Министерство науки и высшего образования Российской Федерации

Томский государственный университет
систем управления и радиоэлектроники

А.Е. Максимов,
С.П. Куксенко

ОСНОВЫ ПОСТРОЕНИЯ КОМПЬЮТЕРНЫХ СЕТЕЙ

Учебно-методическое пособие
по практическим занятиям и самостоятельной работе

Томск
2022

УДК 004.7
ББК 32.971.35
М17

Рецензент:
Заболоцкий А.М., профессор кафедры телевидения и управления,
доктор техн. наук, доцент

Максимов, Александр Евгеньевич
Куксенко, Сергей Петрович
М17 Максимов, А.Е. Основы построения компьютерных сетей: Учебно-методическое пособие по практическим занятиям и самостоятельной работе / А.Е. Максимов, С.П. Куксенко. – Томск: Томск. гос. ун-т систем упр. и радиоэлектроники, 2022. – 61 с.

Настоящее учебно-методическое пособие по практическим занятиям и самостоятельной работе составлено с учетом требований федерального государственного образовательного стандарта высшего образования (ФГОС ВО). В пособии представлены методические указания по практическим и самостоятельным работам, направленные на изучение основ построения компьютерных сетей. Пособие предназначено для студентов высших учебных заведений, обучающихся по направлениям подготовки 11.03.01 – «Радиотехника» и 11.03.02 – «Инфокоммуникационные технологии и системы связи».

Одобрено на заседании кафедры телевидения и управления, протокол № 5 от 10.04.2022.

УДК 004.7
ББК 32.971.35

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

В настоящее время трудно найти человека, который не использует компьютерные сети в повседневной жизни. Однако понимание принципов работы компьютерных сетей у большинства пользователей либо минимально, либо вообще отсутствует. Из-за стремительного развития сетевых технологий и телекоммуникационных систем для подготовки компетентного специалиста учебное заведение должно обеспечить его таким комплексом знаний и умений, который поможет ему продолжить дальнейшее совершенствование навыков совместно с успешным трудоустройством после окончания вуза. Применение современных достижений информационных и коммуникационных технологий в процессе обучения открывает студентам доступ к новым формам обучения, таким как виртуальные лабораторные работы, тем самым повышая его эффективность. При этом в связи со спецификой предметной области, финансовыми ограничениями, а также необходимостью создания различных структурных схем при освоении материала целесообразно использование программных симуляторов и эмуляторов. Поэтому практические работы, приведенные в данном пособии, в подавляющем большинстве основаны на использовании симулятора сети Cisco Packet Tracer. Это программное обеспечение обладает дружественным интерфейсом, отличается легкостью освоения, а также широтой функциональных возможностей, что позволяет успешно изучать учебный материал и применять полученные навыки на практике. Одним из главных достоинств данного программного обеспечения является наличие режима «simulation», с помощью которого можно визуализировать перемещение данных по сети с возможностью изменения скорости анимации. Этот симулятор разрабатывается компанией Cisco, являющейся мировым лидером производства сетевого оборудования.

В пособии приведены указания по выполнению 11 работ, направленных на закрепление материала по трем темам: основные понятия, коммутация и маршрутизация. Для каждой работы в пособии приведены:

- краткая теоретическая справка;
- задание на практическую работу;
- вопросы для самопроверки;
- задание на самостоятельную работу.

В начале каждой работы указан уровень сетевой модели, к которому она относится. В качестве сетевой модели используется наиболее известная эталонная модель OSI, кратко ознакомимся с ее уровнями:

Прикладной
Представления
Сеансовый
Транспортный
Сетевой
Канальный
Физический

1. Физический уровень. На первом уровне модели OSI происходит кодирование и передача физических сигналов (битов) от источника к получателю. На этом уровне используются технологии «Ethernet» (стандарт IEEE 802.3) и Wi-Fi (стандарт IEEE 802.11). Сетевые устройства, которые относят к первому уровню это концентраторы и повторители.

2. Канальный уровень. На втором уровне происходит коммутация устройств внутри сегмента сети и передача кадров между ними. На этом уровне используется физическая адресация (MAC-адресация). Сетевые устройства, которые относят ко второму уровню это коммутаторы.

3. Сетевой уровень. На третьем уровне происходит маршрутизация сетевого трафика между сетями (передача сетевых пакетов из одной сети в другую). На этом уровне используется логическая адресация (IP-адресация). На третьем уровне работает такое сетевое устройство, как маршрутизатор.

4. Транспортный уровень. На этом уровне происходит доставка данных (сегментов или дейтаграмм) по сети. Основными протоколами этого уровня являются TCP и UDP.

5. Сеансовый уровень. Этот уровень отвечает за установление, поддержание и разрыв сеансов связи (сессий), позволяя приложениям взаимодействовать между собой длительное время.

6. Уровень представления. На шестом уровне происходит преобразование форматов сообщений, такое как кодирование или сжатие.

7. Прикладной уровень. На седьмом уровне происходит взаимодействие пользователя с сетью с использованием различных «прикладных» сетевых протоколов (например, HTTP, FTP, POP3).

При выполнении работ требуется ознакомиться с теоретическими сведениями (подразделы «Краткая теоретическая справка»), выполнить практические задания (подразделы «Задание на практическую работу»), ответить на контрольные вопросы (подразделы «Вопросы для самопроверки»), выполнить самостоятельные задания (подразделы «Задание на самостоятельную работу») и оформить общие отчеты по практическим и самостоятельным работам каждого радела. Оформление отчетов требуется выполнять в соответствии с ОС ТУСУР 01-2021 «Работы студенческие по направлениям подготовки и специальностям технического профиля».

1 ФИЗИЧЕСКАЯ СРЕДА ПЕРЕДАЧИ ДАННЫХ

1.1 Краткая теоретическая справка

Для соединения компьютеров и других сетевых устройств в компьютерную сеть (т.е. совокупность технических устройств и физической среды, обеспечивающих передачу сигналов от передатчика к приемнику) необходимы линии связи. В качестве линии связи могут выступать:

- электрические кабели на основе витых пар проводов (twisted pair);
- электрические коаксиальные кабели (coaxial cable);
- оптоволоконные кабели (fiber optic cable);
- беспроводные каналы передачи данных (сотовая связь, Wi-Fi, WiMax и пр.).

Данная практическая работа посвящена изучению особенностей использования в качестве линии связи витой пары. Передача данных по компьютерным сетям регулируется группой стандартов IEEE 802, а при передаче по витой паре – IEEE 802.3 (технология «Ethernet»). Классы и категории (CAT) витой пары описывает стандарт ISO/IEC 11801 (таблица 1.1).

Таблица 1.1 – Классы и категории витой пары

Класс	Категория	Ширина канала, МГц	Число пар проводников	Скорость передачи данных	Примечание
A	1	0,1	1	–	Устарел, использовался для модемных соединений
B	2	1	2	До 4 Мбит/с	Устарел
C	3	16	2 или 4	От 10 до 100 Мбит/с (на расстоянии не более 100 м)	Устарел, впервые добавлена поддержка стандарта IEEE 802.3
D	4	20	4	От 10 до 100 Мбит/с (на расстоянии не более 100 м)	–
	5	100	4	До 100 Мбит/с (на расстоянии не более 100 м)	–
	5E	100	4	До 100 Мбит/с (при исп. 2-х пар) и до 1 Гбит/с (при исп. 4-х пар) (на расстоянии не более 100 м)	–
E	6	250	4	До 10 Гбит/с (на расстоянии не более 55 м)	–
EA	6A	500	4	До 10 Гбит/с (на расстоянии не более 100 м)	–
F	7	600	4	До 10 Гбит/с	–
FA	7A	1000	4	До 40 Гбит/с (на расстоянии не более 50 м) и до 100 Гбит/с (на расстоянии не более 15 м)	–
I	8.1	2000	4	До 10 Гбит/с (на расстоянии не более 100 м)	Аналог CAT 6A
II	8.2	2000	4	До 40 Гбит/с (на расстоянии не более 50 м) и до 100 Гбит/с (на расстоянии не более 15 м)	Аналог CAT 7A

Цветовую маркировку проводников витой пары стандартизирует ассоциация телекоммуникационной промышленности США. Первоначально для построения компьютерных сетей с использованием витой пары рекомендовался стандарт TIA/EIA-568A. Позднее был выпушен обновленный стандарт TIA/EIA-568B, который сейчас чаще всего используется на практике. Стандартом предусматривается «прямой» порядок и «перекрёстный» порядок расположения проводников в коннекторах на противоположных концах витой пары (рисунок 1.1).

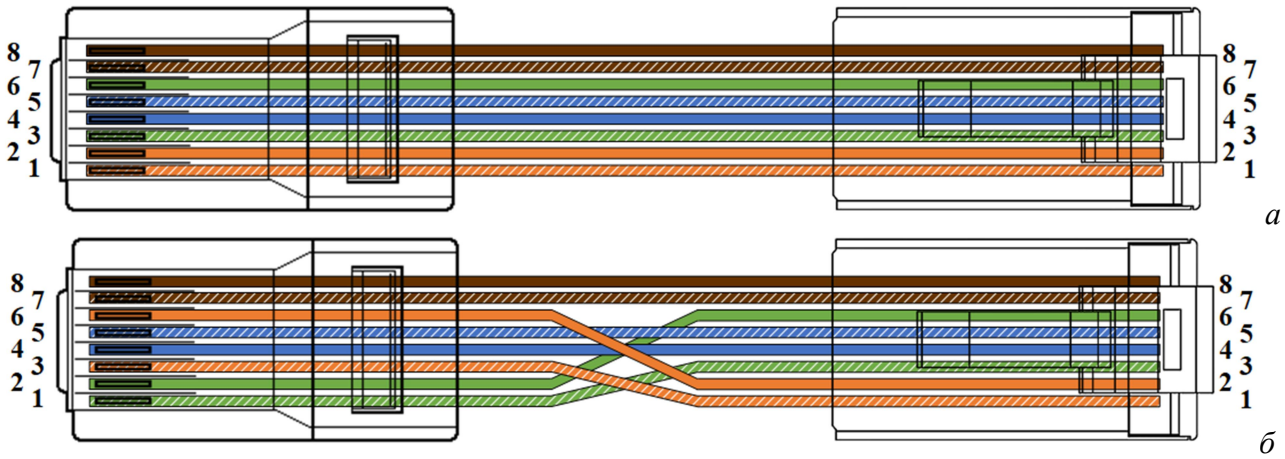


Рисунок 1.1 – «Прямой» порядок (*а*) и «перекрёстный» порядок (*б*) проводников витой пары по TIA/EIA-568B

Для защиты от электрических помех в кабелях используется экранирование. Экранирование применяется как к отдельным парам проводов, которые оборачиваются в алюминиевую фольгу (металлизированную алюминием полиэтиленовую ленту), так и к кабелю в целом в виде общего экрана из фольги и/или оплётки из медной проволоки.

Согласно международному стандарту ISO/IEC 11801, приложение E, для обозначения конструкции экранированного кабеля используется комбинация из трех букв: U – неэкранированный, S – металлическая оплётка (используется только для общего экрана кабеля), F – металлизированная лента (алюминиевая фольга). Из этих букв формируется аббревиатура вида xx/xTP, обозначающая тип общего экрана кабеля и тип экрана для отдельных витых пар (twisted pair).

Распространены следующие типы конструкции экрана:

- неэкранированный кабель (U/UTP);
- экран пар (U/FTP), защищающий от внешних помех и от перекрёстных помех между парами;
- общий экран кабеля (F/UTP, S/UTP, SF/UTP) из фольги, оплётки, или фольги с оплёткой, защищающий от внешних электромагнитных помех;
- индивидуальные экраны пар из фольги и общий экран кабеля из фольги, оплётки, или фольги с оплёткой (F/FTP, S/FTP, SF/FTP), защищающие от внешних помех и от перекрёстных помех между витыми парами.

На рисунке 1.2 представлены примеры различных конструкций экрана.

Экранированные кабели CAT 6A чаще всего используют конструкцию F/UTP, тогда как экранированные кабели CAT 7/7a используют конструкцию S/FTP. Для кабеля CAT 8.1 предусмотрено экранирование минимум U/FTP или F/UTP, а для 8.2 – минимум F/FTP или S/FTP.

Проводники витой пары могут быть цельные одножильные (solid) или многопроволочные (stranded) и быть изготовлены из меди (CU, наиболее дорогой вариант) или омедненного алюминия (CCA). Изоляция проводников обычно изготавливается из полиэтилена высокой плотности (HDPE), а оболочка кабеля – из полиэтилена (PE),

полипропилена (PP) или поливинилхлорида (PVC). В последнее время стали популярны кабели с маркировкой оболочки LSZH (это малодымный безгалогенный компаунд, который замедляет горение, выделяет мало дыма и не образует токсичных и корродирующих газов при горении). Кабели для эксплуатации вне помещений (outdoor) часто имеют подвесной трос (маркируется буквой C) для натяжения между зданиями.

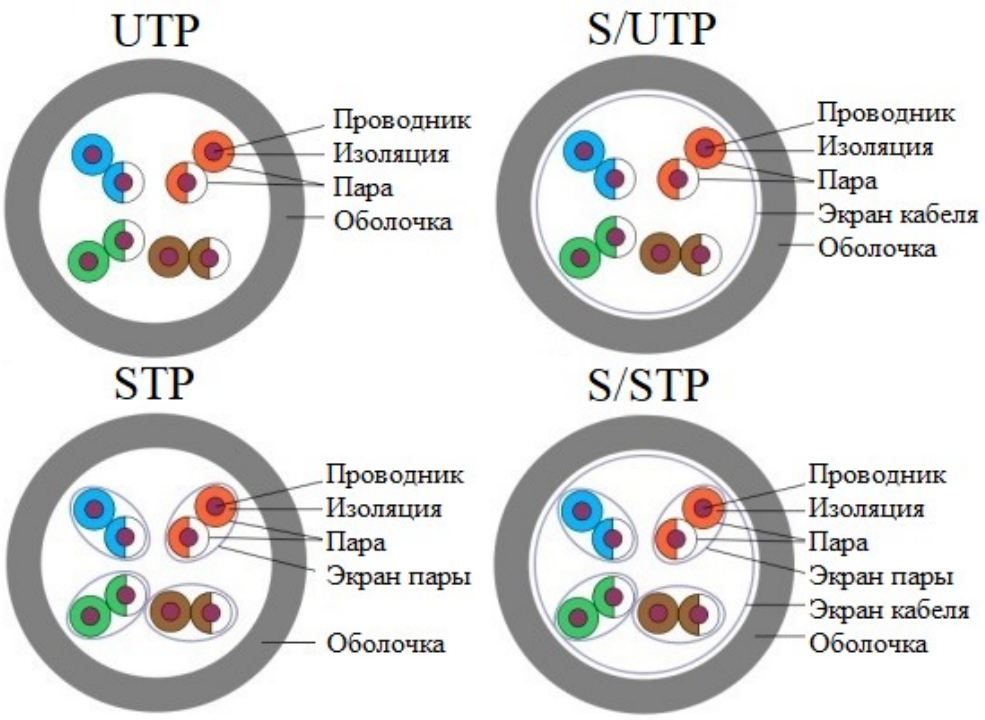


Рисунок 1.2 – Различные типы конструкций экрана

Сечение каждой жилы витой пары маркируется в соответствии со стандартом AWG (American Wire Gauge). Наиболее распространенными являются проводники стандарта 26 AWG (сечение 0,13 мм²), 24 AWG (0,2–0,28 мм²) и 22 AWG (0,33–0,44 мм²).

1.2 Задание на практическую работу

На практическом занятии необходимо изготовить патч-корд (коммутационный шнур, который представляет собой фрагмент кабеля (витой пары) длиной, как правило, до 5 метров, и имеющий с обеих сторон соединители (разъемы, коннекторы)).

Материалы и инструкцию по изготовлению выдает преподаватель.

1.3 Вопросы для самопроверки

1. Какова цветовая маркировка проводников согласно стандарту TIA/EIA-568B?
2. На какое максимальное расстояние может быть передан сигнал по кабелю UTP CAT 5E?
3. Что обозначает TP в аббревиатуре xx/xTP?

1.4 Задание на самостоятельную работу

Необходимо расшифровать маркировку кабеля согласно выданному преподавателем варианту индивидуального задания (таблица 1.2). Затем необходимо составить максимально полную маркировку по изображению отрезка кабеля (рисунок 1.3).

Таблица 1.2 – Варианты индивидуальных заданий

Вариант	Маркировка кабеля
1	U/UTP SOLID CAT 5E CCA LSZH
2	F/UTP CAT 5E 24AWG CU PVC
3	CAT 5E UTP 4 PAIR CCA VERIFIED TO TIA/EIA-568-B
4	U/UTP SOLID 4 PAIR PE OUTDOOR
5	FTP CAT 5E 24AWG CU SOLID
6	F/UTP CAT 6A CCA LSZH VERIFIED TO TIA/EIA-568-B
7	S/FTP CAT 7 4 PAIR CU PP
8	U/UTP CCA 2 PAIR CAT 5E 24AWG
9	F/UTP CAT 5E SOLID PE VERIFIED TO TIA/EIA-568-B
10	4 PAIR U/UTP 23AWG CAT 6 LSZH

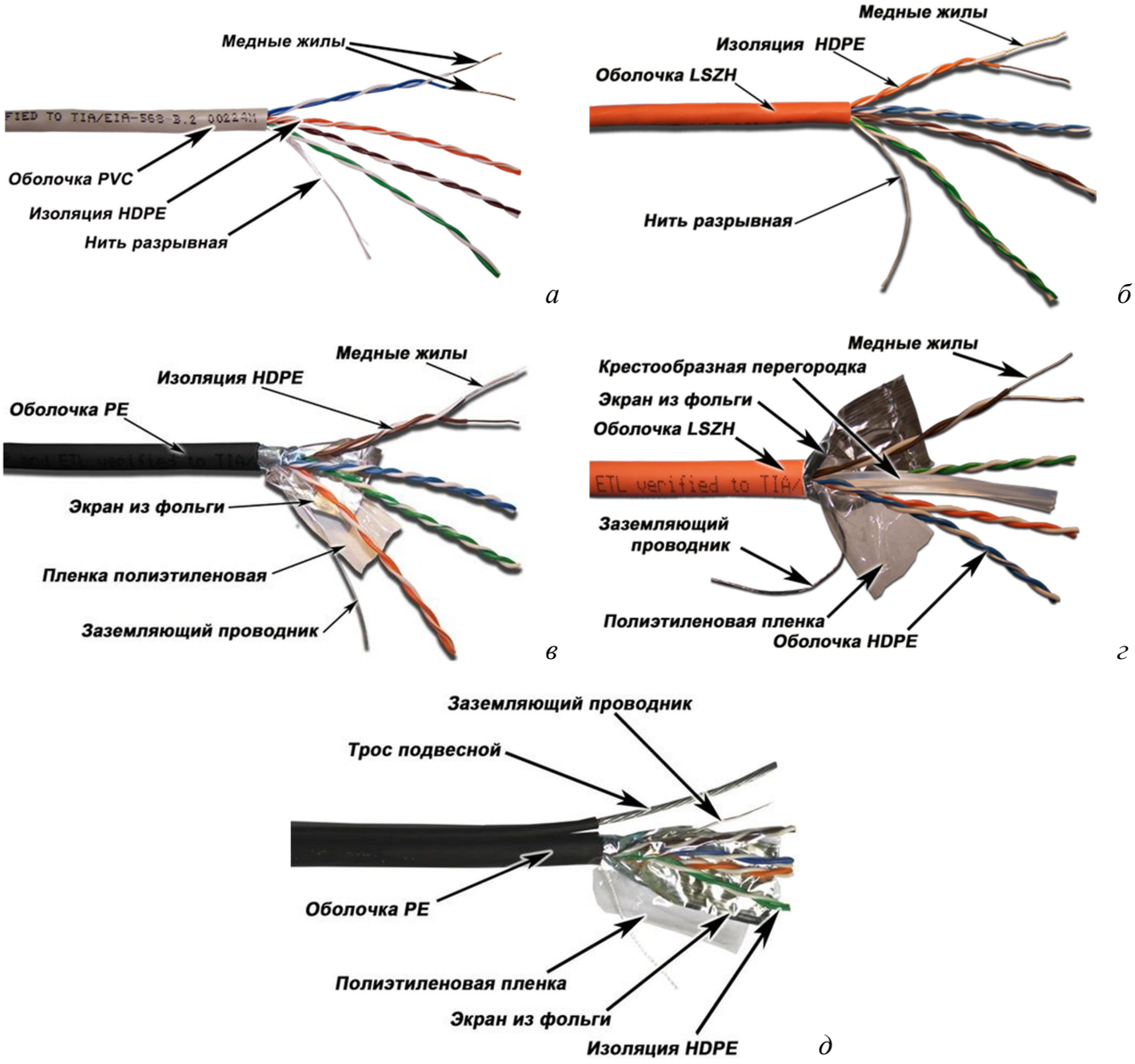


Рисунок 1.3 – Варианты индивидуальных заданий: 1 (*а*); 2 (*б*); 3 (*в*); 4 (*г*); 5 (*д*)

2 ЗНАКОМСТВО С CISCO PACKET TRACER

2.1 Краткая теоретическая справка

Cisco Packet Tracer (CPT) – это мощный сетевой программный симулятор, позволяющий создавать сети с практически неограниченным количеством устройств и устранять неполадки без необходимости покупать настоящие маршрутизаторы или коммутаторы Cisco. CPT позволяет эмулировать различные сетевые протоколы и технологии всех уровней модели OSI (рисунок 2.1), что делает его прекрасным инструментом для изучения принципов работы компьютерных сетей и сетевых устройств, в том числе и других производителей. В данной работе необходимо познакомиться с функциональными возможностями сетевого симулятора CPT.

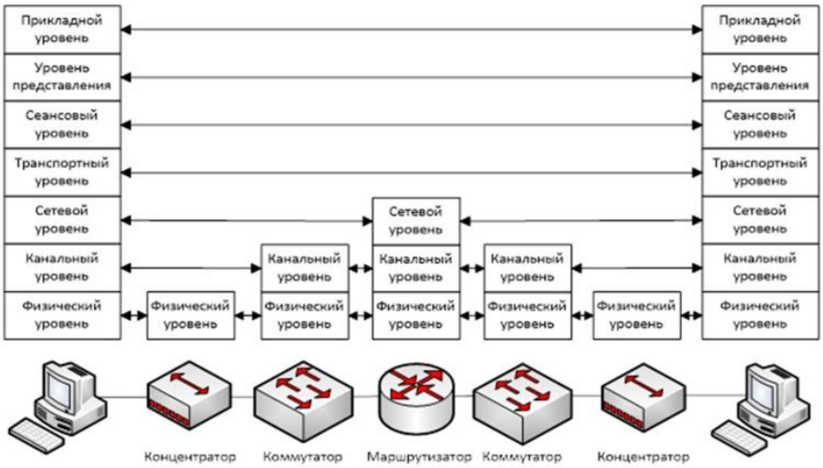


Рисунок 2.1 – Взаимодействие устройств согласно модели OSI

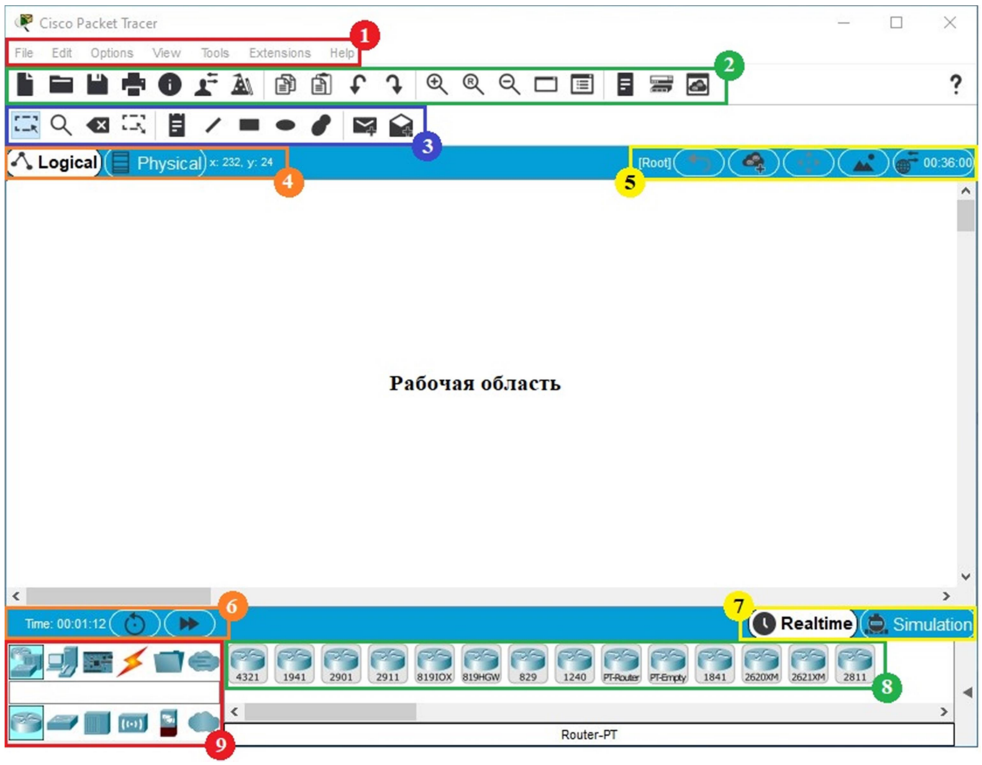


Рисунок 2.2 – Основное окно сетевого симулятора CPT

Запустив программу, пользователь видит главное окно (рисунок 2.2). На рисунке цифрами показаны блоки, описанные далее.

Блок 1: главное меню. Блок содержит стандартные пункты меню Windows приложения:

- Файл (File).
- Правка (Edit).
- Настройки (Options).
- Вид (View).
- Инструменты (Tools).
- Расширения (Extensions).
- Помощь (Help).

Блок 2: панель инструментов 1. Панель содержит ярлыки некоторых инструментов главного меню (сохранение, отмена и повтор последнего действия, масштабирование и пр.).

Блок 3: панель инструментов 2. Панель содержит часто используемые инструменты, такие как: средства выделения, удаления, перемещения и масштабирования объектов. Подробные описания основных инструментов приведены в таблице 2.1.

Таблица 2.1 – Описания основных инструментов блока 3

Обозначение	Описание
	Инструмент **Select** позволяет выделить один или несколько объектов моделируемой компьютерной сети (в «логической» или «физической» топологии).
	Инструмент **Inspect** позволяет просматривать таблицы состояния (таблица маршрутизации и т.д.) объектов моделируемой компьютерной сети.
	Инструмент **Delete** включает режим удаления объектов моделируемой компьютерной сети.
	Инструмент **Resize** используется для изменения размеров графических объектов моделируемой компьютерной сети, размещенных на рабочей области.
	Инструмент **Place Note** позволяет добавить в текущую моделируемую компьютерную сеть текстовую надпись.
	Инструменты **Draw Line** / **Rectangle** / **Ellipse** / **Freeform** позволяют добавлять на рабочую область простые графические объекты: линии, прямоугольники, эллипсы и фигуры произвольной формы соответственно.

Блок 4: переключатели «логической» и «физической» организации рабочей области. В режиме «логической» сети на рабочей области располагаются сетевые устройства (маршрутизаторы, коммутаторы, компьютеры, серверы, и т.д.) и задаются связи между ними, а в режиме «физической» сети задается расположение сетевых устройств и каналов связи в помещениях.

Блок 5: панель управления рабочей областью. Панель содержит кнопки управления отображением рабочей области. Так, можно установить фоновое изображение, а в режиме «физическая» сеть добавить новое здание или помещение внутри здания.

Блок 6: панель управления временем. По умолчанию программа работает в режиме реального времени. Однако чтобы не ожидать загрузки всех устройств этот процесс можно ускорить с помощью кнопки «>>». Также можно перезагрузить все устройства и начать симуляцию заново.

Блок 7: переключатель режима реального времени и режима симуляции. В режиме симуляции («Simulation») пользователь может посмотреть, как информация передается между сетевыми устройствами. В режиме реального времени («Realtime») отображается лишь состояние сетевых устройств.

Блок 9: панель выбора группы сетевых устройств, линий связи и пр. Панель позволяет выбрать тип сетевых устройств и линий связи.

Блок 8: панель выбора сетевых устройств. Панель содержит сетевые устройства и линий связи. Содержимое панели зависит от выбранного типа устройств в блоке 9.

2.2 Задание на практическую работу

После ознакомления с интерфейсом CPT необходимо добавить несколько сетевых устройств на рабочую область (перетянув их мышкой из блока 8 или щелчком мышки указав место в рабочей области, куда следует их поместить). Например, результат добавления на рабочую область двух компьютеров и коммутатора приведен на рисунке 2.3.

Конфигурация сетевого устройства производится по двойному щелчку на нем. Так, в открывшемся окне (рисунок 2.4) пользователь может включить/отключить питание устройства (соответствующим выключателем на его изображении в области «Physical Device View»), изменить аппаратурную конфигурацию добавив или удалив модули (область MODULES), изменить изображение для отображения этого устройства в режиме «логической» и «физической» сети.

Выбрав вкладку «Config», пользователь может задать конфигурационные параметры устройства, настроить сетевой интерфейс, определить имя устройства и т.п. На вкладке «CLI» (доступна для коммутаторов и маршрутизаторов) предоставляется доступ к командному интерфейсу устройства (рисунок 2.5).

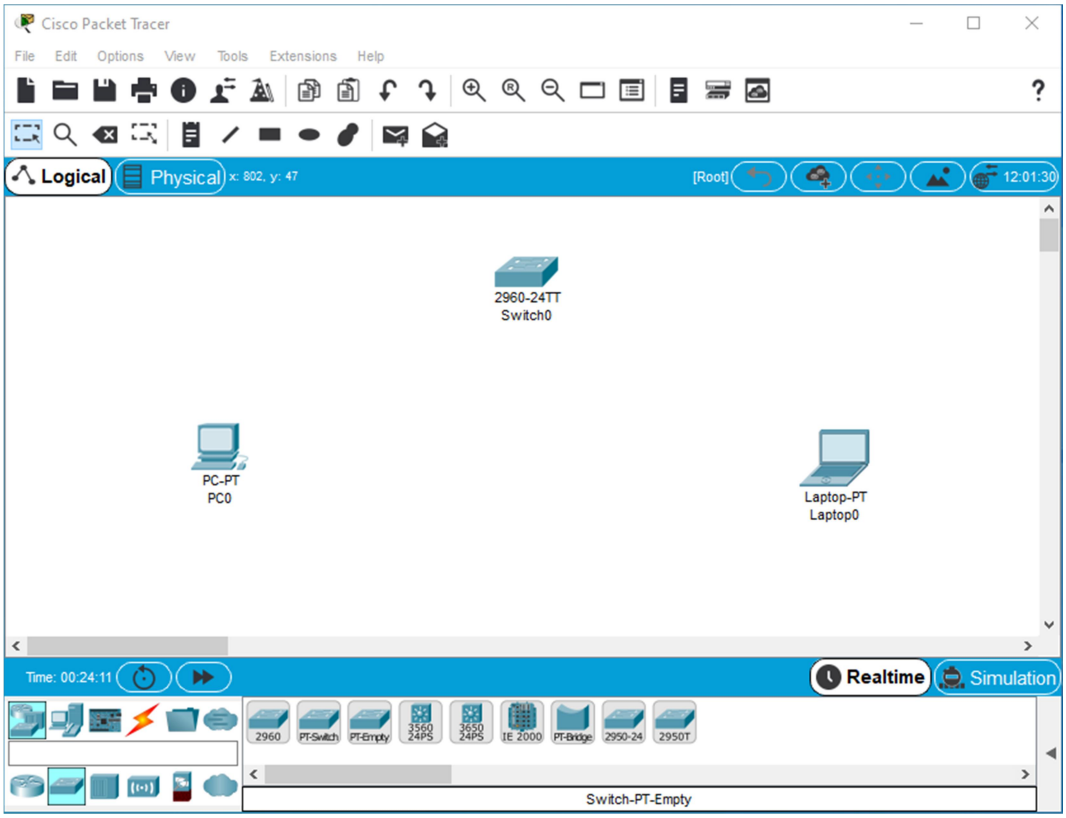


Рисунок 2.3 – Добавление устройств на рабочую область

Для оконечных сетевых устройств (например, компьютеров) на вкладке «Desktop» (рисунок 2.6) расположены эмуляторы работы некоторых утилит рабочего стола (командная строка, интернет-браузер и т.п.). При наведении и удержании курсора мышки в течение несколько секунд на сетевом устройстве отобразится всплывающее окно с краткой информацией о его состоянии (рисунок 2.7).

Более подробная информация доступна через инструмент «Inspect» из блока 3 (рисунок 2.8). Следует отметить, что всплывающее при наведении мыши окно соответствует пункту меню «Port Status Summary Table» инструмента «Inspect».

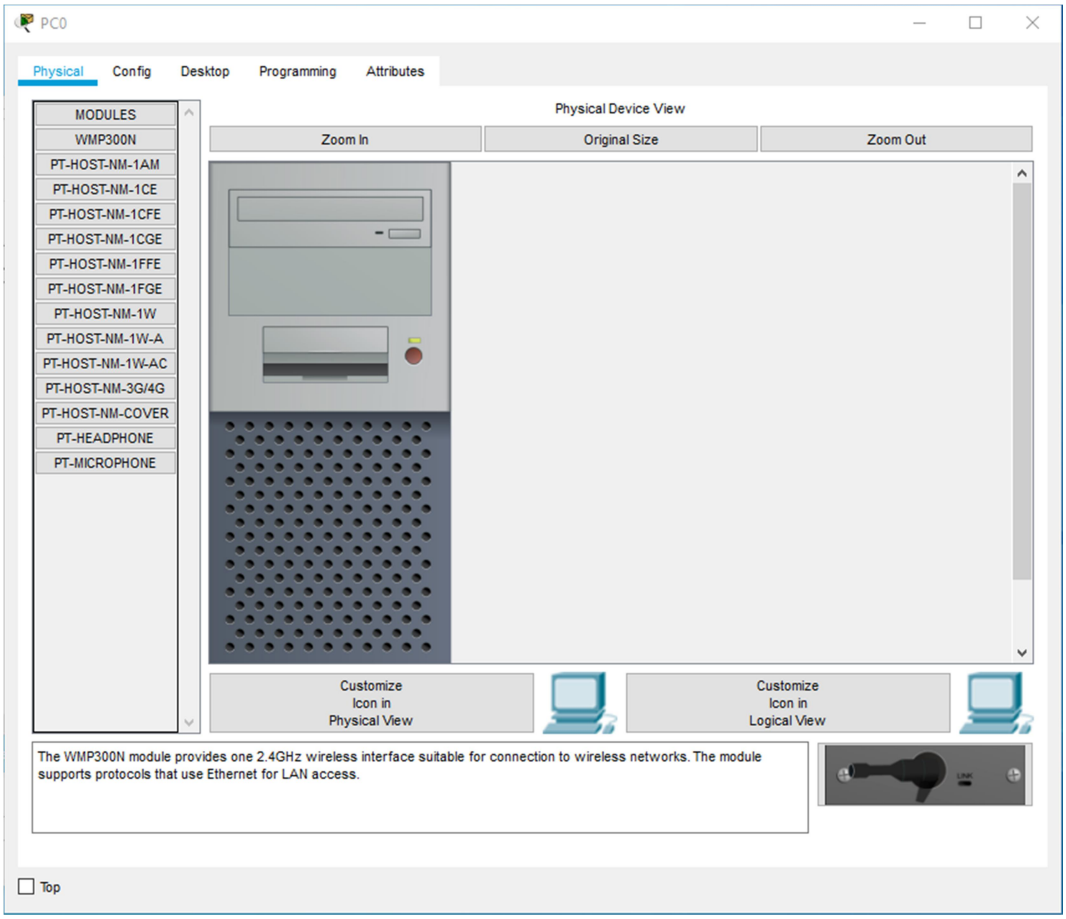


Рисунок 2.4 – Окно конфигурации устройства

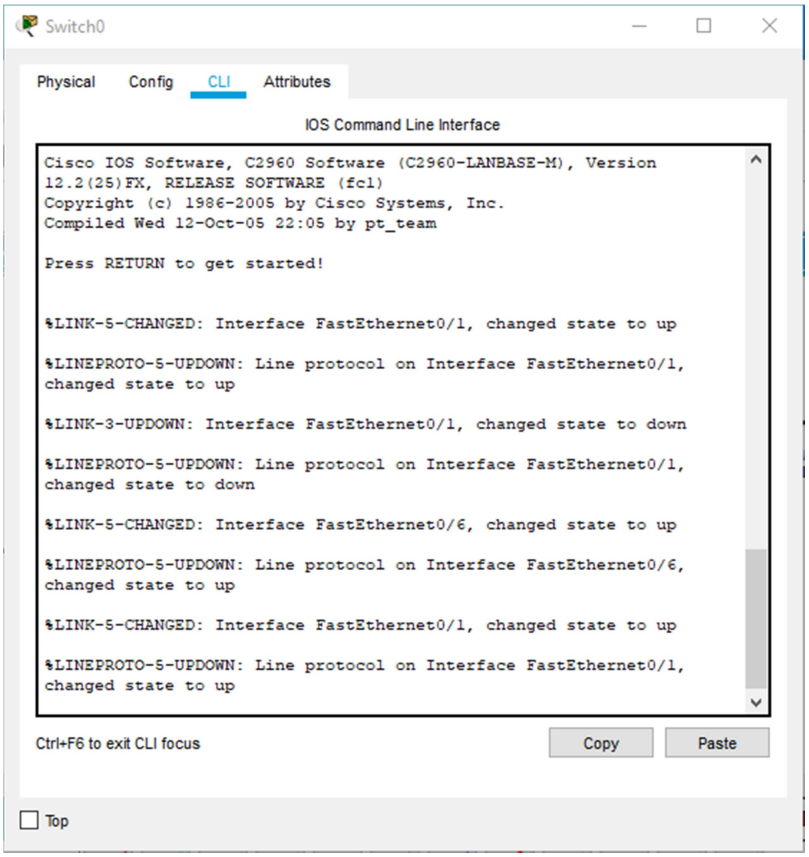


Рисунок 2.5 – Командный интерфейс устройства

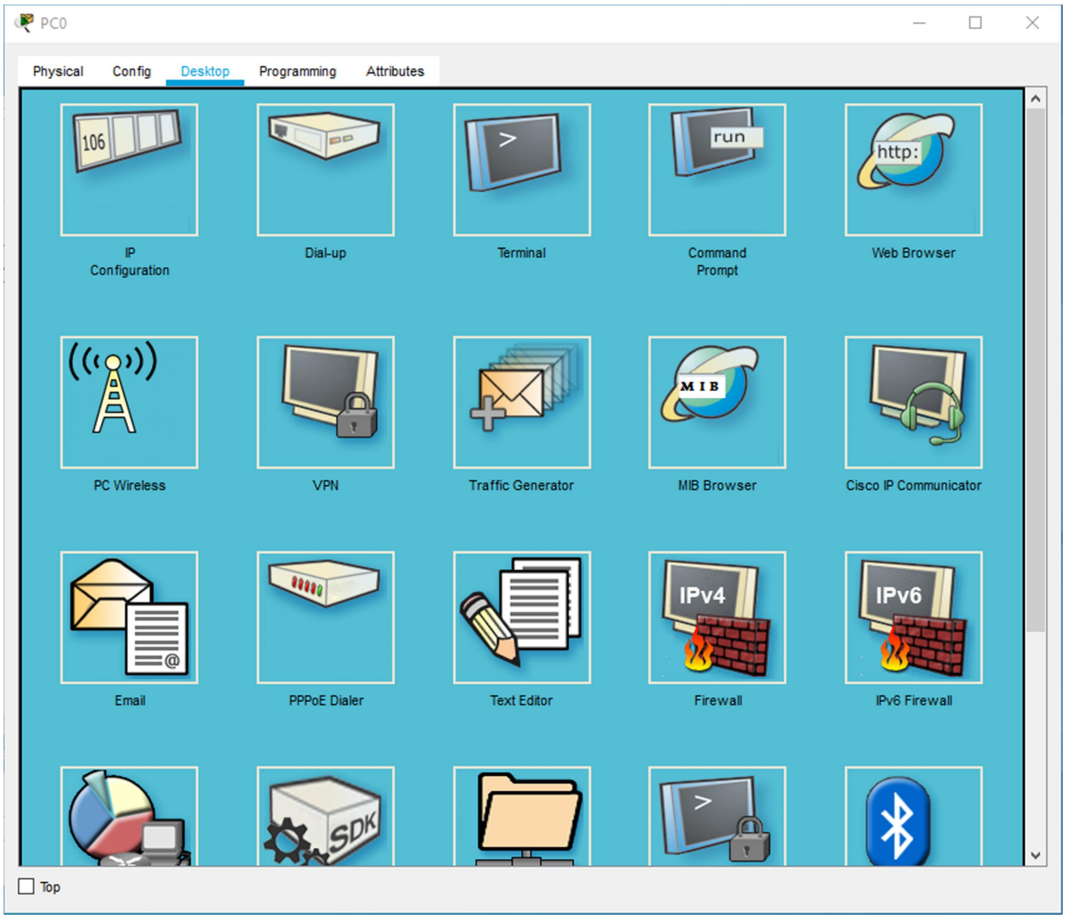


Рисунок 2.6 – Вкладка с эмуляторами сетевых утилит

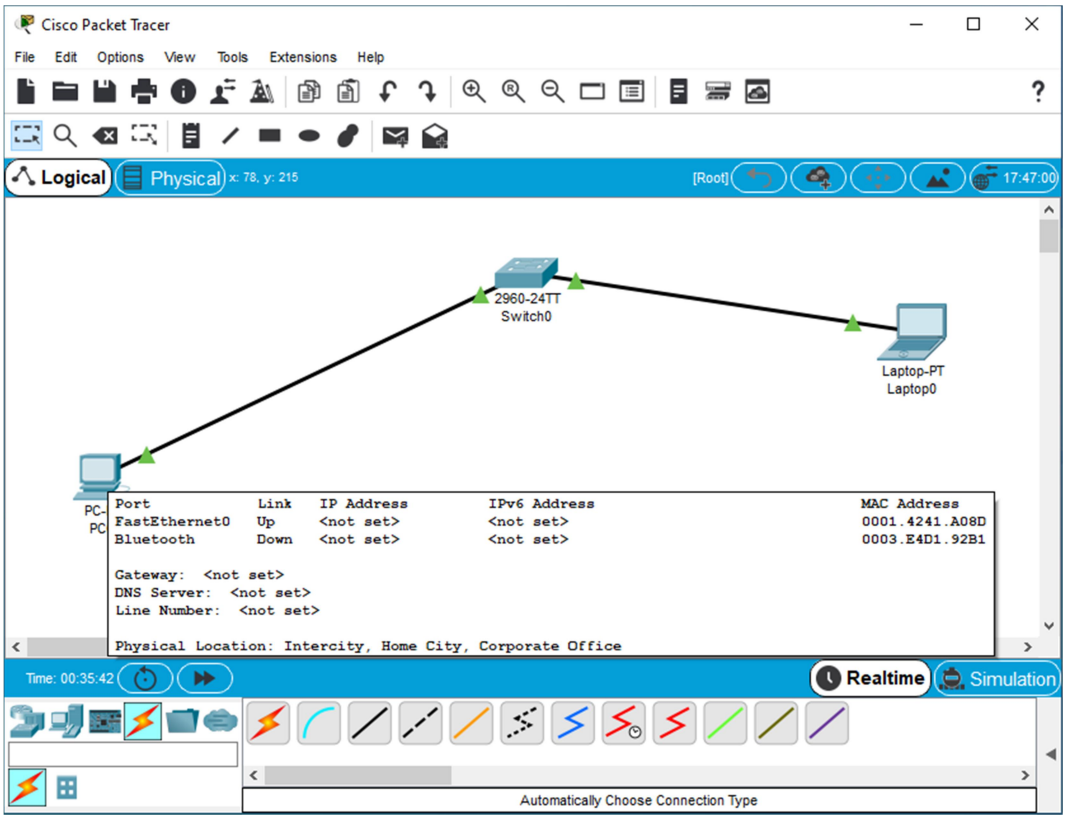


Рисунок 2.7 – Пример всплывающего окна
с краткой информацией о состоянии устройства

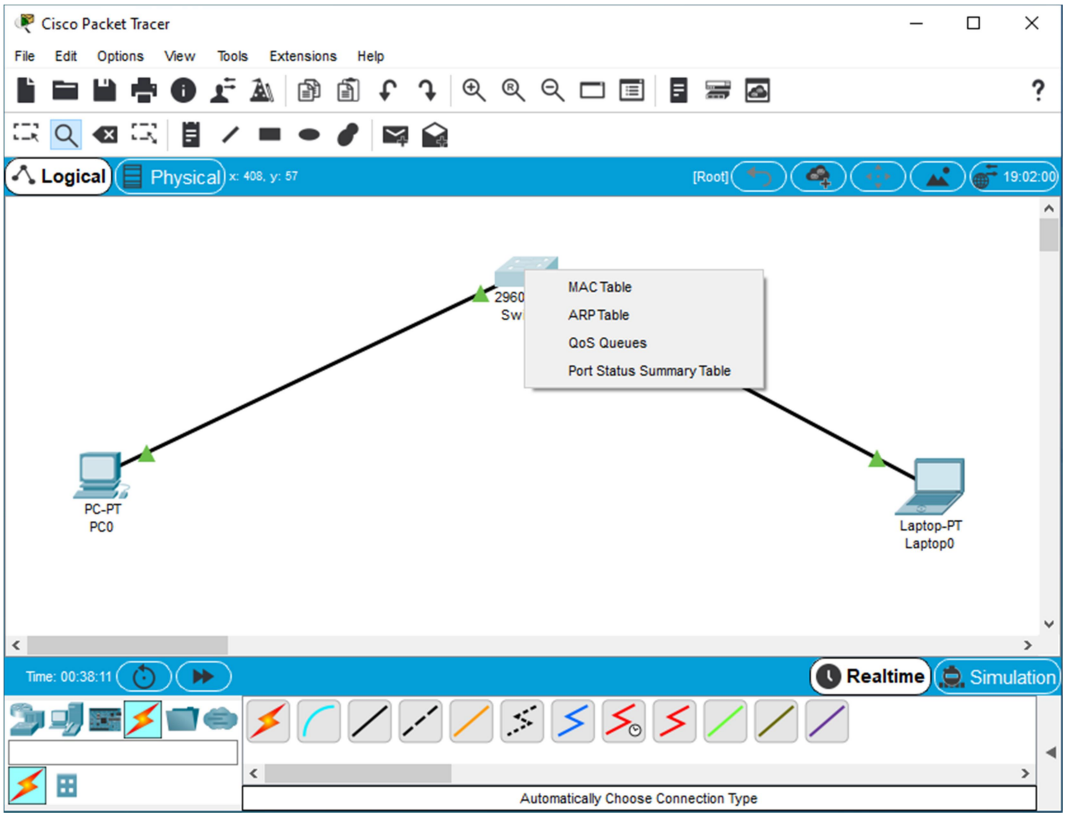


Рисунок 2.8 – Использование инструмента «Inspect»

Для соединения сетевых устройств необходимо выбрать требуемый тип кабеля в блоке 8, указать начальное и конечное устройства и выбрать по одному сетевому порту для каждого из них (рисунок 2.9).

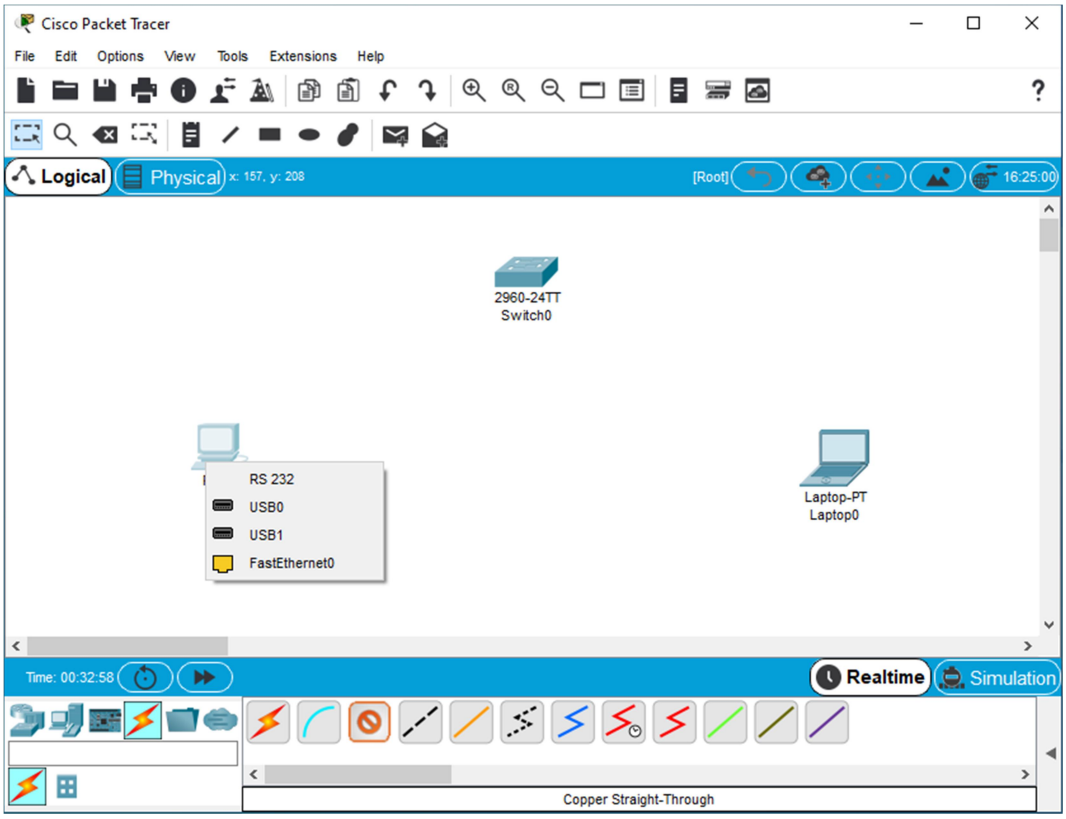


Рисунок 2.9 – Соединение сетевых устройств кабелем

В случае выбора «автоматического определения» (значок «молнии»), порт и тип кабеля будут выбираться автоматически (номер порта будет выбираться в порядке возрастания).

При помощи инструментов из блока 3 пользователь также может добавить на схему текстовую надпись или графические объекты для визуального выделения каких-либо частей схемы или разделения схемы на блоки (рисунок 2.10).

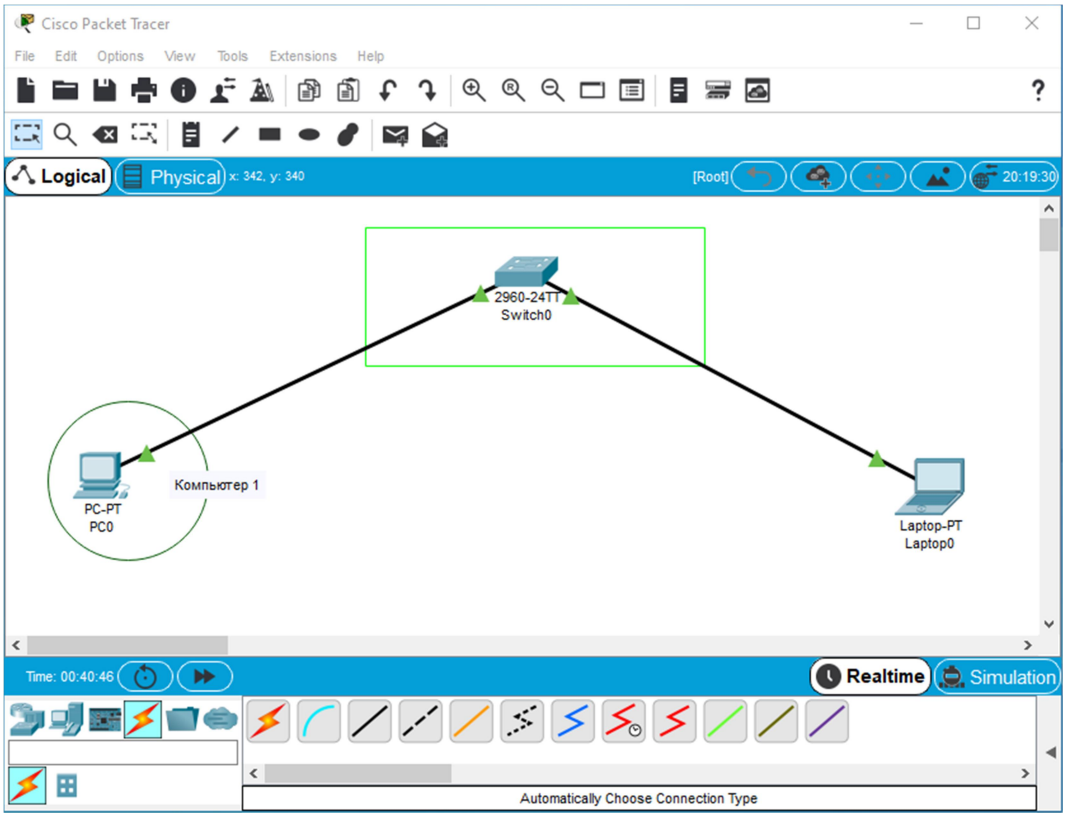


Рисунок 2.10 – Добавление на схему графических объектов

2.3 Вопросы для самопроверки

1. Для чего нужен инструмент «Select»?
2. Чем отличаются режимы работы «логическая» и «физическая» сеть?
3. Чем отличаются режимы «реального времени» и «симуляции»?

2.4 Задание на самостоятельную работу

Большинство сетевых устройств компании Cisco допускают конфигурирование. Для этого пользователь должен подключиться к устройству используя прямое кабельное подключение, удалённое терминальное подключение или Web-интерфейс. Задавая параметры устройства, пользователь определяет его поведение и настраивает порядок его работы.

При подключении к устройству напрямую или через удалённый терминал пользователю предлагается командная строка (Command Line Interface – CLI), в которой он может приступить к конфигурированию устройства.

Интерфейс командной строки для устройств доступен в окне настроек параметров сетевого устройства на вкладке «CLI». Вкладка имитирует прямое кабельное (консольное) подключение к сетевому устройству. Создав новое устройство, на этой вкладке можно наблюдать процесс его загрузки (сервисные сообщения).

Через командную строку пользователь вводит символы, формирующие команды конфигурирования. Это место обозначается «приглашением», состоящим из имени устройства и специализированного символа, отвечающего за подсказку пользователю, в каком режиме сейчас находится командная строка или в какой части конфигурационных параметров сейчас будут производиться действия (см. таблицу 2.2).

Ввод команд завершается нажатием клавиши «Enter», после чего команда начинает интерпретироваться (исполняться). Если команда написана правильно, то будет выполнено соответствующее действие, иначе появится сообщение об ошибке.

Для отмены действия, выполненного какой-либо командой, необходимо выполнить её ещё раз указав перед ней команду «no». В случае если в результате выполнения команды выводится информация, не помещающаяся в одном окне, то в нижней строке выводится сообщение «–More–». Построчная прокрутка текста осуществляется клавишей «Enter», постраничная – клавишей «Пробел». Нажатием клавиш «вверх» и «вниз» на клавиатуре можно подставить в командную строку одну из ранее введенных команд.

Работа с командной строкой осуществляется в нескольких режимах (таблица 2.2). Переход между режимами происходит последовательно: пользовательский режим↔привилегированный режим↔режим глобальной конфигурации.

После подключения к устройству командная строка находится в пользовательском режиме, в котором доступны команды, позволяющие посмотреть часть текущей конфигурации сетевого устройства, запустить процесс проверки работоспособности сети.

Таблица 2.2 – Режимы работы командной строки

Режим	Вход в режим	Вид «приглашения»	Выход из режима
Пользовательский (User EXEC)	Клавиша «Enter» (Командная строка по умолчанию работает в этом режиме)	Router>	Команда «logout»
Привилегированный (Privileged EXEC)	Команда «enable»	Router#	Команда «disable»
Глобальная конфигурация	Команда «configure terminal»	Router (config) #	Команда «exit»
Настройка интерфейсов	Команда «interface» с указанием интерфейса	Router (config-if) #	Команда «exit»

В привилегированном режиме пользователю доступна подробная информация обо всей конфигурации сетевого устройства, а также предоставляется доступ к команде перехода в режим конфигурирования (изменения конфигурационной информации).

Внутри командной строки имеется встроенная контекстная документация (подсказка или помощь), выводимая командной «help» или «?». Если пользователь знает начальные символы команды, но не помнит её продолжение, то следует указать в нужном месте командной строки знак «?», и тогда выведется информация о соответствующих командах или параметрах (например, для «con» варианты «configure» и «connect»). Если существует единственный вариант продолжения команды, ее ввод может быть завершен нажатием клавиши «TAB».

Внутри окна ввода команд можно использовать горячие клавиши:

- *Ctrl+A* – передвинуть курсор на начало строки.
- *Ctrl+E* – передвинуть курсор на конец строки.
- *Ctrl+W* – стереть предыдущее слово.
- *Ctrl+U* – стереть всю линию.

3 ИССЛЕДОВАНИЕ ПРОПУСКНОЙ СПОСОБНОСТИ СЕТИ

3.1 Краткая теоретическая справка

Прикладной
Представления
Сеансовый
Транспортный
Сетевой
Канальный
Физический

Локальная сеть (local area network, LAN) – это компьютерная сеть, покрывающая небольшую территорию (квартиру, аудиторию, здание). В локальной сети компьютеры соединяются с использованием таких сетевых устройств, как концентраторы (хабы) и коммутаторы (свитчи). Основная используемая технология для передачи данных в проводных локальных сетях – Ethernet. В современной ее реализации все компьютеры подключаются к корневому (центральному) сетевому устройству (концентратору или коммутатору) по топологии «звезда». Однако логически технология Ethernet соответствует топологии «общая шина», что проявляется в случайном доступе к общей среде. Такой метод доступа обеспечивает предельную простоту алгоритма работы сети, однако, при повышении нагрузки на сеть, возникают коллизии. Коллизии – такие ситуации, когда два компьютера одновременно пытаются передать данные по общей среде, и эти данные накладываются друг на друга (рисунок 3.1). При возникновении коллизии возникает необходимость повторной передачи данных, что, в итоге, приводит к увеличению задержки передаваемых сигналов и ограничивает величину передаваемого сетевого трафика до 30–40% от номинальной пропускной способности.

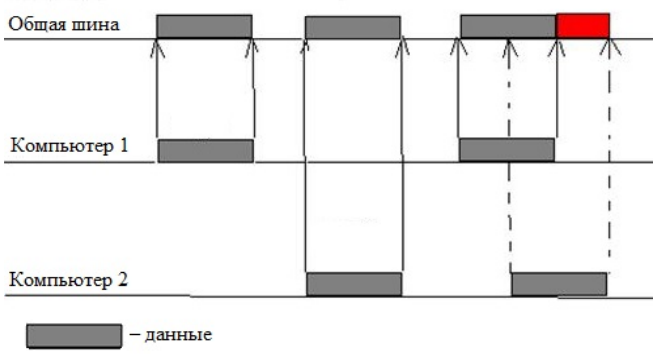


Рисунок 3.1 – Процесс возникновения коллизии

Единая среда формируется в сети, где корневым устройством является концентратор. В такой сети в каждый момент времени могут передаваться данные лишь одного компьютера, и чем больше компьютеров в сети, тем ниже ее пропускная способность. Пропускная способность может быть повышена с помощью логической структуризации, когда корневым устройством становится коммутатор.

Цель работы – исследовать передачу данных в локальных сетях с единой средой и логической структуризацией.

3.2 Задание на практическую работу

Необходимо сформировать сеть с общей средой, объединяющую восемь компьютеров (PC1 – PC8) при помощи четырех промежуточных (Hub1 – Hub4) и одного корневого (Hub) концентратора. В качестве концентраторов использовать устройства «PT-Hub». Топология сети представлена на рисунке 3.2. Концентраторы между собой необходимо соединять «перекрёстным» кабелем («Cross-Over»), а концентраторы с компьютерами – «прямым» («Straight-Through»).

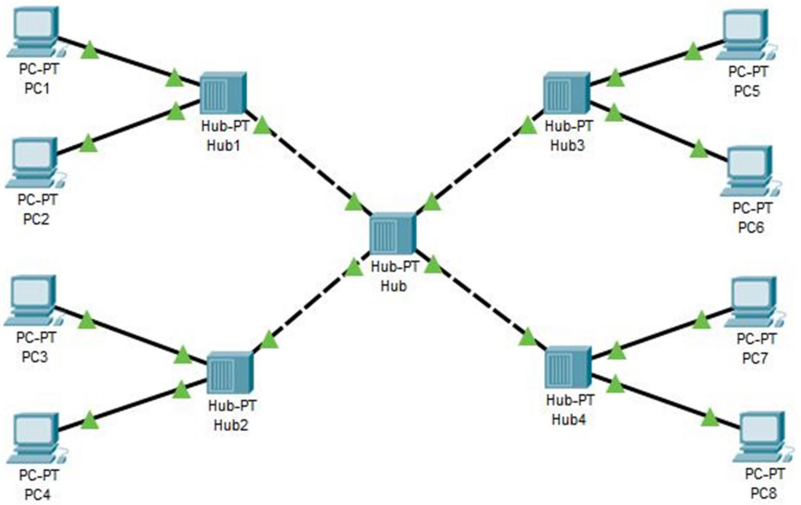


Рисунок 3.2 – Топология сети с концентраторами

После подключения соединительных кабелей к концентраторам производится определение статуса порта. Изменение статуса порта и соединения сопровождается изменением светового индикатора на схеме. В CPT для этого используются маркеры, расположенные на концах линий связи. Маркеры имеют несколько состояний, обозначаемых разными цветами (таблица 3.1)

Таблица 3.1 – Маркеры для отображения статуса портов и состояния соединений

Маркер	Описание состояния
	Порт находится в состоянии «**Down**» (отключено). На физическом уровне не обнаружено каких-либо сигналов.
	Порт находится в состоянии «**Up**» (подключено), т. е. на физическом уровне обнаружен используемый протокол.
(мигает)	Обнаружена активность на канальном уровне. Частота мигания зависит от количества кадров, передаваемых в единицу времени.
	Порт находится в режиме блокировки канального уровня, идет процесс обнаружения возможных сетевых петель. Такое состояние может наблюдаться только на коммутаторах.

Для начала необходимо убедиться, что все используемые порты концентраторов находятся в состоянии «**Up**». Затем необходимо настроить компьютеры в соответствии с таблицей 3.2.

Таблица 3.2 – IP-адреса компьютеров

Имя компьютера	IP-адрес	Маска подсети
PC1	192.168.0.1	255.255.255.0
PC2	192.168.0.2	
PC3	192.168.0.3	
PC4	192.168.0.4	
PC5	192.168.0.5	
PC6	192.168.0.6	
PC7	192.168.0.7	
PC8	192.168.0.8	

Для настройки первого компьютера необходимо щелкнуть по пиктограмме PC1. В открывшемся окне настроек устройства перейти во вкладку «Desktop» и выбрать пункт «IP Configuration» (рисунок 3.3), а затем указать настройки из таблицы 3.2 (IP Address и Subnet Mask).

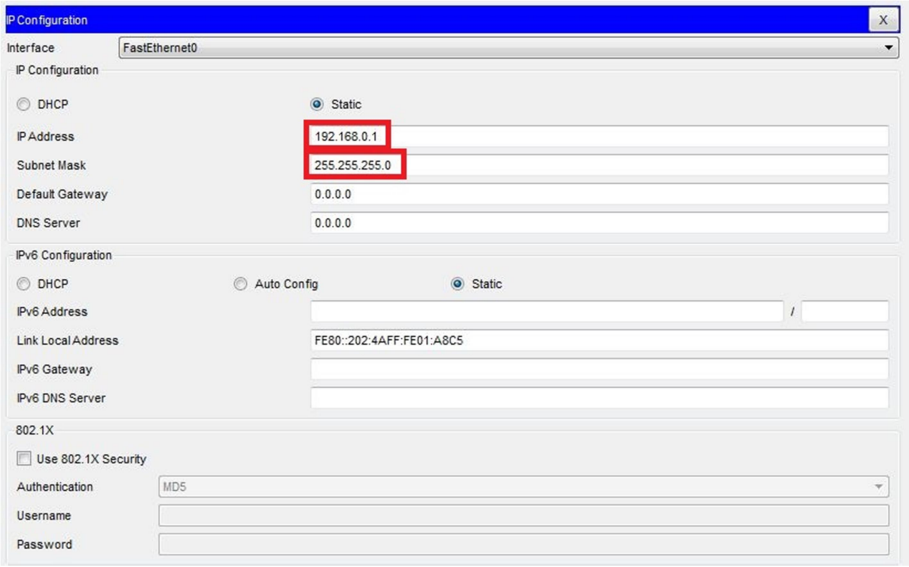


Рисунок 3.3 – Окно «IP Configuration» настроек устройства PC1

Аналогичным образом необходимо настроить остальные компьютеры.

Для проверки правильности настроек компьютера необходимо открыть окно настроек устройства и на вкладке «Desktop» выбрать приложение «Command Promt» (аналог командной строки Windows). В открывшемся окне после приглашения **C:\>** ввести команду «**ipconfig /all**» (описание основных сетевых утилит семейства ОС Windows приведено в приложении Б) и убедиться в правильности введенных сетевых настроек (рисунок 3.4). Процедуру проверки правильности настроек необходимо провести на всех компьютерах.

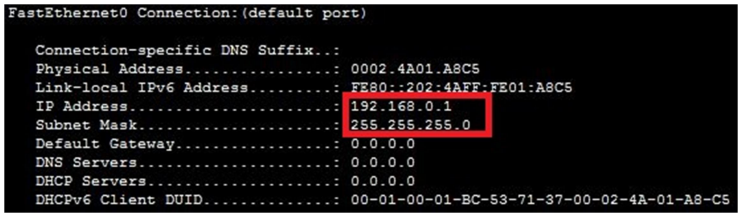


Рисунок 3.4 – Окно «Command Promt» настроек устройства PC1

Доступность компьютера проверяется при помощи посылки контрольного диагностического сообщения по протоколу **ICMP**, по которому любая оконечная станция должна выдать эхо-ответ узлу, отправившему такое сообщение. В сетях на основе стека протоколов **TCP/IP** для проверки соединений используется утилита «**ping**». Эта утилита отправляет запросы протокола **ICMP** узлу сети с указанным IP-адресом. Получив этот запрос, исследуемый узел должен послать пакет с ответом. Первый узел фиксирует поступающие ответы. Время между отправкой запроса и получением ответа (**RTT, Round Trip Time**) позволяет определять двусторонние задержки по маршруту и частоту потери пакетов, т. е. косвенно определить загруженность каналов передачи данных и промежуточных устройств.

Далее надо проверить доступность узла PC2 из узла PC1. Для этого на PC1 необходимо запустить интерфейс командной строки «Command Promt» и выполнить команду «**ping 192.168.0.2**». После выполнения команды будет отображено число отправленных («Sent»), полученных («Received») и потерянных («Lost») пакетов. В случае правильной конфигурации сети и компьютеров (PC1, PC2) на все отправленные эхо-запросы будут получены эхо-ответы, о чем свидетельствует запись «0% loss» (рисунок 3.5 *а*). При наличии ошибок в подключениях или настройках узлов будет получено сообщение о потере пакетов «*x*% loss» (рисунок 3.5 *б*). После успешного установления соединения надо проверить

доступность других компьютеров в сети, выполнив команду «**ping <IP-адрес>**» для всех компьютеров в сети.

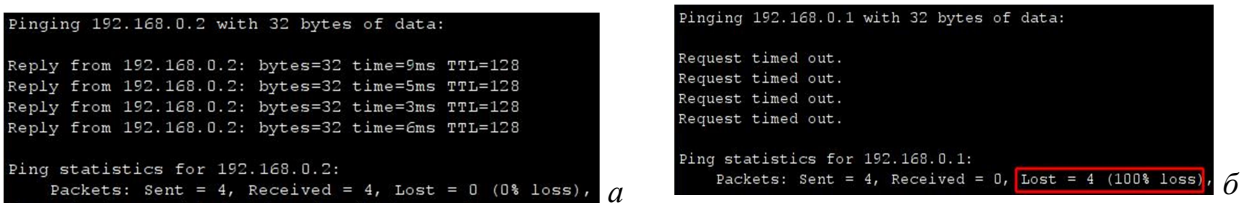


Рисунок 3.5 – Результат выполнения команды «ping»
без потери пакетов (*а*) и с их потерей (*б*)

Протокол **ICMP** является универсальным средством тестирования сетей на основе стека протоколов **TCP/IP**. Так, например, если увеличить размер пакета и отправить запросы с коротким интервалом, не ожидая ответа от удаленного узла, то можно создать серьезную сетевую нагрузку. С учетом этого, при помощи протокола **ICMP** необходимо сформировать трафик между компьютерами PC3 и PC7. Штатная утилита «**ping**» не позволяет отправлять эхо-запрос без получения эхо-ответа на предыдущий запрос или до истечения времени ожидания. Поэтому для организации трафика можно воспользоваться приложением «Traffic Generator».

Для этого в окне управления PC3 во вкладке «Desktop» надо выбрать приложение «Traffic Generator» и указать в нем следующие настройки:

– в разделе «Source Settings» отметить «Auto Select Port»;

– в разделе PDU Settings выбрать и задать:

– Select application – PING;

– Destination IP Address – 192.168.0.7 (адрес получателя);

– Source IP Address – 192.168.0.3 (адрес отправителя);

– TTL – 32;

– TOS – 0 (тип обслуживания, «0» – обычный, без приоритета);

– Sequence Number – 1 (начальное значение счетчика пакетов);

– Size – 500 (размер поля данных пакета в байтах).

– в разделе «Simulations Settings» отметить «Periodic», а значение «Interval» задать равным 0,01.

После нажатия кнопки «Send» между компьютерами PC3 и PC7 начнется активный обмен данными. При этом не надо закрывать окно «Traffic Generator», для того, чтобы трафик не прервался.

Необходимо обратить внимание на изменившуюся активность сетевых интерфейсов (частота мигания зеленых маркеров на линиях связи). Так, активность должна существенно увеличиться.

CPT позволяет наглядно представить прохождение данных по сети, используя режим «Simulation». Надо включить этот режим, а затем нажать на кнопку play (►). Тогда можно проследить прохождение по сети запроса и ответа на него. Чтобы перезапустить симуляцию, надо нажать кнопку «Reset Simulation».

В режиме симуляции можно увидеть, что в неструктурированной сети пакеты, передаваемые с PC3, распространяются по всей сети и поступают на все компьютеры. При этом на всех компьютерах, кроме компьютера назначения PC7, полученные сообщения отбрасываются (помечаются красным цветом).

Далее необходимо вернуться в режим «Realtime» и, не прекращая работу приложения «Traffic Generator», передать контрольный поток пакетов между PC1 и PC8 при помощи команды «**ping –n 100 192.168.0.8»** (параметр «–n» позволяет задать число передаваемых запросов, если не задать его, то отправляется только 4 запроса). Отправив 100 эхо-запросов,

можно оценить исходное качество работы сети по числу потерянных пакетов. Полученные данные надо сохранить для дальнейшей обработки.

После сохранения результатов надо остановить «Traffic Generator», нажав кнопку «Stop», и заменить центральный концентратор коммутатором 2960-24TT (рисунок 3.6).

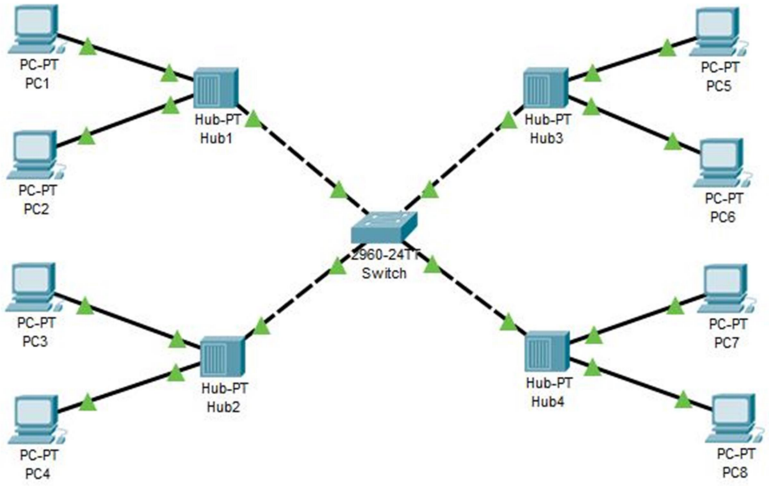


Рисунок 3.6 – Топология сети с центральным коммутатором

При замене центрального концентратора на коммутатор вся сеть разделится на четыре логических сегмента. Надо включить «Traffic Generator» на PC3 и, проследив за работой сети в режим «Simulation», убедиться в том, что пакеты, передаваемые между PC3 и PC7, направляются только в сегменты сети, в которых находятся эти компьютеры. Также необходимо передать контрольный поток пакетов между PC1 и PC8 при помощи команды «**ping –n 100 192.168.0.8**» и оценить, как изменилось число потерянных пакетов в сети.

Далее надо заменить оставшиеся концентраторы на коммутаторы (рисунок 3.7). По маркерам нужно убедиться, что сеть находится в рабочем состоянии. (Установка коммутаторов в каждом сегменте устраняет возможность возникновения коллизий между пакетами пользователей данного сегмента). Для этой сети надо проделать операции, которые выполнялись для предыдущих сетей и сохранить полученные результаты.

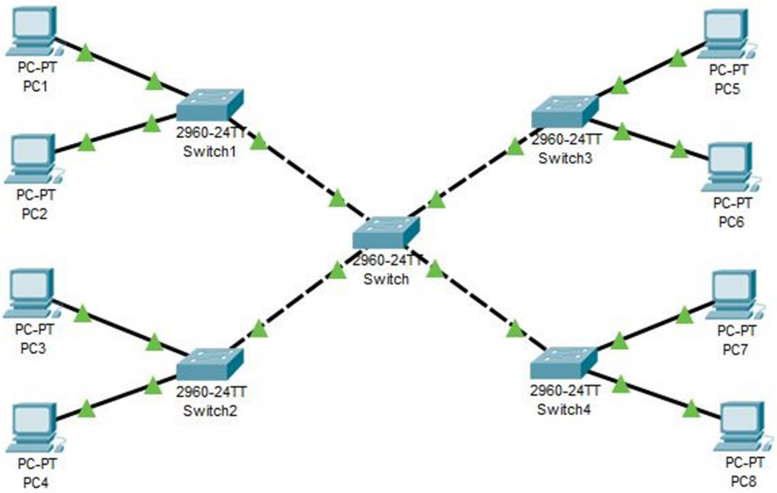


Рисунок 3.7 – Топология сети с коммутаторами

3.3 Вопросы для самопроверки

1. Что такое коллизии?

2. В чем состоит отличие сетей с единой средой и логической структуризацией?
3. Каким образом обычно определяется доступность компьютера в сети?

3.4 Задание на самостоятельную работу

По результатам проделанной работы надо заполнить таблицу 3.3 и сформировать развернутые выводы по ней. Строка, соответствующая первому испытанию, может быть заполнена данными, полученными в предыдущем разделе. Остальные строки заполнить самостоятельно.

Таблица 3.3 – Результаты испытаний пропускной способности сети

№ испытания	Настройки сетевого трафика	Число потерянных пакетов между PC1–PC8		
		Сеть с концентраторами (рисунок 3.2)	Сеть с центральным коммутатором (рисунок 3.6)	Сеть с коммутаторами (рисунок 3.7)
1	PC1–PC8, ping, *n* = 100; PC3–PC7, Traffic Generator, *Size* = 500, *T* = 0,01 с			
2	PC1–PC8, ping, *n* = 100; PC5–PC4, Traffic Generator, *Size* = 5000, *T* = 0,005 с			
3	PC1–PC8, ping, *n* = 100; PC3–PC7, Traffic Generator, *Size* = 500, *T* = 0,01 с; PC5–PC4, Traffic Generator, *Size* = 5000, *T* = 0,005 с			

4 ПРИНЦИП РАБОТЫ КОММУТАТОРА

4.1 Краткая теоретическая справка

В предыдущей работе использовались такие сетевые устройства, как концентратор и коммутатор, без подробных пояснений принципов их работы. Для наглядной демонстрации принципа работы коммутатора и различий между ними предназначена данная работа.

Сетевой коммутатор или **свитч** (switch) – устройство, предназначенное для соединения нескольких узлов компьютерной сети в пределах одного сегмента. В отличие от концентратора, который распространяет трафик от одного подключенного устройства ко всем остальным, коммутатор передает данные только непосредственно получателю. Это повышает производительность и безопасность сети, избавляя остальные сегменты сети от необходимости (и возможности) обрабатывать данные, которые им не предназначены. Коммутаторы работают на канальном (втором) уровне модели OSI (поэтому иногда их называют коммутаторами L2).

Коммутатор хранит в памяти специальную таблицу (таблицу коммутации или MAC-таблицу), в которой указывается соответствие порту коммутатора MAC-адреса устройства, подключенного к этому порту. При включении коммутатора эта таблица пуста, и он работает в режиме обучения. При этом, поступающие на его порты данные передаются на все остальные порты, кроме того порта, через который эти данные получены.

Коммутатор анализирует поступающие данные, определяя MAC-адрес отправителя и помещая его в таблицу коммутации напротив того порта, с которого данные были получены. Далее, если на один из его портов поступят данные, предназначенные для узла с этим MAC-адресом, они будут отправлены только через соответствующий порт. Со временем коммутатор сформирует полную таблицу и трафик локализуется.

Коммутаторы подразделяются на управляемые и неуправляемые. Более сложные управляемые коммутаторы позволяют управлять коммутацией на канальном (втором) и сетевом (третьем) уровне модели OSI (коммутаторы L3). Многие управляемые коммутаторы реализуют дополнительные функции: VLAN, агрегирование и пр. (этим понятиям посвящены последующие работы).

Цель данной работы – научиться анализировать работу сети и оценивать, каким образом заполняется таблица коммутации.

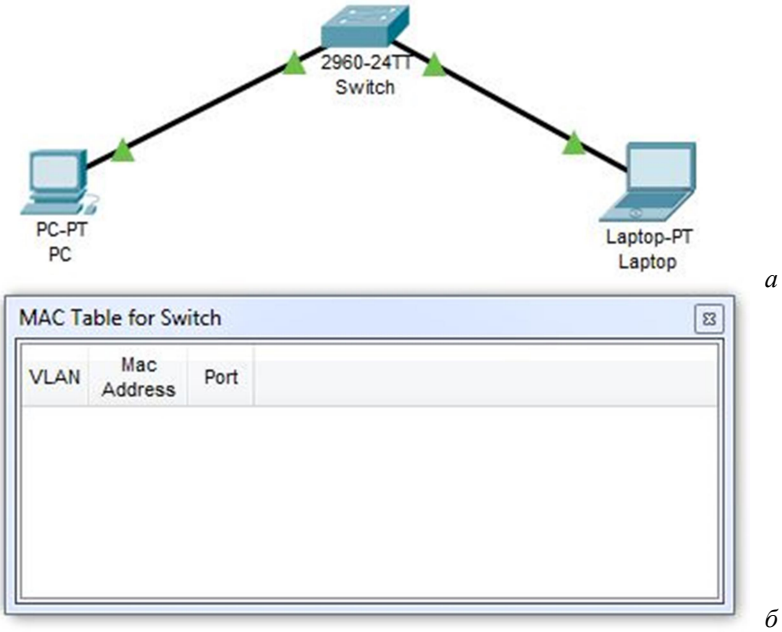
4.2 Задание на практическую работу

Необходимо сформировать небольшую сеть, состоящую из стационарного компьютера, ноутбука и коммутатора 2960-24TT (рисунок 4.1 *а*), а затем отобразить (при помощи инструмента Inspect) таблицу коммутации коммутатора (MAC Table) и убедиться, что она пуста (рисунок 4.1 *б*).

После построения сети надо назначить компьютеру IP-адрес 192.168.0.1, а ноутбуку – 192.168.0.2. После этого определить MAC-адреса устройств (компьютера и ноутбука) при помощи команды «**ipconfig /all**» в приложении «Command Promt» на вкладке «Desktop» (на рисунке 4.2 показан пример выполнения команды для компьютера).

Для наглядности, далее надо нанести на схему IP и MAC-адреса хостов при помощи инструмента Place Note (рисунок 4.3). Дальнейшие действия необходимо совершать в режиме «Simulation». Так, надо проверить связь между компьютером и ноутбуком с

помощью команды «ping». Для этого на компьютере ввести «**ping -n 1 192.168.0.2**», а затем нажать кнопку «play» (►). Далее нужно пронаблюдать, как по мере прохождения запросов заполняется таблица коммутации (рисунок 4.4). Когда она будет заполнена, можно приостановить симуляцию повторным нажатием кнопки «play». Из рисунка 4.4 видно, что к порту *0/1* коммутатора присоединен компьютер, а к порту *0/2* – ноутбук.



а

б

Рисунок 4.1 – Топология сети (*а*) и таблица коммутации коммутатора (*б*)

```
Packet Tracer PC Command Line 1.0
C:\>ipconfig /all

FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Physical Address.....................: 0060.3E88.742C
```

Рисунок 4.2 – Выполнение команды «ipconfig /all»

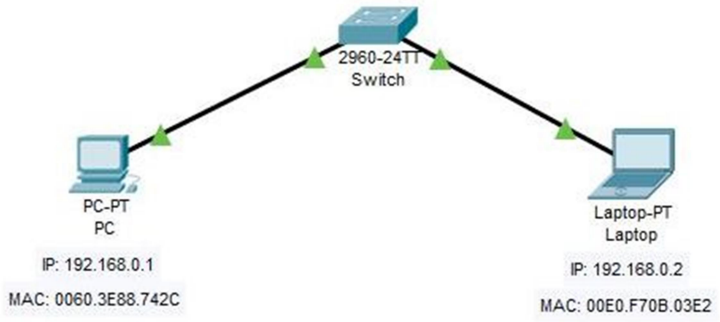


Рисунок 4.3 – Указание IP и MAC-адресов на схеме сети

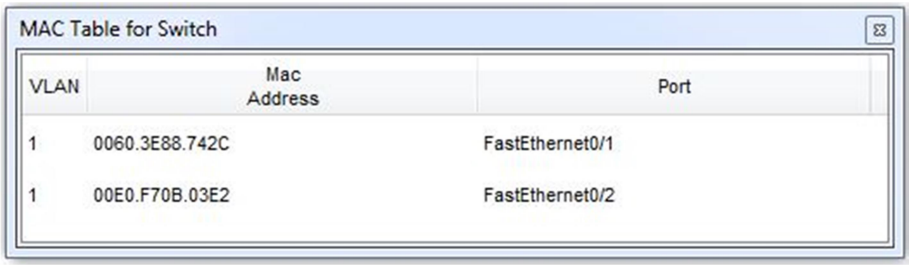


Рисунок 4.4 – Заполненная таблица коммутации

Для того чтобы проанализировать содержимое пакетов и определить, каким образом была заполнена таблица коммутации, надо нажать на первый пакет типа «ARP[1]» в списке событий («Event List») (рисунок 4.5).

Time(sec)	Last Device	At Device	Type
0.000	--	PC	ICMP
0.000	--	PC	ARP
0.001	PC	Switch	ARP
0.002	Switch	Laptop	ARP
0.003	Laptop	Switch	ARP
0.004	Switch	PC	ARP

Рисунок 4.5 – Список событий («Event List»)

В появившемся окне отобразится информация в соответствии с моделью OSI. Следует обратить внимание, на каких уровнях происходит взаимодействие. Затем перейти во вкладку «Outbound PDU Details», в которой отображается содержимое Ethernet-кадра (поскольку протокол ARP работает на втором уровне модели OSI) (рисунок 4.6).

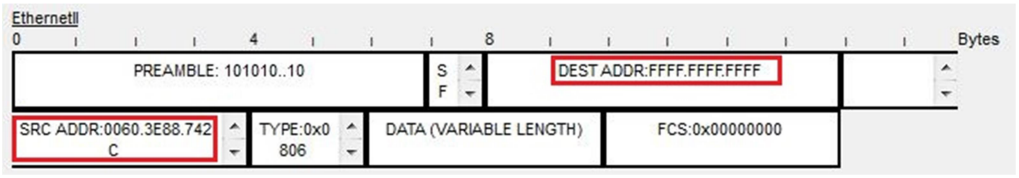


Рисунок 4.6 – Ethernet-кадр

Важно обратить внимание на поля с адресами источника («SRC ADDR») и назначения («DEST ADDR»). В качестве отправителя компьютер указывает себя, а в качестве получателя – широковещательный MAC-адрес (FFFF.FFFF.FFFF), поскольку настоящий MAC-адрес ноутбука компьютеру пока неизвестен.

Получив кадр с адресом FFFF.FFFF.FFFF в поле адреса назначения, коммутатор переправляет его на все активные порты, кроме того порта через который получен кадр, после чего в таблицу коммутации добавляется строка соответствия номера порта коммутатора MAC-адресу компьютера. После того, как ноутбук получит кадр, он выполнит анализ его заголовка. Сравнив MAC-адрес назначения и свой собственный, ноутбук «понимает», что запрос предназначен ему и готовит ответ (рисунок 4.7). В результате, в поле адреса источника Ethernet-кадра будет помещен MAC-адрес его сетевого адаптера. После чего кадр будет отправлен на коммутатор.

Получив кадр, коммутатор проанализирует поле адреса назначения (адрес компьютера) в заголовке и сопоставит его со своей таблицей коммутации и, найдя соответствие, переправит кадр через соответствующий порт, а также скорректирует свою таблицу коммутации, добавив в нее информацию о MAC-адресе ноутбука.

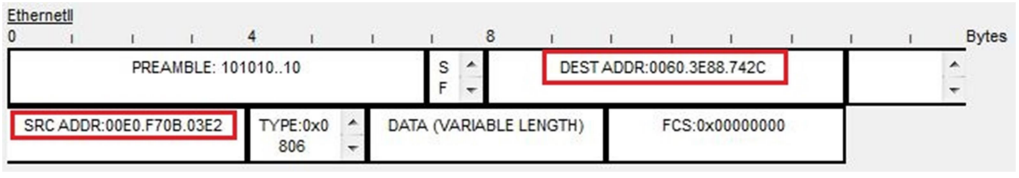


Рисунок 4.7 – Ethernet-кадр

Все следующие ICMP-запросы будет продвигаться по «проложенному пути» без необходимости использования ARP-запросов и «ненужной» широковещательной рассылки кадров по сети.

[1] Сетевой протокол, предназначенный для определения MAC-адреса по IP-адресу.

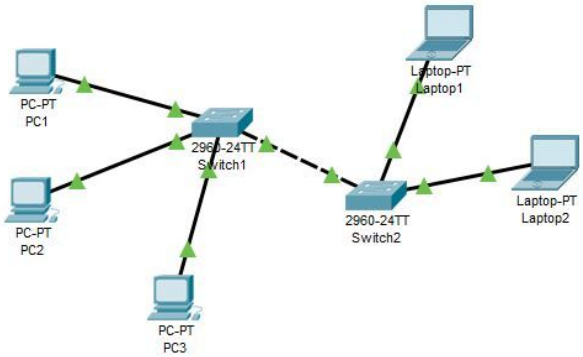
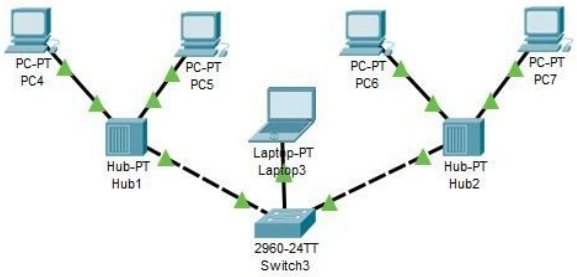
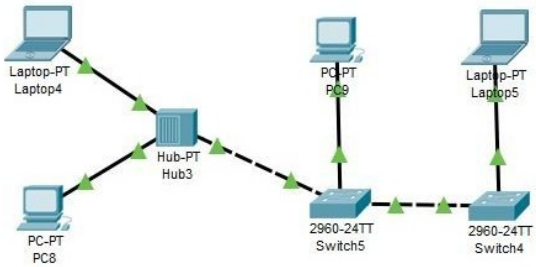
4.3 Вопросы для самопроверки

1. Опишите принцип действия коммутатора.
2. Для чего нужна таблица коммутации?
3. Какие поля содержит таблица коммутации?

4.4 Задание на самостоятельную работу

Проанализировать сеть в соответствии с выданным преподавателем вариантом (таблица 4.1), и определить, как будут выглядеть таблицы коммутации всех коммутаторов после их полного заполнения, и проверить себя, построив сеть в CPT.

Таблица 4.1 – Варианты индивидуальных заданий

Вариант	Топология сети
1	
2	
3	

5 ВИРТУАЛЬНЫЕ СЕТИ

5.1 Краткая теоретическая справка

VLAN – группа узлов сети, трафик которой, в том числе широковещательный, на канальном уровне полностью изолирован от трафика других узлов.

Построение и поддержка VLAN является одной из основных и часто применяемых функций, используемых в сетях с коммутаторами. Создание VLAN на коммутаторе означает разбиение коммутатора на несколько **широковещательных доменов**. Если один и тот же VLAN есть на разных коммутаторах, то порты разных коммутаторов будут образовывать один широковещательный домен. Для того чтобы трафик одной VLAN попадал в другую, применяются сетевые устройства 3-го уровня OSI, а именно маршрутизаторы.

Применение технологии VLAN преследует следующие цели:

– Уменьшение количества широковещательного трафика в сети. Это одна из основных задач, решаемая с помощью VLAN. Сеть, построенная на коммутаторах, даже при значительно разветвленной топологии обязана пропускать широковещательный трафик (MAC-адреса FFFF:FFFF:FFFF) ко всем компьютерам разных сегментов сети. Производительность сети в данные моменты значительно снижается. Использование же VLAN позволяет существенно сократить объем широковещательного трафика за счет того, что широковещательный трафик одной VLAN не передается в другие;

– Гибкое разделение устройств на группы. Как правило, одной VLAN соответствует одна IP-подсеть. Устройства, находящиеся в разных VLAN, будут находиться в разных IP-подсетях. Но в то же время VLAN не привязана к местоположению устройств и поэтому устройства, находящиеся на расстоянии друг от друга, все равно могут быть в одной VLAN независимо от местоположения. Таким образом, сотрудники одного отдела, даже находясь в разных зданиях, могут находиться в одной виртуальной сети;

– Увеличение безопасности и управляемости сети. Когда сеть разбита на VLAN, упрощается задача применения политик и правил безопасности. С VLAN политики можно применять к целым подсетям, а не к отдельному устройству. Кроме того, переход из одной VLAN в другую предполагает прохождение через устройство 3 уровня модели OSI, на котором, как правило, применяются политики, разрешающие или запрещающие доступ из одной VLAN в другие.

Таким образом, достоинством технологии виртуальных сетей является то, что она позволяет создавать полностью изолированные сегменты сети путем логического конфигурирования коммутаторов, не прибегая к изменению физической структуры.

Построение сетей VLAN может осуществляться различными способами. Самым широко используемым является VLAN на основе меток в дополнительном поле кадра (на основе поля «Type» кадра Ethernet) – стандарт IEEE 802.1 Q. У провайдеров услуг широко используется технология VLAN на основе стандарта IEEE 802.1 ad (Q-in-Q VLAN).

Подробнее рассмотрим стандарт IEEE 802.1 Q. Введение стандарта 802.1 Q позволило производителям оборудования преодолеть различия в фирменных реализациях VLAN и добиться совместимости при построении виртуальных локальных сетей. Поддерживают этот стандарт как производители коммутаторов, так и сетевых адаптеров для серверов. Важным для стандарта 802.1 Q являются понятия тегированного кадра и порта.

Тегированный (помеченный) **кадр** – кадр Ethernet, который имеет дополнительное 32-битное поле, помещаемое после поля с MAC-адресом отправителя. В это поле помещается информация о том, какой виртуальной сети принадлежит данный кадр.

Порты коммутатора, поддерживающие VLAN, можно разделить на два множества:

– тегированные порты (tagged-порты, транковые порты, trunk-порты);

– нетегированные порты (untagged-порты, порты доступа, access-порты).

Все виртуальные сети имеют номер (например, VLAN 1, VLAN 15).

Обычно, по умолчанию все порты коммутатора считаются нетегированными членами VLAN 1. В процессе настройки или работы коммутатора они могут перемещаться в другие VLAN. Таким образом, разные порты коммутатора могут принадлежать разным VLAN.

Цель работы – получить навыки создания и использования виртуальных сетей.

5.2 Задание на практическую работу

Необходимо сформировать топологию сети, представленную на рисунке 5.1 (использовать коммутаторы 2960-24TT). Компьютеры необходимо подключать к портам коммутаторов *FastEthernet 0/1*, *FastEthernet 0/2* и *FastEthernet 0/3*, а коммутаторы между собой – к портам *FastEthernet 0/10*. Присвоить IP-адреса компьютерам согласно таблице 5.1. Для наглядности IP-адреса компьютеров нужно нанести на схему.

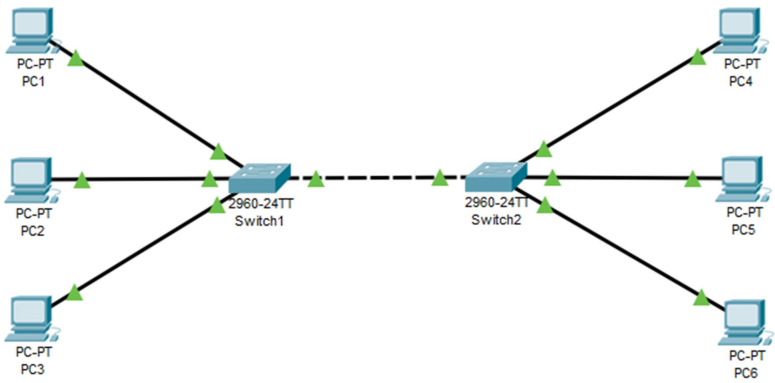


Рисунок 5.1 – Топология сети

Таблица 5.1 – IP-адреса компьютеров

Устройство	IP адрес/Маска подсети
PC1	192.168.10.10/24
PC2	192.168.20.10/24
PC3	192.168.30.10/24
PC4	192.168.10.11/24
PC5	192.168.20.11/24
PC6	192.168.30.11/24

Выполнить настройку коммутаторов. Для этого открыть командный интерфейс (CLI) первого коммутатора (Switch1) и перейти в режим глобальной конфигурации:

```
Switch>enable
Switch#configure terminal
```

Перейти в режим настройки группы портов:

```
Switch(config)#interface range fastEthernet 0/1, fastEthernet 0/2, fastEthernet 0/3
```

Настроить эти порты как нетегированные (порты доступа):

```
Switch(config-if-range)#switchport mode access
```

```
Switch(config-if-range)#exit
```

Настроить порт *FastEthernet 0/10* как тегированный (транковый):

```
Switch(config)#interface fastEthernet 0/10
Switch(config-if)#switchport mode trunk
Switch(config-if)#exit
```

Далее надо создать и присвоить имена всем VLAN, как указано на рисунке 5.2.

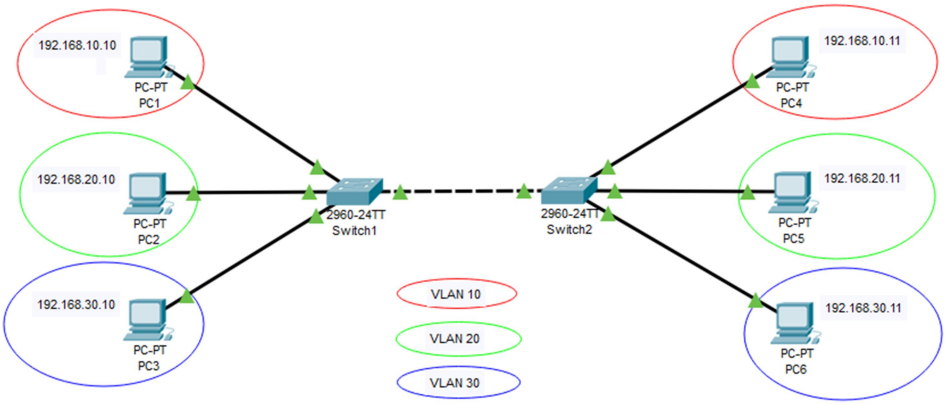


Рисунок 5.2 – Топология сети с указанием VLAN

Для этого выполнить (в режим глобальной конфигурации):

```
Switch(config)#vlan 10
Switch(config-vlan)#name red
Switch(config-vlan)#exit
Switch(config)#vlan 20
Switch(config-vlan)#name green
Switch(config-vlan)#exit
Switch(config)#vlan 30
Switch(config-vlan)#name blue
Switch(config-vlan)#exit
```

Назначить порты соответствующим VLAN:

```
Switch(config)#interface fastEthernet 0/1
Switch(config-if)#switchport access vlan 10
Switch(config-if)#exit
Switch(config)#interface fastEthernet 0/2
Switch(config-if)#switchport access vlan 20
Switch(config-if)#exit
Switch(config)#interface fastEthernet 0/3
Switch(config-if)#switchport access vlan 30
Switch(config-if)#exit
Switch(config)#exit
```

Аналогичным образом настраивается второй коммутатор (Switch2). После настройки обоих коммутаторов надо проверить правильность настроек на каждом из них:

```
Switch#show vlan brief
Switch#show vlan id 10
Switch#show vlan id 20
Switch#show vlan id 30
```

```
Switch#show interfaces trunk
```

В отчете необходимо привести результаты выполнения этих команд (с пояснениями). Также в отчете требуется привести скриншоты всплывающих подсказок, возникающих при наведении мыши на коммутаторы.

После настройки сети надо убедиться в ее работоспособности. Для этого выполнить команду «ping» на каждом компьютере для всех остальных компьютеров и убедиться в правильности настроек.

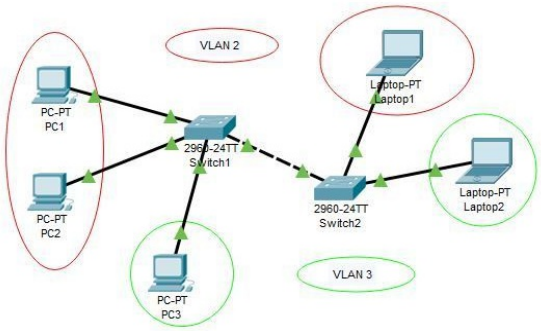
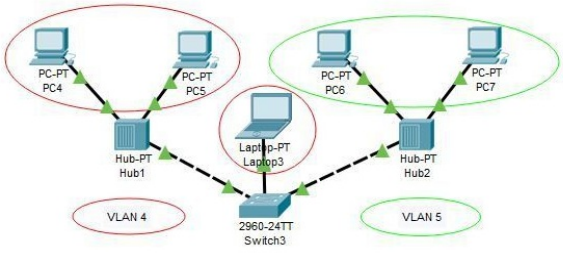
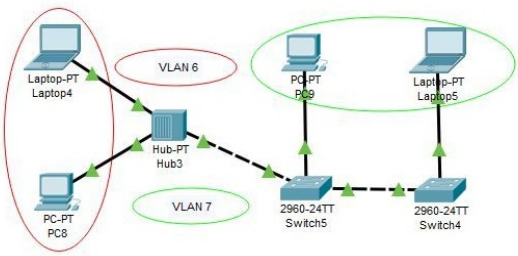
5.3 Вопросы для самопроверки

1. Как расшифровывается аббревиатура VLAN?
2. Какие преимущества есть у технологии VLAN?
3. В чем состоит отличие транковых портов и портов доступа?

5.4 Задание на самостоятельную работу

Используя сеть, созданную в ходе предыдущей работы, надо добавить в нее виртуальные локальные сети. Варианты заданий приведены в таблице 5.2. В отчете, помимо прочего, должны быть приведены скриншоты всплывающих подсказок, возникающих при наведении мыши на коммутаторы.

Таблица 5.2 – Варианты индивидуальных заданий

Вариант	Топология сети
1	
2	
3	

6 СЕМЕЙСТВО ПРОТОКОЛОВ СВЯЗУЮЩЕГО ДЕРЕВА

6.1 Краткая теоретическая справка

STP (Spanning Tree Protocol) – сетевой протокол, а точнее, семейство сетевых протоколов, предназначенных для автоматического удаления петель коммутации из топологии сети на канальном уровне. Первоначально протокол STP описан в стандарте 802.1 d. Позже появились его модификации (RSTP, MSTP, PVST, PVST+), отличающиеся особенностями вычислительных алгоритмов.

В работе использована «классическая» версия протокола. Основным принципом работы протокола является *логическая* блокировка петель при *физической* избыточности топологии. Достигается это с помощью того, что STP отправляет специальные сообщения BPDU и обнаруживает с их помощью фактическую топологию сети. Затем, определяя роли коммутаторов и портов, часть портов блокируется так, чтобы в итоге получить топологию без петель. Для определения того, какие порты должны быть заблокированы, а какие будут передавать данные, STP выполняет следующее:

– выбор корневого коммутатора (Root Bridge);

– определение корневых портов коммутаторов (Root Ports);

– определение выделенных портов коммутаторов (Designated Ports).

Корневым становится коммутатор с наименьшим идентификатором моста (Bridge ID). Только один коммутатор в сети может быть корневым. Для того, чтобы выбрать корневой коммутатор, все коммутаторы отправляют в сеть сообщения BPDU, указывая себя в качестве корневого коммутатора. Если коммутатор получает BPDU от коммутатора с меньшим Bridge ID, то он перестает анонсировать информацию о том, что он корневой и начинает передавать BPDU коммутатора с меньшим Bridge ID. В итоге, только один коммутатор останется корневым и будет передавать BPDU.

Bridge ID (8 байт) состоит из двух полей:

– Приоритет (2 байта) – поле, которое позволяет влиять на выбор корневого коммутатора.

– MAC-адрес (6 байт) – используется как уникальный идентификатор, который, в случае, если приоритеты у двух разных коммутаторов одинаковые, позволяет выбрать корневой коммутатор.

Порт коммутатора, который имеет кратчайший путь к корневому коммутатору, называется корневым портом (Root Port). **У любого не корневого коммутатора может быть только один корневой порт.** Корневой порт выбирается на основе меньшего Root Path Cost – это общее значение стоимости всех соединений до корневого коммутатора.

Если стоимость соединений до корневого коммутатора совпадает, то выбор корневого порта происходит на основе меньшего Bridge ID коммутатора. Если и Bridge ID коммутаторов до корневого коммутатора совпадает, то тогда корневой порт выбирается на основе Port ID.

Коммутатор в сегменте сети, имеющий наименьшее расстояние до корневого коммутатора, называется назначенным (Designated) коммутатором. Порт этого коммутатора, который подключен к рассматриваемому сегменту сети, называется назначенным портом (Designated Port).

Цель работы – изучить особенности функционирования протокола STP.

6.2 Задание на практическую работу

Топология сети, используемая в работе, представлена на рисунке 6.1. Для ее реализации надо использовать коммутаторы 2960-24TT.

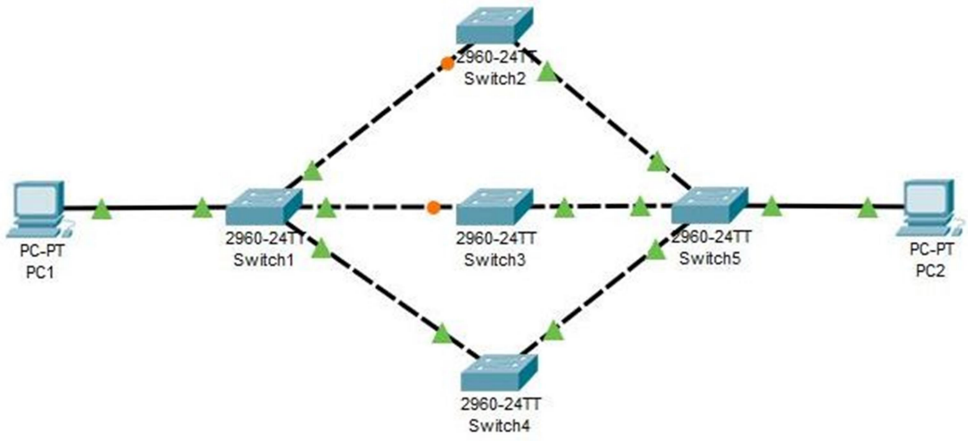


Рисунок 6.1 – Топология сети

После загрузки операционных систем коммутаторов не все их порты находятся в состоянии «Up» ( ), поскольку часть портов находится в режиме блокировки канального уровня ( ). Как известно из работы 3, такое состояние может наблюдаться только на коммутаторах. Оно означает, что порты временно заблокированы для устранения сетевых петель.

Если не блокировать порты в сети из рисунка 6.1, то трафик, передаваемый между PC1 и PC2, распространялся бы по всем возможным соединениям (через Switch2, Switch3 и Switch4), что породило бы существенную дополнительную нагрузку на сеть. Тогда, например, при недоступном (выключенном) компьютере PC2, весь трафик для него беспорядочно бы циркулировал через коммутаторы, что привело бы к широковещательному шторму, вплоть до полной «парализации» работы сети. В этом и состоит главная суть протокола STP. При его использовании коммутаторы отключают порты таким образом, чтобы трафик в каждый сегмент сети передавался только по одному соединению. Важно отметить, что при каждом новом построении сети могут быть отключены другие порты, а не те, которые показаны отключенными на рисунке 6.1. Поясним, от чего это зависит.

Сначала надо самостоятельно определить, какой из коммутаторов является **Root Bridge**, для каждого из коммутаторов определить типы его портов (**Root** или **Designated**).

Для проверки правильности полученных результатов надо выполнить на каждом коммутаторе команду «**show spanning-tree**» (рисунок 6.2). В результате ее выполнения будет отображена таблица, в которой приведены номера портов, их тип (**Root** – корневой, **Desg** – Designated, назначенный или **Altn** – альтернативный, резервный), их статус (**BLK** – Block, заблокирован или **FWD** – forward, доступен) и **стоимость**.

```
Interface        Role Sts Cost
---------------- ---- --- ---------
Fa0/1            Desg FWD 19
Fa0/2            Desg FWD 19
Fa0/3            Root FWD 19
Fa0/10           Desg FWD 19
```

Рисунок 6.2 – Результат выполнения команды «show spanning-tree»

Также над таблицей, в поле **Root ID**, можно увидеть данные корневого коммутатора, а в поле **Bridge ID** – данные текущего коммутатора, включая их приоритеты и MAC-адреса. На корневом коммутаторе можно увидеть надпись «**This bridge is the root**».

Используя полученные результаты, надо нанести на схему сети номера и типы портов, а также стоимости. Проанализировать работу STP при изменении приоритетов коммутаторов и их портов. Для этого изменения использовать 2 способа:

– поменять порты двух соседних коммутаторов с FastEthernet на GigabitEthernet (для изменения стоимости);

– при помощи команды изменения приоритета (в режиме глобальной конфигурации) «**spanning-tree vlan 1 priority #**», где # – приоритет (одно из возможных значений – 0; 4096; 8192; 12288; 16384; 20480; 24576; 28672; 32768; 36864; 40960; 45056; 49152; 53248; 57344; 61440).

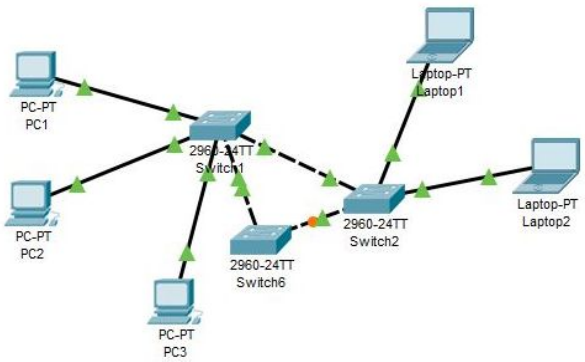
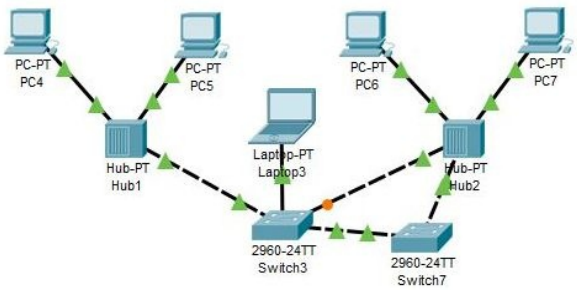
6.3 Вопросы для самопроверки

1. Что такое «широковещательный шторм»?
2. Какие есть преимущества логического блокирования петель при помощи протокола STP по сравнению с физическим устранением петель?
3. В каких случаях заблокированный при помощи протокола STP порт будет разблокирован и начнет передавать полезные данные?

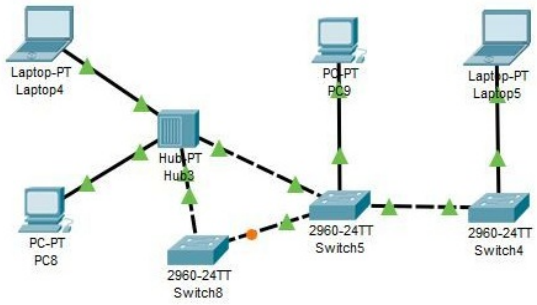
6.4 Задание на самостоятельную работу

Варианты заданий приведены в таблице 6.1. Необходимо доработать сеть из прошлой работы в соответствии с выданным преподавателем вариантом задания (таблица 6.1), добавив в нее еще один коммутатор для получения сетевой петли и проанализировать работу протокола STP. В отчете привести скриншоты сетей с отображенными на них номерами и типами портов, а также их стоимостью.

Таблица 6.1 – Варианты индивидуальных заданий

Вариант	Топология сети
1	
2	

Продолжение таблицы 6.1

3	

7 АГРЕГИРОВАНИЕ КАНАЛОВ

7.1 Краткая теоретическая справка

Прикладной
Представления
Сеансовый
Транспортный
Сетевой
Канальный
Физический

Агрегирование каналов (link aggregation) – технология объединения нескольких параллельных каналов передачи данных Ethernet в один логический, позволяющая увеличить пропускную способность и повысить надёжность сетей.

В терминологии компании Cisco технология агрегирования каналов называется EtherChannel. Существует 2 протокола, позволяющие автоматически создавать и обслуживать каналы EtherChannel:

– PAgP (проприетарный протокол компании Cisco);

– LACP (протокол из стандарта IEEE 802.3 ad).

Поскольку протокол LACP является стандартом IEEE, его можно использовать для создания EtherChannel на оборудования различных производителей, а протокол PAgP будет работать только на оборудовании компании Cisco.

Все порты для агрегирования, как правило, выбираются одного типа и одной скорости. По стандарту 802.3 ad комбинировать порты с разной скоростью допустимо, но на практике такие конфигурации зачастую оказываются неработоспособными.

Агрегирование имеет ограничения. Так, распределение трафика по каналам может быть неравномерным, вплоть до того, что весь трафик идёт по одному каналу. Кроме того, объединять можно не более восьми каналов.

Цель работы – изучить особенности агрегирования каналов по протоколам PAgP и LACP.

7.2 Задание на практическую работу

Для изучения агрегирования каналов надо построить сеть, состоящую из трех коммутаторов (2960-24TT) и двух ноутбуков. Топология сети и номера портов приведены на рисунке 7.1.

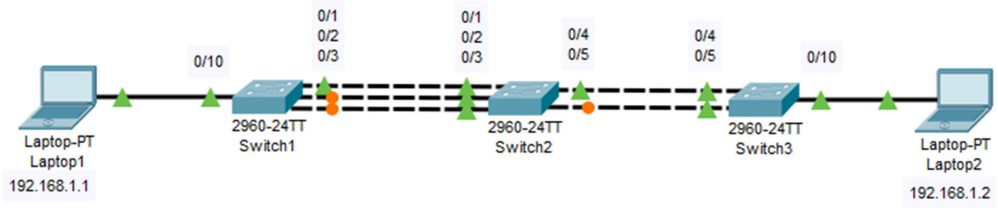


Рисунок 7.1 – Топология сети для изучения агрегирования каналов

Для настройки агрегирования каналов по протоколу LACP между коммутаторами Switch1 и Switch2 надо выполнить следующие команды на обоих коммутаторах:

```
Switch>enable
Switch#configure terminal
Switch(config)#interface range fastEthernet 0/1, fastEthernet 0/2, fastEthernet 0/3
```

Затем на коммутаторе Switch1 выполнить:

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

На коммутаторе Switch2 выполнить:

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

Последние команды создают логические интерфейсы «Port Channel», если они не существовали, и привязывают к ним перечисленные физические интерфейсы (порты) коммутаторов. Единица является номером группы каналов. Активный режим (**mode active**) включает LACP на интерфейсе постоянно, т.е. коммутатор в любом случае является источником LACP пакетов. Пассивный режим (**mode passive**) включает LACP только тогда, когда обнаружено поступление LACP пакетов от другой стороны.

Далее надо настроить агрегирование каналов по протоколу PAgP между коммутаторами Switch2 и Switch3, выполнив следующие команды на обоих коммутаторах:

```
Switch>enable
Switch#configure terminal
Switch(config)#interface range fastEthernet 0/4, fastEthernet 0/5
```

На коммутаторе Switch2 выполнить:

```
Switch(config-if-range)#channel-group 2 mode auto
```

На коммутаторе Switch3 выполнить:

```
Switch(config-if-range)#channel-group 2 mode desirable
```

В последних командах автоматический режим (**mode auto**) включает PAgP, причем коммутатор пассивно ожидает подключения со стороны соседнего коммутатора. Желательный режим (**mode desirable**) включает PAgP, причем коммутатор активно пытается подключиться к соседнеми коммутатору.

Для проверки правильности настроек выполнить:

```
Switch>show etherchannel summary
```

После выполнения команды отобразится таблица, содержащая номер группы, название протокола и номера портов, которые входят в логический интерфейс «Port Channel» (рисунок 7.2).

```
Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------

1      Po1(SU)           LACP   Fa0/1(P) Fa0/2(P) Fa0/3(P)
```

Рисунок 7.2 – Результат команды «show etherchannel summary»

Используя команду «show etherchannel port-channel» можно просмотреть подробную информацию о логическом интерфейсе «Port Channel» (для вывода полной информации надо многократно нажимать клавишу «Enter»).

7.3 Вопросы для самопроверки

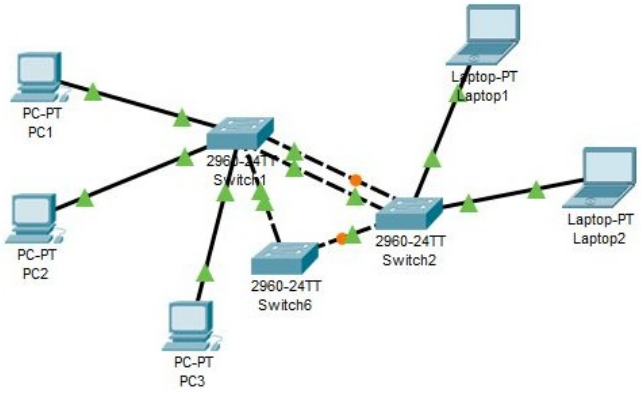
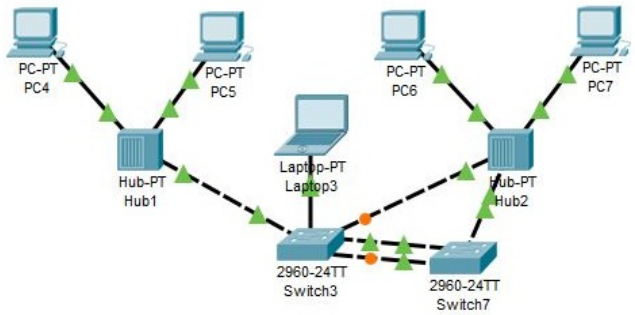
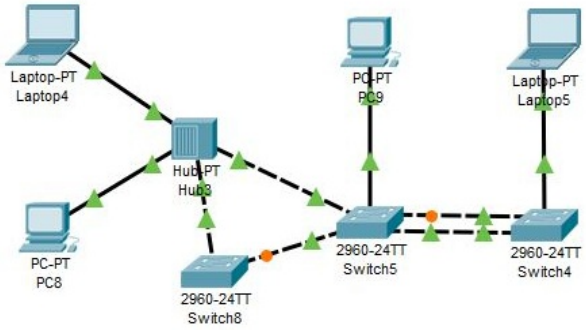
1. В чем различия протоколов LACP и PAgP?
2. Чем отличаются режимы active, passive, auto и desirable?
3. Для чего используют агрегирование каналов?

7.4 Задание на самостоятельную работу

В ходе индивидуального задания надо доработать сеть из прошлой работы в соответствии с выданным преподавателем вариантом (таблица 7.1), добавив в нее

параллельные каналы и настроив их агрегирование. В отчете привести скриншоты сетей с отображенными на них номерами портов, а также скриншоты выполнения команд «**show etherchannel summary**» и «**show etherchannel port-channel**» на всех коммутаторах.

Таблица 7.1 – Варианты индивидуальных заданий

Вариант	Топология сети
1	
2	
3	

8 БЕСКЛАССОВАЯ IP-АДРЕСАЦИЯ

8.1 Краткая теоретическая справка

IP-адрес (Internet protocol address) – уникальный сетевой адрес узла в компьютерной сети, построенной по протоколу IP.

В версии протокола IPv4 IP-адрес имеет длину 4 байта (32 бита). Удобной формой записи IP-адреса является запись в виде четырёх десятичных чисел (октетов) значением от 0 до 255 каждое, разделённых точками, например, 10.11.254.3.

Существует 2 вида IPv4-адресации: классовая и бесклассовая. Исторически первой стала применяться классовая адресация. Адрес в ней состоит из двух логических частей – номера сети и номера узла в сети. Какая часть адреса относится к номеру сети, а какая к номеру узла, определяется значениями первых битов адреса. Всего существует пять классов адресов: A, B, C, D и E. Со второй половины 90-х годов XX века классовая адресация была вытеснена бесклассовой адресацией (CIDR), при которой количество адресов в сети определяется маской подсети.

Маска подсети – битовая маска, определяющая, какая часть IP-адреса узла сети относится к адресу сети, а какая – к адресу самого узла в этой сети. Например, узел с IP-адресом 12.34.56.78 и маской подсети 255.255.255.0 находится в сети 12.34.56.0.

Чаще всего маску подсети записывают вместе с IP-адресом в формате «IP-адрес/количество единичных бит в маске». Число после знака дроби (т. н. длина префикса сети) означает количество единичных разрядов в маске подсети.

В данной практической работе рассматриваются основы бесклассовой IP-адресации и правила разделения IP-сетей на подсети.

Цель работы – освоить правила деления IP-сетей с использованием маски подсети.

8.2 Задание на практическую работу

Рассмотрим пример записи IP-адреса

10.96.0.0/**11**.

Здесь маска подсети имеет двоичный вид

11111111.11100000.00000000.00000000,

или в десятичном

255.224.0.0.

Одиннадцать разрядов IP-адреса отводятся под адрес сети, а остальные (32–11=21) разряды адреса – под локальный адрес в этой сети. Тогда минимальным адресом будет

10.96.0.0 или 00001010.011**00000.00000000.00000000**,

а максимальным

10.127.255.255 или 00001010.011**11111.11111111.11111111**.

Начальный (минимальный) адрес сети резервируется для идентификации подсети, а последний (максимальный) – в качестве ее широковещательного адреса (адреса для передачи информации на все устройства в подсети).

В результате, число доступных адресов узлов в этой подсети составляет 2 097 150 (от 10.96.0.1 до 10.127.255.254), что вычисляется как $2^{(32-11)}-2$.

8.3 Вопросы для самопроверки

1. В чем различия между классовой и бесклассовой адресациями?

2. Как определить число адресов в подсети?

3. Какие из IP-адресов не являются допустимыми для назначения узлу: 23.75.345.200, 216.27.61.134, 102.54.94, 255.255.255.255, 142.179.148.200, 200.42.129.16, 0.124.0.0, 127.0.0.1?

8.4 Задание на самостоятельную работу

Для заданного IP-адреса 152.185.98.54 надо определить номера сети и узла. Маску подсети выбрать в соответствии с выданным преподавателем вариантом (таблица 8.1). Затем для подсети в соответствии с выданным преподавателем вариантом задания (таблица 8.2) необходимо указать: маску подсети в двоичном и десятичном видах, адрес сети и широковещательный адрес, число адресов для узлов и их минимальный и максимальный адреса. Далее надо разбить выделенную сеть (таблица 8.3) на 4 равных подсети и указать для каждой из них число узлов и их минимальный и максимальный IP-адреса. Наконец, разбить выделенную сеть (таблица 8.4) на 3 подсети наиболее экономичным способом при заданном числе узлов в каждой подсети. Надо указать для каждой подсети распределение адресного пространства, а также резерв адресов.

Кроме того, надо выполнить творческую работу по созданию инфографики по теме «IP-адресация». В этом задании надо показать своё видение по наилучшему пониманию темы «IP-адресация», разработав инфографику с наглядным отображением важной информации для понимания этой темы. Пример инфографики приведен в приложении А. Также рекомендуется оценить не менее 5 работ одногруппников.

Таблица 8.1 – Варианты индивидуальных заданий

Вариант	Значение маски подсети
1	/15
2	/18
3	/20
4	/25
5	/28

Таблица 8.2 – Варианты индивидуальных заданий

Вариант	IP-адрес и маска подсети
1	10.10.13.0/30
2	192.168.113.0/28
3	172.25.0.0/23
4	192.168.13.0/25
5	10.96.100.0/26

Таблица 8.3 – Варианты индивидуальных заданий

Вариант	IP-адрес и маска подсети
1	172.17.0.0/16
2	146.87.0.0/16
3	183.37.0.0/16
4	156.98.0.0/16
5	165.42.0.0/16

Таблица 8.4 – Варианты индивидуальных заданий

Вариант	IP-адрес	Число узлов		
		N_1	N_2	N_3
1	192.168.17.0/24	20	15	50
2	192.168.255.0/24	50	28	4
3	192.168.95.0/24	90	60	10
4	192.168.150.0/24	80	20	32
5	192.168.192.0/24	2	61	100

9 СТАТИЧЕСКАЯ МАРШРУТИЗАЦИЯ

9.1 Краткая теоретическая справка

Прикладной
Представления
Сеансовый
Транспортный
Сетевой
Канальный
Физический

Статическими маршрутами являются маршруты к сетям получателя, которые администратор сети вручную вносит в таблицы маршрутизации. Такие маршруты определяют IP-адрес соседнего маршрутизатора или, точнее, локальный выходной интерфейс соседнего маршрутизатора, который используется для направления трафика к сети получателя.

Статический маршрут не может быть автоматически адаптирован к изменениям в топологии сети. Так, если определенный в маршруте маршрутизатор или его интерфейс становятся недоступными, то маршрут становиться нерабочим. Преимуществом статической маршрутизации является то, что исключается весь служебный трафик, связанный с поддержкой и корректировкой маршрутов.

Статическая маршрутизация часто используется, когда:

– администратор нуждается в полном контроле маршрутов;

– необходимо организовать резервирование динамических маршрутов;

– есть сети, достижимые единственно возможным маршрутом;

– нежелательно иметь служебный трафик, необходимый для обновления таблиц маршрутизации;

– используются устаревшие маршрутизаторы, не имеющие необходимого уровня вычислительных возможностей для поддержки динамических протоколов маршрутизации.

Наиболее предпочтительной топологией для использования статической маршрутизации является топология «звезда». Тогда маршрутизаторы, подключенные к центральному узлу сети, имеют только один маршрут для всего трафика, который будет проходить через этот узел. Недостаток статической маршрутизации заключается в том, что со временем сеть может быть расширена за счет установки дополнительных маршрутизаторов с произвольным числом подключенных к ним подсетей. Тогда, число статических маршрутов в таблицах маршрутизации увеличивается пропорционально числу маршрутизаторов в сети. Так, при добавлении новой подсети или маршрутизатора администратор должен добавлять новые маршруты в таблицы маршрутизации на всех маршрутизаторах. При таком подходе может наступить момент, когда большую часть своего рабочего времени администратор будет заниматься поддержкой таблиц маршрутизации в сети. В этом случае необходимо сделать выбор в сторону использования динамических протоколов маршрутизации.

Цель работы – изучить особенности работы и настройки статической маршрутизации.

9.2 Задание на практическую работу

В работе используется топология сети, представленная на рисунке 9.1 (используются маршрутизаторы 2811).

Рисунок 9.1 – Топология сети для изучения статической маршрутизации

При настройке используются следующие IP-адреса и основные шлюзы (рисунок 9.2):
– PC1: IP – 192.168.10.10/24, default gateway – 192.168.10.1;
– PC2: IP – 192.168.110.10/24, default gateway – 192.168.110.1.

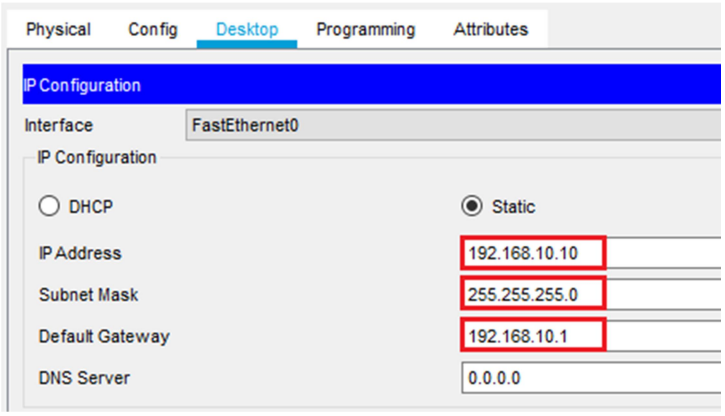


Рисунок 9.2 – Настройка IP-адресации компьютера PC1

Основной шлюз (Default gateway) – это сетевой адрес интерфейса маршрутизатора, в задачи которого входит передача сетевого трафика из одной локальной сети в другую.

Далее надо задать IP-адреса интерфейсам маршрутизатора в соответствии с рисунком 9.3.

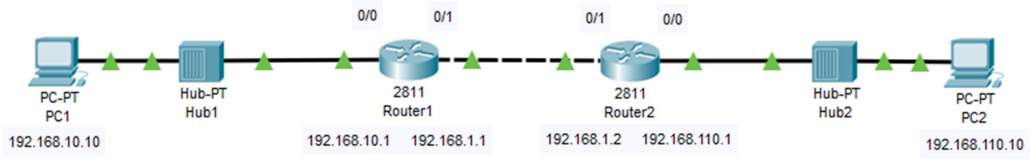


Рисунок 9.3 – Топология сети с указанием IP-адресов

Для настройки маршрутизатора Router1 надо перейти в режим настройки интерфейса:

```
Router>enable
Router#configure terminal
Router(config)#interface FastEthernet0/0
```

Включить выбранный интерфейс (порт)

```
Router(config-if)#no shutdown
```

Задать интерфейсу IP-адрес и маску подсети /24

```
Router(config-if)#ip address 192.168.10.1 255.255.255.0
Router(config-if)#exit
```

Аналогичные действия надо проделать на другом интерфейсе маршрутизатора:

```
Router(config)#interface FastEthernet0/1
Router(config-if)#no shutdown
Router(config-if)#ip address 192.168.1.1 255.255.255.0
```

После настройки маршрутизатора Router1 надо настроить IP-адреса интерфейсам маршрутизатора Router2 (IP-адреса указаны на рисунке 9.3).

На следующем этапе нужно проверить связь между PC2 и PC1 и определить, есть ли связь между компьютерами. Так как не настроена маршрутизация, то связь должна отсутствовать.

Для настройки статической маршрутизации на маршрутизаторе Router1 надо прописать маршрут

```
Router(config)#ip route 192.168.110.0 255.255.255.0 192.168.1.2
```

Аналогично прописать маршрут на маршрутизаторе Router2:

```
Router(config)#ip route 192.168.10.0 255.255.255.0 192.168.1.1
```

Команда «ip route» задает статический маршрут на маршрутизаторе. В ней сначала необходимо указать <имя (номер) сети назначения> и <ее маску>, а затем <адрес интерфейса> соседнего маршрутизатора.

После настройки надо повторно проверить связь между PC2 и PC1. Если связь не появилась, то надо проверить правильность выполнения всех предыдущих пунктов, иначе надо выполнить на каждом маршрутизаторе команду «show ip route», проанализировать и расшифровать полученную с ее помощью информацию.

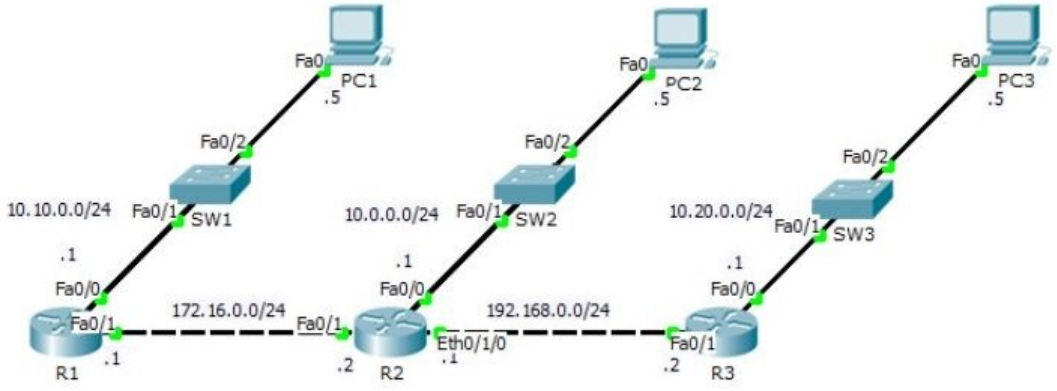
9.3 Вопросы для самопроверки

1. Перечислите достоинства и недостатки статической маршрутизации.
2. Каков синтаксис команды «ip route»?
3. Что такое «default gateway»?

9.4 Задание на самостоятельную работу

При выполнении индивидуального задания надо настроить статическую маршрутизацию для сети в соответствии с выданным преподавателем вариантом задания (таблица 9.1). В отчете привести статические маршруты и подтверждения доступности всех устройств в сети при помощи команды «ping».

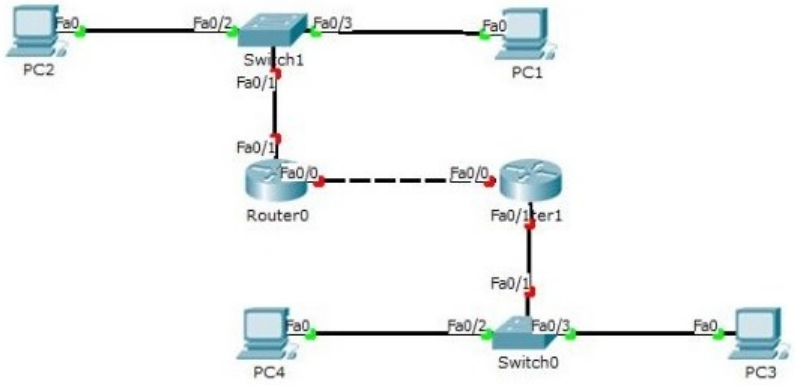
Таблица 9.1 – Варианты индивидуальных заданий

<table>
<tr><th>Вариант</th><th>Топология сети с указанием IP-адресов интерфейсов</th></tr>
<tr><td>1*</td><td>


<table>
<tr><th>Устройство</th><th>Порт</th><th>IP-адрес</th><th>Шлюз по умолчанию</th></tr>
<tr><td>PC1</td><td>Fa0</td><td>10.10.0.5/24</td><td>10.10.0.1</td></tr>
<tr><td>PC2</td><td>Fa0</td><td>10.0.0.5/24</td><td>10.0.0.1</td></tr>
<tr><td>PC3</td><td>Fa0</td><td>10.20.0.5/24</td><td>10.20.0.1</td></tr>
<tr><td>R1</td><td>Fa0/0</td><td>10.10.0.1/24</td><td>-</td></tr>
<tr><td>R1</td><td>Fa0/1</td><td>172.16.0.1/24</td><td>-</td></tr>
<tr><td>R2</td><td>Fa0/1</td><td>172.16.0.2/24</td><td>-</td></tr>
<tr><td>R2</td><td>Fa0/0</td><td>10.0.0.1/24</td><td>-</td></tr>
<tr><td>R2</td><td>Fa1/0</td><td>192.168.0.1/24</td><td>-</td></tr>
<tr><td>R3</td><td>Fa0/1</td><td>192.168.0.2/24</td><td>-</td></tr>
<tr><td>R3</td><td>Fa0/0</td><td>10.20.0.1/24</td><td>-</td></tr>
</table>
</td></tr>
</table>

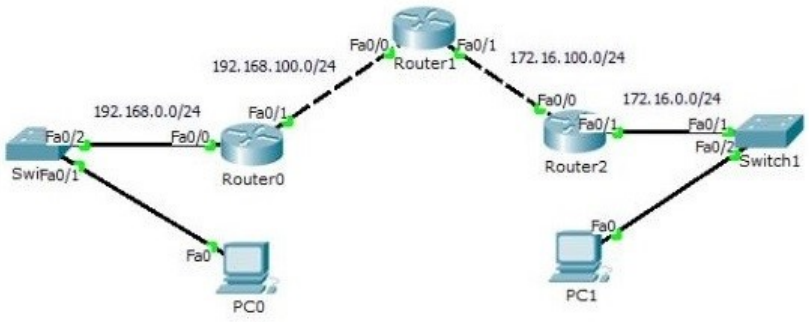
Продолжение таблицы 9.1

2



Устройство	Порт	IP-адрес	Шлюз по умолчанию
PC1	Fa0	192.168.100.25/27	192.168.100.1
PC2	Fa0	192.168.100.26/27	192.168.100.1
PC3	Fa0	192.168.200.25/27	192.168.200.1
PC4	Fa0	192.168.200.26/27	192.168.200.1
Router0	Fa0/1	192.168.100.1/24	-
Router0	Fa0/0	172.16.16.1/24	-
Router1	Fa0/1	192.168.200.1/24	-
Router1	Fa0/0	172.16.16.2/24	-

3



Устройство	Порт	IP-адрес	Шлюз по умолчанию
PC0	Fa0	192.168.0.2/24	192.168.0.1
PC1	Fa0	172.16.0.2/24	172.16.0.1
Router0	Fa0/0	192.168.0.1/24	-
Router0	Fa0/1	192.168.100.2/24	-
Router1	Fa0/0	192.168.100.1/24	-
Router1	Fa0/1	172.16.100.1/24	-
Router2	Fa0/0	172.16.100.2/24	-
Router2	Fa0/1	172.16.0.1/24	-

* Примечания к варианту задания 1. В работе надо на маршрутизаторе R2 задействовать 3 порта (по умолчанию доступно всего 2). Для добавления дополнительных портов надо (рисунок 9.4):

1 отключить питание маршрутизатора соответствующим переключателем;

2 добавить к маршрутизатору модуль расширения «NM-2FE2W» (или «NM-1FE2W») путем его перетаскивания в нужное место;

3 включить питание маршрутизатора и дождаться его загрузки.

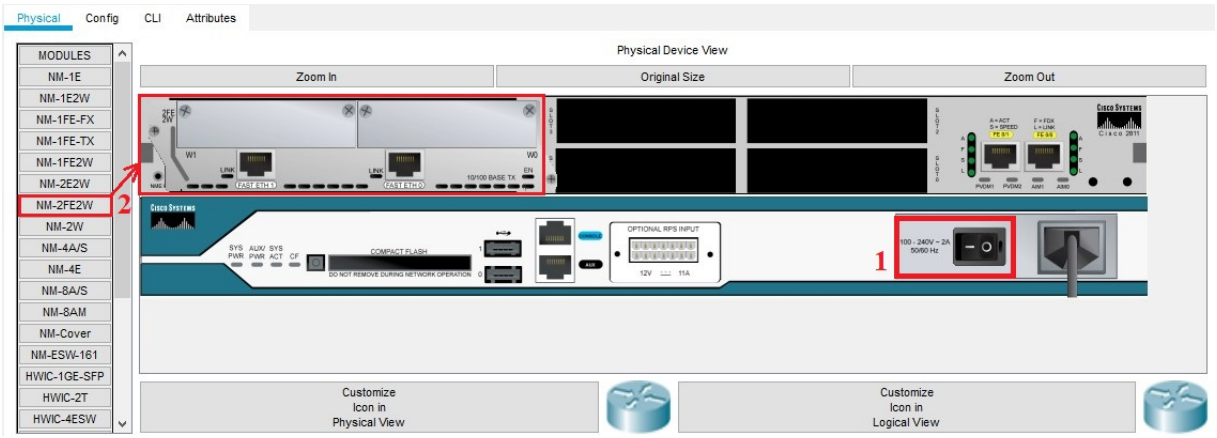


Рисунок 9.4 – Добавление модуля расширения «NM-2FE2W» в маршрутизатор 2811

10 ДИНАМИЧЕСКАЯ МАРШРУТИЗАЦИЯ RIP

10.1 Краткая теоретическая справка

Прикладной
Представления
Сеансовый
Транспортный
Сетевой
Канальный
Физический

Динамическая маршрутизация – это маршрутизация, при которой таблица маршрутизации заполняется и редактируется автоматически. Для динамической маршрутизации используются протоколы RIP, OSPF, BGP, IS-IS.

Одним из простых протоколов динамической маршрутизации является RIP (Routing information protocol, протокол маршрутной информации). Протокол RIP первоначально определен в документе RFC 1058. Наиболее существенны следующие его характеристики:

– в качестве метрики при выборе маршрута используется число переходов (хопов);

– максимальная длина маршрута равняется 15 переходам;

– по умолчанию обновления маршрутной информации рассылаются широковещательным способом.

При работе протокола RIP используется протокол UDP (транспортный уровень модели OSI). Все устройства, поддерживающие RIP, прослушивают UDP порт 520 и осуществляют передачу через него.

В качестве метрики для определения наилучшего маршрута протокол RIP использует расстояние (чем короче маршрут, тем он лучше). Если к пункту назначения существует множество маршрутов, то маршрутизаторы, поддерживающие протокол RIP, выбирают из них кротчайший и записывают его в таблицу маршрутизации. Протокол RIP предотвращает появление петель в маршрутизации, устанавливая максимальное число переходов на маршруте от отправителя к получателю (стандартное значение – 15). При получении маршрутизатором обновления маршрутной информации, содержащего новую или измененную запись, он увеличивает значение метрики на единицу. Если при этом значение метрики превышает 15, то метрика считается бесконечно большой, а маршрут до сети получателя недостижимым.

Цель работы – изучить особенности работы протокола RIP.

10.2 Задание на практическую работу

В работе используется топология сети, представленная на рисунке 10.1. Сначала надо задать компьютерам и маршрутизаторам IP-адреса, компьютерам также основные шлюзы.

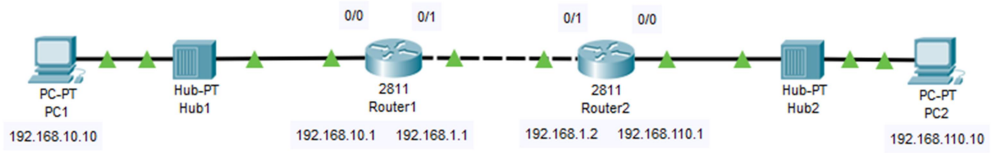


Рисунок 10.1 – Топология сети

Для настройки динамической маршрутизации на маршрутизаторе Router1 надо выполнить:

```
Router(config)#router rip
```

Активировать вторую (более современную) версию протокола

```
Router(config-router)#version 2
```

Перечислить сети (без масок), маршрутизацию между которыми надо осуществлять

```
Router(config-router)#network 192.168.10.0
Router(config-router)#network 192.168.1.0
```

Отключить автосуммаризацию маршрутов

```
Router(config-router)#no auto-summary
```

Маршрутизатор Router2 настраивается аналогичным образом

```
Router(config)#router rip
Router(config-router)#version 2
Router(config-router)#network 192.168.1.0
Router(config-router)#network 192.168.110.0
Router(config-router)#no auto-summary
```

Проверить связь между PC2 и PC1 с помощью команды «ping». Затем надо выполнить на каждом маршрутизаторе команду «show ip route», проанализировать и расшифровать полученную информацию.

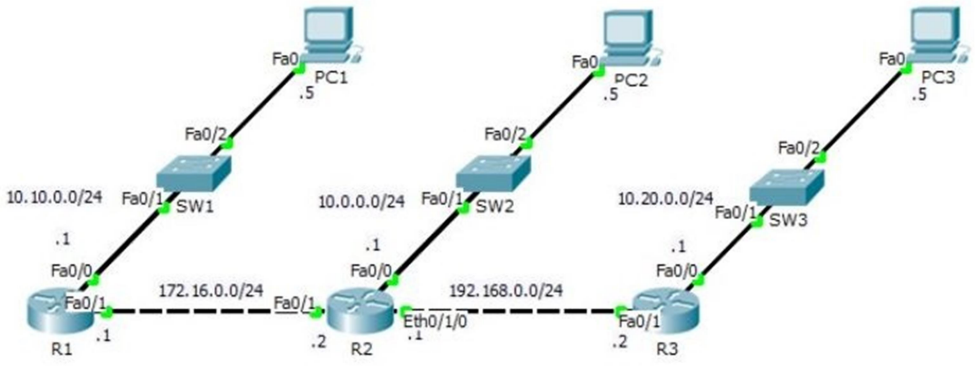
10.3 Вопросы для самопроверки

1. В чем заключаются различия между статической и динамической маршрутизацией?
2. В чем состоят достоинства и недостатки протокола RIP?
3. Что такое метрика и для чего она используется?

10.4 Задание на самостоятельную работу

В ходе выполнения индивидуального задания надо настроить динамическую маршрутизацию RIP v2 для сети в соответствии с выданным преподавателем вариантом (таблица 10.1).

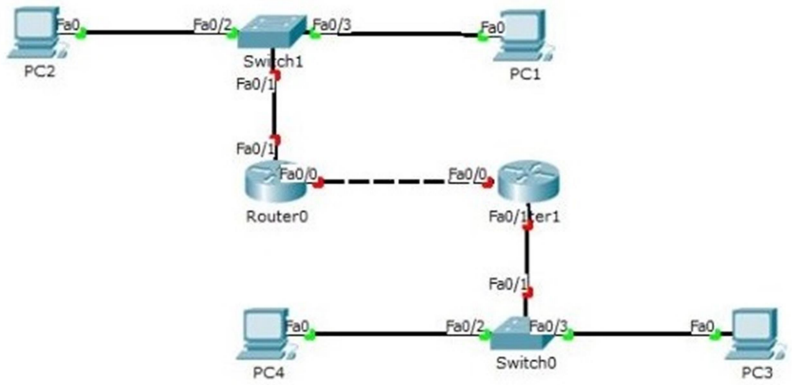
Таблица 10.1 – Варианты индивидуальных заданий

Вариант	Топология сети с указанием IP-адресов интерфейсов
1	

Устройство	Порт	IP-адрес	Шлюз по умолчанию
PC1	Fa0	10.10.0.5/24	10.10.0.1
PC2	Fa0	10.0.0.5/24	10.0.0.1
PC3	Fa0	10.20.0.5/24	10.20.0.1
R1	Fa0/0	10.10.0.1/24	-
R1	Fa0/1	172.16.0.1/24	-
R2	Fa0/1	172.16.0.2/24	-
R2	Fa0/0	10.0.0.1/24	-
R2	Fa1/0	192.168.0.1/24	-
R3	Fa0/1	192.168.0.2/24	-
R3	Fa0/0	10.20.0.1/24	-

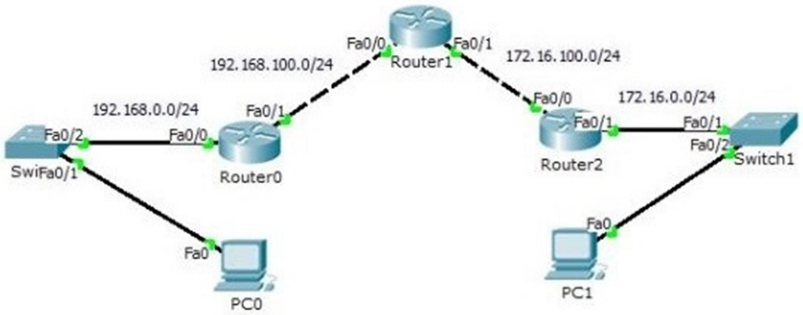
Продолжение таблицы 10.1

2



Устройство	Порт	IP-адрес	Шлюз по умолчанию
PC1	Fa0	192.168.100.25/27	192.168.100.1
PC2	Fa0	192.168.100.26/27	192.168.100.1
PC3	Fa0	192.168.200.25/27	192.168.200.1
PC4	Fa0	192.168.200.26/27	192.168.200.1
Router0	Fa0/1	192.168.100.1/24	-
Router0	Fa0/0	172.16.16.1/24	-
Router1	Fa0/1	192.168.200.1/24	-
Router1	Fa0/0	172.16.16.2/24	-

3



Устройство	Порт	IP-адрес	Шлюз по умолчанию
PC0	Fa0	192.168.0.2/24	192.168.0.1
PC1	Fa0	172.16.0.2/24	172.16.0.1
Router0	Fa0/0	192.168.0.1/24	-
Router0	Fa0/1	192.168.100.2/24	-
Router1	Fa0/0	192.168.100.1/24	-
Router1	Fa0/1	172.16.100.1/24	-
Router2	Fa0/0	172.16.100.2/24	-
Router2	Fa0/1	172.16.0.1/24	-

11 ДИНАМИЧЕСКАЯ МАРШРУТИЗАЦИЯ OSPF

11.1 Краткая теоретическая справка

OSPF (Open shortest path first) – протокол динамической маршрутизации, основанный на технологии отслеживания состояния канала (link-state technology) и использующий для нахождения кратчайшего пути алгоритм Дейкстры. Протокол разработан в 1988 году (последняя версия представлена в RFC 2328). OSPF является протоколом внутреннего шлюза, распространяющим информацию о доступных маршрутах между маршрутизаторами одной автономной системы. Для того чтобы понять, каким образом работает протокол OSPF, необходимо ознакомиться с используемой терминологией:

- *Объявление о состоянии канала* (link-state advertisement, LSA) содержит описание всех каналов маршрутизатора, всех интерфейсов и состояний каналов.
- *Состояние канала* (link state) – состояние канала между двумя маршрутизаторами.
- *Метрика* (metric) – условный показатель «стоимости» пересылки данных по каналу.
- *Автономная система* (autonomous system) – группа маршрутизаторов, обменивающихся маршрутной информацией.
- *Зона* (area) – совокупность сетей и маршрутизаторов, имеющих один и тот же идентификатор зоны.
- *Соседи* (neighbours) – два маршрутизатора, имеющие интерфейсы в общей сети.
- *Состояние смежности* (adjacency) – взаимосвязь между соседними маршрутизаторами, установленная с целью обмена маршрутной информацией.
- *Hello-протокол* (hello protocol) – протокол, используемый для поддержания «соседских отношений».
- *База данных соседей* (neighbours database) – список всех соседей.
- *База данных состояния каналов* (link state database, LSDB) – список всех записей о состоянии каналов.
- *Идентификатор маршрутизатора* (router ID, RID) – уникальное 32-битовое число для идентификации маршрутизатора в пределах одной автономной системы.

Принцип работы протокола OSPF:

1. Маршрутизаторы обмениваются hello-пакетами через все интерфейсы, на которых активирован протокол OSPF. Маршрутизаторы, разделяющие общий канал передачи данных, становятся соседями, когда они «приходят к договоренности» об определённых параметрах, указанных в их hello-пакетах.
2. Маршрутизаторы пытаются перейти в состояние смежности со своими соседями. Переход в состояние смежности определяется типом маршрутизаторов и типом сети, по которой передаются hello-пакеты. OSPF определяет несколько типов сетей и несколько типов маршрутизаторов. Пара маршрутизаторов, находящихся в состоянии смежности, синхронизирует свои базы данных состояния каналов.
3. Каждый маршрутизатор посылает объявления о состоянии канала маршрутизаторам, с которыми он находится в состоянии смежности.
4. Каждый маршрутизатор, получивший объявление от смежного маршрутизатора, записывает передаваемую в нём информацию в свою базу данных состояния каналов и рассылает ее копию всем другим смежным с ним маршрутизаторам.

5. Рассылая объявления внутри одной OSPF-зоны, все маршрутизаторы строят идентичную базу данных состояния каналов.

6. Когда база данных сформирована, каждый маршрутизатор использует алгоритм «первый кратчайший путь» для вычисления графа без потерь, который будет описывать кратчайший путь к каждому известному пункту назначения. Полученный граф – дерево кратчайших путей.

7. Каждый маршрутизатор строит таблицу маршрутизации из своего дерева кратчайших путей.

Цель работы – изучить особенности работы протокола OSPF.

11.2 Задание на практическую работу

В работе используется топология сети, представленная на рисунке 11.1. Сначала надо задать компьютерам и маршрутизаторам IP-адреса, компьютерам также основные шлюзы.

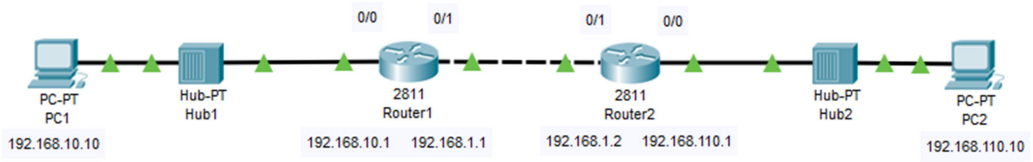


Рисунок 11.1 – Топология сети

Настроить динамическую маршрутизацию OSPF. На маршрутизаторе Router1 для этого выполнить

```
Router(config)#router ospf 1
```

В этой команде единица – это идентификатор номера процесса. Вместо единицы может стоять число от 1 до 65535. Далее надо перечислить сети (с обратными масками), маршрутизация между которыми будет осуществляться

```
Router(config-router)#network 192.168.10.0 0.0.0.255 area 0
Router(config-router)#network 192.168.1.0 0.0.0.255 area 0
```

Обратная маска – это инвертированная в двоичной форме записи маска подсети. Так, маска /24 имеет вид

11111111.11111111.11111111.00000000,

а ее обратная маска –

00000000.00000000.00000000.11111111.

В десятичном виде обратную маску можно получить путем вычитания маски подсети из маски 255.255.255.255. Например,

255.255.255.255 – 255.255.255.0 = 0.0.0.255.

Далее надо задать идентификатор маршрутизатора, иначе он будет присвоен автоматически (им станет наибольший IP-адрес интерфейсов из всех активных)

```
Router(config-router)#router-id 1.1.1.1
```

В привилегированном режиме надо перезапустить процесс OSPF

```
Router#clear ip ospf process
Reset ALL OSPF processes? [no]:yes
```

Аналогичным образом надо настроить маршрутизатор Router2:

```
Router(config)#router ospf 1
Router(config-router)#network 192.168.1.0 0.0.0.255 area 0
```

```
Router(config-router)#network 192.168.110.0 0.0.0.255 area 0
Router(config-router)#router-id 2.2.2.2
Router#clear ip ospf process
```

После выполнения всех настроек надо проверить установление соседства на каждом маршрутизаторе с помощью команды «show ip ospf neighbor». Если настройки выполнены некорректно, то надо повторить вышеописанные действия, иначе перейти к настройке пассивных интерфейсов. Для этого запретить пересылать служебную информацию протокола OSPF на интерфейсы, направленные в пользовательскую сеть, в сторону хостов. Так, на маршрутизаторах надо выполнить

```
Router(config)#passive-interface FastEthernet0/0
```

Проверить связь между PC2 и PC1 с помощью команды «ping». Затем надо выполнить на каждом маршрутизаторе команду «show ip route», проанализировать и расшифровать полученную информацию.

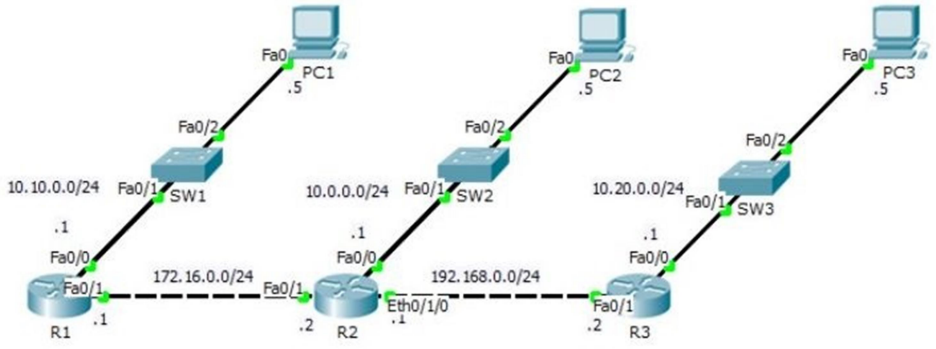
11.3 Вопрос для самопроверки

В чем заключаются сходства и различия протоколов RIP и OSPF, использование какого из них предпочтительней?

11.4 Задание на самостоятельную работу

В ходе выполнения индивидуального задания надо настроить динамическую маршрутизацию OSPF для сети в соответствии с выданным преподавателем вариантом (таблица 11.1). В отчете привести команды для настройки маршрутов, результаты выполнения команды «show ip route» на каждом маршрутизаторе и подтверждения доступности всех устройств (при помощи команды «ping»). Кроме того, надо привести результаты выполнения команды «show ip ospf neighbor».

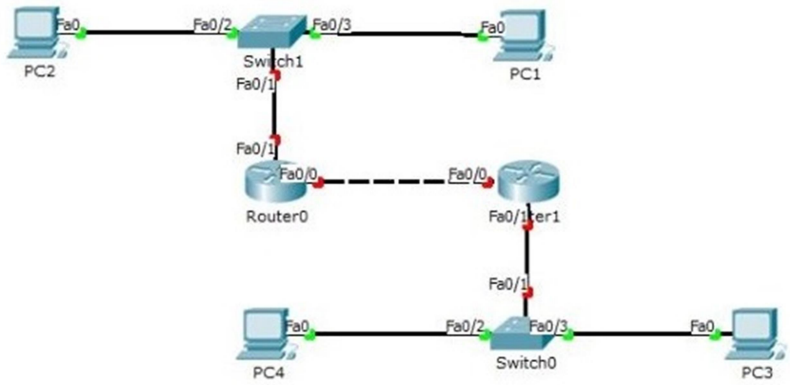
Таблица 11.1 – Варианты индивидуальных заданий

Вариант	Топология сети с указанием IP-адресов интерфейсов
1	

Устройство	Порт	IP-адрес	Шлюз по умолчанию
PC1	Fa0	10.10.0.5/24	10.10.0.1
PC2	Fa0	10.0.0.5/24	10.0.0.1
PC3	Fa0	10.20.0.5/24	10.20.0.1
R1	Fa0/0	10.10.0.1/24	-
R1	Fa0/1	172.16.0.1/24	-
R2	Fa0/1	172.16.0.2/24	-
R2	Fa0/0	10.0.0.1/24	-
R2	Fa1/0	192.168.0.1/24	-
R3	Fa0/1	192.168.0.2/24	-
R3	Fa0/0	10.20.0.1/24	-

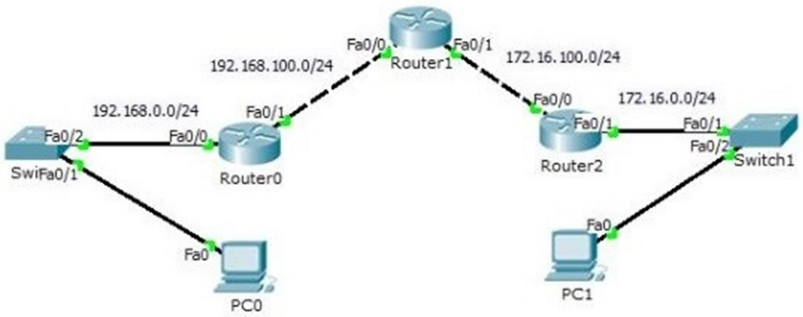
Продолжение таблицы 11.1

2



Устройство	Порт	IP-адрес	Шлюз по умолчанию
PC1	Fa0	192.168.100.25/27	192.168.100.1
PC2	Fa0	192.168.100.26/27	192.168.100.1
PC3	Fa0	192.168.200.25/27	192.168.200.1
PC4	Fa0	192.168.200.26/27	192.168.200.1
Router0	Fa0/1	192.168.100.1/24	-
Router0	Fa0/0	172.16.16.1/24	-
Router1	Fa0/1	192.168.200.1/24	-
Router1	Fa0/0	172.16.16.2/24	-

3



Устройство	Порт	IP-адрес	Шлюз по умолчанию
PC0	Fa0	192.168.0.2/24	192.168.0.1
PC1	Fa0	172.16.0.2/24	172.16.0.1
Router0	Fa0/0	192.168.0.1/24	-
Router0	Fa0/1	192.168.100.2/24	-
Router1	Fa0/0	192.168.100.1/24	-
Router1	Fa0/1	172.16.100.1/24	-
Router2	Fa0/0	172.16.100.2/24	-
Router2	Fa0/1	172.16.0.1/24	-

12 ПЕРЕЧНИ ВОПРОСОВ ДЛЯ ТЕКУЩЕГО И ИТОГОВОГО КОНТРОЛЯ

В данном разделе приведены перечни вопросов для подготовки к текущему (контрольные задания) и итоговому (зачёт) контролю.

12.1 Контрольные задания

1. Перечислите уровни эталонной модели взаимодействия открытых систем (OSI).
2. Куда инкапсулируется пакет с уровня 3 модели OSI?
3. Что декапсулируется из кадра в соответствии с моделью OSI?
4. Расшифруйте аббревиатуры ЛВС и LAN.
5. Прямым или перекрестным кабелем соединяются два компьютера?
6. Что такое канал связи?
7. Дан IP адрес с маской подсети: 126.127.1.31/27. Запишите маску подсети в десятичном виде.
8. Дан IP адрес с маской подсети: 126.127.1.31/27. Запишите количество IP адресов, предназначенных для назначения хостам (оконечным сетевым устройствам).
9. Дан IP адрес с маской подсети: 13.1.254.61/27. Запишите в десятичном виде широковещательный адрес подсети.
10. Сколько подсетей с маской /25 можно получить из сети с маской /27?
11. На каком уровне модели OSI передача информации представляет собой передачу потока бит по среде передачи данных?
12. Как называется механизм коммутатора, когда передача кадра, полученного на одном порту, осуществляется через другой порт в соответствии с таблицей коммутации?
13. Какую длину имеет MAC-адрес (в битах)?
14. Сколько корневых портов может быть у некорневого коммутатора?
15. Как расшифровывается аббревиатура VLAN?
16. Какие протоколы маршрутизации используются в IP-сетях?
17. Чему равно максимальное число переходов на пути к адресату назначения протокола RIP?

12.2 Зачет: теоретическая часть

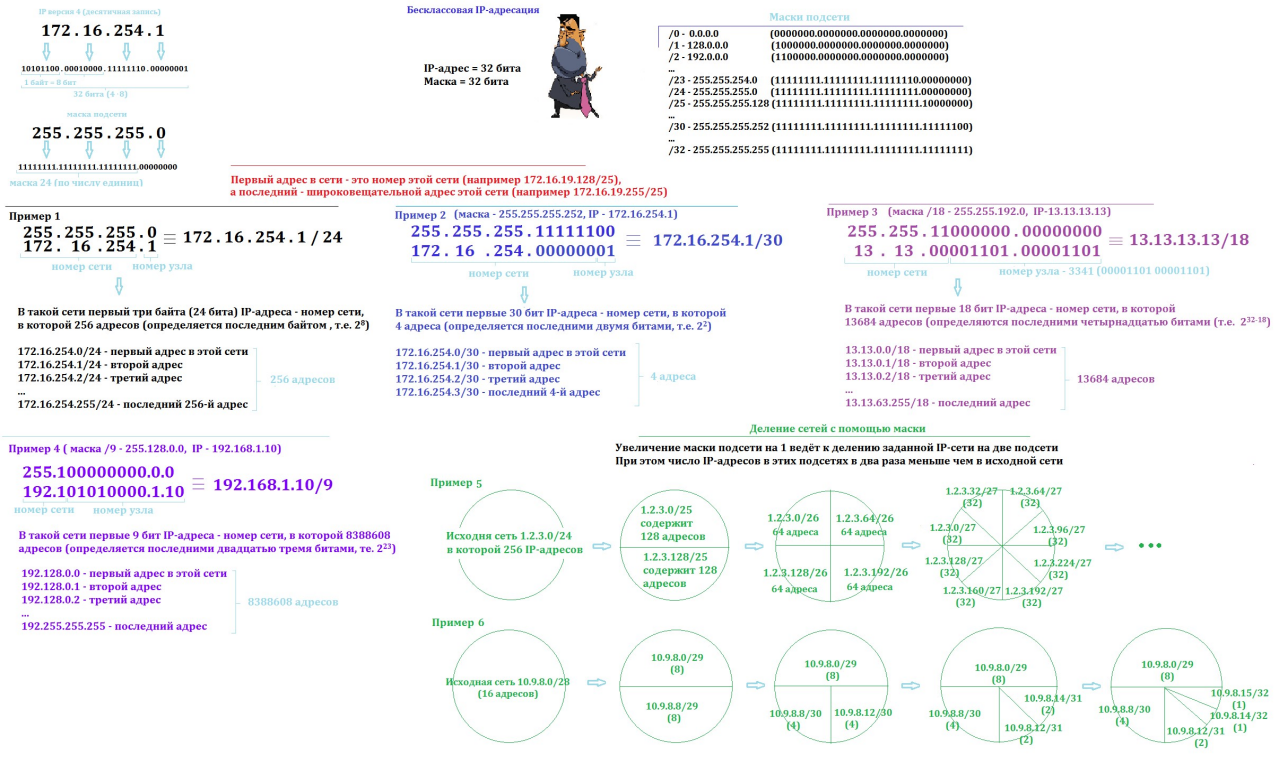
Нужно ответить на два случайных вопроса из следующего списка:
1. Семиуровневая модель OSI.
2. Протокол связующего дерева: назначение, особенности работы и настройки.
3. Динамическая маршрутизация, протокол RIP.
4. Принцип работы коммутатора.
5. Принцип работы маршрутизатора.
6. Бесклассовая IP-адресация.
7. Топологии сетей.
8. Виртуальные сети.
9. Структура IP-пакета.
10. Классификация сетей.
11. Динамическая маршрутизация, протокол OSPF.
12. Агрегирование каналов.
13. Протоколы TCP и UDP.
14. Протокол ARP.
15. Статическая маршрутизация.

12.3 Зачет: практическая часть

Нужно выполнить практическое задание по поиску и устранению неисправностей в Cisco Packet Tracer. Всего нужно обнаружить и исправить три ошибки в схеме согласно выданного преподавателем варианта:

1. VLAN.
2. Агрегирование каналов.
3. Статическая маршрутизация.
4. Динамическая маршрутизация RIP.

ПРИЛОЖЕНИЕ А
(справочное)
ПРИМЕР ИНФОГРАФИКИ ПО ТЕМЕ «IP-АДРЕСАЦИЯ»



ПРИЛОЖЕНИЕ Б
(справочное)
ОПИСАНИЕ СЕТЕВЫХ УТИЛИТ СЕМЕЙСТВА ОС WINDOWS

Сетевые утилиты активно используется сетевыми администраторами для оперативного администрирования сети. В операционной системе Windows сетевые утилиты работают через интерфейс командной строки (cmd.exe). Для запуска некоторых сетевых утилит интерпретатор cmd.exe должен быть запущен для выполнения с использованием опции «Запустить от имени администратора».

Далее рассмотрены сетевые утилиты командной строки для получения информации о сетевых настройках, выполнения операций по конфигурированию и диагностике сети:

- **hostname** – выводит имя локального хоста, используется без параметров;
- **ipconfig** – выводит значения для текущей конфигурации: IP-адрес, маску подсети, адрес шлюза по умолчанию, адрес DNS (Domain Name System);
- **ping** – осуществляет проверку связи с удаленным хостом путем отправки эхо-пакетов ICMP (Internet Control Message Protocol);
- **tracert** – осуществляет проверку маршрута к удаленному компьютеру путем отправки эхо-пакетов протокола ICMP и выводит маршрут прохождения пакетов на удаленный компьютер;
- **arp** – выводит для просмотра и изменения таблицу трансляции адресов, используемую протоколом разрешения адресов ARP (Address Resolution Protocol), который определяет локальный адрес по IP-адресу;
- **route** – модифицирует таблицы маршрутизации IP (отображает содержимое таблицы, добавляет и удаляет маршруты IP).

Далее перечислены основные сведения о перечисленных утилитах, полную справку о каждой из утилит можно получить, введя параметр «/?» после ввода имени утилиты.

Утилита ipconfig

При устранении неисправностей и проблем в сети следует сначала проверить правильность конфигурации. Для этого используется утилита ipconfig (рисунок Б.1). Она полезна на компьютерах, работающих с DHCP (Dynamic Host Configuration Protocol), так как дает пользователям возможность определить, какая конфигурация сети и какие величины были установлены с его помощью.

```
C:\Users\Администратор>ipconfig

Настройка протокола IP для Windows


Адаптер Ethernet Ethernet 2:

   DNS-суффикс подключения . . . . . :    tusur.ru
   Локальный IPv6-адрес канала . . . : fe80::a9a7:13b:6a8
   IPv4-адрес. . . . . . . . . . . . : 192.168.210.
   Маска подсети . . . . . . . . . . : 255.255.255.0
   Основной шлюз. . . . . . . . . . : 192.168.210.1
```

Рисунок Б.1 – Пример использования утилиты ipconfig

Основные параметры:

/all – вывод подробных сведений (выдает весь список параметров для всех сетевых адаптеров, без этого ключа отображается только IP-адрес, маска и шлюз по умолчанию для основного сетевого адаптера);

/renew [имя сетевого адаптера] – обновление IP-адреса для указанного сетевого адаптера;

/release [имя сетевого адаптера] – освобождение IP-адреса для указанного сетевого адаптера.

Таким образом, утилита ipconfig позволяет выяснить, инициализирована ли конфигурация и не дублируются ли IP-адреса:

- если конфигурация инициализирована, то отобразится IP-адрес, маска и шлюз;
- если IP-адреса дублируются, то маска сети будет равна 0.0.0.0;
- если при использовании DHCP компьютер не смог получить IP-адрес, то он будет равен 0.0.0.0.

Утилита ping

Утилита используется для проверки конфигурирования и диагностики ошибок соединения (рисунок Б.2). Она определяет доступность и функционирование конкретного узла или хоста. Использование утилиты ping – лучший способ проверки того, что между компьютерами существует маршрут. Утилита проверяет соединение путем посылки эхо-запросов ICMP и прослушивания эхо-ответов. Утилита ожидает каждый посланный пакет и отображает число переданных и принятых пакетов, поэтому из сообщений утилиты становится ясно, сколько пакетов потеряно, а по этим данным можно судить о качестве связи.

```
C:\Users\Администратор>ping ya.ru

Обмен пакетами с ya.ru [87.250.250.242] с 32 байтами данных:
Ответ от 87.250.250.242: число байт=32 время=96мс TTL=42
Ответ от 87.250.250.242: число байт=32 время=95мс TTL=42
Ответ от 87.250.250.242: число байт=32 время=95мс TTL=42
Ответ от 87.250.250.242: число байт=32 время=95мс TTL=42

Статистика Ping для 87.250.250.242:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    (0% потерь)
Приблизительное время приема-передачи в мс:
    Минимальное = 95мсек, Максимальное = 96 мсек, Среднее = 95 мсек
```

Рисунок Б.2 – Пример использования утилиты ping

По умолчанию передается 4 эхо-пакета длиной 32 байта. Утилита ping позволяет изменить размер и количество пакетов, указать, следует ли записывать маршрут, который она использует, какую величину времени жизни пакета (TTL, time to live) устанавливать, можно ли фрагментировать пакет и т.д.

При получении ответа в поле «время» указывается, за какое время (в миллисекундах) посланный пакет доходит до удаленного хоста и возвращается назад. Так как значение по умолчанию для ожидания отклика равно 1 секунде, то все значения данного поля будут меньше 1000 миллисекунд.

Утилиту можно использовать для тестирования как имени хоста (DNS или NetBIOS), так и его IP-адреса. Если запрос с IP-адресом выполнен успешно, а с именем – неудачно, это значит, что проблема заключается в распознавании соответствия адреса и имени, а не в сетевом соединении.

Основные параметры:

-t – проверяет связь с указанным узлом до нажатия комбинации клавиш CTRL+C;

-n <число> – задает число отправляемых запросов;

-f – устанавливает флаг, запрещающий фрагментацию в пакете;

-i <TTL> – задает срок жизни пакетов;

-w <время_ожидания> – задает время ожидания каждого ответа (в миллисекундах).

Утилита tracert

Утилита предназначена для трассировки маршрута. Она использует поле TTL IP-пакета и сообщения об ошибках ICMP для определения маршрута от одного хоста до другого (рисунок Б.3). Утилита может быть более содержательной и удобной, чем утилита ping, особенно в тех случаях, когда удаленный хост недостижим. С помощью нее можно определить район проблем со связью (у Интернет-провайдера, в локальной сети, в сети удаленного хоста) по тому, насколько далеко будет отслежен маршрут.

```
C:\Users\Администратор>tracert ya.ru

Трассировка маршрута к ya.ru [87.250.250.242]
с максимальным числом прыжков 30:

  1    <1 мс    <1 мс    <1 мс  192.168.210.1
  2     1 ms    <1 мс     3 ms  floor3-router.rk.tusur.ru [212.192.121.129]
  3     1 ms    <1 мс    <1 мс  cl-rk.SUR.net.ru [88.204.72.217]
  4    <1 мс    <1 мс    <1 мс  heimdall.SUR.net.ru [88.204.73.81]
  5     1 ms    <1 мс    <1 мс  asbr-outside.SUR.net.ru [88.204.73.66]
  6     4 ms     8 ms     5 ms  host_62_78_94_221.milecom.ru [62.78.94.221]
  7    88 ms    88 ms    91 ms  host_91_221_180_30.milecom.ru [91.221.180.30]
  8     *        *        *     Превышен интервал ожидания для запроса.
  9   106 ms    98 ms    99 ms  10.3.6.1
 10    95 ms    95 ms    97 ms  ya.ru [87.250.250.242]

Трассировка завершена.
```

Рисунок Б.3 – Пример использования утилиты tracert

Утилита tracert работает следующим образом: посылается по 3 пробных эхо-запроса на каждый хост, через который проходит маршрут до удаленного хоста. На экран при этом выводится время ожидания ответа на каждый пакет. Пакеты посылаются с различными величинами времени жизни. Каждый маршрутизатор, встречающийся по пути, перед перенаправлением пакета уменьшает величину TTL на единицу. Таким образом, время жизни является счетчиком точек промежуточной доставки (хопов). Когда время жизни пакета достигнет нуля, предполагается, что маршрутизатор пошлет в компьютер-источник сообщение ICMP «Время истекло». Маршрут определяется путем посылки первого эхо-запроса с TTL=1. Затем TTL увеличивается на 1 в каждом последующем пакете до тех пор, пока пакет не достигнет удаленного хоста, либо не будет достигнута максимально возможная величина TTL (по умолчанию 30).

Основные параметры:

-h <максЧисло> – максимальное число прыжков при поиске узла;

-w <таймаут> – таймаут каждого ответа в миллисекундах.

Утилита arp

Основная задача протокола ARP – трансляция IP-адресов в соответствующие локальные адреса (рисунок Б.4). Для этого ARP-протокол использует информацию из ARP-таблицы (ARP-кэша). Если необходимая запись в таблице не найдена, то протокол ARP отправляет широковещательный запрос ко всем компьютерам локальной подсети, пытаясь найти владельца данного IP-адреса. В кэше могут содержаться два типа записей: статические и динамические. Статические записи вводятся вручную и хранятся в кэше постоянно. Динамические записи помещаются в кэш в результате выполнения широковещательных запросов. Для них существует понятие времени жизни. Если в течение определенного времени (по умолчанию 2 мин.) запись не была востребована, то она удаляется из кэша.

Основные параметры:

-a – просмотр содержимого кэша для всех сетевых адаптеров;

-s – занесение в кэш статических записей;

-d – удаление из кэша записи для определенного IP-адреса.

```
C:\Users\Администратор>arp -a

Интерфейс: 192.168.210     --- 0x10
  адрес в Интернете      Физический адрес      Тип
  92.168.210.1           c0-26-63-17-c9     динамический
  92.168.210.2           25-11-cc-c8-49     динамический
  92.168.210.115         f0-5d-78-0a-70     динамический
  92.168.210.171         2b-67-02-62-91     динамический
  92.168.210.196         65-ec-b0-02-f9     динамический
  92.168.210.198         5b-39-12-f8-89     динамический
  92.168.210.225         ae-c5-02-85-1e     динамический
  92.168.210.233         1d-60-66-0f-45     динамический
  92.168.210.242         25-aa-2c-de-08     динамический
  92.168.210.255         ff-ff-ff-ff-ff     статический
  24.0.0.22              00-5e-00-00-16     статический
  24.0.0.251             00-5e-00-00-fb     статический
  24.0.0.252             00-5e-00-00-fc     статический
  39.192.152.143         00-5e-40-98-8f     статический
  39.255.255.250         00-5e-7f-ff-fa     статический
  55.255.255.255         ff-ff-ff-ff-ff     статический
```

Рисунок Б.4 – Пример использования утилиты arp

Утилита route

Утилита предназначена для работы с локальной таблицей маршрутизации (рисунок Б.5). Она позволяет добавлять новые маршруты, а также изменять и удалять существующие. Хотя в большинстве случаев этого не требуется, при помощи данной утилиты можно вручную редактировать таблицы маршрутизации.

```
C:\Users\Администратор>route PRINT
===========================================================================
Список интерфейсов
 16...48 5b 39 12 f8    ......Marvell Yukon 88E8056 PCI-E Gigabit Ethernet
  1...........................Software Loopback Interface 1
===========================================================================

IPv4 таблица маршрута
===========================================================================
Активные маршруты:
Сетевой адрес           Маска сети      Адрес шлюза       Интерфейс  Метрика
          0.0.0.0          0.0.0.0    192.168.210.1  192.168.210         35
        127.0.0.0        255.0.0.0         On-link         127.0.0.1    331
  255.255.255.255  255.255.255.255         On-link         127.0.0.1    331
  255.255.255.255  255.255.255.255         On-link   192.168.210.       291
===========================================================================
Постоянные маршруты:
  Отсутствует
```

Рисунок Б.5 – Пример использования утилиты route

Основные параметры:
-f – очистка таблицы маршрутизации;
PRINT – отображение текущего состояния таблицы маршрутизации;
ADD – добавление нового маршрута;
DELETE – удаление маршрута;
CHANGE – изменение существующего маршрута.

СПИСОК РЕКОМЕНДУЕМОЙ ЛИТЕРАТУРЫ

1. Агеев, Е. Ю. Локальные компьютерные сети: Учебное пособие [Электронный ресурс] / Е. Ю. Агеев. – Томск: ТУСУР, 2012. – 105 с.
2. Дибров, М. В. Сети и телекоммуникации. Маршрутизация в IP-сетях в 2 ч. Часть 1: учебник и практикум для вузов / М. В. Дибров. – М.: Издательство Юрайт, 2021. – 333 с.
3. Дибров, М. В. Сети и телекоммуникации. Маршрутизация в IP-сетях в 2 ч. Часть 2: учебник и практикум для вузов / М. В. Дибров. – М.: Издательство Юрайт, 2021. – 351 с.
4. Михальченко, С. Г. Эксплуатация и развитие компьютерных сетей и систем. Разд. 1: учебное пособие / С. Г. Михальченко, Е. Ю. Агеев. – М.: ТУСУР, 2007. – 216 с.
5. Михальченко, С. Г. Эксплуатация и развитие компьютерных сетей и систем. Разд. 2: учебное пособие / С. Г. Михальченко, Е. Ю. Агеев. – М.: ТУСУР, 2007. – 213 с.
6. Одом, У. Компьютерные сети. Первый шаг / У. Одом. – М.: Вильямс, 2005. – 432 с.
7. Олифер, В. Г. Компьютерные сети: Принципы, технологии, протоколы [Текст]: учебник для вузов / В. Г. Олифер, Н. А. Олифер. – 4-е изд. – СПб.: ПИТЕР, 2013. – 944 с.
8. Пуговкин, А. В. Сети передачи данных: Учебное пособие [Электронный ресурс] / А. В. Пуговкин. – Томск: ТУСУР, 2015. – 138 с.
9. Ракитин, Р. Ю. Компьютерные сети: учебное пособие / Р. Ю. Ракитин, Е. В. Москаленко. – Барнаул: АлтГПУ, 2019. – 340 с.