ВВЕДЕНИЕ

Данный курс лабораторных работ направлен на закрепление изученного материала по теме «Компьютерные системы и сети» и предназначен для студентов, обучающихся по направлению «Инфокоммуникационные технологии и системы связи».

Целью лабораторных работ является освоение основных принципов работы в программном продукте компании Cisco Systems под названием «Cisco Packet Tracer». Данное программное обеспечение активно используется для подготовки сетевых инженеров по всему миру, в частности, для успешного прохождения квалификационных экзаменов, каких как: CCENT, CCNA и CCNP. Сертификации Cisco базового уровня CCENT подтверждают базовые знания сетевых технологий и основные навыки поддержки сетей предприятия. Они относительно мало популярны у работодателей, но служат хорошим стартом для изучения сетевых технологий. Сертификации уровня CCNA являются стартовыми и подтверждают общие знания в определённой области сетевых технологий, но не затрагивают сложные технические аспекты. Экзамены Cisco CCNA - самые распространённые по частоте попыток сдачи.

Сертификации уровня CCNP дают глубокие знания, востребованные в конкретных областях применения (корпоративные сети, сети датацентров, сети операторов связи и провайдеров). Экзамены CCNP подтверждают знания и умение применять навыки - по сути, именно они и являются целью для тех, кто хочет эффективно работать в современном IT.

Все приведённые в данном методическом пособии наименования устройств и элементов управления справедливы для версии Cisco Packet Tracer версии 7.1.0.0222, в других версиях, и даже сборках, они могут отличаться.

Курс разбит на четыре лабораторных работы:

1. Знакомство с Cisco PT
2. Коммутация пакетов
3. Маршрутизация
4. Виртуальные локальные сети.

Сокращения и термины:

Протокол (сетевой протокол) – определённый набор правил и/или действий, утверждённых Инженерным советом Интернета (IETF), Институтом инженеров электротехники и электроники (IEEE) или Международной организацией по стандартизации (ISO).

Сетевая модель OSI (Open System Interconnection). Модель *взаимодействия открытых систем* - принятая ISO и ITU (International Telecommunications Union) эталонная модель, состоящая из семи уровней, и описывающая поведение пересылаемых данных на пути от отправителя к получателю. Уровни: 1 - физический, 2 - канальный, 3 - сетевой, 4 - транспортный, 5 - сеансовый, 6 - представления, 7 - прикладной.

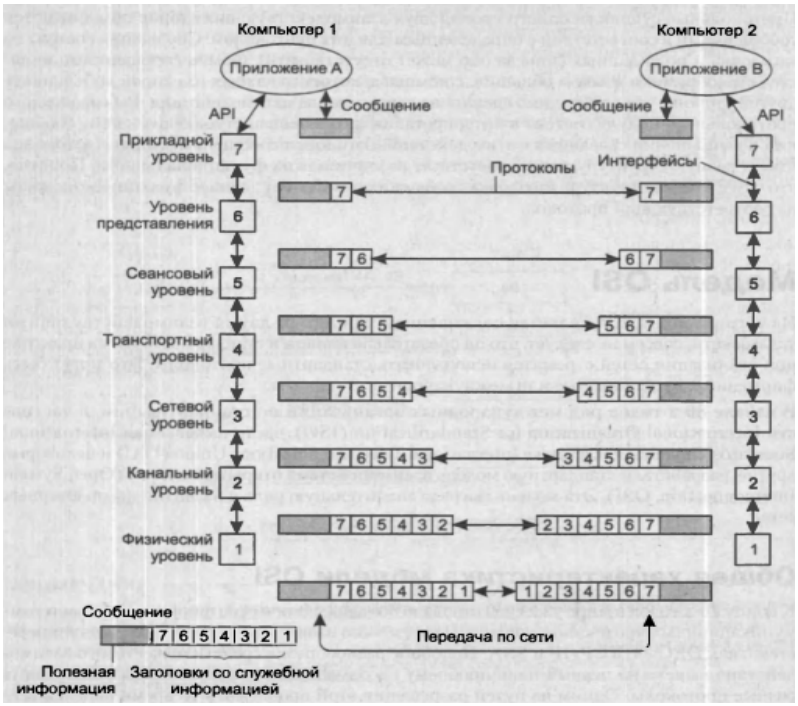


Рис.1. Модель OSI.

Стек протоколов – утверждённый набор протоколов.

Стек протоколов TCP/IP – четырёхуровневая, применяемая на практике модель взаимодействия сетевых устройств. Уровни: 1 – сетевых интерфейсов, 2 – сетевой, 3 – транспортный, 4 – прикладной.

Прикладной уровень	FTP, Telnet, HTTP, SMTP, SNMP, TFTP
Транспортный уровень	TCP, UDP
Сетевой уровень	IP, ICMP, RIP, OSPF
Уровень сетевых интерфейсов	Не регламентируется

Рис.2. Иерархическая структура стека протоколов TCP/IP.

WAN (Wide Area Network) – глобальная сеть, соединяющая компьютеры рассредоточенные территориально.

LAN (Local Area Network) – локальная сеть, объединяющая компьютеры сосредоточенные на небольшой территории.

Топология сети – конфигурация графа, вершинами которого являются конечные узлы сети и/или сетевое оборудование, а рёбрами – связи между узлами.

Основные виды топологий сети: полносвязная (рис.3,а), ячеистая (рис.3,б), кольцевая (рис.3,в), звездообразная (рис.3,г), древовидная (рис.3,д), общая шина (рис.3,е).

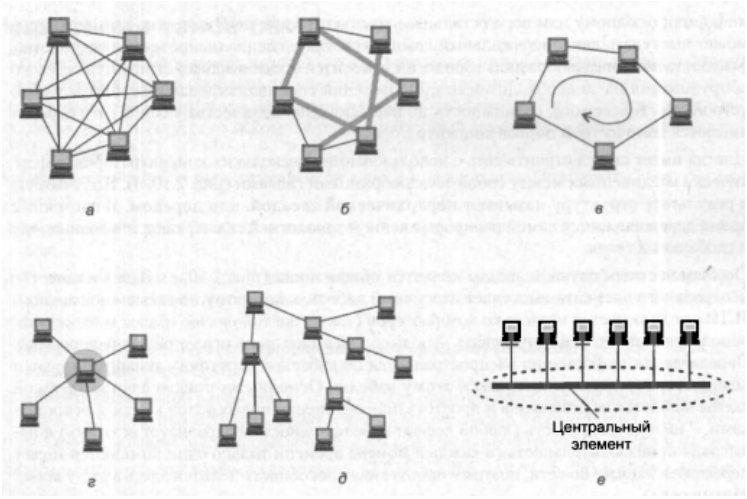


Рис.3. Типовые топологии сетей

Концентратор – сетевое устройство, работающее на физическом уровне модели OSI, перенаправляет сигнал со входного порта на все другие порты.

Коммутатор – поддерживает протоколы двух нижних уровней модели OSI, физического и канального, это позволяет им работать в пределах стандартных топологий. Принимает на один из своих портов сигнал и дублирует его на другой порт, исходя из хранящейся на этом устройстве таблицы коммутации.

Таблица маршрутизации — таблица, содержащая информацию о соответствии адресов сетей интерфейсам (шлюзам по умолчанию).

Маршрутизатор – поддерживает протоколы трех нижних уровней: сетевого - для объединения сетей различных технологий, а протоколы нижних уровней - для взаимодействия с конкретными сетями. Занимается продвижением или фильтрацией информационных пакетов, следуя правилам записанным в таблице маршрутизации.

IP-адрес – иерархический адрес сетевого интерфейса. Старшие байты указывают на номер сети, а младшие на номер узла в этой сети.

MAC-адрес – уникальный идентификатор устройства.

ARP-таблица - таблица, хранящая соответствия IP-адресов MAC-адресам сетевых интерфейсов.

Лабораторная работа №1

«Знакомство с Cisco Packet Tracer»

Общие теоретические сведения.

Cisco Packet Tracer является очень удобным средством моделирования сетей передачи данных. Основные инструменты его интерфейса расположены и организованы вполне логично, что упрощает процесс знакомства с программой, а также значительно сокращает время необходимое для предварительной подготовки. Есть некоторые особенности использования специфичных для Cisco Packet Tracer инструментов, но эти инструмент используются не часто. В большинстве случаев для начала работы достаточно короткого первого знакомства с интерфейсом программы.

Основное окно программы одержит 6 основным меню, 4 из которых используются наиболее часто. На рисунке отмечены наиболее часто используемые меню программы Cisco Packet Tracer.

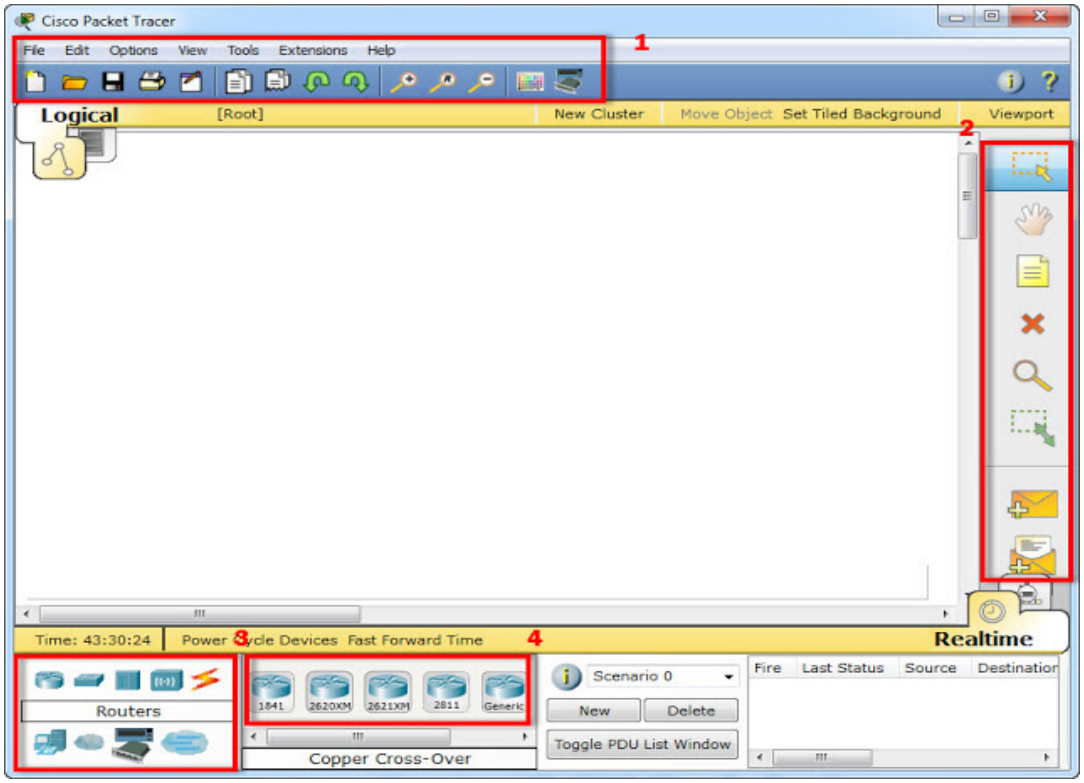


Рис.. Окно программы Cisco Packet Tracer.

Стандартное программное меню **(1)** мало чем отличается от подобного меню в других программах. Исключение составляют два инструмента на графической панели: **Drawing Palette** и **Custom Device Dialog**. Для данного курса они не важны, поэтому опустим их подробное описание.

Правое графическое меню **(2)** содержит достаточно узнаваемые пиктограммы инструментов для работы с проектом и объектами проекта. Каждый из расположенных в данном меню инструментов активируется кликом мышки на соответствующей пиктограмме, а также, для более быстрого доступа, соответствующей клавишей. Несмотря на узнаваемость, принцип использования инструментов не всегда так очевиден, как это кажется с первого взгляда.

Первый инструмент меню (с верху в низ) **Select** (быстрый доступ - **[Esc]**).



Как и в большинстве других программ используется для выделения одного или более объектов. Как правило для последующего перемещения, копирования или удаления.

Следующий инструмент данного графического меню **Move Layout** (**[M]**) используется для прокрутки больших проектов.



Несмотря на то что основное окно программы, используемое для построения проекта. имеет полосы прокрутки, наличие дополнительного инструмента с подобной функцией, активируемого нажатием одной клавиши, может быть очень удобным при работе с большими топологиями. В случае лабораторных работ, настолько большие топологии не предвидятся.

Инструмент **Place Note** (**[N]**) добавляет подпись в любой части проекта. Удобно использовать для комментариев или же для размещения основной информации сценария непосредственно в проекте для дальнейшей работы.



Инструмент **Delete** (**[Del]**) удаляет объект или группу объектов.



Инструмент **Inspect** (**[I]**) несмотря на внешний вид напоминающий лупу, не используется для увеличения объектов проекта.



Данный инструмент позволяет, в зависимости от типа устройства, просматривать содержимое таблицы **ARP**, таблицы маршрутизации, таблицы **NAT** и т.д. Не смотря на кажущееся удобство данного инструмента, для инспекции содержимого данных таблиц лучше по возможности использовать внутренние команды устройства.

Постоянно исключаемый из большей части описаний инструмент **Resize Shape** (**[Alt]+[R]**), предназначен для изменения размеров рисованных объектов (четырехугольников и окружностей).



Так как инструмент рисования не очень удобен в **Cisco Packet Tracer**, то и **Resize Shape** мало кем используется.

Находящиеся в самом низу данного меню инструменты **Add Simple PDU** (**[P]**) и **Add Complex PDU** (**[C]**) предназначены для эмулирования отправки с последующим отслеживанием произвольного пакета данных внутри проекта.





Данная возможность способствует лучшему пониманию моделируемых технологий. Различия двух данных инструментов заключаются в большем количестве возможных параметров при использовании **Add Complex PDU,** в то время как **Add Simple PDU** позволяет это сделать проще и быстрее.

Два графических меню (3 и 4), находящихся в левом углу интерфейса являются наиболее используемыми.

Меню 3 позволяет выбрать тип устройств, а меню 4 непосредственно само устройство. Наиболее используемыми являются:

Routers - позволяет добавлять в проект маршрутизаторы **Cisco**. В **Cisco Packet Tracer** доступны Cisco 1841, Cisco 2820 XM, Cisco 2821 XM, Cisco 2811.

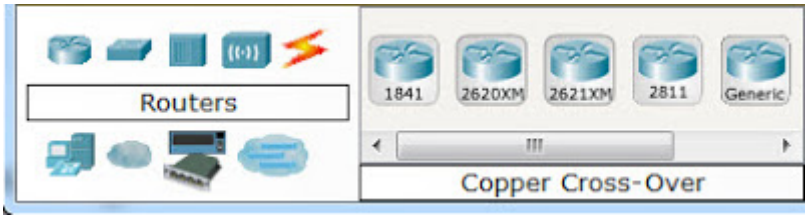


Рис.. Группа устройств Routers.

Switches - используется для добавления коммутаторов **L2**. Доступны следующие модели Cisco Catalyst WS-C2950-24, Cisco Catalyst WS-C2950T-24, Cisco Catalyst WS-C2960-24TT

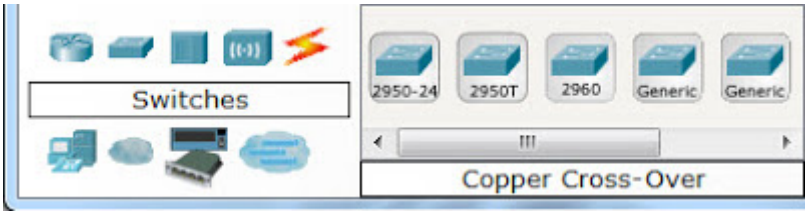


Рис.. Группа устройств Switches.

Connections - выбор типа подключения для объектов топологии проекта.

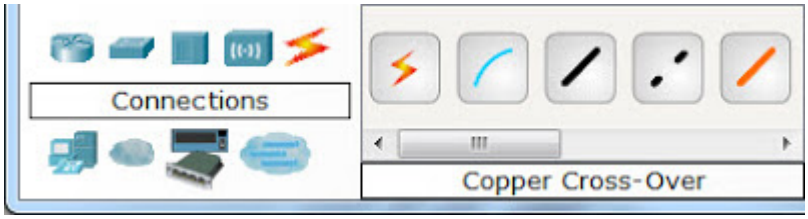


Рис.. Группа элементов Connections.

End devices - выбор конечных устройств. Персональные компьютеры, лэптопы, IP-телефоны и серверы.

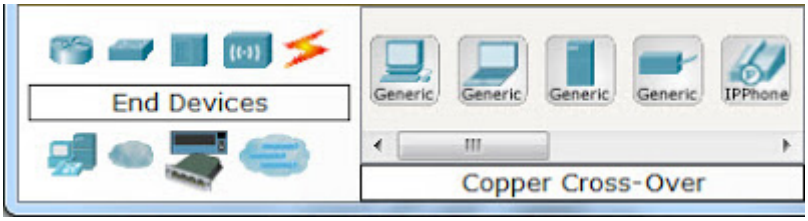


Рис.. Группа устройств End Devices.

Добавление объектов топологии производится просты перетаскиванием.

При соединении различных устройств в единую топологию, используя **Connections**, будет предоставляться выбор физического порта подключения.

Задание на лабораторную работу.

1. Изучить интерфейс программы Cisco Packet Tracer. Дать ответы на контрольные вопросы.
2. Поместить в поле проектирования необходимые компоненты схемы и соединить их между собой так, как показано на рисунке:

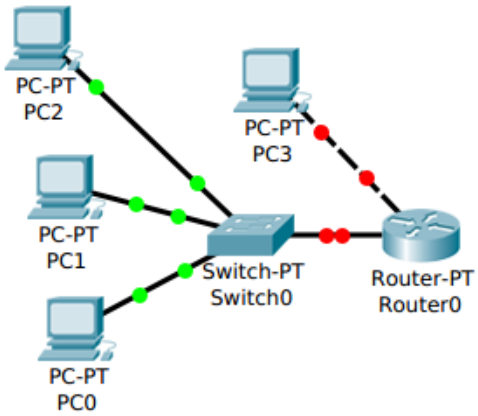


Рис.. Абстрактная схема сети.

При построении заменять элементы схемы, в соответствии с вариантом, на конкретные устройства из таблицы 1.

Таблица 1. Варианты задания.

Вариант	Router	Switch	End devices 0-2	End device 3
1	1941	2960-24TT	PC	Laptop
2	2901	2950-24	Laptop	PC
3	2911	2950T-24	Server	Printer
4	829	2960-24TT	Printer	Server
5	1841	2950-24	IP Phone	PC
6	2811	2950T-24	PC	IP Phone

3. Проанализировать работу устройств с помощью инструмента **Inspect**.
4. Сформировать отчёт, демонстрирующий ход работы (включая данные о работе устройств). Сделать выводы.

Контрольные вопросы.

1. Перечислить основные блоки элементов интерфейса Cisco Packet Tracer.
2. Какие виды соединений представлены в данной программе? Для соединения каких интерфейсов они предназначены?
3. Что понимается под термином локальная вычислительная сеть (LAN)?
4. Что такое маршрутизатор? Для чего служит это устройство?
5. Что такое коммутатор? Для чего служит это устройство?
6. Какие параметры конфигурации получают конечные устройства без дополнительной настройки оборудования (по умолчанию)?

Лабораторная работа №2.

«Коммутация пакетов»

Общие теоретические сведения.

В традиционных телефонных сетях, связь абонентов между собой выполняется с помощью коммутации каналов связи. В начале коммутация телефонных каналов связи выполнялась вручную, далее коммутацию выполняли автоматические телефонные станции (АТС).

Аналогичный принцип используется и в вычислительных сетях. В качестве абонентов выступают территориально удаленные вычислительные машины в компьютерной сети. Физически не представляется возможным предоставить каждому компьютеру свою собственную некоммутируемую линию связи, которой они пользовались бы в течении всего времени. Поэтому практически во всех компьютерных сетях всегда используется какой-либо способ коммутации абонентов (рабочих станций), выполняющий возможность доступа к существующим каналам связи для нескольких абонентов, для обеспечения одновременно нескольких сеансов связи.

Коммутация — это процесс соединения различных абонентов коммуникационной сети через транзитные узлы. Коммуникационные сети должны обеспечивать связь своих абонентов между собой. Абонентами могут выступать ЭВМ, сегменты локальных сетей, факс-аппараты или телефонные собеседники.

Коммутация каналов.

Коммутация каналов подразумевает образование непрерывного составного физического канала из последовательно соединенных отдельных канальных участков для прямой передачи данных между узлами. Отдельные каналы соединяются между собой специальной аппаратурой - коммутаторами, которые могут устанавливать связи между любыми конечными узлами сети. В сети с коммутацией каналов перед передачей данных всегда необходимо выполнить процедуру установления соединения, в процессе которой и создается составной канал.

Время передачи сообщения при этом определяется пропускной способностью канала, длинной связи и размером сообщения.

Коммутаторы, а также соединяющие их каналы должны обеспечивать одновременную передачу данных нескольких абонентских каналов. Для этого они должны быть высокоскоростными и поддерживать какую-либо технику мультиплексирования абонентских каналов.

Достоинства коммутации каналов:

- постоянная и известная скорость передачи данных;
- правильная последовательность прихода данных;
- низкий и постоянный уровень задержки передачи данных через сеть.

Недостатки коммутации каналов:

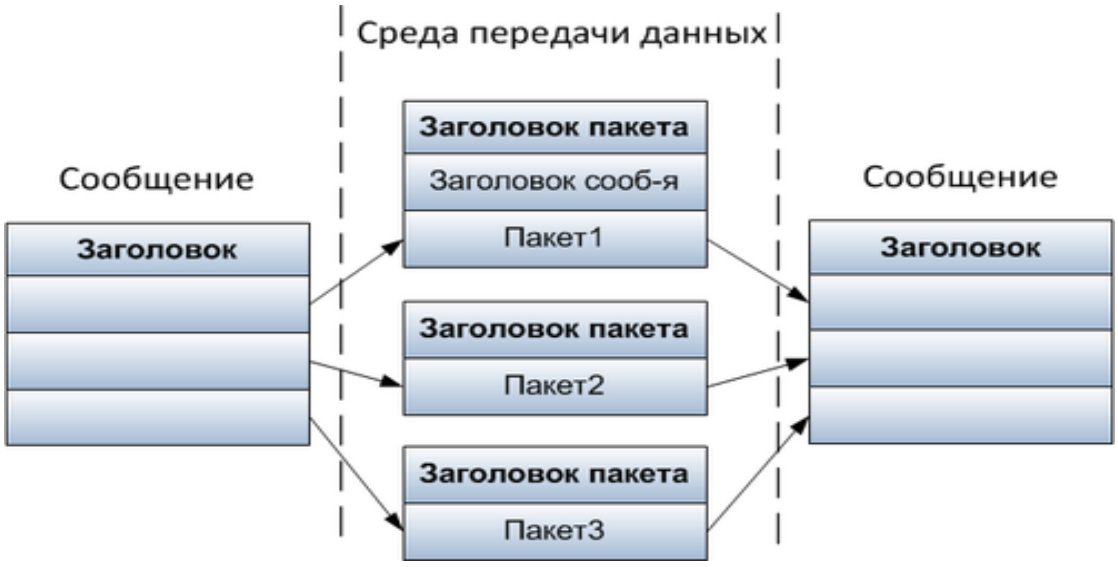
- возможен отказ сети в обслуживании запроса на установление соединения;
- нерациональное использование пропускной способности физических каналов, в частности невозможность применения пользовательской аппаратуры, работающей с разной скоростью. Отдельные части составного канала работают с одинаковой скоростью, так как сети с коммутацией каналов не буферизуют данные пользователей;
- обязательная задержка перед передачей данных из-за фазы установления соединения.

Коммутация пакетов.

Коммутация пакетов - это особый способ коммутации узлов сети, который специально создавался для наилучшей передачи компьютерного трафика (пульсирующего трафика). Опыты по разработке самых первых компьютерных сетей, в основе которых лежала техника коммутации каналов, показали, что этот вид коммутации не предоставляет возможности получить высокую пропускную способность вычислительной сети. Причина крылась в пульси-

рующем характере трафика, который генерируют типичные сетевые приложения.

При коммутации пакетов все передаваемые пользователем сети сообщения разбиваются в исходном узле на сравнительно небольшие части, называемые пакетами. Необходимо уточнить, что сообщением называется логически завершенная порция данных - запрос на передачу файла, ответ на этот запрос, содержащий весь файл, и т. п. Сообщения могут иметь произвольную длину, от нескольких байт до многих мегабайт. Напротив, пакеты обычно тоже могут иметь переменную длину, но в узких пределах, например от 46 до 1500 байт (EtherNet). Каждый пакет снабжается заголовком, в котором указывается адресная информация, необходимая для доставки пакета узлу назначения, а также номер пакета, который будет использоваться узлом назначения для сборки сообщения.



Коммутаторы пакетной сети отличаются от коммутаторов каналов тем, что они имеют внутреннюю буферную память для временного хранения пакетов, если выходной порт коммутатора в момент принятия пакета занят передачей другого пакета.

Достоинства коммутации пакетов:

- более устойчива к сбоям;

- высокая общая пропускная способность сети при передаче пульсирующего трафика;
- возможность динамически перераспределять пропускную способность физических каналов связи.

Недостатки коммутации пакетов:

- неопределенность скорости передачи данных между абонентами сети;
- переменная величина задержки пакетов данных;
- возможны потери данных из-за переполнения буферов;
- возможны нарушения последовательности прихода пакетов.

В компьютерных сетях применяется коммутация пакетов.

Задание на лабораторную работу.

1. Построить схему, изображённую на рисунке:

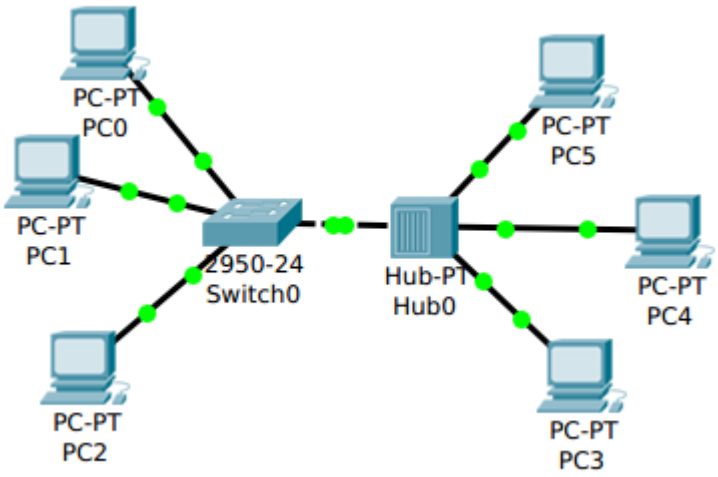


Рис.. Схема коммутации.

2. Назначить каждому из оконечных устройств статический IP-адрес.

Сделать это можно кликнув по устройству PC-PT и, в открывшемся окне PCx во вкладке «Desktop», выбрать утилиту «IP configuration».

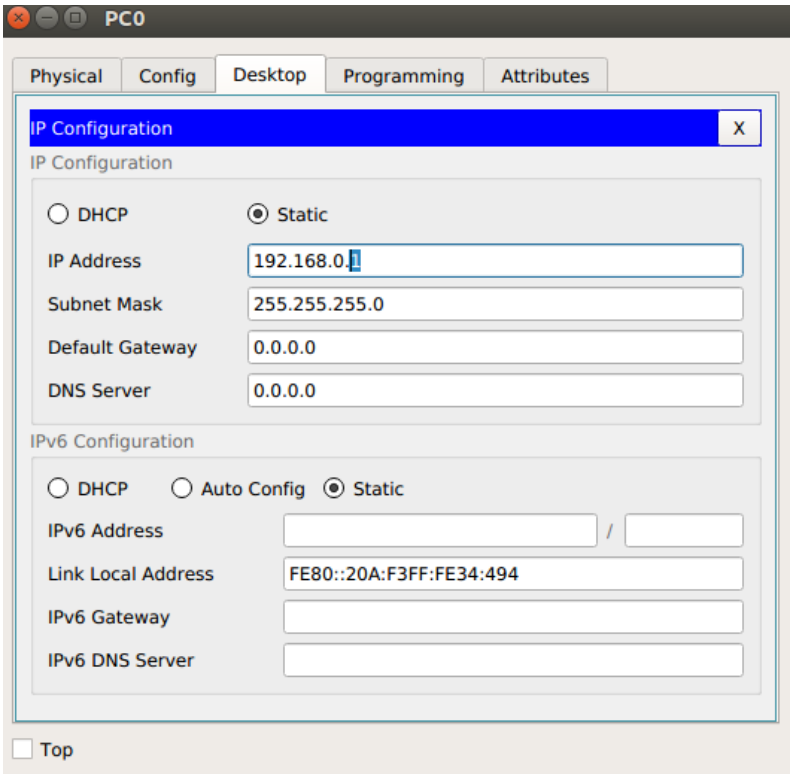


Рис.. Фрагмент внутреннего интерфейса PC-PT.

Далее, выбираем тип задания адреса «static», в поле IP Address указываем IP адрес. Например, 192.168.0.X, где X итерируем для каждого очередного оконечного устройства.

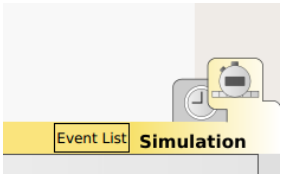
Маска подсети заполняется автоматически. Данные не требуют сохранения, закрываем окно настройки PC-PT.

Рис.. Вид вкладки IP Configuration PC-PT.

3. В соответствие с таблицей 2 по номеру варианта определяем с какого и на какое оконечное устройства будем посылать icmp-эхо пакет.

Для того, чтобы отправить icmp запрос нужно выполнить следующие действия:

В правом нижнем углу интерфейса переключить режим на Simulation mode



(Shift+S).

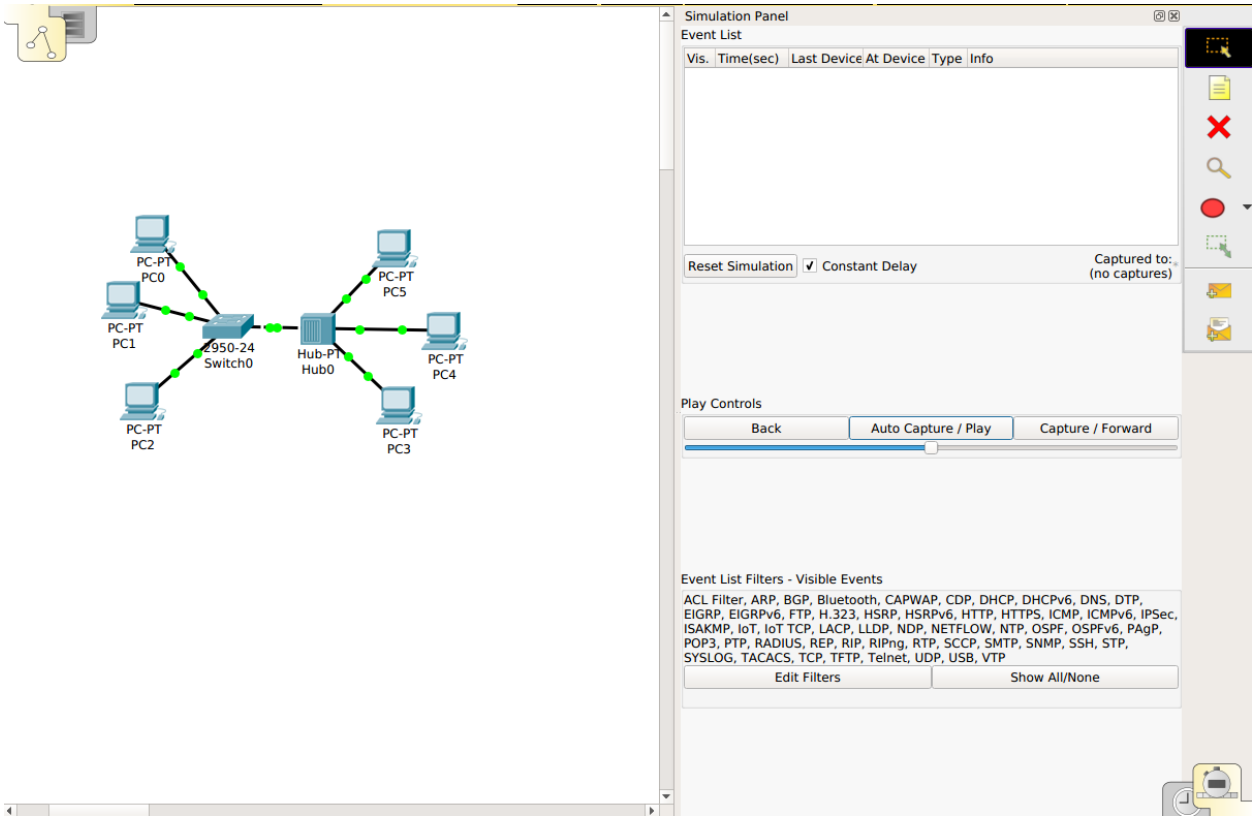


Рис.. Simulation Panel.

Отправим простой пакет от устройства А к устройству Б. Выберите инструмент Add simple PDU, затем наведите курсор мыши на устройство А, кликните один раз, затем наведите курсор на устройство Б и кликните ещё раз.

После этого схема и Simulation Panel приобретают следующий вид:

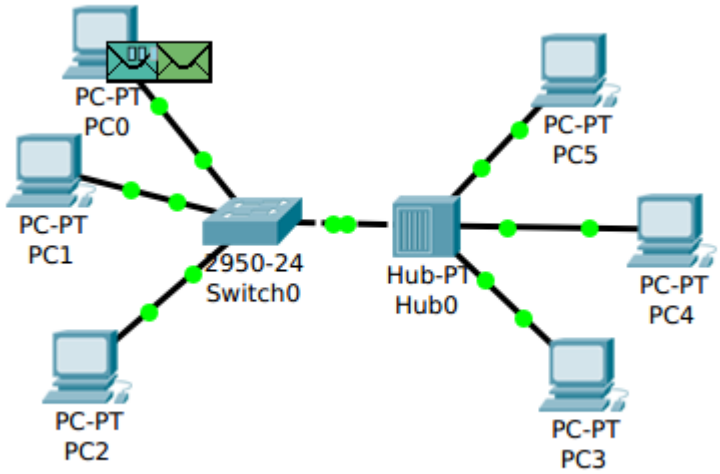


Рис.. Изображение пакетов ICMP и ARP.

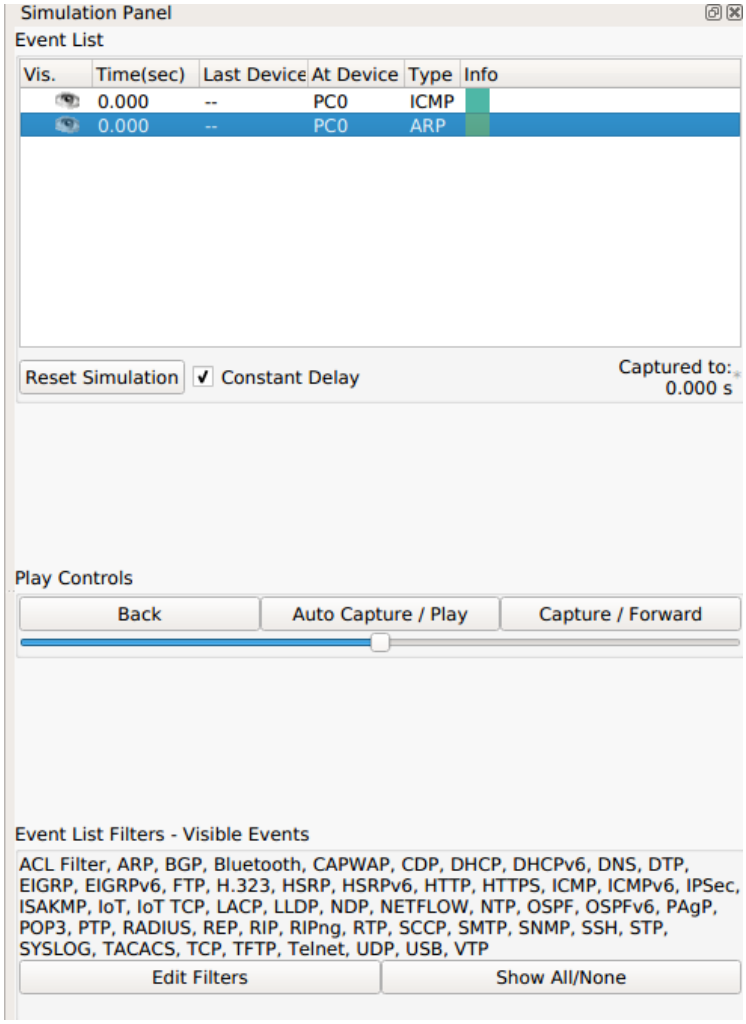


Рис.. ICMP и ARP на simulation panel.

Щёлкнув по строке с соответствующим пакетом, можно увидеть подробную информацию о нём, вплоть до его поуровневого состава.

4. Проследить путь пакета до места назначения. (занести в отчёт с описанием всего происходящего). Для этого в панели play controls нажимаем Capture/Forward, затем фиксируем результат и снова нажимаем Capture/Forward. Повторяем до тех пор, пока icmp-эхо не вернётся в устройство-отправитель.

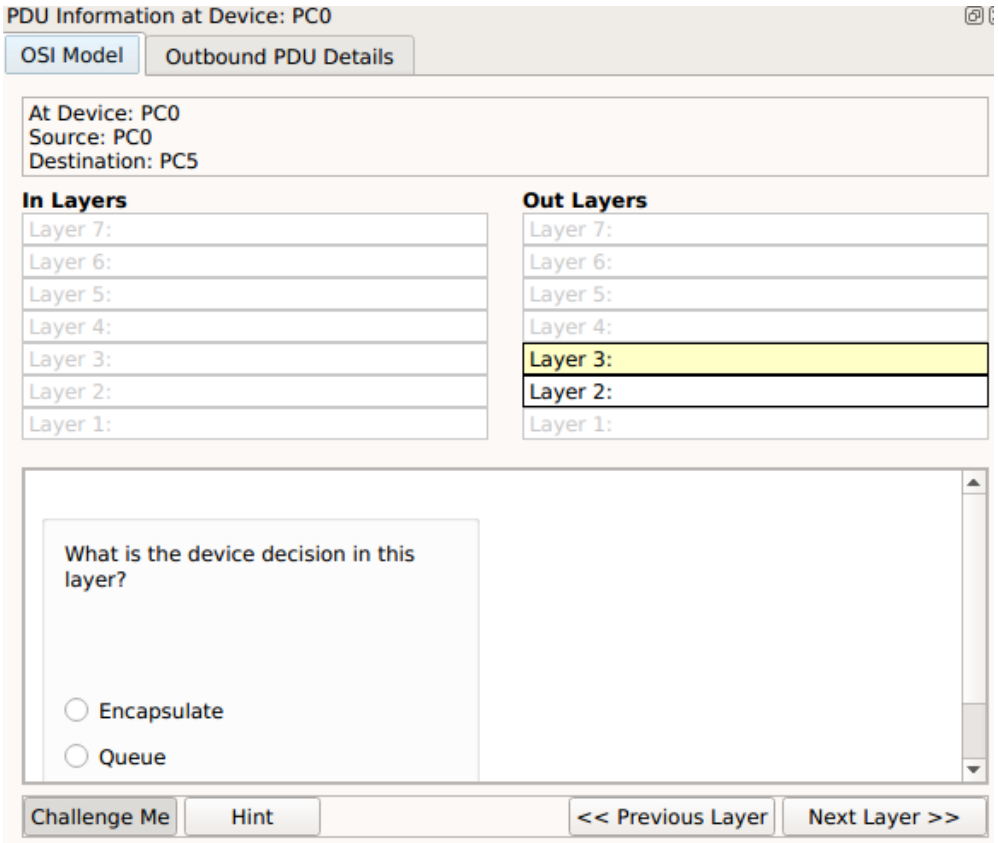


Рис.. Информация о пакете.

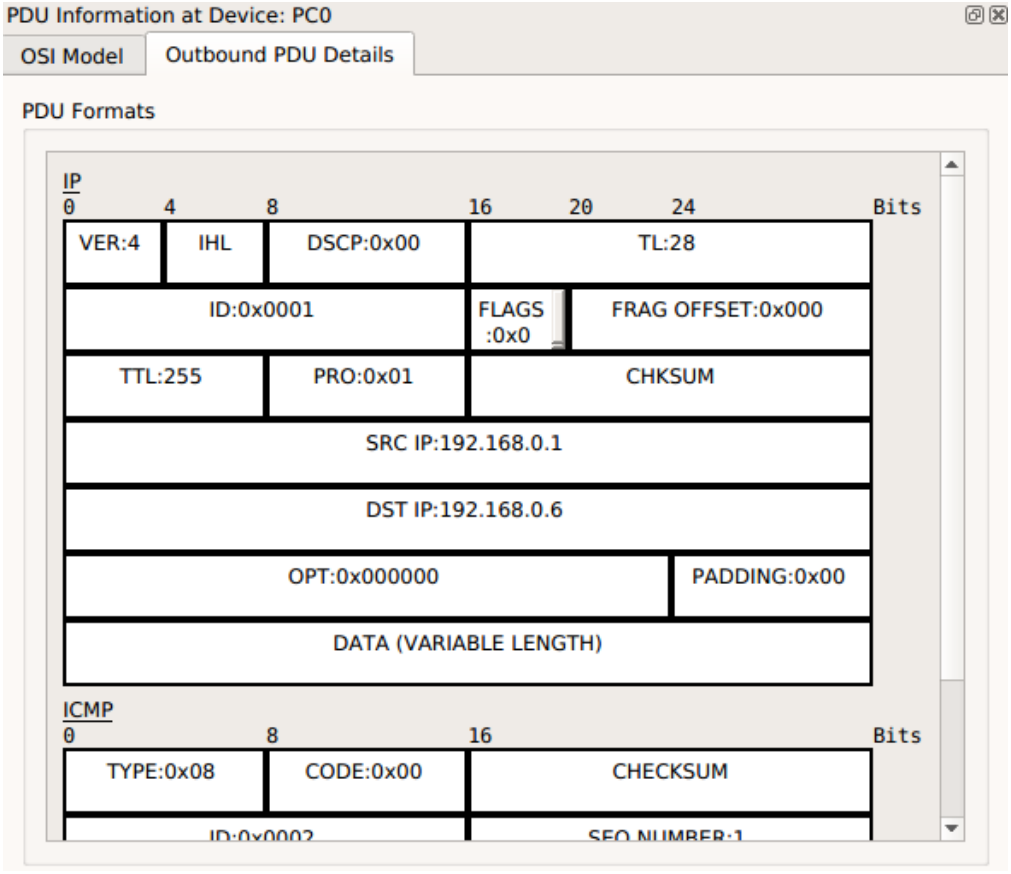


Рис.. Формат пакета.

Таблица 2. Вариант задания.

Вариант	Узел А (192.168.0.x)	Узел Б (192.168.0.x)
1	1	6
2	5	2
3	3	4
4	4	3
5	2	5
6	6	1

Контрольные вопросы.

1. Что такое сообщение/сегмент/кадр?
2. Что такое инкапсуляция? (по модели OSI)
3. Чем отличается концентратор от коммутатора?
4. Протокол ARP, ARP-таблица.
5. Коммутация пакетов и коммутация каналов, основные различия.
6. Как работает утилита ping по схеме данной лабораторной работы?

Лабораторная работа №3

«Маршрутизация»

Общие теоретические сведения.

Тема маршрутизации пакетов в компьютерных сетях очень обширна и многогранна, мы же рассмотрим небольшой пример, наглядно демонстрирующий работу статической маршрутизации.

Маршрутизация служит для приема пакета от одного устройства и передачи его по сети другому устройству через другие сети. Если в сети нет маршрутизаторов, то не поддерживается маршрутизация. Маршрутизаторы направляют (перенаправляют) трафик во все сети, составляющие объединенную сеть.

Для маршрутизации пакета маршрутизатор должен владеть следующей информацией:

- Адрес назначения
- Соседний маршрутизатор, от которого он может узнать об удаленных сетях
- Доступные пути ко всем удаленным сетям
- Наилучший путь к каждой удаленной сети
- Методы обслуживания и проверки информации о маршрутизации

Маршрутизатор узнает об удаленных сетях от соседних маршрутизаторов или от сетевого администратора. Затем маршрутизатор строит таблицу маршрутизации, которая описывает, как найти удаленные сети.

Если сеть подключена непосредственно к маршрутизатору, он уже знает, как направить пакет в эту сеть. Если же сеть не подключена напрямую, маршрутизатор должен узнать (изучить) пути доступа к удаленной сети с помощью статической маршрутизации (ввод администратором вручную местоположения всех сетей в таблицу маршрутизации) или с помощью динамической маршрутизации.

Динамическая маршрутизация — это процесс протокола маршрутизации, определяющий взаимодействие устройства с соседними маршрутизаторами. Маршрутизатор будет обновлять сведения о каждой изученной им сети. Если в сети произойдет изменение, протокол динамической маршрутизации автоматически информирует об изменении все маршрутизаторы. Если же используется статическая маршрутизация, обновить таблицы маршрутизации на всех устройствах придется системному администратору.

В стеке TCP/IP маршрутизаторы и конечные узлы принимают решения о том, кому передавать пакет для его успешной доставки узлу назначения, на основании так называемых таблиц маршрутизации (routing tables).
Таблица представляет собой типичный пример таблицы маршрутов, использующей IP-адреса сетей, для сети, представленной на рисунке.

Сетевой адрес	Маска сети	Адрес шлюза	Интерфейс	Метрика
129.13.0.0	255.255.0.0	-	129.13.0.1	подключен
198.21.17.0	255.255.255.0	-	198.21.17.6	подключен
213.34.12.0	255.255.255.0	198.21.17.1	198.21.17.6	1
56.0.0.0	255.0.0.0	198.21.17.7	198.21.17.6	1
116.0.0.0	255.0.0.0	198.21.17.7	198.21.17.6	2
116.0.0.0	255.0.0.0	198.21.17.1	198.21.17.6	2
0.0.0.0	0.0.0.0	198.21.17.7	198.21.17.6	-

Рис.. Таблица маршрутизации для Router 2.

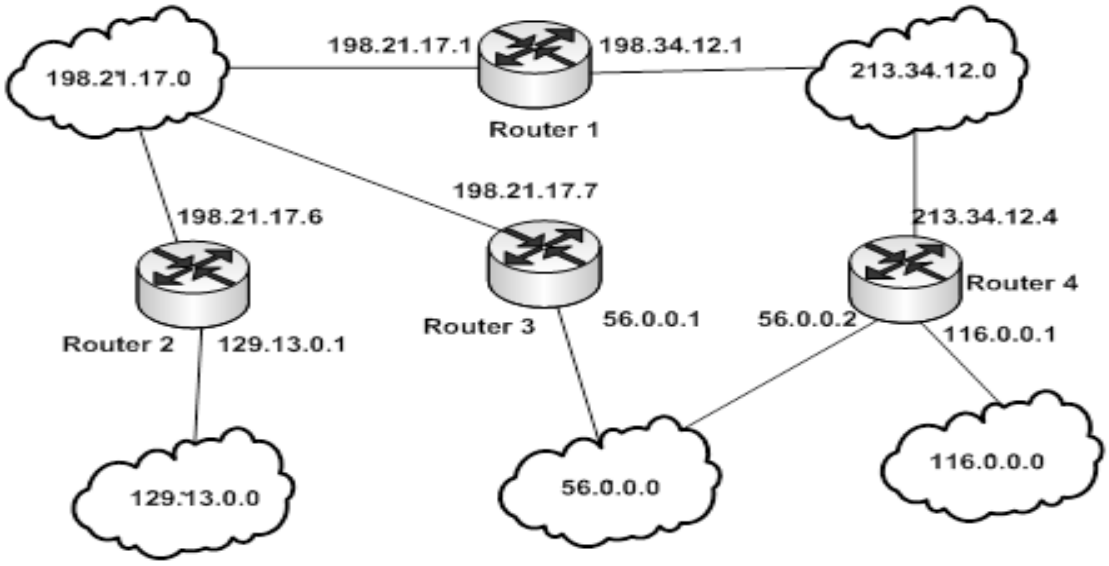


Рис.. Топология сети.

В таблице представлена таблица маршрутизации многомаршрутная, так как содержится два маршрута до сети 116.0.0.0. В случае построения одномаршрутной таблицы маршрутизации, необходимо указывать только один путь до сети 116.0.0.0 по наименьшему значению метрики.

Как нетрудно видеть, в таблице определено несколько маршрутов с разными параметрами. Читать каждую такую запись в таблице маршрутизации нужно следующим образом:

Чтобы доставить пакет в сеть с адресом из поля Сетевой адрес и маской из поля Маска сети, нужно с интерфейса с IP-адресом из поля Интерфейс послать пакет по IP-адресу из поля Адрес шлюза, а «стоимость» такой доставки будет равна числу из поля Метрика.

В этой таблице в столбце "Адрес сети назначения" указываются адреса всех сетей, которым данный маршрутизатор может передавать пакеты. В стеке TCP/IP принят так называемый одношаговый подход к оптимизации маршрута продвижения пакета (next-hop routing) – каждый маршрутизатор и конечный узел принимает участие в выборе только одного шага передачи пакета. Поэтому в каждой строке таблицы маршрутизации указывается не весь маршрут в виде последовательности IP-адресов маршрутизаторов, через которые должен пройти пакет, а только один IP-адрес - адрес следующего маршрутизатора, которому нужно передать пакет. Вместе с пакетом следующему маршрутизатору передается ответственность за выбор следующего шага маршрутизации. Одношаговый подход к маршрутизации означает распределенное решение задачи выбора маршрута. Это снимает ограничение на максимальное количество транзитных маршрутизаторов на пути пакета.

Для отправки пакета следующему маршрутизатору требуется знание его локального адреса, но в стеке TCP/IP в таблицах маршрутизации принято использование только IP-адресов для сохранения их универсального формата, не зависящего от типа сетей, входящих в интерсеть. Для нахождения локаль-

ного адреса по известному IP-адресу необходимо воспользоваться протоколом ARP.

Одношаговая маршрутизация обладает еще одним преимуществом - она позволяет сократить объем таблиц маршрутизации в конечных узлах и маршрутизаторах за счет использования в качестве номера сети назначения так называемого маршрута по умолчанию – default (0.0.0.0), который обычно занимает в таблице маршрутизации последнюю строку. Если в таблице маршрутизации есть такая запись, то все пакеты с номерами сетей, которые отсутствуют в таблице маршрутизации, передаются маршрутизатору, указанному в строке default. Поэтому маршрутизаторы часто хранят в своих таблицах ограниченную информацию о сетях интерсети, пересылая пакеты для остальных сетей в порт и маршрутизатор, используемые по умолчанию. Подразумевается, что маршрутизатор, используемый по умолчанию, передаст пакет на магистральную сеть, а маршрутизаторы, подключенные к магистрали, имеют полную информацию о составе интерсети.

Кроме маршрута default, в таблице маршрутизации могут встретиться два типа специальных записей - запись о специфичном для узла маршруте и запись об адресах сетей, непосредственно подключенных к портам маршрутизатора.

Задание на лабораторную работу.

1. Собрать схему, изображённую на рисунке:

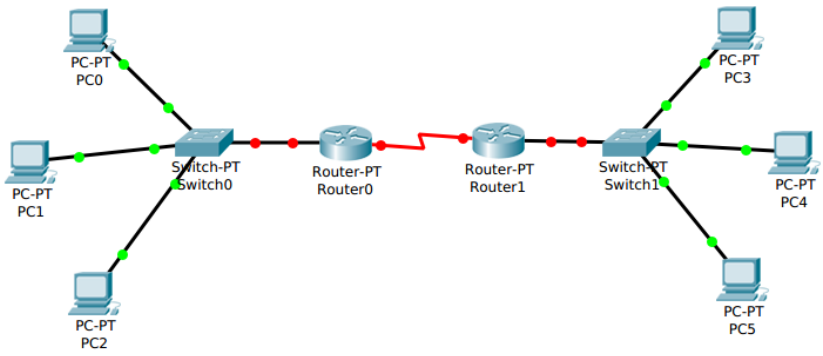


Рис.. Топология сети.

2. Назначить на интерфейсы IP адреса из соответствующих подсетей.

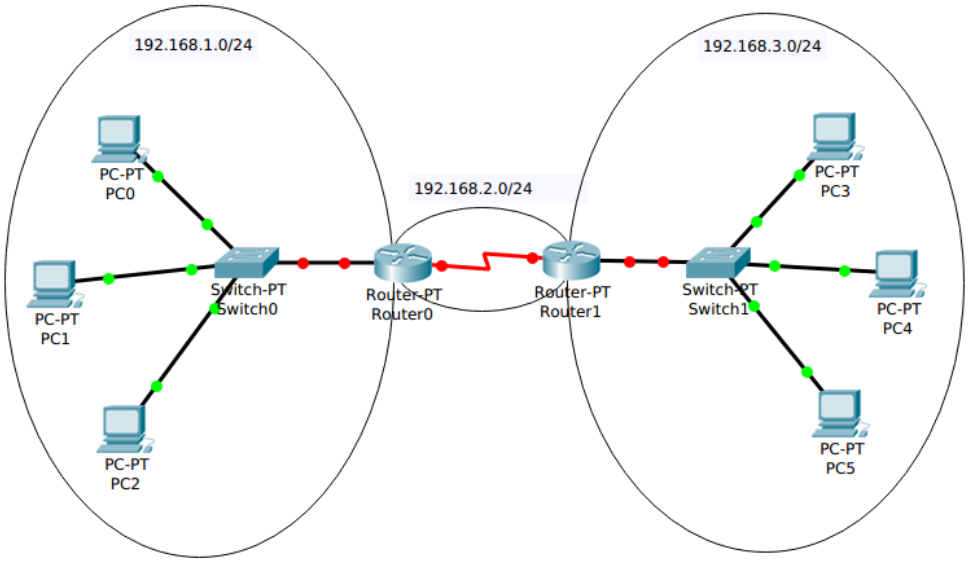


Рис.. Адреса подсетей.

3. Добавить записи о статических маршрутах для роутеров. Для этого щёлкните по иконке роутера Router0, откроется окно настройки Router0, во вкладке Config, слева, в категории ROUTING выбираем Static.

Указываем Network, Mask и Next Hop как показано на рисунке, применяем запись нажатием по кнопке Add. В консоли появилась соответствующая команда, а в таблице маршрутизации — необходимая запись. По аналогии, прописываем так же статический маршрут до соседней подсети на другом роутере.

Так же не забудьте включить интерфейсы роутеров с помощью команды «no shutdown» или вывтавив Port status в положение ON, как это показано на рисунке.

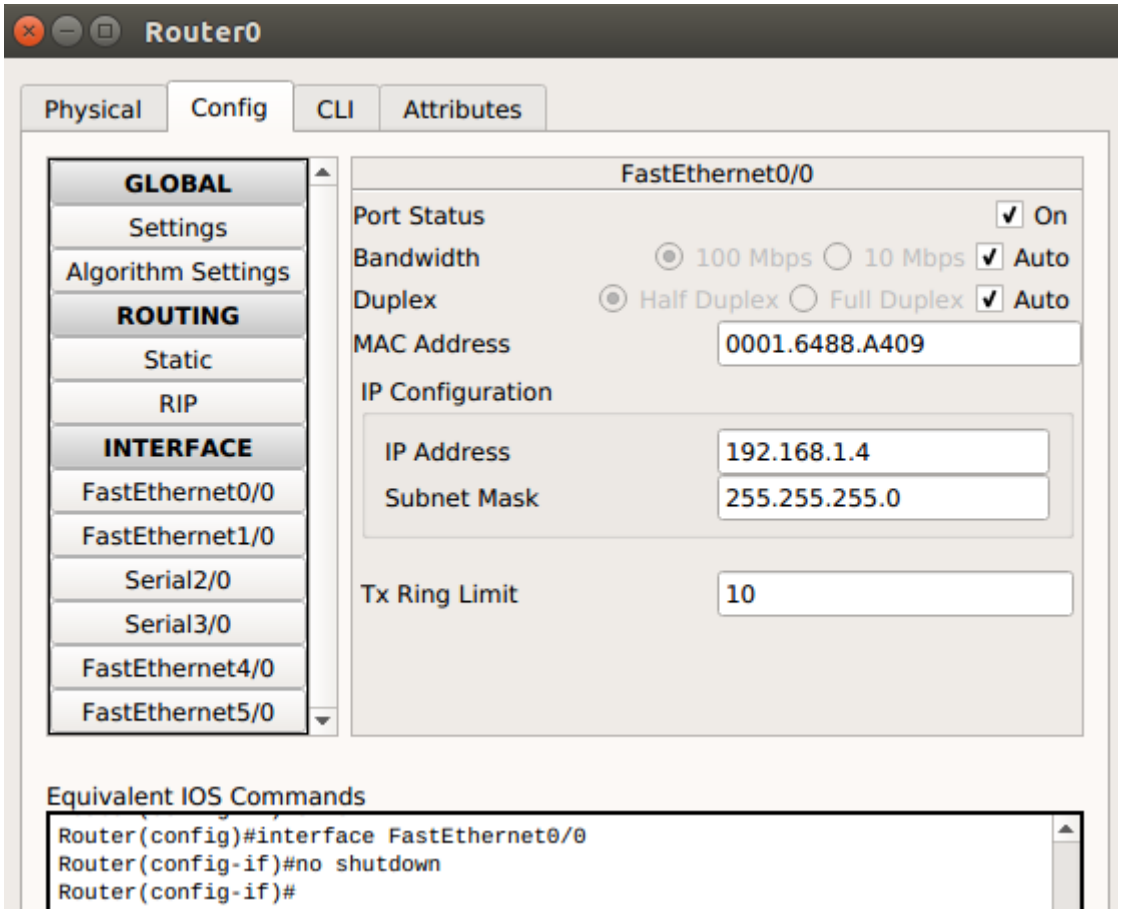


Рис.. Включение интерфейса Fa0/0.

В итоге вы получите работоспособную схему, в которой для каждой подсети прописан статический маршрут до другой подсети.

4. Аналогично заданию лабораторной работы №3, выбрав соответствующий вариант из таблицы 2, пропустите simple PDU через полученную сеть. Зафиксируйте маршрут с комментариями в отчёте. Сделайте выводы.

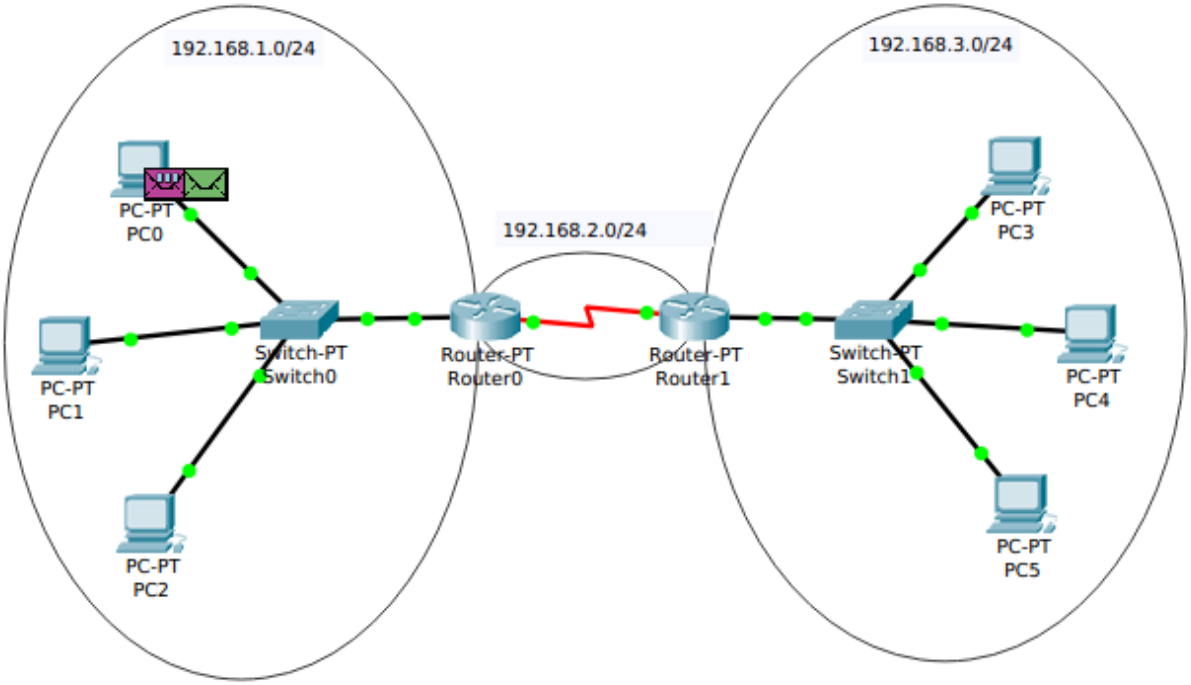


Рис.. ICMP и ARP пакеты в сети со статическими маршрутами.

Контрольные вопросы:

1. Что такое маска подсети, что она определяет?
2. Что такое маршрутизация?
3. В чём заключаются основные различия между статической и динамической маршрутизацией?

Лабораторная работа №4

«Виртуальные локальные сети»

Основные теоретические сведения.

VLAN (Virtual Local Area Network) — группа устройств, имеющих 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'ах, 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.

В современных сетях VLAN — главный механизм для создания логической топологии сети, не зависящей от её физической топологии. VLAN'ы используются для сокращения широковещательного трафика в сети. Имеют большое значение с точки зрения безопасности.

Компьютер при отправке трафика в сеть даже не догадывается,в каком VLAN'е он размещён. Об этом думает коммутатор. Коммутатор знает, что компьютер, который подключен к определённому порту,находится в соответствующем VLAN'е. Трафик, приходящий на порт определённого VLAN'а, ничем особенным не отличается от трафика другого VLAN'а. Другими словами, никакой информации о принадлежности трафика определённому VLAN'у в нём нет.

Однако, если через порт может прийти трафик разных VLAN'ов, коммутатор должен его как-то различать. Для этого каждый кадр (frame) трафика должен быть помечен каким-то особым образом. Пометка должна говорить о том, какому VLAN'у трафик принадлежит.

Наиболее распространённый сейчас способ ставить такую пометку описан в открытом стандарте IEEE 802.1Q. Существуют проприетарные протоколы, решающие похожие задачи, например, протокол ISL от Cisco Systems, но их популярность значительно ниже (и снижается).

Порты коммутатора, поддерживающие VLAN'ы, (с некоторыми допущениями) можно разделить на два множества:

1. Тегированные порты (или транковые порты, trunk-порты в терминологии Cisco).
2. Нетегированные порты (или порты доступа, access-порты в терминологии Cisco);

Тегированные порты нужны для того, чтобы через один порт была возможность передавать данные принадлежащие к различным VLAN и, соответственно, получать трафик нескольких VLAN на один порт. Информация о принадлежности трафика к конкретному VLAN, как было сказано выше, указывается в специальном теге. Без тега коммутатор не сможет различать трафик различных VLAN.

Если порт нетегированный и принадлежит к какому-либо VLAN, то трафик для этого VLAN передается без тега. На Cisco нетегированный порт (access-порт) может быть только в одном VLAN, на некоторых других свитчах (например, ZyXEL, D-Link и Planet) реализация иная.

Если порт тегирован для нескольких VLAN, то в этом случае весь нетегированный трафик будет приниматься специальным родным VLAN (native VLAN). С этим параметром (native, PVID, port VID) возникает много путаницы. Например, свитчи Planet для правильной работы нетегированного порта требуют поместить порт в VLAN, задать режим порта untagged (нетегированный), и прописать номер этого VLAN в PVID этого порта. На коммутаторах HP ProCurve тегированный порт начинает работать как тегированный только если поставить его PVID в "None".

Если порт принадлежит только одному VLAN как нетегированный, то тегированный трафик, приходящий через такой порт, должен удаляться. На деле это поведение обычно настраивается.

Проще всего это понять, если "забыть" всю внутреннюю структуру коммутатора и отталкиваться только от портов. Допустим, есть VLAN с номером

111, есть два порта которые принадлежат к VLAN 111. Они общаются только между собой, с untagged/access-порта выходит нетегированный трафик, с tagged/trunk-порта выходит трафик тегированный в VLAN 111. Все необходимые преобразования прозрачно внутри себя делает коммутатор.

Обычно, по умолчанию все порты коммутатора считаются нетегированными членами VLAN 1. В процессе настройки или работы коммутатора они могут быть перемещены в другие VLAN.

Существуют два подхода к назначению порта в определённый VLAN:

1. Статическое назначение — когда принадлежность порта VLAN'у задаётся администратором в процессе настройки;
2. Динамическое назначение — когда принадлежность порта VLAN'у определяется в ходе работы коммутатора с помощью процедур, описанных в специальных стандартах, таких, например, как 802.1X. При использовании 802.1X для того чтобы получить доступ к порту коммутатора, пользователь проходит аутентификацию на RADIUS-сервере. По результатам аутентификации порт коммутатора размещается в том или ином VLANe (подробнее: 802.1X и RADIUS).

Настройка VLAN в коммутаторах CISCO.

Терминология Cisco:

- access port — порт принадлежащий одному VLAN'у и передающий нетегированный трафик
- trunk port — порт передающий тегированный трафик одного или нескольких VLAN'ов

Коммутаторы Cisco ранее поддерживали два протокола 802.1Q и ISL. ISL — проприетарный протокол использующийся в оборудовании Cisco. ISL полностью инкапсулирует фрейм для передачи информации о принадлежности к VLAN'у.

В современных моделях коммутаторов Cisco ISL не поддерживается.

Создание VLAN'a и задание имени:

```
sw1(config)# vlan 2
sw1(config-vlan)# name test
```

Настройка access портов

Назначение портов 1 и 2 коммутатора в VLAN:

```
sw1(config)# interface range fa0/1 - 2
sw1(config-if)# switchport mode access
sw1(config-if)# switchport access vlan 2
```

Назначение диапазона портов с fa0/4 до fa0/5 в vlan 10:

```
sw1(config)# interface range fa0/4 - 5
sw1(config-if-range)# switchport mode access
sw1(config-if-range)# switchport access vlan 10
```

Просмотр информации о VLAN'ах:

```
sw1# show vlan brief
VLAN Name                       Status    Ports

---- -------------------------------- --------- -------------------------------

1    default                    active    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

2    test                       active    Fa0/1, Fa0/2

10   VLAN0010                   active    Fa0/4, Fa0/5

15   VLAN0015                   active    Fa0/3
```

Задание на лабораторную работу.

Сконфигурировать работоспособную сеть по схеме (Рис.).

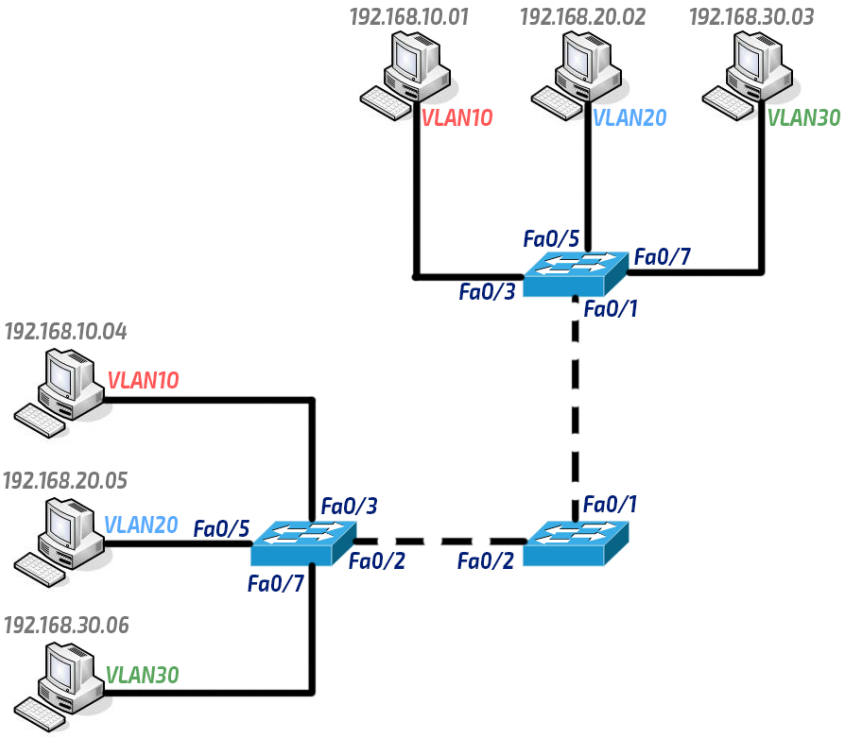


Рис.1. Топология сети.

Проверка корректности работы сети.

Согласно варианту, используя утилиту ping проверить:

1) Для хоста *.*.*.01 возможна передача данных только хосту *.*.*.04
2) Для хоста *.*.*.02 возможна передача данных только хосту *.*.*.05
3) Для хоста *.*.*.03 возможна передача данных только хосту *.*.*.06
4) Для хоста *.*.*.04 возможна передача данных только хосту *.*.*.01
5) Для хоста *.*.*.05 возможна передача данных только хосту *.*.*.02
6) Для хоста *.*.*.06 возможна передача данных только хосту *.*.*.03

Справочная информация.

На коммутаторах порты необходимо назначить следующим образом:

Таблица 3. Схема настройки коммутаторов.

Порты	**Назначение**	**Сеть**
Fa0/1 - Fa02	802.1q Trunks (native VLAN1)	
Fa0/3	VLAN10 – red	192.168.10.0/24

Fa0/5	VLAN20 – blue	192.168.20.0/24
Fa0/7	VLAN30 – green	192.168.30.0/24

Контрольные вопросы.

1. Что такое VLAN? Протокол 802.1q.
2. Trank/access порты.
3. Способы настройки VLAN на коммутаторах CISCO.
4. Максимальное значение VLAN ID? Почему?