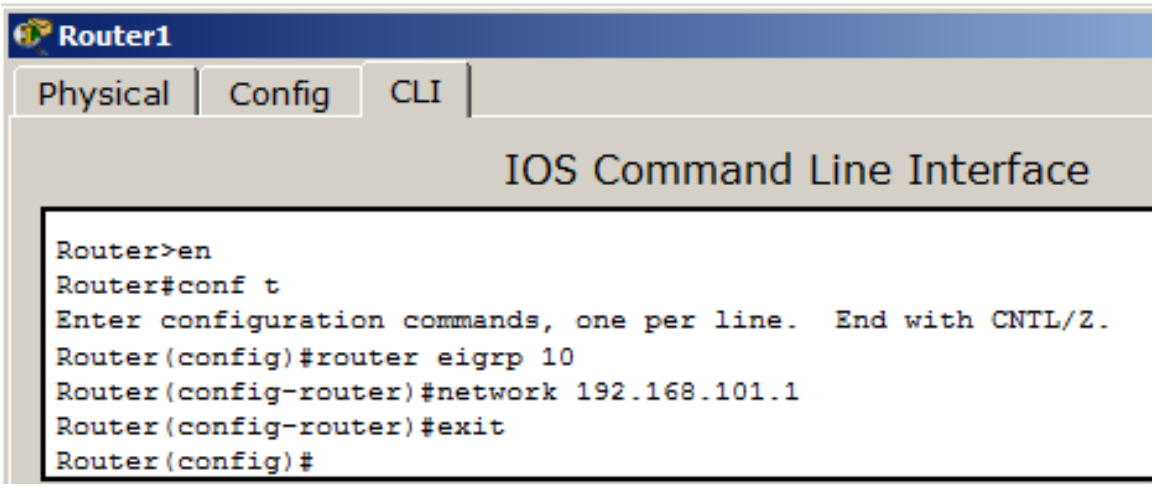


Рисунок - 9.15. Окно настройки маршрутизатора R1.

Программирование R2

Настроим R2 (Рисунок 9.16).

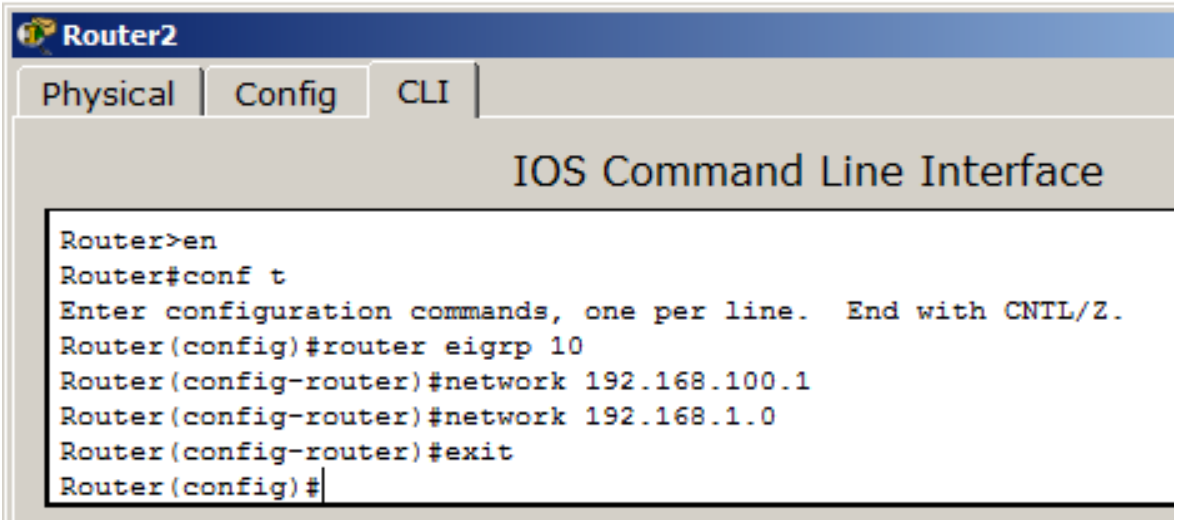


Рисунок - 9.16. Окно настройки R2.

Проверка работы сети

Проверим работу маршрутизатора (Рисунок 9.17).

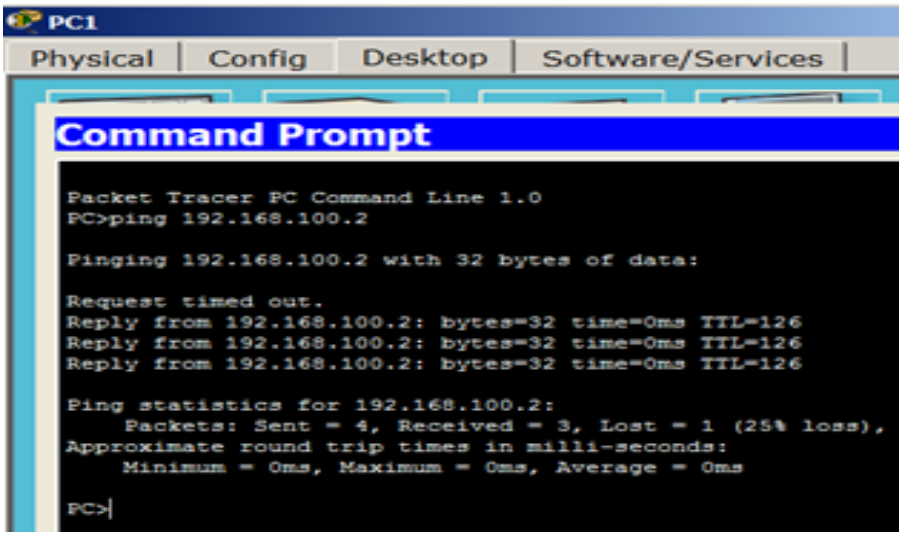


Рисунок - 9.17. Окно с результатами проверки состояния сети.

Динамический маршрутизационный протокол OSPF (Open Shortest Path First)

OSPF (Open Shortest Path First) — это протокол динамической маршрутизации, основанный на технологии link-state (LSA), который использует алгоритм нахождения кратчайшего пути. OSPF использует единую базу данных, которая описывает, к каким сетям подключен каждый маршрутизатор. При описании каждого канала маршрутизаторы ассоциируют его с метрикой — значением, которое характеризует 'качество' канала. Это позволяет маршрутизаторам OSPF учитывать реальную пропускную способность канала и выбирать наилучшие маршруты, в отличие от RIP, где все каналы считаются равными.

Протокол OSPF требует отправки объявлений о состоянии каналов (LSA) на все активные интерфейсы маршрутизаторов в зоне. Эти объявления содержат описание каждого канала и его стоимость. Сообщения LSA отправляются только при изменениях в сети, но не реже одного раза в 30 минут.

OSPF также поддерживает разделение автономной системы на зоны (области). Использование зон помогает снизить нагрузку на сеть и процессоры маршрутизаторов, а также уменьшает размер таблиц маршрутизации.

Работа протокола OSPF

Все маршрутизаторы обмениваются специальными Hello-пакетами на всех интерфейсах с включенным OSPF. Это позволяет идентифицировать соседние маршрутизаторы и устанавливать с ними общий канал передачи

данных. После этого Hello-пакеты отправляются каждые 30 секунд. Маршрутизаторы стремятся установить состояние соседства с другими маршрутизаторами. Этот процесс зависит от типа маршрутизаторов и типа сети, через которую обмениваются Hello-пакетами, а также от атрибутов зоны.

Маршрутизаторы, находящиеся в состоянии соседства, синхронизируют свои базы данных состояния канала между собой. Каждый маршрутизатор отправляет объявления о состоянии канала (LSA) своим соседям. При получении такого объявления маршрутизатор записывает информацию в свою базу данных состояния канала и пересылает копию объявления другим соседям. При распространении объявлений в зоне все маршрутизаторы формируют идентичную базу данных состояния канала.

Каждый маршрутизатор применяет алгоритм SPF (Shortest Path First) для вычисления своего графа кратчайших путей. На основе полученного дерева кратчайших путей маршрутизатор создает свою таблицу маршрутизации.

Прямая и обратная маска

На оборудовании Cisco иногда необходимо использовать обратную маску вместо обычной прямой маски. Например, вместо маски 255.255.255.0 (прямая маска) может использоваться маска 0.0.0.255 (обратная маска). Обратная маска используется в списках контроля доступа (ACL) и для описания сетей в протоколе OSPF, в то время как прямая маска применяется в остальных случаях. Основное различие между ними заключается в том, что прямая маска применяется к сетям, а обратная - к хостам.

Используя обратную маску, можно, например, выбрать хосты с определённым адресом во всех подсетях и разрешить им доступ в Интернет. Поскольку адреса с маской 255.255.255.0, такие как 192.168.1.0, часто применяются в локальных сетях, наиболее распространённая обратная маска - это 0.0.0.255.

Шаблонная маска (wildcard mask) представляет собой маску, которая показывает количество хостов в сети и используется в дополнение к маске подсети. Для каждого октета маски подсети значение 255 интерпретируется как часть маски подсети. Например, для сети 192.168.1.0 с маской подсети 255.255.255.242 шаблонная маска будет 0.0.0.13. Шаблонная маска применяется в конфигурации некоторых маршрутизационных протоколов и является удобным параметром для ограничения списков контроля доступа.

Маскирование шаблонной маски

Существует связь между прямой (маской подсети) и обратной (шаблонной) масками. В сумме для каждого бита эти маски должны равняться 255. Рассмотрим пример:

Для сети 192.168.32.0/28:

1. **Прямая маска подсети**:
   - /28 означает, что первые 28 битов маски подсети равны 1.
   - Соответствующая маска подсети будет: 255.255.255.240.
2. **Шаблонная маска**:
   - Чтобы вычислить шаблонную маску, необходимо вычесть каждую часть прямой маски из 255.
   - Для маски 255.255.255.240, вычисления будут следующими:
     - 255 - 255 = 0
     - 255 - 255 = 0
     - 255 - 255 = 0
     - 255 - 240 = 15

Таким образом, шаблонная маска для сети 192.168.32.0/28 будет: **0.0.0.15**.

Шаблонная маска 0.0.0.15 используется в конфигурации маршрутизационных протоколов для определения диапазона IP-адресов в сети и фильтрации трафика. Для вычисления шаблонной маски (wildcard mask) из маски подсети, нужно инвертировать биты маски подсети. Давайте разберем это подробно:

1. **Маска подсети**:
   - Префикс /28 соответствует маске подсети 255.255.255.240.
   - В двоичном виде это: 11111111.11111111.11111111.11110000.
2. **Инвертируем биты**:
   - Инвертируем биты маски подсети: 00000000.00000000.00000000.00001111.
3. **Преобразуем двоичное число в десятичное**:
   - Двоичное число 00001111 преобразуется в десятичное число 15.

Таким образом, шаблонная маска (wildcard mask) для префикса /28 будет **0.0.0.15**.

Преобразуем этот двоичный номер в десятичный:

В двоичном виде 11110000 соответствует следующим значениям: 128/64/32/16/8/4/2/1. Сложим значения, соответствующие единицам: 8 + 4 + 2 + 1 = 15. Таким образом, наша шаблонная маска будет 0.0.0.15.

4-е Задание. Настройка протокола OSPF для 4 устройств

Соберите схему, показанную на рисунке 9.18.

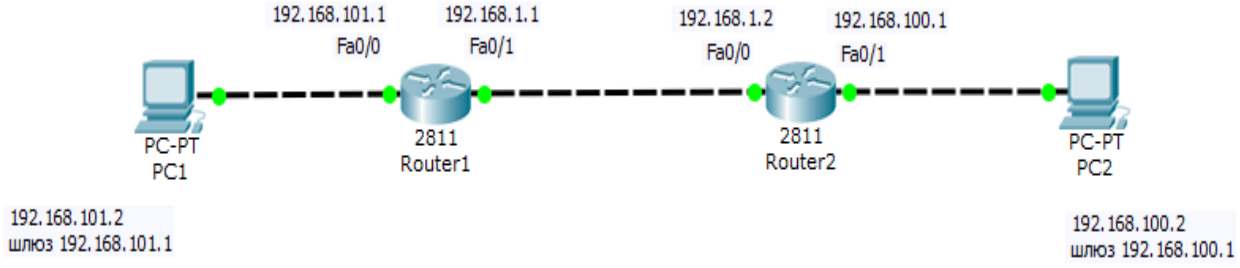


Рисунок - 9.18. Проект настройки протокола OSPF.

Настройка маршрутизаторов

Настроим R1 (Рисунок 9.19).

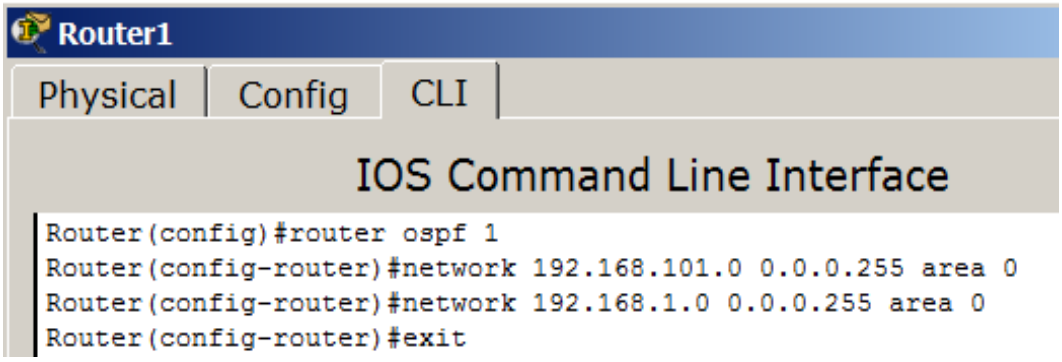


Рисунок - 9.19. Окно настройки маршрутизации на R1.

Теперь установим настройки маршрутизации для R2 (Рисунок 9.20).

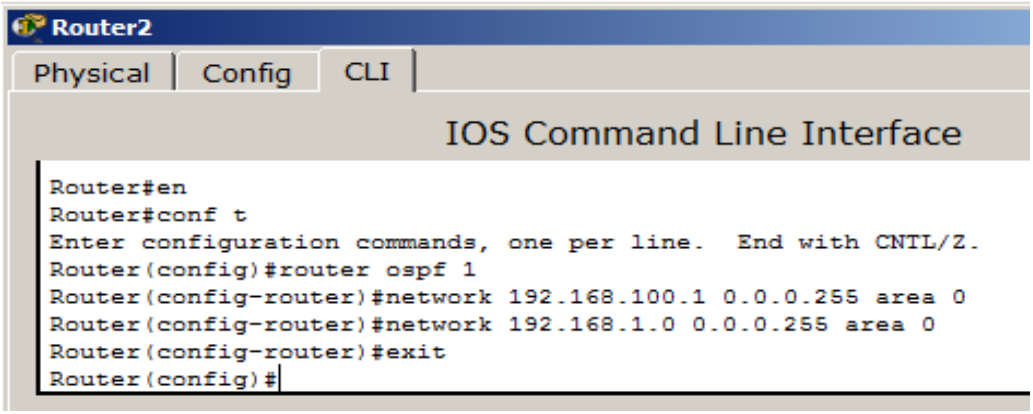


Рисунок - 9.20. Окно настроек R2.

Если вам необходимо сбросить настройки маршрутизатора на CPT, выключите его выключатель питания, а затем снова включите.

Проверьте результат

Для проверки маршрута пингуем ПК из разных сетей (рис. 9.21).

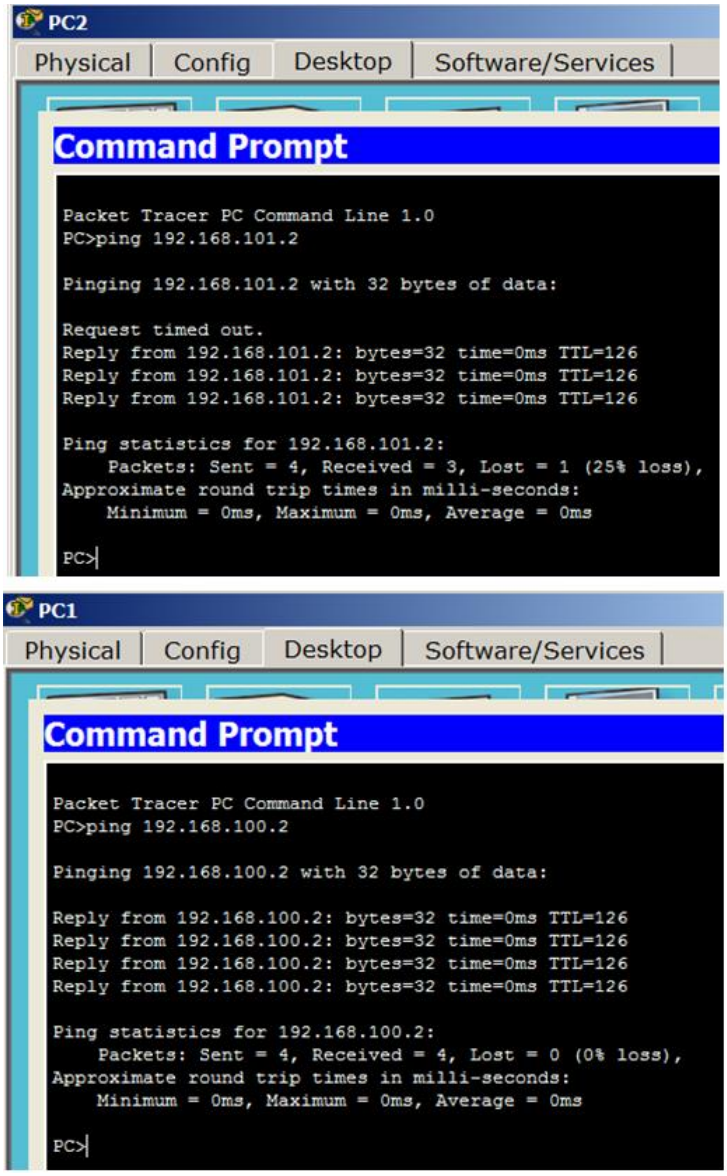


Рисунок - 9.21. Окно результатов проверки производительности OSPF.

Контрольные вопросы:

1. Что такое маршрутизация?
2. Что такое динамическая маршрутизация?
3. Что такое протокол EIGRP?
4. Что такое протокол BGP?
5. Что такое протокол OSPF?
6. Что такое протокол RIP?
7. На сколько типов делятся протоколы маршрутизации?

Практическая работа № 10

Настройте DHCP-сервер в Cisco Packet Tracer.

Цель работы: Овладение навыками изучения и применения DHCP-сервера с помощью программы Cisco Packet Tracer.

Теоретическая часть

Протокол конфигурации динамических хостов (DHCP) представляет собой клиент/серверный протокол, который автоматизированно назначает IP-адреса и другие параметры конфигурации сети, включая маску подсети и стандартный шлюз, к сетевым устройствам. Этот протокол позволяет клиентам получать необходимые настройки TCP/IP от сервера DHCP.

DHCP автоматизирует и централизует процесс назначения IP-адресов. DHCP-сервер управляет пулом IP-адресов и временно выделяет их клиентским устройствам в сети. Так как IP-адреса предоставляются временно, а не навсегда, неактивные адреса возвращаются на сервер для повторного использования.

DHCP-серверы настраиваются в сети для хранения конфигурационных данных TCP/IP и предоставления этих данных новым клиентам, которые поддерживают DHCP. Они делают это через процесс предоставления аренды. Конфигурационные параметры хранятся в базе данных сервера:

- Реальные параметры конфигурации TCP/IP, предоставляемые всем клиентам в сети.
- Действительные IP-адреса, которые хранятся в пуле для назначения клиентам, а также исключенные адреса.
- Зарезервированные IP-адреса, ассоциированные с определенными DHCP-клиентами, что позволяет назначать одному и тому же клиенту постоянный IP-адрес при каждом подключении.
- Срок аренды, или время, в течение которого IP-адрес может использоваться клиентом до необходимости его обновления или повторного запроса.

Когда клиент, поддерживающий DHCP, принимает предложение от DHCP-сервера, он получает следующие данные:

- **IP-адрес**: Адрес, который клиент может использовать в сети.
- **Маска подсети**: Определяет размер подсети и позволяет клиенту правильно интерпретировать IP-адреса в своей сети.
- **Стандартный шлюз**: IP-адрес маршрутизатора, который позволяет клиенту обращаться к устройствам за пределами локальной сети.
- **DNS-сервер**: Адреса серверов DNS, которые клиент может использовать для разрешения доменных имен в IP-адреса.

- **Время аренды**: Период времени, в течение которого IP-адрес остается действительным. После истечения этого времени клиент должен запросить обновление аренды.
- **Опции DHCP**: Дополнительные параметры, такие как время сервера, путь к файлам загрузки и другие конфигурационные параметры, которые могут быть специфичны для данной сети или приложения.

Преимущества DHCP

Надежная конфигурация IP-адресов:

- Использование DHCP снижает вероятность ошибок конфигурации, которые могут возникать при ручной настройке IP-адресов, таких как опечатки или случаи, когда один и тот же IP-адрес назначается нескольким устройствам одновременно.

- Снижение нагрузки на сетевую администрацию:

- DHCP включает следующие функции для уменьшения административных задач:

- Централизованная и автоматизированная конфигурация TCP/IP.

- Возможность определения конфигураций TCP/IP из централизованного местоположения.

- Возможность задания полного набора дополнительных значений конфигурации TCP/IP с помощью параметров DHCP.

- Эффективное управление IP-адресами:

- DHCP упрощает управление IP-адресами для устройств, которые часто перемещаются или подключаются к разным точкам беспроводной сети, обеспечивая их автоматическое обновление и получение новых адресов по мере необходимости.

- Перенаправление начальных сообщений DHCP с помощью агента ретрансляции DHCP:

- DHCP-ретрансляция позволяет направлять начальные сообщения DHCP от клиента к DHCP-серверу, что устраняет необходимость в наличии DHCP-сервера в каждой подсети. Это достигается с помощью ретрансляторов DHCP (DHCP relay agents), которые пересылают запросы от клиентов к удаленным серверам и возвращают ответы обратно клиентам.

Порядок выполенения практической работы

Создание сетевой топологии с двумя отдельными сегментами (192.168.1.x и 192.168.2.x) в Cisco Packet Tracer.

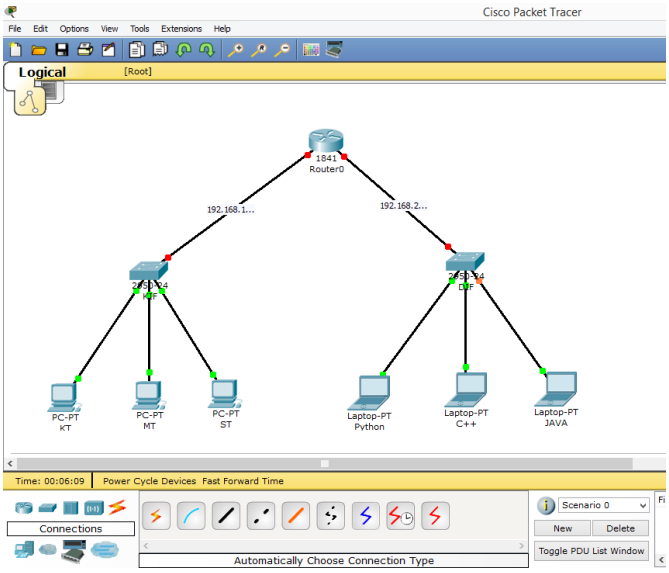


Рисунок - 10.1. Процесс проектирования сети.

В окне CLI маршрутизатора Академии нажмите команду CLI и выберите NO, то есть нет, на экране начальной конфигурации (yes/no) и нажмите Enter. Если на этом экране вы выберете YES, то есть да, маршрутизатор Cisco предложит вам выполнить основные настройки пошагово.

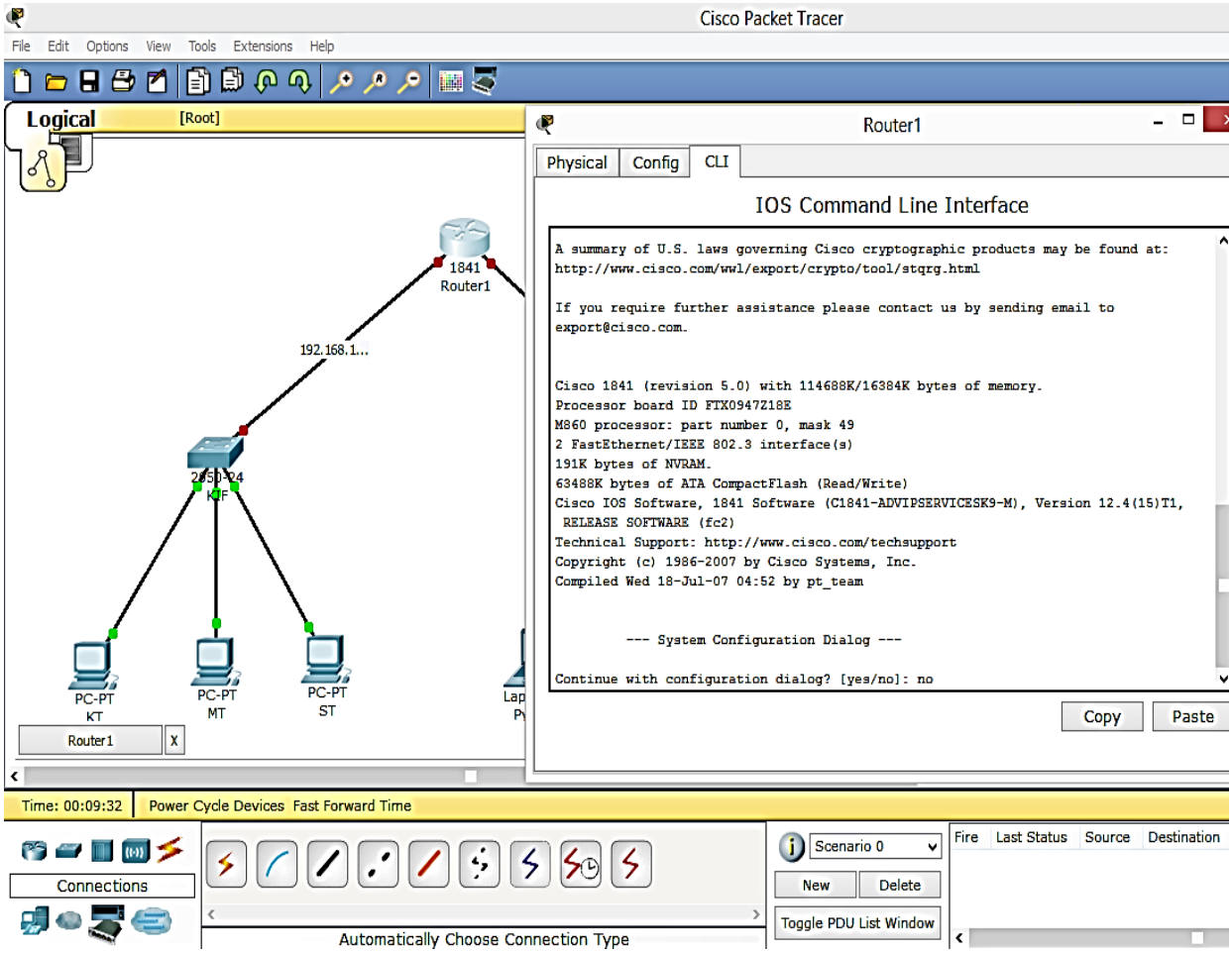


Рисунок - 10.2. Окно CLI.

Назначьте IP-адреса в соответствии с созданной вами топологией сети и подключите открытые порты к интерфейсам маршрутизатора Cisco. Затем выполните следующие команды для автоматического распределения DHCP от маршрутизатора клиентам и закройте настройки.

```
Router>enable
Router#conf t
Router(config)#interface fastEthernet 0/0
Router(config-if)#ip address 192.168.1.1 255.255.255.0
Router(config-if)#no shutdown
Router#conf t
Router(config)#interface fastEthernet 0/1
Router(config-if)#ip address 192.168.2.1 255.255.255.0
Router(config-if)#no shutdown

Router(config-if)#exit
Router(config)#ip dhcp pool LAN1
Router(dhcp-config)#network 192.168.1.0 255.255.255.0
Router(dhcp-config)#default-router 192.168.1.1
Router(dhcp-config)#dns-server 192.168.2.1
Router(dhcp-config)#exit
Router(config)#ip dhcp excluded-address 192.168.1.1
Router(config)#ip dhcp pool LAN2
Router(dhcp-config)#network 192.168.2.0 255.255.255.0
Router(dhcp-config)#default-router 192.168.2.1
Router(dhcp-config)#dns-server 192.168.2.1
Router(dhcp-config)#exit
Router(config)#ip dhcp excluded-address 192.168.2.1
Router(config)#end
Router#wr
```

```
Router>enable
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#interface fastEthernet 0/0
Router(config-if)#ip address 192.168.1.1 255.255.255.0
Router(config-if)#no shutdown

%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state t
o up

Router(config-if)#exit
Router(config)#interface fastEthernet 0/1
Router(config-if)#ip address 192.168.2.1 255.255.255.0
Router(config-if)#no shutdown

%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state t
o up
```

Рисунок - 10.3. Код устройства.

```
Router(config-if)#exit
Router(config)#ip dhcp pool LAN1
Router(dhcp-config)#network 192.168.1.0 255.255.255.0
Router(dhcp-config)#default-router 192.168.1.1
Router(dhcp-config)#dns-server 192.168.1.1
Router(dhcp-config)#exit
Router(config)#ip dhcp excluded-address 192.168.1.1
Router(config)#ip dhcp pool LAN2
Router(dhcp-config)#network 192.168.2.0 255.255.255.0
Router(dhcp-config)#default-router 192.168.2.1
Router(dhcp-config)#dns-server 192.168.2.1
Router(dhcp-config)#exit
Router(config)#ip dhcp excluded-address 192.168.2.1
Router(config)#end

%SYS-5-CONFIG_I: Configured from console by console
Router#wr
Building configuration...
[OK]
Router#
```

Рисунок - 10.4. Код устройства.

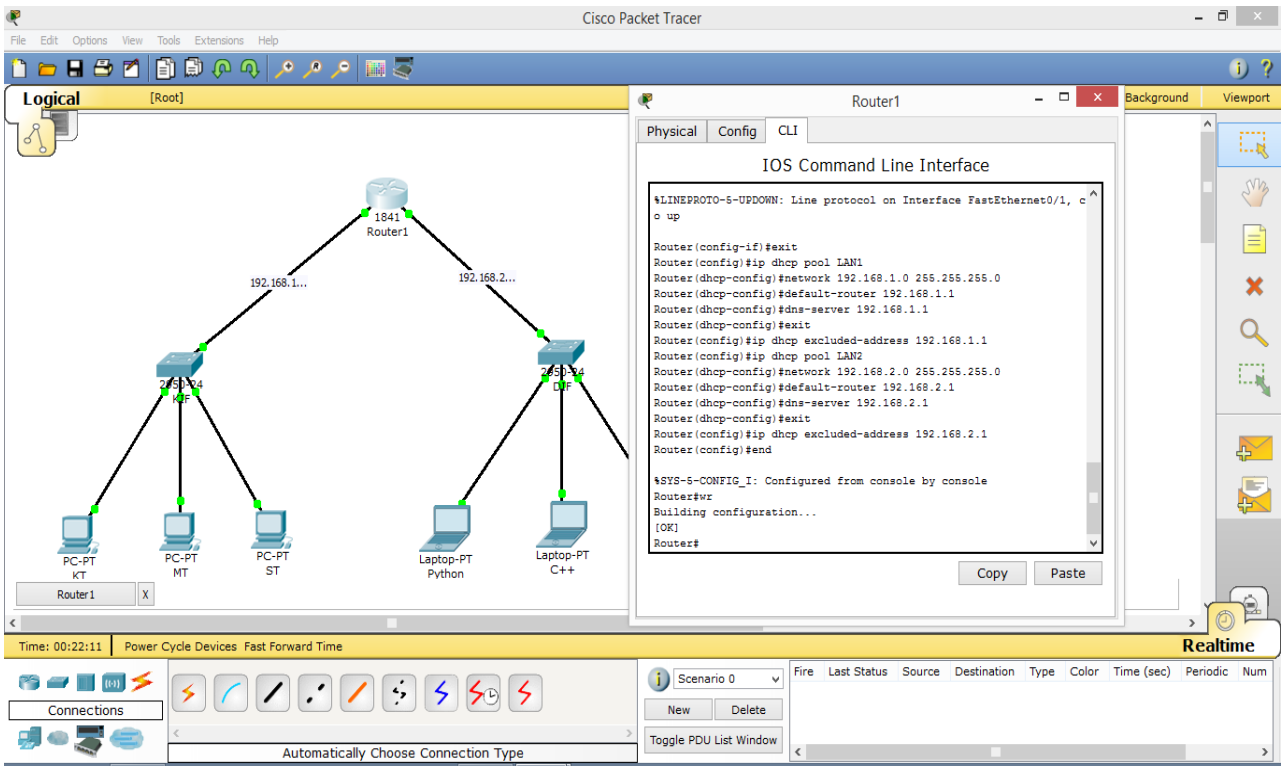


Рисунок - 10.5. Настройка спроектированной сети.

После ввода команд Cisco DHCP, необходимо настроить компьютеры, добавленные на рабочую область Packet Tracer, для автоматического получения IP-адреса. Для этого выберите ПК, в открывшемся окне нажмите "Настройка IP" и затем выберите "DHCP".

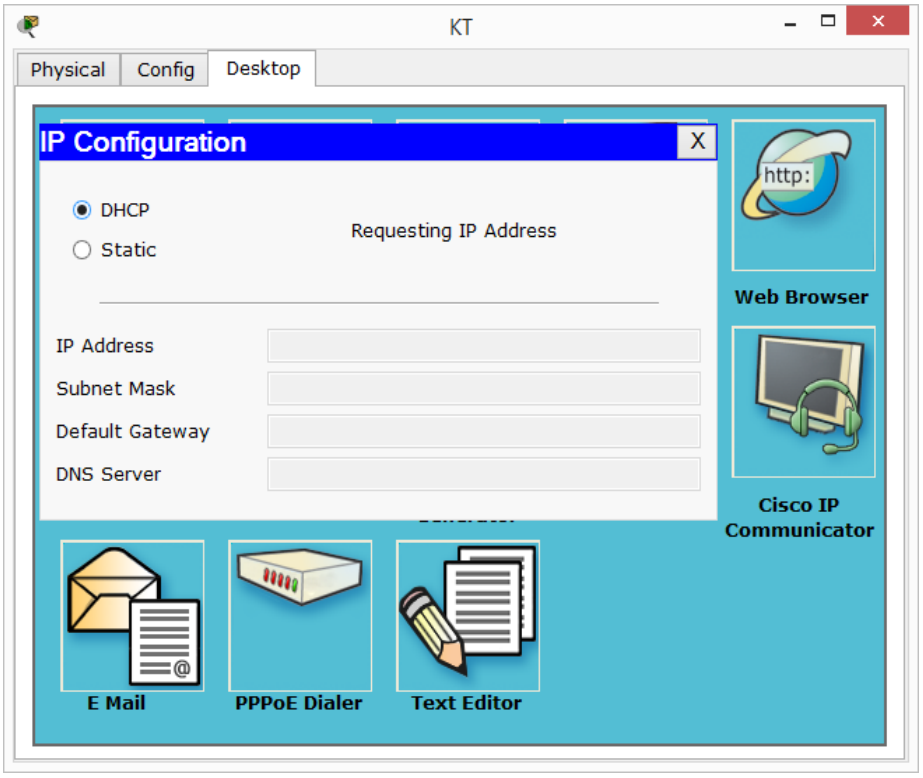


Рисунок 10.6. Окно настройки DHCP.

После включения DHCP на ПК будет отправлен запрос на IP-адрес, как показано на следующем изображении. DHCP ответит на запрос, предоставив IP-адрес.

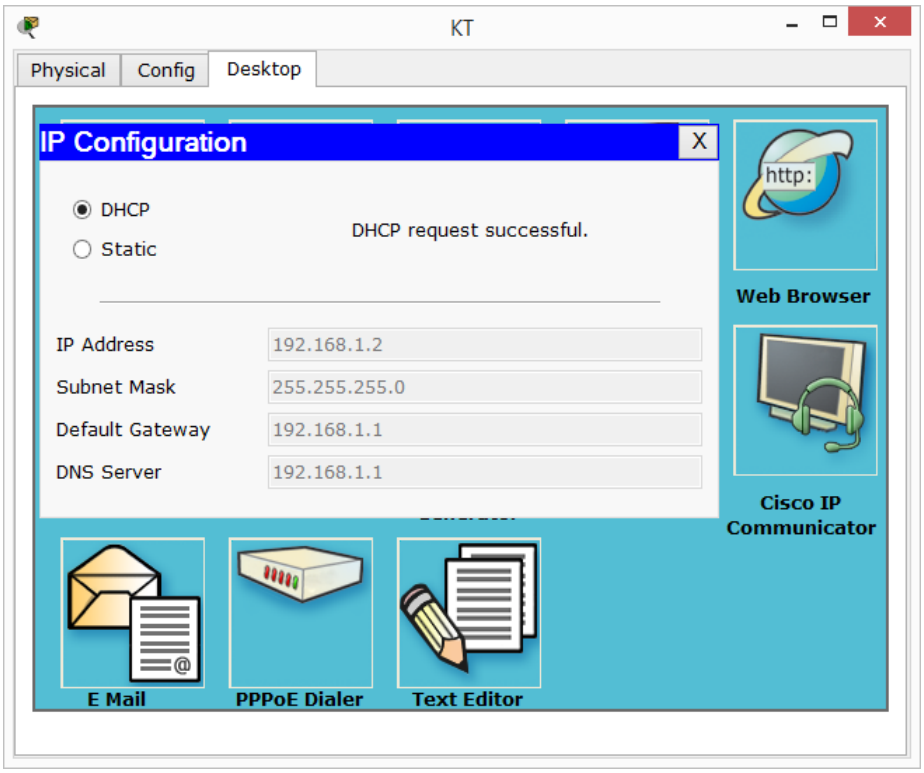


Рисунок - 10.7. Окно настройки DHCP.

Для компьютеров в сети 192.168.2.x включите параметр DHCP и проверьте результат.

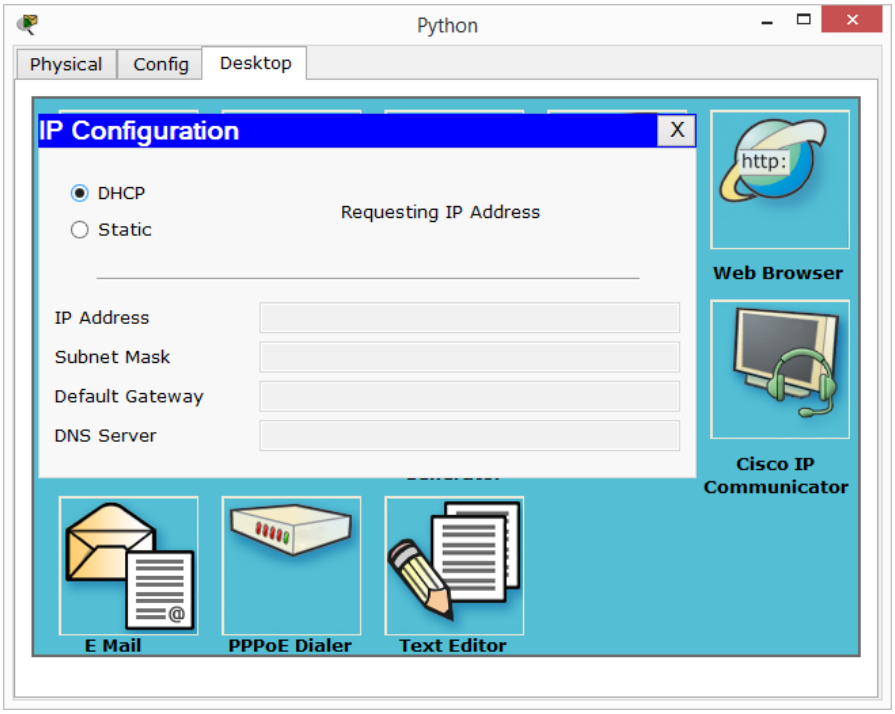


Рисунок - 10.8. Окно настройки DHCP.

Python также успешно получает IP-адрес, так как DHCP на маршрутизаторе Cisco выдает результат для сети 192.168.2.x.

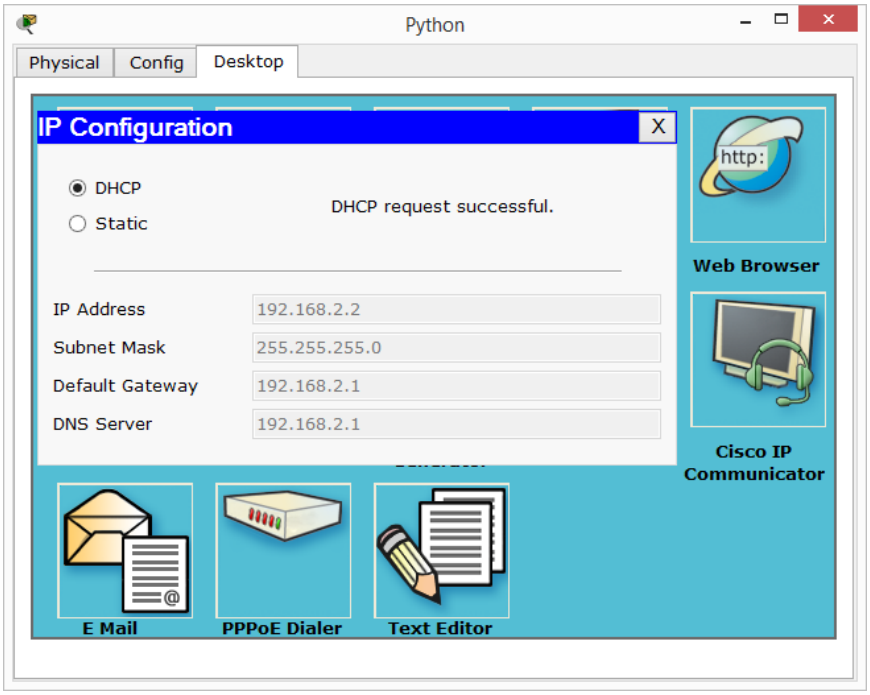


Рисунок - 10.9. Окно настройки DHCP.

Если вы подключите ПК к сети 2.0 и проверите сетевое соединение, это будет успешно, как показано ниже.

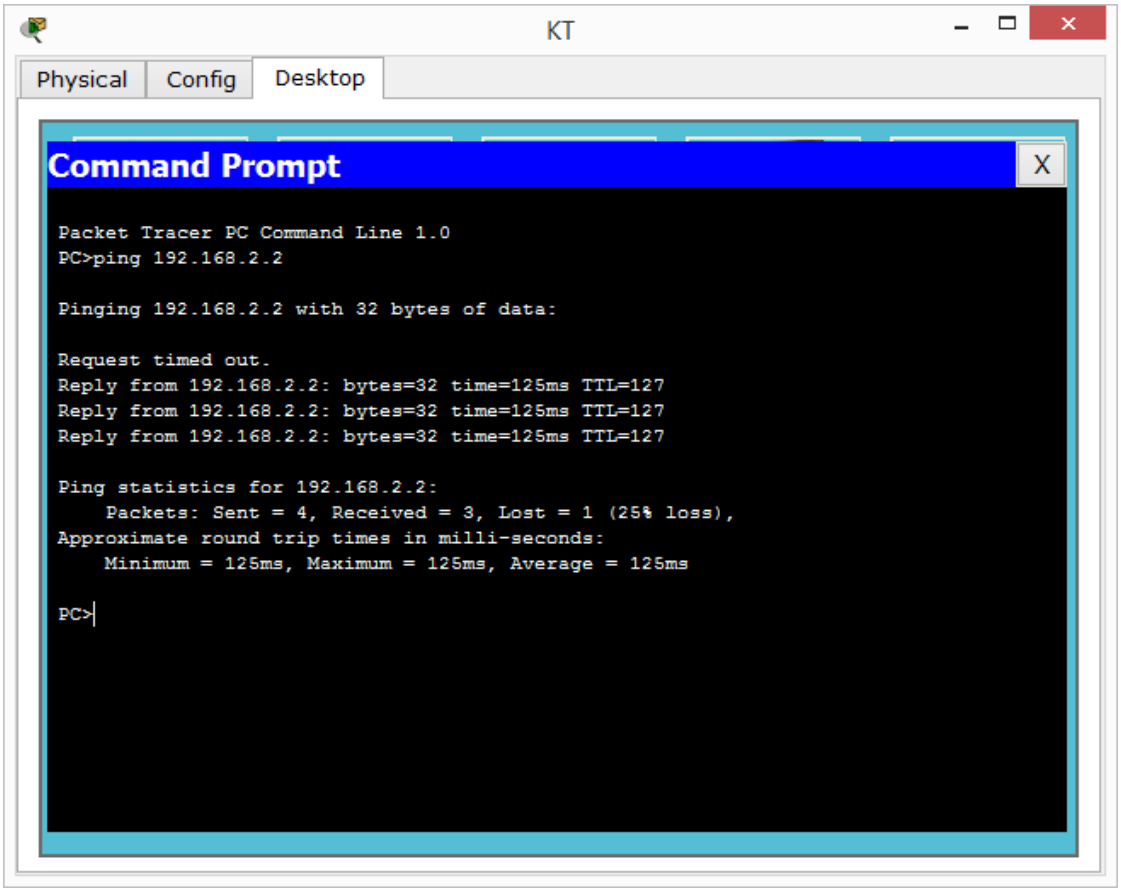


Рисунок - 10.10. Окно Desktop.

Вы можете увидеть назначенные IP-адреса и MAC-адреса клиентов на маршрутизаторе с помощью команды Show IP DHCP.
Router>show ip dhcp binding

```
Router>show ip dhcp binding
IP address       Client-ID/              Lease expiration        Type
                 Hardware address
192.168.1.2      0060.47C3.26A0           --                     Automatic
192.168.2.2      00E0.B0CD.67BD           --                     Automatic
```

Рисунок - 10.11. Адрес устройства.

варианты заданий по практической работе:

1. Подключите к локальной сети 10 компьютеров и 2 маршрутизатора с использованием DHCP.

2. Протестируйте автоматически назначенные IP-адреса и проанализируйте результат.

3. Представьте выполненную работу в виде отчета с изображениями и пояснениями.

Контрольные вопросы:

1. Что такое DHCP и для чего он используется в сети?
2. Какие преимущества использования DHCP по сравнению с ручной настройкой IP-адресов?
3. Какую информацию DHCP-сервер предоставляет клиентам?
4. В чем разница между прямой и обратной маской (subnet mask и wildcard mask)?
5. Как настроить DHCP на маршрутизаторе Cisco?
6. Какие команды используются для проверки DHCP-настроек и назначенных IP-адресов на маршрутизаторе?
7. Какие проблемы могут возникнуть при использовании DHCP в большой сети?
8. Как с помощью DHCP обеспечить безопасность сети?
9. Что такое агент ретрансляции DHCP и для чего он нужен?
10. Каковы основные этапы настройки DHCP в Cisco Packet Tracer?

Практическая работа № 11

Работа с протоколами Telnet и SSH в программе Cisco Packet Tracer.

Цель работы: Овладение навыками работы с протоколами TELNET и SSH в программе Cisco Packet Tracer.

Теоретическая часть

SSH и Telnet — это два сетевых протокола, которые используются для удаленного доступа к компьютеру через сеть или Интернет и управления системой с помощью удаленных команд. Таким образом, оба они считаются терминальными эмуляторами. SSH означает Secure Shell (Безопасная оболочка) и позволяет пользователю обмениваться данными между парами компьютеров в сети с использованием безопасного зашифрованного соединения. Telnet — это основной сетевой протокол, который используется для связи с удаленной системой с помощью текстового терминала.

SSH (Secure Shell) — это сетевой протокол, который используется для установления безопасного соединения между двумя удаленными хостами через Интернет или внутри сети. SSH использует зашифрованный формат для передачи данных между компьютерами, что обеспечивает конфиденциальность и целостность передаваемой информации. SSH широко используется для выполнения удаленных команд благодаря высокому уровню безопасности в системах удаленного доступа. Пользователь может безопасно отправлять конфиденциальную информацию, такую как имя пользователя, пароль и другие команды, поскольку эти данные передаются в зашифрованном виде и их трудно расшифровать и прочитать хакерам. Для аутентификации удаленной системы SSH использует криптографию с открытыми ключами. SSH-серверы прослушивают порт 22 через протокол TCP (Transmission Control Protocol) и могут использоваться в публичной сети. SSH обеспечивает надежную аутентификацию и безопасное общение через небезопасные каналы.

Telnet также является сетевым протоколом, используемым для двустороннего обмена данными между двумя удаленными хостами в сети или Интернете. С помощью этого протокола пользователи могут получить доступ к удаленной системе и взаимодействовать с ней через виртуальный терминал. Однако это небезопасно для использования в ненадежных сетях, таких как Интернет, поскольку Telnet передает данные в виде обычного текста. Поэтому Telnet не подходит для передачи конфиденциальной информации, такой как имена пользователей и пароли, так как эти данные могут быть легко перехвачены и прочитаны. Обычно Telnet подключается через порт 23 по

протоколу TCP и может использоваться для доступа к другим портам и службам. Из-за низкого уровня безопасности Telnet может использоваться в частных сетях.

Порядок выполенения практической работы

1. Создадим небольшую топологию в Cisco Packet Tracer. Настроим Telnet для подключения к маршрутизатору через локальную сеть. После добавления маршрутизатора Cisco, коммутатора и компьютера на рабочую область, подключим все устройства кабелями.

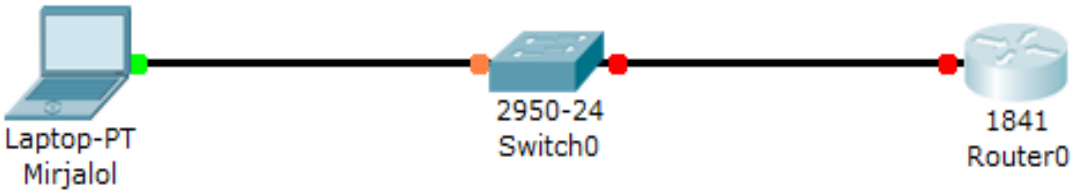


Рисунок 11.1. Проектирование сети.

Дважды щелкните на маршрутизатор, чтобы открыть командную строку CLI. Чтобы пропустить начальную настройку, введите «No» и нажмите Enter.

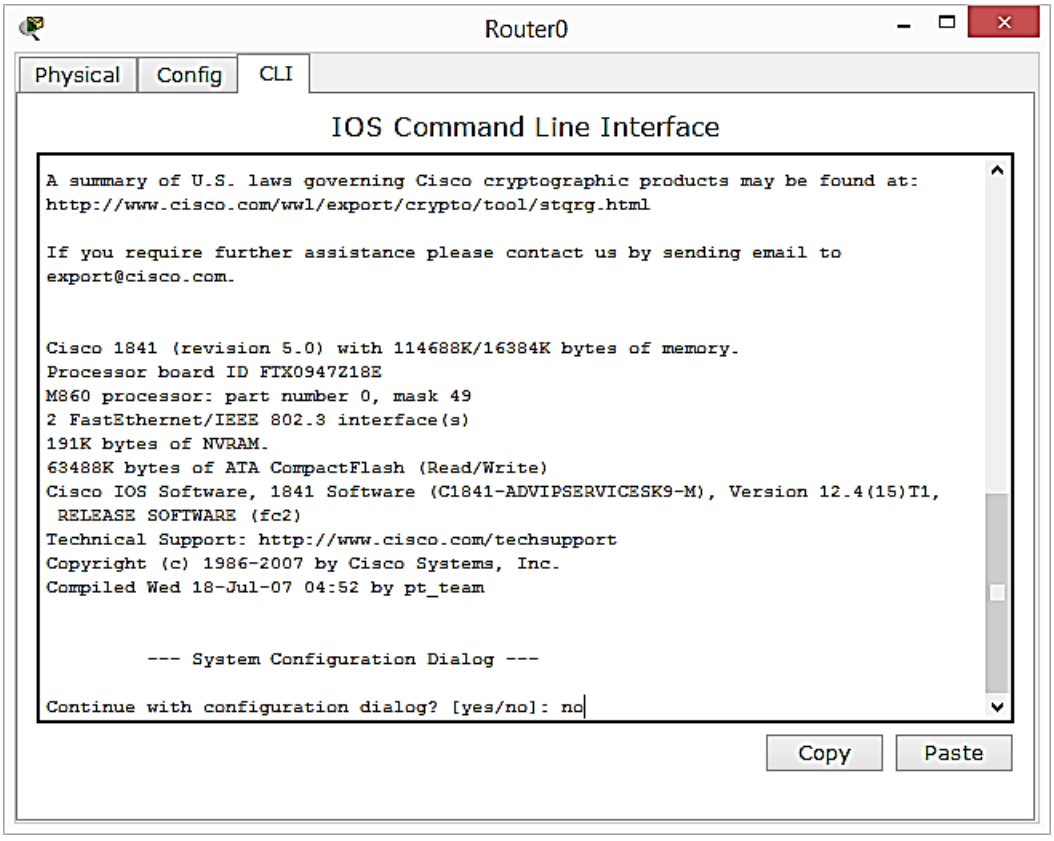


Рисунок - 11.2. Настройка устройства.

Для включения Telnet-протокола на маршрутизаторе выполните следующие команды:

```
Router>en
Router#enable
Router#conf t
Router(config)#interface fastEthernet 0/0
Router(config-if)#ip address 192.168.0.1 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#line vay 0 4
Router(config-line)#login local
Router(config-line)#password telnet123
Router(config-line)#privilege level 15
Router(config-line)#exit
Router(config)#username cisco privilege 15 password cisco123
Router(config)#end
Router#wr
```

```
        --- System Configuration Dialog ---

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


Press RETURN to get started!



Router>en
Router#enable
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#interface fastEthernet 0/0
Router(config-if)#ip address 192.168.0.1 255.255.255.0
Router(config-if)#no shutdown

%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state t
o up

Router(config-if)#exit
Router(config)#line vty 0 4
Router(config-line)#login local
Router(config-line)#password telnet123
Router(config-line)#privilege level 15
Router(config-line)#exit
Router(config)#username cisco privilege 15 password cisco123
Router(config)#end

%SYS-5-CONFIG_I: Configured from console by console
Router#wr
Building configuration...
[OK]
Router#
```

Рисунок - 11.3. Ввод кода в устройство.

4. После настройки маршрутизатора создайте имя пользователя и пароль для подключения по Cisco Telnet. Перед подключением к маршрутизатору выполните следующую конфигурацию на компьютере в рабочей области:

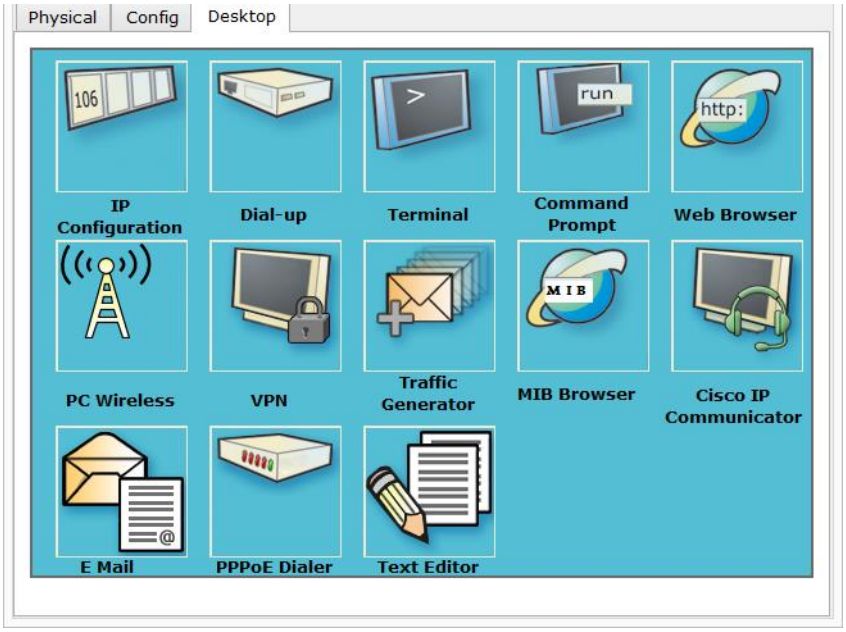


Рисунок - 11.4. Окно рабочего стола.

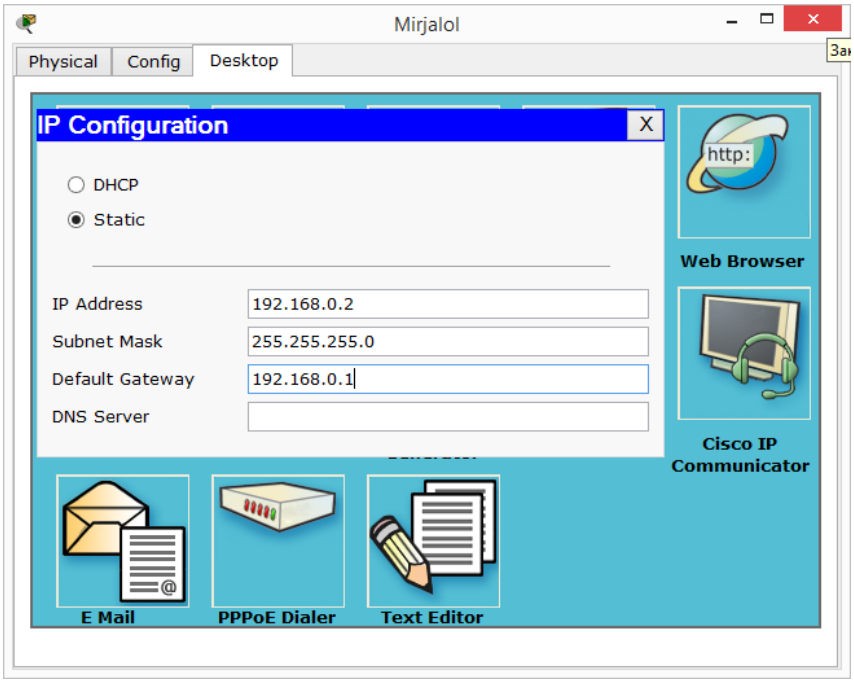


Рисунок - 11.5. Статическая адресация.

Закройте настройки IP и перейдите в командную строку (Command Prompt).

В командной строке введите telnet 192.168.0.1 и нажмите Enter. Затем введите имя пользователя и пароль. В данном случае, Username: cisco, Password: cisco123 (пароль не отображается при вводе).

Рисунок - 11.6. Окно командной строки.

После подключения к маршрутизатору Cisco, вы можете управлять своим устройством через LAN и WAN. Чтобы просмотреть подключения к устройству, выполните команду `show line`.

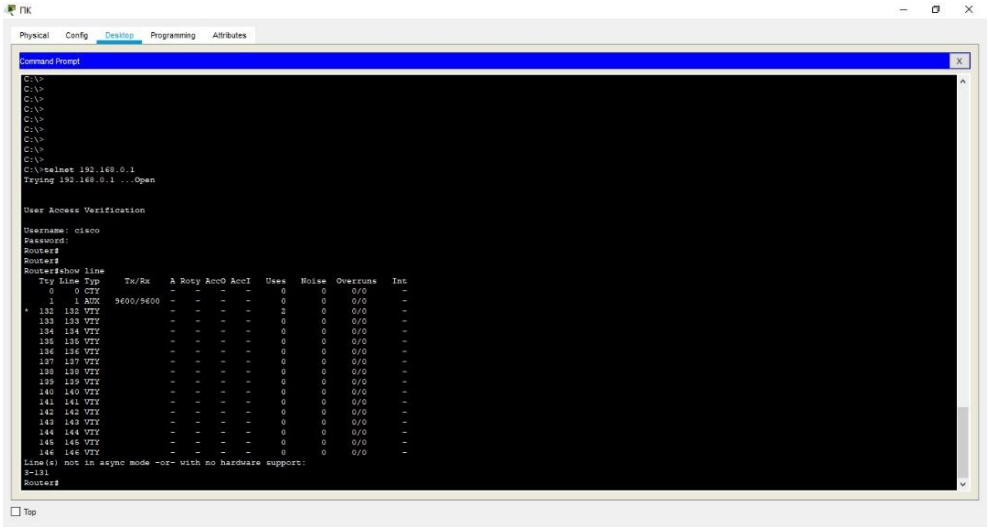


Рисунок - 11.7. Окно подключения к устройству.

Теперь настроим SSH на коммутаторе — для этого необходимо указать имя хоста, доменное имя и создать ключ шифрования.

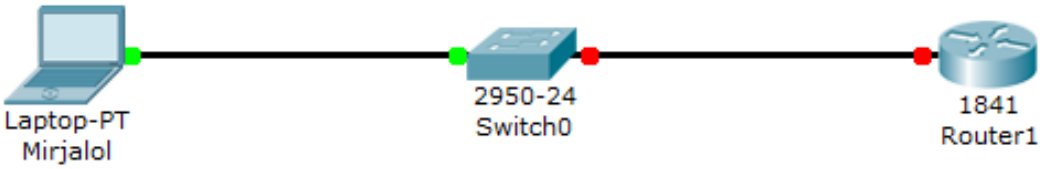


Рисунок - 11.8. Спроектированная сеть.

Дважды щелкните по маршрутизатору и перейдите в командную строку. Для пропуска начальных настроек нажмите клавишу Enter.

Чтобы настроить SSH на вашем маршрутизаторе, выполните следующие команды в указанном порядке:

Router>enable
Router#conf t
Router(config)#hostname ADMIN
ADMIN(config)#interface fastethrnet 0/0
ADMIN(config-if)#ip address 192.168.1.1 255.255.255 .0
ADMIN(config-if)#no shutdown
ADMIN(config-if)#ip domain name ciscoadmin
ADMIN(config)crypto key generate rsa

```
Router>enable
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname ADMIN
ADMIN(config)#interfase fastEthernet 0/0
                     ^
% Invalid input detected at '^' marker.

ADMIN(config)#int
ADMIN(config)#interface fas
ADMIN(config)#interface fastEthernet 0/0
ADMIN(config-if)#ip address 192.168.1.1 255.255.255.0
ADMIN(config-if)#no shutdown

%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state t
o up

ADMIN(config-if)#ip domain name ciscoadmin
ADMIN(config)#cryoto key generatersa
                ^
% Invalid input detected at '^' marker.

ADMIN(config)#
ADMIN(config)#crypto key genera
ADMIN(config)#crypto key generate r
ADMIN(config)#crypto key generate rsa
The name for the keys will be: ADMIN.ciscoadmin
Choose the size of the key modulus in the range of 360 to 2048 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
```

Рисунок - 11.9. Код устройства.

```
How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

ADMIN(config)#ip ssh version 2
*??? 1 0:9:16.396:  %SSH-5-ENABLED: SSH 1.99 has been enabled
ADMIN(config)#ip ssh time-out 10
ADMIN(config)#ip ssh aut
ADMIN(config)#ip ssh authentication-retries 3
ADMIN(config)#line vty 0 4
ADMIN(config-line)#login local
ADMIN(config-line)#pri
ADMIN(config-line)#privilege le
ADMIN(config-line)#privilege level 15
ADMIN(config-line)#tra
ADMIN(config-line)#transport le
ADMIN(config-line)#transport level
ADMIN(config-line)#transport level 15
                                 ^
% Invalid input detected at '^' marker.

ADMIN(config-line)#tra
ADMIN(config-line)#transport input ssh
ADMIN(config-line)#exit
ADMIN(config)#username cisco pri
ADMIN(config)#username cisco privilege 15 pas
ADMIN(config)#username cisco privilege 15 password cisc
ADMIN(config)#username cisco privilege 15 password cisco123
ADMIN(config)#end

%SYS-5-CONFIG_I: Configured from console by console
ADMIN#wr
Building configuration...
[OK]
ADMIN#
```

Рисунок - 11.10. Код устройства.

Теперь настроим параметры персонального компьютера в разделе IP-конфигурации:

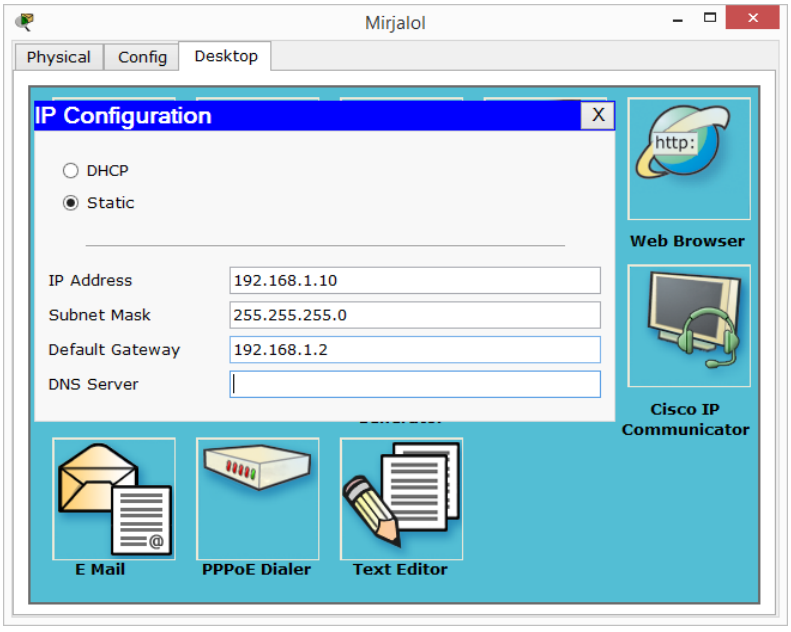


Рисунок - 11.11. Адресация.

Для подключения выполните следующие действия: откройте командную строку на компьютере и введите следующую команду, затем нажмите Enter:

ssh -l cisco 192.168.1.1

- `-l` — значение для входа (логин);
- `cisco` — имя пользователя для подключения к маршрутизатору;
- `192.168.1.1` — IP-адрес маршрутизатора.

Введите созданный пароль, и подключение будет установлено. После выполнения команды `show ssh` можно проверить версию протокола SSH в командной строке.

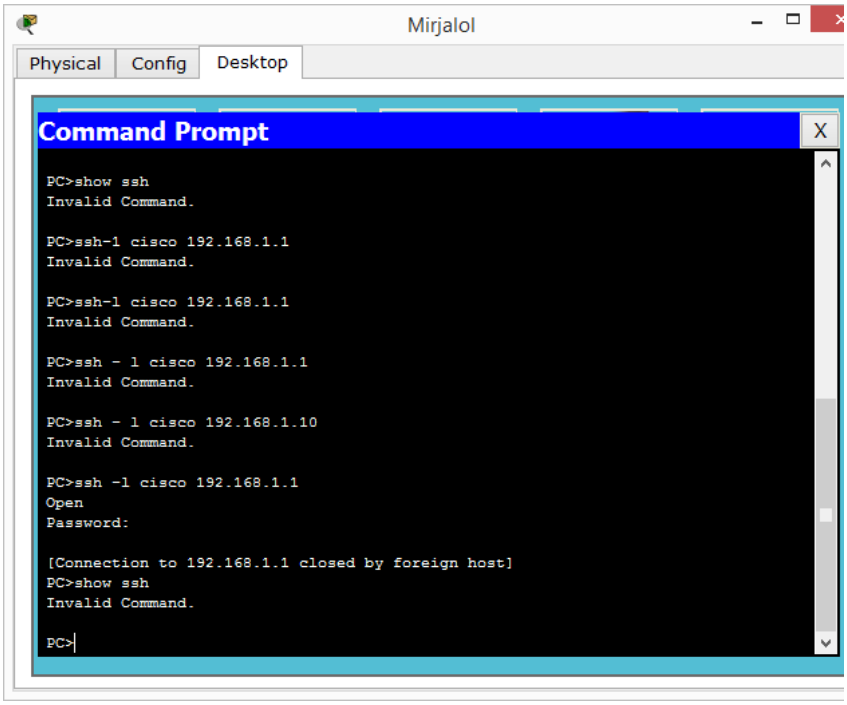


Рисунок - 11.12. Процесс тестирования.

Варианты заданий по практической работе:

1. Спроектируйте локальную сеть и установите соединение через протоколы Telnet и SSH.

2. Протестируйте сеть и проанализируйте результаты.

3. Подготовьте отчет о проделанной работе в виде рисунков и пояснений.

Вопросы для контроля:

1. Что такое Telnet?
2. Что такое SSH?
3. Какие виды протоколов существуют?
4. Какие функции выполняют протоколы Telnet и SSH

Практическая работа № 12

Изучение функции безопасности портов коммутатора

Цель работы: Изучение функции безопасности портов коммутатора, которая позволяет защищать от атак, направленных на заполнение таблицы коммутатора.

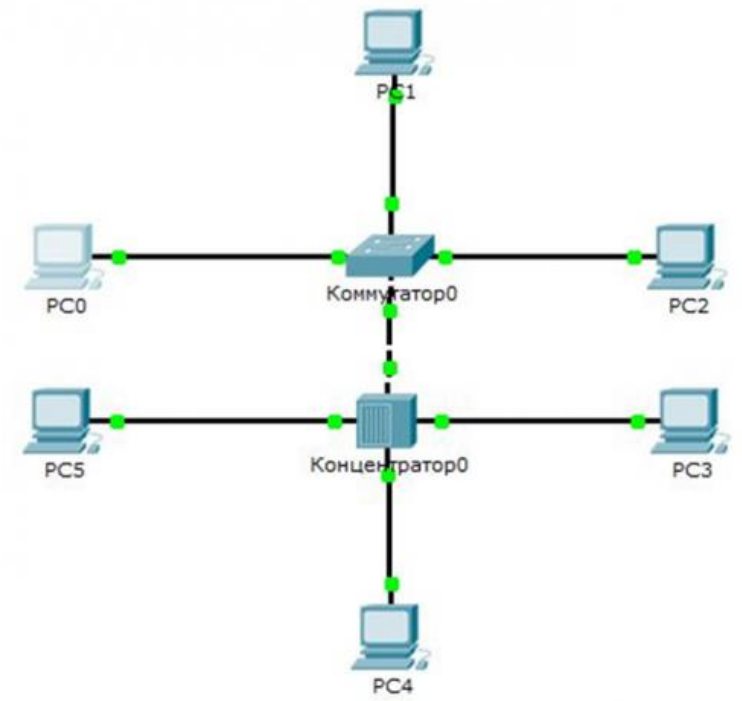


Рисунок - 12.1. Схема сети.

Пример создания локальной сети в Cisco Packet Tracer. Схема сети представлена на рисунке 13.1. Далее приведены пошаговые инструкции. Последовательность действий:

В нижнем левом углу Packet Tracer выберите устройства «Сетевые коммутаторы» и выберите 2950-24, щелкнув левой кнопкой мыши по элементу в правом списке, затем поместите его на рабочую область. Аналогичным образом мы поступим с концентратором сети (Hub-PT) и рабочими станциями (PC-PT), как показано на рисунках 13.2, 13.3 и 13.4.

Рисунок - 12.2. Выбор коммутатора из списка доступных устройств.

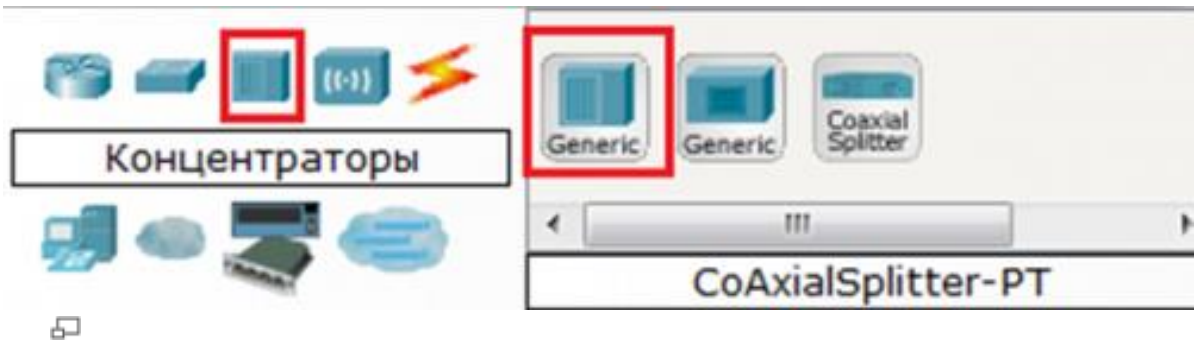


Рисунок - 12.3. Выбор концентратора.

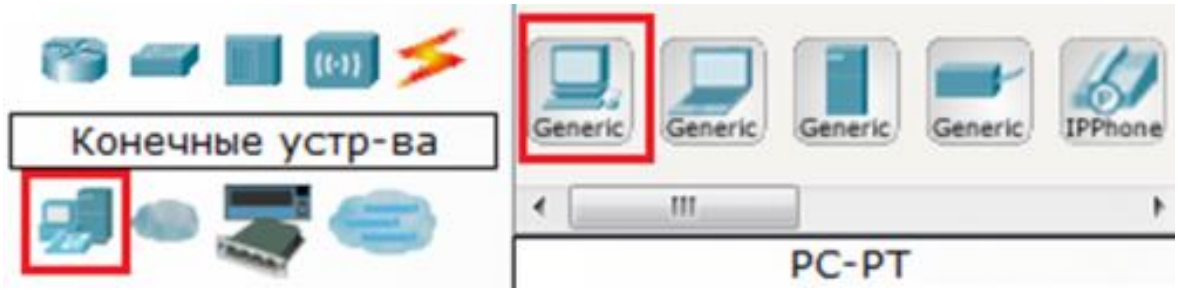


Рисунок - 12.4. Выбор компьютера.

Разместите компьютеры, коммутаторы и концентратор на рабочем месте, как показано на рисунке 13.1. Затем, используя соответствующие интерфейсы, подключите устройства, как показано на рисунке 13.1. Для подключения компьютеров к коммутатору и концентратору используются кабели типа «Copper straight-through» (медные прямые).

Рисунок 12.5. Выбор медного кабеля.

3. Для подключения коммутатора и концентратора друг к другу используется медный перекрестный кабель, как показано на рисунке 13.6.

Рисунок 12.6. Выбор кроссового кабеля.

Кроме того, необходимо выбрать подходящий тип кабеля для соединения двух устройств и выбрать один из доступных портов FastEthernet на одном устройстве и другой из доступных портов FastEthernet на другом устройстве, как показано на рисунках 13.2, 13.3 и 13.4.

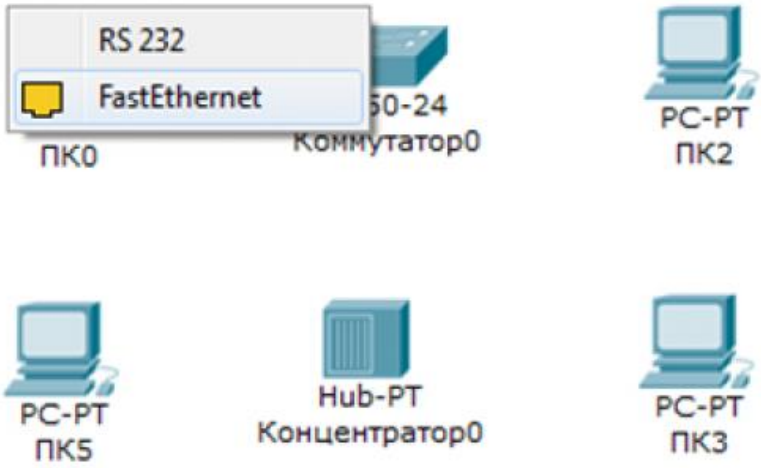


Рисунок 12.7. Выбор свободного порта на компьютере.

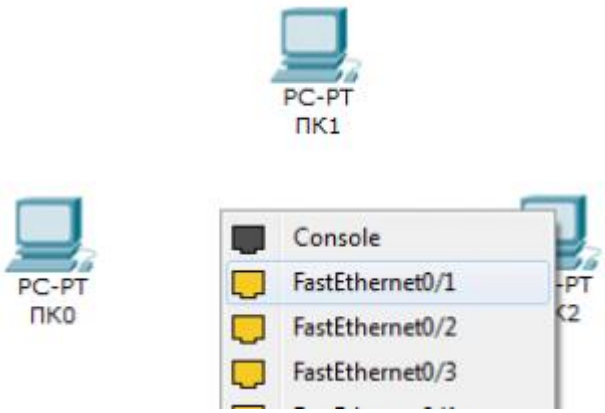


Рисунок 12.8. Выбор свободного порта на коммутаторе.

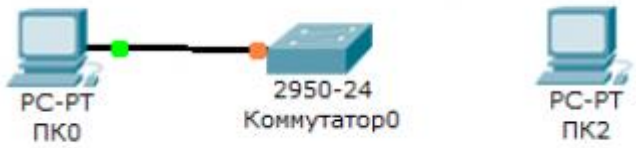


Рисунок 12.9. Подключение PC0 и коммутатора0 правильным медным кабелем.

Подключение всех остальных устройств выполняется таким же образом. Связь между коммутатором и концентратором осуществляется через кроссовый кабель.

Следующий важный этап — настройка. Поскольку мы используем устройства, работающие на начальных уровнях модели OSI (коммутатор второго уровня, концентратор первого уровня), их настройка не требуется. Необходимо только настроить рабочие станции, то есть: IP-адреса и маски подсети. Ниже показана настройка только одной станции (PC0), остальные настраиваются аналогично. Мы дважды кликаем на нужную рабочую станцию, как показано на рисунке 13.7.

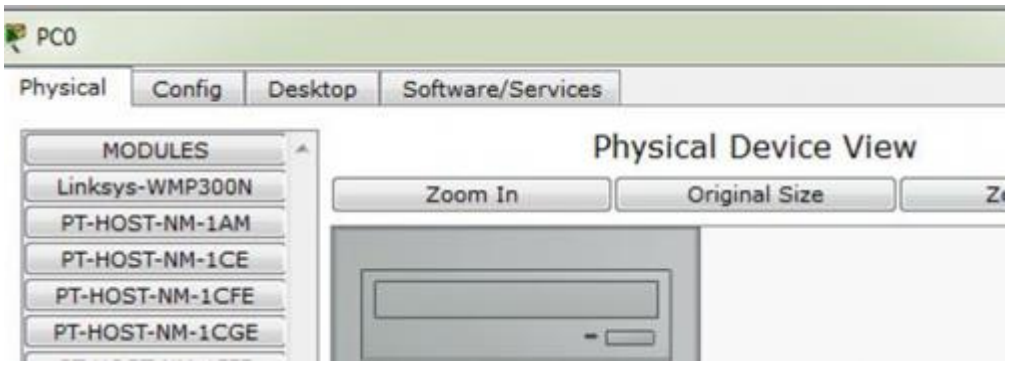


Рисунок 12.10. Окно настройки PC0.

В открывшемся окне выберите вкладку «Рабочий стол», затем установите IP-адрес в разделе «IP-конфигурация», как показано на рисунке 13.11.

Рисунок - 12.11. Окно «Рабочий стол».

Рисунок - 12.12. назначение IP-адреса.

Так же, IP-адреса назначаются всем остальным компьютерам согласно таблице адресов.

Устройство	IP адрес	Маска подсети
PC0	192.168.0.1	255.255.255.0
PC1	192.168.0.2	255.255.255.0
PC2	192.168.0.3	255.255.255.0
PC3	192.168.0.4	255.255.255.0
PC4	192.168.0.5	255.255.255.0
PC5	192.168.0.6	255.255.255.0

12.1-таблица. Таблица адресов.

1. После завершения настройки выполняется процесс ping. Например, он начинается с PC5 и проверяет связь с PC1, при этом важно, чтобы пакеты передавались через коммутатор и концентратор. Для этого дважды щелкните на нужной рабочей станции, в открывшемся окне выберите вкладку «Desktop», а затем выберите командную строку «Command prompt» согласно рисунку 13.13.

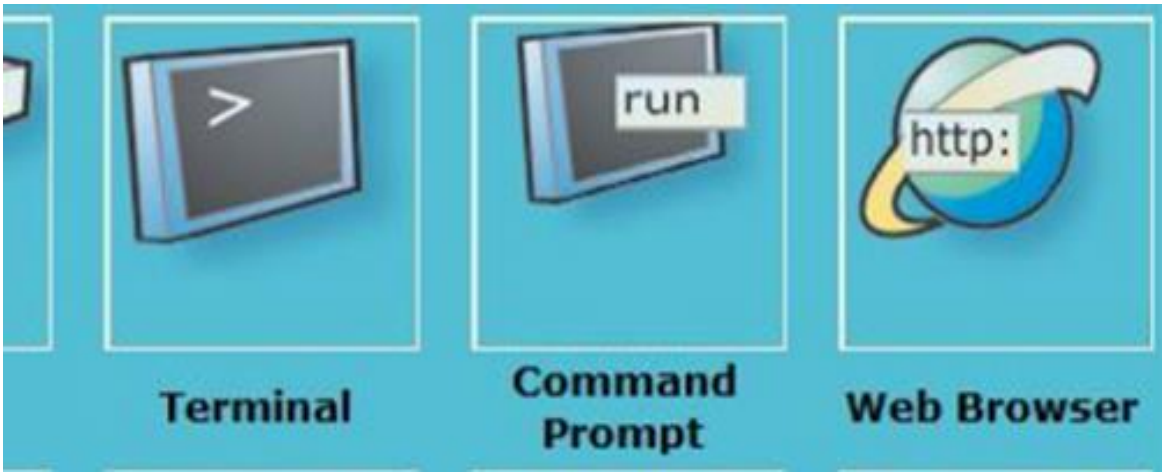


Рисунок - 12.13. Выбор режима командной строки.

Как показано на рисунке 12.14, появится окно командной строки.

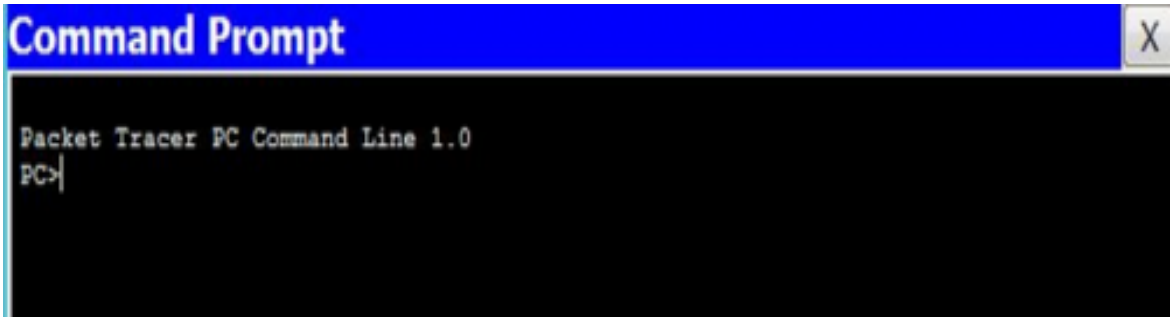


Рисунок - 12.14. Окно командной строки.

Введите команду `PC>ping 192.168.0.4` в командной строке и нажмите Enter. Если все настройки выполнены правильно, будет предоставлена информация, как показано на рисунке 13.15.

```
PC>ping 192.168.0.4

Pinging 192.168.0.4 with 32 bytes of data:

Reply from 192.168.0.4: bytes=32 time=1ms TTL=128
Reply from 192.168.0.4: bytes=32 time=0ms TTL=128
Reply from 192.168.0.4: bytes=32 time=0ms TTL=128
Reply from 192.168.0.4: bytes=32 time=0ms TTL=128

Ping statistics for 192.168.0.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

Рисунок - 12.15. Окно результата от командыPing.

Это означает, что связь установлена и сеть функционирует.

Требования к выполению задания

Требуется построить сеть в Cisco Packet Tracer по данной топологии. После топологии в таблице в разделе Практическая работа указана схема адресов, которые следует использовать.

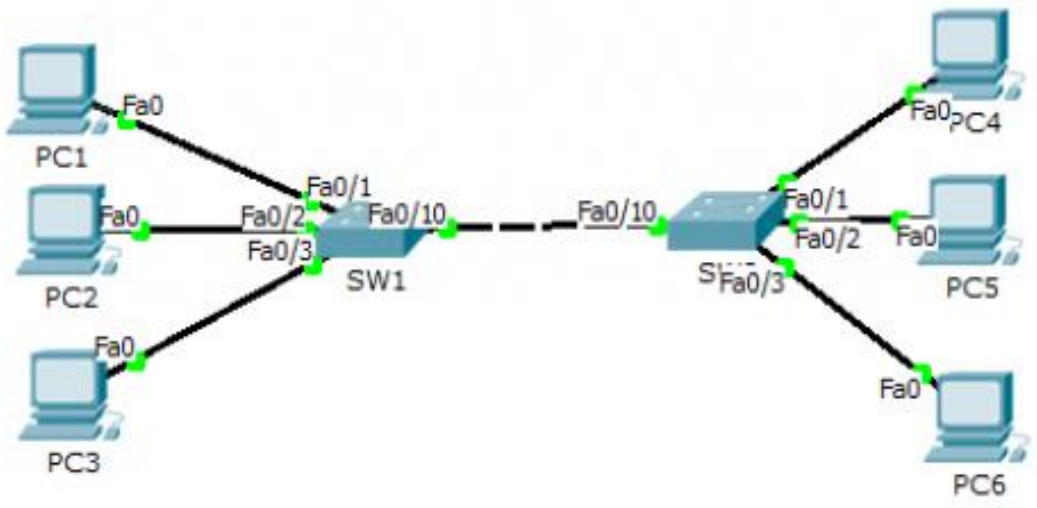


Рисунок - 12.16. Схема сети.

Qurilma	IP manzil	Tarmoqosti maska	Interfeys	Rejimlar (holatlar)
PC1	16.4.0.1	255.0.0.0	Fa0	n/a
PC2	16.4.0.2	255.0.0.0	Fa0	n/a
PC3	16.4.0.3	255.0.0.0	Fa0	n/a
PC4	16.4.0.4	255.0.0.0	Fa0	n/a
PC5	16.4.0.5	255.0.0.0	Fa0	n/a
PC6	16.4.0.6	255.0.0.0	Fa0	n/a
SW1	N/A	N/A	Fa0/1	Shutdown
SW1	N/A	N/A	Fa0/2	Restrict
SW1	N/A	N/A	Fa0/3	Protect
SW2	N/A	N/A	Fa0/1	Shutdown
SW2	N/A	N/A	Fa0/2	Restrict
SW2	N/A	N/A	Fa0/3	Protect

Таблица - 12.2. Таблица адресов.

Последовательность выполняемых действий:

1. Настройте порты SW1 и SW2 в режим доступа.

```
Switch(config)#interface fastethernet0/10
Switch(config-if)#switchport mode access
```

Рисунок - 12.17. Перевод портов в режим доступа.

2. Активируйте безопасность портов на портах SW1 и SW2, обращенных к устройствам.

```
Switch(config-if)#switchport mode access
Switch(config-if)#
Switch(config-if)#switchport port-security
Switch(config-if)#
```

Рисунок - 12.18. Включение безопасности порта.

3. Установите максимальное значение `secure-mac` на портах SW1 и SW2, направленных к устройствам.

```
Switch(config-if)#switchport port-security maximum 1
```

Рисунок - 12.19. Определение количества безопасных MAC-адресов.

4. Настройте динамическое определение безопасных MAC-адресов на SW1

```
Switch(config-if)#
Switch(config-if)#switchport port-security mac-address sticky
```

Рисунок -12.20. Установка динамического определения безопасных MAC-адресов.

5. Настройте действия в случае нарушения ограничений на портах Fa0/1 SW1 и Fa0/1 SW2.

```
Switch(config-if)#
Switch(config-if)#switchport port-security violation shutdown
```

Рисунок - 12.21. Настройка действий при нарушении ограничений.

Shutdown (Выключение) — нарушение безопасности приводит к тому, что интерфейс переходит в состояние error-disabled (ошибка — отключён), и он немедленно отключается, а индикатор порта выключается. Если порт находится в состоянии error-disabled, его можно вывести из этого состояния, введя команду `errdisable recovery cause psecure-violation` или включив интерфейс в режиме конфигурации с помощью команд `shutdown` и `no shutdown`. Это стандартный режим.

6. Покажите действия в случае нарушения настроек на портах Fa0/2 на SW1 и Fa0/2 на SW2.

```
Switch(config-if)#switchport port-security violation restrict
Switch(config-if)#
```

Рисунок - 12.22. Настройка действий в случае нарушения ограничений.

Restrict (Ограничение) — когда количество безопасных MAC-адресов на порту достигает установленного максимального лимита, пакеты с неизвестным источником MAC-адреса удаляются, пока количество безопасных MAC-адресов не упадет ниже максимального числа или пока не увеличится количество разрешенных адресов. В этом режиме при нарушении безопасности отправляется предупреждение — SNMP trap, сообщение в syslog, и увеличивается счетчик нарушений (violation counter

7. Покажите действия при нарушении настроек на портах Fa0/3 SW1 и Fa0/3 SW2.

```
Switch(config-if)#
Switch(config-if)#switchport port-security violation protect
Switch(config-if)#
```

Рисунок - 12.23. Настройка действий при нарушении ограничений.

Вот перевод:

Protect (Защита) — когда количество безопасных MAC-адресов на порту достигает установленного максимума, пакеты с неизвестными MAC-адресами будут отбрасываться до тех пор, пока количество безопасных MAC-адресов не станет меньше максимального количества или разрешенные адреса не увеличатся до максимума. О нарушении безопасности предупреждений не будет.

8. Проверьте результат.

```
Switch#show port-security
Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action
               (Count)       (Count)        (Count)
-------------------------------------------------------------------
       Fa0/1        1             1                0         Shutdown
       Fa0/2        1             1                0          Protect
       Fa0/3        1             1                2         Restrict
-------------------------------------------------------------------
```

Рисунок - 12.24. Результат выполнения команды show port-security.

На основе рисунка 12.24 можно увидеть состояние портов. Fa0/1 — shutdown (выключение), Fa0/2 — protect (защита), Fa0/3 — restrict (ограничение). Столбец Security Violation отображает счетчик нарушений. Значение в этом столбце равно 2, что означает, что было зафиксировано 2 попытки подключения с использованием небезопасного MAC-адреса.

В результате практической работы была рассмотрена функция безопасности портов коммутатора, которая позволяет устанавливать MAC-адреса разрешенных хостов для защиты от атак, направленных на передачу данных через порт и заполнение таблицы коммутации сети.

Варианты заданий по работе:

Задание 1. Изучение функции безопасности портов коммутатора. Спроектируйте локальную сеть в соответствии с требованиями задания.

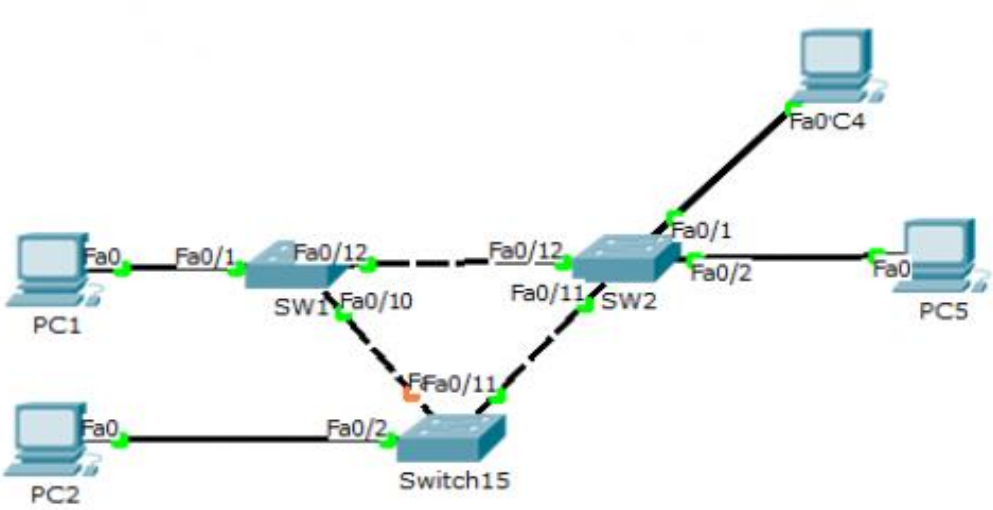


Рисунок - 12.25. Торология сети.

Qurilma	IP manzil	Tarmoqosti maska	Interfeys	Rejimlar (holatlar)
PC1	192.168.0.66	255.255.255.128	Fa0	n/a
PC2	192.168.0.67	255.255.255.128	Fa0	n/a
PC3	192.168.0.68	255.255.255.128	Fa0	n/a
PC4	192.168.0.69	255.255.255.128	Fa0	n/a
SW1	N/A	N/A	Fa0/1	Protect
SW2	N/A	N/A	Fa0/1	Shutdown
SW3	N/A	N/A	Fa0/2	Restrict
Switch15	N/A	N/A	Fa0/2	Shutdown

12.3-таблица. Таблица адресов.

1. Настройте порты Fa0/1 и Fa0/2 на всех коммутаторах в режим доступа (access).

2. Активируйте безопасность портов на всех портах коммутаторов в направлении к устройствам.

3. Установите максимальное значение secure-mac равным двум на всех портах.

4. Настройте динамическое определение secure-mac.

5. Покажите действия, которые должны быть предприняты в случае нарушения настроек на портах согласно таблице 13.25.

6. Проверьте результат. Показать результаты работы преподавателю и обосновать их.

Контрольные вопросы:

1. Что такое безопасность портов?
2. Как устанавливается количество безопасных MAC-адресов?
3. Какую команду использовать для настройки действий при нарушении ограничений?
4. Какой результат выводится при использовании команды `show port-security`?
5. Какова основная цель функции безопасности портов коммутатора?

Список сокращений

- CISO (Chief Information Security Officer) — Главный директор по информационной безопасности
- SOC (Security Operations Center) — Центр операций безопасности
- SIEM (Security Information and Event Management) — Управление информацией и событиями безопасности
- IDS (Intrusion Detection System) — Система обнаружения вторжений
- IPS (Intrusion Prevention System) — Система предотвращения вторжений
- DLP (Data Loss Prevention) — Предотвращение потери данных
- APT (Advanced Persistent Threat) — Продвинутая постоянная угроза
- MFA (Multi-Factor Authentication) — Многофакторная аутентификация
- SSL (Secure Sockets Layer) — Уровень защищённых сокетов
- TLS (Transport Layer Security) — Безопасность транспортного уровня
- PKI (Public Key Infrastructure) — Инфраструктура открытых ключей
- WAF (Web Application Firewall) — Межсетевой экран веб-приложений
- IAM (Identity and Access Management) — Управление идентификацией и доступом
- UEBA (User and Entity Behavior Analytics) — Аналитика поведения пользователей и объектов
- DoS (Denial of Service) — Отказ в обслуживании
- DDoS (Distributed Denial of Service) — Распределённый отказ в обслуживании
- LAN (Local Area Network) — Локальная сеть
- WAN (Wide Area Network) — Глобальная сеть
- MAN (Metropolitan Area Network) — Сеть городского масштаба
- VPN (Virtual Private Network) — Виртуальная частная сеть
- IP (Internet Protocol) — Интернет-протокол
- TCP (Transmission Control Protocol) — Протокол управления передачей
- UDP (User Datagram Protocol) — Протокол пользовательских дейтаграмм
- DNS (Domain Name System) — Система доменных имен
- DHCP (Dynamic Host Configuration Protocol) — Протокол динамической конфигурации хоста
- HTTP (Hypertext Transfer Protocol) — Протокол передачи гипертекста
- HTTPS (Hypertext Transfer Protocol Secure) — Защищённый протокол передачи гипертекста
- FTP (File Transfer Protocol) — Протокол передачи файлов
- NAT (Network Address Translation) — Преобразование сетевых адресов
- QoS (Quality of Service) — Качество обслуживания
- PoE (Power over Ethernet) — Питание через Ethernet
- MAC (Media Access Control) — Управление доступом к среде
- SSID (Service Set Identifier) — Идентификатор набора услуг
- ARP (Address Resolution Protocol) — Протокол разрешения адресов
- ICMP (Internet Control Message Protocol) — Протокол управления сообщениями в Интернете
- OSPF (Open Shortest Path First) — Протокол открытого кратчайшего пути

- IDE (Integrated Development Environment) — Интегрированная среда разработки
- API (Application Programming Interface) — Интерфейс программирования приложений
- SDK (Software Development Kit) — Набор инструментов для разработки программного обеспечения
- GUI (Graphical User Interface) — Графический пользовательский интерфейс
- CLI (Command Line Interface) — Интерфейс командной строки
- OOP (Object-Oriented Programming) — Объектно-ориентированное программирование
- FP (Functional Programming) — Функциональное программирование
- JVM (Java Virtual Machine) — Виртуальная машина Java
- JRE (Java Runtime Environment) — Среда выполнения Java
- JDK (Java Development Kit) — Набор инструментов для разработки на Java
- REPL (Read-Eval-Print Loop) — Цикл чтения-оценки-вывода
- MVC (Model-View-Controller) — Модель-представление-контроллер
- DBMS (Database Management System) — Система управления базами данных
- SQL (Structured Query Language) — Структурированный язык запросов
- ORM (Object-Relational Mapping) — Объектно-реляционное отображение
- CRUD (Create, Read, Update, Delete) — Создание, чтение, обновление, удаление
- VCS (Version Control System) — Система контроля версий
- Git (Global Information Tracker) — Глобальный отслеживатель информации
- SVN (Subversion) — Система управления версиями Subversion
- HTML (Hypertext Markup Language) — Язык разметки гипертекста
- CSS (Cascading Style Sheets) — Каскадные таблицы стилей
- JS (JavaScript) — JavaScript
- AJAX (Asynchronous JavaScript and XML) — Асинхронный JavaScript и XML
- DOM (Document Object Model) — Объектная модель документа
- SSH (Secure Shell) — Защищённая оболочка
- HTTP (Hypertext Transfer Protocol) — Протокол передачи гипертекста
- HTTPS (Hypertext Transfer Protocol Secure) — Защищённый протокол передачи гипертекста
- REST (Representational State Transfer) — Передача состояния представления
- SOAP (Simple Object Access Protocol) — Простой протокол доступа к объектам
- TDD (Test-Driven Development) — Разработка через тестирование
- BDD (Behavior-Driven Development) — Разработка через поведение
- CI (Continuous Integration) — Непрерывная интеграция
- CD (Continuous Deployment/Delivery) — Непрерывное развертывание/доставка
- XML (eXtensible Markup Language) — Расширяемый язык разметки
- JSON (JavaScript Object Notation) — Нотация объектов JavaScript
- VR (Virtual Reality) — Виртуальная реальность
- AR (Augmented Reality) — Дополненная реальность

- MR (Mixed Reality) — Смешанная реальность
- XR (Extended Reality) — Расширенная реальность (обобщённое понятие для VR, AR и MR)
- HMD (Head-Mounted Display) — На головное устройство отображения
- 3DOF (Three Degrees of Freedom) — Три степени свободы (только отслеживание движения головы: поворот, наклон, качание)
- 6DOF (Six Degrees of Freedom) — Шесть степеней свободы (отслеживание движений головы и тела: поворот, наклон, качание, вперёд-назад, влево-вправо, вверх-вниз)
- FOV (Field of View) — Поле зрения
- HUD (Heads-Up Display) — Проекционный дисплей
- VPS (Visual Positioning System) — Система визуального позиционирования
- LIDAR (Light Detection and Ranging) — Лазерное обнаружение и определение дальности
- SLAM (Simultaneous Localization and Mapping) — Одновременная локализация и построение карты
- IMU (Inertial Measurement Unit) — Инерциальный измерительный блок
- DoF (Degrees of Freedom) — Степени свободы
- SDK (Software Development Kit) — Набор инструментов для разработки программного обеспечения (часто используется в контексте VR и AR)
- CV (Computer Vision) — Компьютерное зрение
- ML (Machine Learning) — Машинное обучение
- AI (Artificial Intelligence) — Искусственный интеллект
- MoCap (Motion Capture) — Захват движений
- VPL (Virtual Programming Language) — Виртуальный язык программирования.

ЗАКЛЮЧЕНИЕ

Данное учебное пособие «Основы информационных технологий и информационной безопасности» является глубоким источником знаний по широкому спектру тем, связанных с информационными технологиями и безопасностью в органах правопорядка. Пособие содержит ценные и практически ориентированные материалы, которые помогают курсантам и специалистам эффективно усваивать основные понятия и навыки в области сетевых технологий, изучая сетевые кабели, Cisco Packet Tracer, LAN, VLAN, VPN и проектирование облачных сетей.

Учебное пособие позволяет курсантам полностью понять принципы и методы установки сетевых кабелей, что является основным элементом для создания надежной и эффективной сетевой инфраструктуры. Тренинги с использованием Cisco Packet Tracer предоставляют уникальный практический опыт в моделировании и настройке сетей, что позволяет курсантам изучать основные принципы работы сетевого оборудования.

Проектирование LAN, VLAN, VPN и облачных сетей является важной частью учебного процесса, поскольку оно помогает понять принципы организации сетевых структур различного уровня сложности. Эта часть учебника дает учащимся полное представление о проектировании и реализации современной сетевой архитектуры с учетом безопасности и эффективности.

Кроме того, учебное пособие обучает использованию технологии PoE и DHCP-серверов, которые являются важными элементами современной сетевой инфраструктуры. Развитие IoT-сетей на основе современных сенсоров становится все более актуальным и перспективным направлением в области правопорядка.

В целом, учебное пособие «Основы информационных технологий и информационной безопасности» является бесценным ресурсом для всех, кто интересуется сетями и безопасностью в области правопорядка и стремится к профессиональному росту в этой сфере. Раздел, посвященный сетевым технологиям, предоставляет учащимся все необходимые инструменты и знания для успешного развития и применения современных сетевых технологий в области правопорядка.

СПИСОК ЛИТЕРАТУРЫ

1. Matt Oswalt, Christian Adell, Scott S. Lowe, and Jason Edelman. Network Programmability and Automation Skills for the Next-Generation Network Engineer. O'Reilly Media, Inc., CA. – 2023. 828 p.

2. Simone Onofri, Donato Onofri. Attacking and Exploiting Modern Web Applications. Packt Publishing Ltd. Birmingham, UK. August 2023. – 338 p.

3. Левашов Петр. Киберкрепость: всестороннее руководство по компьютерной безопасности. - СПб.: Питер, 2024. - 544 с.

4. Austin R. Benson, Rediet Abebe, Michael T. Schaub, Ali Jadbabaie, and Jon Kleinberg. Simplicial closure and higher-order link prediction. ArXiv Preprint ArXiv:1802.06916, 2018.

5. Christopher Cowell, Nicholas Lotz, Chris Timberlake. Automating DevOps with GitLab CI/CD Pipelines. Packt Publishing Ltd. Birmingham, UK. 2023. -348 p.

6. Ashish Mishra. Cloud security handbook for architects. Orange Education Pvt Ltd, Delhi, India. 2023. -394 p.

7. Chen Chen, Ruiyue Peng, Lei Ying, and Hanghang Tong. Network connectivity optimization: Fundamental limits and effective algorithms. Proc. of the 24th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, pages 1167–1176, 2018.

8. Marshall Copeland, Matthew Jacobs. Cyber Security on Azure: An IT Professional’s Guide to Microsoft Azure Security. Apress Berkeley, CA. – 2021. - 285p.

9. Управление информационной безопасностью: учебное пособие / Е. Н. Чекулаева, Е. С. Кубашева. – Йошкар-Ола: Поволжский государственный технологический университет, 2020. – 154 с.

10. Jacob G. Oakley. Professional Red Teaming: Conducting Successful Cybersecurity Engagements. Apress Berkeley, CA. – 2019. -215p.

11. Ajay Singh Chauhan. Practical Network Scanning. Packt Publishing Ltd. Birmingham, UK. 2023. -348 p.

12. Aleksandar Bojchevski and Stephan Günnemann. Adversarial attacks on node embeddings via graph poisoning. International Conference on Machine Learning, pages 695–704, PMLR, 2019.

13. Stephen Bonner, John Brennan, Ibad Kureshi, Georgios Theodoropoulos, Andrew Stephen McGough, and Boguslaw Obara. Temporal graph offset reconstruction: Towards temporally robust graph representation learning. IEEE International Conference on Big Data (Big Data), pages 3737–3746, 2018.

14. Andrew S. Tanenbaum, David J. Wetherall. Computer Networks 5th Edition. Pearson Education India. India. 2013. – 809 p.

15. Daniel Zügner, Amir Akbarnejad, and Stephan Günnemann. Adversarial attacks on neural networks for graph data. Proc. of the 24th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, pages 2847–2856, 2018.

16. José Manuel Ortega. Python for Security and Networking Third Edition. Packt Publishing. Birmingham, UK. 2023. -587 p.

17. Безопасность веб-приложений: лучшие практики и уязвимости. Октября 2023. URL: https://itproger.com/news/bezopasnost-veb-prilozheniy-luchshie-praktiki-i-uyazvimosti.

18. В. Олифер, Н. Олифер. Компьютерные сети. Принципы, технологии, протоколы. Учебник для ВУЗов. - СПб.: Питер, 2016. -992 с.

19. Э. Таненбаум, Д. Уэзеролл. Компьютерные сети. 5-е изд. — СПб.: Питер, 2012. - 960 с.

20. CISCO: ‘‘Cisco Visual Networking Index: Forecast and Methodology, 2009–2014,’’ Cisco Systems Inc., June 2010.

21. Harper A., Harris S., Ness J., Eagle C. et al. Gray Hat Hacking: The Ethical Hacker’s Handbook. - McGraw Hill, 2018.

22. Stuttard D., Burnett M. The Web Application Hacker’s Handbook: Discovering and Exploiting Security Flaws. - Spring, 2019.

23. Stamp M. Computer Security and Cryptography. - Wiley, 2021.

24. Stanislav M. Networks and Network Security.

25. Goodrich M. T., Tamassia R. Introduction to Computer Security. - Pearson, 2010.

26. Д.П. Зегжда, Е.Б. Александрова и др. Кибербезопасность цифровой индустрии. Теория и практика функциональной устойчивости к кибератакам. М.: Горячая линия – Телеком, 2020. -560 с.

27. Scardapane S. et al. Microphone array based classification for security monitoring in unstructured environments // AEU - International Journal of Electronics and Communications. -2015, -Vol. 68. –№ 11. -P. 1715-1723.

28. Mohapatra S. K., Sahoo P. K., Wu S-L. Big data analytic architecture for intruder detection in heterogeneous wireless sensor networks // Journal of Network and Computer Applications. -2016. - Vol. 66. – P. 236-249.

29. Das S. K., Kant K., Zhang N. Handbook on Securing Cyber-Physical Critical Infrastructure. - Morgan Kaufmann, 2012.

30. Heartin Kanikathottu. AWS Security Cookbook. Packt Publishing Ltd. Birmingham, UK. 2020. -434p.

ОГЛАВЛЕНИЕ