ДОНСКОЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ

УПРАВЛЕНИЕ ДИСТАНЦИОННОГО ОБУЧЕНИЯ И ПОВЫШЕНИЯ КВАЛИФИКАЦИИ

Кафедра «Вычислительные системы и информационная безопасность»

СБОРНИК УПРАЖНЕНИЙ

к проведению лабораторных работ
по дисциплине

«Сети и системы передачи данных»

Автор
Галушка В.В.

Ростов-на-Дону, 2014

Аннотация

Методические указания предназначены для студентов направления 090900 очной формы обучения.

Автор

к.т.н., доцент
Галушка В.В.

Оглавление

ЛАБОРАТОРНАЯ РАБОТА № 1
КАБЕЛЬНЫЕ ЛИНИИ СВЯЗИ

Цель: Изучить распространённые на практике средства передачи данных в информационных сетях, их основные характеристики и методы работы с ними.

Теоретические сведения

Основу современных вычислительных сетей составляют кабельные линии связи. Кабель состоит из проводников, заключенных в несколько слоев изоляции: электрической, электромагнитной, механической и, возможно, климатической. Кроме того, кабель может быть оснащен разъемами, позволяющими быстро выполнять присоединение к нему различного оборудования. В компьютерных (и телекоммуникационных) сетях применяются три основных типа кабеля:

— коаксиальные кабели с медной жилой;

— кабели на основе скрученных пар медных проводов — неэкранированная и экранированная витая пара;

— волоконно-оптические кабели.

Коаксиальный кабель

Коаксиальный (от лат. co — совместно и axis — ось, то есть «соосный») кабель состоит из несимметричных пар проводников. Каждая пара представляет собой внутреннюю медную жилу и соосную с ней внешнюю жилу, которая может быть полой медной трубой или оплеткой, отделенной от внутренней жилы диэлектрической изоляцией (рис. 1). Внешняя жила играет двоякую роль — по ней передаются информационные сигналы и она является экраном, защищающим внутреннюю жилу от внешних электромагнитных полей.

Рисунок 1 — Коаксиальный кабель.

Существует несколько типов коаксиального кабеля, отли-

чающихся характеристиками и областями применения:

— «Тонкий» коаксиальный кабель. Используется в сетях стандартов 10BASE-2, обеспечивающих скорости передачи данных до 10 Мбит/с на расстоянии до 200 м.

— «Толстый» коаксиальный кабель. Используется в сетях стандартов 10BASE-5, обеспечивающих скорости передачи данных до 10 Мбит/с на расстоянии до 500 м.

— Телевизионный кабель. В компьютерных сетях применяется для подключения антенн беспроводных сетей (Wi-Fi, 3G, LTE-антенн).

Витая пара

Наиболее популярными типами сетевых кабелей, использующихся в локальных сетях, являются кабели неэкранированной витой пары (Unshielded Twisted Pair — UTP), представляющие собой свитые попарно четыре пары проводов (рис. 2). Свивка выполняется для компенсации электромагнитных полей, возникающих при прохождении тока по проводнику и наводящих паразитные электрические напряжения в соседних проводниках, оказавшихся в этом поле.

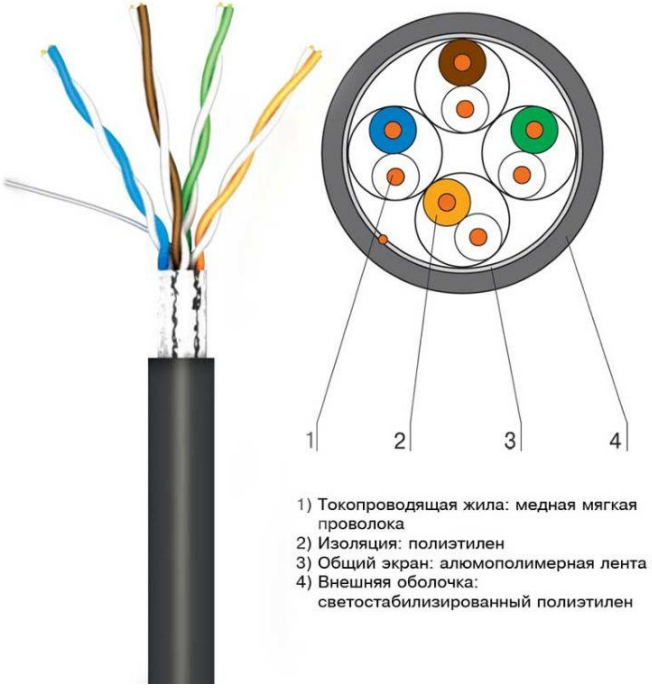


Рисунок 2 — Витая пара.

Кабель на основе неэкранированной витой пары, используемый для проводки внутри здания, разделяется в международных стандартах на 7 категорий. Наибольшее распространение имеют кабели 5-ой категории, которые были специально разработаны для поддержки высокоскоростных протоколов связи. На сегодняшний день наиболее распространены стандарты 100BASE-T и 1000BASE-T со скоростями 100 Мбит/с и 1 Гбитс/с соответственно. Кабели 6 и 7 категории отличаются наличием дополнительной экранировки, причём в категории 7 обязательно экранируются, как каждая пара, так и весь кабель в целом. Основное назначение этих кабелей — поддержка высокоскоростных протоколов на отрезках кабеля большей длины, чем кабель UTP категории 5.

Все кабели UTP независимо от их категории выпускаются в 4-парном исполнении. Каждая из четырех пар кабеля имеет определенный цвет и шаг скрутки.

Все типы кабелей предусматривают наличие специальных коннекторов и методов их соединения с кабелем. Для витой пары используются коннекторы RJ-45 (8P8C). Популярность и повсеместное применение витой пары обусловлено во многом наличием простого способа крепления коннекторов и отсутсвием необходимости применения дорогостоящего оборудования для её монтажа (рис. 3).

Рисунок 3 — Коннектор 8P8C.

Волоконно-оптический кабель

Волоконно-оптический кабель состоит из тонких гибких стеклянных волокон (волоконных световодов), по которым распространяются световые сигналы. Это наиболее качественный тип кабеля — он обеспечивает передачу данных с очень высокой скоростью и к тому же лучше других типов передающей среды обеспечивает защиту данных от внешних помех (в силу особен-

ностей распространения света такие сигналы легко экранировать). Данный вид кабелей используется в сетях стандартов 100BASE-FX, 100BASE-SX, 1000BASE-LX, 10GBASE-LX4, 10GBASE-LR и некоторых других, обеспечивая скорости передачи от 100 Мбит/с до 10 Гбит/с на расстояния от нескольких сотен метров до 40 км.

Каждый световод состоит из центрального проводника света (сердцевины) — стеклянного волокна, и стеклянной оболочки, обладающей меньшим показателем преломления, чем сердцевина (рис. 4). Распространяясь по сердцевине, лучи света не выходят за ее пределы, отражаясь от покрывающего слоя оболочки. В зависимости от распределения показателя преломления и величины диаметра сердечника различают:

—многомодовое волокно со ступенчатым изменением показателя преломления;

—многомодовое волокно с плавным изменением показателя преломления;

—одномодовое волокно.

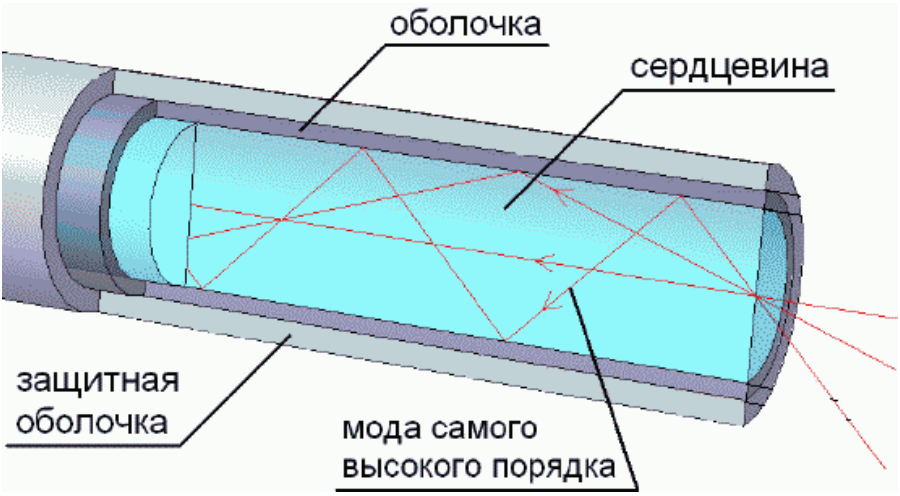


Рисунок 4 — Волоконно-оптический кабель.

Задание

1. Изучите коаксиальный кабель.
2. Изучите волоконно-оптический кабель.
3. Изучите кабель типа неэкранированная витая пара.
4. Выполните монтаж коннекторов с двух сторон ка-

беля витой пары.

Последовательность действий при обжиме витой пары:

1. Очистить кабель от внешней изоляции

2. Разделить пары и проводники

3. Расположить проводники в соответствии со схемой обжима

4. Вставить их в коннектор

5. Вставить коннектор в соответствующее гнездо обжимных клещей

6. Усилием руки зажать проводники в коннекторе

7. С использованием тестера проверить правильность обжима

Контрольные вопросы

1. Какое количество проводников используется в коаксиальном, оптоволоконном кабеле и витой паре?

2. В сетях каких стандартов используется коаксиальный кабель? Какова скорость передачи данных в соответствии с данными стандартами?

3. В сетях каких стандартов используется оптоволоконный кабель? Какова скорость передачи данных в соответствии с данными стандартами?

4. В сетях каких стандартов используется витая пара? Какова скорость передачи данных в соответствии с данными стандартами?

5. Какова схема соединения проводников на разных концах витой пары при прямом обжиме?

6. Для соединения каких типов устройств используется витая пара с прямым обжимом?

7. Какова схема соединения проводников на разных концах витой пары при перекрёстном обжиме?

8. Для соединения каких типов устройств используется витая пара с перекрёстным обжимом?

ЛАБОРАТОРНАЯ РАБОТА № 2
CISCO PACKET TRACER

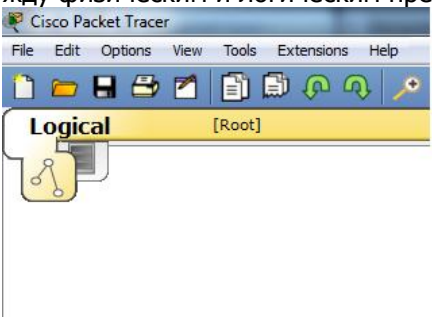
Цель: Изучить программное средство для моделирования сетей — Cisco Packet Tracer, получить базовые навыки проектирование структуры локальной сети.

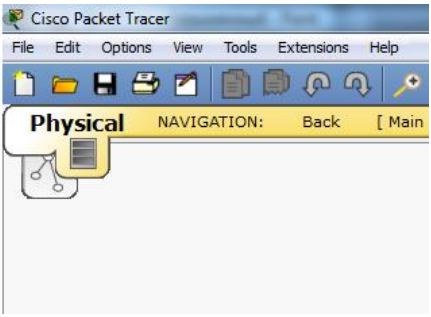
Задание

1. Ознакомление с интерфейсом Cisco Packet Tracer

Packet Tracer — эмулятор сети передачи данных, выпускаемый фирмой Cisco Systems — одним из крупнейших производителей сетевого оборудования.

Интерфейс Cisco Packer Tracer может быть переключён между физическим и логическим представлениями сети.





В нижней части экрана имеется возможность переключения режимов работы сети:

— Realtime — режим реального времени. В данном режиме моделируется обычный работы сети, аналогичный по временным характеристикам работе реального оборудования.

— Simulation — режим симуляции позволяет вручную управлять наступлением очередного события, связанного с передачей данных по сети.

В нижней части экрана имеется меню, в котором представлено оборудование, эмуляция которого возможна в Packet Tracer.

—Routers — маршрутизаторы;

—Switches — свитчи (сетевые коммутаторы);

—Hubs — хабы (концентраторы);

—Wireless Devices — беспроводные устройства;

—Connections — линии связи;

—End Devices — конечные устройства (компьютеры, ноутбуки, телефоны, планшетные ПК);

—Wan Emulation — средства эмуляции глобальных сетей;

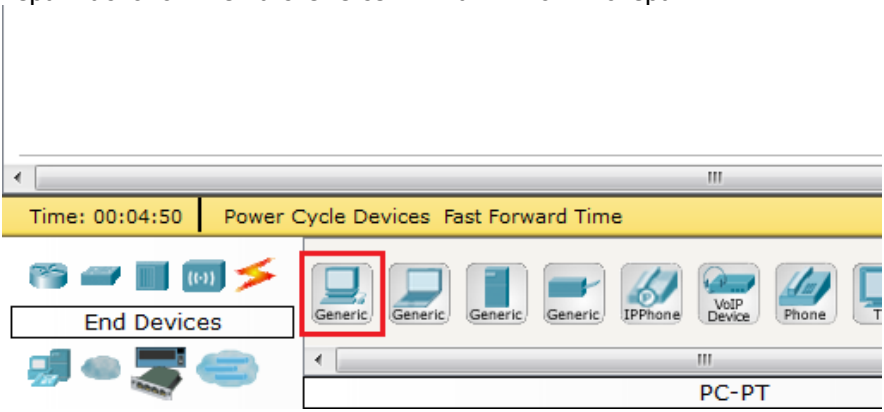
—Custom Made Devices — устройства, созданные пользователем;

—Multiuser Connections — средства эмуляции многопользовательских соединений.

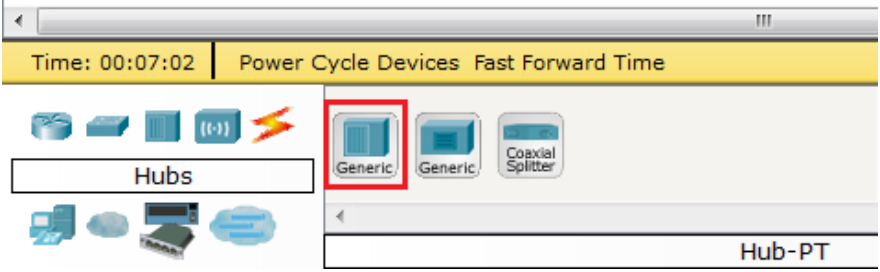
2. Построение простейшей сети

Необходимо построить сеть, объединяющую 4 компьютера.

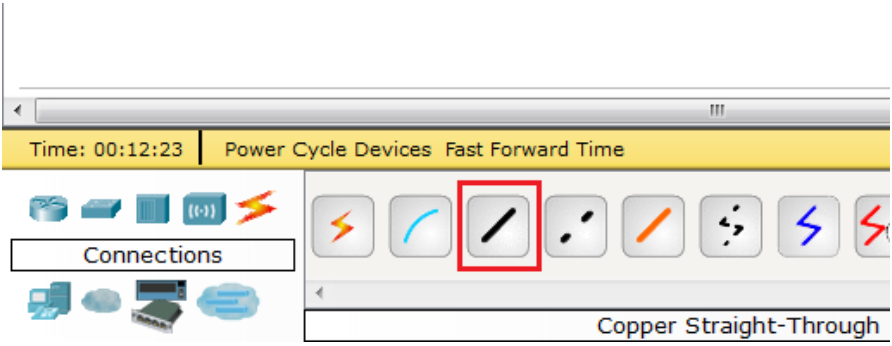
В меню выбора устройств нажмите "End Devices" и в появившемся списке оконечных устройств выберите значок компьютера. Расположите на схеме сети 4 таким компьютера.



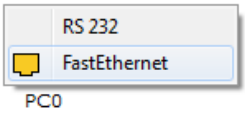
Далее в списке "Hubs" выберите первое из доступных устройств — хаб и расположите его на схеме.



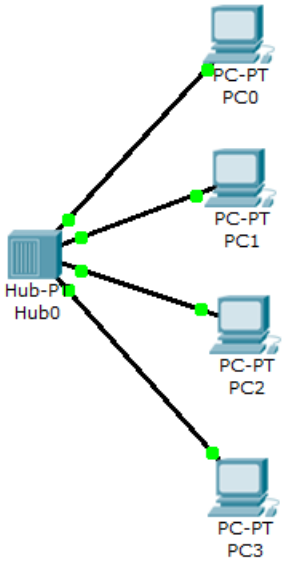
Теперь необходимо соединить все компьютеры с хабом. Для этого нажмите на пункт "Connections" в списке доступных устройств и выберите "Copper Straight-Through", что соответствует медному кабелю витой пары.



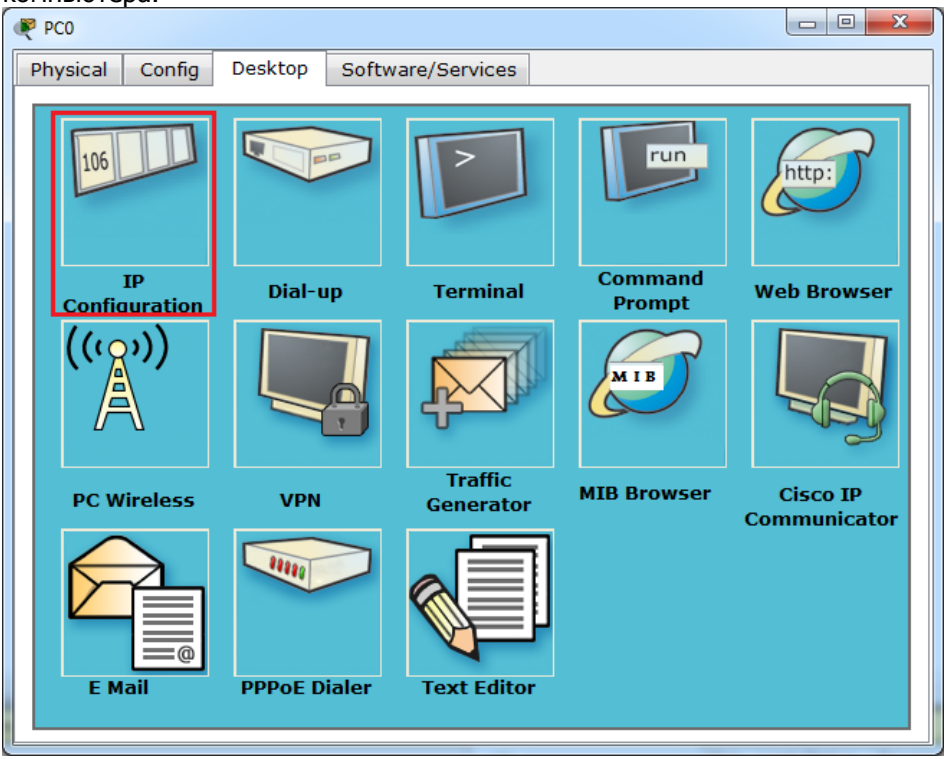
Нажмите на компьютере и в появившемся меню выберите соответствующий порт к которому необходимо подключить кабель — FastEthernet. Затем нажмите на хаб и аналогичным образом выберите один из его портов.



В результате необходимо получить сеть, представленную на рисунке ниже.



После физического соединения компьютеров необходимо присвоить каждому из них IP-адрес. Для этого нажмите один раз на компьютер — в результате откроется окно свойств для данного компьютера.



Выберите "IP Configuration" и введите IP-адресс и маску сети в соответствии с вариантом задания.

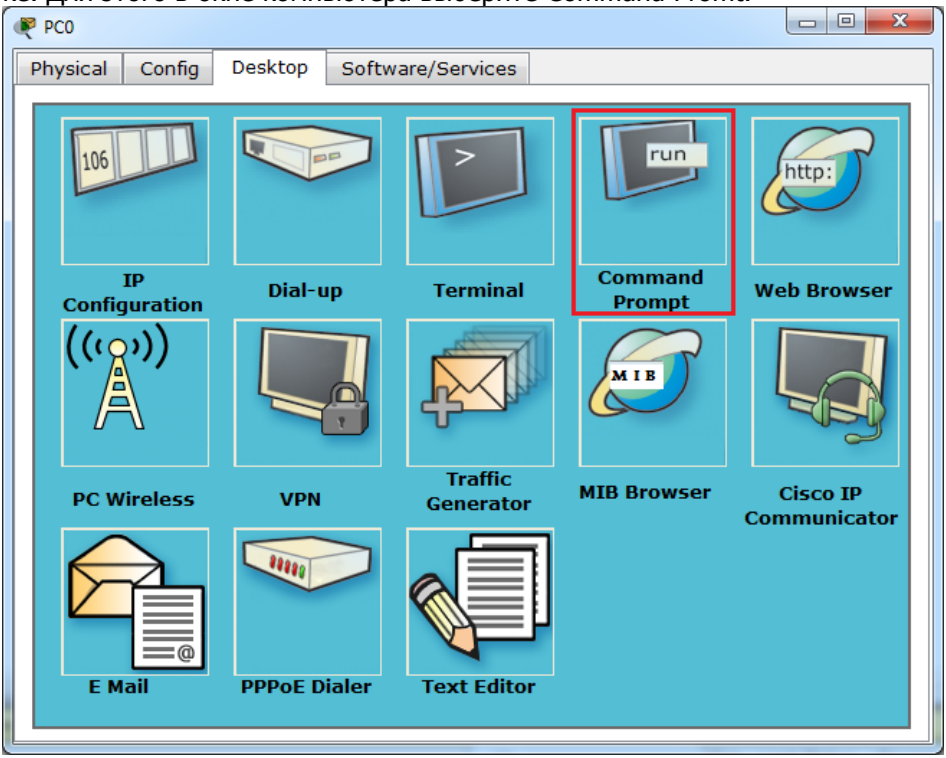
Вариант	Сеть
1,2	200.200.200.152/29
3,4	200.200.200.208/28
5,6	200.200.200.128/27
7,8	200.200.200.192/26
9,10	200.200.200.128/25
11,12	150.100.96.0/23
13,14	150.100.136.0/22
15,16	150.100.160.0/21
17,18	150.100.192.0/20
19,20	150.100.128.0/19
21,22	150.100.64.0/18

Для проверки связи между компьютерами используйте команду

ping адрес

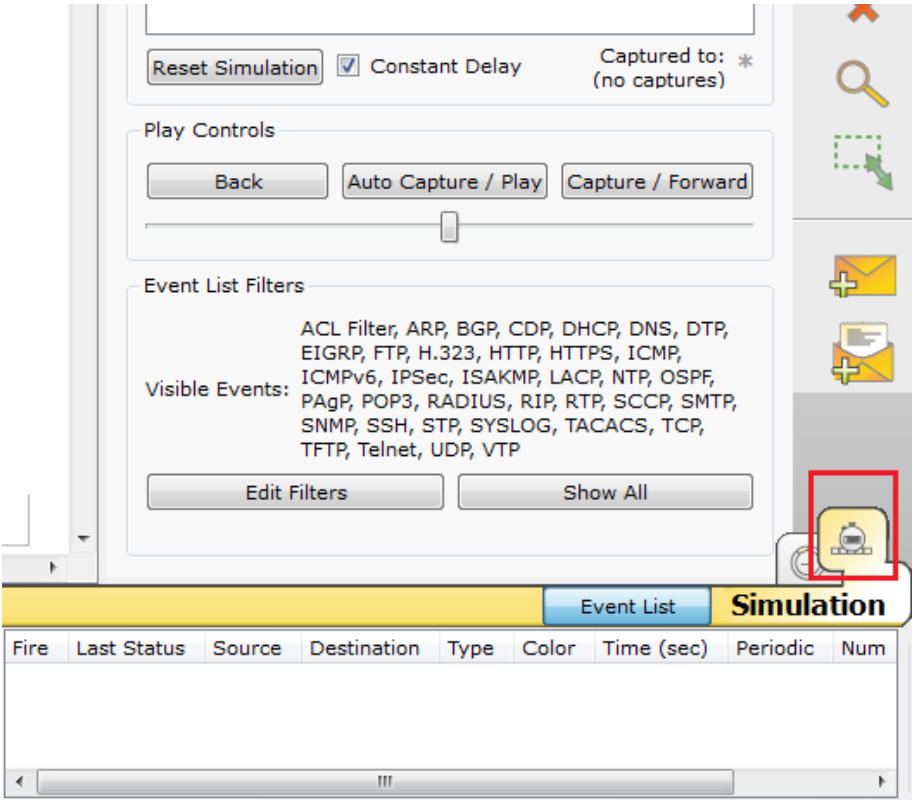
где адрес — IP адрес одного из компьютеров в сети.

Выполнять данную команду необходимо в командной строке. Для этого в окне компьютера выберите Command Promt.



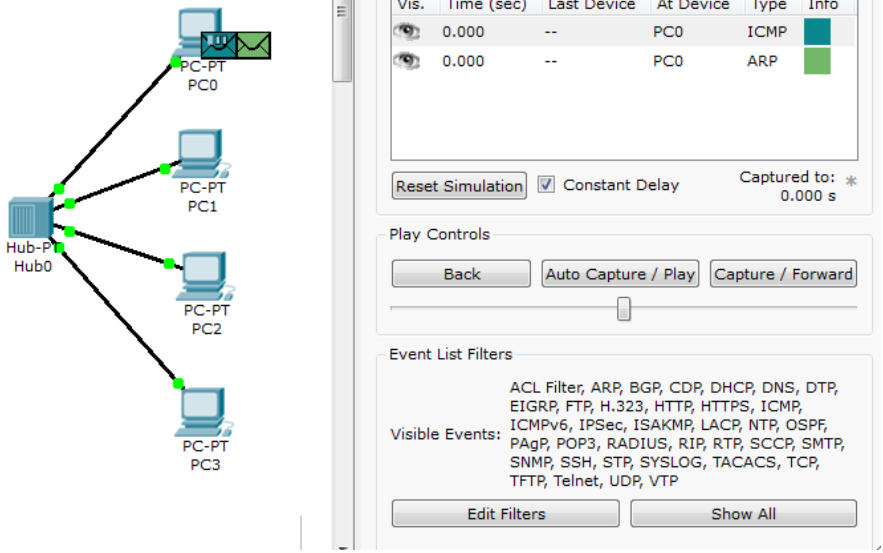
3. Изучение работы концентратора 1-го уровня (хаба)

Для просмотра пакетов, передаваемых по сети, перейдите в режим симуляции (Simulation).

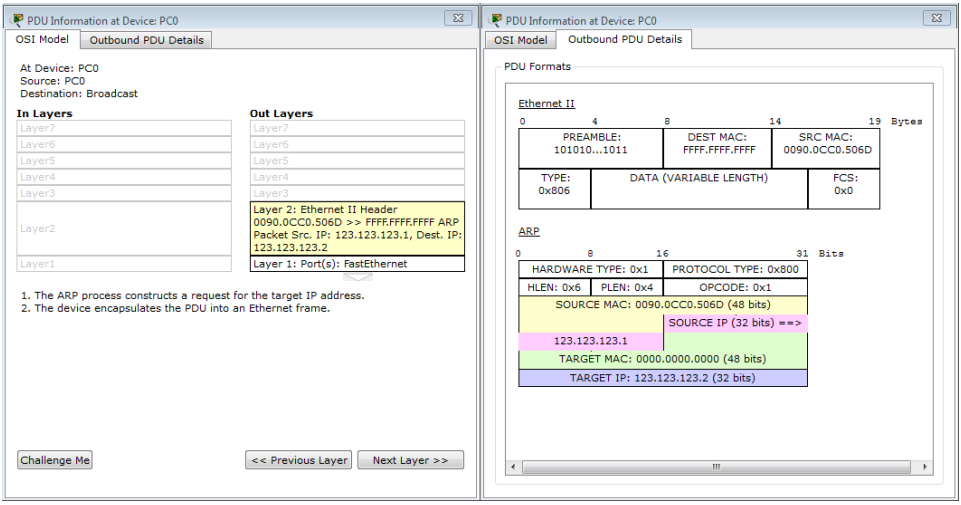


Выполните команду ping на компьютере, на котором не выполняли её ранее. При этом на схеме сети возле данного компьютера должны появиться значки 2 пакетов — ARP-пакета и ICMP-пакета.

Команда ping использует протокол ICMP (Internet Control Message Protocol — протокол межсетевых управляющих сообщений), выполняющий сервисные функции, в том числе проверку доступности узла сети. Узел при этом задаётся своим IP-адресом, однако для доставки ему Ethernet-кадра необходимо знать MAC-адрес. Для получения MAC-адреса узла по его IP-адресу используется протокол ARP (Address Resolution Protocol — протокол определения адреса).



Если нажать на изображение пакета или на поле Info в окне “Event List”, откроется окно с подробной информацией о пакете.



Нажмите кнопку “Capture / Forward” и понаблюдайте за передачей пакетов по сети.

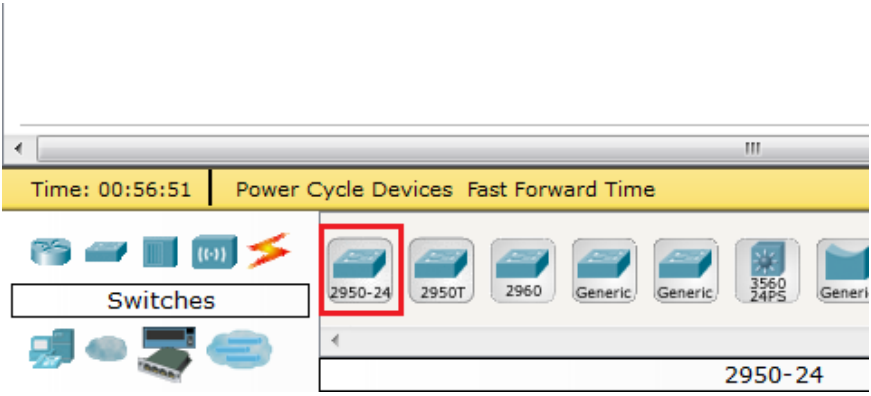
Опишите пути передачи пакетов и содержимое их заголовков.

После окончания симуляции проверьте ARP-таблицу компьютера, на котором выполнялась команда ping. Для этого откройте на нём командную строку и введите

arp -a

4. Изучение работы коммутатора 2-го уровня (свитча)

В построенной схеме сети замените хаб на свитч. Для этого в списке оборудования нажмите “Switches” и выберите первый в списке свитч.



Выполните действия, аналогичные предыдущему заданию и опишите различия в передаче пакетов хабом и свитчем.

Контрольные вопросы

1. Какие функции может выполнять программное средство Cisco Packet Tracer?
2. Чем отличаются хаб и свитч?
3. Что такое маска подсети?
4. Что делает команда ping?
5. Для чего предназначен протокол ARP?

ЛАБОРАТОРНАЯ РАБОТА № 3
СТАТИЧЕСКАЯ МАРШРУТИЗАЦИЯ

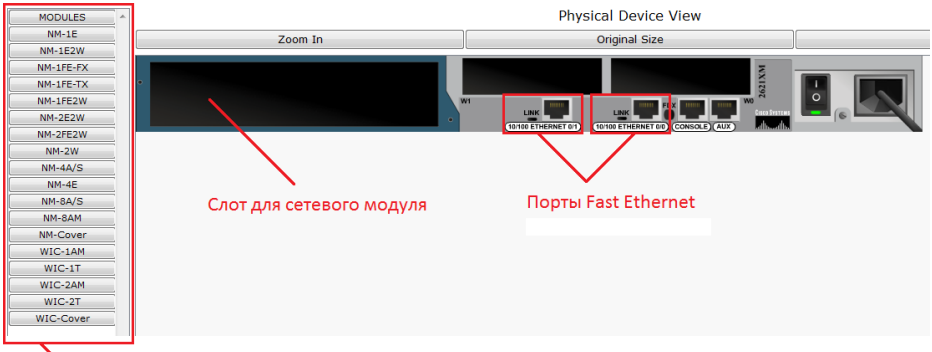
Цель: Изучить способы настройки статической маршрутизации.

Теоретические сведения

В процессе организации межсетевого взаимодействия важное место занимает маршрутизация сообщений между отдельными подсетями. При этом под маршрутизацией понимается процесс доставки сообщения из одной подсети в другую. Данная задача может решаться различными способами. При этом, чем сложнее рассматриваемая система, чем больше подсетей её образуют, тем более нетривиальным является решение задачи доставки сообщений.

Сетевым оборудованием, выполняющим функции маршрутизации, являются маршрутизаторы (router).

Все маршрутизаторы, представленные в Cisco Packet Tracer построены по модульному принципу и позволяют использовать модули для подключения к сетям различных типов.



Чтобы добавить модуль к маршрутизатору:

1. Выключите питание маршрутизатора.
2. Выберите необходимый сетевой модуль. Для сетей стандарта Fast Ethernet можно выбрать один из следующих модулей:
   - NM-1FE2W — включает 1 Fast Ethernet порт;
   - NM-2FE2W — включает 2 Fast Ethernet порта.
3. Перетяните мышкой изображение модуля из нижнего

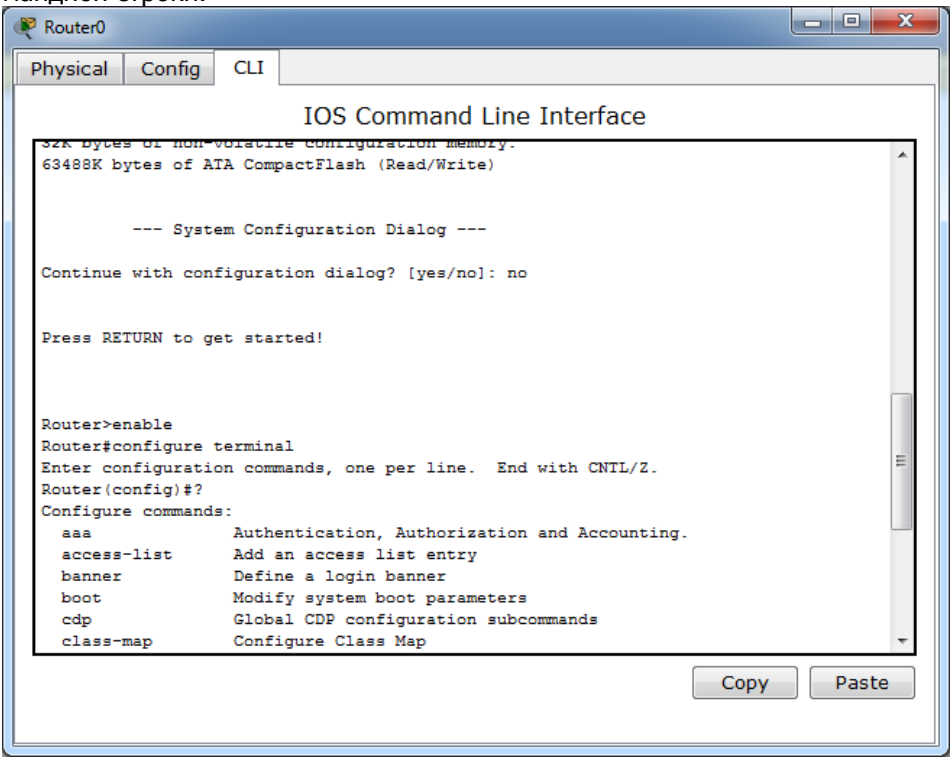
правого угла в подходящий слот маршрутизаора.

4. Включите питание.

После построения инфраструктуры сети необходимо настроить маршрутизаторы:

1. Для работы в сетях, к которым непосредственно подключён маршрутизатор;
2. Для осуществления маршрутизации между сетями.

Настройка маршрутизатора осуществляется в режиме командной строки.



Основные команды Cisco IOS:

1. Настройка интерфейса.

enable — переход в привилегированный режим.

configure terminal — переход в режим конфигурирования.

interface название номер — переход в режим настройки определённого интерфейса.

пример: interface FastEthernet0/0

ip address адрес маска — задаёт IP-адрес текущего интерфейса

пример: ip address 192.168.1.1 255.255.255.0

no shutdown — включает интерфейс
exit — выход из текущего режима
write mem — запись текущей конфигурации в память

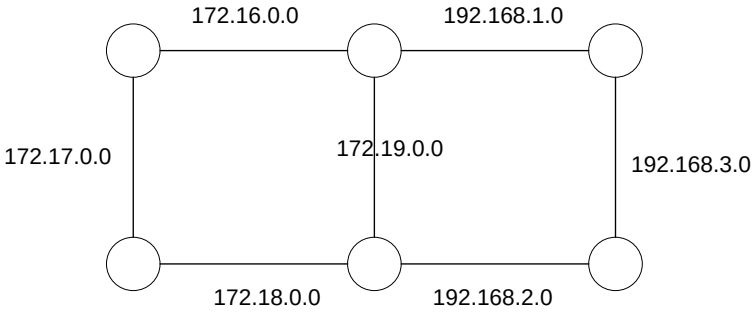
2. Статическая маршрутизация.
В режиме конфигурации маршрутизатора:
ip route сеть маска следующий_марутизатор
пример: ip route 172.18.0.0 255.255.0.0 192.168.1.2
show ip route — просмотр таблицы маршрутизации

3. Динамическая маршрутизация по протоколу RIP
В режиме конфигурации маршрутизатора:
router rip — переход в режим настройки протокола RIP
version 2 — устанавливает версию протокола 2
network адрес — задаёт адрес сети к которой подключен маршрутизатор и информация о которой должна передаваться соседним маршрутизаторам
пример: network 192.168.1.0
network 192.168.2.0
trace — выводит путь до указанного узла
show ip route — показывает таблицу маршрутизации
4. Динамическая маршрутизация по протоколу OSPF
route ospf 1
network адрес маска area зона
пример: network 192.168.1.0 area 0
network 192.168.2.0 area 0

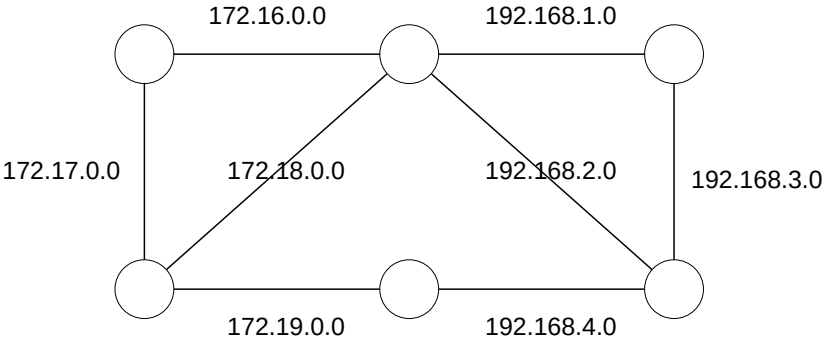
Задание

Настроить статическую маршрутизацию между сетями, представленными на схеме, в соответствии с вариантом задания.

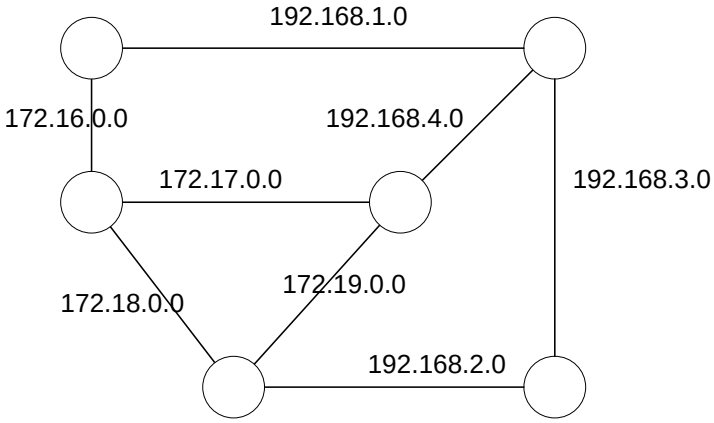
Вариант 1, 2



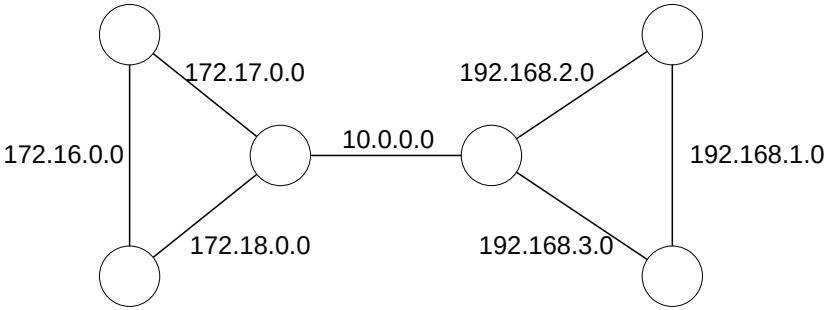
Вариант 3, 4



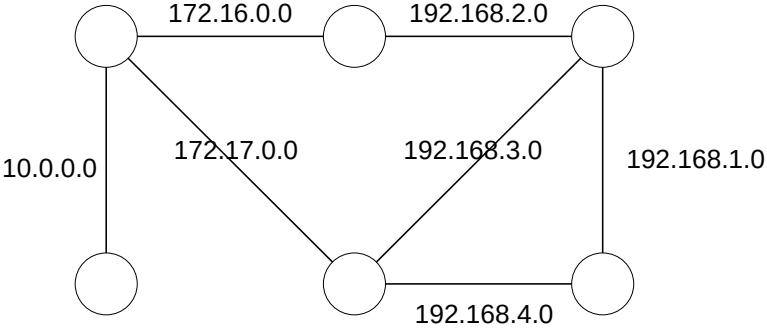
Вариант 5, 6



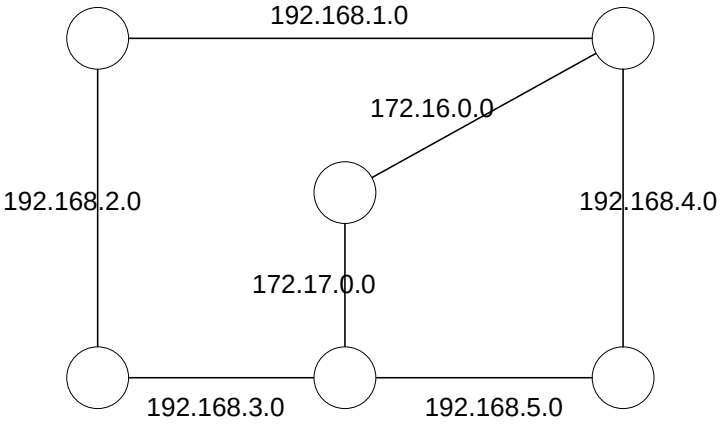
Вариант 7, 8



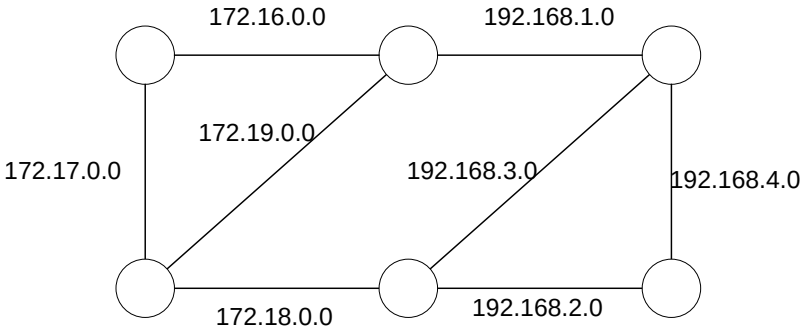
Вариант 9, 10



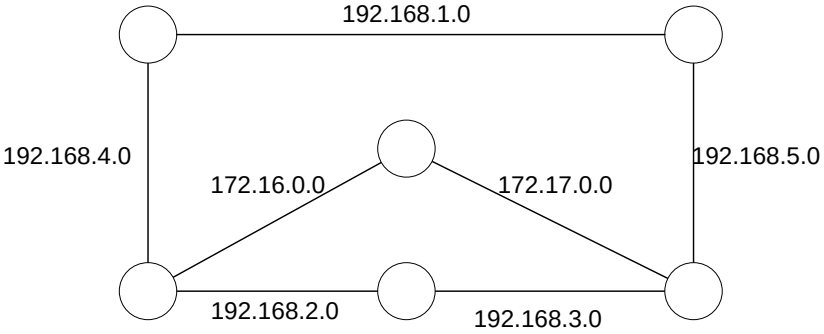
Вариант 11, 12



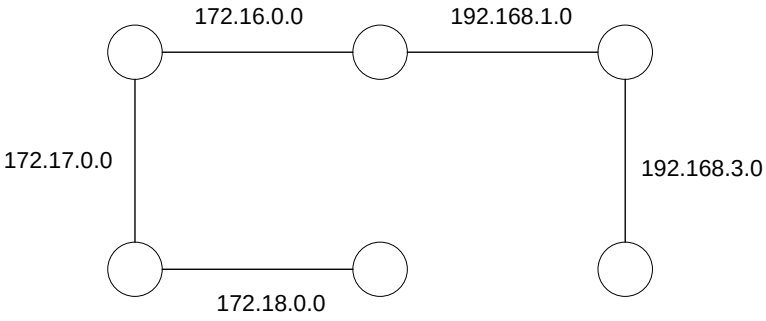
Вариант 13, 14



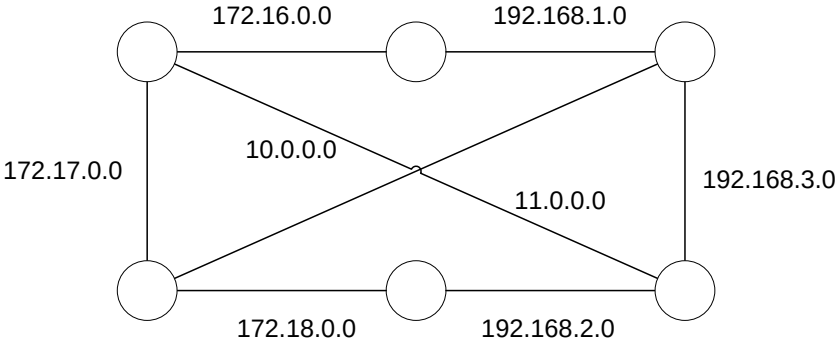
Вариант 15, 16



Вариант 17, 18



Вариант 19, 20



Отчёт по лабораторной работе должен содержать:

1. Титульный лист
2. Цель, задание
3. Схему сети из Packet Tracer с указанными IP-адресами всех портов всех маршрутизаторов
4. Последовательность команд для настройки интерфейсов хотя бы одного маршрутизатора
5. Последовательность команд для настройки статической маршрутизации на каждом маршрутизаторе
6. Таблицы маршрутизации каждого маршрутизатора
7. Несколько результатов команды trace до несоседнего маршрутизатора

Контрольные вопросы

1. Что такое маршрутизация?
2. Что такое маршрут?
3. Какой командой можно просмотреть маршрут пакета?
4. Для чего предназначены таблицы маршрутизации?
5. Какие сведения должна содержать каждая строка в таблице маршрутизации?
6. Исходя из каких соображений должна заноситься информация в таблицы маршрутизации?

ЛАБОРАТОРНАЯ РАБОТА № 4
ДИНАМИЧЕСКАЯ МАРШРУТИЗАЦИЯ

Цель: Изучить способы настройки динамической маршрутизации по протоколам RIP и OSPF.

Теоретические сведения

В зависимости от способа формирования содержимого таблицы маршрутизации различают два вида маршрутизации.

Статическая маршрутизация. Все маршруты прописываются и изменяются администратором системы вручную. Это самый простой способ организации маршрутизации. Однако он подходит только для небольших сетей, изменения в структуре которых происходят достаточно редко. Кроме того, данный способ маршрутизации не годится в случае, когда важно обеспечить высокую надежность межсетевого взаимодействия. Если один из маршрутов окажется по каким-либо причинам недоступен, администратору необходимо будет вручную изменить таблицу маршрутизации на всех маршрутизаторах в сети. До этого момента межсетевое взаимодействие на отдельных участках сети будет невозможно.

Динамическая маршрутизация. Построение таблицы маршрутизации осуществляется посредством специальных протоколов маршрутизации. Участие администратора в этом процессе минимально и сводится к изначальной конфигурации маршрутизаторов. Два наиболее распространенных протокола IP-маршрутизации, используемых в интрасетях, — протоколы RIP (Routing Information Protocol) и OSPF (Open Shortest Path First). Посредством указанных протоколов маршрутизаторы способны информировать друг друга об изменениях в структуре сети. В случае недоступности одного из маршрутов, маршрутизаторы автоматически перестроят свои таблицы маршрутизации и, при возможности, выберут другой маршрут доставки сообщений.

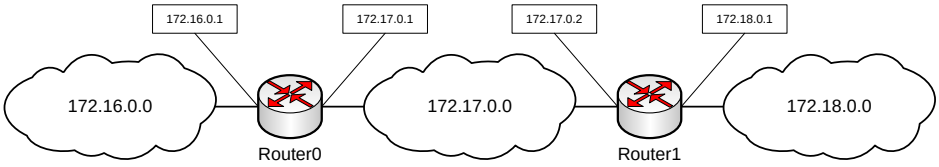
Для настройки динамической маршрутизации по протоколу RIP используются следующие команды:

В режиме конфигурации маршрутизатора:

router rip — переход в режим настройки протокола RIP.

network адрес — задаёт адрес сети к которой подключен маршрутизатор и информация о которой должна передаваться соседним маршрутизаторам.

Рассмотрим пример соединения сетей, представленный на рисунке:



Для настройки маршрутизации по протоколу RIP следует выполнить следующие команды:

на маршрутизаторе Router0:

```
Router>enable
Router#configure terminal
Router(config)#router rip
Router(config-router)#network 172.16.0.0
Router(config-router)#network 172.17.0.0
```

на маршрутизаторе Router1:

```
Router>enable
Router#configure terminal
Router(config)#router rip
Router(config-router)#network 172.17.0.0
Router(config-router)#network 172.18.0.0
```

Настройка динамической маршрутизации по протоколу OSPF выполняется аналогичным образом — для каждого маршрутизатора необходимо указать сети, информацию о которых он будет рассылать другим маршрутизаторам. Для этого используются следующие команды:

route ospf 1 — переход в режим настройки протокола OSPF.
network адрес маска area зона
Например: network 172.16.0.0 area 0
network 172.17.0.0 area 0

Для проверки настроек можно использовать следующие команды:

show ip route — показывает таблицу маршрутизации,
trace адрес — выводит путь до указанного узла.

Задание

Для схем сетей, приведённых в лабораторной работе № 3 настроить динамическую маршрутизацию отдельно по протоколу RIP и отдельно по протоколу OSPF.

Удалить или отключить соединение между двумя маршрутизаторами, не нарушая связности сети (то есть так чтобы осталась возможность из любого узла сети попасть на любой другой узел). Определить, как данные изменения отразятся в таблицах маршрутизации.

Отчёт по лабораторной работе должен содержать:

1. Титульный лист.
2. Цель, задание.
3. Схему сети из Packet Tracer с указанными IP-адресами всех портов всех маршрутизаторов.
4. Последовательность команд для настройки динамической маршрутизации на каждом маршрутизаторе.
5. Таблицы маршрутизации каждого маршрутизатора.
6. Несколько результатов команды trace до несоседнего маршрутизатора.

Контрольные вопросы

1. В чём отличие динамической маршрутизации от статической?
2. Что такое протокол маршрутизации?
3. В чём отличие дистанционно-векторных протоколов маршрутизации от протоколов, основанных на состоянии связей?
4. Какие маршрутизаторы считаются соседними?

ЛАБОРАТОРНАЯ РАБОТА № 5
ПРОТОКОЛ DHCP

Цель: Изучить способы настройки протокола динамической конфигурации хоста.

Теоретические сведения

DHCP (англ. Dynamic Host Configuration Protocol — протокол динамической настройки узла) — сетевой протокол, позволяющий компьютерам автоматически получать IP-адрес и другие настройки, необходимые для работы в сети, такие как маска подсети, шлюз по умолчанию, адрес DNS-сервера.

Централизованное распределение IP-адресов позволяет не только избежать ручного ввода настроек сети на каждом компьютере, но и гарантирует отсутствие повторяющихся адресов внутри сети.

Для настройки DHCP используются следующие команды, вводить которые необходимо в режиме конфигурации маршрутизатора:

ip dhcp excluded-address адрес — позволяет исключить адрес из выдачи по протоколу DHCP.

ip dhcp pool название — создаёт пул (множество) IP-адресов для выдачи узлам сети и переходит в режим его конфигурирования.

В режиме конфигурации пула адресов:

default-router адрес — задаёт адрес, который будет назначен узлам сети в качестве шлюза по умолчанию.

network адрес маска — указывает сеть, из которой должны браться адреса для выдачи узлам сети.

Например, следующие настройки позволяют маршрутизатору подключённому к сети 192.168.0.0 и имеющему в ней адрес 192.168.0.1 выдавать IP-адреса компьютерам, находящимся в этой сети, исключая уже занятый им адрес:

```
Router>enable
Router#configure terminal
Router(config)#ip dhcp excluded-address 192.168.0.1
Router(config)#ip dhcp pool my_net
Router(dhcp-config)#default-router 192.168.0.1
Router(dhcp-config)#network 192.168.0.0 255.255.255.0
```

Задание

Для схем сетей, приведённых в лабораторной работе № 3 настроить автоматическую выдачу IP-адресов, масок и шлюзов по умолчанию в каждой сети.

Отчёт по лабораторной работе должен содержать:

1. Титульный лист.
2. Цель, задание.
3. Схему сети из Packet Tracer с указанными IP-адресами всех портов всех маршрутизаторов.
4. Последовательность команд для настройки протокола DHCP на тех маршрутизаторах, на которых она выполнялась.
5. Скриншоты окна конфигурации с полученными по протоколу DHCP настройками для хотя бы одного компьютера в каждой сети.

Контрольные вопросы

1. Для чего предназначен протокол DHCP?
2. Как работает протокол DHCP?
3. Какие настройки необходимы для работы конечных узлов сети?
4. Что такое шлюз по умолчанию?
5. Какое устройство обычно является шлюзом по умолчанию?

ЛАБОРАТОРНАЯ РАБОТА № 6
ТРАНСЛЯЦИЯ СЕТЕВЫХ АДРЕСОВ

Цель: Изучить способы настройки динамической трансляции сетевых адресов.

Теоретические сведения

NAT (от англ. Network Address Translation — трансляция сетевых адресов) — это механизм в сетях TCP/IP, позволяющий преобразовывать IP-адреса в заголовках пакетов, проходящих через какое-либо устройство.

Узлам сети, находящимся с внутренней стороны устройства NAT, назначаются частные IP-адреса; обычно это делается через службу DHCP или путем статической настройки, выполняемой администратором.

Когда приложение, запущенное на компьютере во внутренней сети, инициирует отправку данных, частный IP-адрес клиента (IP-адрес источника) и клиентский порт (порт источника) вставляются в пакет в поля параметров источника. Поля параметров пункта назначения будут содержать IP-адрес сервера (IP-адрес назначения — удаленный узел) и порт сервера. Поскольку пункт назначения пакета находится вне частной сети, клиент направляет его в основной шлюз, на котором должна быть настроена трансляция адресов и портов.

Устройство NAT перехватывает исходящий пакет и производит сопоставление порта, используя IP-адрес назначения (адрес сервера), порт назначения, внешний IP-адрес устройства NAT, внешний порт, сетевой протокол, а также внутренние IP-адрес и порт клиента.

Устройство NAT ведет таблицу сопоставлений портов и сохраняет созданное сопоставление в этой таблице. Внешние IP-адрес и порт — это общие IP-адрес и порт, которые будут использоваться в текущем сеансе передачи данных вместо внутренних IP-адреса и порта клиента.

Затем устройство NAT «транслирует» пакет, преобразуя в пакете поля источника: частные, внутренние IP-адрес и порт клиента заменяются, внешними IP-адресом и портом устройства NAT.

Преобразованный пакет пересылается по внешней сети и в итоге попадает на заданный сервер.

Получив пакет, сервер полагает, что имеет дело с каким-то одним компьютером, IP-адрес которого допускает глобальную

маршрутизацию. Сервер будет направлять ответные пакеты на внешние IP-адрес и порт устройства NAT, указывая в полях источника свои собственные IP-адрес и порт.

NAT принимает эти пакеты от сервера и анализирует их содержимое на основе своей таблицы сопоставления портов. Если в таблице будет найдено сопоставление порта, для которого IP-адрес источника, порт источника, порт назначения и сетевой протокол из входящего пакета совпадают с IP-адресом удаленного узла, удаленным портом и сетевым протоколом, указанным в сопоставлении портов, NAT выполнит обратное преобразование. NAT заменяет внешний IP-адрес и внешний порт в полях назначения пакета на частный IP-адрес и внутренний порт клиента.

Затем NAT отправляет пакет клиенту по внутренней сети. Однако если NAT не находит подходящего сопоставления портов, входящий пакет отвергается и соединение разрывается.

Благодаря устройству NAT клиент получает возможность передавать данные в глобальной среде Интернета, используя лишь частный IP-адрес; ни от приложения, ни от клиента не требуется никаких дополнительных усилий.

Задание

1. Добавить на схему из лабораторной работы № 3 еще 2 сети с адресами 192.168.0.0/24.

2. На каждом маршрутизаторе, соединяющем новые сети с созданными ранее, настроить трансляцию сетевых адресов.

Настройка трансляции сетевых адресов осуществляется с помощью следующих команд:

В режиме настройки интерфейса:

ip nat inside — указывает, что данный интерфейс находится во внутренней сети.

ip nat outside — указывает, что данный интерфейс находится во внешней сети.

В режиме конфигурации маршрутизатора:

ip access-list extended имя — создаёт список контроля доступа с заданным именем и переходит в режим его настройки.

В режиме настройки списка контроля доступа:

permit ip any any — разрешает всем узлам доступ к любым адресам по любому протоколу.

В режиме конфигурации маршрутизатора:

ip nat inside source list имя interface название_интерфейса overload — включает трансляцию адресов внутренней сети в ад-

рес указанного интерфейса.

3. Создать внутри каждой добавленной сети web-сервер и настроить доступ к нему из внешних сетей.

Для этого в режиме конфигурации маршрутизатора используется команда:

ip nat inside source static протокол(TCP|UDP) внутренний_адрес внутренний_порт внешний_адрес внешний_порт

По мере осуществление трансляции в NAT-таблицах маршрутизаторов накапливается информация, посмотреть которую можно в привилегированном режиме маршрутизатора командой

show ip nat translations

Отчёт по лабораторной работе должен содержать:

1. Титульный лист
2. Цель, задание
3. Команды, использованные для настройки NAT
4. Скриншот заголовков пакета при его прохождении через устройство с NAT.
5. NAT-таблицы маршрутизаторов

Контрольные вопросы

1. Что такое NAT?
2. Как работает трансляция сетевых адресов?
3. Что такое внутренняя сеть и внешняя сеть?
4. Какие диапазон IP-адресов допустимо использовать во внутренней сети? Почему?
5. Что такое порт?
6. Что такое NAT-таблица?
7. Какие сведения содержатся в каждой строке NAT-таблицы?
8. При каком событии в NAT-таблицу добавляется информация?
9. Что такое перенаправление порта и для чего оно используется?

ЛАБОРАТОРНАЯ РАБОТА № 7
ПОСТРОЕНИЕ ВИРТУАЛЬНЫХ ТУННЕЛЕЙ

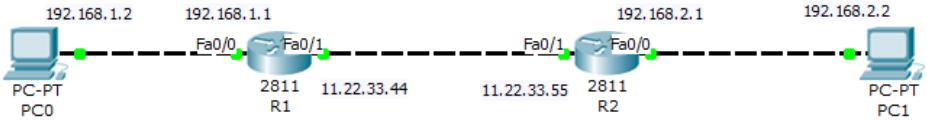
Цель: Изучить возможности построения виртуальных туннелей поверх существующих сетей.

Теоретические сведения

Туннелирование (от англ. tunnelling — «прокладка туннеля) — процесс, в ходе которого создается логическое соединение между двумя конечными точками посредством инкапсуляции различных протоколов.

Generic Routing Encapsulation (GRE) — протокол туннелирования сетевых пакетов, разработанный фирмой Cisco. Этот протокол используется для передачи пакетов одной сети, через другую сеть. GRE туннель представляет собой соединение точка-точка, его можно считать одной из разновидностей VPN туннеля, без шифрования. Основное достоинство GRE это возможность передавать широковещательный трафик, что позволяет пропускать через такой туннель протоколы маршрутизации использующие его. При использовании публичных сетей необходимо совместно с GRE применять IPSec для реализации защищенных VPN соединений.

Ниже приведен пример создания простого туннеля между двумя сетями.



R1	R2
R1(config)# interface Tunnel0 R1(config-if)# ip address 172.16.0.1 255.255.0.0 R1(config-if)# tunnel source FastEthernet0/1 R1(config-if)# tunnel destination 11.22.33.55	R2(config)# interface Tunnel0 R2(config-if)# ip address 172.16.0.2 255.255.0.0 R2(config-if)# tunnel source FastEthernet0/1 R2(config-if)# tunnel destination 11.22.33.44

В первой строке создаётся виртуальный интерфейс для организации туннеля. Во второй строке данному интерфейсу при-

сваивается адрес. Адреса туннельных интерфейсов должны принадлежать одной сети (в данном случае 172.16.0.0). В следующих двух строка указываются адреса начала и конца тоннеля.

После настройки интерфейсов необходимо задать маршруты в удалённые сети через адреса виртуальных интерфейсов:

R1(config)# ip route 192.168.2.0 255.255.0.0 172.16.0.2

R2(config)# ip route 192.168.1.0 255.255.0.0 172.16.0.1

Результат команды tracert, выполненной на компьютере PC0.

```
PC>tracert 192.168.2.2

Tracing route to 192.168.2.2 over a maximum of 30 hops:

  1    78 ms      31 ms      31 ms      192.168.1.1
  2    *          63 ms      49 ms      172.16.0.2
  3    *          93 ms      94 ms      192.168.2.2

Trace complete.
```

На рисунке видно, что сначала пакет отправляется на шлюз по умолчанию, затем на адрес виртуального туннельного интерфейса и конце на компьютер назначения.

Задание

1. Добавить 3 сети к схеме, разработанной на предыдущей лабораторной работе. Перед добавлением необходимо убедиться, что между всеми маршрутизаторами сети настроена маршрутизация и каждый узел доступен с любого другого узла сети. Для адресации внутри сетей можно использовать любые частные адреса из тех, которые еще не присутствуют на схеме. При подключении данных сетей необходимо использовать маршрутизатор серии 2811.
2. Настроить тунеллирование между данными сетями.

Отчёт по лабораторной работе должен содержать:

1. Титульный лист
2. Цель, задание
3. Схему сети
4. Команды, использованные для создания туннелей

5. Команды, использованные для настройки маршрутизации между виртуальными сетями

6. Скриншот содержимого пакета при его прохождении по виртуальному туннелю

7. Скриншоты результатов команды tracert, выполненной на компьютерах внутри добавленных локальных сетей

Контрольные вопросы

1. Что такое туннель?

2. Для решения каких задач может использоваться туннелирование?

3. Что такое виртуальный интерфейс?

4. Что такое инкапсуляция пакетов?

5. Какие параметры необходимо задать для построения туннеля?