Ордена Трудового Красного Знамени федеральное государственное
бюджетное образовательное учреждение высшего образования
Московский технический университет связи и информатики

Факультет «Сети и системы связи»
Кафедра «Сети связи и системы коммутации»

Сборник практических и лабораторных работ
по специальному курсу

«Технологии связи»

для учащихся 10 класса

Е.Е. Маликова, М.Г. Канищева

Москва 2021

В сборнике изложены основы работы с сетевым симулятором компании Cisco, приведены лабораторные работы и практические задания, позволяющие практически ознакомиться с настройкой сетевого оборудования с использованием Cisco Packet Tracer. Подробно изложена последовательность выполнения работ, сопровождающаяся пояснениями и иллюстрациями.

Для выполнения работ на компьютере обучающихся должны быть установлены сетевой эмулятор Cisco Packet Tracer и операционная система Microsoft Windows.

Оглавление

ВВЕДЕНИЕ

В настоящее время системы связи достигли высокого уровня развития, это требует от персонала, занимающегося их обслуживанием, соответствующих знаний и практических навыков. Уже на стадии обучения в средней школе необходимо практически осваивать работу с современными технологиями. Представленный сборник практических и лабораторных работ позволяет обучающимся в интерактивной форме усвоить целый ряд современных сетевых технологий. В пособии на примере построения простейшей компьютерной сети рассматривается процесс работы с сетевым симулятором Cisco Packet Tracer. Показана последовательность создания топологии сети, работы в командной строке сетевого оборудования и просмотра осуществленных настроек.

Cisco Packet Tracer - это эмулятор сети, созданный компанией Cisco.

Данное приложение позволяет строить сети на разнообразном оборудовании в произвольных топологиях с поддержкой различных протоколов.

Программное решение Cisco Packet Tracer позволяет имитировать работу различных сетевых устройств: маршрутизаторов, коммутаторов, точек беспроводного доступа, персональных компьютеров, IP-телефонов и т.д. Работа с интерактивным симулятором дает ощущение настройки реальной сети, состоящей из десятков или даже сотен устройств.

Настройки, в свою очередь, зависят от характера устройств: одни можно настроить с помощью команд операционной системы Cisco IOS, другие – за счет графического веб-интерфейса, третьи – через командную строку операционной системы или графические меню.

Благодаря такому свойству Cisco Packet Tracer, как режим визуализации, пользователь может отследить перемещение данных по сети, появление и изменение параметров IP-пакетов при прохождении данных через сетевые устройства, скорость и пути перемещения IP-пакетов.

Для настройки сетевого оборудования имеются разнообразные команды операционной системы Cisco IOS.

Все лабораторные работы и практические задания сопровождаются краткими теоретическими сведениями, дающими возможность подготовиться к их выполнению и понять основы рассматриваемой технологии, а также контрольными вопросами для самопроверки и подготовки к защите.

Практическая работа №1. Технология маршрутизации в IP-сетях

Цель работы

Изучить принципы маршрутизации в сети Интернет и структуру IP-адреса устройств сети.

Задание

1. Ознакомиться с классовой моделью IP-адресации;
2. Изучить принципы формирование подсетей с помощью масок подсети;
3. Выполнить тест.

Краткая теория

Прежде чем разобраться, как происходит маршрутизация в сети Интернет необходимо выяснить, как формируется сетевой адрес каждого устройства в данной сети. Прежде всего, этот адрес должен быть уникальным, т.е. однозначно определять любое устройство в сети Интернет. Сетевой адрес абонента сети IP (IP-адрес) версии 4 (IPv4) состоит их 32 бит. Маршрутизация пакетов в сетях передачи данных возможна благодаря тому, что IPv4-адрес структурирован и состоит из двух логических частей: идентификатора сети (NetID – Network Identification) и идентификатора узла (HostID – Host Identification), который однозначно определяет устройство в сетевом сегменте.

Хронологически первым методом разделения IP- адресов является так называемая ***классовая модель*** IP- адресации. Согласно этой модели, все пространство IP- адресов делится на пять классов в зависимости от значения первых четырех бит адреса IPv4.

Первые три класса **A, B** и **C** используются для индивидуальной (unicast) адресации сетей и узлов, класс **D** - для многоадресной или групповой рассылки (multicast), а класс **E** зарезервирован для экспериментов. Классы **A, B**, и **C** имеют различную длину сетевой части и адреса узла (рис. 1). Рассмотрим эти классы более подробно.

Класс A идентифицируется первым битом сетевого адреса, который всегда равен 0. Адрес оконечного устройства, принадлежащего к классу **A**, всегда начинается с цифры 0. Количество сетей в классе **A** составит: $2^7 - 2 = 126$, так как адреса 0.0.0.0 и 127.0.0.0 зарезервированы и не могут быть использованы в качестве сетевых адресов. Любые адреса, которые начинаются с числа в диапазоне от 1 до 126 в первом байте, являются адресами класса **A**.

В классе A количество возможных оконечных устройств в сети задается 24 битами. Тогда число оконечных устройств в сети равно: $2^{24} - 2 = 16777214$. Вычитание цифры 2 в этих вычислениях определяется тем, что адрес, в которых все биты равны 1 является широковещательным адресом, а адрес, в котором все биты равны 0, является адресом сети.

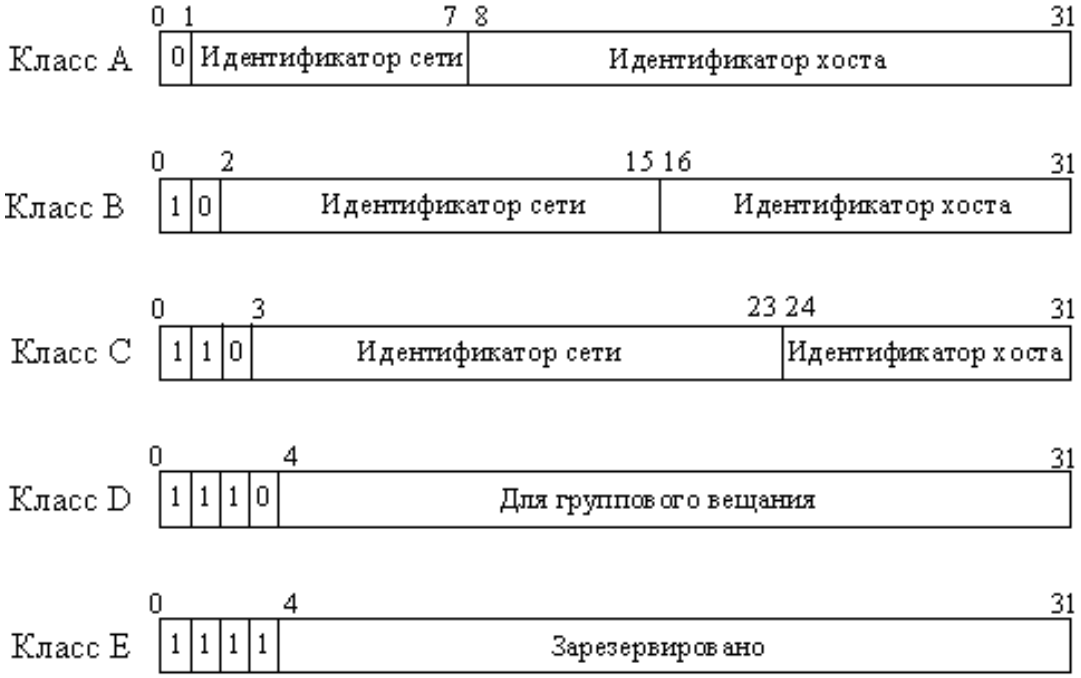


Рисунок 1 - Классы IP-адресов формата IPv4

Класс B идентифицируется 2-мя первыми битами равными 10. Тогда, наименьшее число, которое используется для адресов в этом классе равно 10000000 (десятичное 128), а наибольшее - 10111111 (десятичное 191). Первые два байта используются для идентификатор сети, а оставшиеся два байта для идентификатора узла, т.е. в классе **B** количество сетей равно $2^{14} = 16384$, а количество оконечных устройств будет соответственно равно $2^{16} - 2 = 65534$.

Класс C определяется первыми 3-мя битами, равными 110. Таким образом, наименьшее доступное число - 11000000 (десятичное 192), а наибольшее - 11011111 (десятичное 223). Адреса сетей класса **C** задаются 21 битом и только 8 битов определяют адреса оконечных устройств. Тогда количество сетей равно $2^{21} = 2\ 097\ 152$, в каждой из которых находится $2^8 - 2 = 254$ узла.

Класс D идентифицируется 4-мя битами первого байта адреса, равными 1110. Остальные биты используются для адресации многоадресной группы. Адресное пространство класса **D** зарезервировано для групповой рассылки. Идентификаторов сетей и узлов в классе **D** не выделяется. Первый октет адресов этого класса может принимать значения от 11100000 до 11101111 или, в десятичном виде от 224 до 239.

Класс E является экспериментальным и в настоящее время не используется для адресации в сети Internet. Первые четыре бита адреса класса **E** всегда равны 1111. Следовательно, значение первого октета находится в диапазоне от 11110000 до 11111111 или от 240 до 255 - в десятичном виде.

В таблице 1 приведены диапазоны значений первого байта IP- адреса для сетей всех классов.

Таблица 1 - Диапазоны значений первого байта в IP- адресах для сетей всех классов

Класс IP- адреса	**Диапазон IP-адресов**
Класс A/0	От 1 до 126 (от 00000001 до 01111111)
Класс B/10	От 128 до 191 (от 10000000 до 10111111)
Класс C/110	От 192 до 223 (от 11000000 до 11011111)
Класс D/1110	От 224 до 239 (11100000 до 11101111)
Класс E/1111	От 240 до 255 (от 111110000 до 11111111)

Диапазон адресов 127.x.x.x зарезервирован в качестве так называемого петлевого (loopback) адреса, который используется для тестирования и диагностики.

Формирование подсетей

Для более эффективного использования адресного пространства были внесены изменения в существующую классовую систему адресации. В рекомендации RFC 950 IETF была описана процедура разбиения сети на подсети, и в структуру IPv4 адреса был добавлен еще один уровень - подсеть (subnetwork). Появление еще одного уровня иерархии не изменило самого адреса IPv4, он остался 32-разрядным, а часть адреса, отведенная ранее под идентификатор узла, была разделена на две части: идентификатор подсети и идентификатор узла (рис. 2).

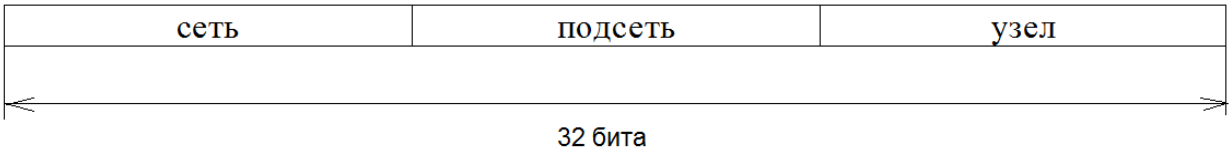


Рисунок 2 - Трехуровневая иерархия IPv4- адреса

С появлением трех уровневой иерархии IPv4-адреса потребовались дополнительные методы, которые помогли бы определить, какая часть IPv4-адреса указывает на идентификацию подсети, а какая – на идентификацию узла. Было предложено использовать битовую маску (bit mask), которая отделяет часть адресного пространства идентификатора сети (Net ID) от адресного пространства идентификатора узлов (Host ID). Такая битовая маска называется ***маской подсети (subnet mask).*** Маска подсети – это 32-х битное

число, двоичная запись которого содержит единицы в тех разрядах, которые должны определяться как идентификатор сети.

Для сетей классов A, B, C определены фиксированные маски подсети, которые жестко определяют количество возможных IPv4-адресов и механизм маршрутизации (табл. 2).

Таблица 2 - Маски подсети для стандартных классов сетей.

Класс сети	Маска подсети	Количество бит идентификатора
A	255.0.0.0	8
B	255.255.0.0	16
C	255.255.255.0	24

Чтобы получить адрес сети, зная IPv4 адрес и маску подсети, необходимо применить к ним операцию логического «И» (рис. 1.3).

IP адрес	11000000	10101000	00000001	00000010	192.168.1.2.
Маска	11111111	11111111	11111111	00000000	255.255.255.0
адрес	11000000	10101000	00000001	00000000	192.168.1.0

Рисунок 3 - Получение адреса сети из IPv4- адреса и маски подсети

В тех позициях IPv4- адреса, в которых в маске подсети стоят двоичные единицы, находится идентификатор сети, а где двоичные 0 - идентификатор узла. При применении масок подсети сети можно разделить на меньшие по адресу подсети путем расширения Net ID и уменьшения Host ID. Это дает возможность создавать большее число сетей с меньшим количеством узлов в них.

Тест к разделу «Технология маршрутизации в IP-сетях»

1. Укажите длину адреса IPv4?
+ 32 бита;
-128 бит;
-64 бита;
- 32 байта.

2. Выберите маску подсети для сети класса А?
- 255.255.255.0;
-255.255.0.0;
+255.0.0.0;
- 255.255.255.255.

3. К какому классу относится следующий IP-адрес 192.168.2.1?
- класс А;
- класс В;
+ класс С;
- класс D.

4. Какое максимальное количество узлов может быть в сети класса С?
+254;
-128;
- 65534;
- 1024.

5. Задан IP-адрес устройства 36.1.3.2. Определите адрес сети.
- 36.1.3.0;
-36.1.0.0;
+36.0.0.0;
-36.1.3.2.

6. Задан IP-адрес устройства 196.168.10.2. Определите адрес сети, в которой находится данное устройство.
- 196.168.10.2;
+196.168.10.0;
- 196.168.0.0;
- 196.0.0.0.

7. Укажите диапазон IP-адресов для сетей класса В?
- 1 - 126;
+128 - 191;
- 192 – 223;
- 240 -255.

8. Переведите в десятичную систему IP- адрес, представленный в двоичном формате 11000000 00000110 00001111 10000011.

- 176.8.15.3;
- 192.5.17.2;
+192.6.15.3;
- 170.5.8.1.

9. Переведите в двоичную форму IP- адрес, представленный в десятичном формате 192.168.2.1
+11000000 10100100 00000010 00000001
- 00000011 00100101 01000000 00000001
- 11001100 00111000 11000000 10100000
- 00001111 11110000 11100000 00111000

10. Какая из перечисленных цифровых последовательностей не является IP-адресом?
- 176.12.3.4;
+ 256.2.1.1;
- 196.14.20.1
- 209.11.33.11.

Практическая работа №2. Изучение модели взаимодействия открытых систем

Цель работы

Изучить семиуровневую модель взаимодействия открытых систем.

Задание

1. Ознакомиться с моделью взаимодействия открытых систем (OSI) ;
2. Ознакомиться с моделью TCP/IP;
3. Ответить на вопросы.

В вычислительных сетях основными элементами являются стандартные компьютеры, каждый из которых работает под управлением собственной операционной системы. При этом каждый компьютер может пользоваться ресурсами других компьютеров, подключенных к сети. Для этого в компьютерах устанавливаются сетевые адаптеры, соединенные кабельной системой и вводятся некоторые добавления к операционным системам компьютеров. Компьютер, ресурсы которого должны быть доступны всем пользователям, имеет модуль, постоянно находящийся в режиме ожидания запросов – сервер (его главная задача – обслуживать (server) запросы на доступ к ресурсам). На компьютерах, которые хотят получить доступ к этим общим ресурсам, к операционной системе добавляется модули для выработки запросов – клиенты. Возникает сетевая операционная система, поддерживающая несколько видов служб для пользователей: файловую службу, службу печати, службу электронной почты, службу удаленного доступа и т.д.

Основной проблемой сетей передачи данных (СПД) являлась проблема совместимости. Первоначально различные организации (банки, железные дороги, авиаперевозчики) создавали свои частные сети передачи данных, охватывающие большие территории, со специфическими операционными системами, то есть с ведомственными стандартами. В результате чего сети этих организаций могли передавать данные только между компьютерами, поставленными определенными производителями.

Но по мере того как возникала потребность связи между компьютерами, принадлежащим различным организациям (банки, авиаперевозки), ведомства связи разных стран приходили к мысли о создании сетей передачи данных общего пользования - СПДОП (PDN - Public Digital Network). После долгих обсуждений сначала на национальных уровнях, а затем и на международном уровнях была разработана семиуровневая модель взаимодействия открытых систем –(Open System Interconnection – OSI). Ее разработала все-

мирной организацией по стандартизации ISO (International Organization Standardization) в начале 80-х годов прошлого века (рис. 1).

Организация ISO основывалась на многоуровневом подходе, используемом при описании сложных систем. При этом все множество модулей разбивается на уровни, образующие некоторую иерархию. Формализованные правила, определяющие последовательность и форматы сообщений, которыми обмениваются сетевые компоненты разных узлов, лежащие на одном уровне, называются *протоколами.* Соседние уровни, находящиеся в одном узле взаимодействуют с помощью четко определенных правил, обмениваясь стандартными сообщениями. Это взаимодействие соседних уровней определяется *интерфейсом.*

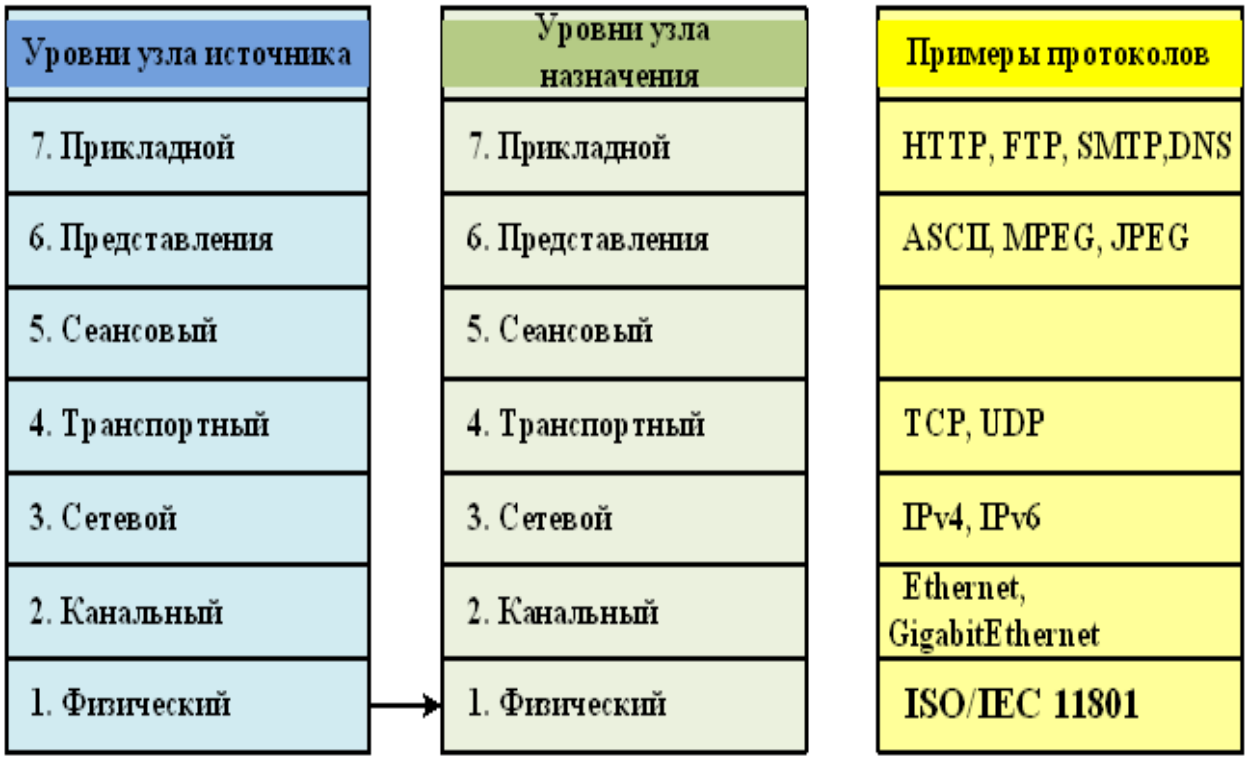


Рисунок 1 - Семиуровневая модель OSI

7 уровень - прикладной обеспечивает управление взаимодействием прикладных процессов, возникающих при взаимодействии компьютеров (рис.2).

Процессы эти могут быть различными: обращение к поисковой системе, передача данных с одного компьютера на другой, обращение к счету через банкомат. На этом уровне эти процессы формализуются пользователем в определенные команды.

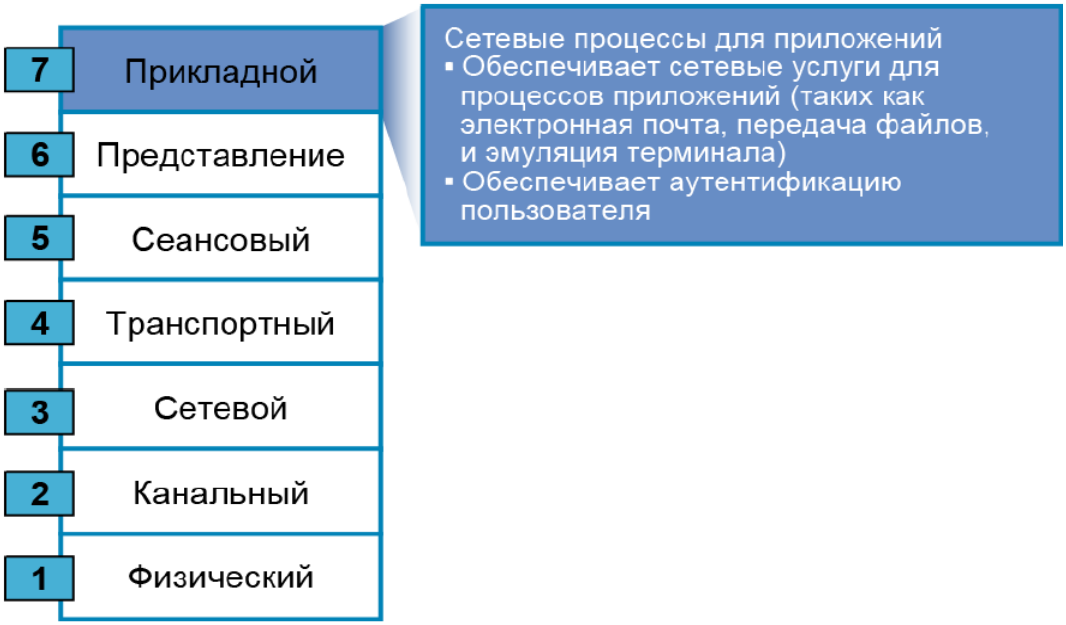


Рисунок 2 – Прикладной уровень модели OSI

6 уровень - уровень представления производит перекодировку сообщения, которое поступило с 7-го уровня (рис.3). Модель OSI называется *открытой* (Open), так как не накладывает ограничений на типы применяемых компьютеров, которые, как правило, используют различные коды для представления информации, поэтому на этом уровне осуществляется пересчет данных в единое кодовое представление, принятое в сети связи. На этом же уровне также может выполняться шифрование и дешифрование данных, обеспечивающее секретность обмена данными для всех прикладных служб.

Рисунок 3 –Уровень представления модели OSI

5 уровень - сеансовый, предназначенный для открытия сеанса связи между удаленными процессами пользователя (рис. 4). Он управляет диалогом, фиксирует, какая из сторон является активной в настоящий момент, предоставляет средства синхронизации. Протокол пятого уровня – сеансовый протокол на практике используется немногими приложениями, он редко реализуется в виде отдельного протокола, его функции часто объединяются с функциями прикладного уровня.

Передача сообщений от сеансового уровня к транспортному осуществляется через некоторые точки доступа, называемые *портами* (П). Открытие сеанса связи предполагает занятие (открытие) некоторого порта исходящей связи. Номер этого порта приписывается сообщению. При входящей связи занимается порт входящей связи. То есть каждая пара взаимодействующих прикладных процессов в сети отмечается номерами исходящего и входящего портов.

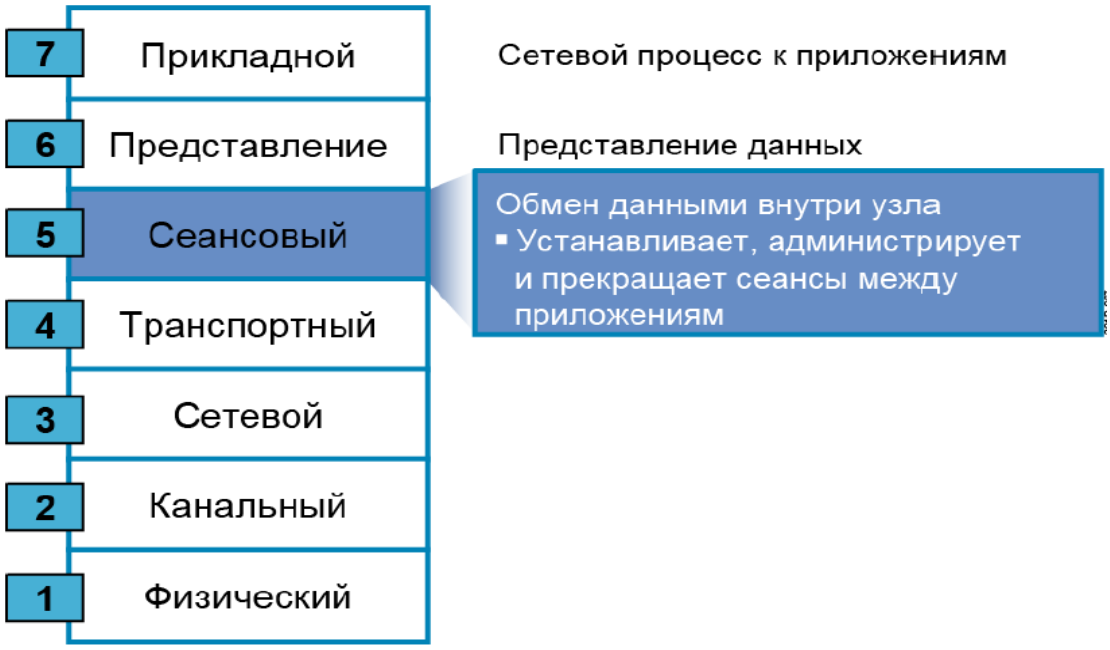


Рисунок 4 –Сеансовый уровень модели OSI

Как происходит взаимодействие на верхних трех уровнях, знают только разработчики конкретных приложений. Эти уровни часто представляют в виде одного уровня приложений. Сетевых инженеров обычно интересуют уровни, которые находятся ниже.

4 уровень - транспортный делит сообщение узла источника информации на части, при этом добавляет заголовок и формирует сегменты определенного объема (рис. 5). В узле назначения происходит обратный процесс. В заголовке сегмента задаются номера порта источника и назначения, кото-

рые адресуют службы верхнего уровня приложений для обработки данного сегмента. Также этот уровень обеспечивает надежную доставку пакетов. При обнаружении потерь и ошибок на этом уровне формируется запрос повторной передачи, при этом используется протокол TCP(Transmission Control Protocol). Когда необходимость проверки правильности доставленного сообщения отсутствует, то используется протокол дейтаграмм пользователя (User Datagram Protocol –UDP).

Рисунок 5 –Транспортный уровень модели OSI

3 уровень - сетевой задает пакету логические сетевые адреса узла назначения и узла источника (IP-адреса), определяет маршрут, по которому будет отправлен пакет данных, транслирует логические сетевые адреса в физические (MAC- адреса) и наоборот. Для этого в протоколах сетевого уровня применяются различные *алгоритмы маршрутизации*.

2 уровень – канальный, на котором пакеты, поступающие с третьего уровня, формируются по одному, или по несколько в *кадры* (frame) (Рис.6) . На этом уровне реализуются механизмы обнаружения и коррекции ошибок между двумя соседними узлами. На этом уровне задаются физические адреса устройства-отправителя и устройства-получателя данных (MAC-адреса).

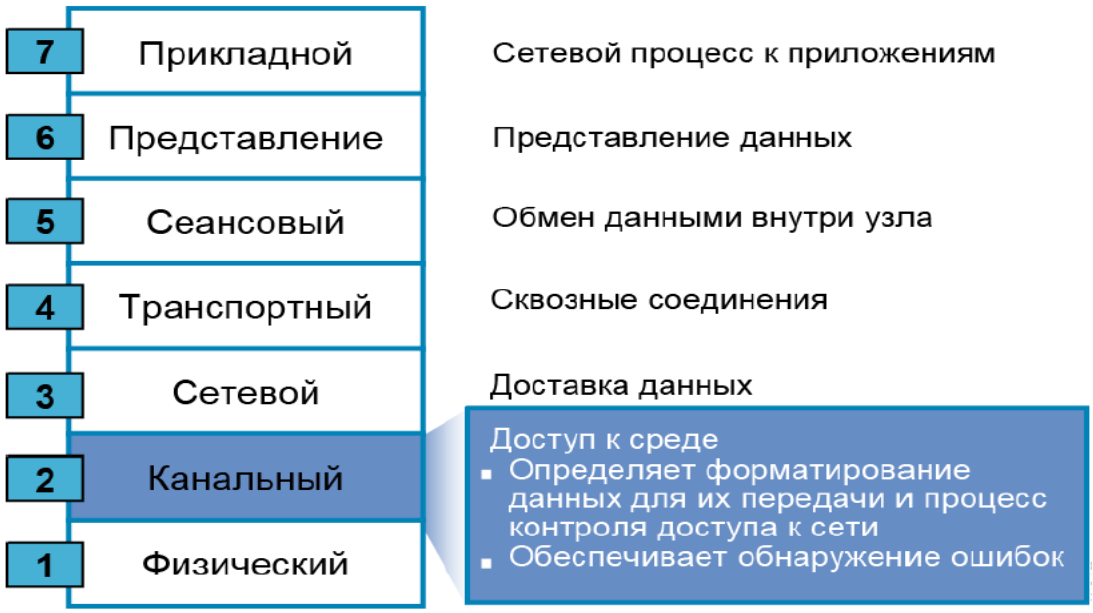


Рисунок 6 –Канальный уровень модели OSI

1 уровень - физический, на нем осуществляется побитовая передача кадров по линиям связи. На этом уровне определяются физические характеристики среды передачи. Единицей информации при обмене данными на физическом уровне является бит. На этом уровне производится кодирование данных, синхронизация передаваемых битов информации.

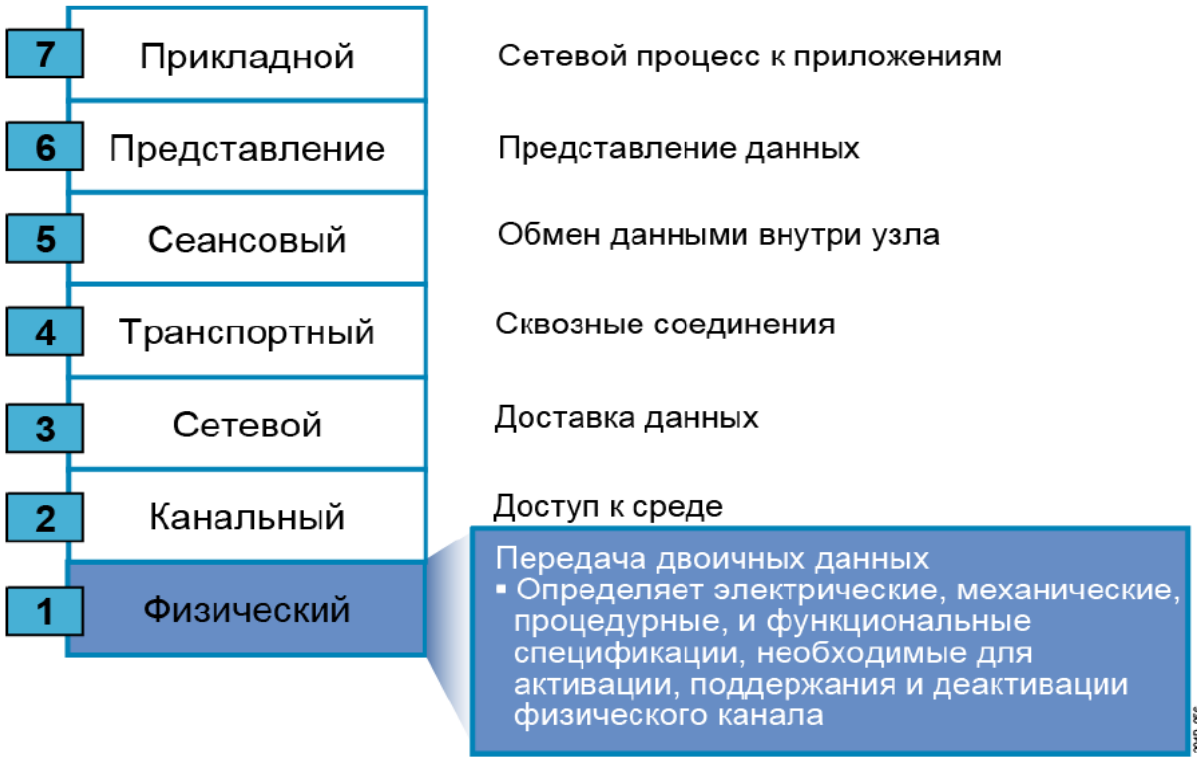


Рисунок 7 – Физический уровень модели OSI

Протоколы с 4- го по 7-й уровень называются *протоколами верхних уровней,* а протоколы уровней 1 – 3, соответственно, – *протоколами нижних уровней.*

Стандарты Ethernet определяют проводные соединения и электрические сигналы на физическом уровне, а также формат пакетов и протоколы управления доступом к среде на канальном уровне модели OSI. Когда говорят Ethernet, то под этим обычно понимают любой из вариантов этой технологии. В более узком смысле, Ethernet – это сетевой стандарт, основанный на технологиях экспериментальной сети Ethernet Network, которую фирма Xerox разработала и реализовала в 1975 году. В 1980 году фирмы DEC, Intel и Xerox совместно разработали и опубликовали стандарт Ethernet версии II. Поэтому стандарт Ethernet иногда называют стандартом DIX по заглавным буквам названий фирм.

Помимо семиуровневой OSI модели на практике применяется четырехуровневая модель TCP/IP. Рассмотрим более подробно эту модель (рис. 8).

Прикладной уровень модели TCP/IP по названию совпадает с названием модели OSI, но по функциям гораздо шире, поскольку охватывает три верхних уровня (Приложений, Представления и Сеансовый). **Транспортный** уровень обеих моделей и по названию, и по функциям одинаков. **Сетевой** (Network) уровень модели OSI соответствует межсетевому (**Internet**) уровню модели TCP/IP, а два нижних уровня (канальный и физический) представлены объединенным уровнем сетевого доступа (**Network Access**).

На транспортном уровне в заголовке сегмента задаются номера портов приложений источника и назначения. Протоколы транспортного уровня (TCP, UDP) взаимодействуют с определенными протоколами уровня приложений.

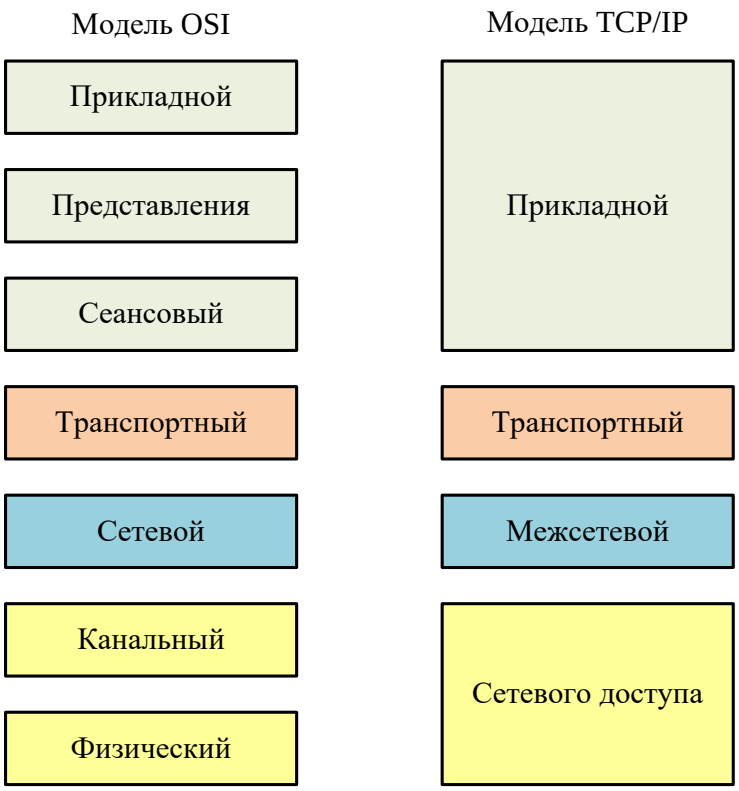


Рисунок 8 – Сравнение моделей OSI и TCP/IP

Контрольные вопросы

1. Какие уровни модели OSI вы знаете?
2. Какие уровни модели TCP/IP вы знаете?
3. Каковы основные функции Уровня 1 модели OSI?
4. Каковы основные функции Уровня 2 модели OSI?
5. Каковы основные функции Уровня 3 модели OSI?
6. Каковы основные функции Уровня 4 модели OSI?
7. Каковы основные функции Уровня 5 модели OSI?
8. Каковы основные функции Уровня 6 модели OSI?
9. Каковы основные функции Уровня 7 модели OSI?
10. На каком уровне модели OSI задаются IPадреса?
11. Какие устройства функционируют на уровне 3 модели OSI?
12. Какие устройства функционируют на уровне 2 модели OSI?
13. Какие устройства функционируют на уровне 1 модели OSI?
14. Какие уровни моделей OSI и TCP/IP одинаковы по функциям и по названию?

Практическая работа №3. Сетевая технология Ethernet

Эволюция локальных сетей неразрывно связана с развитием технологии Ethernet, которая по сей день остается самой распространенной технологией локальных сетей.

В первых сетях Ethernet (стандарты 10Base-2 и 10Base-5) использовалась физическая шинная топология, когда каждый ПК соединялся с другими ПК с помощью единого коаксиального кабеля, используемого в качестве среды передачи данных (рисунок 1).

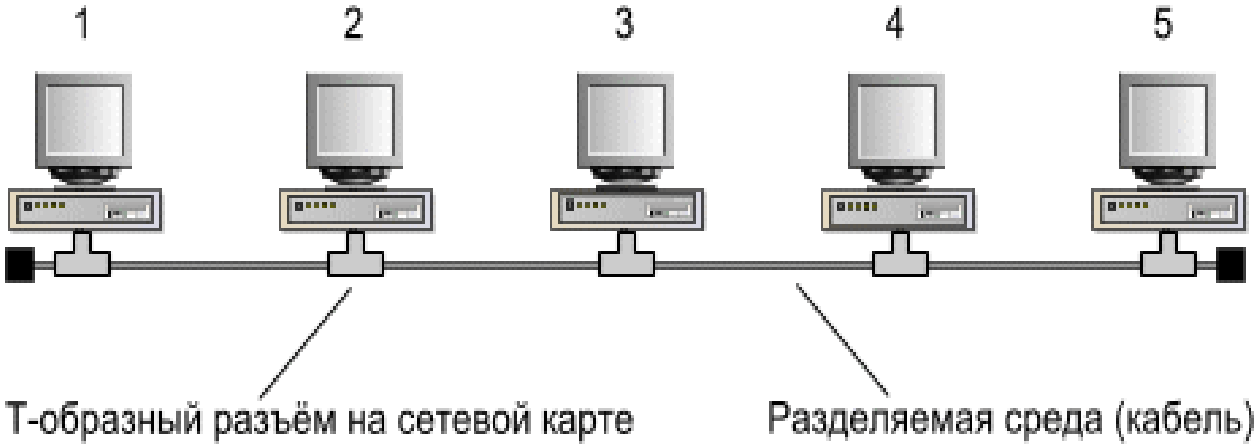


Рисунок 1 – Соединение ПК между собой с помощью коаксиального кабеля

Этот метод связи компьютеров впервые был опробован при создании радиосети ALOHA Гавайского университета в начале 70-х годов. Радиоканал определенного диапазона частот являлся общей средой для всех передатчиков, использующих частоты этого диапазона. Сеть ALOHA работала по методу случайного доступа, когда каждый узел мог начать передачу пакета в любой момент времени. Если он после этого не дожидался подтверждения приема в течение определенного времени, то посылал этот пакет снова.

Позже эта технология разделения единой среды передачи была применена для проводного варианта LAN. Непрерывный сегмент коаксиального кабеля стал аналогом общей радиосреды. Все ПК присоединялись к этому сегменту кабеля.

Поскольку в сети используется общая электрическая шина, то если 2 или более электрических сигнала будут передаваться одновременно, они будут накладываться и сталкиваться (коллизия) – исходные сигналы при наложении станут нераспознаваемыми. Т.е. в стандарте Ethernet алгоритм работы сети разрешает только одному устройству одновременно пересылать данные в сеть. Такой алгоритм был **назван множественным доступом с контролем несущей и обнаружением коллизий** (Carrier Sense Multiple Access With Col-

lision Detection – CSMA/CD). Область сети, в которой создаваемые пакеты могут испытать коллизию, называют **доменом коллизий. И у**стройства прежде, чем начать передавать данные должны были убедиться, что среда передачи свободна.

Таким образом, общие принципы алгоритма CSMA/CD следующие:

-устройство, которое хочет передать фрейм, ожидает отсутствия передачи в локальной сети, т.е. пересылка фрейма не выполняется до тех пор, пока присутствует электрический сигнал в общей шине:

- при возникновении коллизии (столкновения 2-х сигналов) устройства, которые создали коллизию, ожидают в течение случайного интервала времени, а затем пробуют повторную передачу.

Несмотря на то, что такие сети были простыми в установке, они обладали существенными недостатками: ограничены по размеру, функциональности, недостаточно надежны, а также неспособны справляться со значительным увеличением сетевого трафика. Максимальная длина кабеля в стандарте 10Base-2 равна 185 метров, а в 10Base-5 - 500 метров, цифры из стандарта соответствуют максимальной длине кабеля 2 (200 метров примерно), 5(500 метров).

В некоторых случаях недостаточно такой длины кабеля для подключения устройств и тогда применяют **повторители (repeater)** (рисунок 2). Повторители это сетевые устройства, функционирующие на первом уровне модели OSI. Данные с устройства отправителя преобразуются в электрические или световые импульсы. Когда сигналы покидают передающую станцию, они являются четкими и легко распознаваемыми. Однако, чем больше длина 20Абеля, тем более слабым и менее различимым становится сигнал. Целью использования повторителя является регенерация сетевых сигналов на битовом уровне, что позволяет передавать их на большее расстояние. Поскольку повторители не интерпретируют значение битов, а только детектируют и генерируют электрические сигналы, они относятся к первому уровню модели OSI.

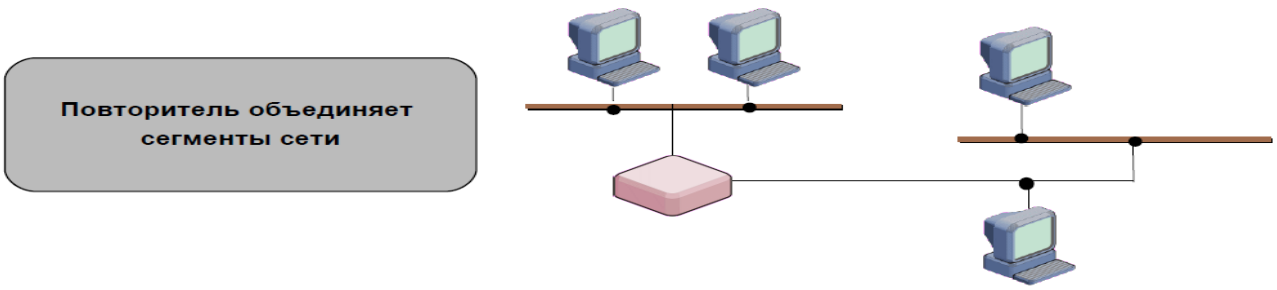


Рисунок 2 – Использование повторителей

Следующим шагом стала разработка стандарта 10 Base-T с физической топологией типа звезда, в которой каждый узел подключался отдельным 21Абелем к центральному устройству – **концентратору или hab.** Hub повторяет сигналы, поступившие с одного из его портов на все остальные активные порты, т.е Hub это многопортовый повторитель. При этом существенно повысилась надежность сети, так как каждое устройство подключается по отдельному кабелю к концентратору, следовательно, повреждение одного 21 Абеля приводит к неработоспособности только одного устройства. Поскольку концентраторы и повторители имеют похожие характеристики, то первые называют многопортовыми повторителями. В то время как повторитель имеет только 2 порта, концентатор (Hub) имеет от 4 до 20 портов (рис. 3).

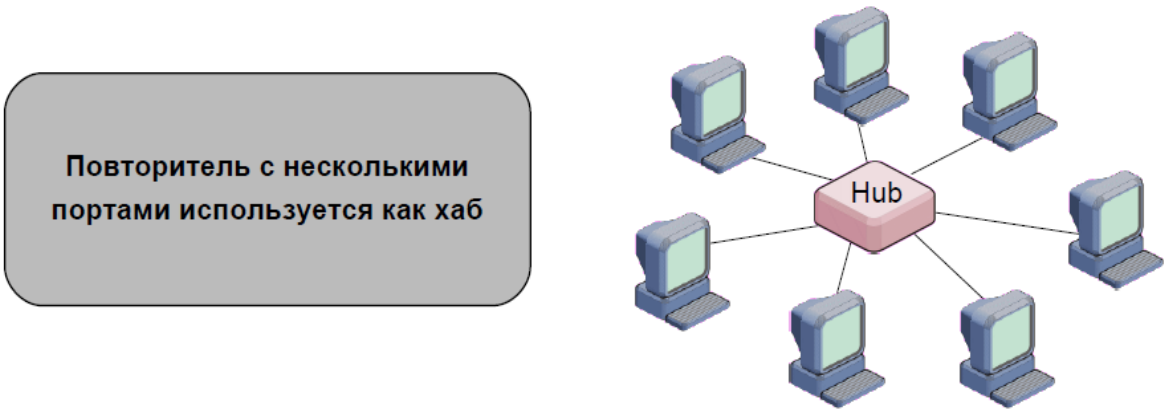


Рисунок 3 – Использование концентраторов

В 1990 году фирма Kalpana выпустила на рынок первый коммутатор (switch), получивший название Etherhetswitch, который **он мог одновременно устанавливать несколько соединений между разными парами портов.**

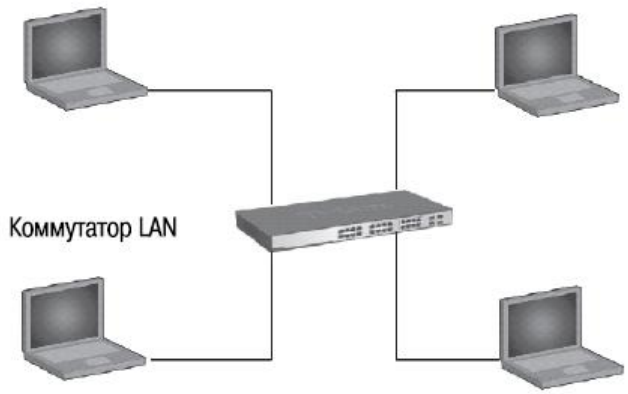


Рисунок 4 – Коммутатор в локальной сети

При передаче кадра (frame) в нем создавался отдельный канал, по которому данные пересылались «напрямую» от порта источника к порту получателю с максимально возможной для данной технологии скоростью.

Для предотвращения коллизий крупные локальные сети делятся на сегменты или домены коллизий, с помощью маршрутизаторов или коммутаторов. Непосредственно к маршрутизатору конечные узлы обычно не подключаются; подключение выполняется через коммутаторы. Каждый порт коммутатора оснащен процессором, память которого позволяет создавать буфер для хранения поступающих кадров. Общее управление процессорами портов осуществляет системный модуль.

Каждый сегмент, образованный портом (интерфейсом) коммутатора с присоединенным к нему узлом (компьютером) или с концентратором со многими узлами, является сегментом (доменом) коллизий. При возникновении коллизии в сети, реализованной на концентраторе, сигнал коллизии распространяется по всем портам концентратора. Однако на другие порты коммутатора сигнал коллизии не передается (рисунок 5).

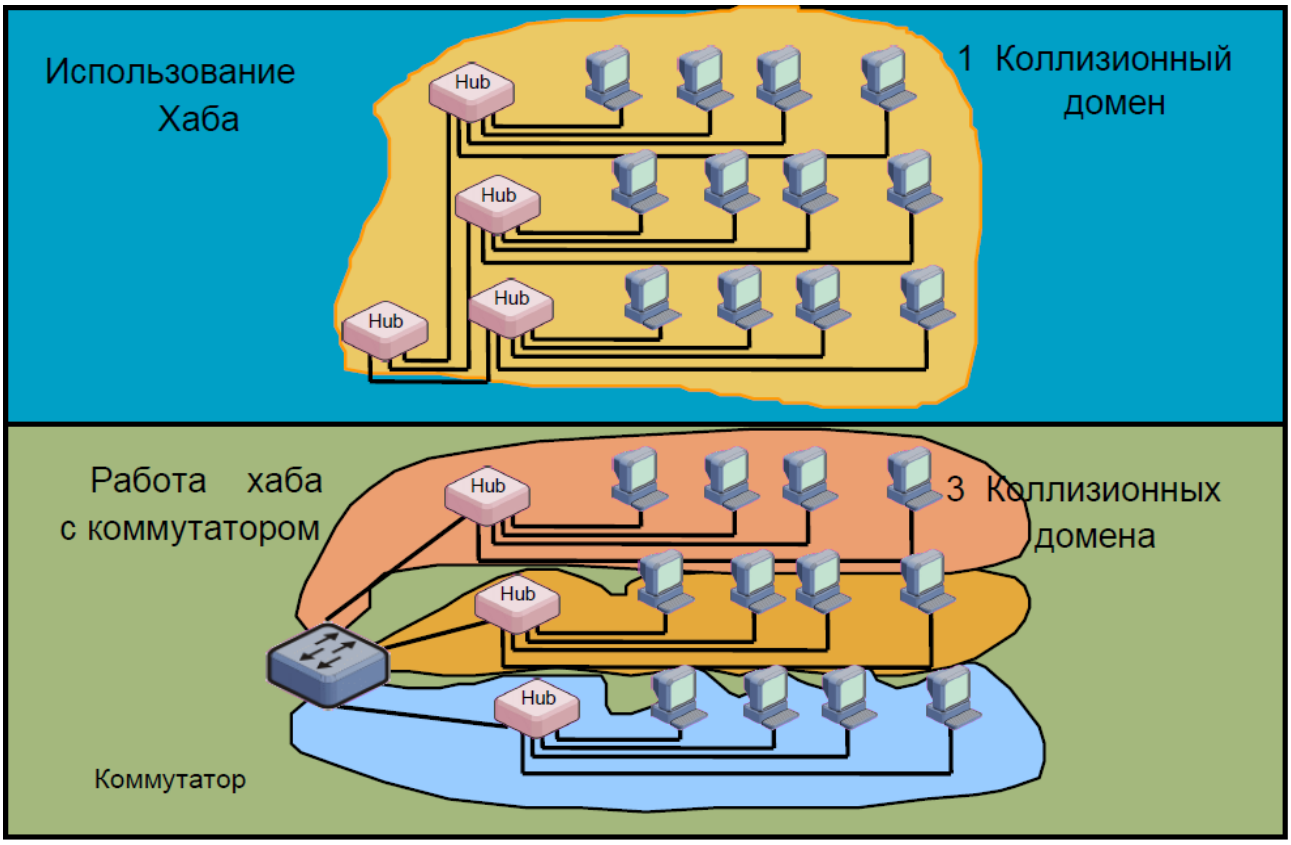


Рисунок 5 – Использование коммутаторов и концентраторов для построения сетей

Для того чтобы в сети Ethernet стала возможной локальная доставка кадров, необходима определенная система адресации, т.е. присвоения имен компьютерам и интерфейсам. Каждый компьютер имеет уникальный способ

самоидентификации. Никакие два физических адреса в сети не должны быть одинаковыми. Физические адреса, называемые адресами *управления доступом к передающей среде (Media Access Control - MAC_адрес)*, записаны в сетевом адаптере NIC. Для MAC адреса используются и другие названия: аппаратный адрес, NIC –адрес, адрес второго уровня и Ethernet – адрес.

MAC-адреса в сети Ethernet используются для уникальной идентификации отдельных устройств. Каждое устройство (ПК, маршрутизатор, коммутатор и т.д.), имеющее Ethernet-интерфейс, должно иметь MAC- адрес, в противном случае другие устройства не смогут обмениваться с ним данными.

Стандарты семейства Ethernet охватывают только два нижних уровня семиуровневой модели OSI – физический и канальный. На сегодняшний день физические стандарты Ethernet обладают большим разнообразием. Исторически первыми были стандарты Ethernet, которые обеспечивали передачу данных со скоростью 10Мбит/с. Затем появился стандарт, получивший название **FastEthernet (FE)**, который обеспечивал возможность передачи данных со скоростью100Мбит/с. Дальнейшим развитием технологии Ethernet явились стандарты **GigabitEthernet** (**GE**), позволяющие передавать информацию со скоростью 1 Гбит/с.

Контрольные вопросы

1.Как называется основной используемый в технологии Ethernet метод доступа к разделяемой среде передачи данных?

2**.** Какова максимально допустимая длина толстого коаксиального кабеля в технологии Ethernet без использования повторителя?

3. Какая максимальная скорость передачи данных поддерживается технологией Fast Ethernet?

4. Что из указанного ниже используется коммутатором для принятия решения о пересылке фрейма?

5. На каком уровне модели OSI работает коммутатор?

6. Что представляет собой MAC –адрес?

7. Опишите особенности построения сетей на коммутаторах и концентраторах.

8. Для каких целей применяются повторители?

9. Как строились первые сети Ethernet?

10. Опишите принципы алгоритма CSMA/CD.

Лабораторная работа №1. Построение простейшей компьютерной сети с использованием Cisco Packet Tracer

Цель работы

Изучить процесс построения сетевой топологии и настройки оборудования с использованием сетевого симулятора Cisco Packet Tracer.

Задание

1. Ознакомиться с основными понятиями построения простейшей компьютерной сети и работы с сетевым симулятором Cisco Packet Tracer.
2. Запустить Cisco Packet Tracer.
3. Просмотреть все вкладки.
4. Построить простейшую компьютерную сеть.

Порядок выполнения работы

1.Знакомство с основами работы в сетевом симуляторе

При запуске сетевого симулятора Cisco Packet Tracer открывается окно с рабочей областью, куда можно добавлять различное сетевое оборудование и соединять его согласно требуемой топологии (рисунок 1).

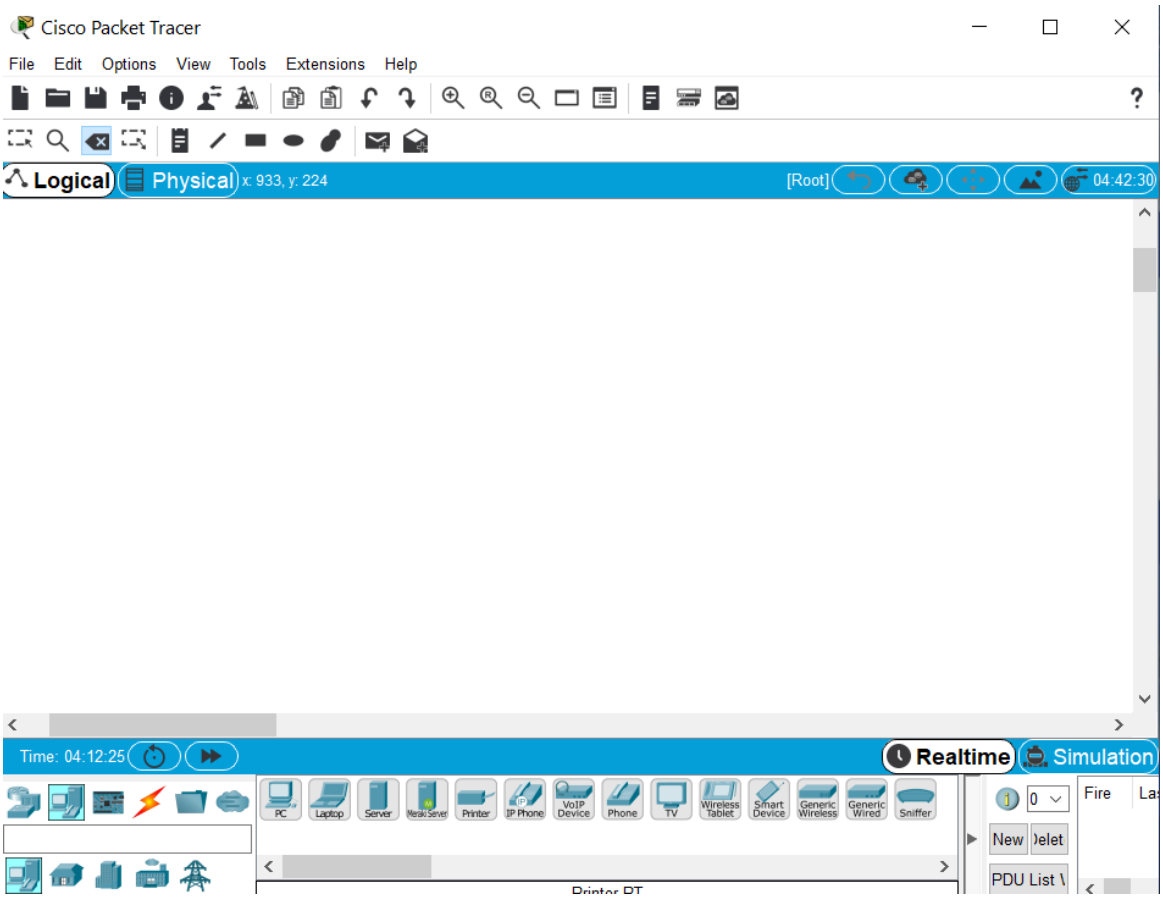


Рисунок 1 - Рабочее окно сетевого симулятора Cisco Packet Tracer

Для выбора сетевого оборудования необходимо в меню, расположенном в нижнем левом углу рабочего окна, нажать на нужный тип устройства. Компьютеры, серверы, ноутбуки, VoIP-телефоны и другие оконечные устройства находятся во вкладке End Devices (рисунок 2).

Рисунок 2 - Вкладка с оконечными сетевыми устройствами

Маршрутизаторы (Routers) и коммутаторы (Switches) находятся во вкладке Network Devices. В разделах Routers и Switches представлен целый ряд сетевого оборудования компании Cisco (рисунки 3 и 4).

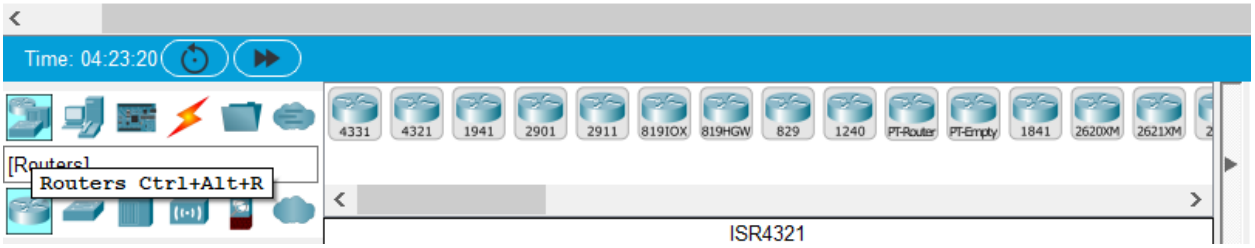


Рисунок 3 - Маршрутизаторы Cisco

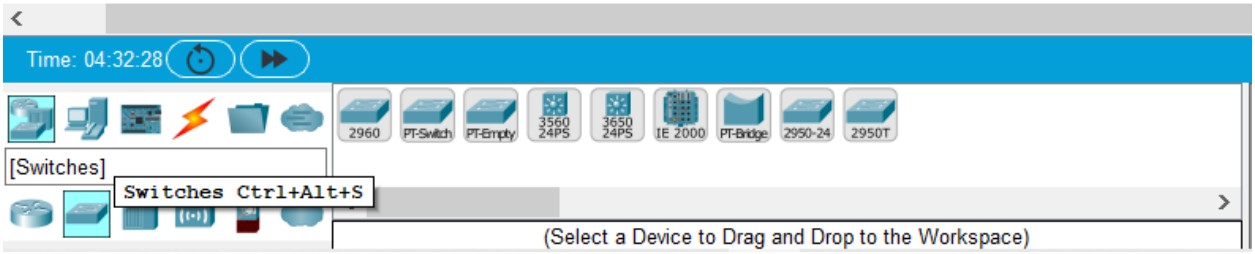


Рисунок 4. Коммутаторы Cisco

Во вкладке Connections находятся значки различного способа соединения оборудования (как проводного, так и беспроводного), указанные на рисунке 5.

Рисунок 5 - Обозначения способов соединения оборудования

При соединении оборудования с помощью медных кабелей наиболее используемыми являются прямой и перекрестный кабель.

Прямой кабель (straight through cable) – для соединения типа компьютер/коммутатор, коммутатор/маршрутизатор, т.е. для устройств разного уровня модели OSI.

Перекрёстный кабель (crossover cable) – для соединения типа компьютер/компьютер, коммутатор/коммутатор, маршрутизатор /маршрутизатор, т.е. для устройств одного уровня модели OSI.

Построение простейшей сети

Постройте простейшую компьютерную сеть, показанную на рисунке 6.

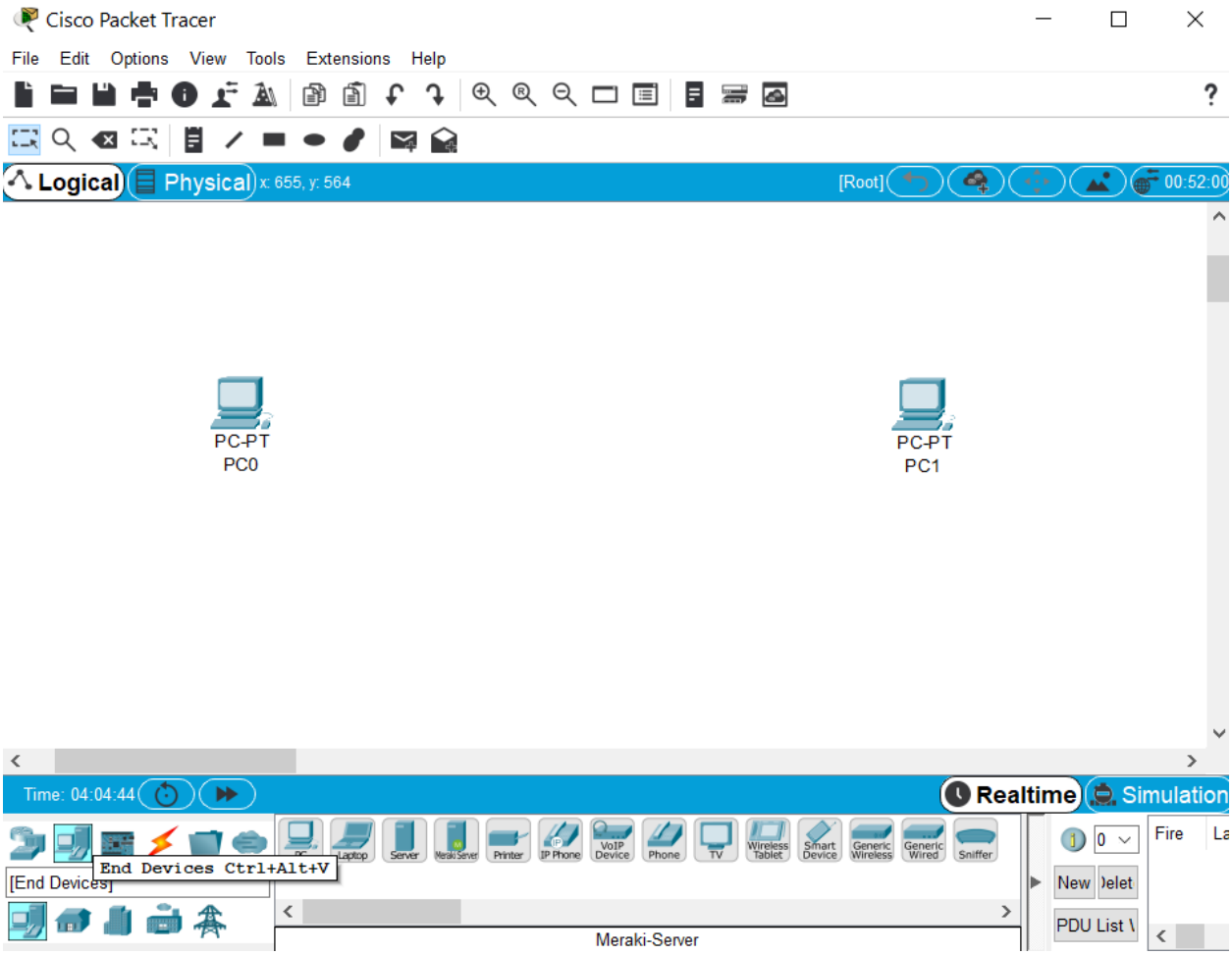


Рисунок 6 - Добавление компьютеров в рабочую область Cisco Packet Tracer

Для этого выбираем иконку End Device (конечные устройства) и находим там PC (персональный компьютер). Добавляем персональные компьютеры (PC0 и PC1) в рабочую область Cisco Packet Tracer. Перейдите во вкладку

Connections и выберите перекрестный тип кабеля (рис.7). Выберите тип соединения, нажмите на PC0, затем на нужный интерфейс (FastEthernet0).

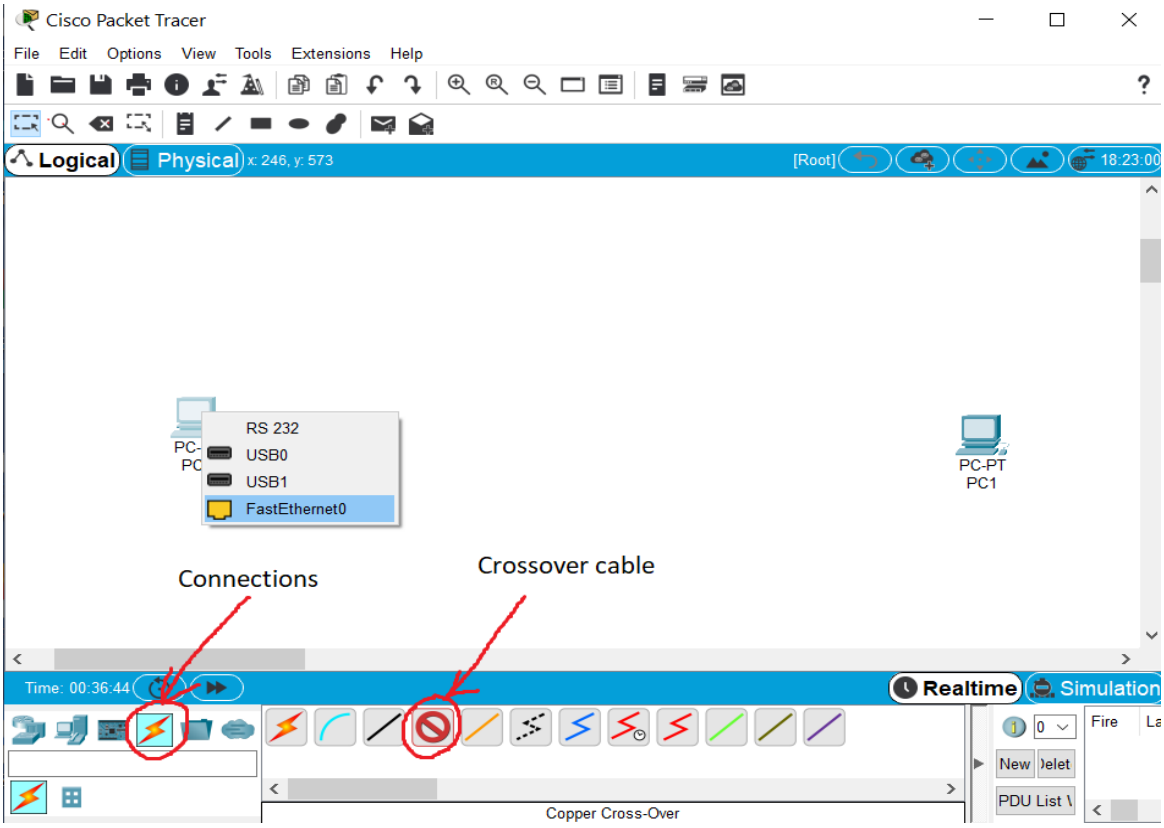


Рисунок 7 - Выбор типа кабеля

Соедините два компьютера между собой (рис. 8).

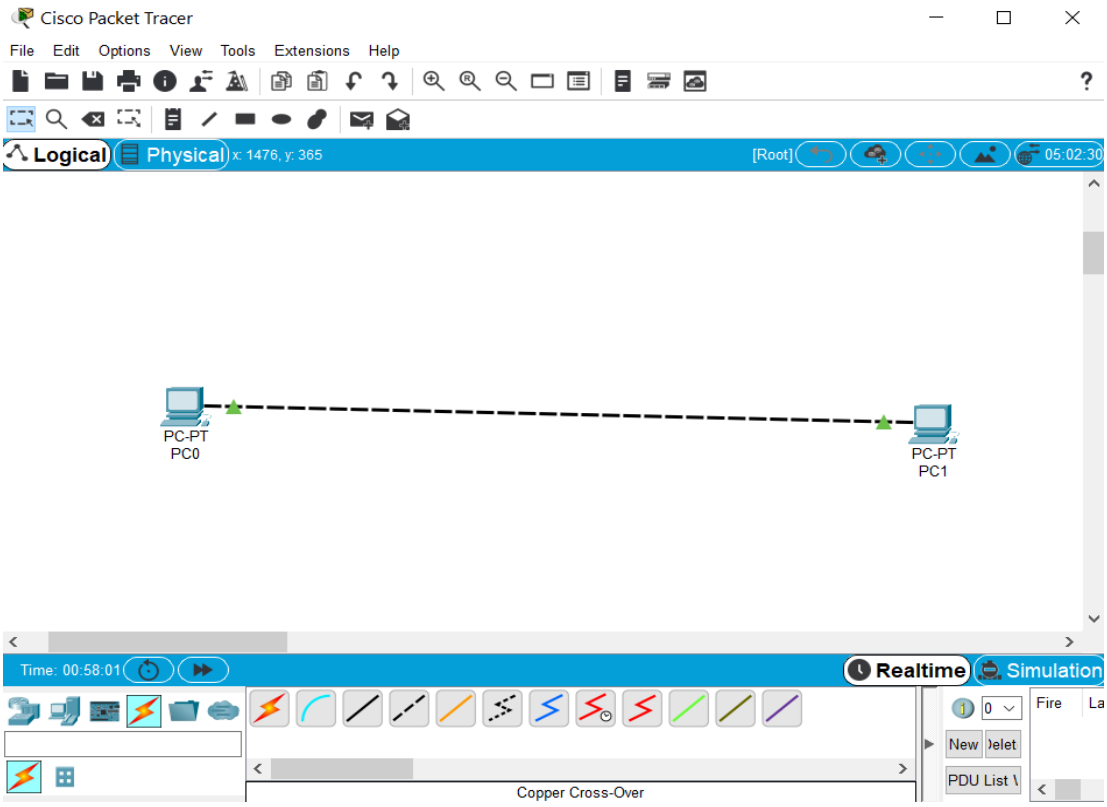


Рисунок 8 - Топология построенной сети

Перейдите к настройке компьютеров. Нажмите левой кнопкой мыши на компьютер PC0 и перейдите во вкладку Deskstop (рис.9), а там выберите вкладку в IP Configuration. Теперь введите IP-адрес 192.168.1.1 для PC0. Это адрес класса C. Щелкните левой кнопкой мыши на Subnet Mask и маска класса C - 255.255.255.0 автоматически появится в окне Subnet Mask (рис.10). Аналогичные действия произведите для второго компьютера (PC0). Присвойте ему адрес 192.168.1.2.

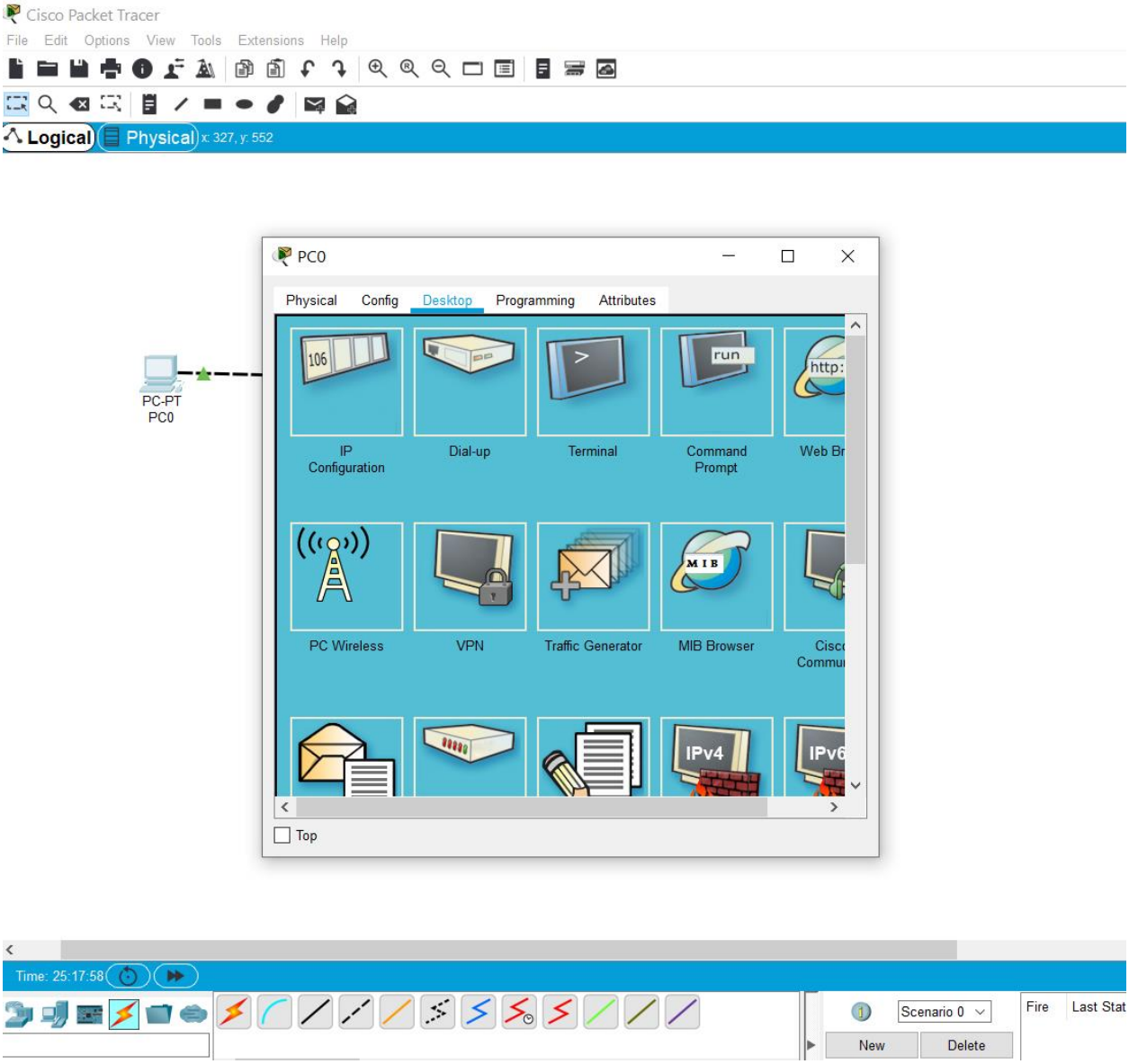


Рисунок 9 - Переход во вкладку Deskstop

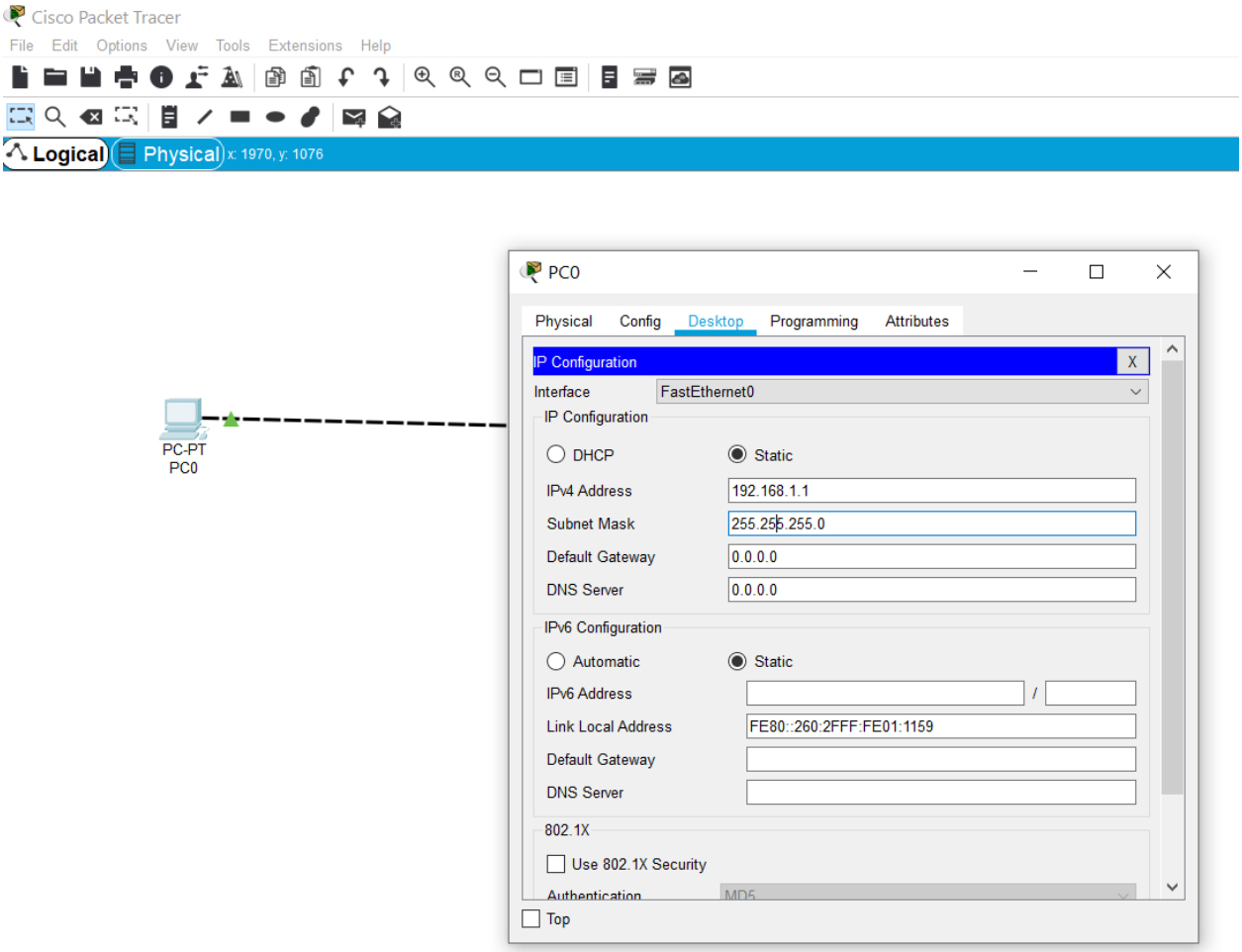


Рисунок 10 - IP-адрес и маска подсети для PC0

Проверьте сетевую связность между компьютерами. Для этого один раз нажмите левой кнопкой мыши на устройстве PC0 и перейдите в закладку Desktop, а затем нажмите Command Prompt . Введите команду:

C:\>ping 192.168.1.2

Результат выполнения данной команды приведен на рисунке 11. На рисунке видно, что для проверки связности сети компьютер PCO отправил компьютеру PC1 четыре пакета, и все они были получены приемной стороной. Аналогично можно произвести ту же самую проверку со стороны компьютера PC1.

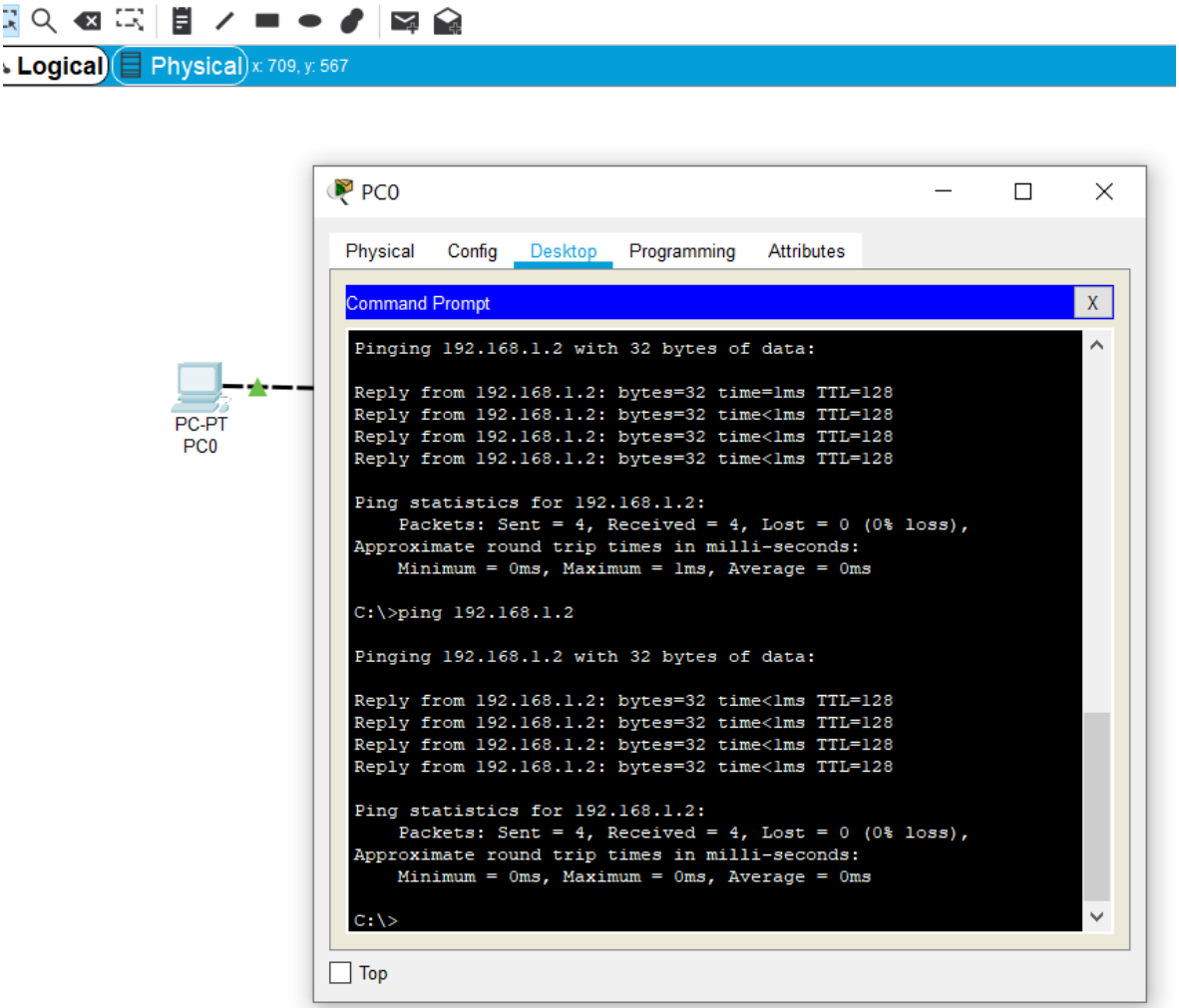


Рисунок 11 – Проверка связности простейшей сети

Для визуализации процесса прохождения пакета воспользуемся функцией Add Simple PDU. Пусть компьютер PC0 отправляет пакет на компьютер PC1. Для этого нажимаем на вкладку Add Simple PDU (рис.12).

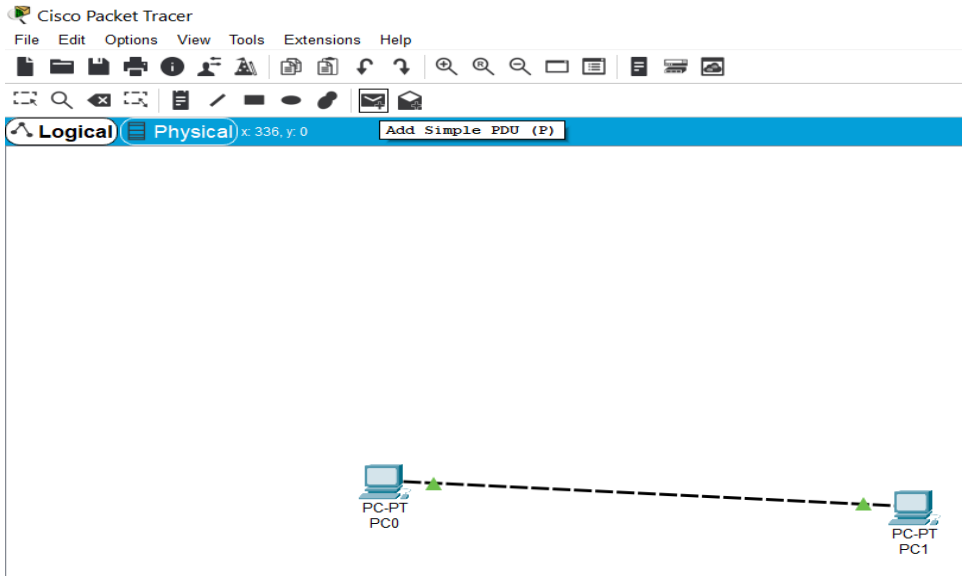


Рисунок 12 - Переход во вкладку Add Simple PDU

Для того, чтобы задать маршрут следования пакета необходимо нажать сначала на PC0, а затем на PC1, т.е. пакеты будут отправлены от PC0 к PC1 (рис.13).

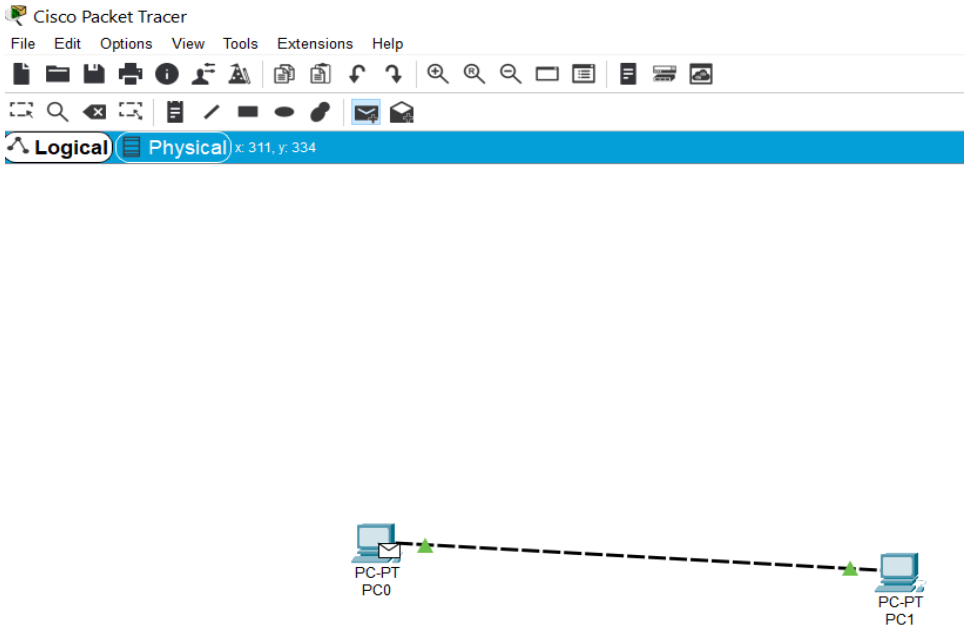


Рисунок 13 – Отправление пакетов от PC0 к PC1

Далее переходим во вкладку Simulation Mode (Режим моделирования), перетаскиваем синий ползунок влево (рис.14) и можем детально просмотреть передвижение пакета.

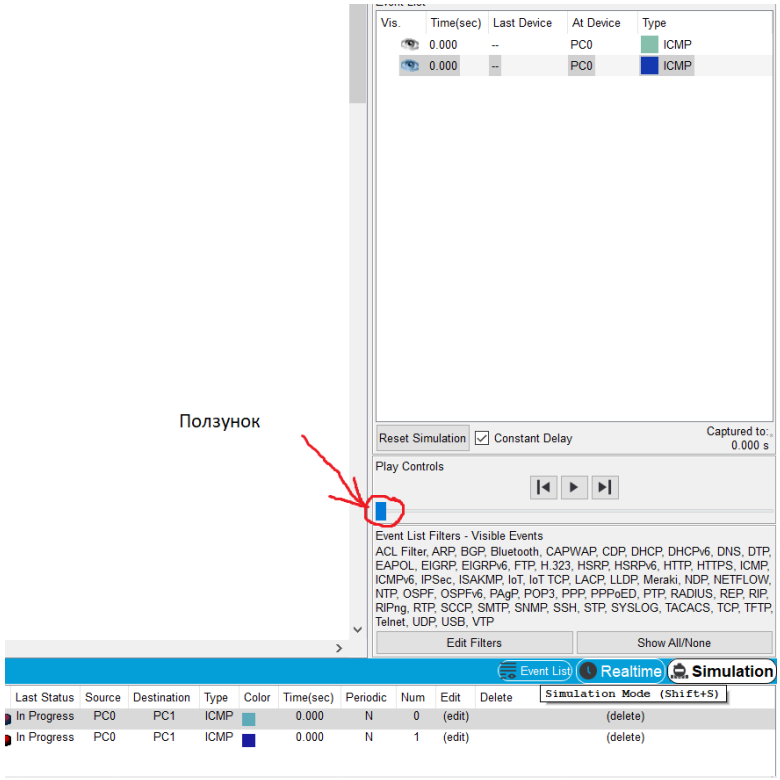


Рисунок 14 – Переход во вкладку Simulation Mode

Переходим во вкладку Play Controls и нажимаем на кнопку Capture then forward (рис. 15). Пакет начинает передвигаться от PC0 к PC1.

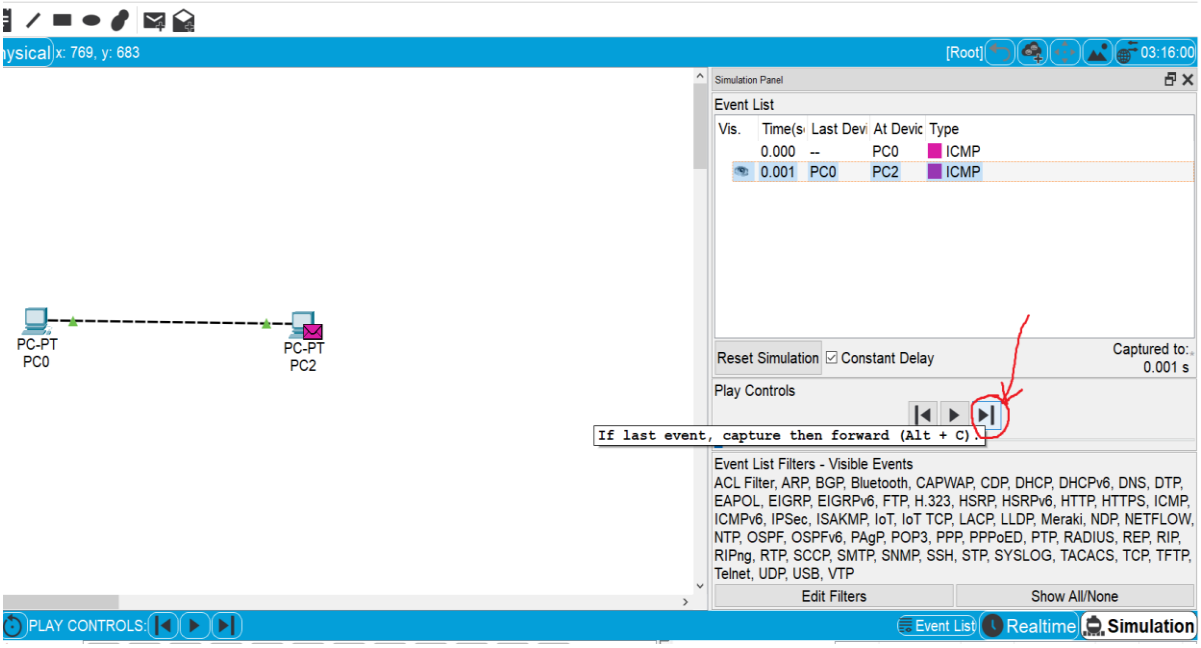


Рисунок 15 – Передвижение пакета от PC0 к PC1

Можно посмотреть содержимое пакета (рис.16). Для этого надо на него нажать левой кнопкой мыши. Здесь показаны все уровни модели OSI. Но на рисунке представлены три нижних уровня. Если вы хотите изменить масштаб в Cisco Packet Tracer, то неоходимо выполнить следующие действия:

Options->preferences->font->size->apply.

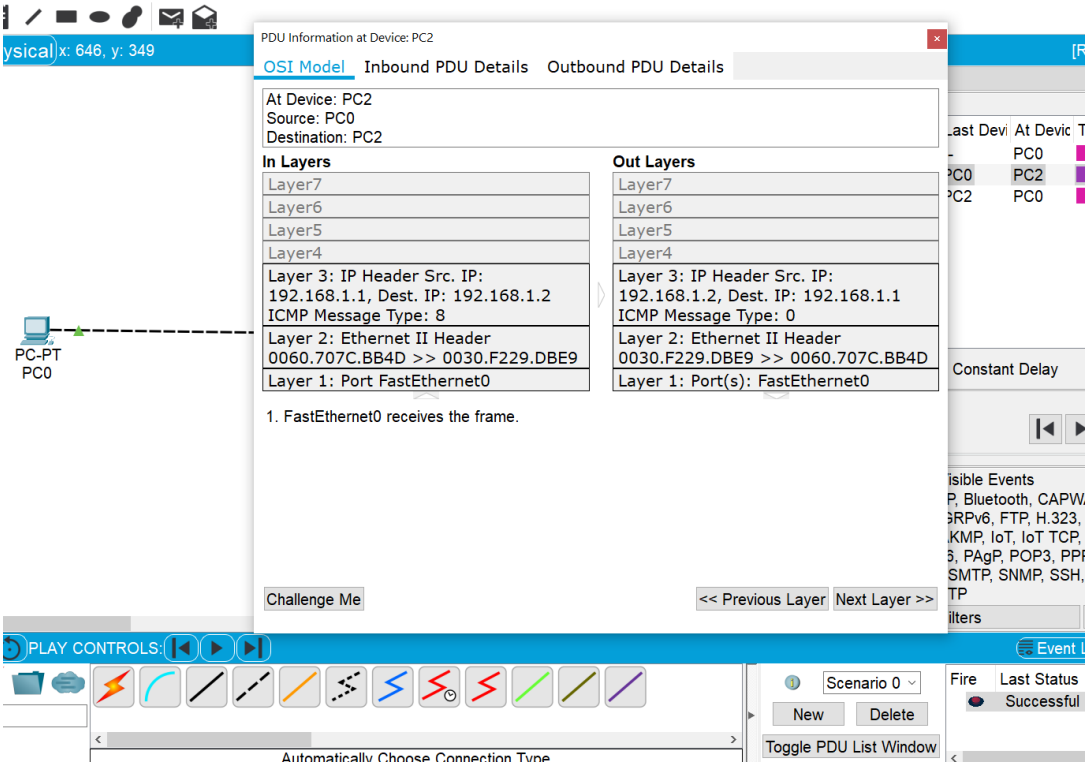


Рисунок 16 – Содержимое отправленного пакета

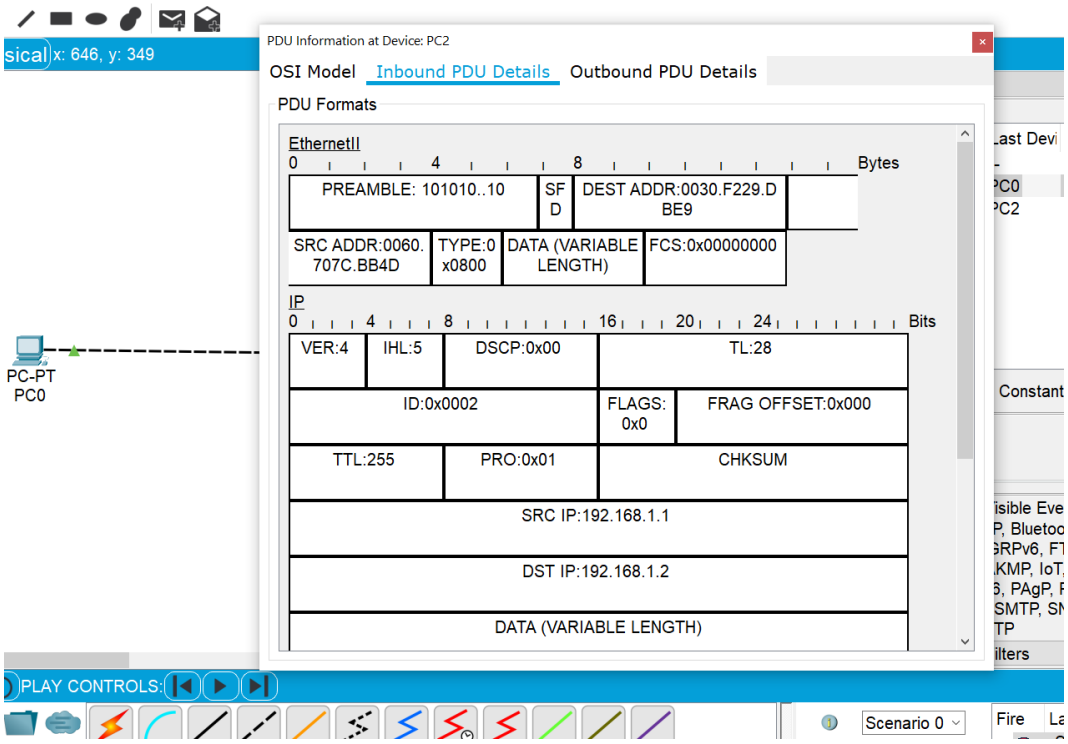


Рисунок 17 – Содержимое пакета во вкладке Inbound PDU Details

С помощью сетевого эмулятора Cisco Packet Tracer удобно изучать различные заголовки пакета. Но для этого необходимо получить дополнительные знания.

Содержание отчета

В индивидуальном отчёте должны быть указаны цель, задание, представлены необходимые снимки экрана и пояснения к ним. Следует проанализировать полученные данные и дать ответы на контрольные вопросы.

Контрольные вопросы

1. Что такое IP-адрес, какие функции он выполняет?
2. Из каких частей состоит IP-адрес?
3. Какие типы IP-адресов вы знаете?
4. Что такое маска подсети?
5. Какие функции необходимо выполнить, чтобы компьютеры могли взаимодействовать между собой?
6. Какие функции выполняет команда **ping**?
7. Какая команда, предоставляющая доступ к привилегированному режиму в оборудовании Cisco?

8. Какая команда, выводящая основную сетевую информацию ПК, сервера (IP-адрес, маску подсети, шлюз по умолчанию)?
9. Какой режим предоставляет доступ к полному перечню команд по настройке устройства?
10. Какой режим предоставляет доступ к ограниченному перечню команд, которые не влияют на настройки устройства?

Лабораторная работа №2. Основные команды операционной системы Cisco IOS

Цель работы

Изучить основные команды операционной системы Cisco IOS.

Задание

4. Ознакомиться с командами пользовательского режима;
5. Ознакомиться с командами привилегированного режима;
6. Ответить на вопросы.

Краткая теория

Cisco Packet Tracer – сетевой симулятор оборудования компании Cisco. Позволяет создавать различные сетевые топологии и анализировать передачу информации между сетевыми устройствами.

Ниже перечислены основные служебные команды, использующиеся в данном учебно-методическом пособии:

ipconfig – команда, выводящая основную сетевую информацию ПК, сервера (IP-адрес, маску подсети, шлюз по умолчанию);

ping A.B.C.D – команда, посылающая эхо-запрос на IP-адрес A.B.C.D, используется для тестирования сетевой связности устройств;

enable – команда, предоставляющая доступ к привилегированному режиму в оборудовании Cisco;

configure terminal – команда, предоставляющая режим глобальной конфигурации в оборудовании Cisco;

no shutdown – команда, переводящая порт в активное состояние (на коммутаторах все порты изначально активны), в оборудовании Cisco;

exit – команда, возвращающая в предыдущий раздел конфигурирования в оборудовании Cisco;

write memory – команда, записывающая все изменения в постоянную память устройства в оборудовании Cisco;
show running-config – команда, позволяющая просмотреть прошивку оборудования, основные настройки портов и различных технологий в оборудовании Cisco.

При работе с коммутаторами, маршрутизаторами используется CLI (Command Line Interface) — интерфейс командной строки. Имеются два режима работы в CLI:
> — пользовательский режим, предоставляет доступ к ограниченному перечню команд, которые не влияют на настройки устройства;
— привилегированный режим, предоставляет доступ к полному перечню команд по настройке устройства.

При входе в сетевое устройство (например, коммутатор) командная строка имеет вид:

Switch>

Чтобы получить доступ к полному набору команд, необходимо сначала активизировать привилегированный режим. Для этого вводится команда:

Switch> **enable**

После этого устройство переходит в привилегированный режим:

Switch#

О переходе в привилегированный режим будет свидетельствовать появление в командной строке приглашения в виде знака #.

Из привилегированного режима можно получать информацию о настройках системы и получить доступ к режиму глобального конфигурирования и других специальных режимов конфигурирования, включая режимы конфигурирования интерфейса, сетевого устройства, карты маршрутов и т.п.

Для выхода из привилегированного режима необходимо набрать команду:

Switch# **disable**

После этого на экране появится запись, подтверждающая, что устройство перешло в режим пользователя:

Switch>

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

Switch> **exit**

Режим глобального конфигурирования — реализует мощные однострочные команды, которые решают задачи конфигурирования. В этом режиме приглашение имеет вид:

Switch(config)#

Команды в любом режиме IOS распознаёт по первым уникальным символам. При нажатии клавиши табуляции система IOS сама дополнит команду до полной формы.

При вводе в командной строке любого режима имени команды и знака вопроса (?) на экран выводятся комментарии к команде. При вводе одного знака результатом будет список всех команд режима. На экран может выводиться много строк, поэтому иногда внизу экрана будет появляться подсказка - More -. Для продолжения следует нажать enter или пробел.

Команды режима глобального конфигурирования определяют поведение системы в целом. Кроме этого, команды режима глобального конфигурирования включают команды переходу в другие режимы конфигурирования, которые используются для создания конфигураций, требующих многострочных команд. Для входа в режим глобального конфигурирования используется команда привилегированного режима configure.

Основные команды сетевого устройства

Перетащите сетевое устройство маршрутизатор на экран.

1. Войдите сетевое устройство Router0 (вкладка CLI).

Router>

2. Нам нужно увидеть список всех доступных команд в этом режиме. Введите команду, которая используется для просмотра всех доступных команд:

Router>**?**

При этом клавишу Enter нажимать не надо. На экране появится список всех доступных команд для роутера в режиме пользователя.

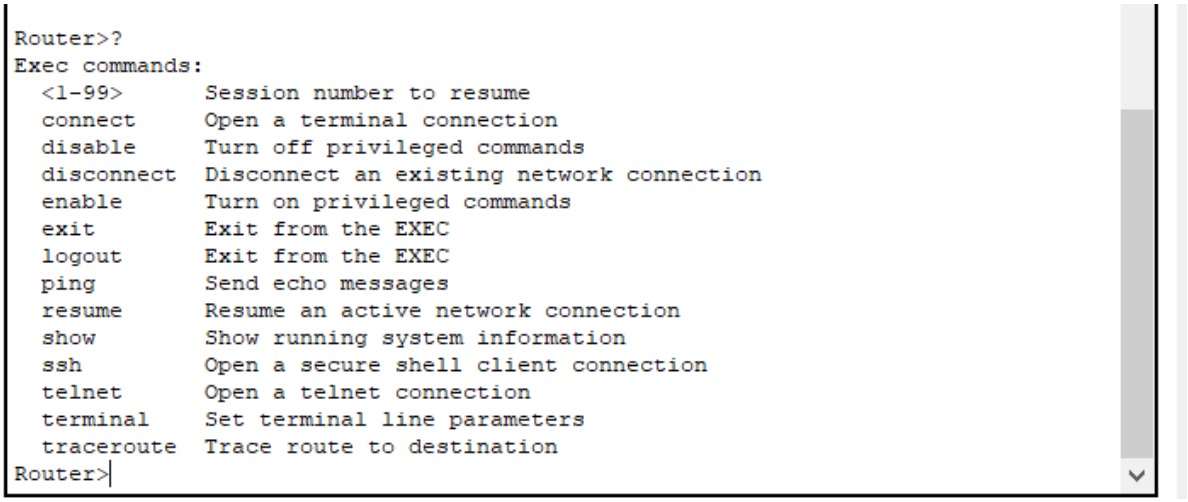


Рисунок 1 – Список доступных команд для роутера в режиме пользователя

3. Теперь войдите в привилегированный режим с помощью команды:

Router>**enable**

На экране появится значок привилегированного режима

Router#

4. Просмотрите список доступных команд в привилегированном режиме

Router#**?**

Рисунок 2 – Список доступных команд в привилегированном режиме

5. Перейдите в режим конфигурации с помощью команды:

Router#**config terminal**

После этого появляется режим конфигурации для роутера:

Router(config)#

6. Имя хоста сетевого устройства используется для локальной идентификации.
Установите "Router0" как имя вашего сетевого устройства.

Router(config)#**hostname Router0**
Router0(config)#

7. Пароль доступа позволяет вам контролировать доступ в привилегированный режим. Это очень важный пароль, потому что в привилегированном режиме можно вносить конфигурационные изменения. Установите пароль доступу, например "mtuci".

Router0(config)#**enable password mtuci**

Давайте проверим этот пароль. Выйдите из сетевого устройства и попытайтесь зайти в привилегированный режим.

Router0>**en**

Password:*****

Router0#

Здесь знаки: ***** - это ваш ввод пароля. Эти знаки на экране не видны.

Основные Show команды

1.Перейдите в пользовательский режим с помощью команды **disable.** Введите команду для просмотра всех доступных show команд.

Router0>**show ?**

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

2. Просмотр времени:

Router0>**show clock**

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

Router0>**show flash**

4. Сетевое устройство по умолчанию сохраняет 10 последних введенных команд (рис. 3)

Router0>**show history**

5. Существуют команды, которые позволят вам вернуться к командам, введённым ранее. Нажмите на клавишу стрелка вверх или <Ctrl> P.
6. Две команды позволят вам перейти к следующей команде, сохранённой в буфере. Нажмите на стрелку вниз или <Ctrl> N.

```
Router0>
Router0>show?
show
Router0>show flash

System flash directory:
File  Length   Name/status
  3   33591768 c1841-advipservicesk9-mz.124-15.T1.bin
  2   28282    sigdef-category.xml
  1   227537   sigdef-default.xml
[33847587 bytes used, 30168797 available, 64016384 total]
63488K bytes of processor board System flash (Read/Write)


Router0>show?
show
Router0>show history
  enable
  config terminal
  disable
  en
   disable
  show
  show clock
  show flash
  show history
Router0>
```

Рисунок 3 – Результаты выполнения команд Router0>**show flash** и Router0>**show history**

7. Чтобы увидеть список хостов и IP-адреса всех их интерфейсов необходимо набрать следующую команду:

Router0>**show hosts**

8. Следующая команда выводит детальную информацию о каждом интерфейсе (рис. 4).
Router0>**show interfaces**

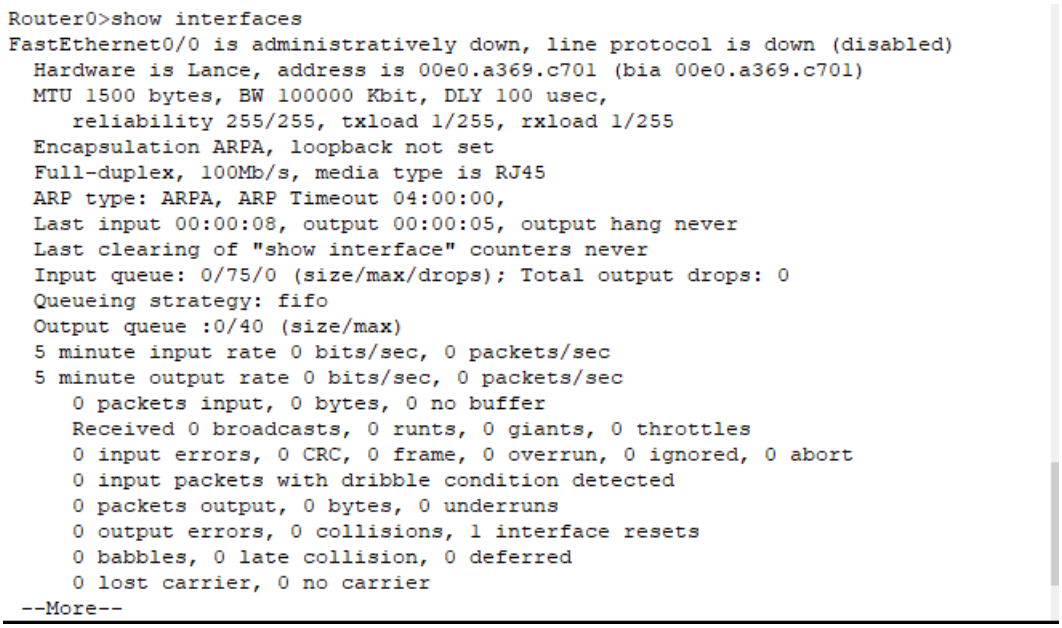


Рисунок 4 – Результат выполнения команды Router0>**show interfaces**

9. Команда выведет информацию о каждой telnet сессии, если они есть:

Router0>**show sessions**

10. Следующая команда показывает конфигурационные параметры терминала:
Router0>**show terminal**

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

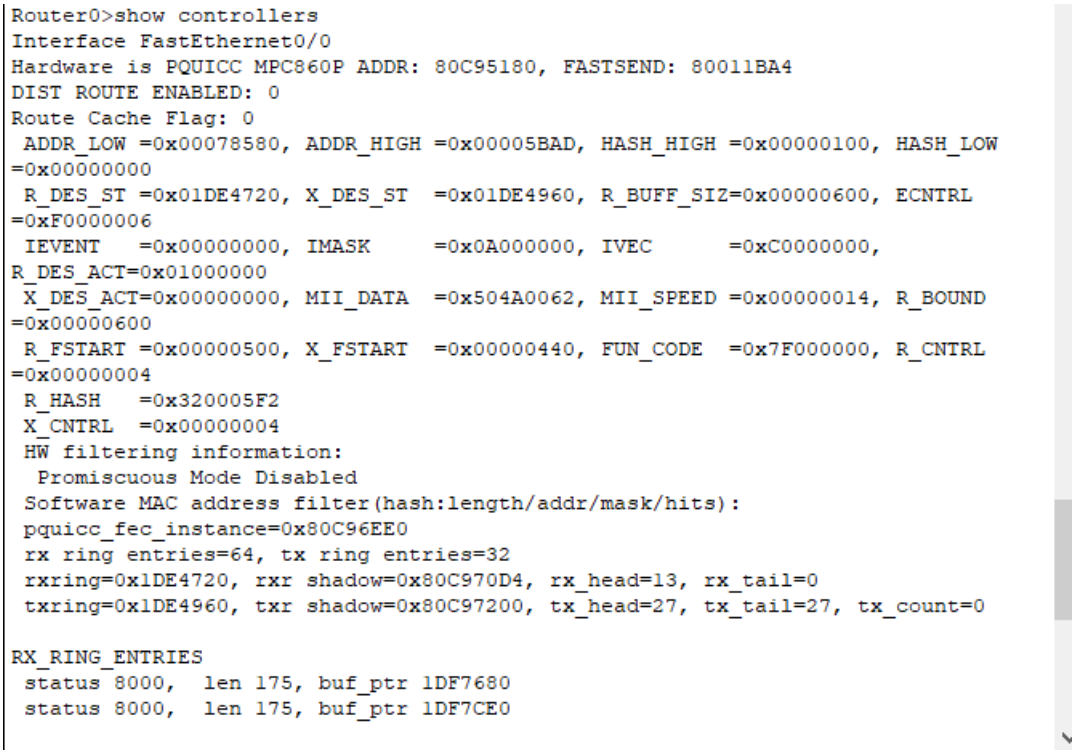
Router0>**show users**

12. Команда Router0>**show controllers** показывает состояние контроллеров интерфейсов (рис. 5).

Далее перейдём в привилегированный режим с помощью команды
Router0>**en.**
При этом не забудьте ввести пароль, который вы назначили.

Введите команду для просмотра всех доступных show команд.

Router0#**show ?**



```
Router0>show controllers
Interface FastEthernet0/0
Hardware is PQUICC MPC860P ADDR: 80C95180, FASTSEND: 80011BA4
DIST ROUTE ENABLED: 0
Route Cache Flag: 0
 ADDR_LOW =0x00078580, ADDR_HIGH =0x00005BAD, HASH_HIGH =0x00000100, HASH_LOW
=0x00000000
 R_DES_ST =0x01DE4720, X_DES_ST  =0x01DE4960, R_BUFF_SIZ=0x00000600, ECNTRL
=0xF0000006
 IEVENT   =0x00000000, IMASK     =0x0A000000, IVEC      =0xC0000000,
R_DES_ACT=0x01000000
 X_DES_ACT=0x00000000, MII_DATA  =0x504A0062, MII_SPEED =0x00000014, R_BOUND
=0x00000600
 R_FSTART =0x00000500, X_FSTART  =0x00000440, FUN_CODE  =0x7F000000, R_CNTRL
=0x00000004
 R_HASH   =0x320005F2
 X_CNTRL  =0x00000004
 HW filtering information:
  Promiscuous Mode Disabled
 Software MAC address filter(hash:length/addr/mask/hits):
 pquicc_fec_instance=0x80C96EE0
 rx ring entries=64, tx ring entries=32
 rxring=0x1DE4720, rxr shadow=0x80C970D4, rx_head=13, rx_tail=0
 txring=0x1DE4960, txr shadow=0x80C97200, tx_head=27, tx_tail=27, tx_count=0

RX_RING_ENTRIES
 status 8000,  len 175, buf_ptr 1DF7680
 status 8000,  len 175, buf_ptr 1DF7CE0
```

Рисунок 5 – Результат выполнения команды Router0>**show controllers**

Привилегированный режим включает в себя все show команды пользовательского режима и ряд новых. Посмотрим активную конфигурацию в памяти сетевого устройства. Для этого необходим привилегированный режим. Активная конфигурация автоматически не сохраняется и будет потеряна в случае сбоя электропитания. Чтобы сохранить настройки роутера используйте следующие команды:

сохранение текущей конфигурации:
Router# **write memory**
Или
Router# **copy run start**

Просмотр сохраненной конфигурации:
Router0#**show running-config**

В строке more, нажмите на клавишу пробел для просмотра следующей страницы информации.
Следующая команда позволит вам увидеть текущее состояние протоколов третьего уровня:

Router#**show protocols**

Введение в конфигурацию интерфейсов.

Рассмотрим команды настройки интерфейсов сетевого устройства.
На сетевом устройстве Router0 войдём в режим конфигурации:

Router0#**conf t**

Router1(config)#

Теперь ми хотим настроить Ethernet интерфейс. Для этого мы должны зайти в режим конфигурации интерфейса:

Router0(config)#**interface FastEthernet0/0**
Router0(config-if)#
Посмотрим все доступные в этом режиме команды с помощью (рис. 6):

Router0(config-if)#**?**

```
Router0(config-if)#?
  arp                 Set arp type (arpa, probe, snap) or timeout
  bandwidth           Set bandwidth informational parameter
  cdp                 CDP interface subcommands
  channel-group       Add this interface to an Etherchannel group
  crypto              Encryption/Decryption commands
  custom-queue-list   Assign a custom queue list to an interface
  delay               Specify interface throughput delay
  description         Interface specific description
  duplex              Configure duplex operation.
  exit                Exit from interface configuration mode
  fair-queue          Enable Fair Queuing on an Interface
  hold-queue          Set hold queue depth
  ip                  Interface Internet Protocol config commands
  ipv6                IPv6 interface subcommands
  lldp                LLDP interface subcommands
  mac-address         Manually set interface MAC address
  mtu                 Set the interface Maximum Transmission Unit (MTU)
  no                  Negate a command or set its defaults
  pppoe               pppoe interface subcommands
  pppoe-client        pppoe client
  priority-group      Assign a priority group to an interface
  service-policy      Configure QoS Service Policy
 --More--
```

Рисунок 6 - Результат выполнения команды Router0(config-if)#**?**

Для выхода в режим глобальной конфигурации наберите exit. Снова войдите в режим конфигурации интерфейса:

Router0(config)#**int fa0/0**

Здесь использовано сокращенное имя интерфейса.
Для каждой команды мы можем выполнить противоположную команду, поставивши перед ней слово no. Следующая команда включает этот интерфейс:

Router0(config-if)#**no shutdown**

Добавим к интерфейсу описание:

Router0(config-if)#**description Ethernet interface on Router 0**

Чтобы увидеть описание этого интерфейса, перейдите в привилегированный режим и выполните команду show interface (рис. 7):

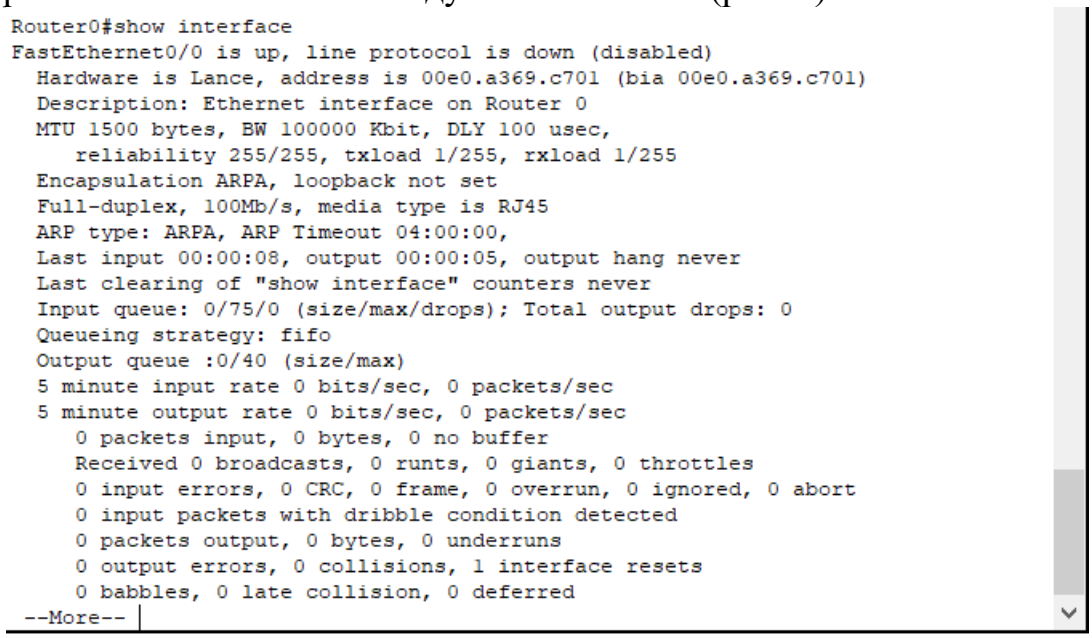


Рисунок 7 – Результат выполнения команды show interface

Контрольные вопросы

1. Какой командой можно посмотреть текущие настройки роутера?
2. Какими командами настраивается сетевой интерфейс роутера?
3. Как просмотреть конфигурационные настройки коммутатора?
4. Перечислите основные режимы конфигурации при настройке коммутатора?
5. Перечислите основные режимы конфигурации при настройке роутера.
6. Как посмотреть таблицу маршрутизации на роутере?
7. Какие команды формируют таблицу маршрутизации роутера?
8. Для чего нужна команда Router0#**conf t**
9. Какие действия происходят при выполнении команды Router0(config-if)#**no shutdown?**
10. Для каких целей применяется команда Router# **write memory?**

Практическая работа №4. Изучение принципов работы коммутаторов

Цель работы

Изучить принципы работы коммутаторов и концентраторов.

Задание

1. Изучить более подробно функции трех нижних уровней модели OSI ;
2. Ознакомиться с правилами составления таблицы коммутации;
3. Ответить на вопросы теста.

Обмен между соответствующими уровнями узлов А и В происходит определенными единицами информации. На трех верхних уровнях модели OSI – это **данные.** На транспортном уровне – **сегменты**, на сетевом уровне – **пакеты**, на канальном уровне – **кадры**, а на физическом уровне – последовательность битов.

К техническим средствам физического уровня относятся повторители сигналов (repeater), многопортовые повторители или концентраторы (hub), преобразователи среды (transceiver), например, преобразователи электрических сигналов в оптические и наоборот. На канальном уровне это коммутаторы (switch). На сетевом уровне – маршрутизаторы (router).

Рисунок 1 - Устройства и единицы информации соответствующих уровней

На каждом уровне модели OSI происходит присоединение заголовков со служебной информацией. Передаваемое сообщение, сформированное приложением, проходит три верхних уровня и поступает на транспортный уровень, где делится на части и каждая часть инкапсулируется (помещается) в

сегмент данных (рис.2). В заголовке сегмента содержится номер протокола уровня приложений, который подготовил данное сообщение. На сетевом уровне сегмент инкапсулируется в пакет данных, заголовок которого содержит сетевые (логические) адреса отправителя информации (источника) – Source Address (**SA**) и получателя (назначения) – Destination Address (**DA**) или **IP-адреса**.

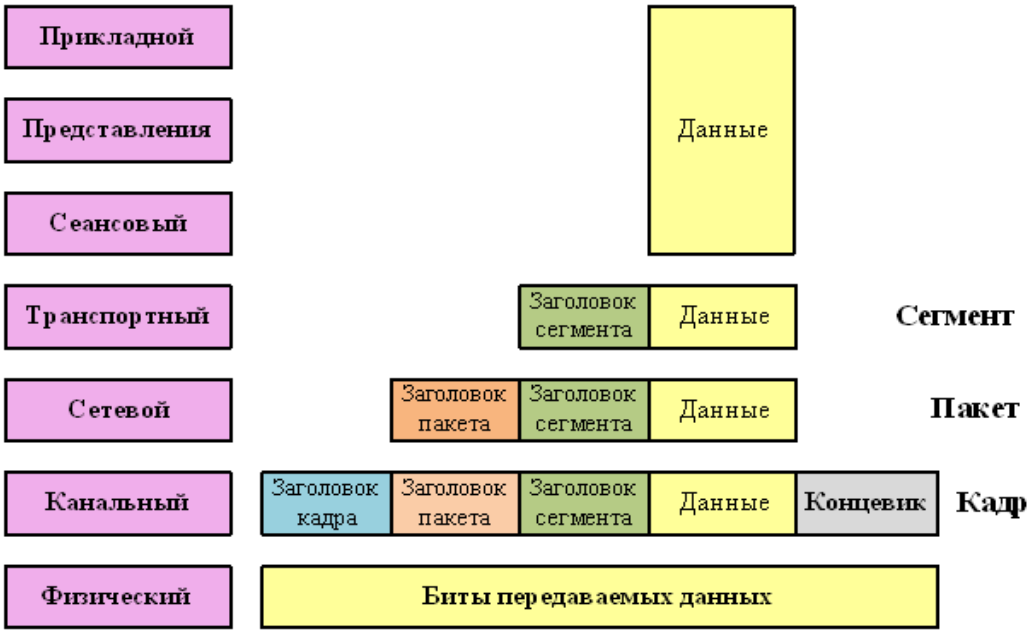


Рисунок 2 – Процесс инкапсуляции данных

Рассмотрим более подробно устройства, находящиеся на двух нижних уровнях модели OSI.

Компьютер может подключаться отдельным кабелем к ***концентратору*** (Hub), который повторяет сигналы, поступившие с одного из его портов на все остальные активные порты, т.е. это многопортовый повторитель. Целью использования повторителя является регенерация (восстановление) сетевых сигналов, которые представляют собой электрические или световые импульсы. Это позволяет передавать их на большее расстояние. Повторитель имеет только 2 порта, а концентратор (Hub) имеет от 4 до 20 портов.

На канальном уровне модели OSI находятся ***коммутаторы*** (switch), , которые выполняет функции коммутации по заранее известным MAC-адресам. Эти адреса назначаются производителем оборудования и являются уникальными. MAC – адрес состоит из 6 байт. Старшие 3 байта это идентификатор фирмы-производителя, а младшие 3 байта назначаются уникальным образом самим производителем. MAC – адрес обычно представляется в шестнадцатеричной форме. Например, 00-D0-50-5F-4E-12. Адрес, состоящий из всех единиц FF-FF-FF-FF-FF-FF, является широковещательным адресом

(broadcast), когда передаваемая в кадре информация предназначена всем станциям локальной сети.

Первоначально в коммутаторе отсутствует информация о том, какие компьютеры и с какими MAC-адресами подключаются к его порту. Поэтому коммутатор, получив кадр, передает его на все свои порты, за исключением того, на который кадр был получен, и одновременно запоминает MAC-адрес источника в таблице коммутации.

Например, если компьютер с MAC-адресом 00-0C-29-9B-E6-B5 передает кадр данных узлу 00-20-5C-01-22-22 (рис. 3), то в таблице коммутации появится первая запись. В этой записи будет указано, что компьютер с MAC-адресом 00-0C-29-9B-E6-B5 присоединен к порту № 1. При передаче данных от компьютера 00-20-5C-01-22-22 к компьютеру 00-0C-29-9B-E6-B5 в таблице коммутации появится вторая запись и т.д. Таким образом, число записей в адресной таблице может быть равно числу узлов в сети, построенной на основе коммутатора.

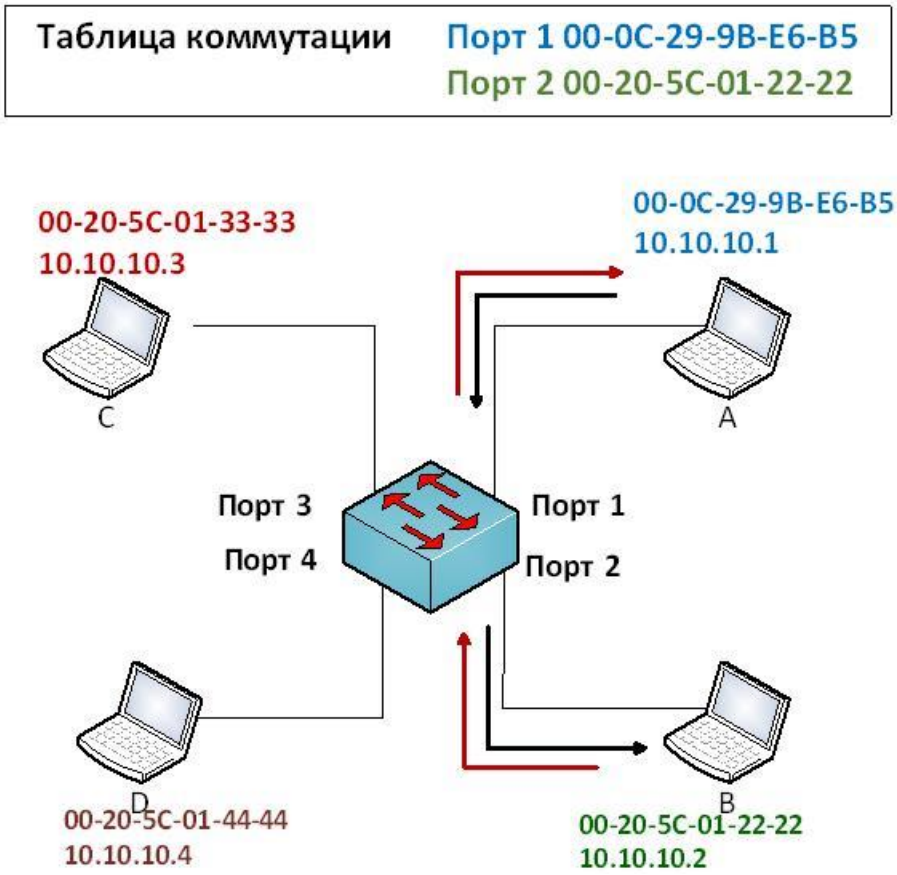


Рисунок 3 – Передача кадра между портами коммутатора

Когда адресная таблица коммутации сформирована, продвижение кадров с входного интерфейса коммутатора на выходной происходит на основа-

нии записей в адресной таблице. При получении кадра коммутатор проверяет, существует ли MAC-адрес узла назначения в таблице коммутации.

Также при получении кадра от одной из узлов (например, узла A), коммутатор может формировать широковещательный кадр, который распространяется по всем портам, кроме порта, на который подключен узел A. Этот опрос производится для того, чтобы коммутатор мог определить, какие рабочие станции находятся на всех портах. В ответ станции B, C и D посылают ответы с указанием своих MAC-адресов. После заполнения всей таблицы коммутации (MAC-таблицы) коммутатор входит в нормальный режим коммутации кадров.

С появлением в сети новых узлов адресная таблица пополняется. Если в течение определенного времени какой-то узел не передает данные, то считается, что он в сети отсутствует, тогда соответствующая запись из таблицы удаляется. При необходимости администратор может включать в таблицу статические записи, которые не удаляются динамически. Такую запись может удалить только сам администратор.

Максимальное значение пропускной способности коммутатора всегда достигается на кадрах максимальной длины, так как при этом доля накладных расходов на служебную информацию кадра гораздо ниже, чем для кадров минимальной длины, а время выполнения коммутатором операций по обработке кадра, приходящееся на один байт пользовательской информации, существенно меньше.

Тест к разделу «Изучение принципов работы коммутаторов»

1. Укажите широковещательный MAC-адрес (Broadcast) в шестнадцатеричной форме:
-AB:FF:FF:FF:FF:CD
-AC:89:FF:13:EF:CD
+FF:FF:FF:FF:FF:FF
-AB:EE:FF:09:FF:67

2. На кадрах какой длины достигается максимальное значение пропускной способности коммутатора?
+ На кадрах максимальной длины
- На кадрах минимальной длины
- На кадрах средней длины
- Длина кадра не влияет на пропускную способность коммутатора

3.Укажите длину MAC-адреса в битах:
-36
+48
-24
-6.
4. Какие единицы информации применяются на канальном уровне?
+ Кадры
-Сегменты
-Биты
- Пакеты.
5. Какие единицы информации применяются на физическом уровне?
- Кадры
-Сегменты
+Биты
- Пакеты.
6. На каком уровне модели OSI работает коммутатор?
-1
+2
-3
-4
7. Какая информация содержится в заголовке сегмента данных?
- Сетевые адреса отправителя информации и получателя;
+ Номер протокола уровня приложений, который подготовил данное сообщение.
-MAC- адреса источника и получателя.
8. Переведите MAC- адрес 00-D0-50-5F-4E-12 в двоичную форму.

- 0001 1000 1101 0000 0101 1111 0111 1110 0100 1110 0001 0010
+ 0000 0000 1101 0000 0101 0000 0101 1111 0100 1110 0001 0010
- 1100 0011 1101 0011 0101 1111 0100 1110 0100 1110 0001 1110
- 1111 1100 1101 1100 0101 1111 0100 1110 0100 1110 0001 1111
9. Для чего применяется концентратор в компьютерных сетях?
+ Повторяет сигналы, поступившие с одного из его портов на все остальные активные порты;
- Выполнения функции коммутации по заранее известным MAC-адресам.
- Для выбора оптимального маршрута в сети.

10.Переведите двоичную форму записи MAC- адреса

1100 1111 0001 0000 0000 1010 1110 0101 1111 0000 0101 0011
в шестнадцатеричную форму.
- CA-B0-E6-FC-D3
+ CF-10-0A-E5-F0-53
- CA-B5-E6-AC-B7
- 78 –C3-E6-AC-B7.

Лабораторная работа №3. Организация простейшей компьютерной сети с помощью коммутатора и концентратора

Цель работы

Построить простейшую компьютерную сеть с использованием коммутаторов и концентраторов.

Задание

1. Запустить Cisco Packet Tracer.
2. Построить простейшую компьютерную сеть с использованием концентратора.
3. Построить простейшую компьютерную сеть с использованием коммутатора.
4. Сравнить работу этих сетей.

Краткая теория

Если в сети появляется более двух компьютеров, то для организации сети необходимо использовать специализированные устройства. Для этого используются концентраторы (Hub), которые функционируют на первом уровне модели OSI, либо как коммутаторы (Switch), которые работают на втором уровне модели OSI. Концентратор (Hub) повторяет сигналы, поступившие с одного из его портов на все остальные активные порты. Коммутатор выполняет функции коммутации по заранее известным MAC-адресам.

Основное преимущество концентратора это его низкая стоимость. Он имеет следующие недостатки: невысокая скорость и отсутствие безопасности. В настоящее время концентратор применяется довольно редко на компьютерных сетях. Концентратор в отличие от коммутатора отправляет пакеты на все порты, кроме порта источника. Так, например, если компьютер PC0 отправляет пакеты PC1, то концентратор отправляет этот пакет на все компьютеры, которые к нему подключены, кроме порта источника.

Коммутатор в отличие от этого отправляет пакеты только на тот порт, который необходим. Происходит это за счет использования таблицы MAC-адресов, в которой за каждым портом коммутатора закреплен определенный MAC-адрес устройства.

Порядок выполнения работы

1. Запустить Cisco Packet Tracer;
2. Необходимо создать сеть, в которой имеется 4 компьютера. Для этого во вкладке END Devices выбираем персональные компьютеры PC, присваиваем им IP –адреса, как было показано в лабораторной работе №1. IP- адреса можно взять следующие: 192.168.1.1, 192.168.1.2, 192.168.1.3, 192.168.1.4. Маску класса С 255.255.255.0 оставляем. Присвоение IP-адреса PC0 показано на рисунке 1.

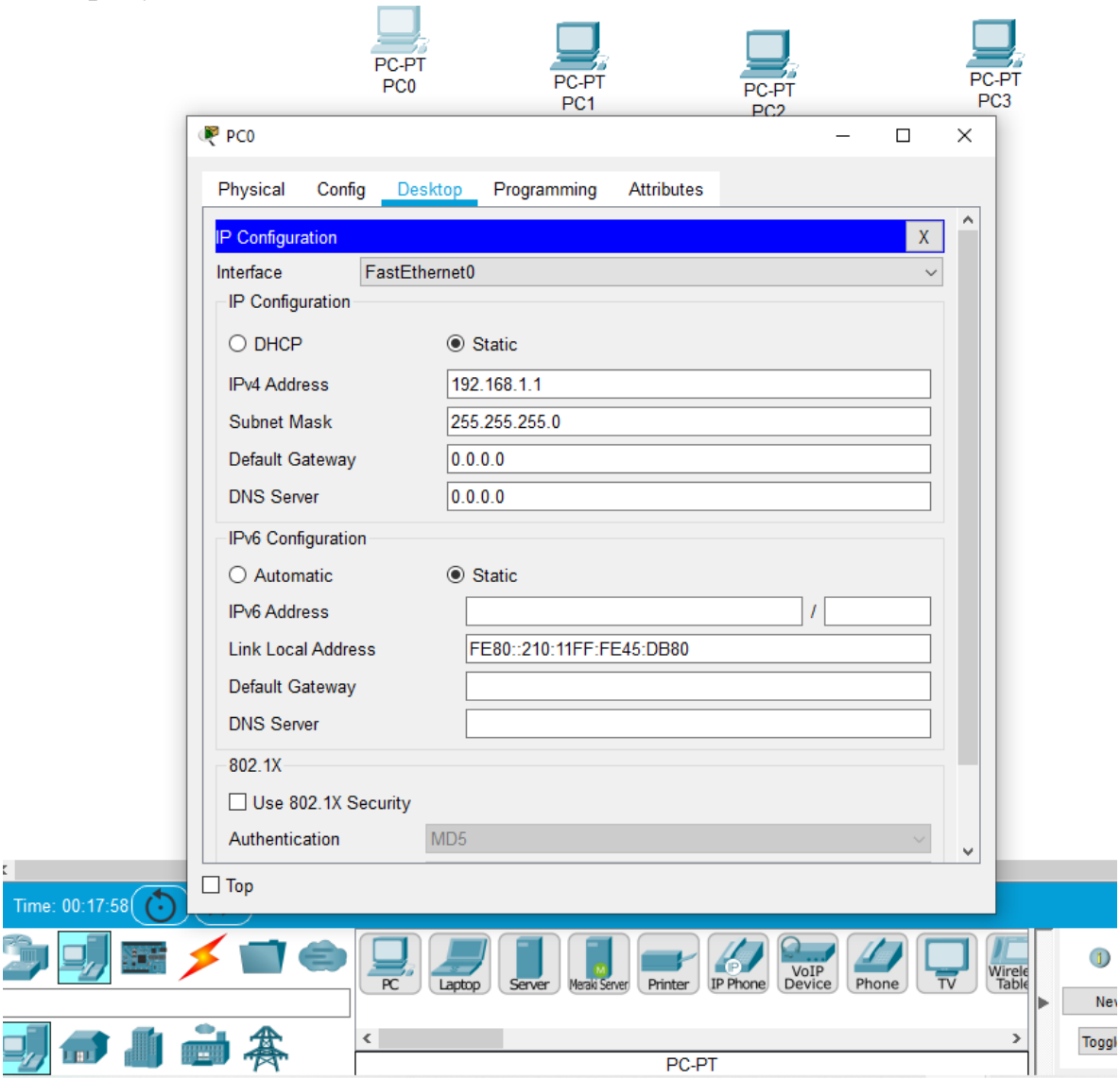


Рисунок 1 – Присвоение IP- адреса для PC0

3. Далее во вкладке Network Devices выбираем коммутатор. Возьмем самый распространенный коммутатор компании Cisco (Switch 2960 -24 TT). Далее выбираем тип кабеля. Выбираем прямой кабель. У PC0 берем единственный порт FastEthernet0 (рис.2). Для соединения коммутатора с PC0 выбираем на нем первый порт FastEthernet0/1 (рис. 3).

4.

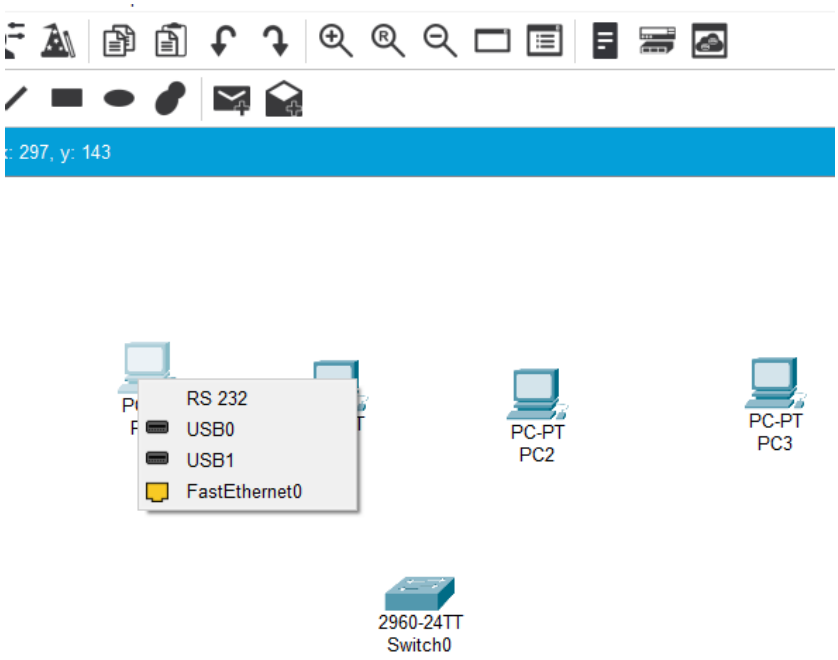


Рисунок 2 – Выбор порта FastEthernet0 на PC0 для соединения с коммутатором

Аналогично соединяем остальные компьютеры с коммутатором. В результате получаем следующую сеть. На компьютерах зеленые линии загорелись сразу (рис. 4), а коммутаторам требуется некоторое время. Как только линии загорелись зелеными, наша сеть начинает функционировать (рис. 5).

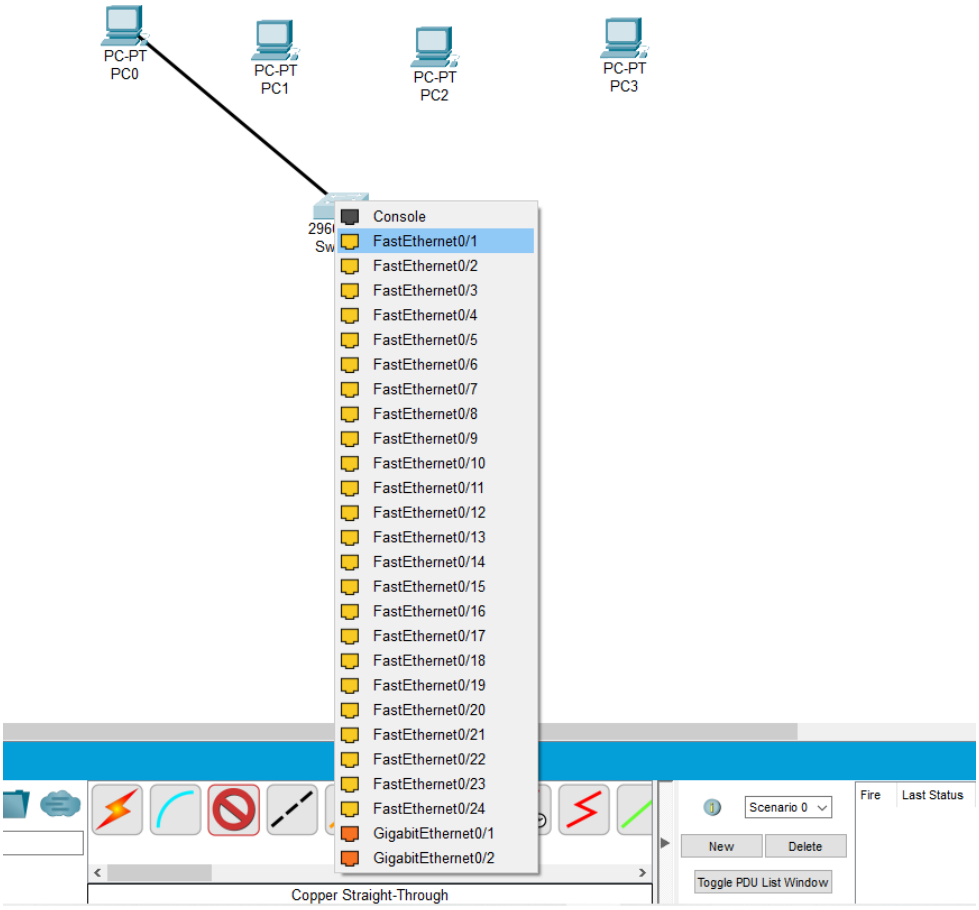


Рисунок 3 – Выбор порта FastEthernet0/1 на коммутаторе для соединения с PC0

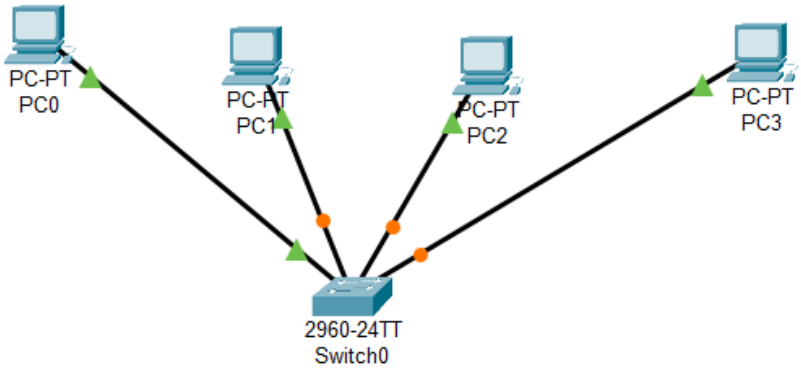


Рисунок 4 – Линии между компьютерами и коммутаторами находятся в неактивном режиме

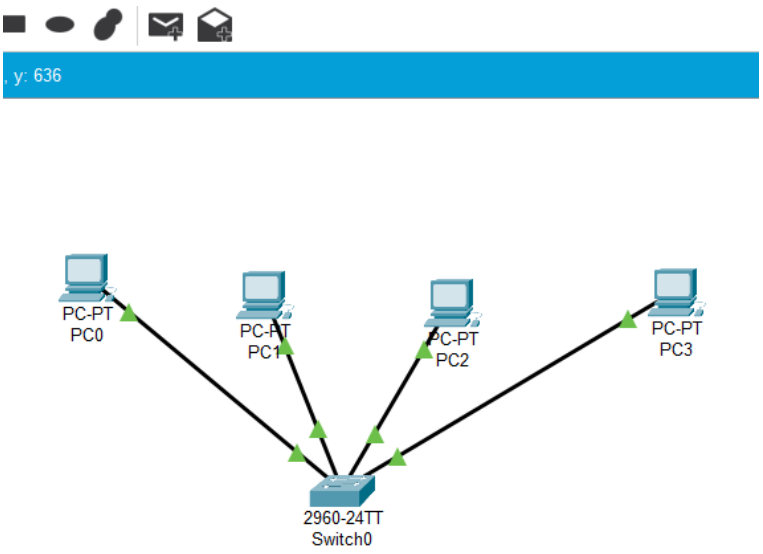


Рисунок 5 – Линии между компьютерами и коммутаторами находятся в активном режиме

Можно щелкнуть левой кнопкой мыши на коммутаторе и посмотреть его порты. Во вкладке Physical показано, что на коммутаторе имеется 24 порта FastEthernet и 2 порта GigabitEthernet (рис. 6).

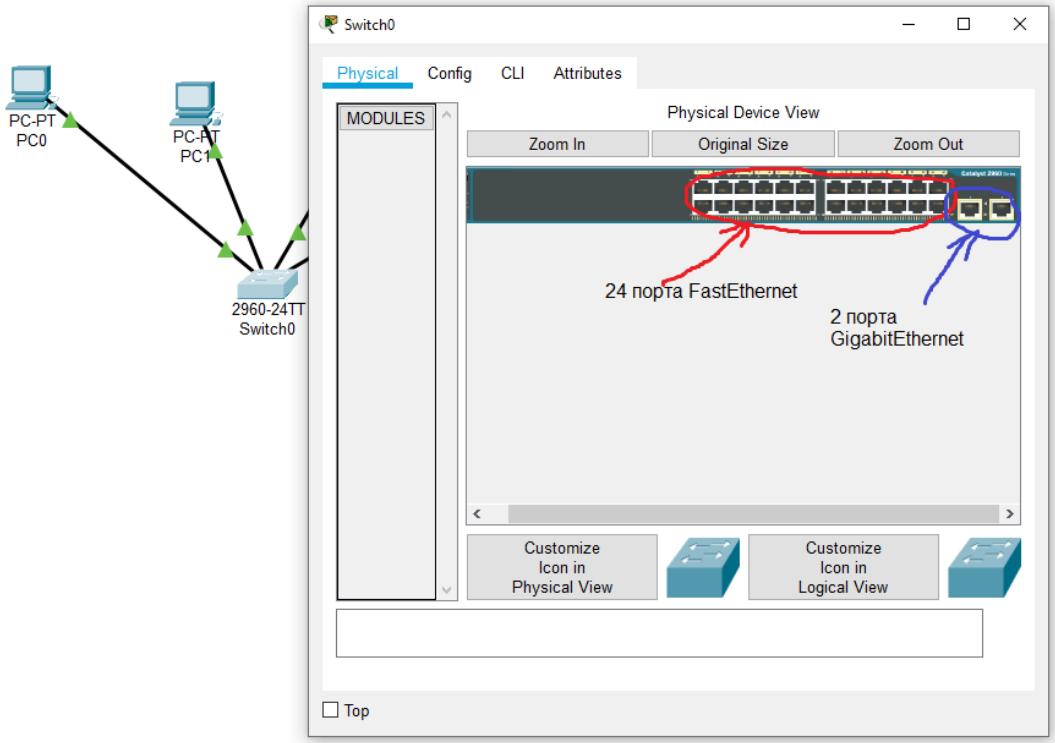


Рисунок 6 – Порты на коммутаторе

Далее необходимо проверить работоспособность этой сети. Эту функцию мы уже проверяли в лабораторной работе №1. Для этого один раз

нажмите левой кнопкой мыши на устройстве PC0 и перейдите в закладку Desktop, а затем нажмите Command Prompt . Введите команду:

C:\>ping 192.168.1.2

Аналогично проверьте взаимодействие с другими компьютерами сети и введите их IP- адреса:

C:\>ping 192.168.1.3

C:\>ping 192.168.1.4.

Результат выполнения данной команды приведен на рисунке 7.

Аналогичную проверку можно осуществить и на других компьютерах сети.

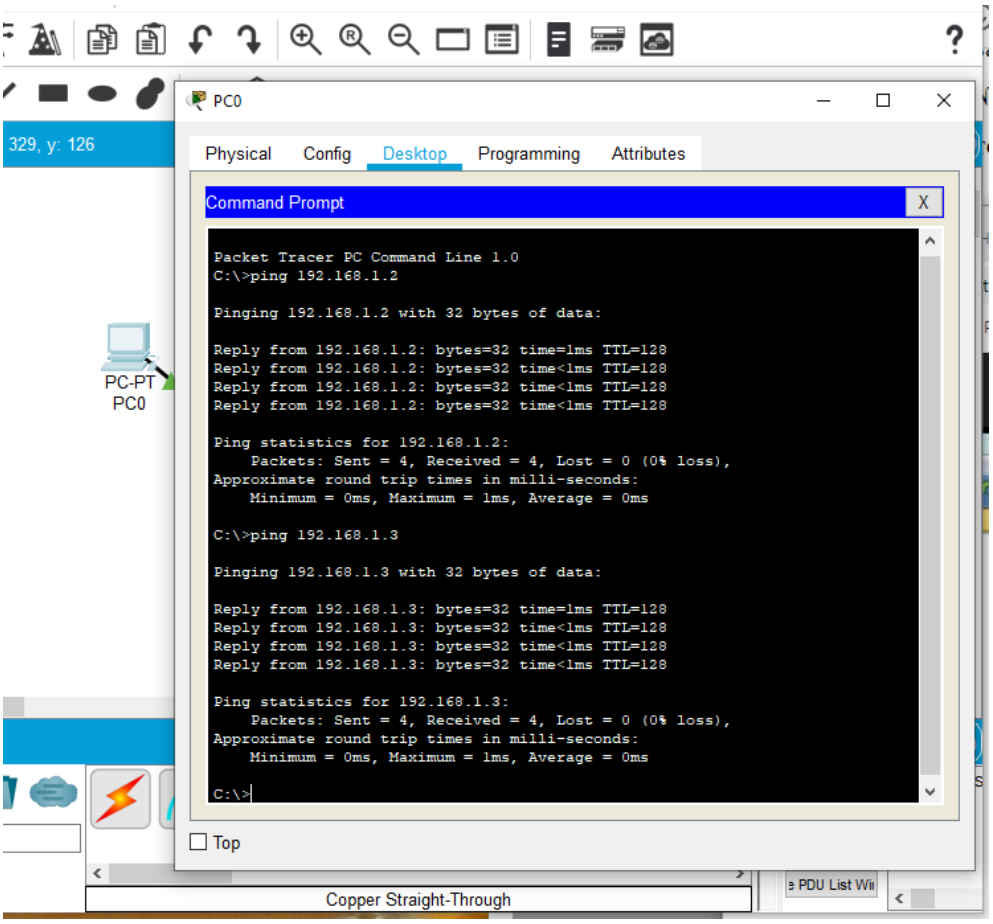


Рисунок 7 – Проверка связности построенной сети

Теперь построим вторую сеть на концентраторе (Hub). Чтобы ускорить процесс создания сети, выделяем 4 компьютера (рис. 8), нажимаем Ctrl и перетаскиваем их вниз (рис. 9). Далее заходим во вкладку Hubs и выбираем концентратор (рис. 10).

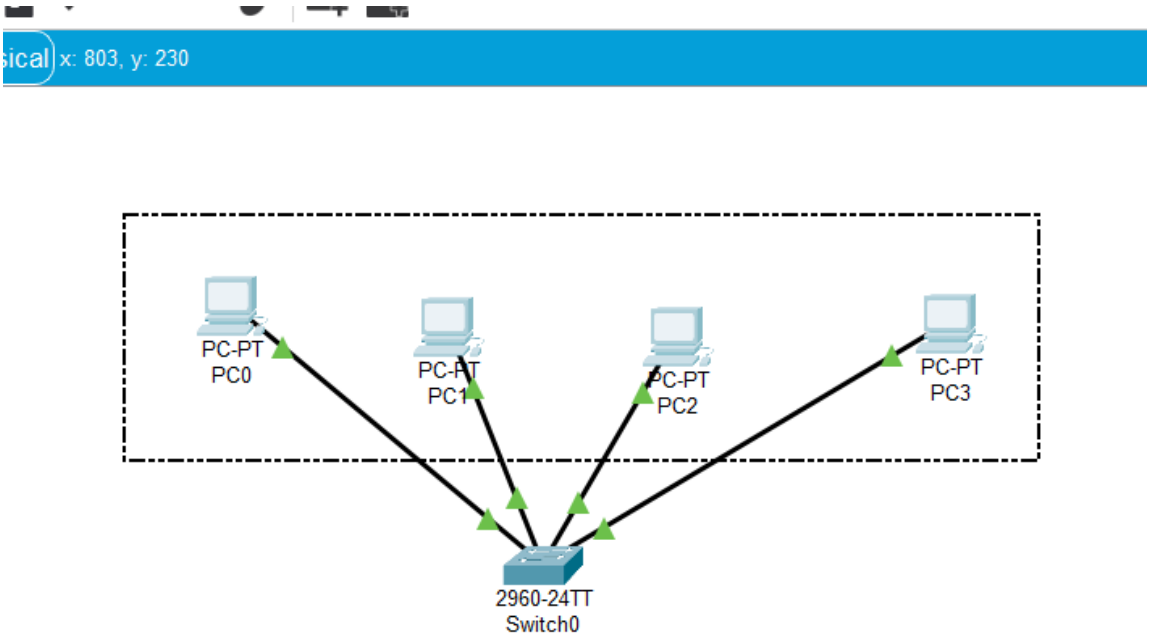


Рисунок 8 – Выделяем компьютеры для создания второй сети

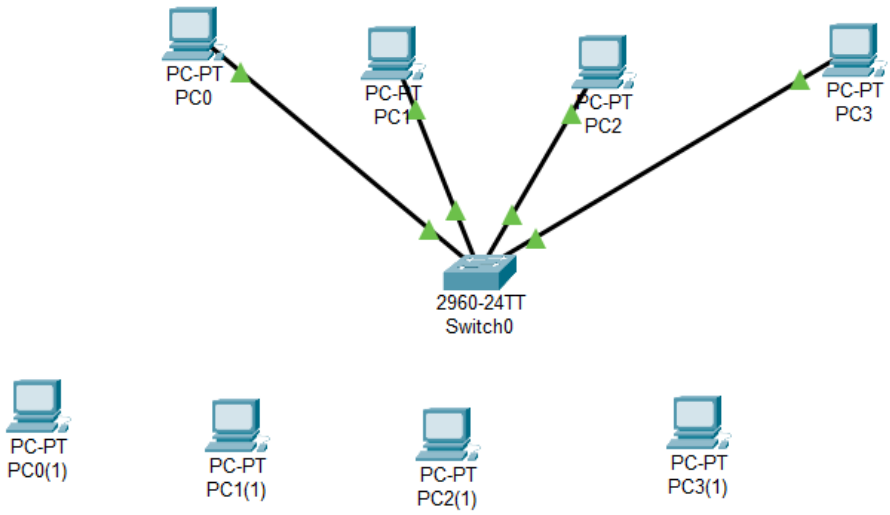
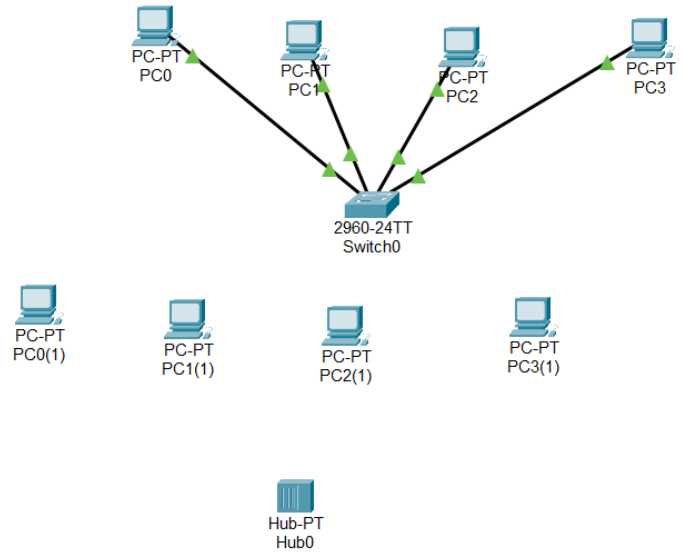


Рисунок 9 – Четыре вновь созданных компьютера для второй сети



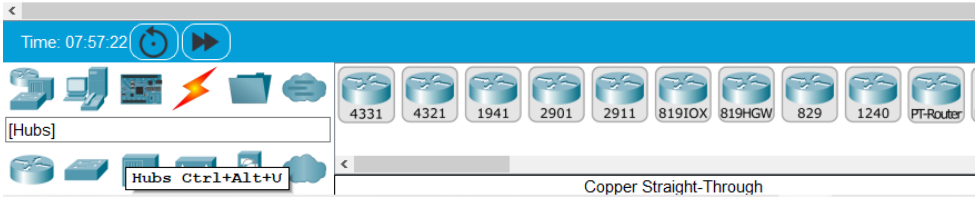


Рисунок 10 – Выбор концентратора (Hub) для второй сети

Далее соединяем компьютеры с концентратором с помощью кабеля. В Cisco Packet Tracer можно автоматически выбрать кабель (рис. 11). Выбираем автоматический выбор и подключаем компьютеры к концентратору (рис.12).

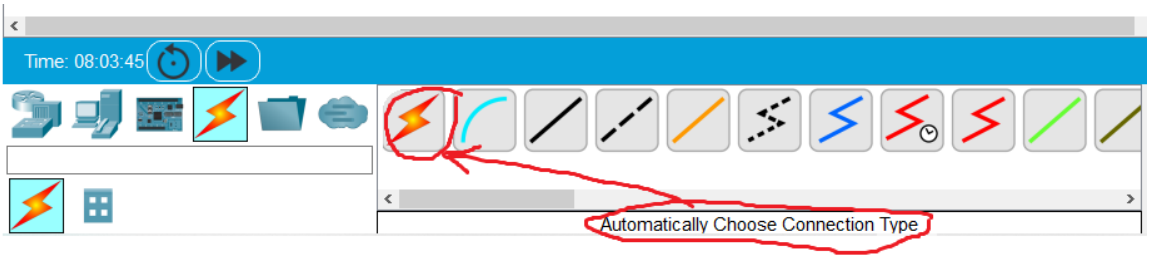


Рисунок 11 – Автоматический выбор кабеля в Cisco Packet Tracer

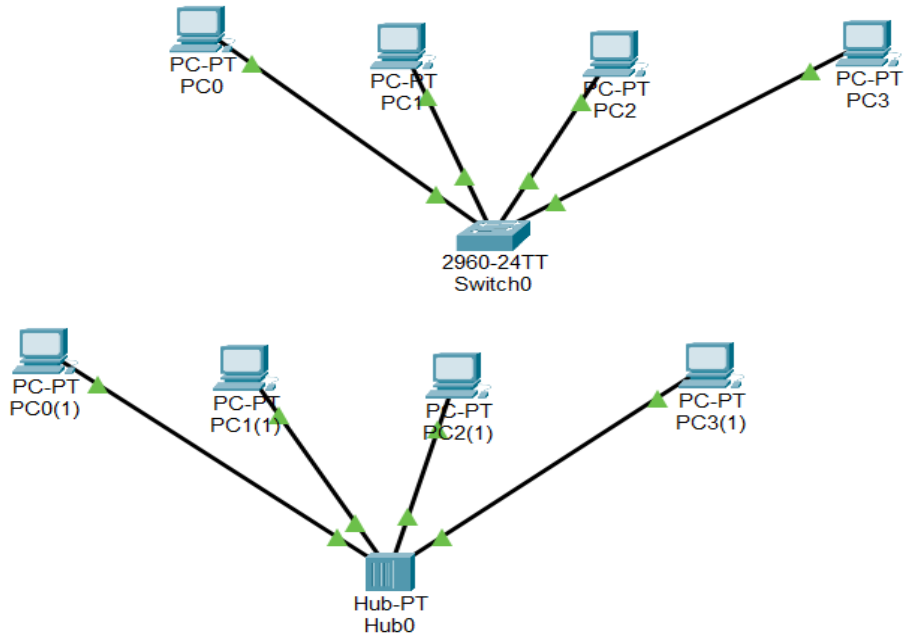


Рисунок 12 – Построение двух компьютерных сетей

Здесь линии сразу загораются зеленым цветом. Проверим работоспособность второй сети (рис. 13). Сеть успешно функционирует.

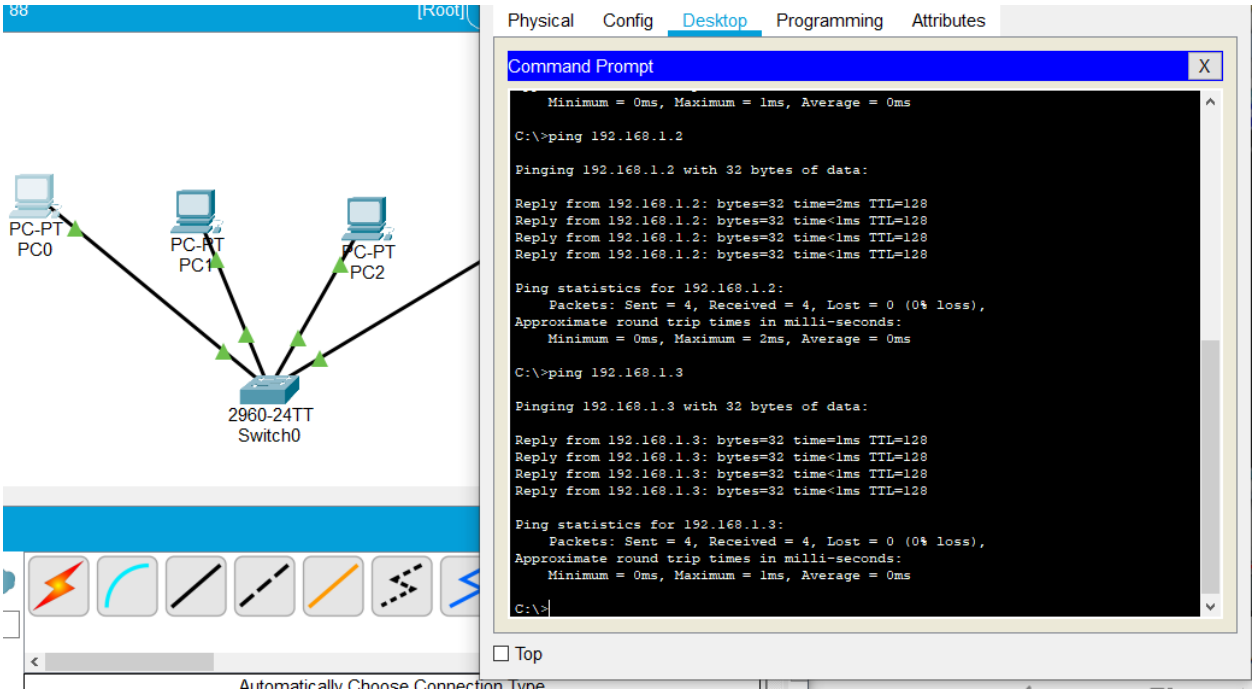


Рисунок 13 – Проверка работоспособности второй сети

Для визуализации процесса прохождения пакета воспользуемся функцией Add Simple PDU. Предположим, что компьютер PC0 отправляет пакет на компьютер PC1. То же самое будет происходить и во второй сети.

Для того, чтобы задать маршрут следования пакета необходимо нажать сначала на PC0, а затем на PC1, т.е. пакеты будут отправлены от компьютера PC0 к PC1.

Далее переходим во вкладку Simulation Mode (Режим моделирования), перетаскиваем синий ползунок влево и можем детально просмотреть передвижение пакета. Переходим во вкладку Play Controls и нажимаем на кнопку Capture then forward для анимации пакета (рис. 14). Пакет начинает передвигаться от PC0 к PC1. Пакет в первой сети приходит на коммутатор, а во второй сети на концентратор. После этого опять нажимаем на кнопку Capture then forward и пакет продолжает свое движение.

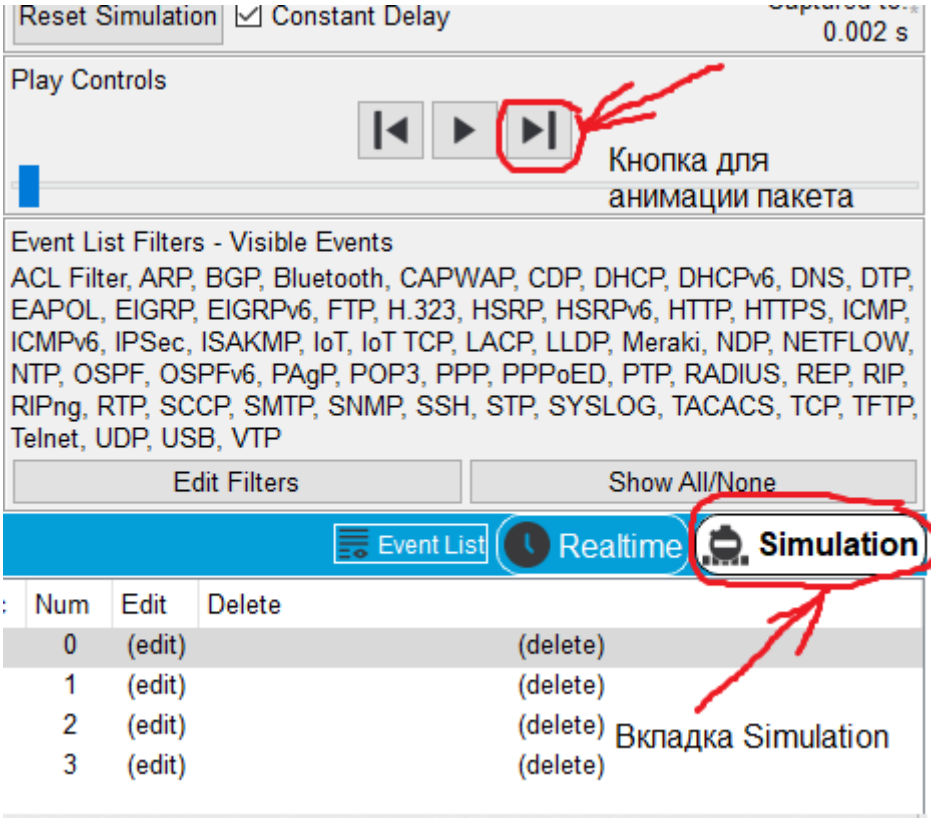


Рисунок 14 – Управление передвижением пакета

На рисунке 15 показано, что коммутатор отправляет пакет только в нужный порт, а концентратор (Hub) во все доступные порты, кроме порта источника. Вторая схема является небезопасной, так как если на компьютерах PC2 и PC3 будут находиться злоумышленники, то они могут получать информацию, которая им не предназначена.

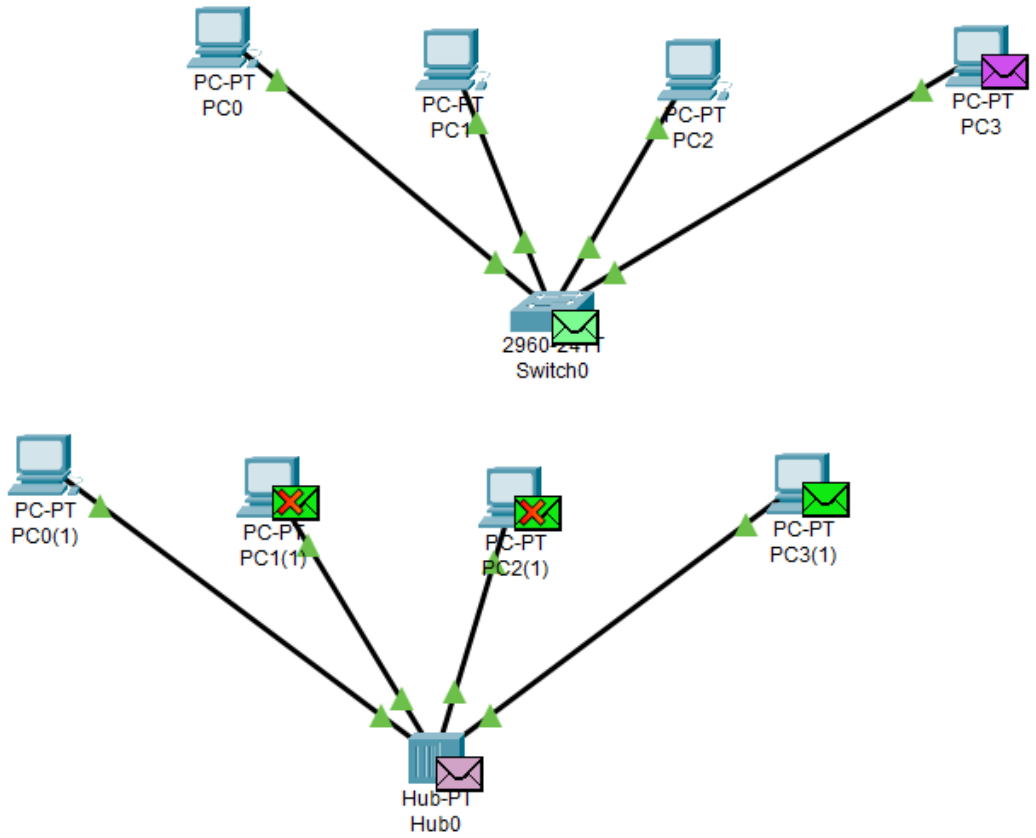


Рисунок 15 – Сравнение принципов работы первой и второй сетей

Мы можем заглянуть в пакет и посмотреть его содержимое (рис.16). Для этого надо на него нажать левой кнопкой мыши.

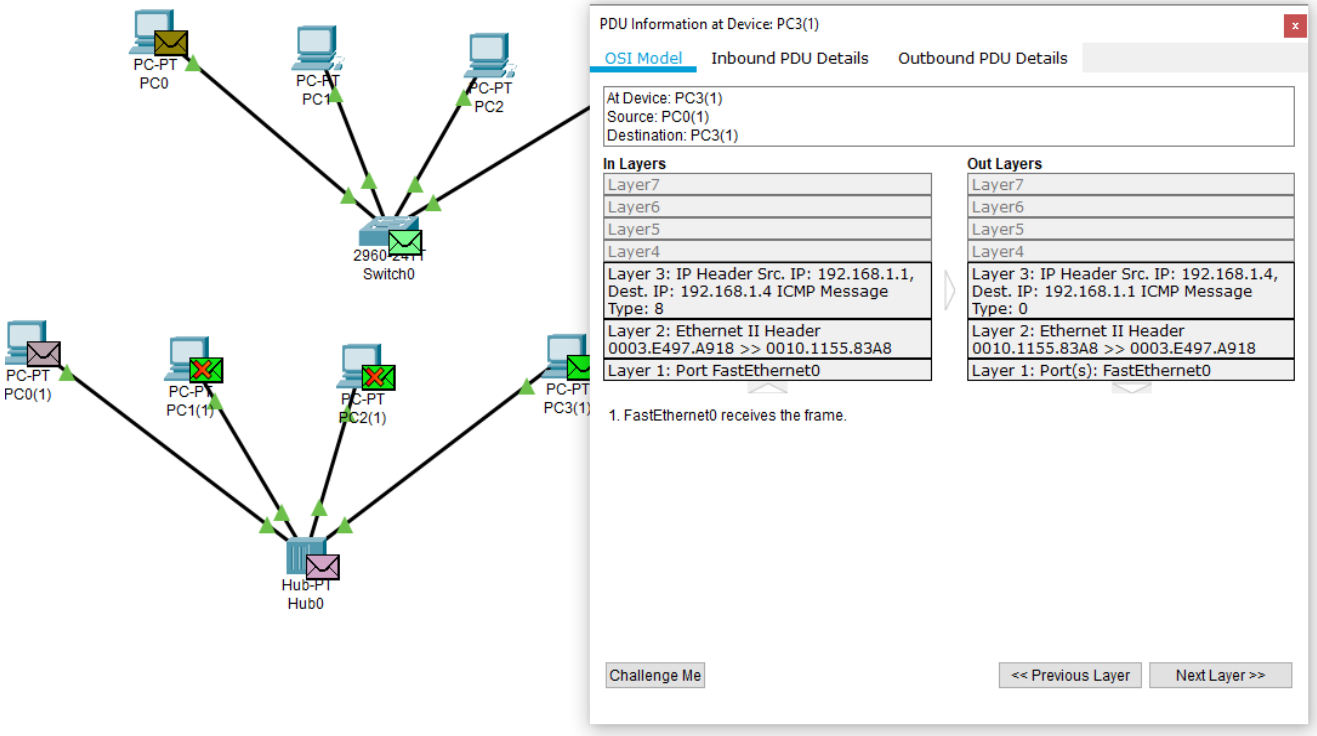


Рисунок 16 – Содержимое отправленного пакета

Теперь компьютер PC4 отправляет обратно пакет PC0. При отправке производим аналогичные действия с помощью кнопки Capture then forward для анимации пакета (рис. 14). Происходит точно такое же явление. Т.е. коммутатор отправляет пакет в определенный порт, куда подключен PC0, а концентратор (hub) во все доступные порты. Убедитесь в этом самостоятельно.

Содержание отчета

В индивидуальном отчёте должны быть указаны цель, задание, представлены необходимые снимки экрана и пояснения к ним. Следует проанализировать полученные данные и дать ответы на контрольные вопросы.

Контрольные вопросы

1. В чем отличие коммутатора от концентратора?
2. Для чего нужна таблица коммутации?
3. Как происходит заполнение таблицы коммутации?
4. Что представляет собой MAC- адрес?
5. Почему строить сеть на концентраторе небезопасно?
6. Как можно посмотреть содержимое пакета с помощью Cisco Packet Tracer?
7. Как проверить работоспособность спроектированной сети в Cisco Packet Tracer?
8. Как быстро построить вторую сеть в Cisco Packet Tracer?
9. Какие устройства относятся к физическим средствам физического уровня?
10. Какие устройства относятся к физическим средствам канального уровня?
11. Какие устройства относятся к физическим средствам сетевого уровня?
12. Сравните содержимое отправленных пакетов на концентраторе и коммутаторе относительно модели OSI.

Практическая работа №5. Изучение принципов работы маршрутизаторов

Цель работы

Изучить принципы работы маршрутизаторов.

Задание

1. Ознакомиться с правилами составления таблицы маршрутизации;
2. Ознакомиться с локальными и глобальными сетями;
3. Ответить на вопросы.

Функции маршрутизаторов

Маршрутизация является функцией третьего уровня модели OSI. Основным устройством, отвечающим за осуществление процесса маршрутизации, является **маршрутизатор (**Router**).** Процесс прокладывания наилучшего маршрута к адресату назначения получил название **маршрутизация.**

Функционирование маршрутизаторов происходит по правилам сетевого протокола IP – Internet Protocol. Заголовок пакета содержит сетевые IP-адреса узла назначения и узла источника. Для определения наилучшего пути передачи данных через связываемые сети, маршрутизаторы строят таблицы маршрутизации и обмениваются сетевой маршрутной информацией с другими маршрутизаторами. Маршрутизаторы принимают решения, базируясь на сетевых логических адресах (IP-адресах) в заголовке пакета и обращаясь к таблицам маршрутизации. Администратор может создавать статические маршруты и поддерживать таблицы маршрутизации вручную. Однако большинство таблиц маршрутизации создается и поддерживается динамически, за счет использования протоколов маршрутизации (Routing Protocol), которые позволяют маршрутизаторам автоматически обмениваться информацией о сетевой топологии друг с другом.

Главными функциями маршрутизаторов являются:

- выбор наилучшего пути для пакетов к адресату назначения;

- продвижение принятого пакета с входного интерфейса на соответствующий выходной интерфейс.

Процесс прокладывания маршрута происходит последовательно от одного маршрутизатора к другому. При этом каждый маршрутизатор анализирует сетевую часть адреса узла назначения в заголовке поступившего пакета.

Оценка наилучшего пути производится на основе метрики. Например, метрика может учитывать количество маршрутизаторов на пути к адресату, скорость линий связи и т.д.

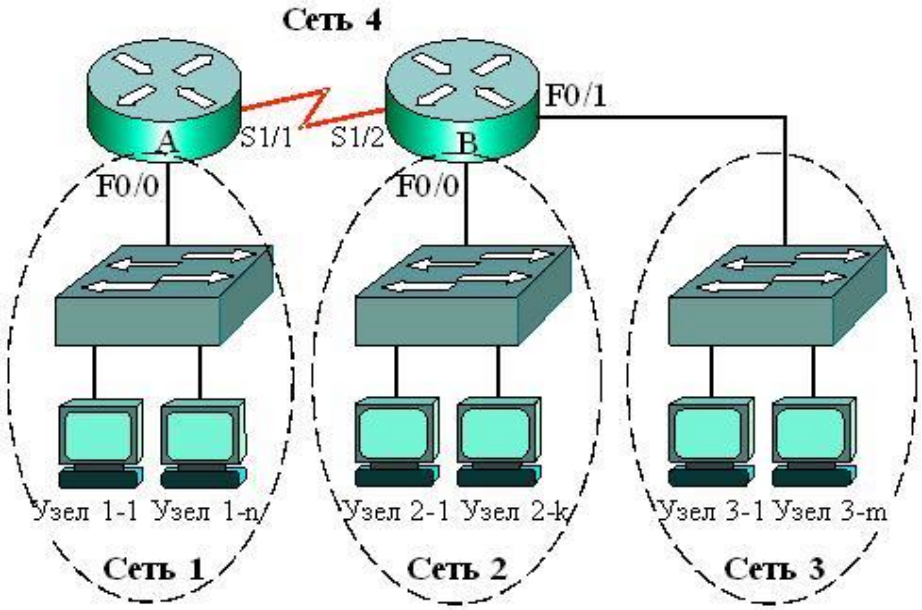


Рисунок 1 – Принцип маршрутизации в сетях

Каждый маршрутизатор создает таблицу маршрутизации, где задаются:

- источник созданного маршрута;
- адрес сети назначения, маска;
- административное расстояние или другой аналогичный параметр;
- значение метрики;
- адрес следующего перехода;
-выходной интерфейс маршрутизатора на пути к сети назначения.

```
Командная строка

C:\Documents and Settings\VASIN>netstat -r

Таблица маршрутов
===========================================================================
Список интерфейсов
0x1 ........................... MS TCP Loopback interface
0x2 ...00 24 8c 4c 4e a6 ...... Realtek RTL8168C(P)/8111C(P) PCI-E Gigabit Ether
net NIC - ¦ьэшяюЁЄ яырэшЁют·шър ярък€ют
0x3 ...00 23 4e df bd aa ...... 11b/g Wireless LAN Mini PCI Express Adapter III
- ¦ьэшяюЁЄ яырэшЁют·шър ярък€ют
0x20005 ...00 53 45 00 00 00 ...... WAN (PPP/SLIP) Interface
===========================================================================
===========================================================================
Активные маршруты:
Сетевой адрес           Маска сети      Адрес шлюза       Интерфейс  Метрика
          0.0.0.0          0.0.0.0     10.225.75.13    10.225.75.13       1
     10.225.75.13  255.255.255.255        127.0.0.1       127.0.0.1      50
     10.225.254.6  255.255.255.255     10.225.75.13    10.225.75.13       1
   10.255.255.255  255.255.255.255     10.225.75.13    10.225.75.13      50
        127.0.0.0        255.0.0.0        127.0.0.1       127.0.0.1       1
      169.254.0.0      255.255.0.0  169.254.133.190  169.254.133.190      20
  169.254.133.190  255.255.255.255        127.0.0.1       127.0.0.1      20
  169.254.255.255  255.255.255.255  169.254.133.190  169.254.133.190      20
        224.0.0.0        240.0.0.0  169.254.133.190  169.254.133.190      20
        224.0.0.0        240.0.0.0     10.225.75.13    10.225.75.13       1
  255.255.255.255  255.255.255.255     10.225.75.13    10.225.75.13       1
  255.255.255.255  255.255.255.255  169.254.133.190  169.254.133.190      1
  255.255.255.255  255.255.255.255  169.254.133.190               3      1
Основной шлюз:        10.225.75.13
===========================================================================
Постоянные маршруты:
  Отсутствует

C:\Documents and Settings\VASIN>
```

Рисунок 2 - Пример таблицы маршрутизации

Если в таблице маршрутизации не создан путь к сети назначения пакета, то маршрутизатор отбрасывает такой пакет.

Локальные и глобальные сети

Локальные сети (Local Area Network – **LAN**) функционируют в пределах ограниченного географического пространства (в пределах комнаты, этажа, здания или группы близко расположенных зданий). Совокупность нескольких локальных сетей, объединенных линиями связи, называют составной, распределенной или **глобальной** сетью **(**Wide Area Network – **WAN)**. Глобальные сети обеспечивают связь между далеко расположенными локальными сетями, удаленными пользователями (рис. 3).

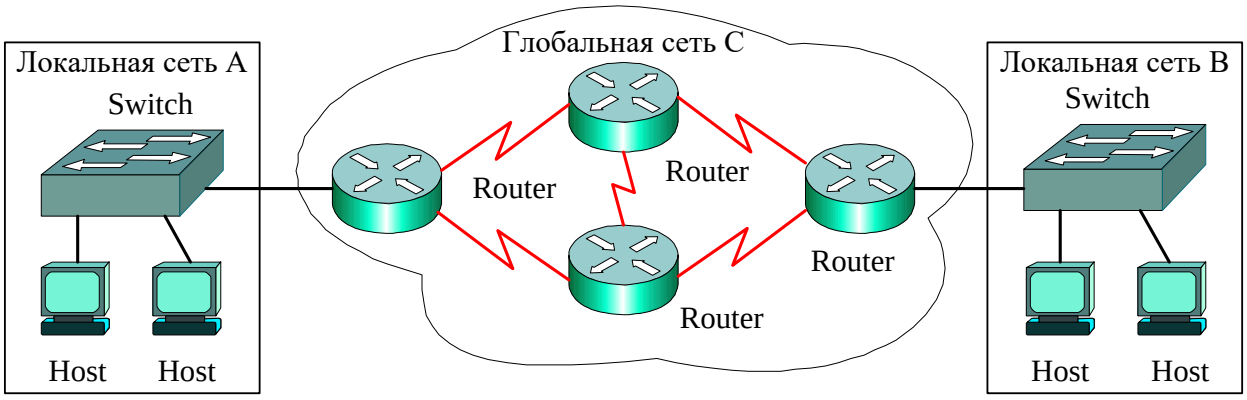


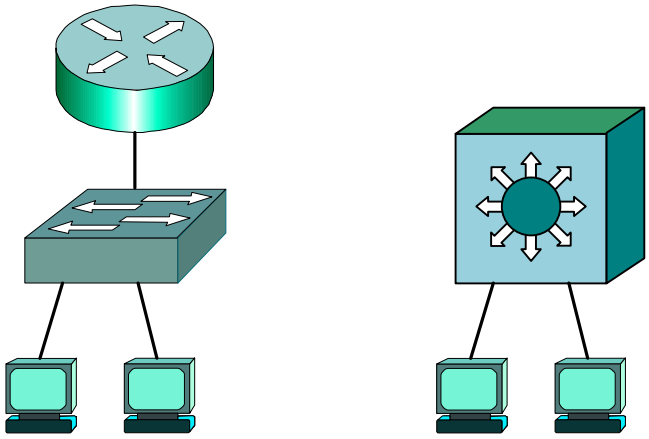
Рисунок 3 - Локальные и глобальные сети

Маршрутизаторы имеют интерфейсы как локальных, так и глобальных соединений. К локальным сетям, созданным на коммутаторах, маршрутизатор присоединен через интерфейсы, которые на рисунке 1 обозначены через F0/0 и F0/1. Так F0/1 что означает: интерфейс FastEthernet, слот 0, порт 1; (слот – объединение портов). Глобальные соединения представлены последовательными или серийными (serial) интерфейсами S0/1, S0/2.

Коммутаторы третьего уровня

Во многих сетях пакетной коммутации используются комбинации устройств: маршрутизатор, коммутатор, конечные узлы (рис. 4 а). В этом случае коммутатор реализует коммутацию и фильтрацию кадров локальной сети на основе MAC-адресов, т.е. выполняет функции устройства второго уровня модели OSI. Маршрутизацию и передачу пакетов между сетями выполняет маршрутизатор, который характеризуется широким спектром функ-

ций. Коммутатор характеризуется большим количеством портов и высокой производительностью.



а) б)

Рисунок 4 - Элементы сети

Поэтому в новых сетевых элементах (коммутаторах-маршрутизаторах) объединили функции коммутатора и маршрутизатора (рис. 4 б). Такое устройство получило название коммутатора уровня 3 модели OSI. Коммутатор уровня 3 пересылает данные, базируясь на IP- и MAC-адресах назначения. Пересылка данных происходит с высокой скоростью, характерной для классических коммутаторов уровня 2.

Контрольные вопросы

1. Назовите основные функции маршрутизатора.
2. Какая часть IP-адреса класса B 152.12.3.8 является номером сети?
3. Что такое метрика маршрута?
4. Дайте определение локальной сети.
5. Дайте определение глобальной сети.
6. Какие функции выполняет коммутатор третьего уровня?
7. Что обозначает интерфейс на маршрутизаторе F0/0?
8. Какие интерфейсы на маршрутизаторе используются для объединения локальных сетей в глобальную сеть?
9. Что представляет собой таблица маршрутизации?
10. Дайте определение маршрутизации.

Лабораторная работа № 4. Построение простейшей компьютерной сети с использованием маршрутизатора и коммутатора

Цель работы

Построить простейшую компьютерную сеть с использованием маршрутизатора и коммутатора с помощью сетевого симулятора Cisco Packet Tracer.

Задание

1. Запустить Cisco Packet Tracer.
2. Собрать необходимую топологию сети, запустить и настроить виртуальное оборудование.
3. Согласно пунктам выполнения лабораторной работы, сделать необходимые снимки экрана. Изучить полученную информацию и оформить ее в соответствии с требованиями раздела «Содержание отчета».

Краткая теория

Ниже перечислены основные служебные команды, использующиеся в данном учебно-методическом пособии:

ipconfig – команда, выводящая основную сетевую информацию ПК, сервера (IP-адрес, маску подсети, шлюз по умолчанию);

ping A.B.C.D – команда, посылающая эхо-запрос на IP-адрес A.B.C.D, используется для тестирования сетевой связности устройств;

enable – команда, предоставляющая доступ к привилегированному режиму в оборудовании Cisco;

configure terminal – команда, предоставляющая режим глобальной конфигурации в оборудовании Cisco;

no shutdown – команда, переводящая порт в активное состояние (на коммутаторах все порты изначально активны), в оборудовании Cisco;

exit – команда, возвращающая в предыдущий раздел конфигурирования в оборудовании Cisco;

write memory – команда, записывающая все изменения в постоянную память устройства в оборудовании Cisco;

show running-config – команда, позволяющая просмотреть прошивку оборудования, основные настройки портов и различных технологий в оборудовании Cisco.

Порядок выполнения работы

Соберите сетевую топологию согласно рисунку 1. Топология содержит 2 ПК, маршрутизатор (Cisco 1841) и коммутатор (Cisco 2960). Для этого выберите из необходимых вкладок сетевое оборудование, зажмите его значок и перенесите в рабочую область согласно рисунку 1.

Рисунок 1 - Подготовка сетевой топологии

Выберите тип соединения, нажмите на PC0, затем на нужный интерфейс (FastEthernet0), нажмите на коммутаторе и из выпадающего списка выберите требуемый порт (например, FastEthernet 0/1) как на рисунке 2. Повторите для других устройств. Соедините их согласно таблице 1.

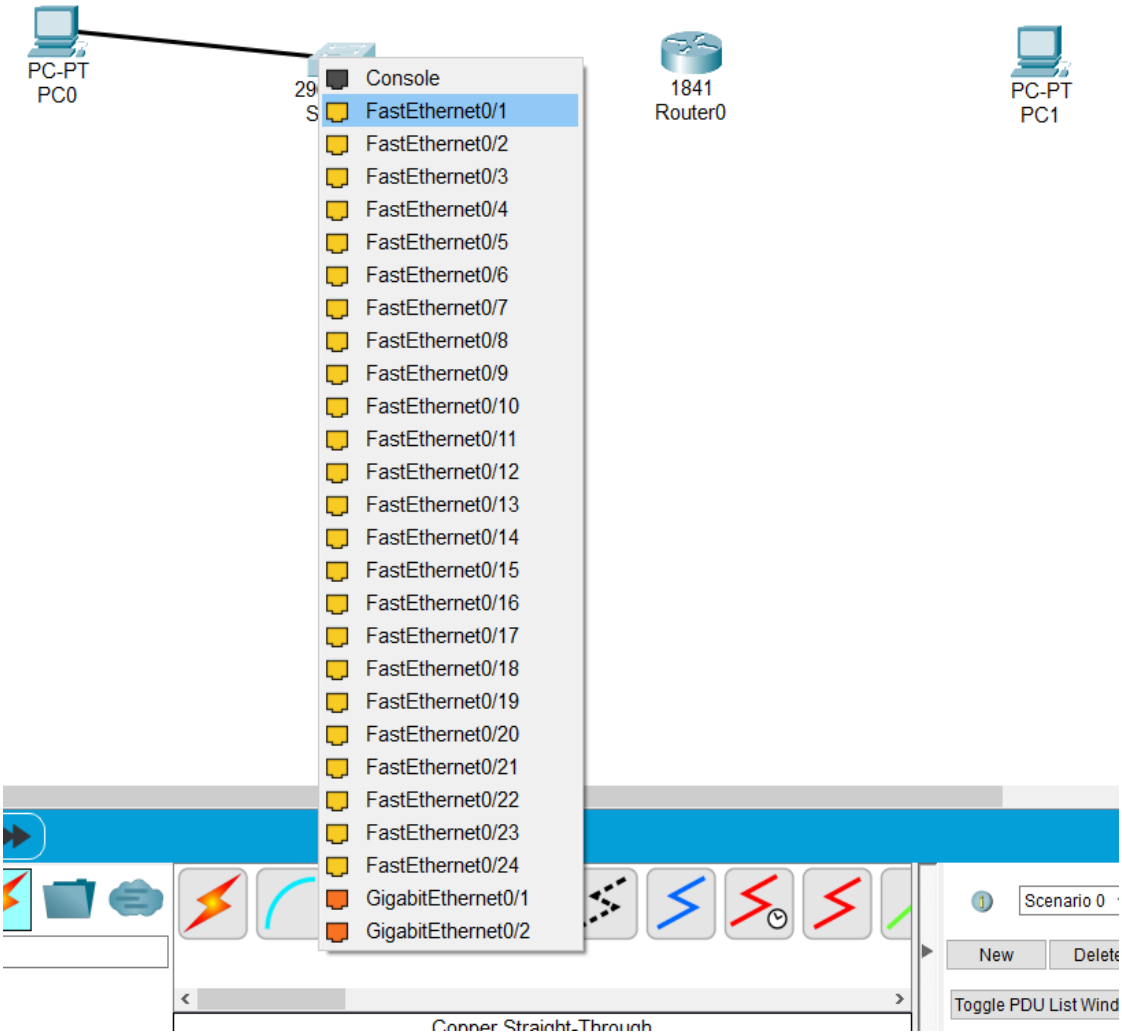


Рисунок 2 - Соединение сетевых устройств и выбор нужного интерфейса

В результате необходимо собрать топологию согласно рисунку 3. Сделайте снимок экрана. Обратите внимание на цвет интерфейсов. В каком они состоянии?

Рисунок 3 - Топология сети

Назначьте всем устройствам сетевые адреса согласно таблице 1.

Таблица №1 Сетевые адреса устройств

Сетевой элемент	Интерфейс	IP-адрес	Маска подсети	Шлюз по умолчанию
Cisco 1841	FastEthernet0/0	192.168.1.1	255.255.255.0	-
	FastEthernet0/1	192.168.0.1	255.255.255.0	-
PC0	FastEthernet0	192.168.1.3	255.255.255.0	192.168.1.1
PC1	FastEthernet0	192.168.0.3	255.255.255.0	192.168.0.1

Для назначения сетевых адресов компьютерам, нажмите левой кнопкой мыши на устройстве и перейдите в закладку Desktop (рис. 4), а затем нажмите на IP Configurations.

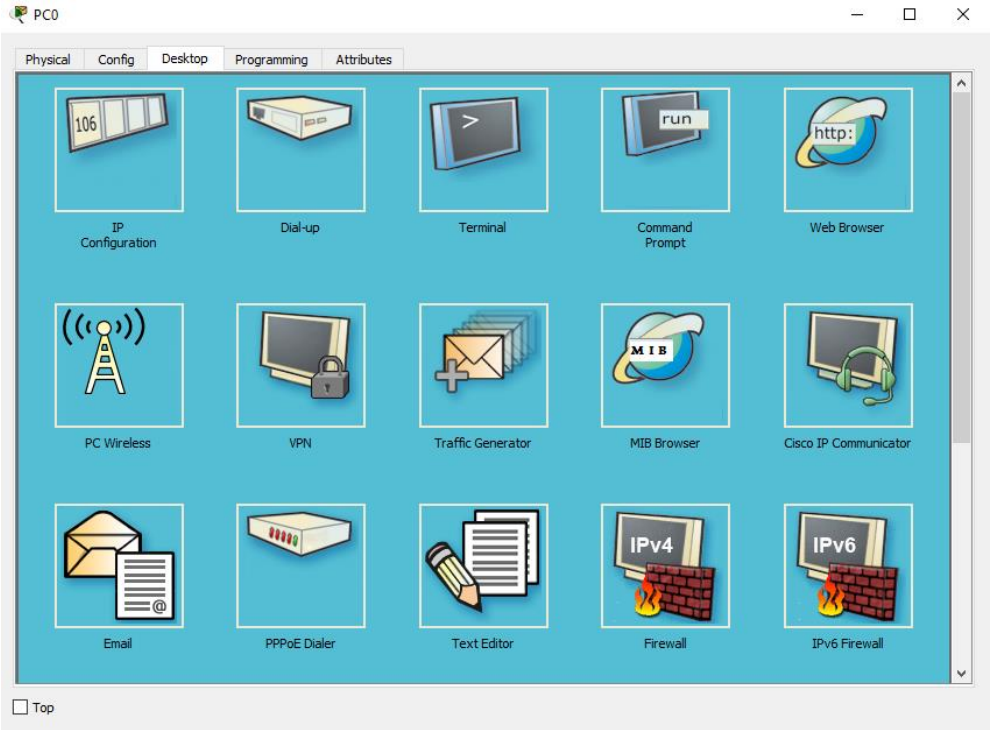


Рисунок 4 - Закладка Desktop PC0

Введите IP-адрес, маску подсети и шлюз по умолчанию, как показано на рисунке 5 для PC0.

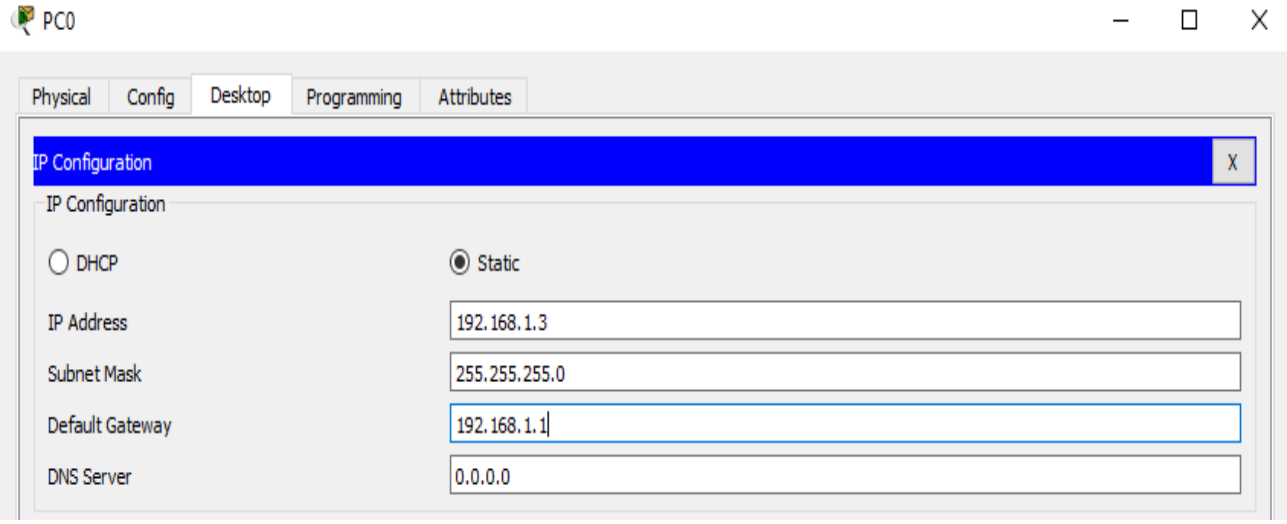


Рисунок 5 - Конфигурация PC0

Необходимо удостовериться в правильности введенных настроек. Для этого один раз нажмите левой кнопкой мыши на устройстве и перейдите в закладку Desktop, а затем нажмите на Command Prompt (рисунок 5). Введите команду:

C:\>ipconfig

Результаты показаны на рисунке 6. Повторите для PC1 (рис. 7).

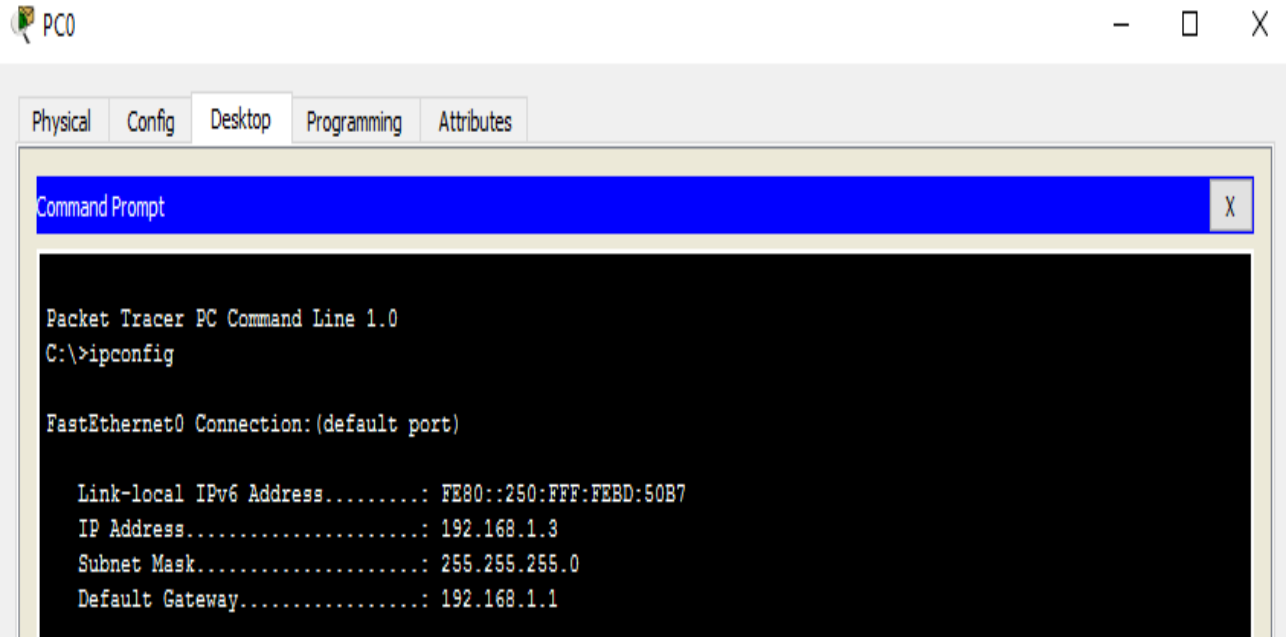


Рисунок 6 - Проверка конфигурации компьютера PC0

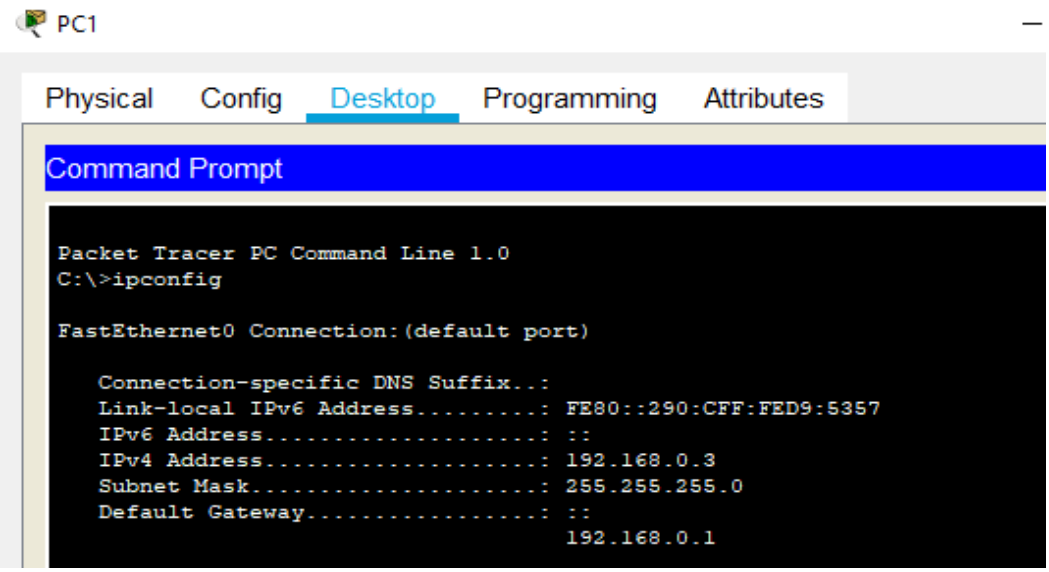


Рисунок 7. Проверка конфигурации PC1

Проверьте сетевую связность между компьютерами, для этого введите на PC0 команду (рисунок 8):

C:\>ping 192.168.0.3

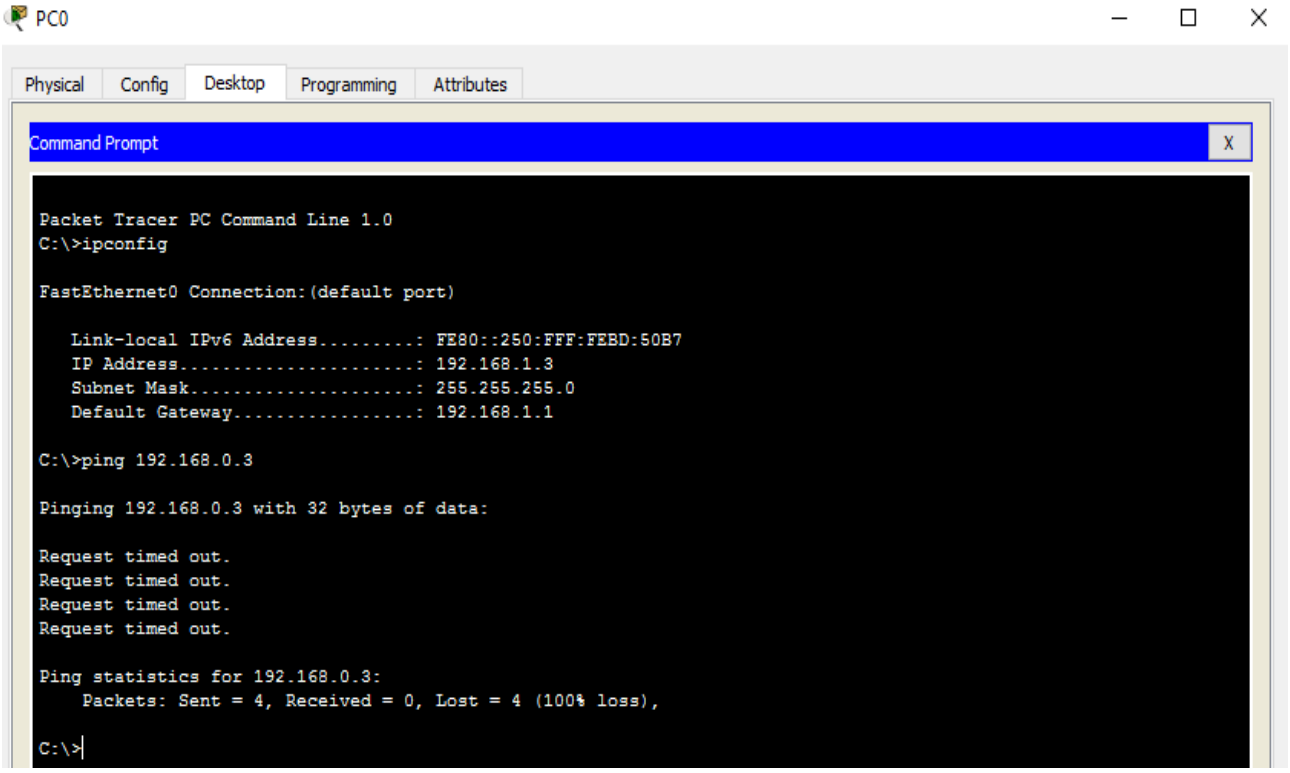


Рисунок 8 - Отправка эхо-запроса с PC0 на PC1

Сделайте снимок экрана. Почему эхо-запросы с помощью команды **ping** не прошли?

Настройте маршрутизатор, для этого один раз нажмите на устройство и перейдите во вкладку CLI, на задаваемый вопрос введите **no**, затем вводите следующие команды (для завершения команды нажмите клавишу **Tab**):

Router>enable
Router#
Router#configure terminal
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(config-if)#exit
Router(config)#interface fastEthernet 0/1
Router(config-if)#ip address 192.168.0.1 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#end
Router#write memory

Убедитесь в правильности сделанных настроек и подведите курсор к маршрутизатору (рис. 9).

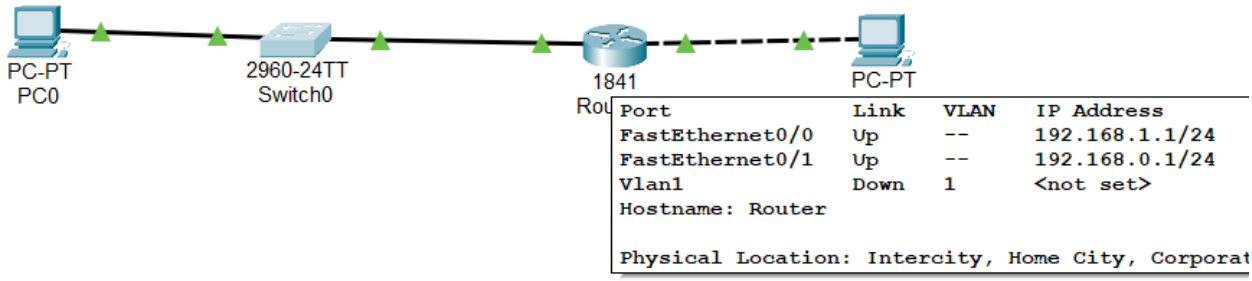


Рисунок 9 - Настройки интерфейсов маршрутизатора

На рисунке видно, что изменился цвет состояния интерфейсов. Почему это произошло?

Проверьте сетевую связность между компьютерами, для этого введите на PC0 команду (рисунок 10):

C:\>ping 192.168.0.3

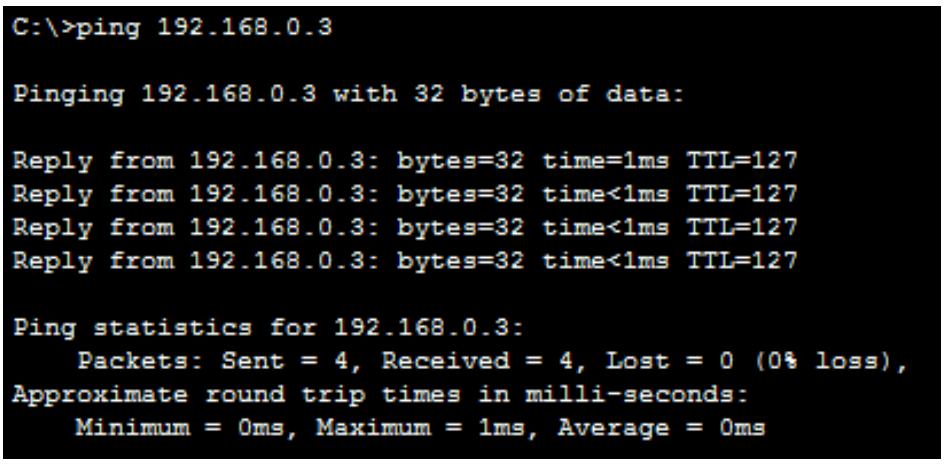


Рисунок 10 - Отправка эхо-запроса с PC0 на PC1

Успешно ли выполнен эхо-запрос с помощью команды **ping**? Почему?

Выведите в CLI маршрутизатора сведения об интерфейсах (рисунок 11). Для этого введите команду:

Router#show ip interface brief

```
Router#show  ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/0        192.168.1.1     YES manual up                    up
FastEthernet0/1        192.168.0.1     YES manual up                    up
Vlan1                  unassigned      YES unset  administratively down down
Router#
```

Рисунок 11 - Краткая информация о состоянии интерфейсов маршрутизатора

ARP (Address Resolution Protocol — протокол определения адреса) — протокол в компьютерных сетях, предназначенный для определения MAC-адреса по известному IP-адресу. Проанализируйте работу протокола ARP на маршрутизаторе (рисунок 12):

Router#show arp

```
Router#show arp
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  192.168.0.1            -   0050.0F8D.6202  ARPA   FastEthernet0/1
Internet  192.168.0.3            4   00E0.B0AD.9A18  ARPA   FastEthernet0/1
Internet  192.168.1.1            -   0050.0F8D.6201  ARPA   FastEthernet0/0
Internet  192.168.1.3            4   0050.0FBD.50B7  ARPA   FastEthernet0/0
Router#
```

Рисунок 12 - Таблица информации по работе ARP

Выведите в CLI коммутатора сведения об интерфейсах (рисунок 13):

Switch>enable

Switch#show ip interface brief

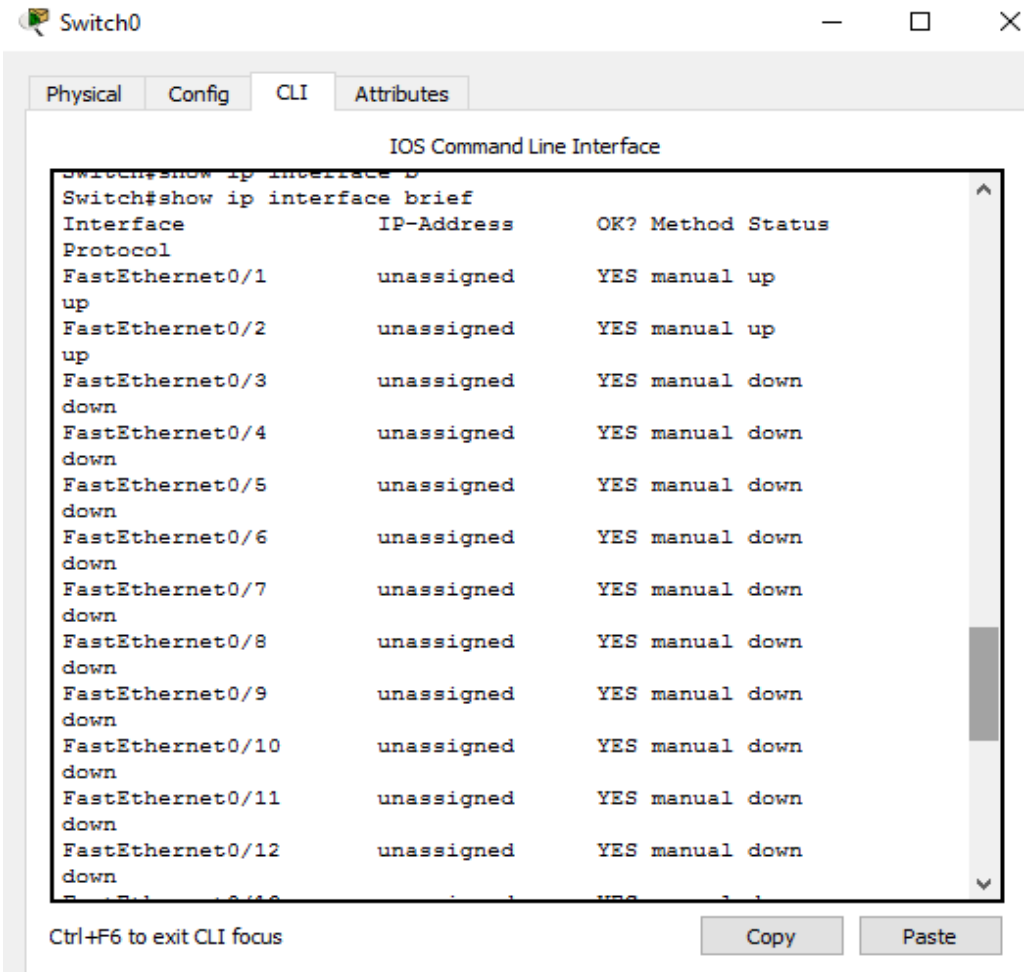


Рисунок 13 - Краткая информация о состоянии интерфейсов коммутатора

В чем отличие краткой информации об интерфейсах коммутатора и маршрутизатора?

Содержание отчета

В индивидуальном отчёте должны быть указаны цель, задание, представлены необходимые снимки экрана и пояснения к ним. Следует проанализировать полученные данные и дать ответы на контрольные вопросы.

Контрольные вопросы

1. Из какого количества бит состоит IP- адрес?
2. Какое максимальное значение любого из октетов IP-адреса?
3. Какой комбинации в двоичной форме соответствует IP-адрес 192.165.3.8?
4. Сколько адресов узлов может быть использовано в сети класса С?

5. Напишите маску подсети класса B.
6. Вычислите адрес сети класса A по известному IP-адресу 120.7.3.6?
7. Какие две части адреса сетевого уровня используют маршрутизаторы для передачи данных через сеть?
8. Назовите функцию команды **ipconfig**?
9. Укажите функцию команды **enable**?
10. Какая команда переводит порт в активное состояние?
11. Какая команда предоставляет режим глобальной конфигурации в оборудовании Cisco?
12. Какая команда возвращает в предыдущий раздел конфигурирования в оборудовании Cisco?

Практическая работа №6. Изучение технологии виртуальных локальных сетей VLAN (Virtual Local Area Network)

Цель работы

Изучить технологию VLAN.

Задание

1. Ознакомиться с преимуществами технологии VLAN;
2. Изучить, как могут быть построены сети VLAN ;
3. Ответить на вопросы.

Виртуальными локальными сетями VLAN (Virtual Local Area Network) называются локальные сети, созданные на единой аппаратной базе (т. е. на коммутаторах, соединенных между собой физическими каналами), но логически изолированные друг от друга.

VLAN имеет те же свойства, что и физическая локальная сеть, но позволяет конечным членам группироваться вместе, даже если они не находятся в одной физической сети. Такая организация может быть сделана на основе программного обеспечения вместо физического перемещения устройств.

VLAN дает возможность значительно оптимизировать работу локальной сети за счет разгрузки отдельных ее сегментов от "лишнего" трафика и решить некоторые вопросы безопасности в сети, разграничив доступ пользователей. Сети VLAN имеют следующие преимущества:

- помогает структурировать сеть;
- используется для обеспечения безопасности;
- используют для объединения;
- уменьшает количество широковещательного трафика.

Широковещательный трафик используется для ряда протоколов (ARP, DHCP и т.д.). В случае большой сети широковещательный трафик может привести к нерациональному использованию канала. При организации VLAN, пользователи, находящиеся в разных сегментах, не будут получать широковещательные кадры, которые предназначены пользователям других VLAN.

С помощью технологии VLAN можно создавать рабочие группы, основываясь на функциональности, а не на физическом расположении сегментов. Она позволяет администратору логически создавать, группировать и перегруппировывать сетевые сегменты без изменения физической инфраструктуры и отсоединения пользователей и серверов. VLAN обеспечивает дополнительные преимущества для безопасности. Пользователи одной рабочей группы не могут получить доступ к данным другой группы, потому что каждая VLAN – это закрытая и логически определенная группа.

Представьте компанию, в которой отдел кадров, работающий с конфиденциальной информацией, расположен на трех этажах здания. Инженерный департамент и отдел Маркетинга также размещаются на трех этажах (рис. 1). Каждый этаж в здании обеспечен сетью Ethernet средствами этажных коммутаторов: по одному коммутатору на этаж.

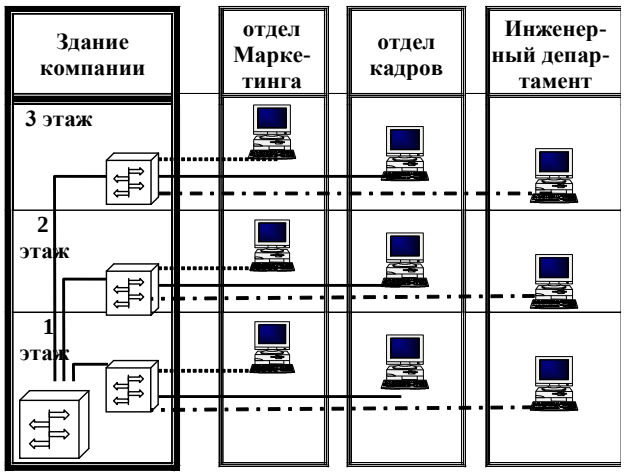


Рисунок -1 Пример построения VLAN для компании

Используя технологию VLAN, работники Инженерного отдела и отдела Маркетинга могут быть расположены на всех трех этажах здания, а их ПК будут входить в состав двух VLAN (VLAN1, VLAN2). Сотрудники отдела кадров, которые также размещаются на всех трех этажах, будут использовать ПК, входящие в состав VLAN3. Сетевой трафик, создаваемый отделом кадров, будет доступен только сотрудникам этого департамента, а группы инженерного отдела и маркетинга не смогут получить доступ к конфиденциаль-

ным данным отдела кадров. Очевидно, есть другие требования для обеспечения полной безопасности, и VLAN может быть частью общей стратегии сетевой безопасности.

Таким образом, в VLAN группа устройств, имеют возможность взаимодействовать между собой напрямую на канальном уровне, хотя физически при этом они могут быть подключены к разным сетевым коммутаторам. И наоборот, устройства, находящиеся в разных VLAN, невидимы друг для друга на канальном уровне, даже если они подключены к одному коммутатору, и связь между этими устройствами возможна только на сетевом и более высоких уровнях.

По умолчанию на каждом порту коммутатора имеется сеть VLAN1 или VLAN управления. Сеть управления не может быть удалена, однако могут быть созданы дополнительные сети VLAN и этим альтернативным VLAN могут быть дополнительно назначены порты.

У коммутатора может быть два типа портов:

access port используется для подключения оконечных устройств (компьютеры, ноутбуки, IP-телефоны, видеокамеры, сервера и т.д.). Любой кадр, который проходит через access-порт, помечается номером, принадлежащим этому VLAN.

Второй тип портов это **trunk port.** Он необходим для соединения между собой коммутаторов.

Trunk port — порт, передающий трафик одного или нескольких VLAN. По умолчанию в транке разрешены все VLAN. Для того чтобы через соответствующий VLAN в транке передавались данные, как минимум, необходимо чтобы VLAN был активным. Активным VLAN становится тогда, когда он создан на коммутаторе и в нём есть хотя бы один порт в состоянии up/up.

Сети VLAN могут быть определены по:

- номеру порта (наиболее частое использование);
- MAC адресу (редко применяется);
- идентификатору пользователя User ID (очень редко применяется);
- сетевому IP-адресу (редко в связи с ростом использования DHCP).

VLAN, базирующаяся на номере порта, позволяет определить конкретный порт в VLAN. Это наиболее простой и часто используемый метод определения VLAN. VLAN, построенная на портах, применяется в тех случаях, когда рабочие станции используют протокол динамической настройки TCP/IP (DHCP).

Технология VLAN, базирующаяся на MAC адресах, позволяет пользователям находиться в той же VLAN, даже если они перемещаются с одного места на другое. Этот метод требует, чтобы администратор определил MAC-адрес каждой рабочей станции и затем внес эту информацию в коммутатор. Данный метод может вызвать большие трудности при поиске неисправностей, если пользователь изменил MAC-адрес.

Виртуальные сети, базирующиеся на сетевых IP-адресах, позволяют пользователям находиться в той же VLAN, при перемещении их с одного места на другое. Этот метод перемещает VLAN, связывая ее с сетевым IP-адресом рабочей станции для каждого коммутатора, к которому пользователь подключен.

Контрольные вопросы

1. Что такое технология VLAN? Какие ее основные преимущества?
2. Какие типы портов используются при настройке VLAN?
3. Как необходимо настроить коммутаторы для соединения с ПК и с другим коммутатором?
4. Почему компьютеры, подключенные в разные коммутаторы, но находящиеся в одном VLAN, перестают взаимодействовать между собой при исключении этого VLAN из trunk-порта?
5. Какая команда позволяет определить, в каком режиме работает порт коммутатора?
6. Перечислите основные способы назначения VLAN.
7. Что выполняет команда **switchport mode access**?
8. Какую команду необходимо ввести, чтобы назначить trunk-порт?
9. Какая команда позволяет вывести информацию по всем интерфейсам коммутатора?
10. Что позволяет сделать trunk-режим портов?

Лабораторная работа №5. Изучение технологии виртуальных локальных сетей VLAN. Часть 1

Цель работы

Изучить и практически освоить процесс настройки технологии виртуальных локальных сетей VLAN (Virtual Local Area Network) с использованием сетевого симулятора Cisco Packet Tracer. Научиться настраивать порты коммутатора в режимы access.

Задание

1. Ознакомиться с основными понятиями технологии виртуальных локальных сетей VLAN (Virtual Local Area Network);
2. Запустить Cisco Packet Tracer;
3. Собрать необходимую топологию сети, запустить и настроить виртуальное оборудование;
4. Согласно пунктам выполнения лабораторной работы, сделать необходимые снимки экрана. Изучить полученную информацию и оформить ее в соответствии с требованиями раздела «Содержание отчета».

Порядок выполнения работы

Открываем Cisco Packet Tracer. Находим коммутатор 2960. Добавляем его в рабочую область. Затем добавляем четыре персональных компьютера PC0-PC1. Для того чтобы ускорить процесс, можно нажать на клавишу Ctrl, на экране появится крестик. И затем нажимаем этим крестиком в те места, где мы хотим расположить наши компьютеры. В результате получаем следующую топологию сети (рис. 1).

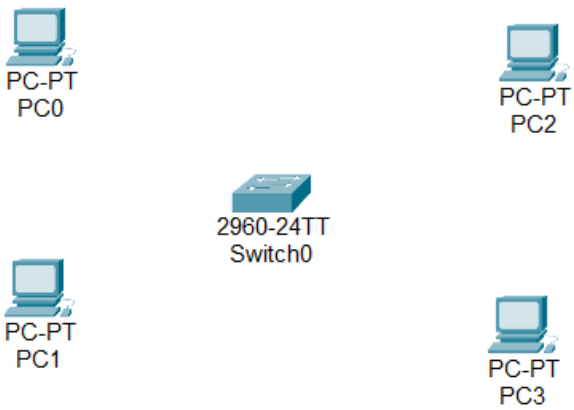


Рисунок 1 - Топология сети

Далее приступаем к соединению между устройствами. Так как здесь соединяются устройства разных уровней модели OSI, то используем прямой кабель. Также зажимаем клавишу Ctrl, нажимаем на значок компьютера и подключаем каждый компьютер. При этом выбираем на коммутаторе необходимые порты FastEthernet. На рисунке 2 показано подключение PC0 к порту FastEthernet 0/1 коммутатора 2960. Аналогично подключаем остальные PC. Коммутатор PC3 подключается к порту FastEthernet 0/4.

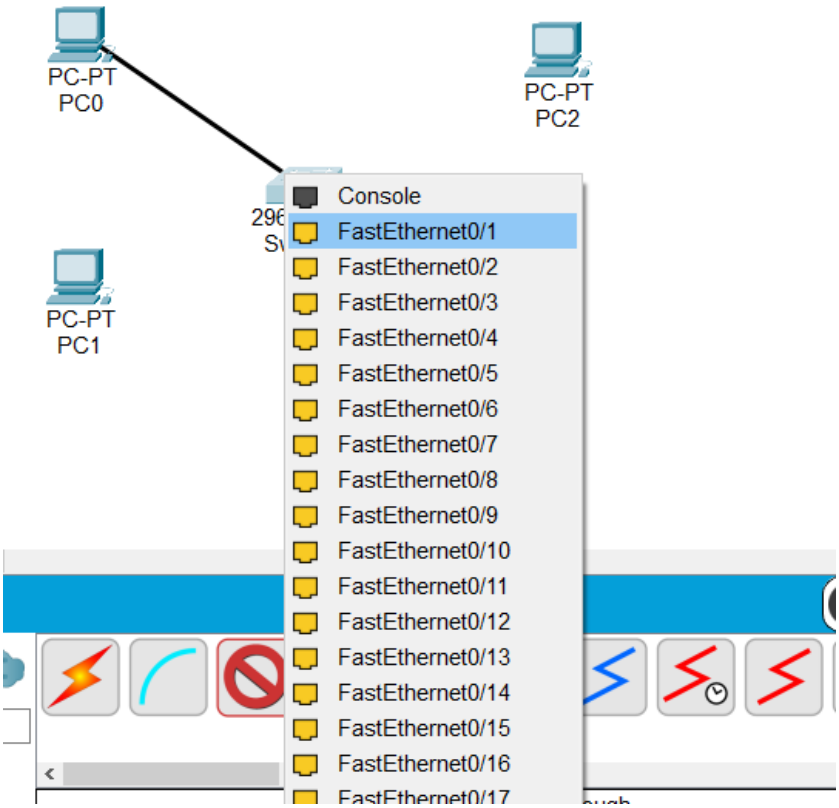


Рисунок 2 – Подключение компьютера PC1 к коммутатору 2960

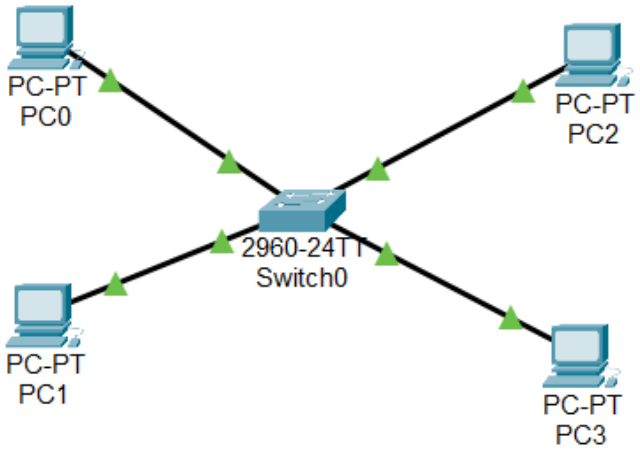


Рисунок 3 - Соединение между элементами сети

Далее разобьем нашу сеть на 2 сегмента. Пусть компьютеры PC0 и PC2 принадлежат к одному сегменту, а PC1 и PC3 к другому. Выбираем сверху фигуру Прямоугольник (Draw rectangle) и нужный цвет фигуры (рис.4), далее делим сеть нам 2 сегмента разного цвета (рис. 5).

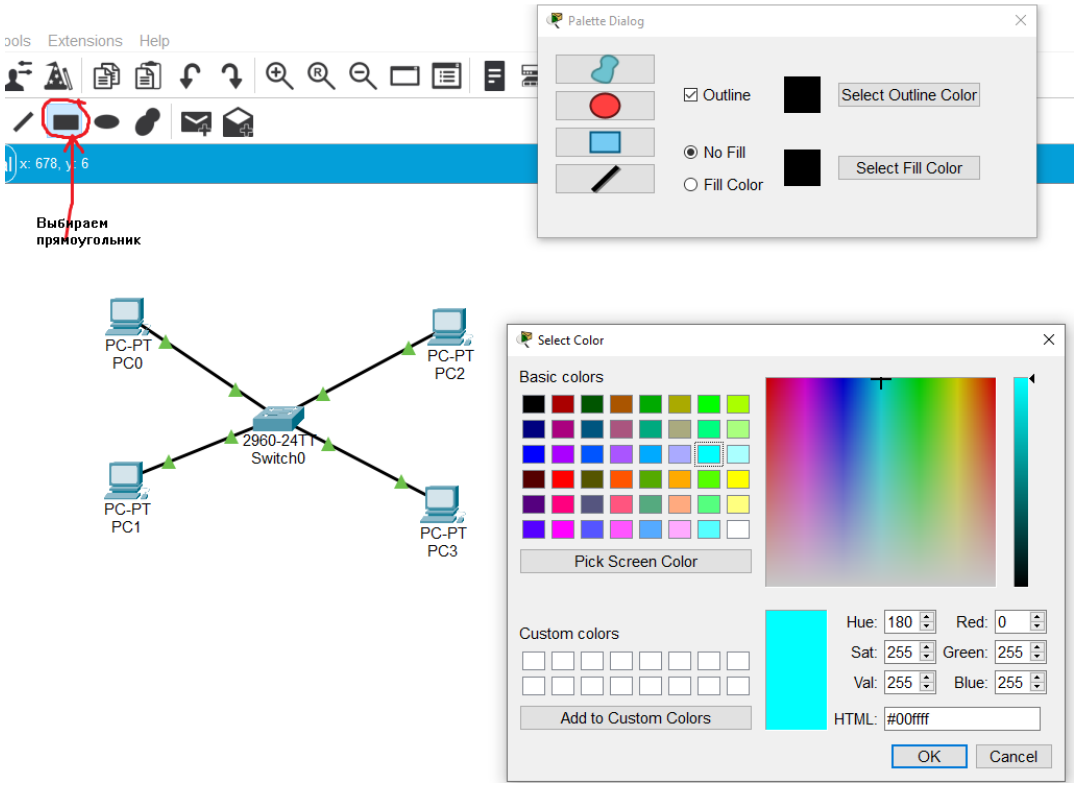


Рисунок 4 - Деление сети на сегменты с помощью значка Draw rectangle

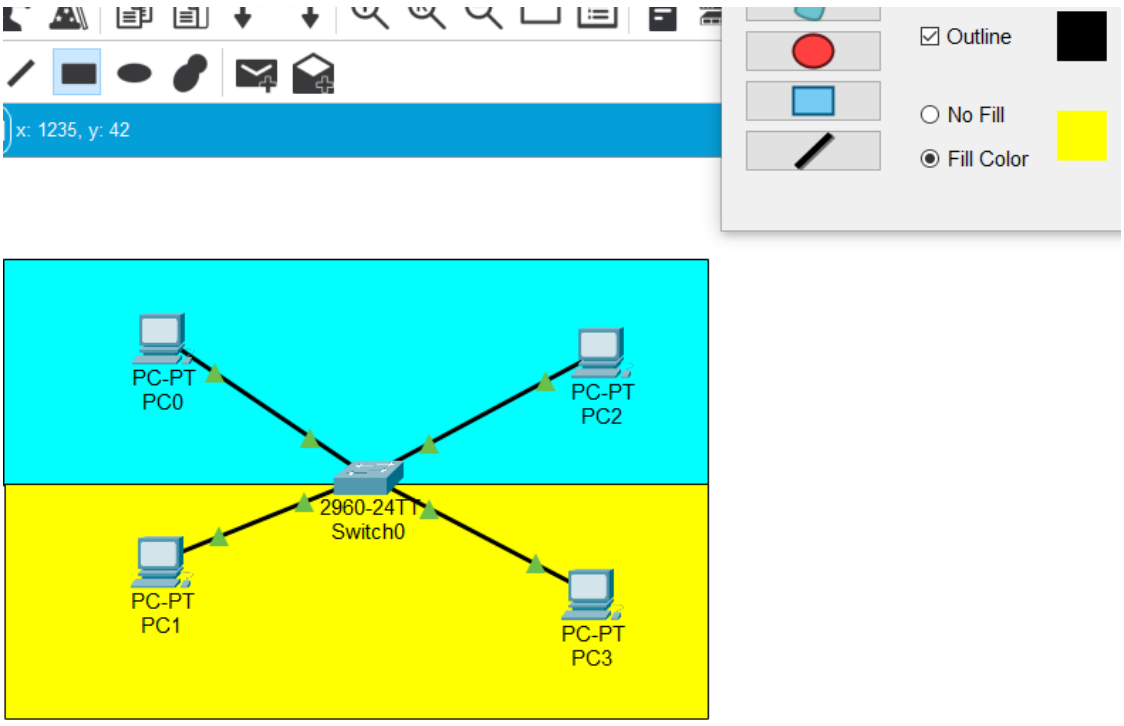


Рисунок 5 - Сеть с двумя сегментами

Для того, чтобы проверить номера интерфейсов FastEthernet для коммутатора, необходимо до создания VLAN проверить номера всех интерфейсов коммутатора, которые подключены к компьютерам. Для этого, необходимо подвести курсор к зеленым треугольникам на линиях, соединяющих компьютеры с коммутаторами. Номера интерфейсов высветятся рядом с зелеными треугольниками (рис. 6).

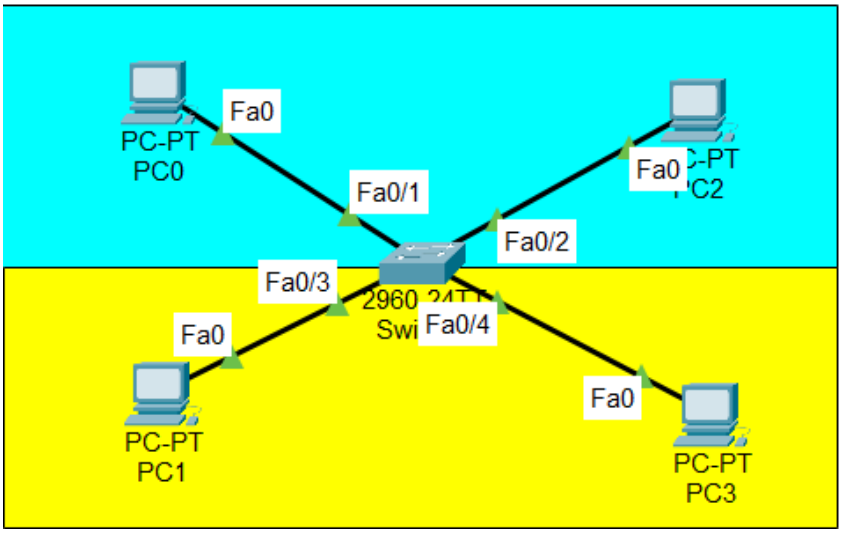


Рисунок 6 - Проверка номеров интерфейсов FastEthernet

Теперь нам нужно отделить данные одного сегмента от другого. Выходим в настройки коммутатора и входим в консоль (CLI) (рис. 7).

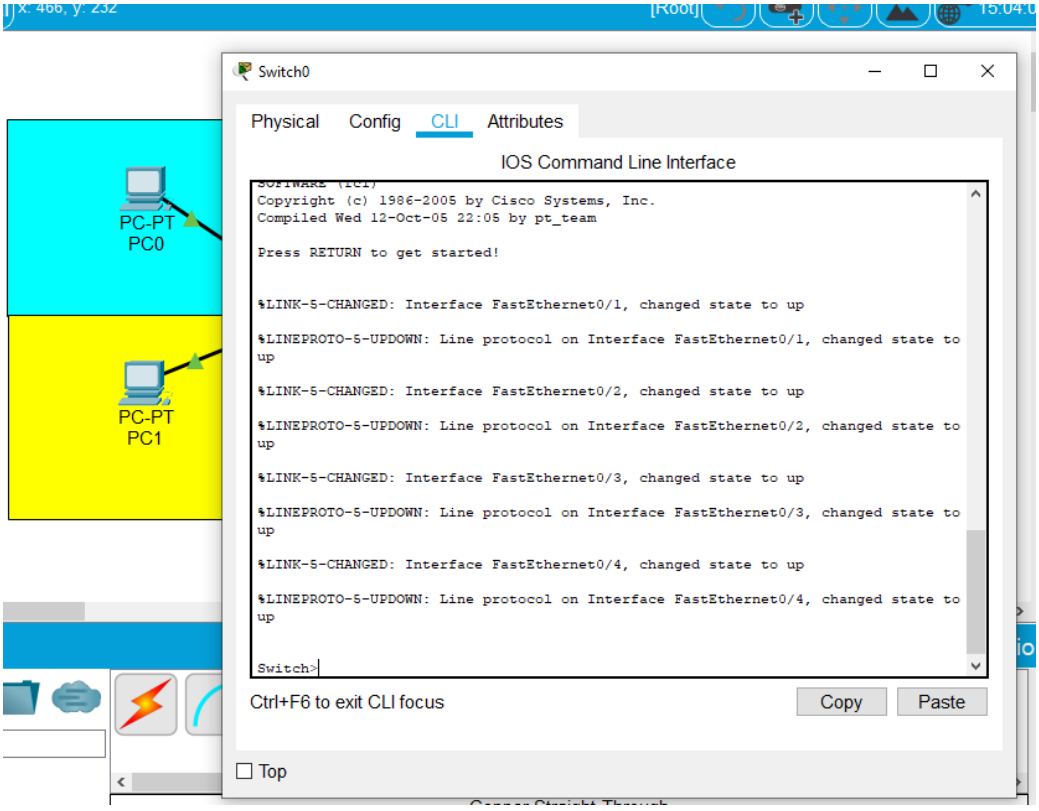


Рисунок 7- Консоль коммутатора

Набираем команду **Switch>enable**
И входим в привилегированный режим. Далее вводим команду
Switch#configure terminal
Создайте новый VLAN, назовем его VLAN 2, дайте ему название **professors** и назначьте портам коммутатора, к которым подключены компьютеры, режим передачи трафика и VLAN 2:

Switch(config)#vlan 2
Switch(config-vlan)#name professors
Switch(config-vlan)#exit

Настройка портов коммутатора :

Switch(config)#interface FastEthernet 0/1
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 2
Switch(config-if)# exit

Switch(config)#interface FastEthernet 0/2
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 2
Switch(config-if)# end

На этом настройка портов закончена.
Проверьте правильность настроек с помощью команды :

Switch#show vlan

Она выводит основную информацию о VLAN, (рисунок 8).

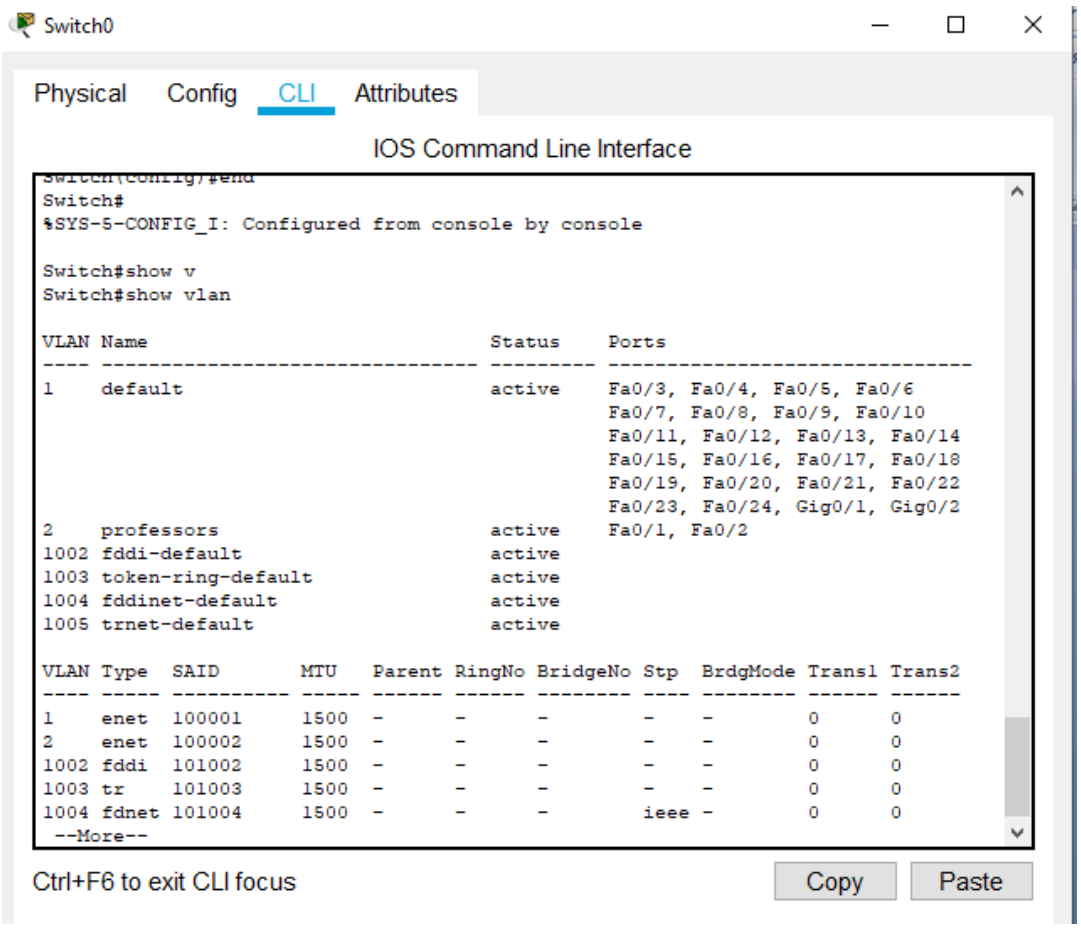


Рисунок 8 - Основная информация по VLAN

Здесь показана вся информация по VLAN. Видно, что первый VLAN, который существует на всех коммутаторах CISCO по умолчанию (default) выставлен на всех портах кроме портов FastEthernet 0/1 и FastEthernet 0/2, которые мы определили в VLAN 2.

Для вывода краткой информации по созданным VLAN введите команду (рисунок 9):

Switch# show vlan brief

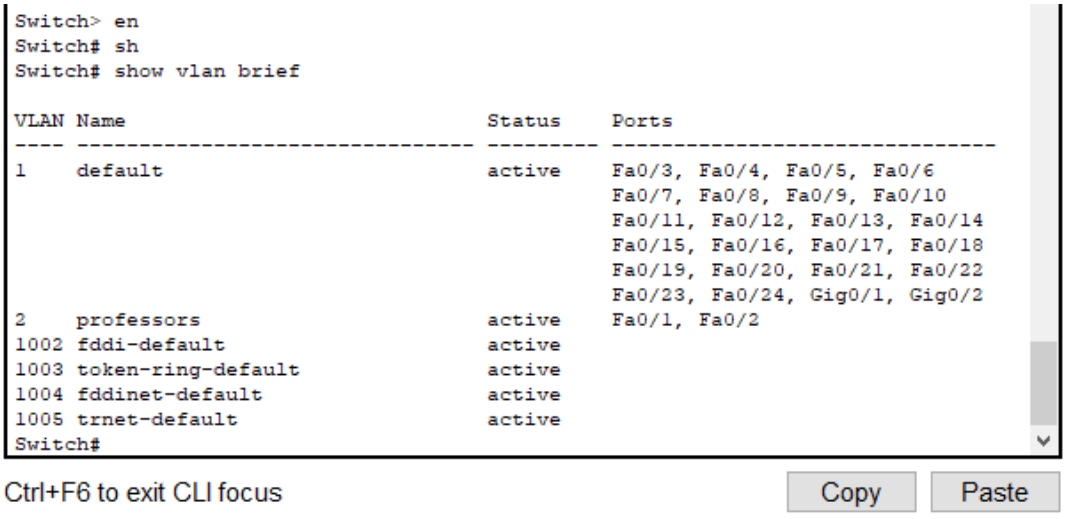


Рисунок 9 - Краткая информация по VLAN

Проделаем аналогичные действия для второго сегмента. Назовем его **students**. Пусть это будет VLAN 3.

Далее набираем команды:

Switch#configure terminal
Switch(config)#vlan 3
Switch(config-vlan)#name students
Switch(config-vlan)#exit

Настройка интерфейсов:

Switch(config)#interface FastEthernet 0/3
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 3
Switch(config-if)#exit
Switch(config)#interface FastEthernet 0/4
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 3
Switch(config-if)#end

Для вывода краткой информации по созданным VLAN введите команду (рисунок 10):

Switch# show vlan brief

```
Switch>en
Switch#sh
Switch#show v
Switch#show vlan brief

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

Рисунок 10 - Краткая информация по VLAN 3

Перейдем к настройке компьютеров и зададим им IP-адреса (Табл. 1). В IP- адресах компьютеров третья цифра IP-адреса соответствует номеру VLAN. Для этого выйдем в настройки PC0 и во вкладке Desktop выбираем IP-Configuration (рис. 11).

Таблица №1 Сетевые адреса компьютеров

Сетевой элемент	Интерфейс	IP-адрес	VLAN
PC0	FastEthernet0	192.168.2.1	2
PC1	FastEthernet0	192.168.3.1	3
PC2	FastEthernet0	192.168.2.2	2
PC3	FastEthernet0	192.168.3.2	3

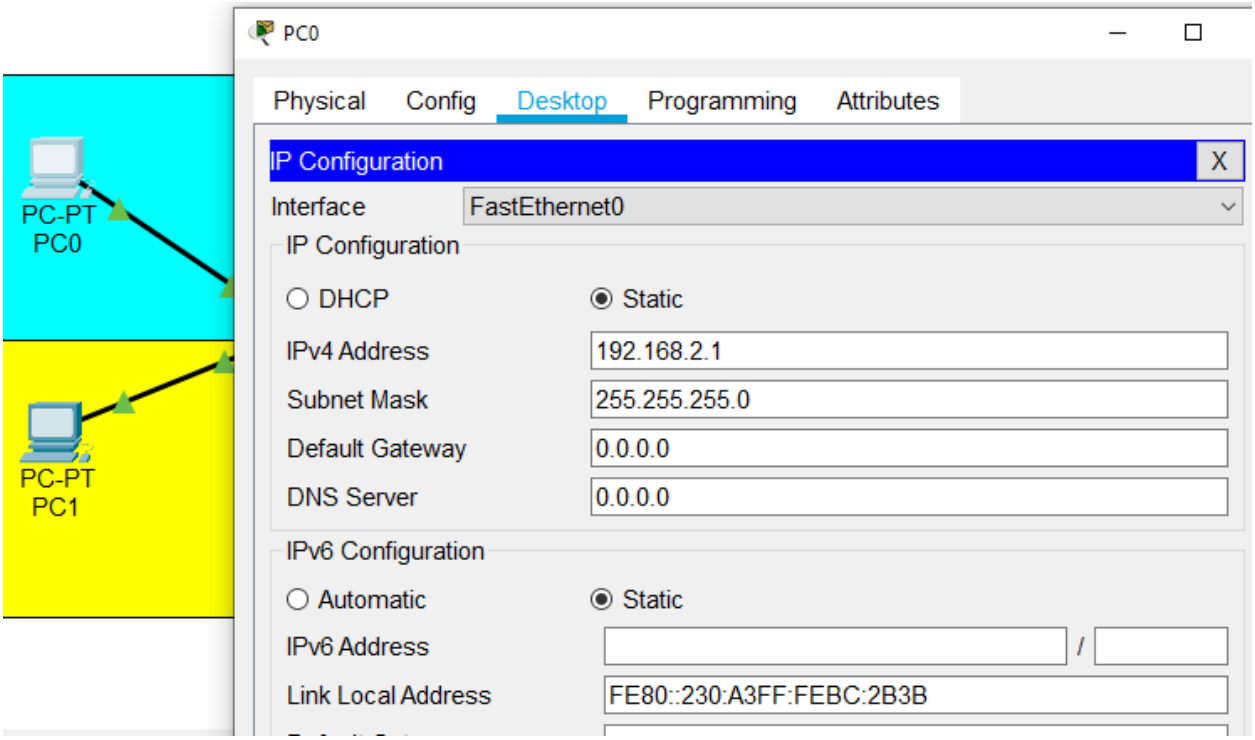


Рисунок 11- Настройка компьютера PC0

В соответствии с таблицей 1 настраиваем и остальные компьютеры сети.

Проверим связность компьютеров в первом сегменте (рис. 12).

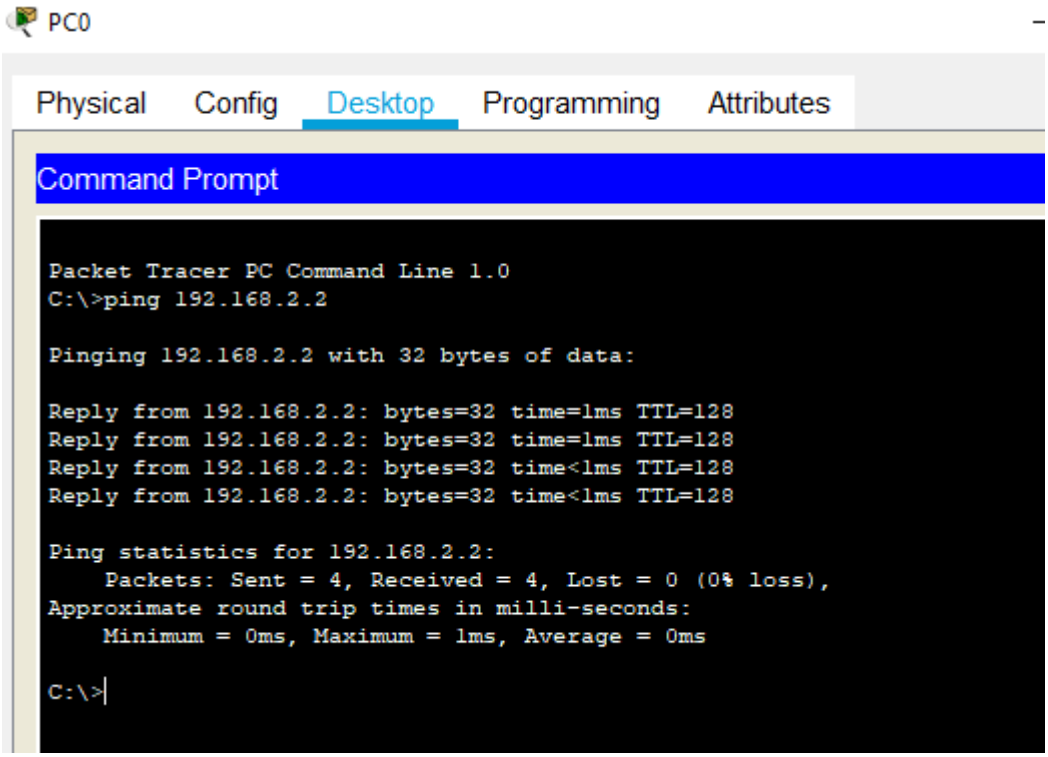


Рисунок 12 - Проверка связности компьютеров в одном сегменте

Попробуем проверить связь компьютеров в разных сегментах. Пакеты между ними не пересылаются (рис. 13). Т.е. связность между компьютерами разных сегментов отсутствует.

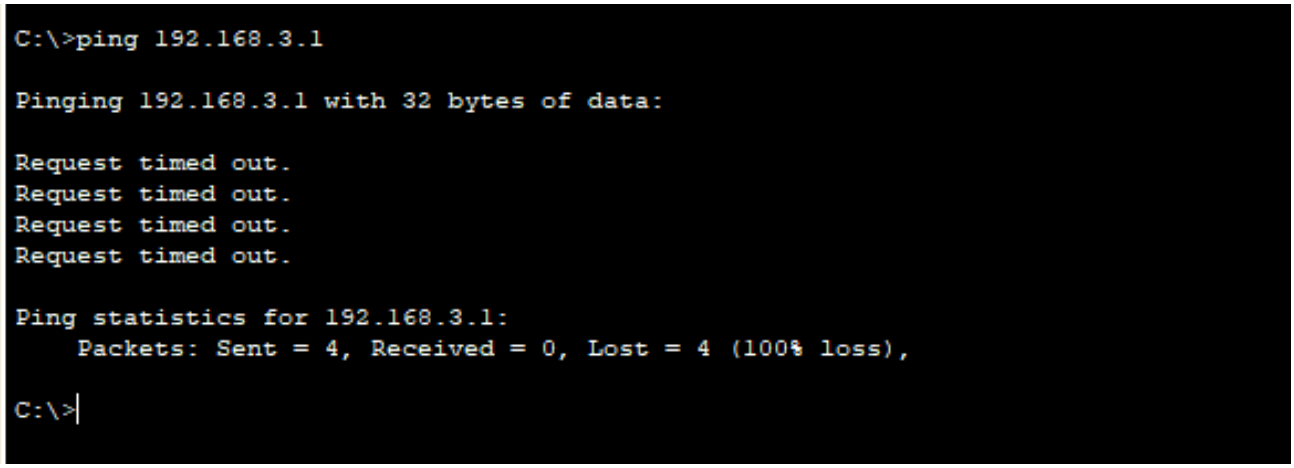


Рисунок 13 - Проверка связности компьютеров в разных сегментах

Произведем аналогичную проверку у компьютеров из второго сегмента. Таким образом, мы убедились, что между сегментами professors и students связность отсутствует. Т.е. мы сделали 2 независимые VLAN. Рекомендуется сохранить данную конфигурацию для выполнения лабораторной работы «Изучение технологии виртуальных локальных сетей VLAN». Часть 2.

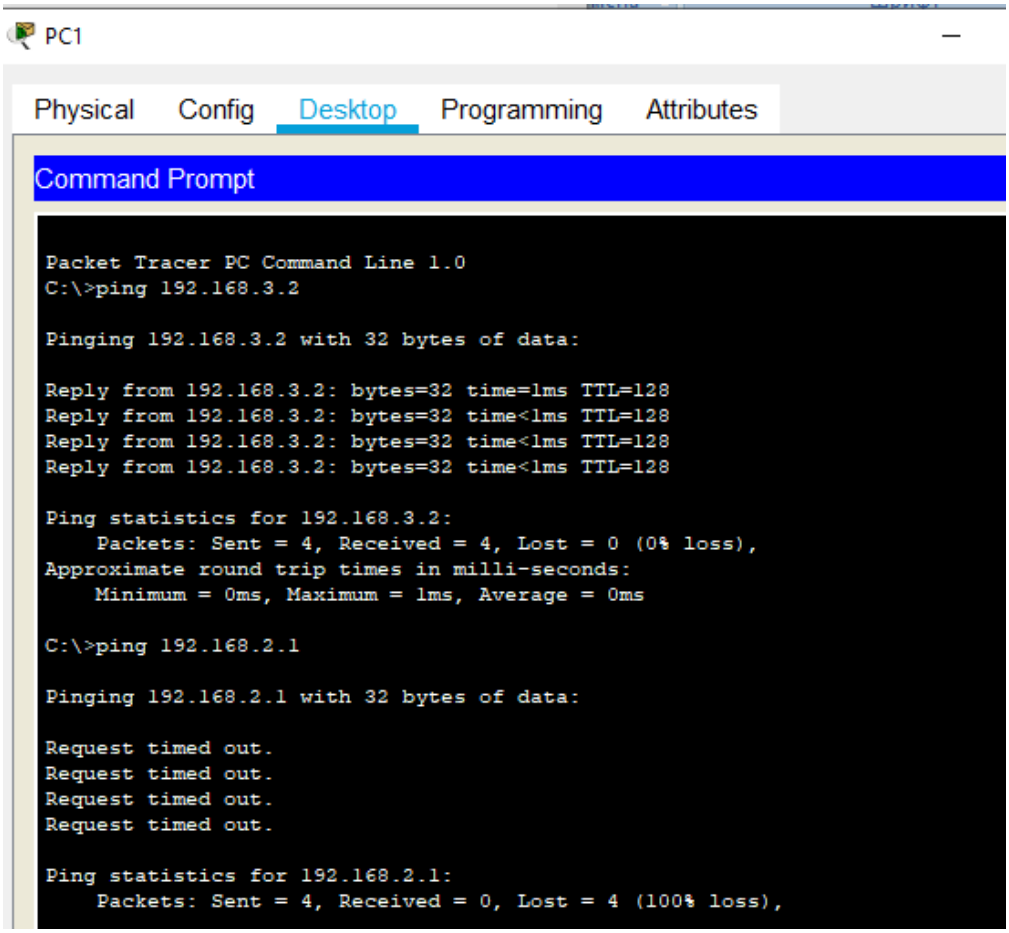


Рисунок 14 - Проверка связности компьютеров во втором сегменте

Содержание отчета

В индивидуальном отчёте должны быть указаны цель, задание, представлены необходимые снимки экрана и пояснения к ним. Следует проанализировать полученные данные и дать ответы на контрольные вопросы.

Контрольные вопросы

1. Опишите последовательность создания VLAN?
2. Как проверить связность компьютеров в разных VLAN?
3. Для чего используется команда **Switch# show vlan brief?**
4. Как проверить правильность настройки компьютеров?
5. Для чего применяется команда **Switch(config-if)#switchport mode access?**
6. Что обозначает аббревиатура TTL на рисунке 12?
7. Почему для соединения ПК и коммутатора используется прямой кабель?
8. Какого класса IP- адреса используются в данной работе?
9. Продемонстрируйте продвижение пакета внутри одного VLAN в данной работе.
10. Что выполняет команда switchport access vlan 3?

Лабораторная работа №6. Изучение технологии виртуальных локальных сетей VLAN. Часть 2

Цель работы

Изучить и практически освоить процесс настройки технологии виртуальных локальных сетей VLAN (Virtual Local Area Network) с использованием сетевого симулятора Cisco Packet Tracer. Научиться настраивать порты коммутатора в режимы trunk.

Задание

1. Ознакомиться с основными понятиями технологии виртуальных локальных сетей VLAN (Virtual Local Area Network).
2. Запустить сеть, которая использовалась в предыдущей работе
3. Собрать новую топологию сети, запустить и настроить виртуальное оборудование.
4. Согласно пунктам выполнения лабораторной работы, сделать необходимые снимки экрана. Изучить полученную информацию и оформить ее в соответствии с требованиями раздела «Содержание отчета».

Порядок выполнения работы

В данной работе мы будем использовать схему сети из предыдущей лабораторной работы. Необходимо удалить сегменты. Сделаем это с помощью значка delete в левом верхнем углу (рис. 1).

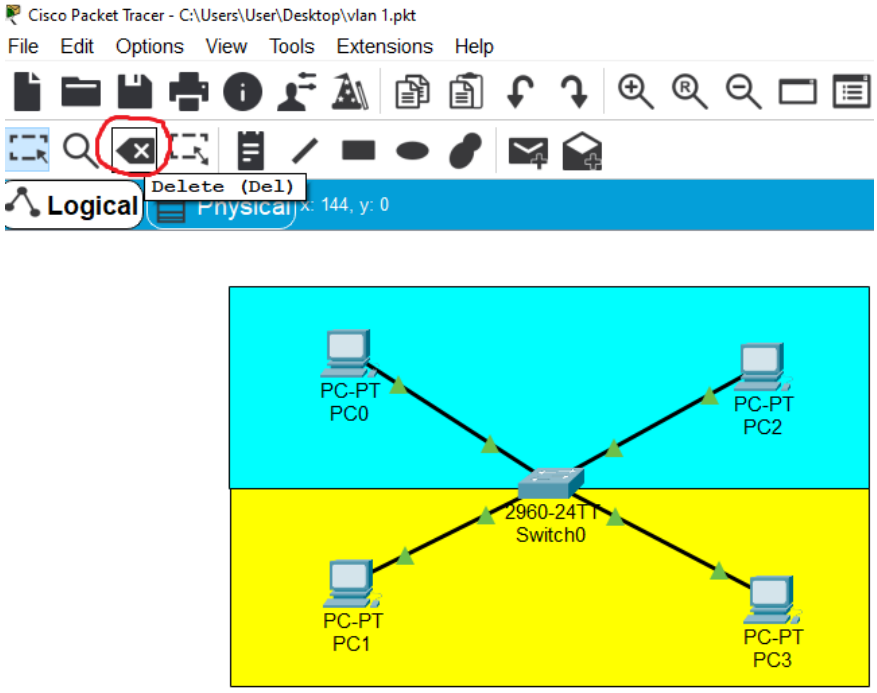


Рисунок 1 – Значок для удаления элементов сети

С помощью появившегося крестика удаляем 2 сегмента. Для этого необходимо щелкнуть крестиком на сегменте. Далее щелкаем на значок Select и выделяем всю область сети (рис. 2). После этого нажимаем на кнопку Ctrl, нажимаем на нашу сеть и перетаскиваем ее вправо, для того, чтобы сделать точно такую же копию нашей сети (рис. 3).

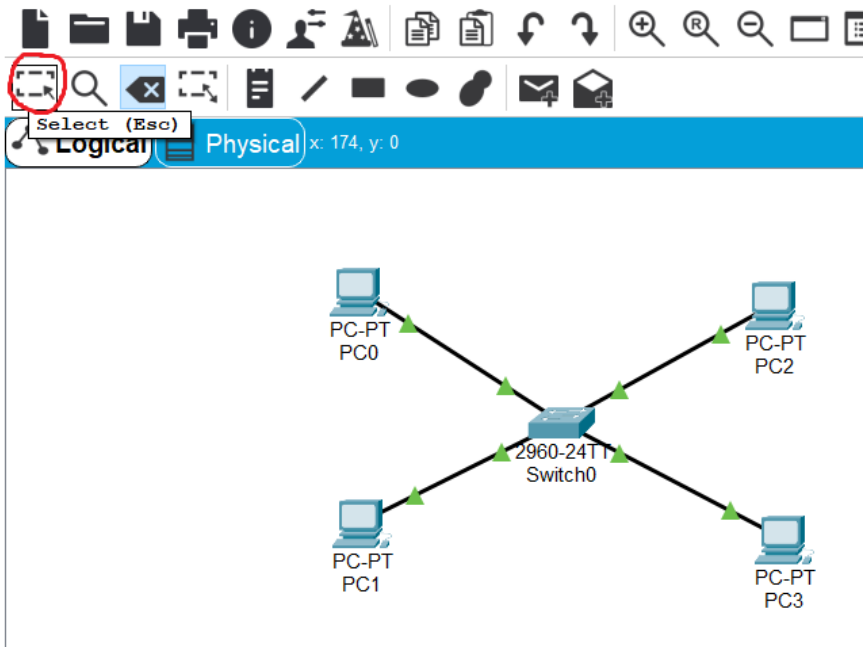


Рисунок 2 - Значок для копирования элементов сети

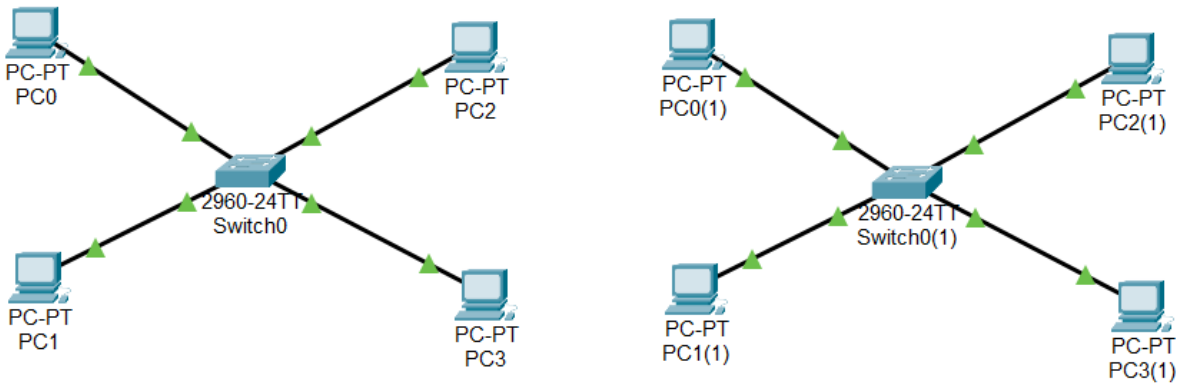


Рисунок 3 - Вторая сеть, полученная после операции копирования

Теперь необходимо соединить два коммутатора 2960. Так как они относятся к одному уровню модели OSI, то соединять их нужно перекрестным кабелем. Пусть они будут соединены портами GigabitEthernet. Для соединения коммутаторов лучше брать самые высокопроизводительные порты (рис. 4).

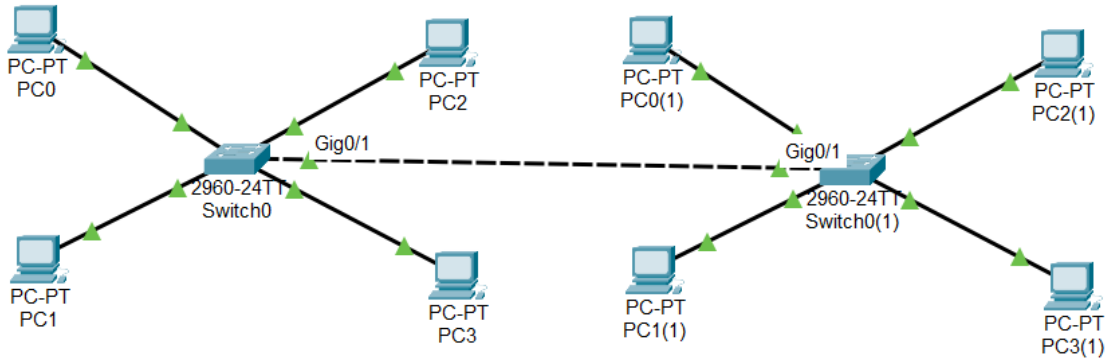


Рисунок 4 - Соединение двух коммутаторов с помощью высокопроизводительных портов GE

Поскольку мы сделали точную копию наших компьютеров PC0-PC3, то необходимо изменить IP-адресацию на вновь созданных компьютерах в соответствии с таблицей 1. Таблица №1. IP-адресация для компьютеров сети

Сетевой элемент	IP-адрес	VLAN
PC0	192.168.2.1	2
PC1	192.168.3.1	3
PC2	192.168.2.2	2
PC3	192.168.3.2	3
PC0 (1)	192.168.2.3	2
PC1 (1)	192.168.3.3	3
PC2 (1)	192.168.2.4	2
PC3 (1)	192.168.3.4	3

Пример изменения IP-адреса для компьютера PC0(1) показан на рисунке 5.

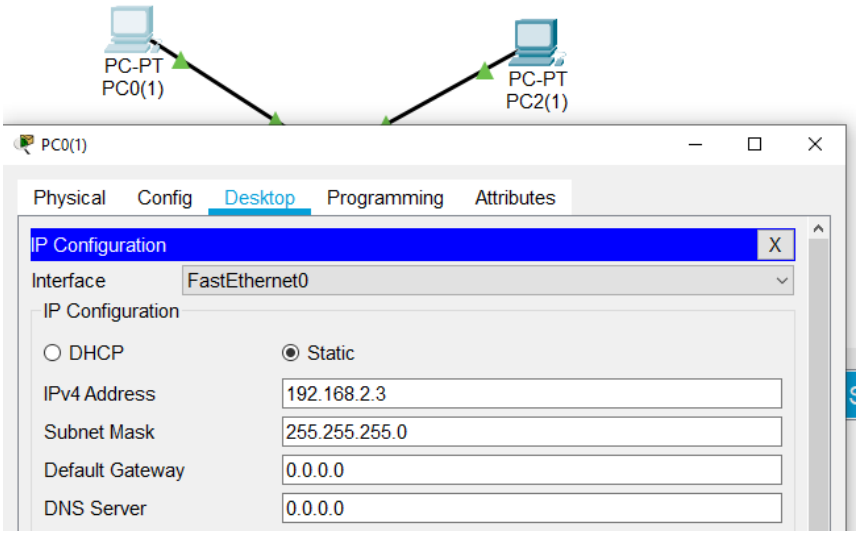


Рисунок 5 - Изменение IP- адреса для компьютера PC0(1)

На рисунке 6 показана схема компьютерной сети, которая разделена на 2 фрагмента.

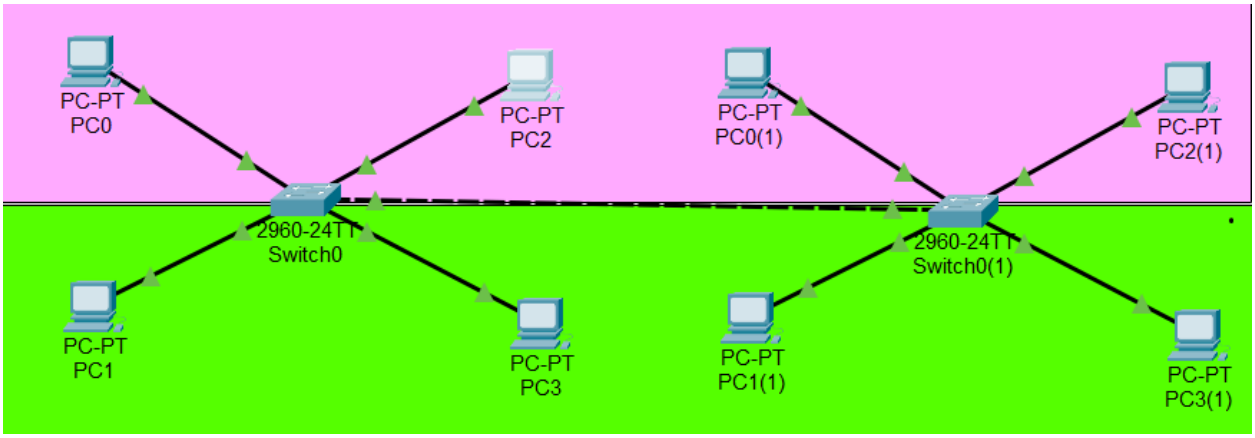
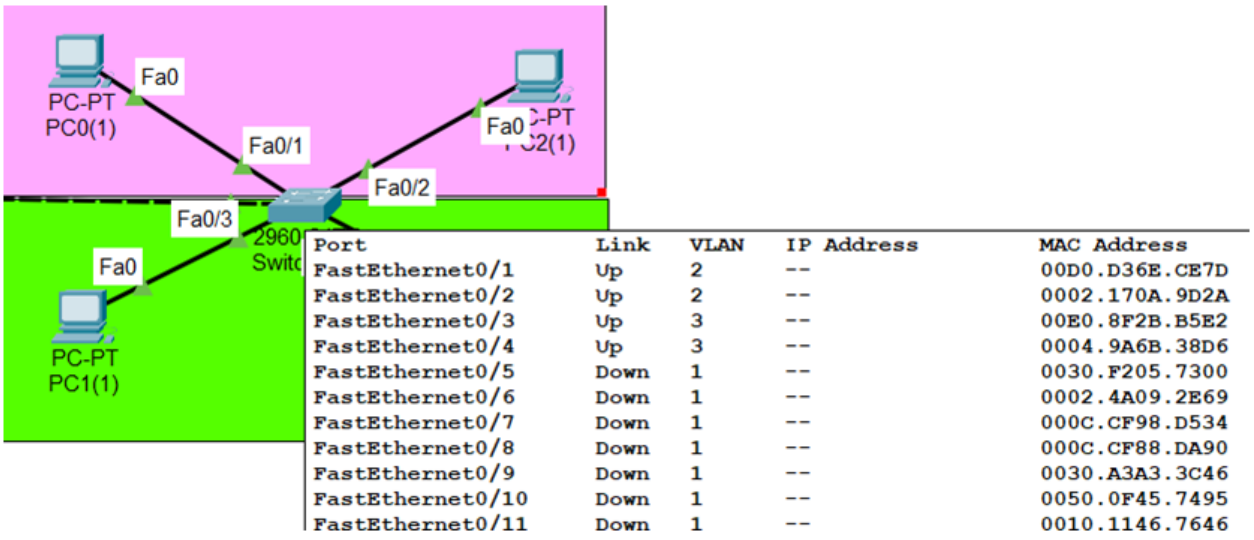


Рисунок 6 - Схема компьютерной сети, состоящая их двух фрагментов

Для того, чтобы проверить настройки второго коммутатора, то наводим на него курсор и смотрим порты и в каком они VLAN.



Port	Link	VLAN	IP Address	MAC Address
FastEthernet0/1	Up	2	--	00D0.D36E.CE7D
FastEthernet0/2	Up	2	--	0002.170A.9D2A
FastEthernet0/3	Up	3	--	00E0.8F2B.B5E2
FastEthernet0/4	Up	3	--	0004.9A6B.38D6
FastEthernet0/5	Down	1	--	0030.F205.7300
FastEthernet0/6	Down	1	--	0002.4A09.2E69
FastEthernet0/7	Down	1	--	000C.CF98.D534
FastEthernet0/8	Down	1	--	000C.CF88.DA90
FastEthernet0/9	Down	1	--	0030.A3A3.3C46
FastEthernet0/10	Down	1	--	0050.0F45.7495
FastEthernet0/11	Down	1	--	0010.1146.7646

Рисунок 7 - Проверка портов второго коммутатора

Таким образом, access – порты у нас уже настроены.

Для организации взаимодействия компьютеров, подключенных к разным коммутаторам, но находящихся в одном VLAN необходимо настроить trunk-порты, которые позволяет разбить физическое соединение на несколько сегментов. Далее переходим в режим конфигурирования для Switch0, для этого необходимо открыть вкладку CLI и ввести следующие команды:

Switch#configure terminal
Switch(config)#interface gigabitEthernet 0/1
Switch(config-if)#switchport mode trunk

Switch(config-if)#switchport trunk allowed vlan 2,3 (эта команда разрешает проходить через этот порт трафику VLAN 2 и 3)

Exit

Такие же настройки сделайте на коммутаторе Switch0(1).

Далее необходимо проверить связность между компьютерами. На рисунке 8 показана проверка связности между компьютером PC0 и PC0(1) а также между PC0 и PC1. Проверьте самостоятельно связность между другими компьютерами и объясните результаты.

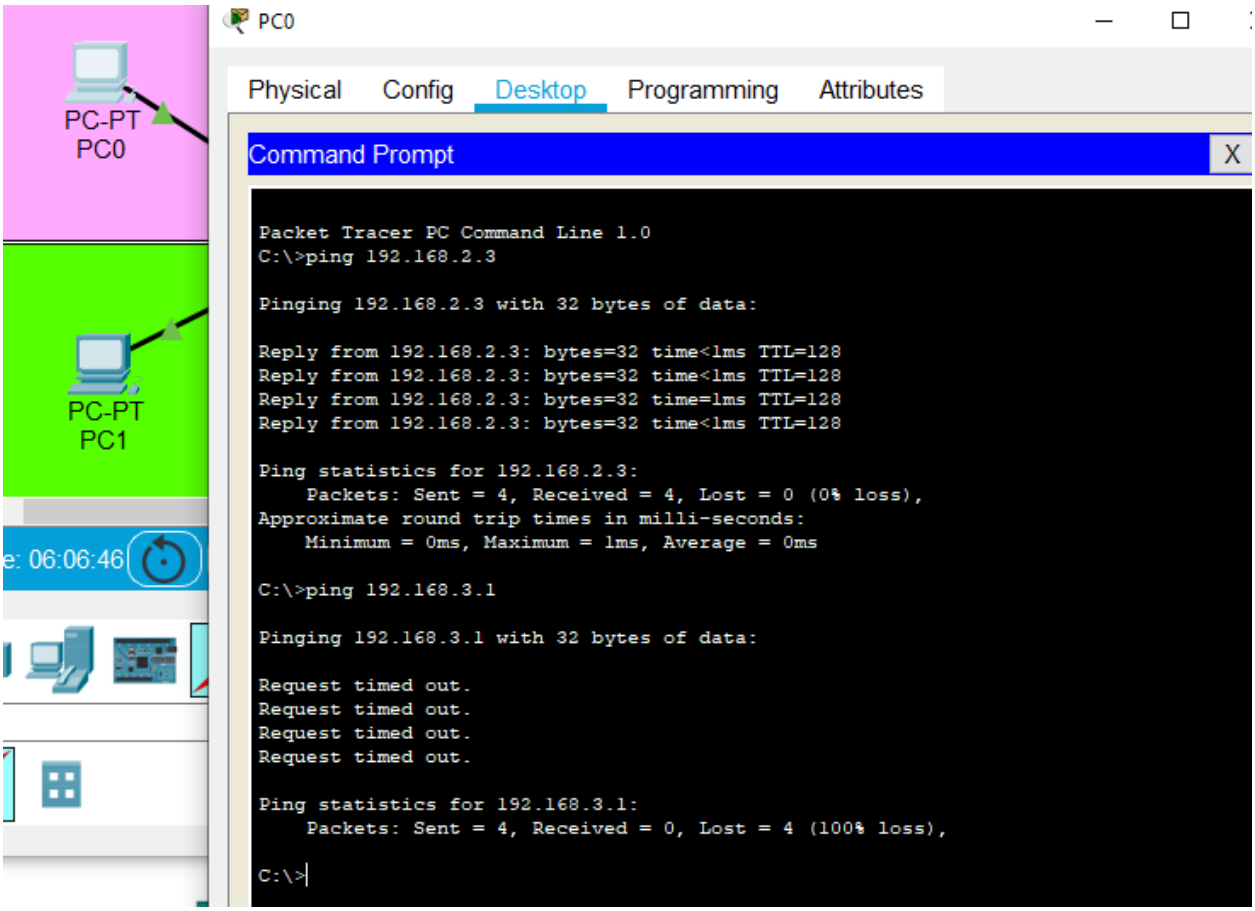


Рисунок 8 - Проверка связности между PC0 и PC0(1) и между PC0 и PC1

Содержание отчета

В индивидуальном отчёте должны быть указаны цель, задание, представлены необходимые снимки экрана и пояснения к ним. Следует проанализировать полученные данные.

Контрольные вопросы

1. Для чего применяется команда **Switch(config-if)#switchport trunk allowed vlan 2,3** в данной лабораторной работе?
2. Как проверить связность компьютеров в одной VLAN?
3. Опишите последовательность настройки **access** портов**?**

4. Как настроить trunk- порты между коммутаторами?
5. Могут ли абоненты VLAN 3 получать широковещательный трафик, предназначенный для абонентов VLAN 2**?**
6. Опишите функцию trunk- порта?
7. Какого класса IP- адреса используются в данной работе?
8. Как можно определить номера интерфейсов на коммутаторе?
9. В какой подсети находится компьютер с адресом 192.168.3.2?
10. Что означает команда **Switch(config)#**?

Практическое занятие № 7. Агрегирование каналов в коммутаторах

Цель работы

Изучить принципы статического и динамического агрегирования каналов.

Задание

1.Ознакомиться с принципами статического агрегирования каналов;

2. Ознакомиться с принципами динамического агрегирования каналов.

3.Ответить на вопросы.

Краткая теория

Часто для повышения пропускной способности и коммутатора удобно объединить несколько каналов. Это позволит также обеспечить резервирование в случае выхода из строя одного из каналов. Такая группа каналов рассматривается как единый интерфейс, а нагрузка равномерно распределяется между ними. Технология, которая позволяет это сделать называется Link Aggregation (объединение звеньев) (рис. 1). При этом для равномерного распределения трафика требуется, чтобы физические характеристики звеньев были одинаковы. На рисунке 1 три физических соединения между коммутаторами объединяются в одно логическое. Все соединения агрегированного канала являются активными и передают информацию.

Важным моментом при реализации объединения портов в агрегированный канал является распределение трафика по ним. Если пакеты одного сеанса будут передаваться по разным портам агрегированного канала, то может возникнуть проблема на более высоком уровне модели OSI. Например, если два или более смежных кадров одного сеанса станут передаваться через разные порты агрегированного канала, то из-за неодинаковой длины очередей в

их буферах может возникнуть ситуация, когда из-за неравномерной задержки передачи кадра более поздний кадр обгонит предыдущий.

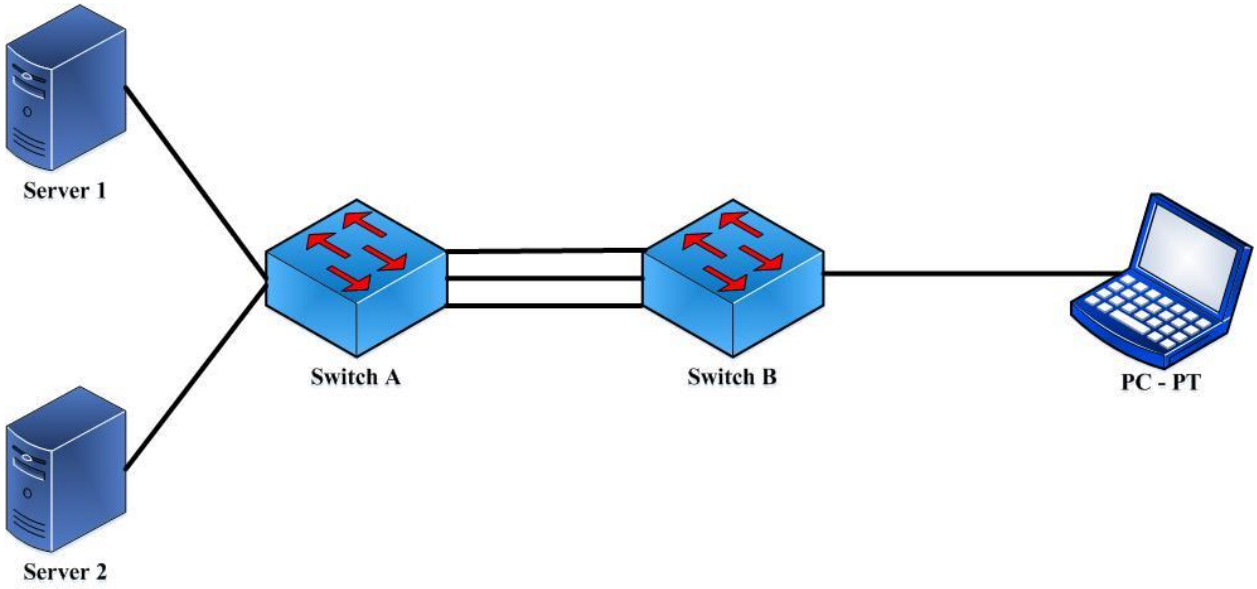


Рисунок 1 - Агрегирование каналов в коммутаторах

Поэтому в большинстве реализаций механизмов агрегирования используются методы статического, а не динамического распределения кадров по портам, т.е. закрепление за определенным портом агрегированного канала потока кадров определенного сеанса между двумя узлами. В этом случае все кадры будут проходить через одну и ту же очередь и их последовательность не изменится.

Объединение каналов следует рассматривать как вариант настройки сети, используемый преимущественно для соединений «коммутатор – коммутатор» или «коммутатор – сервер», требующих более высокой скорости передачи, чем может обеспечить одиночная линия связи. Также эту функцию можно применять для повышения надежности важных каналов связи. В случае повреждения линии связи объединенный канал быстро перенастраивается (не более чем за 1 сек.), а риск дублирования и изменения порядка кадров незначителен.

Обычно коммутаторы поддерживают два типа агрегирования каналов связи:

• статическое;

• динамическое.

При статическом агрегировании каналов (установлено по умолчанию), все настройки на коммутаторах выполняются вручную, и они не допускают динамических изменений в агрегированной группе. Его преимуществом является отсутствие дополнительных задержек при поднятии агрегированного

канала и изменении его настроек. Недостаток – отсутствие согласования настроек с удаленной стороной.

Для организации динамического агрегирования каналов между коммутаторами и другими сетевыми устройствами используется протокол управления агрегированным каналом – Link Aggregation Control Protocol (LACP). Протокол LACP определяет метод управления объединением нескольких физических портов в одну логическую группу и предоставляет сетевым устройствам возможность автосогласования каналов (их добавления или удаления) путем отправки управляющих кадров протокола LACP непосредственно подключенным устройствам с поддержкой LACP. Пакеты LACP отправляются устройством через все порты, на которых активизирован протокол. Порты, на которых активизирован протокол LACP, могут быть настроены для работы в одном из двух режимов: **активном** (*active*) или **пассивном** (*passive*). Это стандартный протокол, он поддерживается такими коммутаторами, как Cisco, D-Link, HP и др. Т.е. данный протокол можно настроить не только между коммутаторами Cisco, но и Cisco - D-Link, Cisco – HP и т.д.

При работе в активном режиме порты выполняют обработку и рассылку управляющих кадров протокола LACP. При работе в пассивном режиме порты выполняют только обработку управляющих кадров LACP. Для того чтобы динамический канал обладал функцией автосогласования, рекомендуется порты, которые входят в агрегированную группу, с одной стороны канала настраивать как активные, а с другой канала – как пассивные.

Следует отметить, что у портов, объединяемых в агрегированный канал, нижеперечисленные характеристики должны обладать одинаковыми настройками:

- тип среды передачи;
- скорость;
- режим работы;
- метод управления потоком (Flow Control) .

Преимущества протокола LACP – согласование настроек с удаленной стороной, что позволяет избежать ошибок в сети. Недостатки - дополнительная задержка при поднятии агрегированного канала или изменении его настроек.

В следующей лабораторной работе рассмотрим пример статического агрегирования коммутаторов.

Контрольные вопросы

1. Для чего применяется агрегирование каналов?
2. Какие требования предъявляются к агрегированным каналам?

3. Какие методы агрегирования каналов вы знаете?
4. Опишите принципы статического агрегирования каналов.
5. Опишите принципы динамического агрегирования каналов.
6. Как происходит распределение нагрузки между каналами при статическом агрегировании?
7. Как происходит распределение нагрузки между каналами при динамическом агрегировании?
8. На каком участке сети может применяться агрегирование каналов?
9. Опишите преимущества и недостатки статического агрегирования каналов?
10. Опишите преимущества и недостатки динамического агрегирования каналов?

Лабораторная работа №7. Статическое агрегирование каналов

Цель работы

Изучить статическое агрегирование каналов.

Задание

Создать высокопроизводительную сеть путём статического агрегирования каналов двух коммутаторов и проверить ее работоспособность.

Порядок выполнения работы

1.Открываем Cisco Packet Tracer.

2. Добавляем 2 коммутатора 2960 и два компьютера PC0 и PC1. Затем соединяем их с помощью кабеля. При этом компьютеры присоединяем к портам FastEthernet 0/3 каждого коммутатора (рис. 1). Для агрегирования каналов будем использовать порты FastEthernet 0/1 и FastEthernet 0/2 коммутаторов.

3. Перед объединением двух коммутаторов настроим порты FastEthernet 0/1 и FastEthernet 0/2. Для этого переходим во вкладку CLI, заходим в привилегированный режим – **Switch #.** Затем выходим в режим глобального конфигурирования – **Switch(config) #** с помощью сокращенной команды **conf t**. Поскольку интерфейсы будут иметь одинаковые настройки, то мы можем их настроить с помощью одной команды **interface range fa0/1-2.**

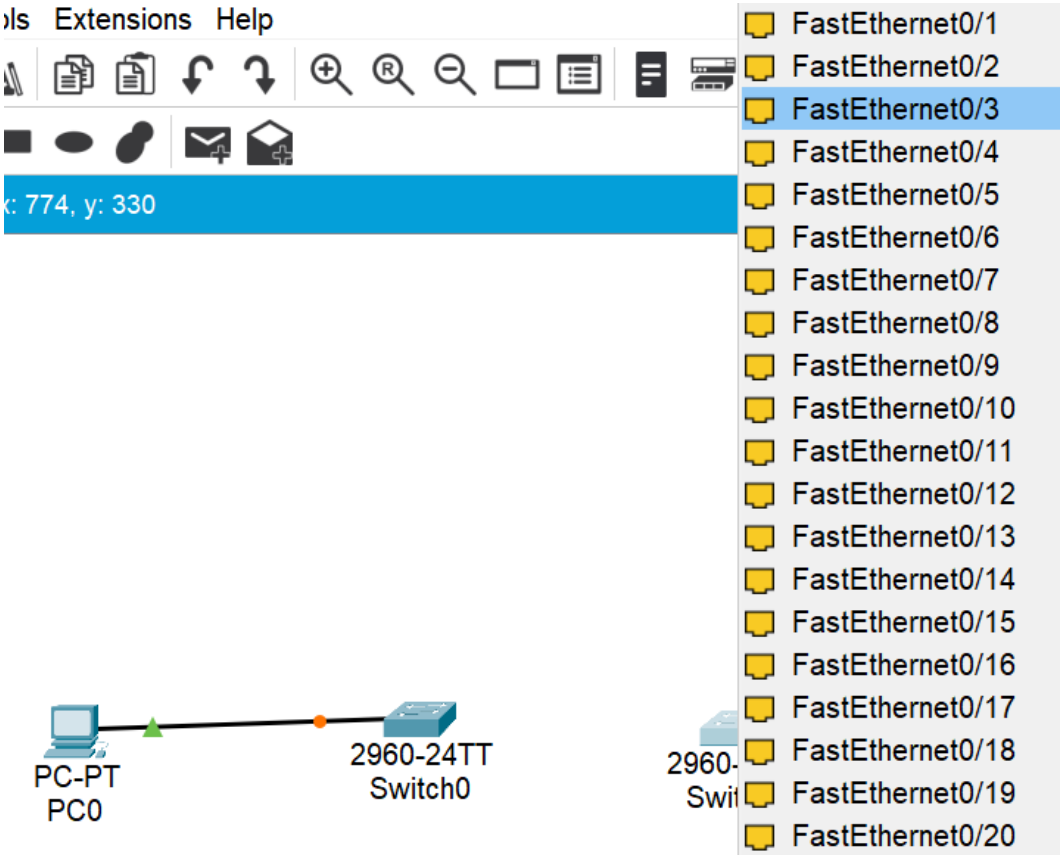


Рисунок 1 – Подключение компьютеров к портам FastEthernet 0/3

Таким образом, настройка коммутаторов во вкладке CLI должны выглядеть следующим образом:

Switch >

Switch >en

Switch #

Switch #conf t

Switch(config)#

Switch(config)#interface range fa0/1-2

Switch(config-if-range)#channel-group 1 mode ? (знак ? показывает все доступные режимы, мы выбираем режим **on**)

Switch(config-if-range)#channel-group 1 mode on

Как видно на рисунке 2, создался логический интерфейс Port-channel 1, который объединяет 2 физических интерфейса.

Switch(config-if-range)#end – заканчиваем настройку

Switch# wr mem – сохраним результаты.

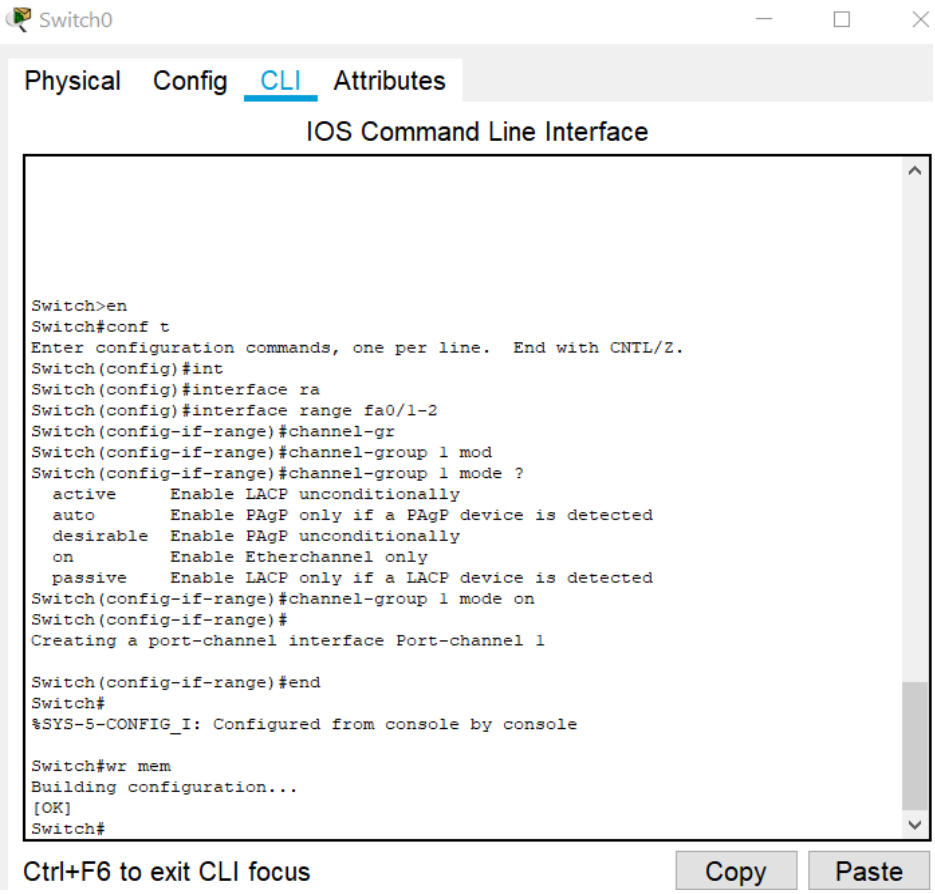


Рисунок 2- Настройка интерфейсов для Switch 0

Произведем аналогичные настройки для второго коммутатора (рис. 3).

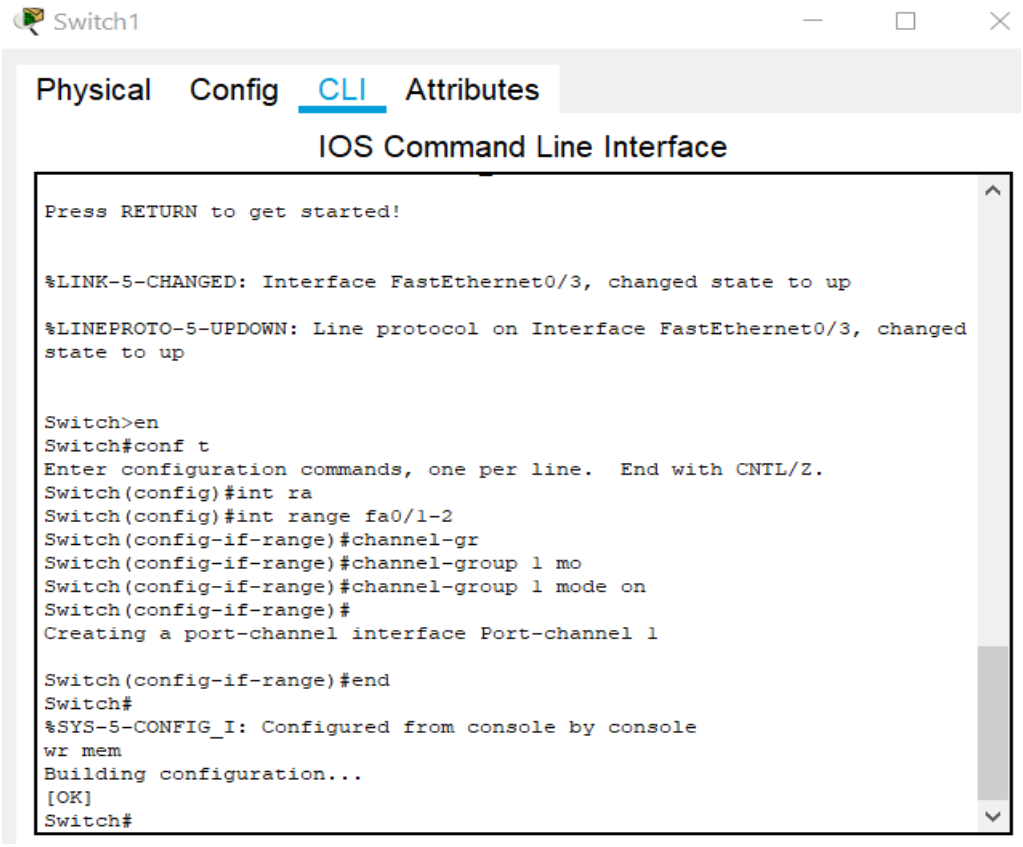


Рисунок 3 – Настройка интерфейсов для Switch 1

4. Соединим два коммутатора с помощью интерфейсов FastEthernet 0/1 и FastEthernet 0/2 и пропишем IP-адреса для каждого компьютера (рис. 4).

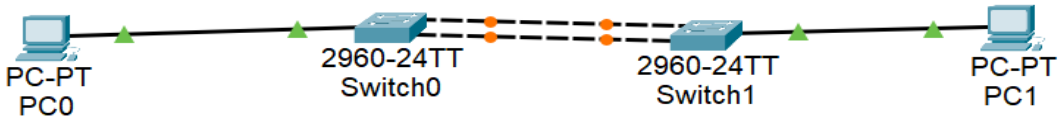


Рисунок 4 - Соединение коммутаторов с помощью интерфейсов FastEthernet 0/1 и FastEthernet 0/2

Для компьютеров PC0 и PC1 задаем следующие IP-адреса (табл. 1).

Таблица 1. IP- адреса для PC0 и PC1

Сетевой элемент	IP-адрес	Маска
PC0	192.168.1.1	255.255.255.0
PC1	192.168.1.2	255.255.255.0

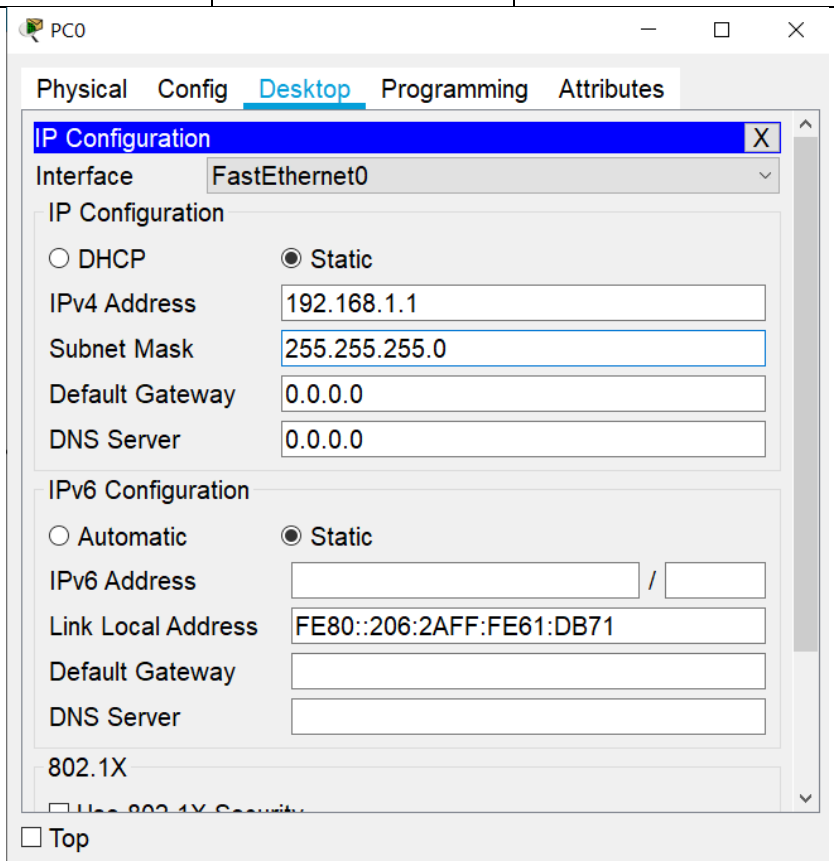


Рисунок 5 – Назначение IP- адреса для PC0

Проверим соединение между коммутаторами с помощью команды ping (рис. 6). Проверка показала, что команда ping прошла успешно. Таким образом, мы получили агрегированный канал между двумя коммутаторами, Но пропускная способность этого канала не 100 Мбит/с, а в 2 раза больше.

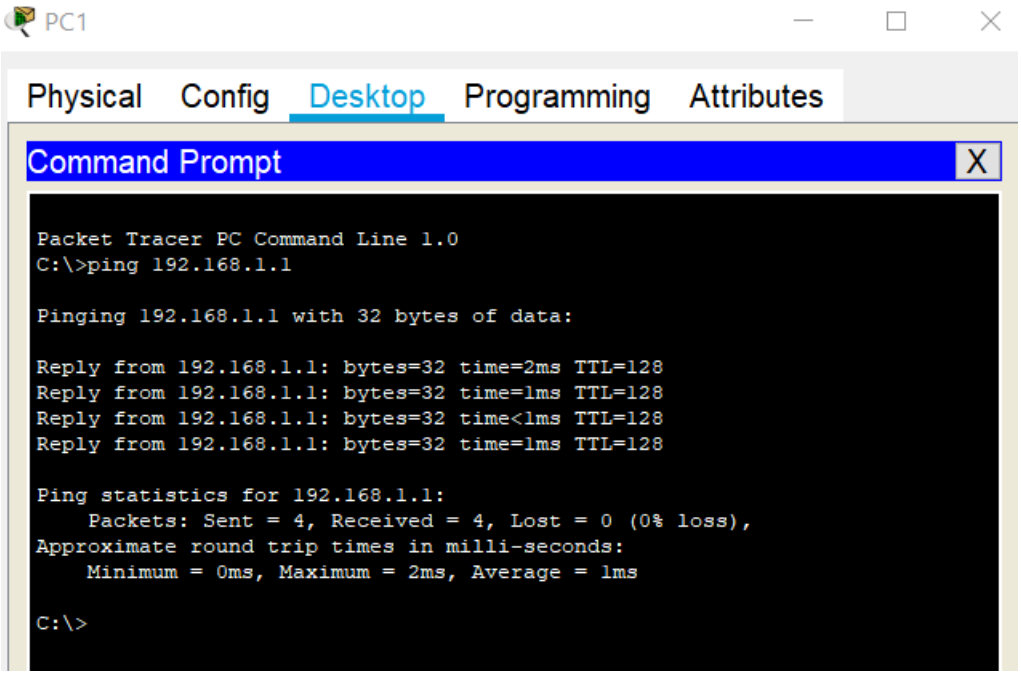


Рисунок 6 - Проверка соединения между коммутаторами

5. Для проверки отказоустойчивости агрегированного звена выведем из строя один из интерфейсов. Пусть это будет FastEthernet 0/2 на Switch 1.

Switch >
Switch >en
Switch #
Switch #conf t
Switch(config)#
Switch(config)#interface fa0/2
Switch(config-if)#shutdown

После этого видно, что второй интерфейс находится в нерабочем состоянии. Проверим связность между коммутаторами с помощью команды ping . Команда выполнена успешно, так второй интерфейс находится в рабочем состоянии (рис. 7).

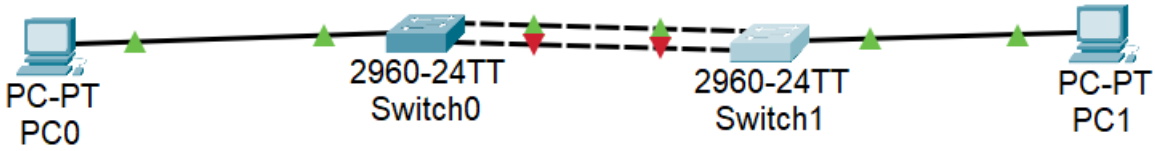


Рисунок 7 - Интерфейс FastEthernet 0/2 выведен из работы

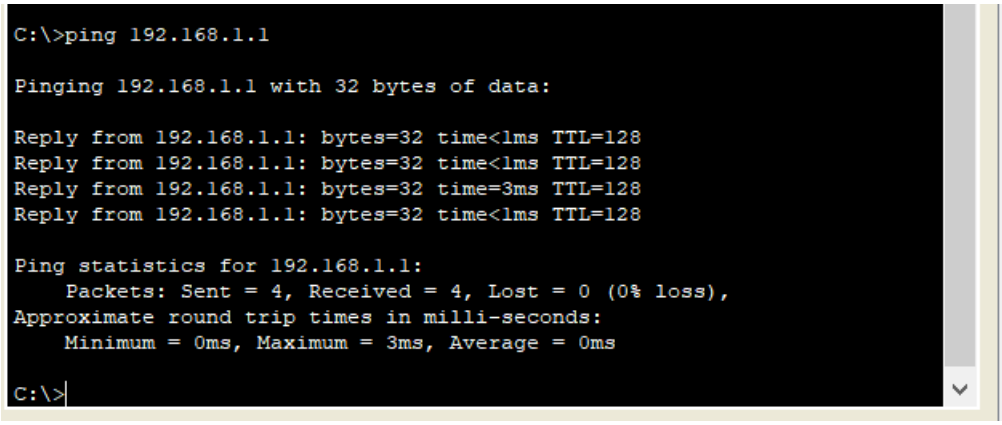


Рисунок 8 - Проверка соединения между коммутаторами после вывода из работы интерфейса FastEthernet 0/2

Содержание отчета

В индивидуальном отчёте должны быть указаны цель, задание, представлены необходимые снимки экрана и пояснения к ним. Следует проанализировать полученные данные и дать ответы на контрольные вопросы.

Контрольные вопросы

1. Как может осуществляться передача пакетов одной сессии, если они будут передаваться по разным портам агрегированного канала? Приведите примеры.
2. Что произойдет, если в агрегированном канале, один выйдет из строя?
3. Чем отличается статическое агрегирование каналов связи от динамического агрегирования?
4. Что нужно сделать для проверки отказоустойчивости агрегированного звена?
5. Какой вид агрегирования каналов установлен в коммутаторе по умолчанию?
6. Опишите функции логического интерфейса Port-channel 1?
7. Для каких целей применяется агрегация каналов?
8. Как распределяется трафик по каналам при объединении портов?
9. Какие характеристики должны быть у портов, агрегированных в канал?
10. Почему в большинстве реализаций механизмов агрегирования используются методы статического, а не динамического распределения кадров по портам?
11. Как называется технология, которая позволяет обеспечить резервирование в случае выхода из строя одного из каналов?
12. Что представляет собой технология агрегирования каналов?

Лабораторная работа №8. Динамическое агрегирование каналов

Цель работы

Рассмотреть сеть, построенную по топологии «Звезда», когда коммутаторы 2-го уровня подключаются к коммутатору 3-го уровня. Изучить динамическое агрегирование каналов.

Задание

Создать высокопроизводительную сеть путём динамического агрегирования каналов коммутаторов и проверить ее работоспособность.

Порядок выполнения работы

1.Открываем Cisco Packet Tracer.

2. Добавляем 3 коммутатора 2960 и один коммутатор 3-го уровня - 3560. Для соединения каждого коммутатора 2960 с коммутатором 3560 перейдем в настройки коммутатора 3-го уровня (рис. 1).

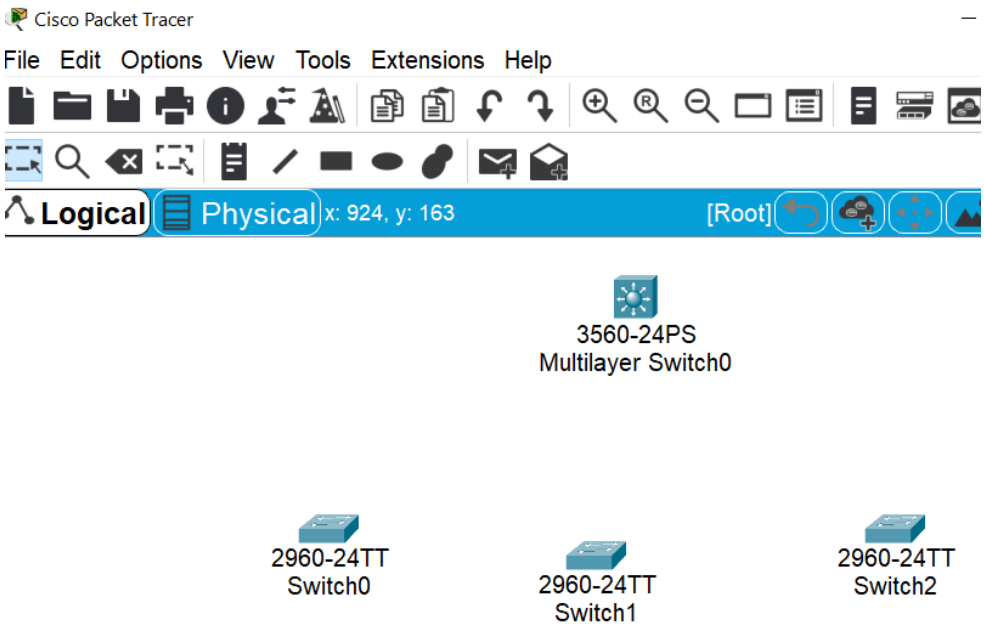


Рисунок 1 – Коммутаторы 2 и 3 уровня

3. Настроим порты FastEthernet на коммутаторе 3560. Для этого переходим во вкладку CLI, заходим в привилегированный режим – **Switch #.** Затем выходим в режим глобального конфигурирования – **Switch(config) #** с помощью сокращенной команды **conf t**. Поскольку интерфейсы будут иметь одинаковые настройки, то мы можем их настроить с помощью одной команды **interface range fa0/1-2.**

Таким образом, настройка коммутаторов во вкладке CLI должны выглядеть следующим образом:

Switch >

Switch >en

Switch #

Switch #conf t

Switch(config)#

Switch(config)#interface range fa0/1-2

Switch(config-if-range)#channel-protocol ? (знак ? показывает все доступные протоколы, мы выбираем протокол LACP)

Switch(config-if-range)#channel- protocol lacp

Далее присваиваем ему channel-group 1

Switch(config-if-range)#channel-group 1 mode active

Switch(config-if-range)#exit

Как видно на рисунке 2, создался логический интерфейс channel-group 1, который объединяет 2 физических интерфейса FastEthernet 0/1-2.

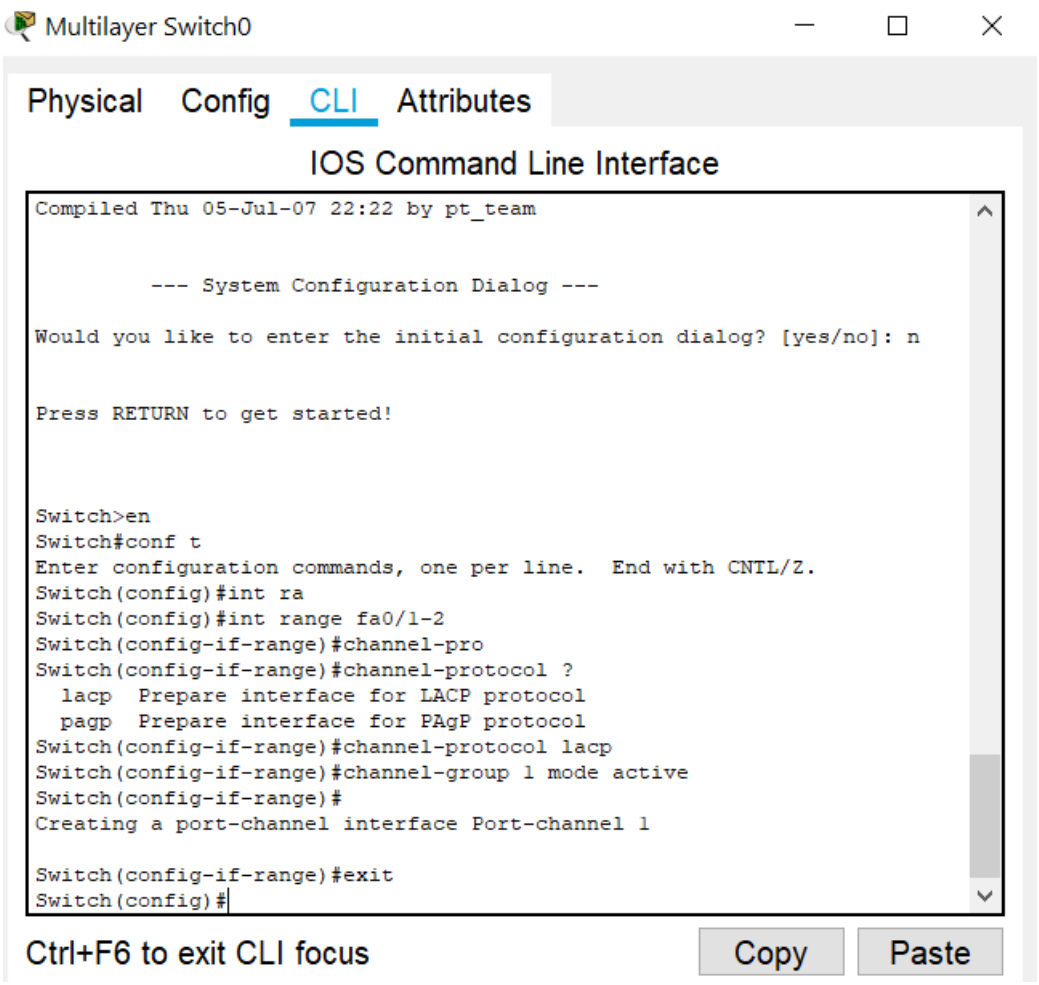


Рисунок 2 - Настройка интерфейсов fa0/1-2 на коммутаторе 3560

Далее аналогичным образом настраиваем интерфейсы FastEthernet 0/3-4 и FastEthernet 0/5-6 и создаем channel-group 2 и channel-group 3.

Switch(config)#interface range fa0/3-4
Switch(config-if-range)#channel-protocol ?
Switch(config-if-range)#channel- protocol lacp
Switch(config-if-range)#channel-group 2 mode active
Switch(config-if-range)#exit

Switch(config)#interface range fa0/5-6
Switch(config-if-range)#channel-protocol ?
Switch(config-if-range)#channel- protocol lacp
Switch(config-if-range)#channel-group 3 mode active

Далее заканчиваем настройки и сохраняем их.

Switch(config-if-range)#end
Switch# wr mem

Результаты настройки интерфейсов fa0/3-4 и fa0/5-6 показаны на рисунке 3.

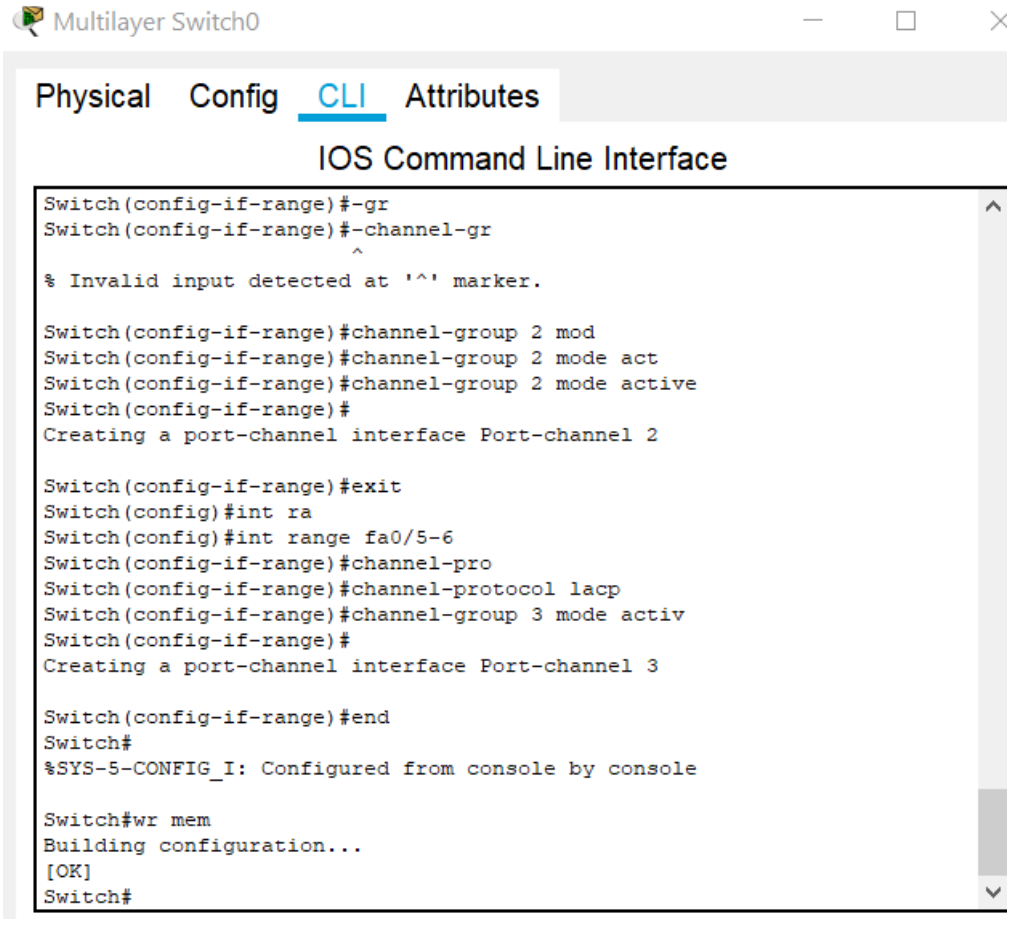


Рисунок 3 - Настройка интерфейсов fa0/3-4 и fa0/5-6 на коммутаторе 3560

4.Теперь произведем настройки для коммутаторов 2960. Настройку проводим для портов fastEthernet 0/1-2, при настройке channel-group выбираем режим passive, так как рекомендуется использовать параметр active только с одной стороны. Но поскольку мы его уже использовали на центральном коммутаторе, то здесь настраиваем passive (рис. 4).

Switch >en
Switch #
Switch #conf t
Switch(config)#
Switch(config)#interface range fastEthernet 0/1-2
Switch(config-if-range)#channel- protocol lacp
Switch(config-if-range)#channel-group 1 mode passive
Switch(config-if-range)#end
Switch# wr mem

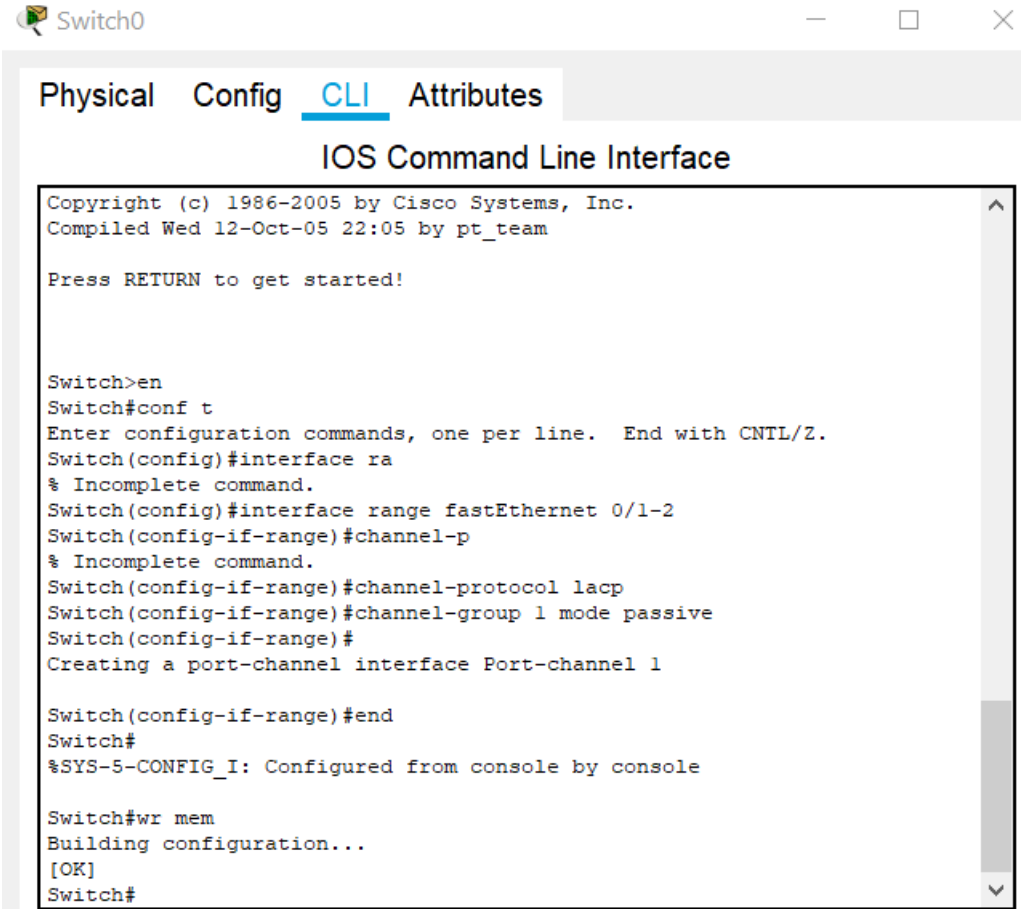


Рисунок 4 - Настройка интерфейсов fa0/1-2 на коммутаторе 2960

Аналогичные действия производим на остальных двух коммутаторах.

5. Далее соединим коммутаторы. Поскольку это устройства разного уровня, то соединяем их прямым кабелем. Соединения производим в соот-

ветствии с теми настройками, которые мы прописали на каждом коммутаторе (табл. 1).

Таблица 1. Настройка интерфейсов на коммутаторах

Коммутатор	Интерфейсы на коммутаторах 2960	Интерфейсы на коммутаторе 3560
Switch 0	FastEthernet 0/1 FastEthernet 0/2	FastEthernet 0/1 FastEthernet 0/2
Switch 1	FastEthernet 0/1 FastEthernet 0/2	FastEthernet 0/3 FastEthernet 0/4
Switch 2	FastEthernet 0/1 FastEthernet 0/2	FastEthernet 0/5 FastEthernet 0/6

Все интерфейсы загорелись зеленым цветом, что показывает, что сеть функционирует. Далее на центральном коммутаторе введем команду:

Switch# show eth

Увидим все группы портов, которые мы объединили по протоколу LACP (рис. 5).

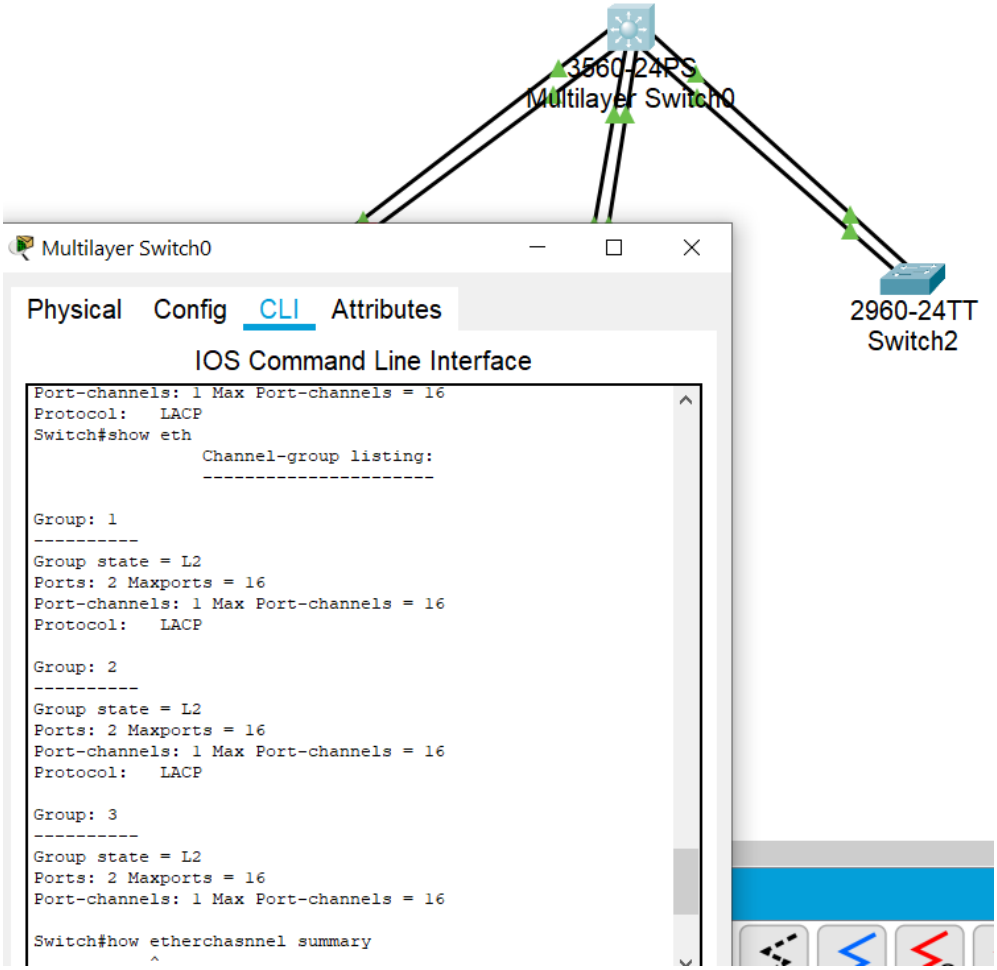


Рисунок 5 - Проверка настроенных портов в коммутаторе 3560

Контрольные вопросы

1.В чем отличие работы портов коммутатора в пассивном и активных режимах?

2.Какие характеристики портов, объединённых в агрегированные каналы, должны быть одинаковые?

3.Какой режим работы нужно в данной лабораторной работе нужно выбрать для коммутатора Cisco 2960 и почему?

4. Как можно проверить отказоустойчивость интерфейса FastEthernet 0/1 на коммутаторе 2-го уровня?

5. Какие режимы работы возможны при настройке канала-группы?

6. Зачем портам присваивается активный или пассивный режимы?

7. Опишите преимущества протокола LACP.

8. Коммутаторы, каких уровней модели OSI используются в данной работе? В чем их отличие?

9. Какими командами выводятся из строя, и вводится в строй интерфейсы коммутатора?

10. На каких участках сети применяется технология агрегирования каналов и почему?

11. С помощью, какой команды можно посмотреть группы портов коммутатора?

Практическое задание №8. Использование коммутаторов 2-го и 3-го уровней для построения компьютерных сетей

Цель работы

Изучить принципы построения сетей на коммутаторах 2-го и 3-го уровней.

Задание

1.Ознакомиться с иерархической моделью компьютерной сети;

2. Ознакомиться с характеристиками коммутаторов;

3.Ответить на вопросы.

Иерархическая модель определяет подход к проектированию сетей и включает в себя три логических уровня (рис. 1):

• уровень доступа (*access layer*);

• уровень распределения/агрегации (*distribution layer*);

• уровень ядра (*core layer*).

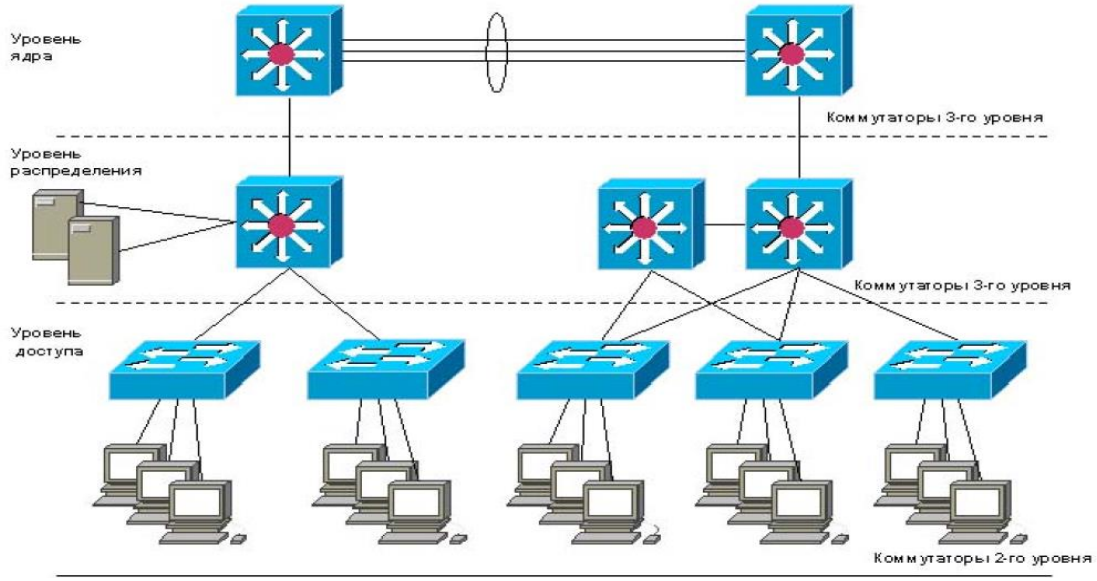


Рисунок 1 - Иерархическая модель компьютерной сети

Уровень ядра находится на самом верху иерархии и отвечает за надежную и быструю передачу больших объемов данных. Трафик, передаваемый через ядро, является общим для большинства пользователей. Сами пользовательские данные обрабатываются на уровне распределения, который, при необходимости, пересылает запросы к ядру.

Уровень распределения (агрегации) является связующим звеном между уровнями доступа и ядра. Он выполняет функции маршрутизации, обеспечения качества обслуживания, безопасности сети, агрегирование каналов, переход от одной технологии к другой (например, от FE к GE).

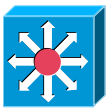
Уровень доступа управляет доступом пользователей (компьютеры, серверы, видеокамеры, IP-телефоны и т.д.) к ресурсам сети. Эти коммутаторы производят сегментирование сети с помощью известной нам технологии VLAN. Коммутаторы уровня доступа могут соединяться между собой только через коммутаторы уровня распределения.

Коммутаторы можно классифицировать в соответствии с уровнями модели OSI, на которых они передают, фильтруют и коммутируют кадры. Различают *коммутаторы уровня 2 (Layer 2 switch)* и *коммутаторы уровня 3 (Layer 3 switch).*

Коммутаторы уровня 2 (L2- коммутаторы) анализируют входящие кадры, принимают решения об их дальнейшей передаче на основе MAC-адресов. Они не осуществляет анализ информации протоколов верхних уровней модели OSI. Эти коммутаторы обычно применяются на уровне доступа сети.

Коммутаторы 2-го уровня на схемах обозначаются  . Коммутацию трафика они производят на основе MAC- адресов. Они коммутируют трафик между портами и между VLAN. Соединение коммутаторов 2-го уровня между собой возможно только через коммутаторы 3-го уровня.

Коммутаторы уровня 3 (L3 - коммутаторы) осуществляют обработку трафика на основе адресов канального уровня и сетевого уровня модели OSI. Коммутаторы 3-го уровня применяются на уровнях ядра и распределения.

На схемах они обозначаются следующим образом  .

Коммутаторы второго уровня подключаются к коммутатору третьего уровня с помощью топологии «Звезда». Такая схема может применяться, например, в многоэтажном здании, где на каждом этаже стоят коммутаторы 2-го уровня, которые по агрегированным каналам соединяется далее с коммутаторами 3-го уровня.

Коммутаторы 3-го уровня поддерживают IP- маршрутизацию, т.е. могут работать с сетевыми устройствами по IP-адресам. Они не только могут разбить сеть на VLAN, но и маршрутизировать трафик между различными сегментами сети. Данные коммутаторы чаще всего используются, как коммутаторы уровня распределения и предназначены для объединения коммутаторов уровня доступа. Он применяется в локальных сетях.

Если не использовать на схеме, изображенной на рисунке 1 коммутаторы уровня распределения, то для соединения коммутаторов 2-го уровня между собой по схеме «каждый с каждым» необходимо организовать гораздо больше соединений, чем при использовании коммутаторов 3-го уровня. Коммутаторы 3 уровня можно отнести уже к разряду маршрутизаторов, но они могут использоваться для маршрутизации трафика только внутри сети. Например, такой коммутатор нельзя использовать для маршрутизации трафика в сеть Интернет. Таким образом, коммутатор 3-го уровня не может заменить маршрутизатор, который ставится на границе сети (рис. 2). У маршрутизатора есть ряд дополнительных функций, например функции межсетевого экрана, NAT (преобразование сетевых адресов), организация VPN т.д. Коммутатор третьего уровня гораздо дешевле маршрутизатора, но он превосходит по производительность маршрутизатора в десятки раз.

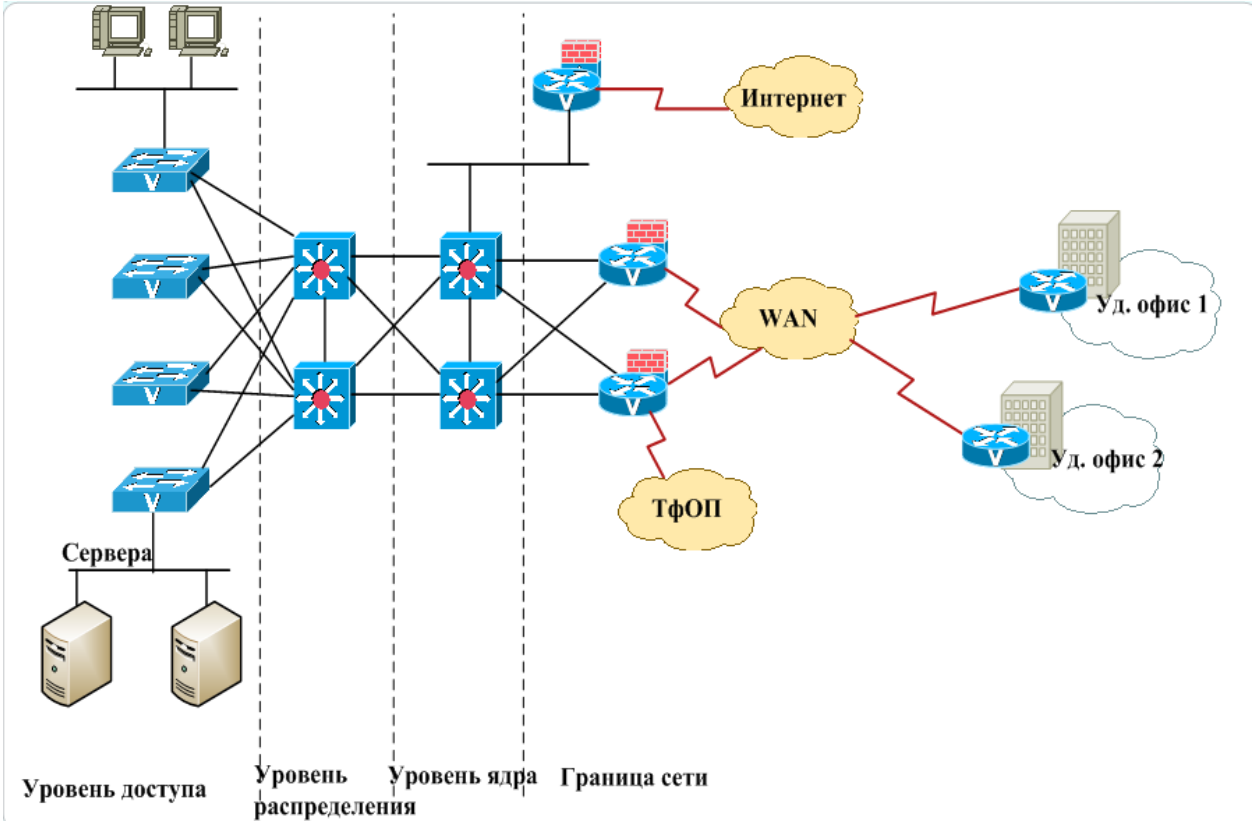


Рисунок 2 - Пример типичной структуры предприятия

Характеристики, влияющие на производительность коммутаторов

Производительность коммутатора. Основными показателями коммутатора, характеризующими его производительность, являются:

- скорость фильтрации кадров;
- скорость продвижения кадров;
- пропускная способность;
- задержка передачи кадра.
- размер буфера (буферов) кадров;
- производительность коммутирующей матрицы;
- производительность процессора или процессоров;
- размер таблицы коммутации;

Скорость фильтрации (filtering) определяет скорость, с которой коммутатор выполняет следующие этапы обработки кадров:

- прием кадра в свой буфер;
- отбрасывание кадра, в случае обнаружения в нем ошибки;
- отбрасывание кадра в соответствии с настроенными на порте фильтрами;

Скорость продвижения (forwarding) определяет скорость, с которой коммутатор выполняет следующие этапы обработки кадров:

- прием кадра в свой буфер;
- просмотр таблицы коммутации с целью нахождения порта назначения на основе MAC-адреса получателя кадра;
- передача кадра в сеть через найденный по таблице коммутации порт назначения.

Обе эти характеристики измеряются обычно *в кадрах в секунду*.

Пропускная способность коммутатора измеряется количеством пользовательских данных (обычно в мегабитах или гигабитах в секунду), переданных в единицу времени через его порты.

Задержка передачи кадра (forward delay) измеряется как время, прошедшее с момента прихода первого байта кадра на входной порт коммутатора до момента появления этого байта на его выходном порту. Задержка складывается из времени, затрачиваемого на буферизацию кадра, а также времени, затрачиваемого на обработку кадра коммутатором, а именно на просмотр таблицы коммутации, принятие решения о продвижении и получение доступа к среде выходного порта.

Для обеспечения временного хранения кадров в тех случаях, когда их невозможно немедленно передать на выходной порт, коммутаторы, в зависимости от реализованной архитектуры, оснащаются буферами на входных, выходных портах или общим буфером для всех портов. Размер буфера влияет как на задержку передачи кадра, так и на скорость потери пакетов. Поэтому чем больше объем буферной памяти, тем менее вероятны потери кадров.

Контрольные вопросы

1. Назовите функции коммутаторов 2-го уровня
2. Назовите функции коммутатора 3-го уровня
3. Какие характеристики влияют на производительность коммутатора?
4. Какие функции выполняет уровень ядра в иерархической модели сети?
5. Опишите функции уровня распределения?
6. Как определяется задержка передачи кадра коммутатора?
7. Что определяет скорость фильтрации кадров?
8. На каком уровне иерархической модели сети применяются коммутаторы 2-го уровня?
9. На каких уровнях иерархической модели сети применяются коммутаторы 3-го уровня?
10. Как измеряется задержка передачи кадра коммутатором?

Лабораторная работа №9. Использование коммутаторов третьего уровня для построения компьютерных сетей

Цель работы

Изучить принципы работы коммутатора третьего уровня

Задание

Построить сеть, состоящую из коммутатора 3-го уровня и трех компьютеров и установить соединения между коммутаторами. Сравнить принципы работы коммутаторов 2-го и 3-го уровней.

Порядок выполнения работы

1.Открываем Cisco Packet Tracer.

2. Создать сеть, изображенную на рисунке 1. Мы хотим разбить эту сеть на 3 сегмента, чтобы наши коммутаторы могли связываться между собой.

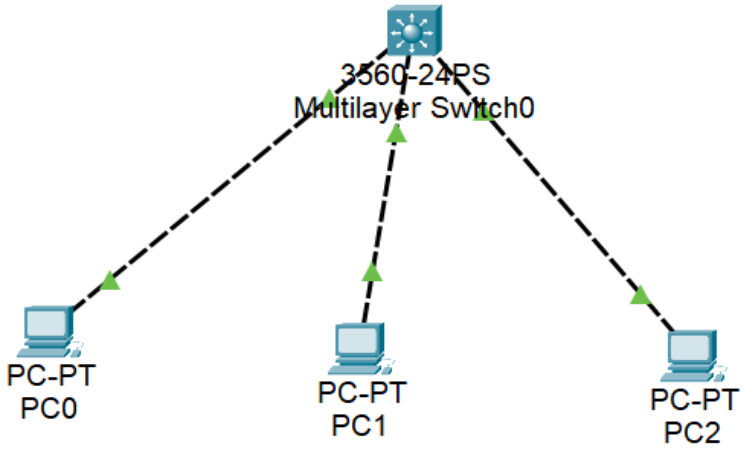


Рисунок 1- Сеть для изучения коммутаторов 3-го уровня

3.Переходим в настройки коммутатора в 3560, в CLI (рис. 2). Мы хотим разбить сеть на три VLAN (VLAN2, VLAN3, VLAN4). Для этого набираем следующие команды:

Switch >en
Switch #
Switch #conf t
Switch(config)#vlan 2
Switch(config- vlan)#name VLAN2
Switch(config-if- vlan)#exit

Switch(config)#vlan 3
Switch(config- vlan)#name VLAN3

Switch(config-if- vlan)#exit

Switch(config)#vlan 4
Switch(config- vlan)#name VLAN4
Switch(config-if- vlan)#end

```
Switch>
Switch>
Switch>en
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#vlan 2
Switch(config-vlan)#name VLAN2
Switch(config-vlan)#exit
Switch(config)#vlan 3
Switch(config-vlan)#name VLAN3
Switch(config-vlan)#exit
Switch(config)#vlan 4
Switch(config-vlan)#name VLAN 4
                           ^
% Invalid input detected at '^' marker.

Switch(config-vlan)#name VLAN4
Switch(config-vlan)#
Switch(config-vlan)#end
Switch#
%SYS-5-CONFIG_I: Configured from console by console
```

Рисунок 2 - Настройка коммутатора 3560

4. Теперь определим порты, в которые подключаются пользователи, к определенному VLAN. Сначала подведем курсор к коммутатору и посмотрим состояние портов (рис. 3).

Port	Link	VLAN	IP Address	IPv6 Address
FastEthernet0/1	Up	1	<not set>	<not set>
FastEthernet0/2	Up	1	<not set>	<not set>
FastEthernet0/3	Up	1	<not set>	<not set>
FastEthernet0/4	Down	1	<not set>	<not set>
FastEthernet0/5	Down	1	<not set>	<not set>
FastEthernet0/6	Down	1	<not set>	<not set>
FastEthernet0/7	Down	1	<not set>	<not set>
FastEthernet0/8	Down	1	<not set>	<not set>
FastEthernet0/9	Down	1	<not set>	<not set>
FastEthernet0/10	Down	1	<not set>	<not set>
FastEthernet0/11	Down	1	<not set>	<not set>
FastEthernet0/12	Down	1	<not set>	<not set>
FastEthernet0/13	Down	1	<not set>	<not set>
FastEthernet0/14	Down	1	<not set>	<not set>
FastEthernet0/15	Down	1	<not set>	<not set>
FastEthernet0/16	Down	1	<not set>	<not set>
FastEthernet0/17	Down	1	<not set>	<not set>
FastEthernet0/18	Down	1	<not set>	<not set>
FastEthernet0/19	Down	1	<not set>	<not set>
FastEthernet0/20	Down	1	<not set>	<not set>
FastEthernet0/21	Down	1	<not set>	<not set>
FastEthernet0/22	Down	1	<not set>	<not set>
FastEthernet0/23	Down	1	<not set>	<not set>
FastEthernet0/24	Down	1	<not set>	<not set>
GigabitEthernet0/1	Down	1	<not set>	<not set>

Рисунок 3 - Состояние портов коммутатора

Пропишем порт FastEthernet 0/1 в VLAN2, порт FastEthernet 0/2 в VLAN3, а порт FastEthernet 0/3 в VLAN4. Для этого произведем конфигурацию на коммутаторе (рис. 4). Заходим в его настройки и набираем команды:

Switch >en
Switch #
Switch #conf t
Switch(config)#
Switch(config)#interface fastEthernet0/1
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 2
Switch(config-if-range)#exit

Тоже самое указываем для других интерфейсов.

Switch(config)#interface fastEthernet0/2
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 3
Switch(config-if-range)#exit

Switch(config)#interface fastEthernet0/3
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 4
Switch(config-if-range)#end

```
Switch#
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#int fa0/1
Switch(config-if)#swi
Switch(config-if)#switchport mode ac
Switch(config-if)#switchport mode access
Switch(config-if)#sw
Switch(config-if)#switchport access vl
Switch(config-if)#switchport access vlan 2
Switch(config-if)#exit
Switch(config)#int fa0/2
Switch(config-if)#sw
Switch(config-if)#switchport mode access
Switch(config-if)#sw
Switch(config-if)#switchport access vlan 3
Switch(config-if)#exit
Switch(config)#int fa0/3
Switch(config-if)#sw
Switch(config-if)#switchport mode access
Switch(config-if)#sw
Switch(config-if)#switchport access vlan 4
Switch(config-if)#end
Switch#
```

Рисунок 4 - Конфигурация на коммутаторе

Смотрим состояние портов с помощью команды (рис. 5):

Switch# show run

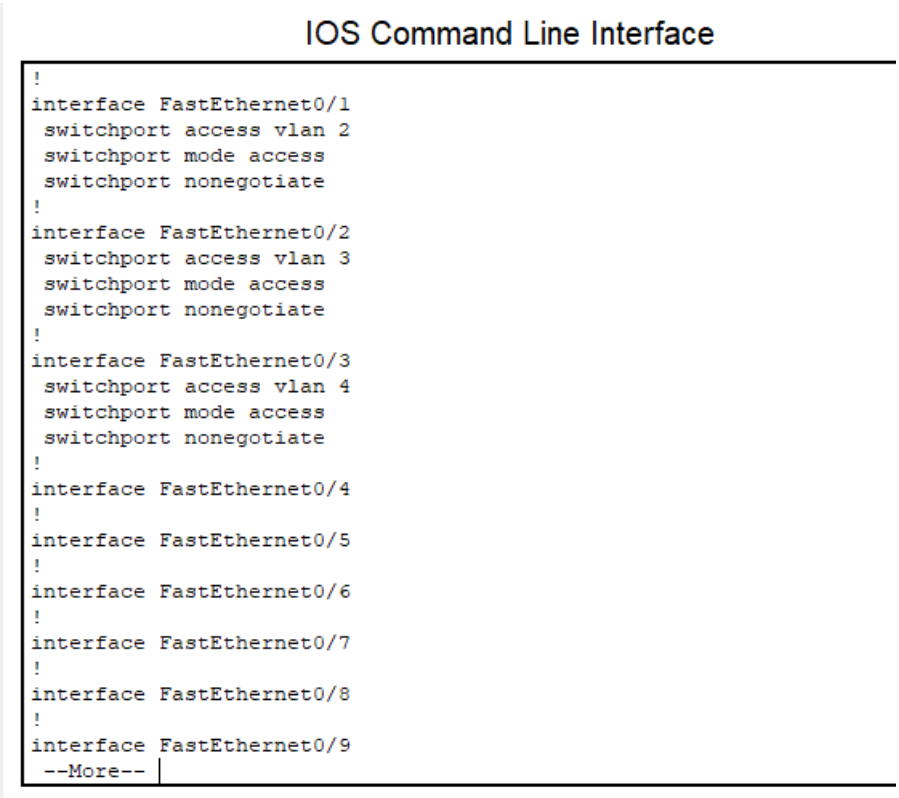


Рисунок 5 - Состояние портов коммутатора после настройки

Поскольку это коммутатор 3-го уровня, то необходимо настроить IP-адреса на созданных сегментах. Для этого в режиме глобального конфигурирования заходим в интерфейс vlan 2, vlan 3, vlan 4 и присваиваем им IP-адреса.

Switch #
Switch #conf t
Switch(config)#int vlan 2
Switch(config-if)#ip address 192.168.2.1 255.255.255.0
Switch(config-if)#exit

Switch(config)#int vlan 3
Switch(config-if)#ip address 192.168.3.1 255.255.255.0
Switch(config-if)#exit

Switch(config)#int vlan 4
Switch(config-if)#ip address 192.168.4.1 255.255.255.0
Switch(config-if)#end

С помощью команды **Switch# show run** можно увидеть IP-адреса, присвоенные виртуальным интерфейсам (рис. 6).

```
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#int vlan 2
Switch(config-if)#ip address 192.168.2.1 255.255.255.0
Switch(config-if)#exit
Switch(config)#int vlan 3
Switch(config-if)#ip adress 192.168.3.1 255.255.255.0
                     ^
% Invalid input detected at '^' marker.

Switch(config-if)#ip address 192.168.3.1 255.255.255.0
Switch(config-if)#exit
Switch(config)#int vlan 4
Switch(config-if)#ip address 192.168.4.1 255.255.255.0
Switch(config-if)#
Switch(config-if)#end
Switch#show run
Building configuration...

Current configuration : 1610 bytes
!
version 12.2(37)SE1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Switch
```

Рисунок 6 - Присвоение IP-адресов виртуальным интерфейсам

```
interface Vlan1
 no ip address
 shutdown
!
interface Vlan2
 mac-address 00e0.b0b4.e401
 ip address 192.168.2.1 255.255.255.0
!
interface Vlan3
 mac-address 00e0.b0b4.e402
 ip address 192.168.3.1 255.255.255.0
!
interface Vlan4
 mac-address 00e0.b0b4.e403
 ip address 192.168.4.1 255.255.255.0
!
ip classless
!
ip flow-export version 9
!
!
!
!
!
 --More-- |
```

Рисунок 7 - Проверка настройки интерфейсов

Зададим следующие IP-адреса компьютерам (табл.1).

Талица 1. IP- адреса для компьютеров

Сетевой элемент	IP-адрес	Маска	Шлюз
PC0	192.168.2.2	255.255.255.0	192.168.2.1
PC1	192.168.3.2	255.255.255.0	192.168.3.1
PC2	192.168.4.2	255.255.255.0	192.168.4.1

И проверим связь между PC0 и коммутатором. Соединение проходит.

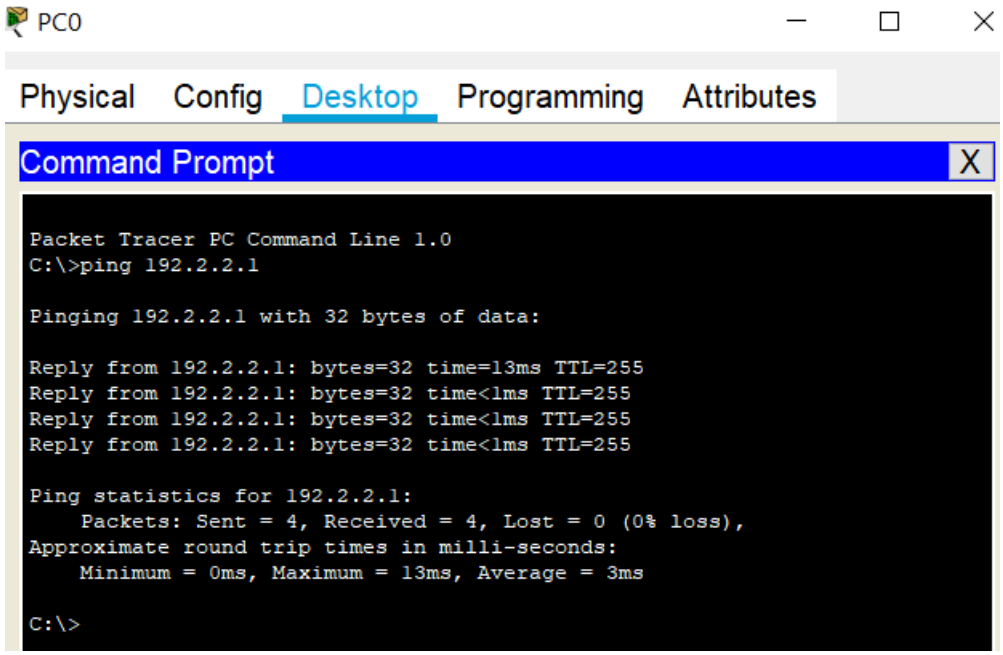


Рисунок 8 - Проверка связи между PC0 и коммутатором

Аналогично проверьте связи между коммутатором и PC1 и PC2. Связи нет. Для того, чтобы связь прошла необходимо на коммутаторе добавить следующие настройки.

Switch #

Switch #conf t

Switch(config)#ip routing

Switch(config)#end

Теперь проверим связь между коммутаторами, например, между PC1 и PC0. Проверим это с помощью команды ping. Связь проходит (рис. 9). Проверьте связь между остальными компьютерами.

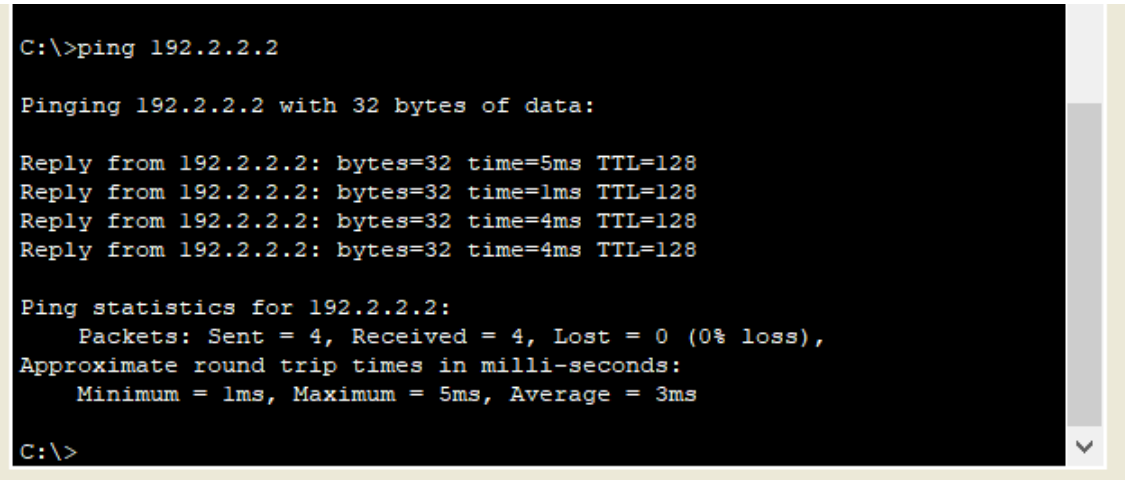


Рисунок 9 - Связь между PC1 и PC0

Контрольные вопросы

1. Опишите последовательность разбиения сети на три VLAN.
2. Почему коммутаторы третьего уровня и персональные компьютеры связаны между собой перекрестным кабелем?
3. Как прописать порт порт FastEthernet 0/1 в VLAN?
4. Как произвести настройку IP- адресов на коммутаторе 3-го уровня?
5. С помощью какой команды можно посмотреть присвоенные IP-адреса?
6. Назовите основные показатели, которые определяют производительность коммутатора.
7. Как определяется пропускная способность коммутатора?
8. Как связаны между собой коммутаторы уровня доступа в иерархической модели компьютерной сети?
9. Опишите функции коммутаторов доступа в иерархической модели компьютерной сети?
10. Назовите функции коммутаторов уровня ядра сети.

Практическая работа №9. Назначение службы DNS и протокола DHCP

Цель работы

Изучить назначение службы DNS и протокола DHCP

Задание

1.Ознакомиться с пространством доменных имен;

2. Ознакомиться с принципами работы протокола DHCP;

3.Ответить на вопросы.

Назначение службы DNS

Для человека символические имена более удобны, чем числовые адреса. В сети Интернет используется система доменных имен, организованная следующим образом. Имеются корневые **домены**. Домен – определенная зона в системе доменных имен (DNS) Интернета, выделенная какой-либо стране, организации. Например, домен **ru** относится к сетям России, корневой домен **de** относится к сетям Германии и т.д. Есть специальные корневые домены: домен **com** (Cisco.com) зарезервирован для коммерческих компаний, домен **org** зарезервирован за некоммерческими организациями.

В стеке TCP/IP применяется доменная система имен, которая имеет иерархическую древовидную структуру, допускающая в имени наличие про-

извольного количества составных частей (рис. 1). Дерево имен начинается с корня, обозначаемое точкой. Затем следует старшая символьная часть имени, вторая по старшинству символьная часть имени и т.д. Младшая часть имени соответствует конечному узлу сети.

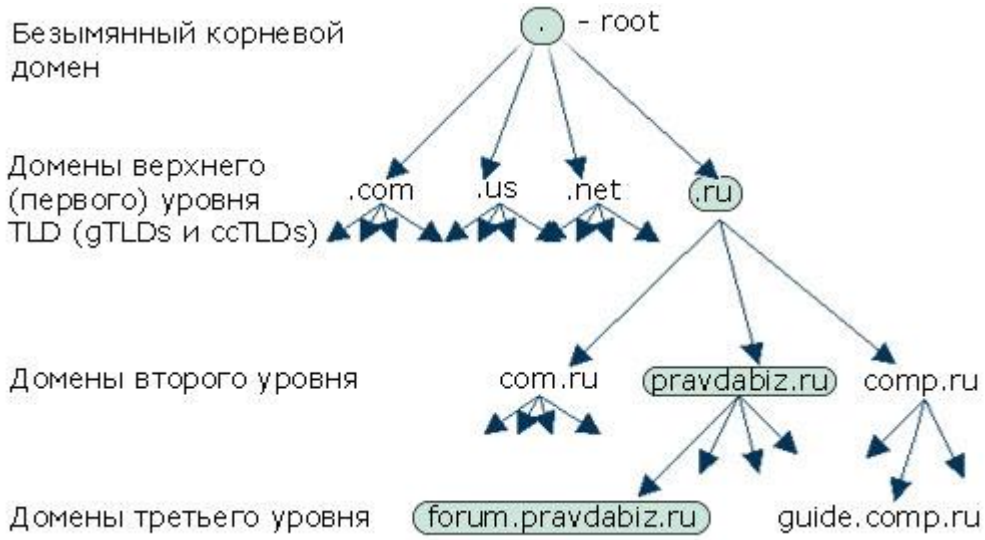


Рисунок 1 -Пространство доменных имен

Составные части доменного имени отделяются друг от друга точкой (рис. 2). Все приложения в сети Интернет используют протокол IP. Поэтому для обмена данными с поставщиком услуг Интернет надо знать IP-адрес сервера поставщика услуг. Если пользователь задает некоторое доменное имя, то его компьютер обращается к специальному серверу в сети Интернет, называемому сервером DNS. У такого сервера имеется база данных о доменных именах, и доменное имя конвертируется в IP-адрес. Запрос и ответ передается через IP-сеть в соответствии со специальным протоколом, также называемым DNS.

Рисунок 2 - Пример доменного имени

Если вы используете доменные имена, то ваш компьютер должен располагать адресом ближайшего DNS-сервера. Конечно, каждыйDNS-сервер не может располагать информацией обо всех доменных именах в мире. Предположим, ваш ближайший DNS-сервер не располагает такой информацией, тогда запрос будет передан следующему DNS-серверу и т.д.

Если ваш ближайший DNS-сервер получает ответ от удаленного DNS-сервера, он запоминает эту информацию, и в дальнейшем поиск IP-адреса происходит быстрее.

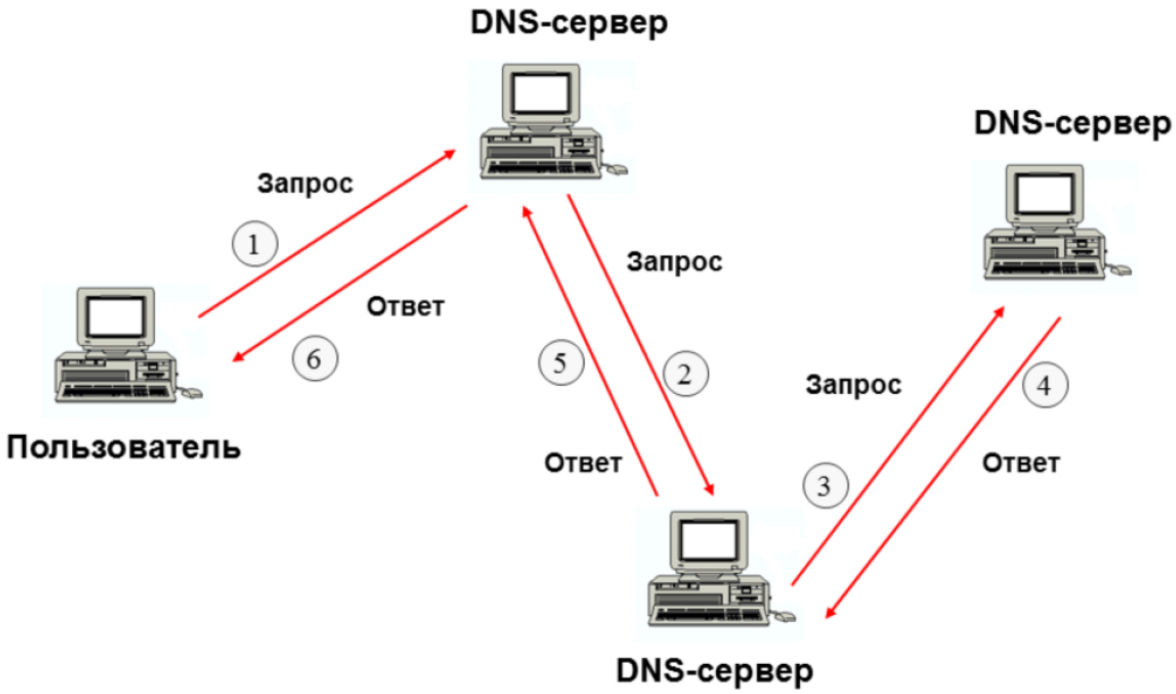


Рисунок 3 - Работа службы доменных имен

Для нормальной работы сети каждому устройству должен быть присвоен IP-адрес. Процедура присвоения адресов происходит в ходе конфигурирования компьютеров и маршрутизаторов. В предыдущих лабораторных работах мы вручную прописывали IP-адреса у каждого компьютера. Конечно, если в сети имеется несколько компьютеров, то прописать IP-адрес для каждого из них не составит большого труда. Но если сеть состоит из большого числа компьютеров, например, 50 или 100, то это становится уже более сложной задачей. А если на сети происходят какие-то изменения, то администратору сети опять придется менять IP-адреса вручную. При этом администратор должен помнить, какие IP-адреса он использовал, а какие еще свободны. При конфигурировании сети помимо IP-адресов устройству назначается маска сети, IP-адрес машрутизатора, IP-адрес DNS- сервера, доменное имя компьютера. Даже при небольшом размере сети это очень утомительная процедура для администратора.

Для автоматического процесса конфигурирования компьютеров (хостов) был придуман протокол DHCP (Dynamic Host Configuration Protocol), который позволяет автоматически настраивать IP-адреса на компьютерах пользователя. Он работает по принципу клиент-сервер. Рассмотрим более подробно работу протокола DHCP. В данном процессе участвуют две стороны. Первая сторона это DHCP – клиент. Это может быть обычный компьютер, ноутбук или смартфон, который подключается через сеть Wi-Fi, это та сторона, которая хочет получить IP-адрес. Вторая сторона это DHCP-сервер, который выдает IP-адреса. В качестве DHCP-сервера может выступать обычный маршрутизатор или специальный сервер. Рассмотрим этот процесс более подробно (рис. 4).

Рисунок 4 - Принципы работы протокола DHCP

В локальной сети одновременно может присутствовать несколько DHCP-серверов, которые должны действовать согласованно.

1.При подключении компьютера к сети он пытается найти DHCP-сервер и выполняет запрос на широковещательный адрес 255.255.255.255, рассылая пакет DHCPDISCOVER. В этом запросе он указывает свой MAC-адрес. Этот запрос обозначает, что компьютеру нужен IP-адрес и он обращается за ним к серверам DHCP. Все компьютеры локальной сети получают такой запрос, но обрабатывается он только DHCP-серверами.

2. Все DHCP-серверы отвечают на запрос сообщением DHCPOFFER, предлагая значение IP-адреса.

3.Хост выбирает один из предложенных адресов и посылает широковещательный запрос DHCPREQUEST, сообщая, что один из предложенных адресов выбран. Такой запрос содержит идентификатор сервера, предложившего выбранный IP-адрес.

4.Сервер, предложивший выбранный IP-адрес, отвечает подтверждением DHCPPARK.

5.После окончания работы хост отправляет сообщение DHCPRELEASE, освобождая выбранный IP-адрес.

В качестве сервера DHCP в компьютерных сетях могут использоваться машины, работающие под управлением Windows Server, Linux, FreeBSD или других серверных операционных систем, а также аппаратные устройства, такие как, маршрутизаторы и точки доступа. Минимальная настройка сервера DHCP заключается в определении диапазона свободных IP-адресов.

DHCP-сервер может работать в следующих режимах:

- ручное назначение статических адресов;
- автоматическое назначение статических адресов;
- автоматическое распределение динамических адресов.

В **ручном** режиме администратор помимо списка доступных адресов снабжает DHCP-сервер информацией о жестком соответствии IP-адресов физическим адресам или другим идентификаторам клиентских узлов. DHCP-сервер, пользуясь этой информацией, всегда выдаст определенному DHCP-клиенту один и тот же назначенный ему администратором IP-адрес, а также другие конфигурационные параметры.

В режиме **автоматического** назначения статических адресов DHCP-сервер самостоятельно без вмешательства администратора произвольным образом выбирает компьютеру IP-адрес из списка наличных IP-адресов. Адрес дается клиенту в постоянное пользование, т.е. между информацией, идентифицирующей клиента и его IP-адресом, как и при ручном назначении, существует постоянное соответствие. При всех последующих запросах сервер возвращает клиенту тот же IP-адрес.

При **динамическом** распределении адресов DHCP-сервер выдает адрес клиенту на ограниченное время, называемое сроком аренды. Когда компьютер, который является клиентом DHCP, удаляется из сети, назначенный ему IP-адрес автоматически освобождается. Это дает возможность использовать этот IP-адрес при подключении другого компьютера. Так, например, если сотрудник уехал в командировку со своим ноутбуком, то освободившийся IP-адрес может использовать другой сотрудник данной организации. Таким образом, общее количество IP-адресов, необходимое организации равно числу сотрудников, которые присутствуют в офисе.

При динамическом распределении адресов администратору при настройке DHCP-сервера достаточно один раз указать диапазон адресов, а каждый вновь прибывший сотрудник будет физически подключать в сеть свой компьютер, на котором запускается DHCP-клиент.

Контрольные вопросы

1. Опишите назначение службы DNS
2. Какие функции DHCP-сервера вы можете назвать?
3. Опишите ручной способ назначение статических адресов.
4. Опишите автоматическое назначение статических адресов.
5. Какие особенности автоматического распределения динамических адресов?
6. Пользователь выходит в сеть Интернет со своего смартфона через сеть Wi-Fi. Какой способ назначения IP-адреса будет применен в данном случае?
7. Опишите сигнальный обмен по протоколу DHCP.
8. Что такое домен?
9. Напишите доменное имя вашей организации.
10. Какие устройства могут выступать в роли DHCP- сервера?

Лабораторная работа №10. Изучение протокола DHCP с использованием Cisco Packet Tracer

Цель работы

Изучить принципы работы протокола DHCP.

Задание

Построить сеть, состоящую из маршрутизатора, коммутатора и трех компьютеров. В качестве DHCP сервера необходимо использовать маршрутизатор. Прописать список IP-адресов, которые необходимо назначать устройствам в данной сети и проверить работоспособность сети.

Порядок выполнения работы

1.Открываем Cisco Packet Tracer.

2. Создать сеть, изображенную на рисунке 1.

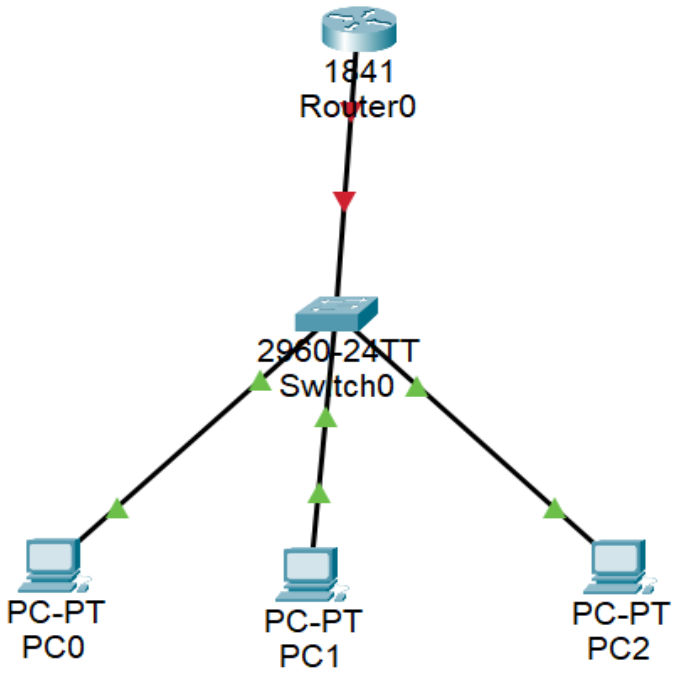


Рисунок 1 - Сеть для исследования протокола DHCP

Далее отказываемся от системной конфигурации и на вопрос « Continue with configuration dialog?» отвечаем **no**.

Настраиваем маршрутизатор с помощью следующих команд:

Router>en
Router #
Router #conf t
Router (config)#int fa0/0
Router (config-if)#no shutdown
Router (config-if)#ip address 192.168.1.1 255.255.255.0
Router (config-if)#exit

Теперь надо создать DHCP pool, т.е. пространство IP-адресов, которое мы будем использовать в данной сети. Дадим ему название DHCP. В данной схеме в качестве DHCP сервера выступает машрутизатор (роутер), поэтому и адреса назначаем из сети, в которой находится маршрутизатор, т.е. из сети 192.168.1.0. Каждому компьютеру нам необходимо выдать IP-адрес, а также адрес шлюза, через который маршрутизируется трафик (шлюз по умолчанию - Default gateway). В качестве шлюза по умолчанию записываем IP-адрес маршртизатора- 192.168.1.1. Также для доступа в сеть Интернет необходимо указать DNS сервер. В качестве примера зададим DNS компании Google.

Router (config)#ip dhcp pool DHCP
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 8.8.8.8
Router (dhcp-config)#exit

Предположим у нас есть сервер с IP-адресом 192.168.1.100 (на схеме не показан). Мы должны исключить его из пула адресов, чтобы этот адрес не присваивался другим устройствам сети. Серверам, которым необходим постоянный доступ в сеть Интернет, не рекомендуется выдавать динамические IP-адреса. Им лучше назначать статические адреса. Для исключения адреса 192.168.1.100 напишем следующую команду:

Router (config)#ip dhcp excluded-address 192.168.1.100

Также исключим IP-адрес, который есть у роутера.

Router (config)#ip dhcp excluded-address 192.168.1.1
Router (config)#exit
Router (config)#wr mem

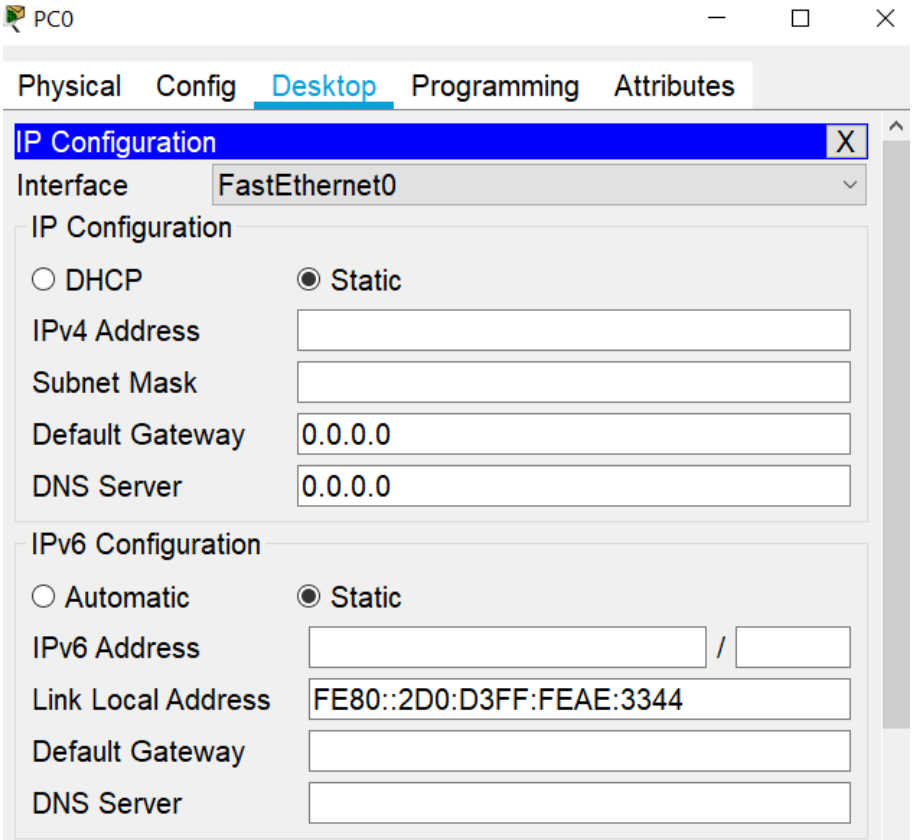


Рисунок 2 - По умолчанию стоит параметр Static

Меняем параметр Static на DHCP и компьютер PC0 автоматически получает IP-адрес, маску, адрес шлюза, а также DNS-сервер.

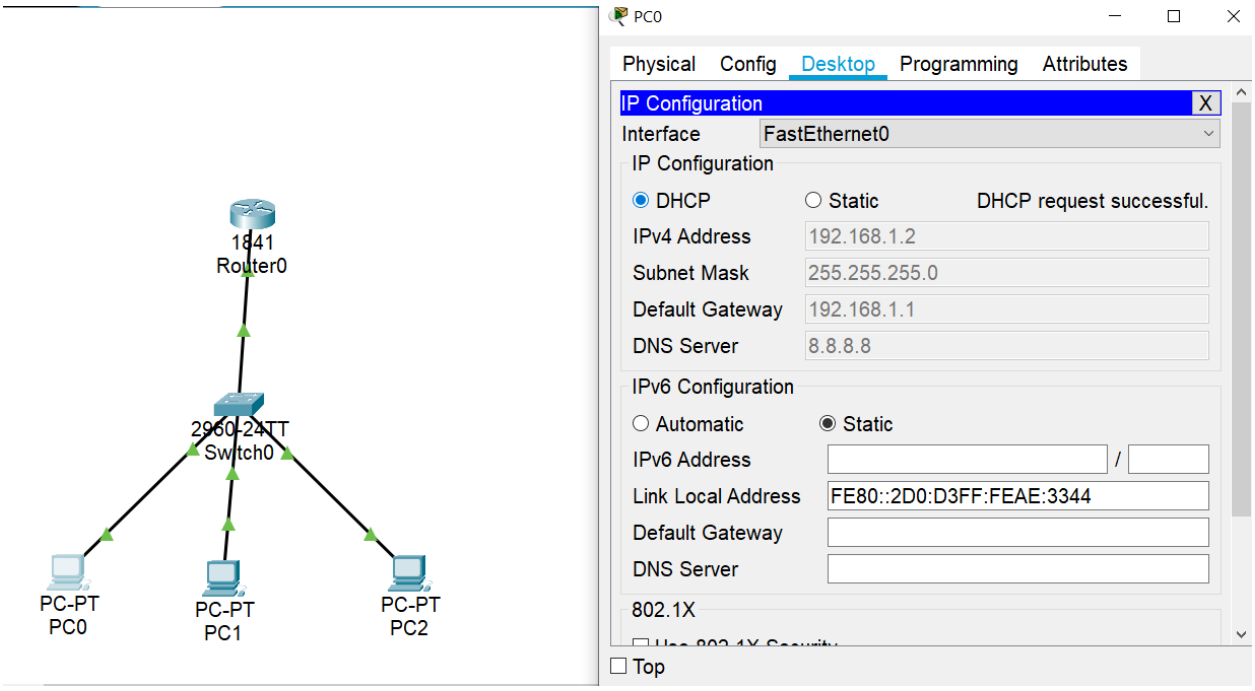


Рисунок 3 - Компьютер получил IP-адрес по протоколу DHCP

Аналогично и другие компьютеры получают IP-адреса. Компьютер PC1 получает адрес 192.168.1.3, а PC2 – 192.168.1.4.

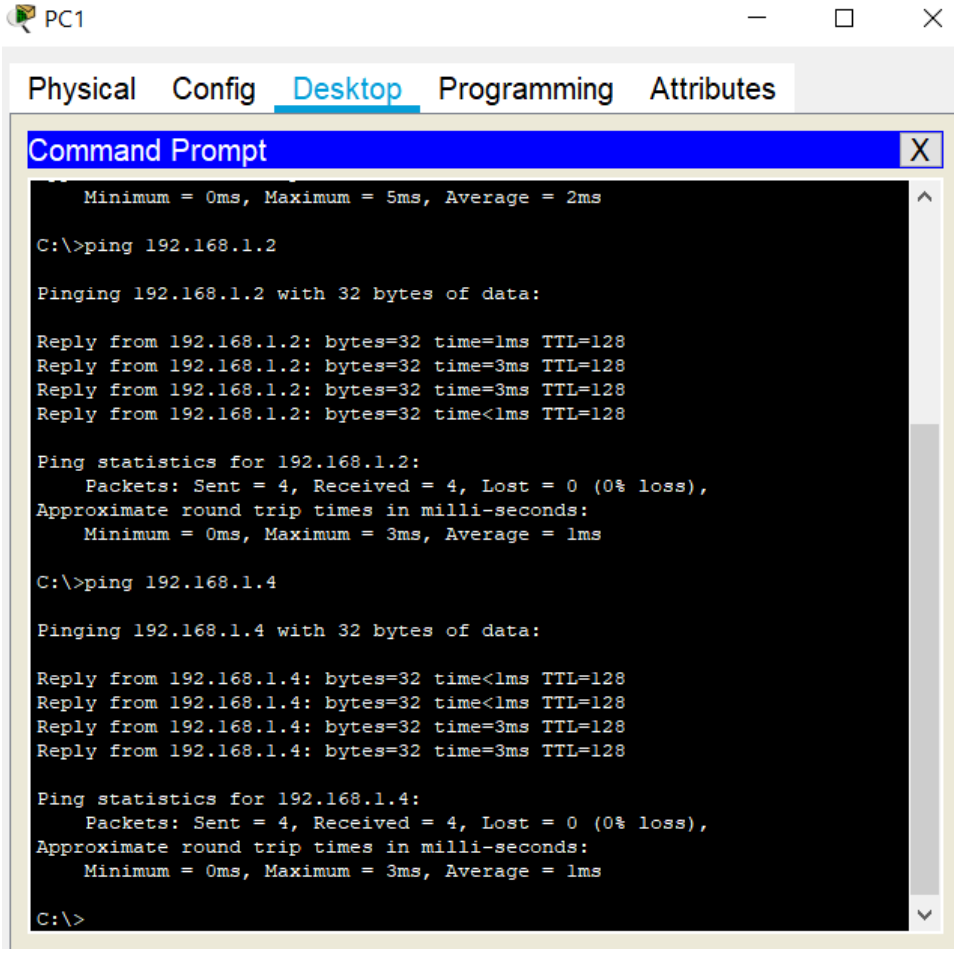


Рисунок 4 - Проверка связи между компьютерами PC0, PC1 и PC2

Проверим взаимосвязь между компьютерами. Так для PC1 проверка связи показана на рисунке 4. Проверить связность между всеми компьютерами.

Содержание отчета

В индивидуальном отчёте должны быть указаны цель, задание, представлены необходимые снимки экрана и пояснения к ним. Следует проанализировать полученные данные.

Практическая работа №10.Статическая и динамическая маршрутизации

Цель работы

Изучить принципы статической и динамической маршрутизации

Задание

1.Ознакомиться со статической маршрутизацией;
2. Ознакомиться с динамической маршрутизацией;
3.Ответить на вопросы.

Маршрутизация является функцией третьего уровня модели OSI. Под термином ‘‘маршрутизация’’подразумевают процесс определения наиболее эффективного пути от одного устройства к другому. Основным устройством, отвечающим за осуществление процесса маршрутизации, является ***маршрутизатор.***

Маршрутизатор выполняет две ключевые функции:

-поддерживает таблицы маршрутизации и обменивается информацией об изменениях в топологии сети с другими маршрутизаторами. Эта функция реализуется с помощью одного или нескольких протоколов маршрутизации;

-когда пакеты приходят на один из интерфейсов, маршрутизатор, руководствуясь таблицей маршрутизации, должен определить, куда именно следует отправить пакет.

При этом он использует одну или несколько ***метрик маршрутизации*** для того чтобы установить оптимальный путь, по которому должен следовать сетевой трафик. Метрика маршрутизации это параметр, по которому определяется наиболее предпочтительный маршрут. Для определения наилучшего межсетевого маршрута вычисляются различные метрики: полоса пропускания, задержки, надежность, загрузка, стоимость и др.

Маршрутизаторы используют протоколы маршрутизации для обмена таблицами маршрутизации и совместного использования информации о доступных маршрутах.

При **статической** маршрутизации все записи в таблице имеют неизменяемый статически статус, что подразумевает бесконечный срок их жизни. Записи о маршрутах составляются и вводятся в память каждого маршрутизатора вручную администратором сети. При изменении состоянии сети администратор должен отразить эти изменения в таблице маршрутизации. Статическая маршрутизация не подходит для большинства сложных систем, так как сети включают избыточные связи, смешанные топологии и разнообразные протоколы. При статической маршрутизации администратор полностью контролирует сеть, т.е. какой маршрут прописали, так и будет работать сеть. Это является ее плюсом.

При **динамической (адаптивной)** маршрутизации все изменения в конфигурации сети автоматически отражаются в таблицах маршрутизации благодаря протоколам маршрутизации. Эти протоколы собирают информацию о топологии связей в сети, что позволяет им оперативно отражать все текущие изменения. В таблицах маршрутизации обычно имеется информация об интервале времени, в течение которого данный маршрут будет оставаться действительным. Это время называется время жизни маршрута (TTL). Если по истечении времени жизни существование маршрута не подтверждается протоколом маршрутизации, то он считается не рабочим и пакеты по нему больше не посылаются.

Достоинства динамической маршрутизации:

- автоматическое добавление маршрута;

- организация отказоустойчивости сети. Так, если сеть доступна по двум или более маршрутам, то при недоступности основного маршрута произойдет автоматическое переключение на другой маршрут.

Недостатки динамической маршрутизации:

- более высокая загрузка вычислительных ресурсов сети (память и процессор);

-требуется более высокая квалификация инженеров при поиске неисправностей;

- сеть менее предсказуема, т.е. если сеть очень сложная, то не всегда можно сказать, как пойдет тот или иной маршрут.

Сами протоколы динамической маршрутизации можно классифицировать по нескольким критериям.

По алгоритмам:

1) дистанционно-векторные протоколы (Distance-vector Routing Protocols) – RIP;

2) протоколы состояния каналов связи (Link-state Routing Protocols) - OSPF, IS-IS.

Иногда выделяют третий класс, усовершенствованные дистанционно-векторные протоколы (advanced distance-vector), для того чтобы подчеркнуть существенные отличия протоколов от классических дистанционно-векторных, например EIGRP.

По области применения:

1) протоколы междоменной маршрутизации (EGP) - BGP ;

2) протоколы внутридоменной маршрутизации (IGP): OSPF, RIP, EIGRP, IS-IS.

IGP (Interior Gateway Protocol). IGP-протоколы используются для передачи информации о маршрутах в пределах автономной системы (AS). Как правило, для упрощения, можно воспринимать автономную систему, как сеть одной компании. К современным IGP-протоколам, как правило, предъявляются такие требования:

1) быстрая сходимость;

2) выбор маршрутов в зависимости от физических характеристик сети (полоса пропускания, задержка);

3) поддержка масок переменной длины (VLSM);

4) возможность суммировать маршруты.

Если говорить об использовании IGP-протоколов в сетях крупных провайдеров, то также можно добавиться такие требования:

1) поддержка большого количества маршрутов;

2) совместимость и поддержка других технологий.

EGP (Exterior Gateway Protocol). EGP-протоколы используются для передачи информации между автономными системами (AS). На текущий момент представителем этого класса является один протокол BGP. Хотя, чаще всего, BGP используется для передачи маршрутов между разными AS, он может также использоваться и внутри корпоративной сети. Особенно, когда сеть большая.

OSPF (Open Shortest Path First) — протокол динамической маршрутизации. Он используется для передачи информации между маршрутизаторами в пределах одной автономной системы (AS).

Протокол OSPF разбивает процедуру построения таблицы маршрутизации на 2 этапа. К первому относится построение и поддержание базы данных о состоянии связей сети, ко второму построение оптимального маршрута и генерация таблиц маршрутизации.

Построение и поддержание базы данных о состоянии связей сети

Сети связи могут быть представлены в виде графа, в которых вершинами графа являются маршрутизаторы, а ребрами – связи между ними. Каждый маршрутизатор обменивается со своими соседями о текущей конфигурации графа связей сети.

Для контроля состояния связей между собой маршрутизаторы передают каждые 10 секунд сообщения Hello. Если это сообщение не поступает от соседа, то маршрутизатор делает вывод, что состояние связи между ними изменилось на неработоспособное и вносит соответствующие корректировки в свою базу данных. Одновременно он отсылает своим соседям объявления о состоянии связей - LSA (Link State Advertisment).

Построение оптимального маршрута и генерация таблиц маршрутизации

Задача нахождения оптимального пути на графе является достаточно сложной. Для ее решения используется алгоритм Дейкстры. Каждый маршрутизатор в соответствии с этим алгоритмом ищет оптимальные маршруты от своих интерфейсов до всех известных ему сетей. В каждом найденном маршруте запоминается только один шаг – до следующего маршрутизатора. Эти данные и попадают в таблицу маршрутизации. При изменении состояния связей в сети, каждый маршрутизатор заново ищет оптимальные маршруты и корректирует свою таблицу маршрутизации. Если в сети появляется новый маршрутизатор, он объявляет о себе сообщением Hello.

Вычислительная сложность алгоритма Дейкстры предъявляет высокие требования к мощности процессоров маршрутизаторов. Каждые 30 минут маршрутизаторы обмениваются всеми записями баз данных, т.е. синхронизируют их для более надежной работы сети.

Контрольные вопросы

1. К какому уровню модели OSI относится марщрутизация?
2. Какие функции выполняет маршрутизатор?
3. Что такое метрика маршрутизации?
4. Опишите цель таблицы маршрутизации?
5. Что представляет собой статическая маршрутизация?
6. Что представляет собой динамическая маршрутизация?
7. Назовите достоинства и недостатки статической маршрутизации?
8. Назовите достоинства и недостатки динамической маршрутизации?
9. Как можно классифицировать протоколы динамической маршрутизации?
10. Приведите примеры протоколов динамической маршрутизации.

Лабораторная работа №11. Изучение процесса работы протокола динамической маршрутизации OSPF с использованием Cisco Packet Tracer

Цель работы

Изучить и практически освоить процесс настройки протокола динамической маршрутизации OSPF с использованием сетевого симулятора Cisco Packet Tracer. Научиться настраивать протокол OSPF на маршрутизаторах, проверять доступность различных узлов сети.

Задание

1. Ознакомиться с основными понятиями динамической маршрутизации и протокола OSPF в частности.
2. Запустить Cisco Packet Tracer.
3. Собрать необходимую топологию сети, запустить и настроить виртуальное оборудование.
4. Согласно пунктам выполнения лабораторной работы, сделать необходимые снимки экрана. Изучить полученную информацию и оформить ее в соответствии с требованиями раздела «Содержание отчета».
5. Ответить на вопросыю

Порядок выполнения работы

1.Предварительная настройка сетевого оборудования

Соберите сетевую топологию согласно рисунку 1. Топология содержит 3 ПК и 3 маршрутизатора (Cisco 2911), на которых необходимо настроить динамическую маршрутизацию с использованием OSPF.

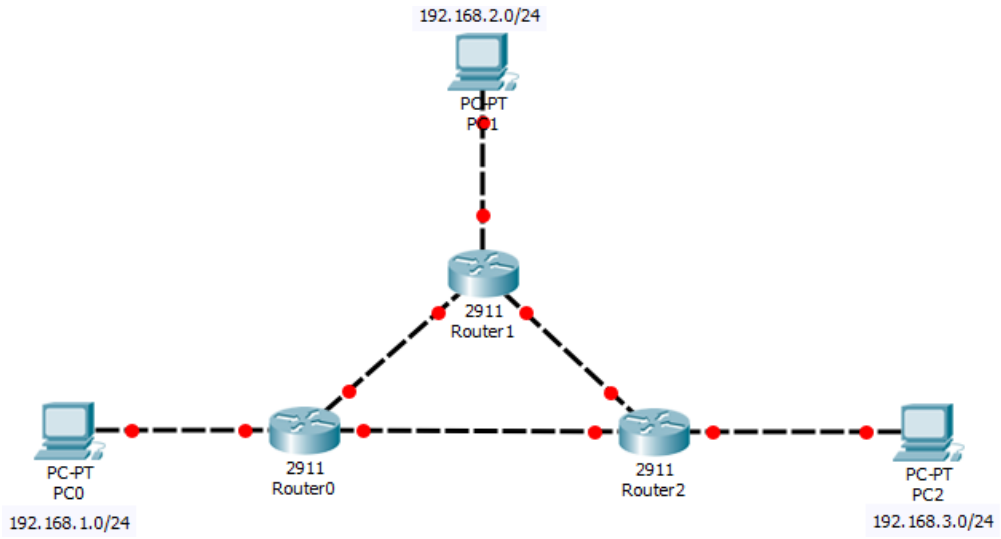


Рисунок 1 - Топология сети

Каждому компьютеру присвойте IP-адрес: PC0 – 192.168.1.2/24 (шлюз по умолчанию 192.168.1.1); PC1 – 192.168.2.2/24 (шлюз по умолчанию 192.168.2.1); PC2 – 192.168.3.2/24 (шлюз по умолчанию 192.168.3.1). Для того чтобы назначить сетевые адреса компьютерам, один раз нажмите левой кнопкой мыши на устройстве и перейдите в закладку Desktop, а затем нажмите на IP Configurations. Введите IP-адрес, маску подсети и шлюз по умолчанию в соответствующие поля, как это показано на рисунке 2 для PC0. Повторите для других компьютеров.

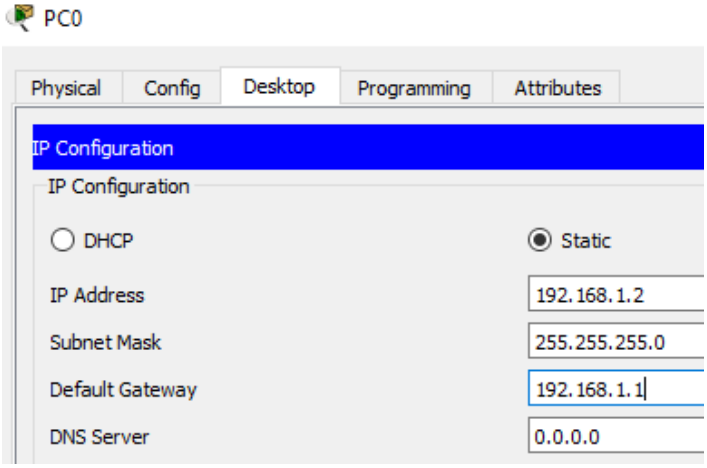


Рисунок 2 - Конфигурация для PC0

Необходимо удостовериться в правильности введенных настроек. Для этого один раз нажмите левой кнопкой мыши на устройстве и перейдите в закладку Desktop, а затем нажмите на Command Prompt. Введите команду:

C:\>ipconfig

Сделайте снимок экрана. Повторите для других PC.

Настройте все маршрутизаторы согласно таблице 1.

Таблица 1. Сетевые адреса маршрутизаторов

Маршрутизатор	Интерфейс	IP-адрес	Маска подсети
Router0	Gig0/0	10.10.10.1	30 бит – 255.255.255.252
	Gig0/1	10.10.11.1	30 бит – 255.255.255.252
	Gig0/2	192.168.1.1	24 бита – 255.255.255.0
Router1	Gig0/0	10.10.10.2	30 бит – 255.255.255.252
	Gig0/1	10.10.12.1	30 бит – 255.255.255.252
	Gig0/2	192.168.2.1	24 бита – 255.255.255.0
Router2	Gig0/0	10.10.12.2	30 бит – 255.255.255.252
	Gig0/1	10.10.11.2	30 бит – 255.255.255.252
	Gig0/2	192.168.3.1	24 бита – 255.255.255.0

Настройте маршрутизатор Router0, для этого один раз нажмите по устройству и перейдите во вкладку CLI, на задаваемый вопрос введите **no**, затем вводите следующие команды (для завершения команды пользуйтесь клавишей **Tab**):

```
Router>enable
Router#configure terminal
Router(config)#interface gigabitEthernet 0/0
Router(config-if)#ip address 10.10.10.1 255.255.255.252
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#interface gigabitEthernet 0/1
Router(config-if)#ip address 10.10.11.1 255.255.255.252
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#interface gigabitEthernet 0/2
Router(config-if)#ip address 192.168.1.1 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#exit
Router#wr mem
```

Повторите настройки для маршрутизаторов Router1 и Router2 с адресами, взятыми из таблицы. Проверьте доступность шлюзов с каждого ПК. Для этого один раз нажмите левой кнопкой мыши на устройстве и перейдите в закладку Desktop, а затем нажмите на Command Prompt (рисунок 3) и введите команду ping**.**

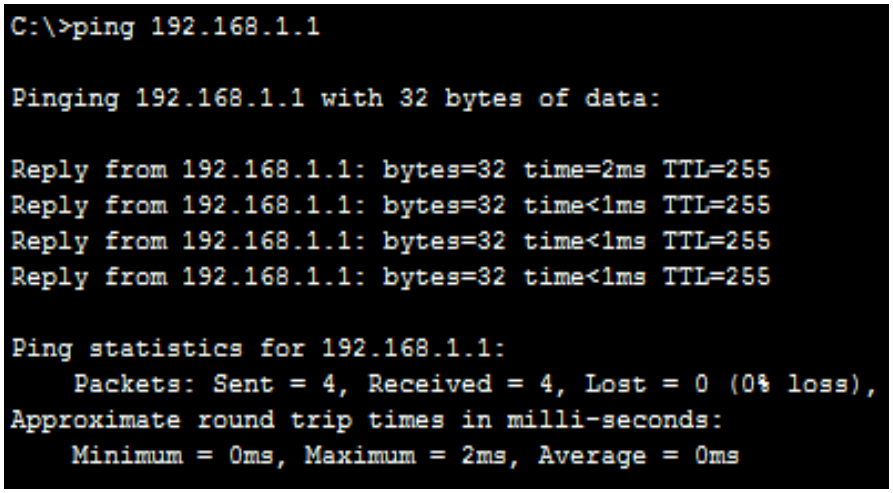


Рисунок 3 - Проверка связности для компьютера PC0

2.Настройка OSPF протокола

Прежде чем настроить протокол динамической маршрутизации, следует настроить адрес на loopback-интерфейсе. Это необходимо для корректной работы протокола OSPF. Loopback-интерфейс – логический интерфейс, не привязанный к физическим. Аналогичный адрес есть на любом из компьютеров.

Настраиваем loopback-интерфейс на Router0:

Router>enable
Router#configure terminal
Router(config)#interface loopback 0
Router(config-if)#ip address 192.168.100.1 255.255.255.255 (192.168.100.0/32 – сеть для всех loopback-интерфейсов. Маска 32 бита подразумевает всего один IP-адрес)
Router(config-if)#no shutdown
Router(config-if)#exit

Приступаем непосредственно к настройке OSPF, для этого входим в режим конфигурирования роутера, выбираем протокол ospf и задаем номер процесса 1:

Router(config)#router ospf 1

Указываем все сети, которые подключены к нашему маршрутизатору:
Router(config-router)#network 192.168.1.0 0.0.0.255 area 0 (0.0.0.255 – обратная маска (смотрите таблицу), все маршрутизаторы должны быть в одной области **area 0**)
Router(config-router)#network 10.10.10.0 0.0.0.3 area 0
Router(config-router)#network 10.10.11.0 0.0.0.3 area 0
Router(config-router)#end
Router#wr mem
Как только мы ввели эти команды OSPF автоматически включается на всех интерфейсах, которые соответствуют данном у диапазону адресов.
Router#show running-config (после введения команды используйте клавиши «Пробел» или «Enter» для просмотра настроек) найдите в выведенных настройках строчки с назначенными портам адресами и занесите снимок экрана в отчет (рисунок 4.).

```
interface Loopback0
 ip address 192.168.100.1 255.255.255.255
!
interface GigabitEthernet0/0
 ip address 10.10.10.1 255.255.255.252
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 ip address 10.10.11.1 255.255.255.252
 duplex auto
 speed auto
!
interface GigabitEthernet0/2
 ip address 192.168.1.1 255.255.255.0
 duplex auto
 speed auto
!
interface Vlan1
 no ip address
 shutdown
!
router ospf 1
 log-adjacency-changes
 network 192.168.1.0 0.0.0.255 area 0
 network 10.10.10.0 0.0.0.3 area 0
 network 10.10.11.0 0.0.0.3 area 0
```

Рисунок 4 - Настройки портов и OSPF на маршрутизаторе Router0

Для маршрутизаторов Router1 и Router2 повторить настройки, при этом для них адреса loopback-интерфейсов 192.168.100.2 и 192.168.100.3 соответственно, area 0 для Router1 и Router2. Соседние сети можно посмот реть в настройках каждого роутера. После настройки OSPF на маршрутизаторе Router1 появится сообщение:

01:10:34: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.100.1 on GigabitEthernet0/0 from LOADING to FULL, Loading Done

Оно означает, что был найден «сосед». Занесите снимок экрана в отчет. Повторите для маршрутизатора Router2.

На маршрутизаторе Router2 введите:

Router#show ip ospf neighbor

Видно, что маршрутизатор нашел двух «соседей» (рисунок 5):

```
Neighbor ID     Pri   State           Dead Time   Address
Interface
192.168.100.2     1   FULL/DR         00:00:31    10.10.12.1
GigabitEthernet0/0
192.168.100.1     1   FULL/DR         00:00:31    10.10.11.1
GigabitEthernet0/1
```

Рисунок 5 - Вывод информации о «соседях» маршрутизатора Router2

Для получения информации из таблицы маршрутизации введите команду:
Router#show ip route

Записи, рядом с которыми есть символ «O», означают, что маршрут создан с использованием протокола динамической маршрутизации OSPF (рисунок 6).

```
     10.0.0.0/8 is variably subnetted, 5 subnets, 2 masks
O       10.10.10.0/30 [110/2] via 10.10.12.1, 00:08:35,
GigabitEthernet0/0
                      [110/2] via 10.10.11.1, 00:08:35,
GigabitEthernet0/1
C       10.10.11.0/30 is directly connected, GigabitEthernet0/1
L       10.10.11.2/32 is directly connected, GigabitEthernet0/1
C       10.10.12.0/30 is directly connected, GigabitEthernet0/0
L       10.10.12.2/32 is directly connected, GigabitEthernet0/0
O    192.168.1.0/24 [110/2] via 10.10.11.1, 00:08:35,
GigabitEthernet0/1
O    192.168.2.0/24 [110/2] via 10.10.12.1, 00:08:35,
GigabitEthernet0/0
     192.168.3.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.3.0/24 is directly connected, GigabitEthernet0/2
L       192.168.3.1/32 is directly connected, GigabitEthernet0/2
     192.168.100.0/32 is subnetted, 1 subnets
C       192.168.100.3/32 is directly connected, Loopback0
```

Рисунок 6 - Информация из таблицы маршрутизации

Буква «O» обозначает, что данный маршрут прописался с использованием протокола OSPF. На рисунке видно, что с роутера R2 сеть 192.168.1.0/24 доступна через адрес 10.10.11.1, а этот адрес находится на роутере R0. А сеть 192.168.2.0 доступна через адрес 10.10.12.1, а это адрес интерфейса роутера R1. Повторите вывод информации о «соседях» и данных из таблицы маршрутизации для Router0 и Router1. Проверьте доступность PC0 с маршрутизатора Router2:

Router# ping 192.168.1.2

Router#traceroute 192.168.1.2

Занесите снимок экрана в отчет (рисунок 7) и повторите для PC1:

```
Router# 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

Router#tr
Router#traceroute 192.168.1.2
Type escape sequence to abort.
Tracing the route to 192.168.1.2

  1   10.10.11.1      1 msec    0 msec    0 msec
  2   192.168.1.2     0 msec    0 msec    0 msec
```

Рисунок 7 - Проверка с Router2 маршрута до компьютера PC0

Сохраните схему сети для выполнения следующей лабораторной работы.

Контрольные вопросы

1. Опишите принципы работы протокола OSPF.
2. Какой алгоритм для нахождения оптимального пути применяется в протоколе OSPF?
3. Для чего используется алгоритм Дейкстры в протоколе OSPF?
4. Как корректируется таблица маршрутизации при применения протокола OSPF?
5. Опишите последовательность настройки маршрутизаторов в данной лабораторной работе.
6. Опишите последовательность настройки OSPF – протокола.
7. Опишите принципы работы протокола маршрутизации IGP.
8. Что такое метрика маршрутизации? Для чего она используется?
9. Приведите достоинства и недостатки статической маршрутизации.
10. Опишите достоинства и недостатки динамической маршрутизации.

Лабораторная работа №12. Изучение отказоустойчивости протокола динамической маршрутизации OSPF

Цель работы

Проверять отказоустойчивость сети, для которой был настроен протокол OSPF.

Задание

1. Для выполнения работы необходимо открыть схему сети из лабораторной работы №12.

2. Проверить отказоустойчивость сети и сделать необходимые снимки экрана. Изучить полученную информацию и оформить ее в соответствии с требованиями раздела «Содержание отчета».

3. Ответить на контрольные вопросы.

Откроем схему, которую вы построили в предыдущей лабораторной работе (рис.1).

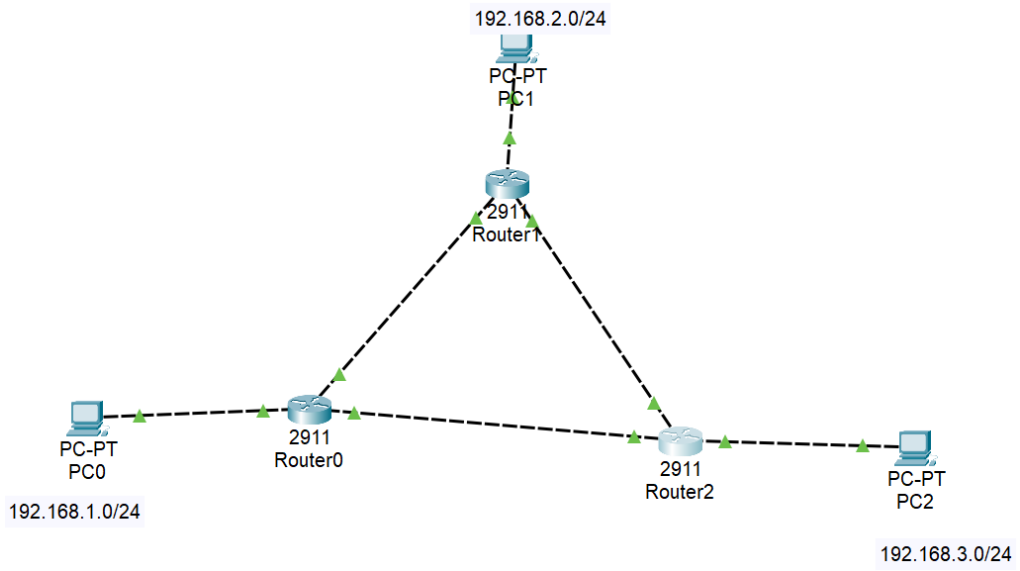


Рисунок 1 - Схема исследуемой сети

Как было показано в предыдущей работе, что с роутера R2 сеть 192.168.1.0/24 доступна через канал, который соединяет роутеры R2 и R0, а сеть 192.168.2.0 доступна через роутер R1. Попробуем вывести из строя канал между роутерами R2 и R0. Для этого нужно выйти в настройки роутера R2 и набрать следующие команды:

Router>enable

Router#configure terminal

Router(config)#interface gigabitEthernet 0/1

Router(config-if)#shutdown

После этого звено между роутерами R2 и R0 вышло из рабочего состояния (рис. 2).

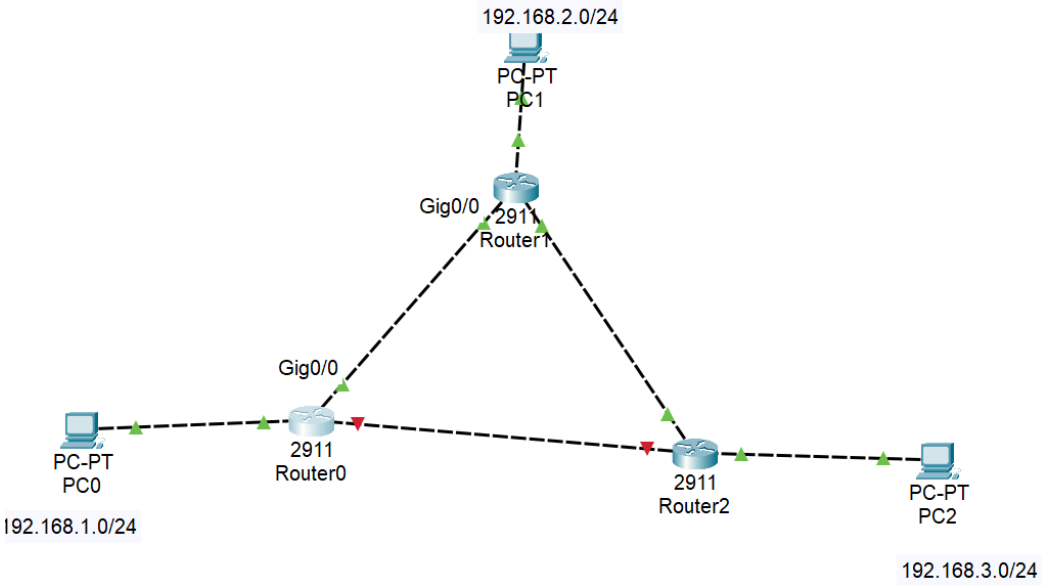


Рисунок 2 - Звено между R2 и R0 находится в нерабочем состоянии

Теперь проверим связь между компьютерами PC2 и PC0, для этого с PC2 пошлем команду ping на PC0. Проверим, установится ли связь и сколько пакетов при этом потеряется. При тестировании необходимо определить 1000 запросов ping.

ping 192.168.1.2 -n 1000

На PC2 определить, сколько было потеряно пакетов (рисунок 3).

```
Reply from 192.168.1.2: bytes=32 time<1ms TTL=125
Reply from 192.168.1.2: bytes=32 time<1ms TTL=125
Reply from 192.168.1.2: bytes=32 time<1ms TTL=125
Reply from 192.168.1.2: bytes=32 time=1ms TTL=125
Reply from 192.168.1.2: bytes=32 time<1ms TTL=125
Reply from 192.168.1.2: bytes=32 time<1ms TTL=125
Reply from 192.168.1.2: bytes=32 time<1ms TTL=125
Reply from 192.168.1.2: bytes=32 time=10ms TTL=125
Reply from 192.168.1.2: bytes=32 time=12ms TTL=125
Reply from 192.168.1.2: bytes=32 time=3ms TTL=125
Reply from 192.168.1.2: bytes=32 time=13ms TTL=125
Reply from 192.168.1.2: bytes=32 time<1ms TTL=125
Reply from 192.168.1.2: bytes=32 time<1ms TTL=125
Reply from 192.168.1.2: bytes=32 time=11ms TTL=125
Reply from 192.168.1.2: bytes=32 time<1ms TTL=125

Ping statistics for 192.168.1.2:
    Packets: Sent = 999, Received = 996, Lost = 3 (1% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 24ms, Average = 3ms

Control-C
```

Рисунок 3 - Отправка ping-пакетов с PC2

Для того, чтобы остановить процесс передачи пакетов необходимо нажать комбинацию клавиш Ctrl+C. В данном случае было потеряно 3 из 999 пакетов. Обычно на реальном оборудовании можно произвести настройки, чтобы пакеты не терялись.

Для получения информации из таблицы маршрутизации на Router2 введите команду:

Router#show ip route

На рисунке 4 видно, что сеть 192.168.1.0 доступна теперь через адрес 10.10.12.1, т.е. через маршрутизатор Router1, так же как и сеть 192.168.2.0 (рисунок 4.).

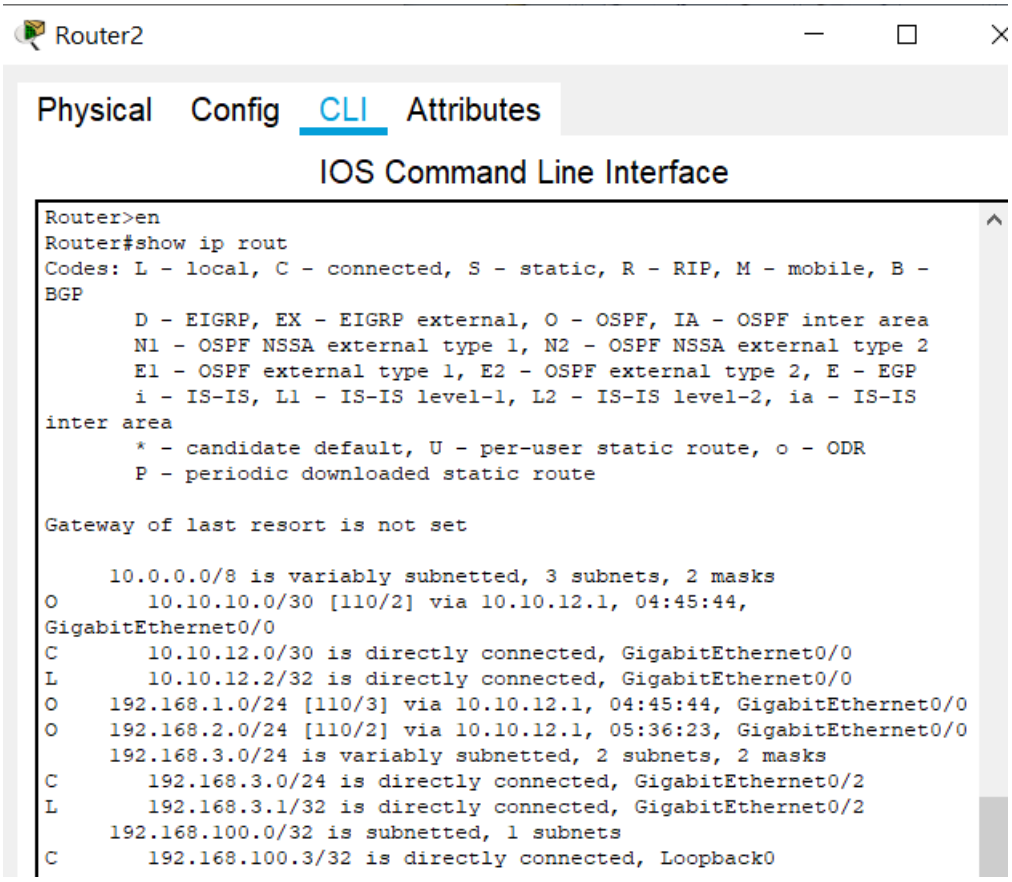


Рисунок 4 - Изменения в таблице маршрутизации

Исследуйте маршрут до 192.168.1.2, убедитесь, что он идет через 10.10.12.1 (рисунок 5). Для этого на PC2 введите команду:

tracert 192.168.1.2

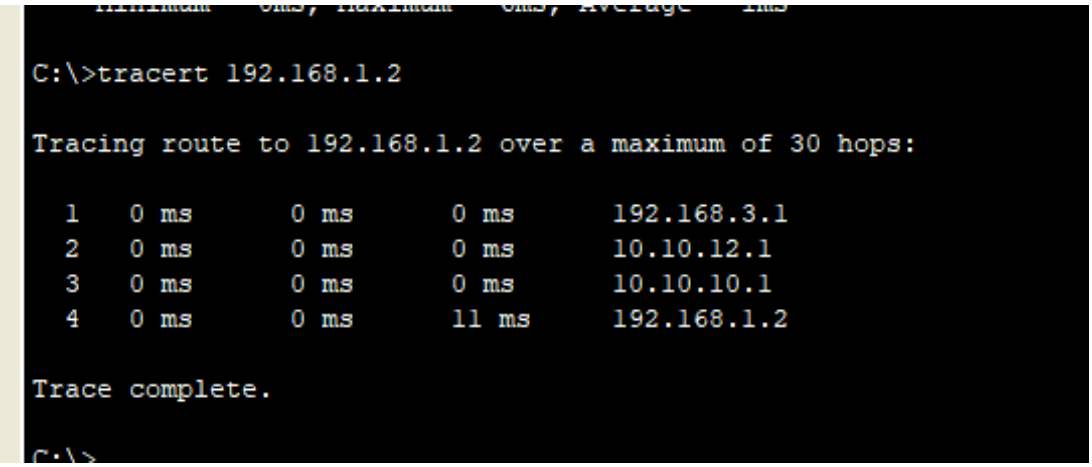


Рисунок 5 - Новый маршрут между PC2 до PC0

Содержание отчета

В индивидуальном отчёте должны быть указаны цель, задание, представлены необходимые снимки экрана и пояснения к ним. Следует проанализировать полученные данные и дать ответы на контрольные вопросы.

Контрольные вопросы

1. Что такое маршрутизация? Зачем она нужна и какие функции выполняет?
2. Какие виды маршрутизации бывают? В чем их различие?
3. Что такое таблица маршрутизации?
4. Опишите цель таблицы маршрутизации?
5. Что такое протокол OSPF? На каком математическом алгоритме он основан? Каковы его основные особенности?
6. Объясните принцип работы протокола маршрутизации OSPF по восстановлению связности сети исходя из полученных результатов.
7. Проведите оценку количества потерянных пакетов и время, потребовавшиеся на восстановление маршрутов исходя из ваших результатов.
8. Какую информацию выводит команда **show ip route**?
9. Как определить, что при настройке OSPF, был обнаружен соседний маршрутизатор?
10. Как изменится маршрут после обрыва связи между соседними маршрутизаторами?

Практическая работа №11. Бесклассовая адресация IPv4

Цель работы

Изучить принципы бесклассовой адресации IPv4

Задание

1.Ознакомиться причинами отказа от классовой маршрутизации;

2. Ознакомиться с принципами разбиения сети на подсети при помощи технологии VLSM;

3.Ответить на вопросы.

С точки зрения эффективности использования адресного пространства классовая модель адресации оказалась нерациональной. Например, если у нас есть диапазон адресов класса B, то в такой сети может быть максимально

65535 устройств. А в существующей сети имеется, например, 2000 компьютеров. Таким образом, оставшиеся 63535 адресов не будут использоваться. В случае классовой адресации сеть можно разбить на подсети одинакового размера.

Постепенно с ростом сети Интернет произошел отказ от классовой схемы адресации, и была принята бесклассовая модель IPv4-адресации, в которой отсутствует привязка к классу сети и маске подсети по умолчанию. Бесклассовая адресация использует маски сети переменной длины (Variable Length Subnet Mask – VLSM) и технологию межклассовой междоменной маршрутизации (Classless Inter Domain Routing - CIDR). Термин «маска переменной длины обозначает, что сеть может быть разбита на подсети с различными масками подсети. IP-адрес записывается при этом следующим образом - IP-адрес/длина префикса. Число после символа «/» означает количество единичных разрядов в маске подсети. Например, сетевой адрес 192.168.1.7 с маской подсети 255.155.255.248 также может быть записан следующим образом 192.168.1.7/29. Число 29 обозначает, что в маске подсети 29 единичных бит.

Допустим, что организации выделена сеть класса С 192.168.1.0/24 (рис.1). Требуется разделить ее на 6 подсетей. В подсетях 1,2,3,4 должно быть 10 узлов, в 5-й подсети – 50, в 6-й подсети -100. Теоретически для сети 192.168.1.0/24 допустимое количество узлов равно 254, а разбить такую сеть на подсети с требуемым количеством узлов без использования технологии VLSM невозможно.

Сначала нужно разделить сеть 192.168.1.0/24 на две подсети. Для этого из четвертого октета необходимо занять 1 бит доя идентификатора подсети, т.е. для идентификации узлов остается 7 бит. В итоге получилось 2 подсети 192.168.1.0/25 и 192.168.1.128/25. В каждой сети может быть 2^7-2=126 узлов. Первую сеть оставим для 6 подсети, а вторую разделим еще на 2 подсети. Для этого возьмем один бит из сети оставшихся, отведенных под идентификатор узла, Таким образом, получается 2 подсети 192.168.1.128/26 и 192.168.1.192/26, в каждой из которых допустимое количество узлов равно 2^6-2=62. Первую подсеть оставляем для пятой подсети, в которой должно быть 50 узлов, а из второй сформируем еще 4 подсети. Для этого займем еще 2 бита из оставшихся 6 бит, отведенных под идентификатор узла. В результате получим 4 подсети с 2^4-2=14 узлами в каждой, что позволит создать требуемое количество узлов, необходимое для подсетей 1,2,3,4.

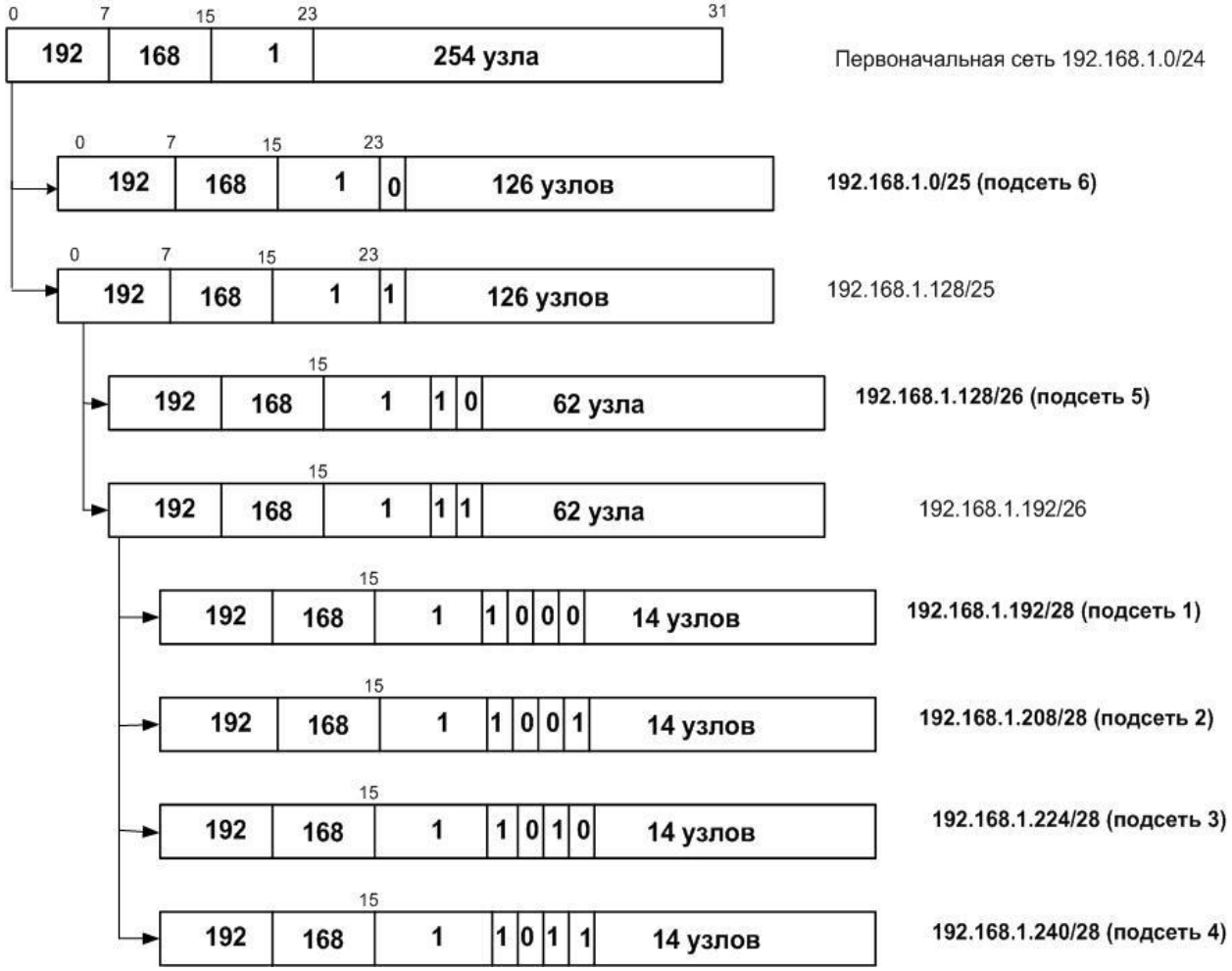


Рисунок 1 - Пример разбиения сети 192.168.1.0/24 на подсети при помощи технологии VLSM

В таблице 1 приведены примеры масок подсети, а также количество узлов и IP-адресов при бесклассовой адресации. Из таблицы видно, что чем длиннее маска сети, тем меньшее количество узлов может находиться в данной сети.

Маска подсети должна сообщать сетевому устройству, занимающемуся обработкой конкретного пакета, какая часть IP-адреса в нем определяет адрес сети, а какая часть – адрес сетевого интерфейса в этой сети. Маршрутизатор выполняет логическое перемножение IP-адреса на маску подсети для того, чтобы получить адрес сети, в которую следует отправить данный пакет.

Таблица 1. Бесклассовая IP-адресация

№№	Маска подсети	Количество узлов	Количество IP-адресов	Обратная маска
1	255.255.255.255 /32	1	1	0.0.0.0
2	255.255.255.254 /31	2	2	0.0.0.1
3	255.255.255.252 /30	2	4	0.0.0.3
4	255.255.255.248 /29	6	8	0.0.0.7
5	255.255.255.240 /28	14	16	0.0.0.15
6	255.255.255.224 /27	30	32	0.0.0.31
7	255.255.255.192 /26	62	64	0.0.0.63
8	255.255.255.128 /25	126	128	0.0.0.127
9	255.255.255.0 /24	254	256	0.0.0.255
10	255.255.254.0 /23	510	512	0.0.1.255
11	255.255.252.0 /22	1022	1024	0.0.3.255
12	255.255.248.0 /21	2046	2048	0.0.7.255
13	255.255.240.0 /20	4094	4096	0.0.15.255
14	255.255.224.0 /19	8190	8192	0.0.31.255
15	255.255.192.0 /18	16 382	16 384	0.0.63.255
16	255.255.128.0 /17	32 766	32 768	0.0.127.255
17	255.255.0.0 /16	65 534	65 536	0.0.255.255
18	255.254.0.0 /15	131 070	131 072	0.1.255.255
19	255.252.0.0 /14	262 142	262 144	0.3.255.255
20	255.248.0.0 /13	524 286	524 288	0.7.255.255
21	255.240.0.0 /12	1 048 574	1 048 576	0.15.255.255
22	255.224.0.0 /11	2 097 150	2 097 152	0.31.255.255
23	255.192.0.0 /10	4 194 302	4 194 304	0.63.255.255
24	255.128.0.0 /9	8 388 606	8 388 608	0.127.255.255
25	255.0.0.0 /8	16 777 214	16 777 216	0.255.255.255
26	254.0.0.0 /7	33 554 430	33 554 432	1.255.255.255
27	252.0.0.0 /6	67 108 862	67 108 864	3.255.255.255
28	248.0.0.0 /5	134 217 726	134 217 728	7.255.255.255
29	240.0.0.0 /4	268 435 454	268 435 456	15.255.255.255
30	224.0.0.0 /3	536 870 910	536 870 912	31.255.255.255
31	192.0.0.0 /2	1 073 741 822	1 073 741 824	63.255.255.255
32	128.0.0.0 /1	2 147 483 646	2 147 483 648	127.255.255.255
33	0.0.0.0 /0	4 294 967 294	4 294 967 296	255.255.255.255

Пусть задан IP-адрес 192.190.15.45. Это сеть класса С с маской 24 бита. Произведем побитовое логическое умножение IP-адреса и маски подсети в двоичной форме:

IP- адрес 11000000 10101000 00001111 10010001

Маска 11111111 11111111 11111111 00000000

Адрес сети 11000000 10101000 00001111 00000000

Адрес хоста 00000000 00000000 00000000 10010001

Широковещательный адрес в конкретной сети образуется из адреса сети, путем заполнения последних нулевых бит единицами. Следовательно широковещательный адрес для сети 192.190.15.45 будет

Широковещ. адрес 11000000 10101000 00001111 11111111 (192.190.15.255).

Контрольные вопросы

1. Может ли пакет с IP-адресом 172.24.10.1 маршрутизироваться в Ip-сети?
2. Можно ли назначить узлу в локальной сети IP-адрес 192.190.1.31/27?
3. Для адреса 10.2.2.1 укажите класс сети, номер сети и номер узла.
4. Для сети 128.63.2.100 укажите класс сети, номер сети и номер узла.
5. Может ли существовать такой IP-адрес 256.241.201.10?
6. Как маршрутизатор узнает адрес сети для отправки пакета?
7. Укажите недостатки классовой маршрутизации.
8. Какие преимущества имеет бесклассовая адресация?
9. Как происходит деление сети на подсети при масках переменной длины?
10. Как записывается адрес? Приведите примеры.

Практическая работа №12. Применение технологии NAT

Цель работы

Изучить принципы бесклассовой адресации IPv4

Задание

1.Ознакомиться с принципами применения технологии NAT на сети;
2. Ознакомиться с глобальными и частными IP- адресами;
3.Ответить на вопросы.

В сети Интернет идентификация устройства осуществляется уникальным адресом IPv4, который не должен повторяться в глобальной сети. Такие адреса называются ***глобальные*** (белыми) IP-адресами. Данные адреса маршрутизируются в сети Интернет, т.е. они доступны из любой точки мира. Не существует двух устройств с одинаковыми IP-адресами, которые были бы подключены к открытой сети. Получают такие адреса у Интернет-провайдеров.

Из-за быстрого роста сети Интернет количество свободных IP-адресов уменьшается. В протоколе IPv4 всего порядка 4,3 млрд. IP-адресов.

Поскольку число публичных адресов ограничено, поэтому в каждом из классов IPv4- сетей определили так называемое ***частные*** (серые) IP-адреса,

которые предназначены для использования в локальных компьютерных сетях и не маршрутизируются в сеть Интернет. Данные адреса могут повторяться.

Для локальных сетей, не подключенных к Интернету, можно использовать любые возможные адреса, уникальные в пределах данной сети. Глобальные адреса находятся в пределах от 10.0.0.1 до 223.255.255.254 за исключением частных IPv4.

Адресное пространство частных IPv4 состоит из трех блоков:

1) 10.0.0.0- 10.255.255.255 (класс A);

2) 172.16.0.0- 172.31.255.255 (класс B);

3) 192.168.0.0- 192.168.255.255 (класс C).

Но при этом встает вопрос: как обеспечить доступ компьютеров с частными IP-адресами в сеть Интернет? Ведь частные адреса не маршрутизируются в сети Интернет. Для решения этой проблемы требуется использовать технологию NAT.

NAT (от англ. Network Address Translation — «преобразование сетевых адресов») — это механизм в сетях TCP/IP, позволяющий преобразовывать IP-адреса транзитных пакетов. (Другими словами, пакет, проходя через маршрутизатор, может поменять свой адрес источника и/или назначения).

NAT выполняет три важных функции.

1. Позволяет экономить IP-адреса (только в случае использования NAT в режиме PAT - Port Address Translation), транслируя несколько внутренних частных IP-адресов в один внешний глобальный IP-адрес (или в несколько, но меньшим количеством, чем внутренних). По такому принципу построено большинство сетей в мире: на небольшой район домашней сети местного провайдера или на офис выделяется 1 глобальный (внешний) IP-адрес, за которым работают и получают доступ интерфейсы с частными (внутренними) IP-адресами.

2. Позволяет предотвратить или ограничить обращение снаружи к внутренним хостам, оставляя возможность обращения изнутри наружу. При инициации соединения изнутри сети создаётся трансляция. Ответные пакеты, поступающие снаружи, соответствуют созданной трансляции и поэтому пропускаются. Если для пакетов, поступающих снаружи, соответствующей трансляции не существует, они не пропускаются.

3. Позволяет скрыть определённые внутренние сервисы внутренних хостов/серверов. По сути, выполняется та же указанная выше трансляция на определённый порт, но возможно подменить внутренний порт официально зарегистрированной службы (например, 80-й порт TCP (HTTP-сервер) на внешний 54055-й). Это необходимо для повышения безопасности и сокрытия «непубличных» ресурсов.

Применение NAT позволяет скрыть адреса узлов своей сети, чтобы не дать возможности злоумышленникам составить представление о структуре и масштабах корпоративной сети, а также о структуре и интенсивности исходящего и входящего трафика.

Традиционная технология NAT подразделяется на технологии *базовой трансляции сетевых адресов* (Basic Network Address Translation, Basic NAT) и *трансляции сетевых адресов и портов* (Network Address Port Translation, NAPT). В технологии Basic NAT для отображения используются только IP-адреса, а в технологии NAPT – еще так называемые транспортные идентификаторы, в качестве которых чаще всего выступают порты TCP и UDP.

Базовая трансляция сетевых адресов

Если количество локальных узлов, которым необходимо обеспечить выход во внешнюю сеть меньше или равно имеющемуся количеству глобальных адресов, то для каждого частного адреса гарантировано однозначное отображение на глобальный адрес. В такой ситуации целью трансляции является не столько решение проблемы недостатка адресов, сколько обеспечение безопасности.

Частные адреса узлов могут отображаться на глобальные адреса статически. Соответствие внутренних адресов внешним адресам задается таблицей, поддерживаемой маршрутизатором или файерволом, на котором установлено программное обеспечение NAT. Файервол - это система, которая предотвращает несанкционированный доступ к сети, он блокирует любой сетевой трафик, который является подозрительным.

Рассмотрим небольшой пример (рис. 1). Пусть узел A сети 1 (адрес 10.0.1.4) посылает пакет в сеть 2 узлу D (адрес 10.0.2.3). В таблице NAT на роутерах R1 и R2 имеется информация, указанная на рисунке 1.

Когда узел A посылает узлу пакет узлу D, то он помещает в заголовок пакета в качестве адреса глобальный адрес узла D - 185.130.15.1 . Пакет направляется к маршрутизатору R1, которому известен маршрут к сети B. Перед отправкой пакета модуль NAT, работающий на данном мапшрутизаторе, используя свою таблицу отображения, заменяет в поле адреса источника частный адрес 10.0.1.4 соответствующим ему глобальным адресом 183.230.25.2.

Когда пакет после путешествия во внешней сети, поступает на R2, на котором также находится NAT, глобальный адрес назначения 185.130.15.1

преобразуется в частный IP-адрес – 10.0.2.1. Пакеты, передаваемые в обратном направлении проходят аналогичную процедуру трансляции адресов.

Таблица NAT- отображения сети A

Частные адреса	Глобальные адреса
10.0.1.4	183.230.25.2
10.0.1.5	183.230.25.3
10.0.1.7	183.230.25.4

Таблица NAT- отображения сети B

Частные адреса	Глобальные адреса
10.0.2.1	185.130.15.1
10.0.2.3	185.130.15.2
10.0.2.9	185.130.15.3

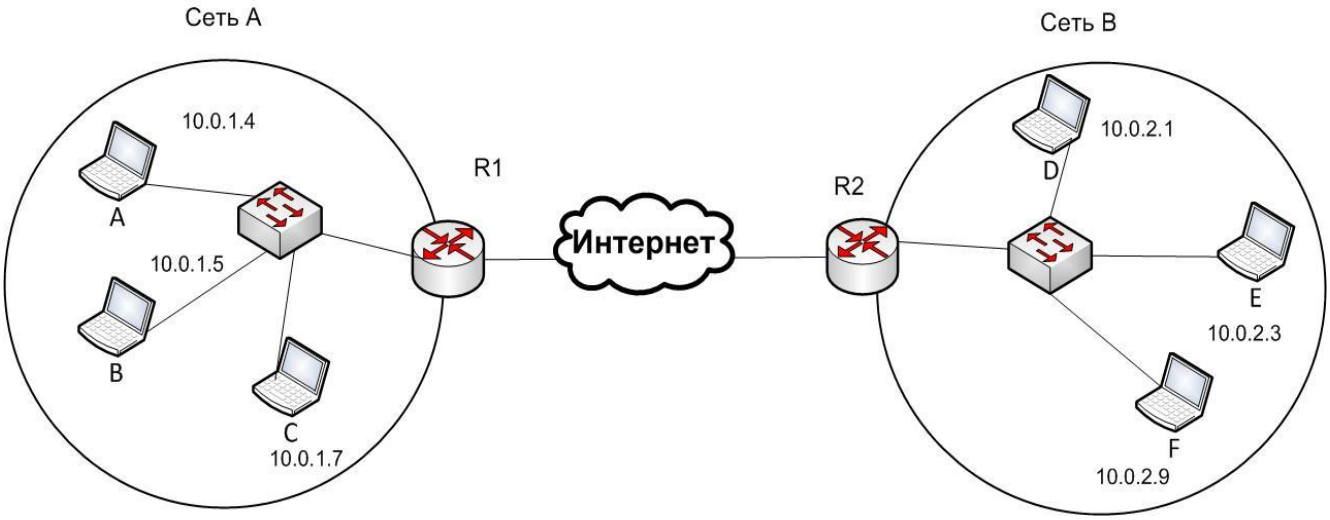


Рисунок 1 - Базовая трансляция сетевых адресов

Трансляция сетевых адресов и портов

Пусть организация имеет локальную IP-сеть, а внешнему интерфейсу пограничного маршрутизатора назначается только один глобальный IP-адрес. Остальным узлам сети назначены частные адреса. Технология NATP позволяет всем узлам сети одновременно взаимодействовать с внешними сетями, используя единственный глобальный IP -адрес. При этом пакеты из внешних сетей должны каким-то образом находить определенный узел-отправитель в локальной сети, поскольку в поле адреса источника помещается один и тот же адрес – внешнего интерфейса маршрутизатора.

Для однозначной идентификации узла – отправителя используется номер порта протоколов UDP или TCP. Но из внутренней сети может исходить несколько запросов с совпадающими номерами портов отправителя. Решение состоит в том, что при прохождении пакета из внутренней во внешнюю сеть, каждой паре портов (внутренний частный адрес, номер порта TCP или UDP

отправителя) ставится в соответствие пара (глобальный адрес внешнего интерфейса, назначенный номер порта TCP или UDP). Назначенный порт выбирается произвольно, но он должен быть уникальным. Соответствие фиксируется в таблице NAT-отображения (рис. 2).

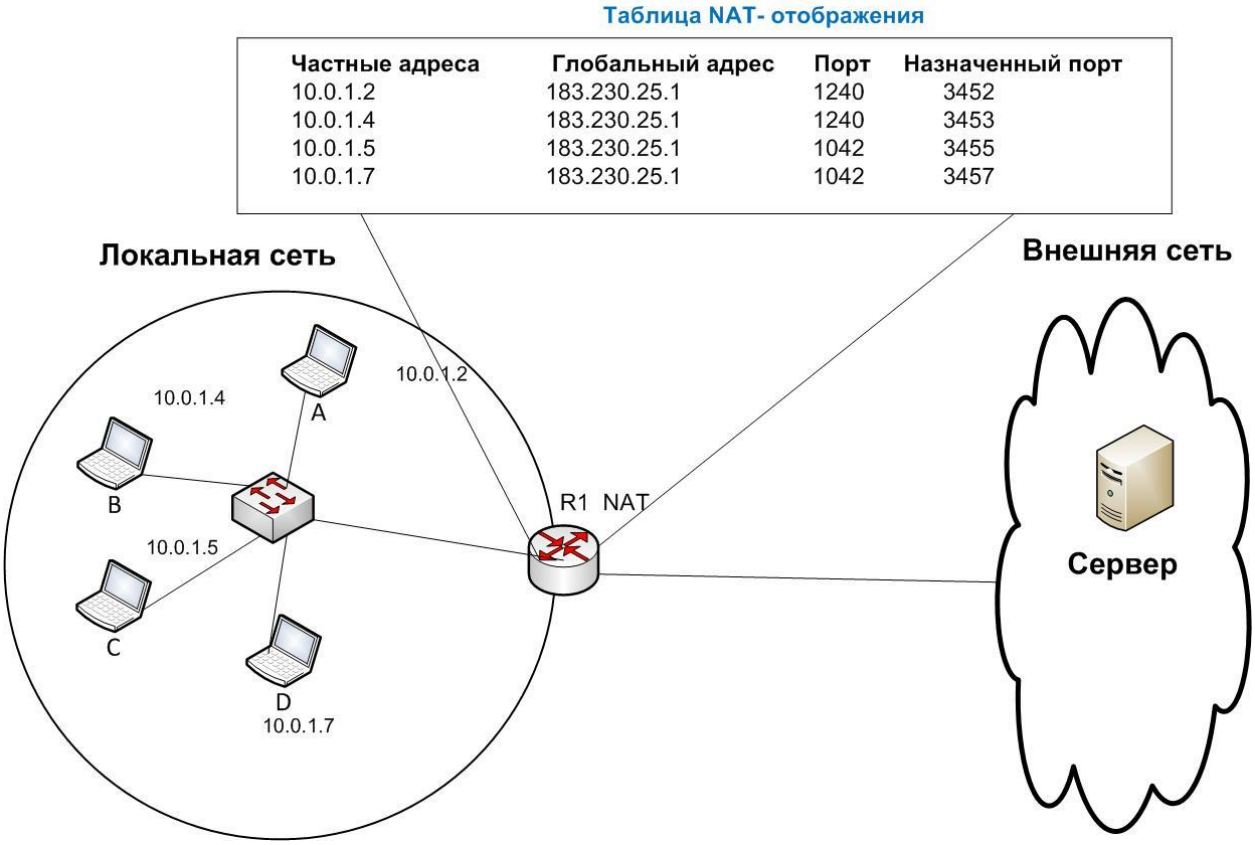


Рисунок 2 - Трансляция сетевых адресов и портов для исходящих сеансов TCP и UDP

На рисунке 2 приведен пример, когда в локальной сети используются частные адреса из блока 10.0.0.0. Внешнему интерфейсу маршрутизатора назначен IP-адрес 183.230.25.1.

Контрольные вопросы

1. Поясните, в чем разница между глобальными и частными адресами.
2. Из каких блоков состоит адресное пространство частных IPv4?
3. Что представляет собой технология NAT?
4. Какие функции выполняет технология NAT?
5. Какие технологии NAT вы знаете?
6. Что подразумевает базовая трансляция сетевых адресов?
7. Опишите назначение файервола.
8. Что подразумевает трансляция сетевых адресов и портов?
9. Что представляет собой таблица NAT – отображения в Basic NAT ?
10. Что представляет собой таблица NAT – отображения в NATP?

Лабораторная работа №13. Изучение технологии NAT

Цель работы

Изучить и практически освоить процесс настройки технологии NAT с использованием стандартных и расширенных списков доступа (access-list) для организации взаимосвязи подразделений компании и обеспечения доступа в Интернет.

Задание

1. Ознакомиться основными функциями технологии NAT.
2. Запустить Cisco Packet Tracer.
3. Собрать необходимую топологию сети, запустить и настроить виртуальное оборудование.
4. Согласно пунктам выполнения лабораторной работы, сделать необходимые снимки экрана. Изучить полученную информацию и оформить ее в соответствии с требованиями раздела Содержание отчета.
5. Ответить на контрольные вопросы.

Порядок выполнения работы

Предварительная настройка сетевого оборудования

Соберите сетевую топологию согласно рисунку 1.

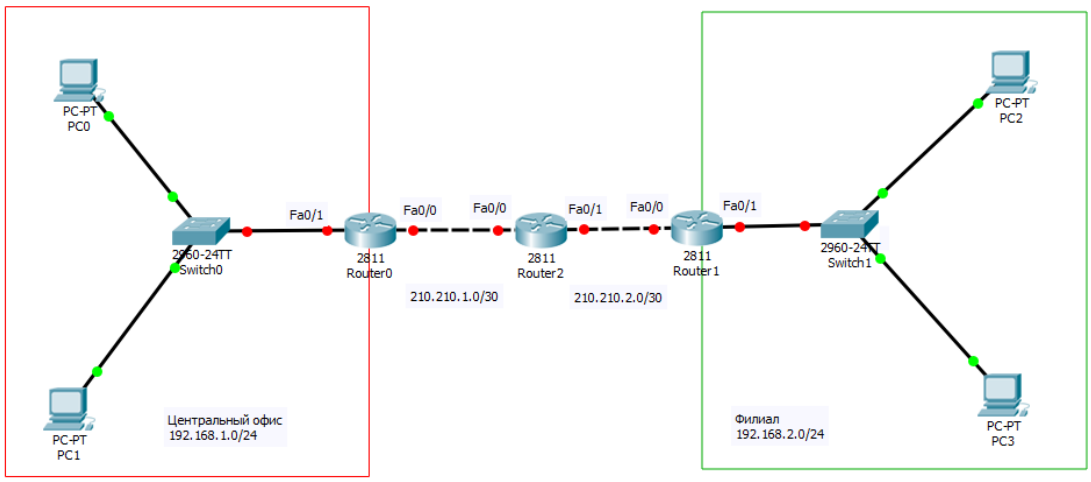


Рисунок 1 - Топология сети

Топология сети состоит из сетевого оборудования центрального офиса: 2 персональных компьютера, коммутатор (Cisco 2960), пограничный маршрутизатор (Cisco 2811), используемый для выхода в Интернет и связи с фили-

алом, В филиале 2 находится 2 персональных компьютера, коммутатор (Cisco 2960) и пограничный маршрутизатор (Cisco 2811), используемый для выхода в Интернет и связи с центральным офисом. Также имеется маршрутизатор (Cisco 2811) Интернет провайдера, который симулирует сеть Интернет. Сетевые адреса всех устройств указаны в таблице 1.

Таблица 1

Сетевые адреса устройств

Сетевой элемент	Интерфейс	IP-адрес	Маска подсети
PC0	FastEthernet 0	192.168.1.2 (шлюз по умолчанию 192.168.1.1)	255.255.255.0 (24 бита)
PC1	FastEthernet 0	192.168.1.3 (шлюз по умолчанию 192.168.1.1)	255.255.255.0 (24 бита)
PC2	FastEthernet 0	192.168.2.2 (шлюз по умолчанию 192.168.2.1)	255.255.255.0 (24 бита)
PC3	FastEthernet 0	192.168.2.3 (шлюз по умолчанию 192.168.2.1)	255.255.255.0 (24 бита)
Router0 (центральный офис)	FastEthernet 0/0	210.210.1.2	255.255.255.252 (30 бит)
	FastEthernet 0/1	192.168.1.1	255.255.255.0 (24 бита)
Router1 (филиал)	FastEthernet 0/0	210.210.2.2	255.255.255.252 (30 бит)
	FastEthernet 0/1	192.168.2.1	255.255.255.0 (24 бита)
Router2 (Интернет провайдер)	FastEthernet 0/0	210.210.1.1	255.255.255.252 (30 бит)
	FastEthernet 0/1	210.210.2.1	255.255.255.252 (30 бит)

Каждому компьютеру присвойте IP-адрес. Для того чтобы назначить сетевые адреса компьютерам, один раз нажмите левой кнопкой мыши на устройстве и перейдите в закладку Desktop, а затем нажмите на IP Configurations. Введите IP-адрес, маску подсети и шлюз по умолчанию в соответствующие поля, как это показано на рисунке 2 для PC0. Повторите для других компьютеров.

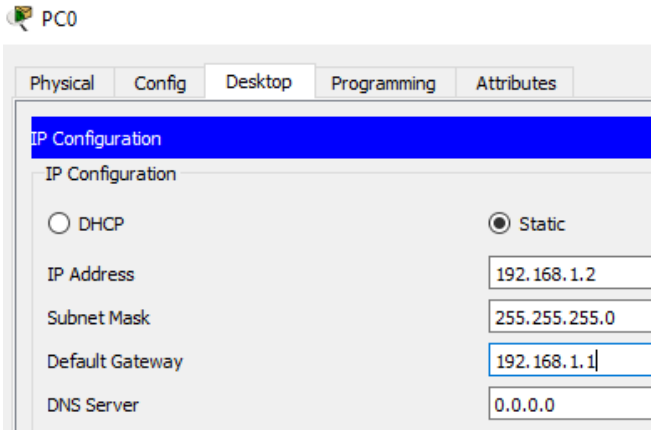


Рисунок 2 - Конфигурация PC0

Необходимо удостовериться в правильности введенных настроек. Для этого один раз нажмите левой кнопкой мыши на устройстве и перейдите в закладку Desktop, а затем нажмите на Command Prompt. Введите команду:

C:\>ipconfig

Сделайте снимок экрана. Повторите для других PC.

Настройте маршрутизатор центрального офиса Router0, для этого один раз нажмите по устройству и перейдите во вкладку CLI, на задаваемый вопрос введите **no**, затем вводите следующие команды (для завершения команды нажмите клавишу **Tab**):

Router>enable
Router#configure terminal
Router(config)#interface fastEthernet 0/0
Router(config-if)#ip address 210.210.1.2 255.255.255.252
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#interface fastEthernet 0/1
Router(config-if)#ip address 192.168.1.1 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#exit

Назначьте маршрут по умолчанию для организации сетевой связности с филиалом и выхода в Интернет:

Router(config)#ip route 0.0.0.0 0.0.0.0 210.210.1.1
Router(config)#end
Router#wr mem
Router#show running-config (после введения команды используйте клавиши «Пробел» или «Enter» для просмотра настроек) найдите в выведенных настройках строчки с назначенными портам адресами и занесите снимок экрана в отчет (рисунок 3).

```
interface FastEthernet0/0
 ip address 210.210.1.2 255.255.255.252
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 192.168.1.1 255.255.255.0
 duplex auto
 speed auto
!
interface Vlan1
 no ip address
 shutdown
!
ip classless
ip route 0.0.0.0 0.0.0.0 210.210.1.1
```

Рисунок 3 - Вывод информации по проведенным настройкам Router0

Повторите настройки для маршрутизатора филиала, взяв необходимую информацию из таблицы 1.

Настройте маршрутизатор Интернет провайдера (используются глобальные IP-адреса):

Router>enable
Router#configure terminal
Router(config)#interface fastEthernet 0/0
Router(config-if)#ip address 210.210.1.1 255.255.255.252
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#interface fastEthernet 0/1
Router(config-if)#ip address 210.210.2.1 255.255.255.252
Router(config-if)#no shutdown
Router(config-if)#end

Настройка NAT

На Router0 и Router1 настройте NAT для доступа в Интернет (внутри корпоративной сети используются частные IP-адреса, которые не маршрутизируются в сети Интернет). Для настройки Router0 введите следующие команды:

Router>enable
Router#configure terminal
Router(config)#interface fastEthernet 0/0
Router(config-if)#ip nat outside
Router(config-if)#exit
Router(config)#interface fastEthernet 0/1
Router(config-if)#ip nat inside
Router(config-if)#exit

Создайте и настройте access-list (определяем трафик, который будем выпускать в Интернет):

Router(config)#ip access-list standard FOR-NAT
Router(config-std-nacl)#permit 192.168.1.0 0.0.0.255 (указываем сети)
Router(config-std-nacl)#exit
Router(config)#ip nat inside source list FOR-NAT interface fastEthernet 0/0 overload
Router(config)#end
Router#wr mem
Router#show running-config найдите в выведенных настройках строчки с созданным и настроенным access-list и занесите снимок экрана в отчет.

Проверьте доступность интерфейсов Router2 с PC0, т.е. возможность выхода в сеть Интернет с ПК центрального офиса. Для этого один раз нажмите левой кнопкой мыши на устройстве (PC0) и перейдите в закладку Desktop, а затем нажмите на Command Prompt (рисунок 4) и введите команду:

C:\>ping 210.210.1.1

Занесите снимок экрана в отчет.

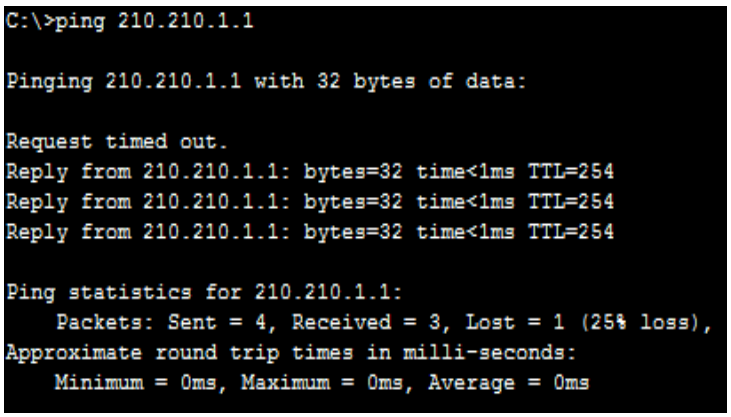


Рисунок 4 - Проверка доступности Интернета из центрального офиса

Маршрутизатор Интернет провайдера доступен, следовательно, NAT настроен верно.

Повторите настройки NAT для маршрутизатора филиала с необходимым изменением IP-адресов, а также проверьте связность PC2 с Router2 (IP-адрес 210.210.2.1) и занесите снимок экрана в отчет.

Содержание отчета

В индивидуальном отчёте должны быть указаны цель, задание, краткое описание лабораторного стенда, представлены необходимые снимки экрана и пояснения к ним. Следует проанализировать полученные данные и дать ответы на контрольные вопросы.

Контрольные вопросы

1. Опишите порядок выполнения лабораторной работы
2. Как производится настройка маршрутизатора центрального офиса?
3. Как производится настройка маршрутизатора провайдера?
4. Как производится настройка NAT для роутеров?
5. Что обозначает команда **Router>enable** при настройке маршрутизатора**?**
6. Что обозначает команда **Router(config)#ip route** при настройке маршрутизатора**?**
7. Как вы определили в процессе выполнения данной лабораторной работы, что NAT настроен правильно?
8. Как вывести информацию по проведенным настройкам Router0?
9. Приведите примеры частных IP- адресов?
10. Опишите преимущества технологии NAT.

Итоговый тест

1. Какое сообщение отправляется первым при загрузке DHCP-клиента?
а) DHCPREQUEST.
б) DHCPBOOT.
в) DHCPDISCOVER +
г) Ни одно из перечисленных.

2. Из каких двух частей состоит IP-адрес?
а) Из адреса сети и адреса узла +
б) Из адреса сети и MAC-адреса.
в) Из адреса узла и MAC-адреса.
г) Из MAC-адреса и маски подсети.

3. Какой Internet-протокол используется для установления соответствия между известным IP-адресом и неизвестным MAC-адресом?
а) UDP.
б) ICMP.
в) ARP+
г) RARP.

4.Какой из перечисленных ниже протоколов относится к транспортному уровню?
а) UCP.
б) UDP +
в) TDP.
г) TDC.

5.Что из указанного ниже используется коммутатором для принятия решения о пересылке фрейма?
а) IP-адрес.
б) MAC-адрес +
в) Сетевой адрес.
г) Адрес узла.

6.Какая часть IP_адреса класса B 154.19.2.7 является номером сети?
а) 154.
б) 154.19. +
в) 154.19.2.
г) 154.19.2.7.

7. Какая часть адреса 129.219.51.18 описывает сеть?
а) 129.219. +

б) 129.
в) 14.1.
г) 1.

8. Какой из перечисленных ниже адресов является широковещательным в сети 123.10.0.0 с сетевой маской 255.255.0.0?

а) 123.255.255.255.
б) 123.10.255.255. +
в) 123.13.0.0.
г) 123.1.1.1.

9. Сколько адресов узлов может быть использовано в сети класса С?
а) 253.
б) 254. +
в) 255.
г) 256.

10. Выполнив логическую операцию, которую совершает маршрутизатор над IP-адресом 121.8.2.5 и маской 255.0.0.0, вычислите адрес сети/подсети.

а) 121.8.1.0.
б) 121.8.0.0.
в) 121.8.2.0.
г) 121.0.0.0 +

11. Сколько битов было заимствовано для создания подсетей в адресе класса С 197.15.22.31 с маской 255.255.255.224?
а) 1.
б) 2.
в) 3. +
г) Ни один из перечисленных выше ответов не является правильным.

12. Выполнив логическую операцию, которую совершает маршрутизатор над IP-адресом 172.16.2.10 и маской 255.255.255.0, вычислите адрес подсети.
а) 172.0.0.0.
б) 172.16.0.0.
в) 172.16.2.0. +
г) Ни один из перечисленных выше ответов не является правильным.

13.Какие две части адреса сетевого уровня используют маршрутизаторы для передачи данных через сеть?

а) Адрес сети и адрес узла. +
б) Адрес сети и MAC_адрес.
в) Адрес узла и MAC_адрес.
г) MAC_адрес и маску подсети.

14.Задан IP-адрес 172.16.2.160, маска 255.255.255.192. Укажите широковещательный адрес сети:

а) 172.16.2.191+
б) 172.16.2.255
в) 172.16.2.0
г) 172.16.2.160.

15.Для предыдущего примера укажите номер подсети

а) 172.16.2.128+
б) 172.16.2.0
в) 172.16.2.190
г) 172.16.2.160.

16. Укажите широковещательный MAC-адрес (Broadcast) в шестнадцатеричной форме:
а) AB:FF:FF:FF:FF:CD
б) AC:89:FF:13:EF:CD
в**)** FF:FF:FF:FF:FF:FF +
г) AB:EE:FF:09:FF:67

17. Какой протокол входит в стек протоколов TCP/IP и реализует процесс нахождения MAC-адреса устройства по известному сетевому IP-адресу.
а) ARP +
б) RARP
в) UDP
г) OSPF

18. Заголовок пакета протокола IPv4 имеет длину
а) 20 байт +
б) 40 байт
в) 10 байт
г) 24 байта

19. Какой транспортный протокол осуществляет обмен дейтаграммами без подтверждения и гарантированной доставки?
а) UDP +
б) TCP.
в) IRQ.
г) LLC.

20. Какой из протоколов используется на транспортном уровне?
а) UCP.
б) TCP +
в) TDP.
г) TDC.

21. Какое наибольшее десятичное число может быть записано в 1 байте?
а) 254.
б) 256.
в) 255 +
г) 257.

22. Какое двоичное число соответствует десятичному числу 151?
а) 10100111.
б) 10010111 +
в) 10101011.
г) 10010011.

23.Какое десятичное число соответствует двоичному числу 11011010?
а) 186.
б) 202.
в) 218 +
г) 222.

24. Сколько уровней имеет эталонная модель OSI?

а) Четыре.
б) Пять.
в) Шесть.
г) Семь+

25. Какой порядок уровней является правильным?
а) 1 - физический, 2 - канальный, 3 - транспортный, 4 - сетевой, 5 - уровень представления данных, 6 - сеансовый, 7 - уровень приложений.
б) 1 - физический, 2 - канальный, 3 - сетевой, 4 - транспортный, 5 - сеансовый, 6 - уровень представления данных, 7 - уровень приложений +
в) 1- физический, 2 - канальный, 3 - сетевой, 4 - сеансовый, 5 - транспортный, 6 - уровень представления данных, 7 -уровень приложений.

г) 1- физический, 2 - сетевой, 3 - сеансовый, 4 - канальный, 5 - транспортный, 6 - уровень приложений, 7 - уровень представления данных.

26. Какой уровень в модели протоколов TCP/IP отвечает за логическую адресацию узлов сети Интернет?

а) Уровень приложений.
б) Транспортный уровень.
в) Уровень Internet.+
г) Уровень доступа к сети.

27. Что представляют первые шесть шестнадцатеричных цифр MAC-адреса?

а) Серийный номер интерфейса.
б) Уникальный идентификатор организации +
в) Уникальный идентификатор интерфейса.
г) Ничто из вышеперечисленного.

28. Какую длину в битах имеет MAC- адрес?

а) 12.
б) 24.
в) 48 +
г) 64.

29. Как должно выглядеть приглашение командной строки при настройке интерфейса?

а) **router(config)#**.
б) **router(config_in)#**.
в) **router(config_intf)#**.
г) **router(config_if)#**. +

30. Какие два режима доступа к командам операционной системы маршрутизатора Cisco существуют?

а) Пользовательский и привилегированный +
б) Пользовательский и гостевой.
в) Привилегированный и гостевой.
г) Гостевой и анонимный.

31. В каком режиме необходимо производить изменение конфигурации маршрутизатора Cisco?

а) Пользовательском.
б) Привилегированном +
в) Режиме администратора.
г) Root.

32. Каким образом сетевой уровень направляет пакеты от отправителя получателю?

а) Путем анализа таблицы IP-маршрутизации +
б) Посредством использования ответов протокола ARP.
в) Путем ссылки на имя сервера.
г) Путем ссылки на мост.

33. Какое из выражений наилучшим образом описывает одну из функций третьего (сетевого) уровня эталонной модели OSI?

а) Этот уровень отвечает за надежность связи между узлами сети.
б) Этот уровень отвечает за физическую адресацию и анализ сетевой топологии.
в) Этот уровень определяет наилучший маршрут для передачи данных по сети +
г) Этот уровень управляет обменом данными между уровнями представления двух систем.

34. Укажите номер сети для IP-адреса 130.113.64.16.

а) 130.113.0.0 +
б) 130.113.64.0
в) 130.0.0.0
г) ни один из вышеперечисленных

35. Укажите номер узла IP-адреса 130.113.64.16.

а) 0.113.64.16
б) 130.0.0.0
в) 0.0.64.16 +
г) 130.113.64.0

36. Задана таблица MAC-адресов коммутатора. Какое действие выполнит коммутатор, если к нему поступит кадр с адресом 0260.8c01.7777?

Номер порта	MAC – адрес
E0	0260.8c01.1111
E1	0260.8c01.2222
E2	0260.8c01.3333
E3	0260.8c01.4444

а) Коммутатор пошлет шировещательный кадр по порту E0;
б) Коммутатор пошлет шировещательный кадр по порту E1 ;
в) Коммутатор пошлет шировещательный кадр по порту E2 ;
г) Коммутатор пошлет шировещательный кадр по порту E3;
д) Коммутатор отфильтрует этот кадр +


technology
information
communication
computer
internet
digital
computingmedia
network
development
hardware
electricity
database
knowledge
system
infrastructure
data
equipment
display
design
relationship
teamwork
desktop
laptop
presentation
electronic
business
interactive
connection
screen
function
storage
analysis
innovation
global
group
future
email
connectivity
computation
pattern
integration
search
mobile
link
social
share
host
statistic
ethernet
wireless
graphic
science
modern
motherboard
world