государственное бюджетное профессиональное образовательное учреждение
«Пермский химико-технологический техникум»
(ГБПОУ «ПХТТ»)

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ВЫПОЛНЕНИЮ ПРАКТИЧЕСКИХ РАБОТ

для специальности 10.02.05 «Обеспечение информационной безопасности автоматизированных систем»
по МДК.01.05 «Эксплуатация компьютерных сетей»

2019

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Место дисциплины в ОПОП. МДК.01.05 «Эксплуатация компьютерных сетей» является обязательным разделом профессионального модуля ПМ.01 Эксплуатация автоматизированных систем в защищенном исполнении.

В результате освоения ПМ.01 Эксплуатация автоматизированных систем в защищенном исполнении обучающийся должен:

уметь:

- выполнять мониторинг и анализ работы локальной сети с помощью программно-аппаратных средств;
- осуществлять диагностику и поиск неисправностей локальной сети;
- участвовать в проектировании, эксплуатации и диагностике компьютерных сетей;
- выявлять и оценивать угрозы безопасности информации;
- реализовывать технологии VPN и VLAN;

знать:

- типы сетей, серверов, сетевую топологию;
- типы передачи данных, стандартные стеки коммуникационных протоколов;
- установку и конфигурирование сетевого оборудования;
- основы проектирования и монтажа локальных вычислительных сетей;
- принципы построения телекоммуникационных вычислительных сетей (ТВС);
- технологию виртуальных частных сетей VPN;
- технологию виртуальных сетей VLAN;
- методы и средства обеспечения информационной безопасности;
- защиту от несанкционированного доступа, основные принципы защиты информации;

Формируемые МДК.01.05 компетенции:

ПК 1.1. Производить установку и настройку компонентов, автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации.

ПК 1.2. Администрировать программные и программно-аппаратные компоненты автоматизированной (информационной) системы в защищенном исполнении.

ПК 1.3. Обеспечивать бесперебойную работу автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации.

ПК 1.4. Осуществлять проверку технического состояния, техническое обслуживание и текущий ремонт, устранять отказы и восстанавливать работоспособность автоматизированных (информационных) систем в защищенном исполнении.

В результате освоения МДК.01.05 у обучающегося по базовой подготовке формируются общие компетенции (ОК):

ОК1. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.

ОК2. Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.

ОК3. Планировать и реализовывать собственное профессиональное и личностное развитие.

ОК4. Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.

ОК5. Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.

ОК7. Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.

ОК 8. Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержание необходимого уровня физической подготовленности.

ОК 9. Использовать информационные технологии в профессиональной деятельности.

ОК 10. Пользоваться профессиональной документацией на государственном и иностранном языках.

Методические указания предназначены для проведения практических занятий по МДК.01.05 «Эксплуатация компьютерных сетей».

Методические указания разработаны в соответствии с рабочей программой профессионального модуля ПМ.01 Эксплуатация автоматизированных систем в защищенном исполнении по специальности 10.02.05 «Обеспечение информационной безопасности автоматизированных систем».

Содержание методических указаний по выполнению практических работ соответствует требованиям Федерального государственного стандарта среднего профессионального образования по специальности 10.02.05 «Обеспечение информационной безопасности автоматизированных систем».

Методические указания включают практические работы по темам:

- Обжим кабеля в разъём 8P8C;
- Адресация и коммутация в локальной вычислительной сети. Протоколы icmp, arp, dhcp.
- Стек протоколов TCP/IP. Протоколы транспортного уровня OSI: TCP, UDP;
- Изучение технологии VLAN. Настройка VLAN;
- Настройка динамической маршрутизации в ЛВС с помощью протоколов RIP и OSPF;
- Настройка статической маршрутизации в локальной вычислительной сети.

Каждая практическая работа содержит сведения о теме, цели ее проведения и формируемых компетенциях, включает пояснение к работе, содержание отчета, контрольные задания или вопросы, список литературы.

К выполнению практических работ обучаемые приступают после подробного изучения соответствующего теоретического материала и прохождения инструктажа по технике безопасности.

Характер практических работ носит частично- репродуктивный.

ПРАВИЛА ВЫПОЛНЕНИЯ ПРАКТИЧЕСКИХ РАБОТ

Практическое занятие по МДК.01.05 «Эксплуатация компьютерных сетей» проводится в компьютерном классе. Необходимыми структурными элементами практического занятия являются инструктаж, проводимый преподавателем, а также организация обсуждения итогов выполнения практического задания. По окончании выполнения задания студент оформляет отчет.

Оценка за выполнение практических занятий выставляется по пятибалльной системе и учитывается как показатель текущей успеваемости студентов.

ОПИСАНИЕ РАБОЧЕГО МЕСТА ОБУЧАЮЩЕГОСЯ

1. Практические работы по МДК.01.05 «Эксплуатация компьютерных сетей» выполняются в компьютерном классе.

2. Для выполнения практических работ необходимы:

- персональный компьютер;
- операционная система Windows;
- приложения MS Office;
- cisco Packet Tracer 7.2.1;
- витая пара Cat-5;
- коннекторы с разъёмом 8P8C;
- кримпер;
- WireShark;
- методические указания.

ПРАКТИЧЕСКИЕ РАБОТЫ

Практическая работа №1

Обжим кабеля в разъём 8P8C

Цель работы:

Работа с кабельными соединениями сети.

Формируемые компетенции: ПК1.1, ПК1.2, ПК1.3, ПК1.4, ОК1-ОК10.

Оборудование:

персональный компьютер, операционная система Windows, приложения MS Office, витая пара Cat-5, коннекторы с разъёмом 8P8C, кримпер;

Пояснения к работе

Теоретический материал.

Витая пара представляет собой вид кабеля связи, содержащий одну или несколько пар изолированных проводников, скрученных между собой (с небольшим числом витков на единицу длины), покрытых пластиковой оболочкой (рис. 1).

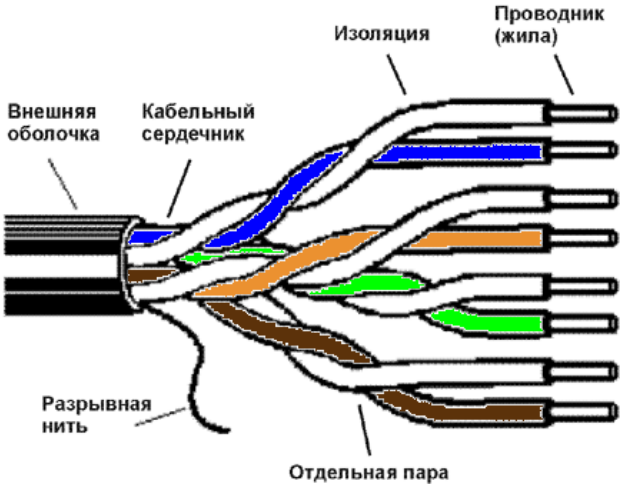


Рисунок 1 – Витая пара (8 проводников, 4 пары) (100Base-T4)

Обычно встречается 8 проводников (4 перевитые пары), реже – 4 проводника (2 пары, 100Base-T2). Количество проводников, а также толщина, шаг скрутки пар, тип изоляции витых пар определяется категорией витой пары, которая обозначается на внешней оболочке кабеля. Обратите внимание на маркировку кабеля используемого в лаборатории.

Таким образом, витые пары различаются по:

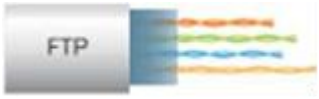
- категориям cat.1-7 (определяется частотой передаваемого сигнала);
- типам: UTP, FTP, STP (определяется экранированием проводов);
- видам изоляции;
- количеству пар.

Экранирование витой пары.

Для защиты от электрических помех при использовании высокочастотных сигналов в кабелях категорий 6а-8 используется экранирование. Экранирование применяется как к отдельным витым парам, так и к кабелю в целом в виде общего экрана.

UTP или **U/UTP** (Unshielded twisted pair - неэкранированная витая пара) - кабель не имеет защитного экрана. Широкое применение получил при монтаже локальной сети внутри помещений благодаря своей гибкости, а так же в условиях где есть возможность разнести кабель со значительными источниками электромагнитных помех.

FTP или **F/UTP** (Foiled twisted pair - фольгированная витая пара) - кабель аналогичен UTP, но имеет один внешний защитный слой из фольги. Обычно алюминиевая фольга или пленка применяются для защиты медных жил кабеля и продления его срока службы.



Индивидуальный экран (**U/FTP**) – экранирование фольгой каждых отдельных пар. Защищает от внешних помех и от перекрёстных помех между витыми парами.

STP (Shielded twisted pair - экранированная витая пара) - кабель имеет отдельный экран для каждой пары и внешнюю экранирующую защиту в виде сетки. Получил широкое применение при монтаже в сложных электромогнитных условиях: не возможности разнести витую пару с

мощным источником помех, большой кабельной длины маршрута, небольшие наводки по периметру которого, в комплексе дают плачевный результат.

S/UTP – кабель имеет только внешнюю экранирующую защиту в виде сетки.

S/FTP – кабель имеет внешнюю экранирующую защиту в виде сетки и отдельный экран из фольги для каждой пары.

SF/UTP – кабель имеет только внешнюю экранирующую защиту в виде сетки и фольги.

Таблица 1 – Характеристика типов экранов витой пары

Обозначение по ISO/IEC 11801	Общий экран	Экран для пар
U/UTP	нет	нет
U/FTP	нет	фольга
F/UTP	фольга	нет
S/UTP	оплётка	нет
SF/UTP	оплётка, фольга	нет
F/FTP	фольга	фольга
S/FTP	оплётка	фольга
SF/FTP	оплётка, фольга	фольга

Категории витой пары.

Для знакомства с категориями витой пары, их характеристиками и возможностями использования в компьютерной сети – заполните таблицу 2. Для заполнения используйте рекомендуемую литературу, а также информационные ресурсы сети Internet. На рисунке 2 приведены иллюстрации витой пары различных категорий.

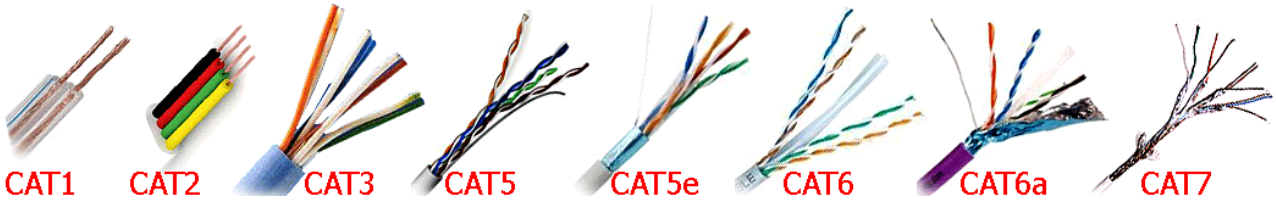


Рисунок 2 – Категории витой пары

Таблица 2 – Характеристики категорий витой пары

Категория витой пары	**Число пар**	**Частота сигнала, МГц**	**Пропускная способность**	**Обозначение (спецификация)**	**Экранирование**
Категория 1	1	0,1 (0,4)	До 1 Мбит/с	-	-
Категория 2	2	1 (4)	До 4 Мбит/с	-	-
Категория 3	4	16	До 10 /100 Мбит/с	10Base-T 100Base-T4	-
Категория 4	4	20	До 10/100 Мбит/с	10Base-T 100Base-T4	-
Категория 5	4	100	До 100 Мбит/с	100Base-TX	-
Категория 5e	4	100	До 100/1000 Мбит/с	100Base-TX / 1000Base-TX	-
Категория 6	4	250	До 1000 Мбит/с	1000Base-TX	-
Категория 6a	4	500	От 1000 Мбит/с - 10 Гбит/с	1000Base-TX	+
Категория 7	4	До 1200	До 100 Гбит/с	-	Общий внешний экран, фольгированная защита каждой пары

Заполнив таблицу и проанализировав информацию, становится заметной тенденция увеличения максимальной пропускной способности сети и частоты работы кабеля с увеличением номера категории витой пары. Это обусловлено повышением требований к подавлению перекрестных помех (XT) и эффективности изоляции проводников.

Два главных физических различия между наиболее распространёнными в настоящее время кабелями Cat-5 и Cat-6 – это количество витков витой пары на единицу длины и толщина оплетки (рис. 5). Длина витка не стандартизирована, но обычно у категории Cat-5(e) 1.5-2 витка на сантиметр, а у категории Cat-6 количество витков больше 2. Внутри одного кабеля,

каждая цветная пара также обладает различной длиной витка, основанной на простых числах. Длины витков подобраны таким образом, чтобы два различных витка никогда не совпадали. Такое решение не позволяет парам проводников плотно прилегать друг к другу по всей длине, что уменьшает влияние переходного затухания (влияние токов наводки на соседние пары кабеля). Количество витков на каждую цветную пару обычно уникально для каждого производителя. Как можно видеть на картинке выше, на 1 дюйм у каждой цветной пары приходится разное количество витков.

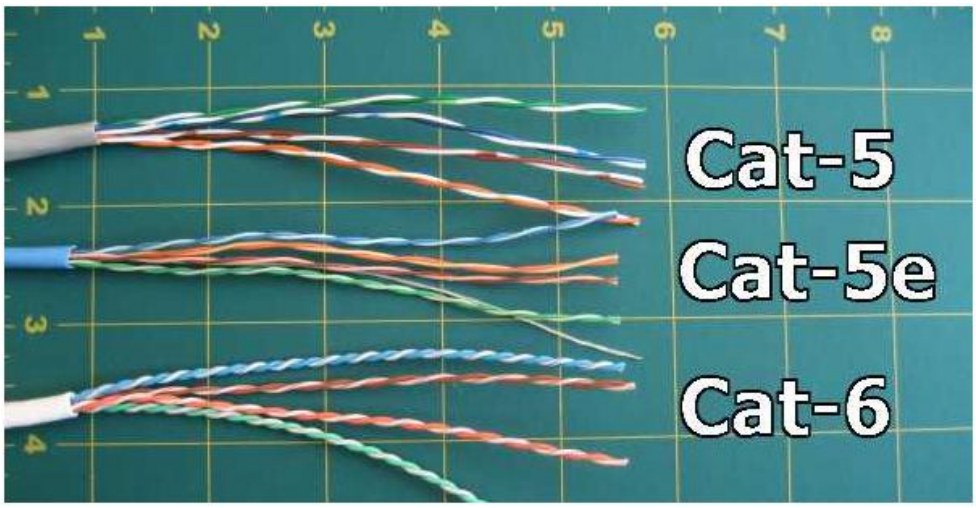


Рисунок 5 – Витая пара категорий 5, 5е, 6

Способы передачи по витой паре.

Каждая пара проводов в кабеле используется либо для передачи, либо для приёма информационного сигнала.

Если для передачи электрических сигналов воспользоваться обычной парой параллельных проводов для передачи знакопеременного списка большой частоты, то возникающие вокруг одного из них магнитные потоки будут вызывать помехи в другом (рис. 3). Для исключения этого явления (перекрестных помех) провода перекручивают между собой.

Рисунок 3 – Пара параллельных проводов

Существует два способа передачи сигналов по витым парам: несбалансированная передача (несимметричные цепи) и балансная передача (симметричные цепи).

Несбалансированная передача (несимметричные цепи). Несимметричные цепи применяются для построения систем пожарных и охранных сигнализаций и для передачи постоянных питающих напряжений, то есть низкочастотных сигналов на короткие расстояния. При несбалансированной передаче используется несимметричная цепь, то есть один из проводников заземляется с одной или с двух сторон (рис. 4). Сигналы передаются по остальным проводникам и изменяются относительно земли. По своей природе несимметричные цепи очень чувствительны к внешнему электромагнитному излучению (ЭМИ).

На рисунке видно, что на входе приемника, на сигнальном проводнике присутствует сумма напряжений сигнала *U*с и наводок *U*н от внешнего ЭМИ.

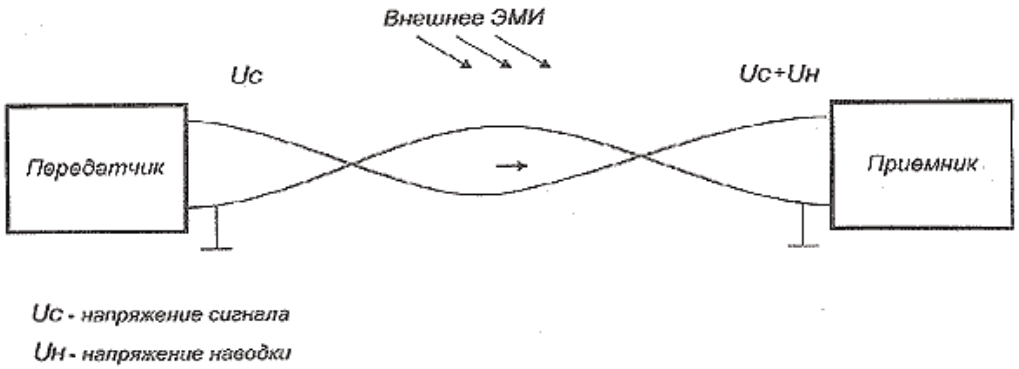


Рисунок 4 – Несимметричная сеть

Токи наводок на заземляющем проводнике стекают на землю, поэтому на нем *U*н равно нулю. С другой стороны, сигнальный провод является источником излучения электромагнитной энергии во внешнее пространство. Это приводит к значительному затуханию сигнала в процессе его распространения. Некоторое улучшение характеристик несимметричных цепей достигается в случае использования общего заземленного экрана (коаксиальный кабель), однако такое решение существенно повышает стоимость и трудоемкость монтажа кабельной системы.

Достоинством несимметричных цепей является то, что для передачи N сигналов требуется только N+1 проводников (N сигнальных плюс один общий заземляющий).

Балансная передача (симметричные цепи). Все виды ЛВС используют балансную передачу сигналов по витым парам. Схема симметричной цепи, в которой используется балансный принцип передачи информации, изображена на рисунке 5.

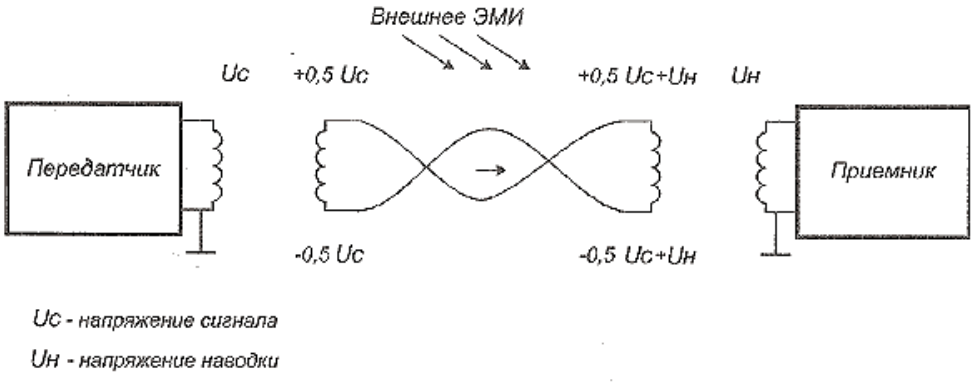


Рисунок 5 – Симметричная цепь передачи сигнала

Во вторичные обмотки передается только разность потенциалов на первичной обмотке. Из рисунка выше видно, что токи наводки в полностью симметричной цепи приводят к противофазному изменению напряжения *U*н на первичной обмотке трансформатора приемника, так что результирующий мешающий сигнал не передается во вторичную обмотку (передаётся только сигнал *U*с). Поэтому, в отличие от несимметричных, симметричные цепи значительно более устойчивы к внешним мешающим влияниям.

Основными недостатками симметричных цепей с балансной передачей являются, во-первых, необходимость использования для приема и передачи *N* сигналов 2x*N* проводников (на каждый сигнал 2 провода) и, во-вторых, невозможность передачи постоянной составляющей сигнала.

Ниже в таблице 3 показаны используемые в компьютерной сети с технологией Fast Ethernet проводники витой пары, и их предназначение.

Таблица 3 – Назначение проводников витой пары по стандартам

Контакт	Сигнал	Цвет	
		MDI (TIA/EIA-568-B)	MDI-X (TIA/EIA-568-A)
1	Передача +	Белый/оранжевый	Белый/зелёный
2	Передача -	Оранжевый	Зелёный
3	Приём +	Белый/зелёный	Белый/оранжевый
4	Не используется	Синий	Синий
5	Не используется	Белый/синий	Белый/синий
6	Приём -	Зелёный	Оранжевый
7	Не используется	Белый/коричневый	Белый/коричневый
8	Не используется	Коричневый	Коричневый

Ознакомьтесь с назначением проводников на практике.

Расположение выводов коннектора и порта 8P8C (10Base-T/100Base-TX) показано на рисунке 10. Сигналы на выводах разъёмов 8P8C описаны в таблице 6.

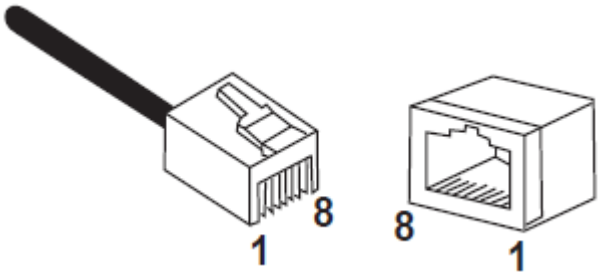


Рисунок 6 – Расположение выводов разъёмов 8P8C 10Base-T/100Base-TX

Режимы работы сетевых Ethernet портов.

Порт Ethernet 10Base-T/100Base-TX любого сетевого устройства может иметь одну из двух возможных конфигураций: MDI или MDI-X (табл. 3). Порты Ethernet персональных компьютеров, маршрутизаторов или мостов, как правило, имеют конфигурацию MDI, тогда как порты для витой пары коммутаторов или концентраторов обычно имеют конфигурацию MDI-X. В связи с этим появилась необходимость организации прямых и перекрёстных (кроссоверных) соединений сетевых устройств. Перекрёстное соединение используется для соединения однотипных устройств друг с другом, например, двух компьютеров или двух сетевых коммутаторов. Прямое

соединение предназначено для соединения различных по типу устройств, таких как компьютер с сетевым коммутатором (рис. 7).

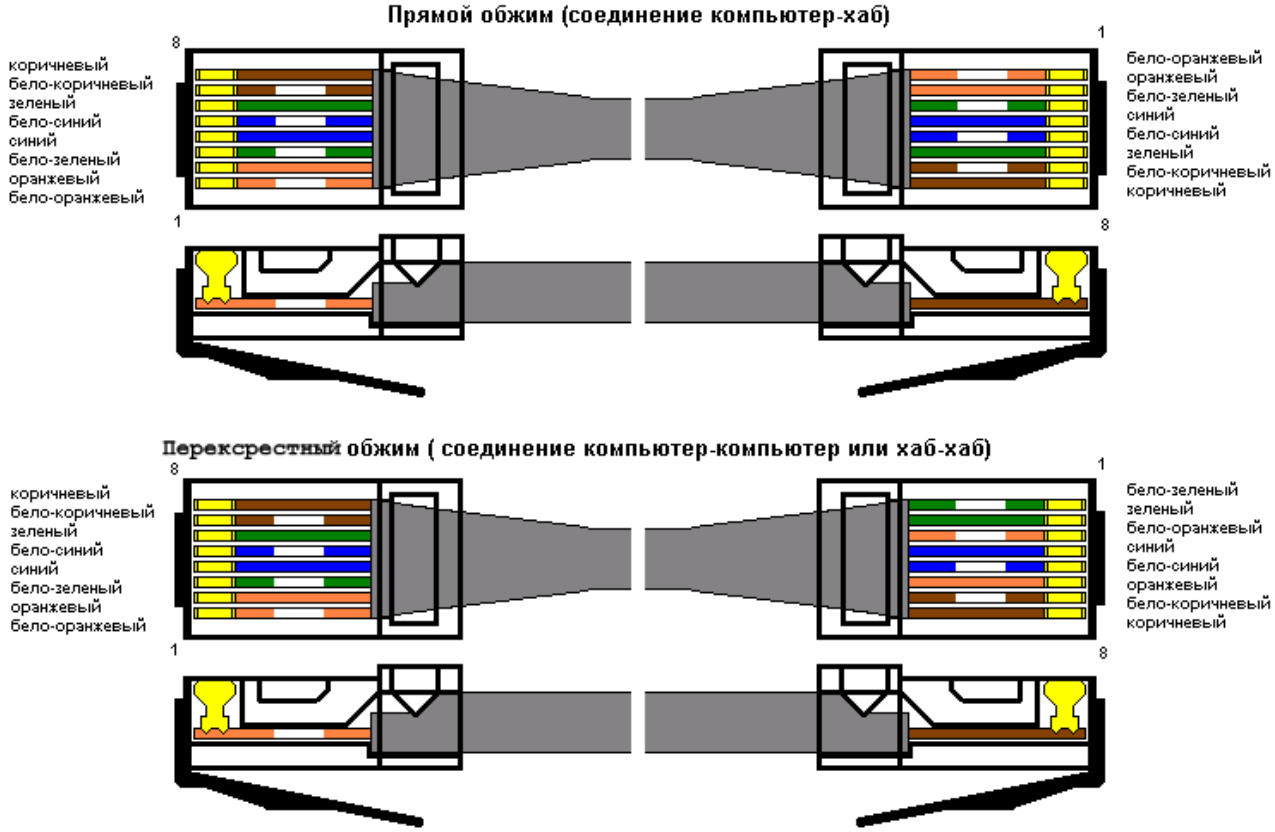


Рисунок 7 – Прямой и перекрестный обжим витой пары

В настоящее время большинство портов Ethenet сетевых устройств автоматически определяет конфигурацию порта подключенного конечного узла и выбирает нужный режим. Это позволяет использовать как прямые, так и перекрёстные соединения.

Для закрепления полученных знаний выполните обжимку витой пары в разъём 8P8C по стандарту T568B. Данные по контактам представлены в таблице 3, и проиллюстрированы на рисунке 11. Держите разъём контактами вверх и от себя, и используйте раскладку проводников слева-направо маркированных цветами как это показано на рисунке 8.

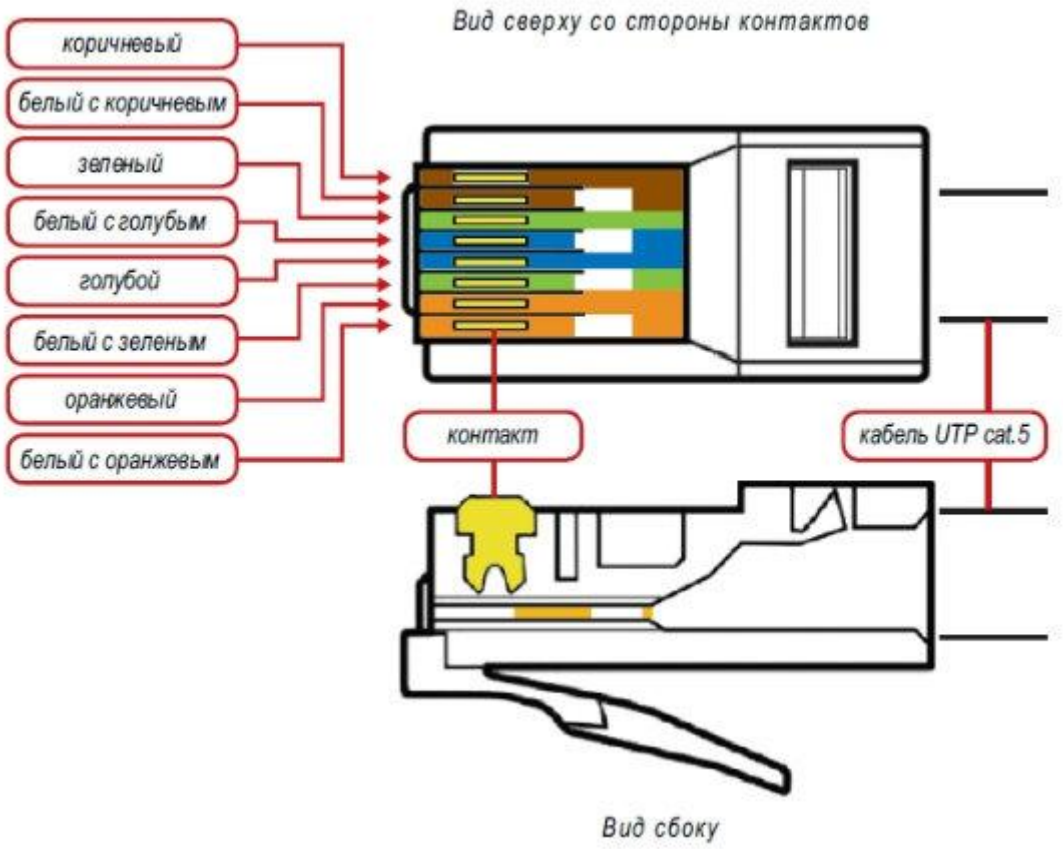


Рисунок 8 – Раскладка проводников кабеля в разъёме 8P8C по T568B

Для выполнения обжимки воспользуйтесь специализированным инструментом (рис. 9). Для удаления внешней изоляции с концов кабеля используйте стриппер. После этого распутайте витые пары в порядке для обжимки (слева-направо) и воспользуйтесь кусачками для выравнивания проводников. Для обжима витой пары в разъём используйте кримпер.

Рисунок 9 – Инструмент для обжимки витой пары:
стриппер (слева), кримпер (справа)

После обжимки кабеля необходимо убедиться в наличии контакта проводников. Используйте кабельный тестер (рис. 10) для проверки

соединения, подключив тестер и модуль тестера к обжатым противоположным концам кабеля.

Рисунок 10 – Кабельный тестер

Задание

Изучение категорий витой пары, типов экранирования и её характеристик. Соединение проводников кабеля «витая пара» по стандарту TIA/EIA-568-B. Обжим кабеля в разъём 8P8C.

Содержание отчета:

- формулировка задачи;
- результат обжима кабеля в разъём 8P8C.

Указания к выполнению работы:

1. Изучить теоретический материал.

2. Обжать кабеля в разъём 8P8C.

Контрольные вопросы:

1. Что такое технология Ethernet?

2. Назовите виды кабелей связи.

3. Назовите характеристика типов экранов витой пары.

4. Перечислите виды соединений сетевых устройств связи.

Литература

1. Работа с литературными источниками:

Олифер В.Г., Олифер Н.А. - Компьютерные сети. Принципы, технологии, протоколы (4-ое изд.) - 2010.

ЧАСТЬ I. ОСНОВЫ СЕТЕЙ ПЕРЕДАЧИ ДАННЫХ

Глава 2. Общие принципы построения сетей. Физическая передача данных по линиям связи. Проблемы связи нескольких компьютеров

ЧАСТЬ II. ТЕХНОЛОГИИ ФИЗИЧЕСКОГО УРОВНЯ

Глава 8. Линии связи. Типы кабелей. Структурированная кабельная система зданий

ЧАСТЬ III. ЛОКАЛЬНЫЕ ВЫЧИСЛИТЕЛЬНЫЕ СЕТИ

Глава 13. Коммутируемые сети Ethernet. Скоростные версии Ethernet

2. Работа с мультимедийными источниками:

a. Топологии сети и алгоритмы доступа к среде передачи
https://www.youtube.com/watch?v=peJE-oC0-i8

b. Категории витой пары
https://www.youtube.com/watch?v=0HYgleWK4HU

c. Обжим кабеля в разъём 8P8C
https://www.youtube.com/watch?v=7kOg3Ciae9c
https://www.youtube.com/watch?v=JBM9TSBeo5Y

d. Заделка витой пары в патч-панель
https://www.youtube.com/watch?v=eZ7IlLYEXYY
https://www.youtube.com/watch?v=9PpK12MlI_U

e. Кодирование 4B/5B
https://www.youtube.com/watch?v=3NIdellYW5o

f. Кодирование MLT-3
https://www.youtube.com/watch?time_continue=173&v=Mj_mIbmcims

Практическая работа №2

Адресация и коммутация в локальной вычислительной сети. Протоколы icmp, arp, dhcp.

Цель работы:

Получение знаний и умений конфигурации различных видов адресации и коммутации в локальной вычислительной сети, работающей под управлением коммуникационного стека протоколов TCP/IP.

Формируемые компетенции: ПК1.1, ПК1.2, ПК1.3, ПК1.4, ОК1-ОК10.

Оборудование:

персональный компьютер, операционная система Windows, приложения MS Office, cisco Packet Tracer 7.2.1.

Пояснения к работе

Теоретический материал.

Запустите программную среду сетевого моделирования Cisco Packet Tracer. Главное окно программы показано на рисунке 1.

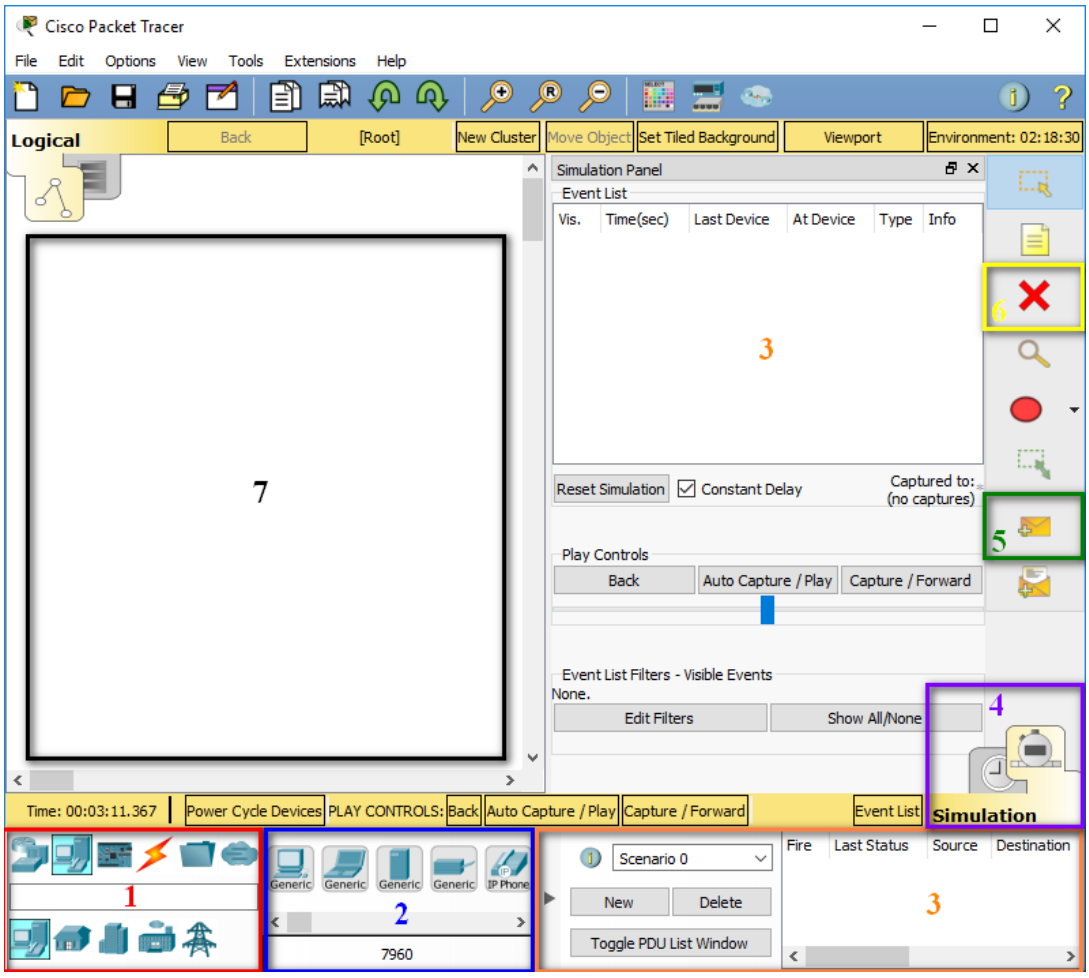


Рисунок 1 – Главное окно программы

Ознакомьтесь с областями окна программы (рис. 1):

1: Область выбора типа сетевого оборудования

2: Область выбора определенного устройства заданного типа

3: Область управления созданными пакетами

4: Область выбора режима реального времени или режима симуляции

5: Кнопка создания ICMP пакета – ping

6: Кнопка удаления объекта

7: Рабочая область.

Для изучения принципов работы коммуникационного оборудования переведите программу в режим симуляции. Создайте в рабочей области модели два сегмента сети, включающих по три рабочих станции, соединённых концентратором и коммутатором, соответственно (рис. 2). Для создания сети используйте следующие виды сетевого оборудования:

- Конечные узлы (раздел «End devices»):
  - Generic  .
- Активное сетевое оборудование (раздел «Network Devices» - «Hubs», «Switch»):
  - Hub  – концентратор.
  - Switch Cisco Catalyst 2950-24  – автономный, управляемый коммутатор 10/100 Ethernet с фиксированной конфигурацией обеспечивает подключение 24 пользователей в малых и средних сетях.
- Пассивное сетевое оборудование (оборудование, не получающее питание от электрической сети), кабельная система (раздел «Connections»):
  -  Copper straight-through (медный провод прямой обжимки).

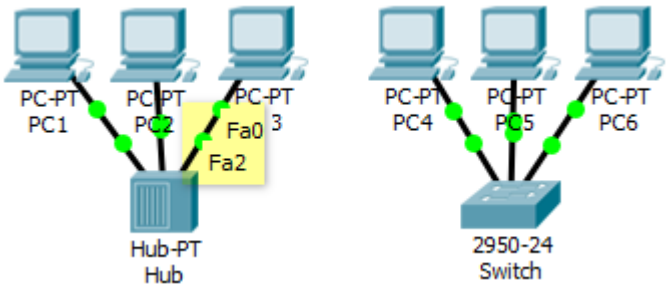


Рисунок 2 – Модель двух сегментов сети

После создания сети необходимо добиться работоспособности соединений (индикаторы соединений на концах линий связи должны иметь зелёный цвет). Для этого необходимо перейти в режим реального времени и вернуться в режим симуляции.

При конфигурировании сетевых интерфейсов важно не запутаться в их номерах и назначаемых для них сетевых адресов. Чтобы посмотреть между какими портами сетевых устройств организовано соединение достаточно подвести курсор манипулятора «мышь» к одному из интерфейсов соединения (графический примитив «круг»). На рисунке 2 показано, что для анализируемого соединения используются интерфейсы FastEthernet0 и 2 для устройств PC3 и Hub, соответственно.

Настройте статическую IP-адресацию в сегментах сети. Для этого назначьте сетевым интерфейсам компьютеров различных сегментов IP-адреса из следующих сетей класса C:

1. 192.168.1.0\24.
2. 192.168.2.0\24.

Для назначения адресов компьютерам сети кликните на значке компьютера. В появившемся окне выберите закладку – Desktop, затем кликните на значке – IP Configuration. В появившемся окне назначьте настройки:

- IP address,
- Subnet Mask.

После назначения адресации перейдите в режим симуляции и откройте лист событий модели «Event List». Перейдите в раздел фильтрации сетевого трафика «Event List Filters – Visible Events», нажмите кнопку сброса

фильтров «**Show All/None**» и после кнопку редактирования фильтра «**Edit Filter**» и выберите отображение в модели только ICMP трафика (рис. 3).

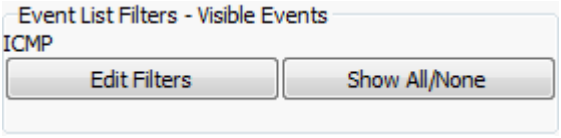


Рисунок 3 – Настройка сетевого фильтра

ICMP – протокол обмена управляющими сообщениями ICMP (Internet Control Message Protocol) позволяет маршрутизатору (шлюзу) сообщить конечному узлу об ошибках, с которыми маршрутизатор столкнулся при передаче какого-либо IP-пакета от данного конечного узла. ICMP протокол используется при диагностике сети с помощью программ ping и tracert.

С помощью кнопки создания ICMP пакета (рис. 1) создайте пакет от одного произвольного сетевого интерфейса компьютера к другому. В области управления созданными пакетами будет создан ICMP пакет. Откройте сетевой пакет на компьютере и посмотрите содержимое пакета (заголовок и поле данных ICMP). (рис. 4).

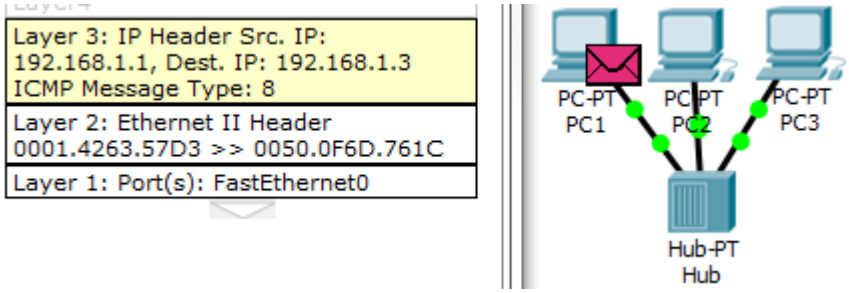


Рисунок 4 – Анализ полей данных пакета и кадра

С помощью кнопки **Capture/Forward** переместите пакет дальше по пути его следования. Откройте кадр на концентраторе и посмотрите на каком уровне модели OSI работает устройство, с какими данными оно работает (биты, кадр, пакет, сегмент). Продолжите моделирования и объясните дальнейший прямой и обратный путь прохождения пакета в сети с позиции используемой сетевым устройством адресации.

Нажмите кнопку **Delete** для удаления сетевого трафика (сценария передачи) и исследуйте аналогично сегмент сети с коммутатором. На каком уровне модели работает коммутатор и соответственно с каким типом адреса он работает?

Для того чтобы разобраться в принципе адресной передачи данных коммутатором используя инструмент «увеличительное стекло» Packet Tracer, откройте и проанализируйте таблицу **MAC table**, которая заполняется при передаче данных через коммутатор.

Для соединения ранее созданных автономных сетей в единую сеть, будем использовать коммутационное устройство – маршрутизатор 2621XM (рис. 5).

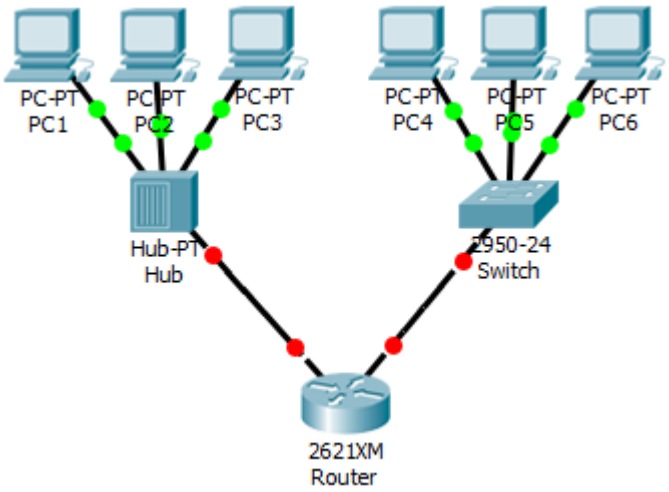


Рисунок 5 – Модель сети

Для обеспечения работоспособности сети необходимо сконфигурировать используемые интерфейсы маршрутизатора:

1. Определите какие интерфейсы маршрутизатора подключены к каждой сети.

2. Настройте интерфейсы маршрутизатора в разделе «**Config-Interface**»:

   a. Port Status

   b. IP Address

   c. Subnet Mask

   IP адрес интерфейса выбирается строго из сети устройства!

3. Перейдите в общие настройки **Settings** и сохраните данные маршрутизатора в энергонезависимой памяти NVRAM.

4. Сконфигурированные интерфейсы маршрутизатора будут выполнять роль шлюзов, поэтому для взаимодействия компьютеров из

различных сетей необходима конфигурация адреса шлюза на рабочих станциях (**IP Configuration - Default GateWay**).

Для того чтобы убедиться в работоспособности сети перейдите в режим реального времени и используйте программу ping в командной строке компьютера (**Desktop-Command Prompt**) для проверки соединения компьютеров различных сетей.

.

2. Изучение принципов работы протокола ARP.

В локальной вычислительной сети, работающей под управлением коммуникационного стека протоколов TCP/IP, используется два вида адреса – локальный (MAC) и сетевой (IP) адрес. При работе в сети часто известен только сетевой адрес целевого узла и не известен его MAC-адрес. Для получения MAC адреса узла по его IP-адресу используется протокол определения адреса ARP (Address Resolution Protocol).

Принцип работы ARP-протокола:

- Узел, которому нужно выполнить отображение IP-адреса на локальный адрес, формирует ARP запрос, вкладывает его в кадр протокола канального уровня, указывая в нем известный IP-адрес, и рассылает запрос широковещательно.
- Все узлы локальной сети получают ARP запрос и сравнивают указанный там IP-адрес с собственным.
- В случае их совпадения узел формирует ARP-ответ, в котором указывает свой IP-адрес и свой локальный адрес и отправляет его уже направленно, так как в ARP запросе отправитель указывает свой локальный адрес.

Для изучения принципа работы протокола на практике:

1. Переведите сеть в режим симуляции и удалите все созданные сетевые сценарии.
2. Настройте фильтр на отображение ICMP и ARP пакетов.

3. Откройте произвольную рабочую станцию-отправителя и очистите его ARP-таблицу через командную строку «`arp -d`».

4. Перейдите в среду моделирования и создайте эхо-запрос (ICMP) от станции отправителя к произвольной станции получателя этой же сети.

5. Заметьте, что в окне управления трафиком перед пакетом ICMP создан пакет ARP.

6. Проведите моделирование и зафиксируйте путь прохождения ARP-пакета (кадра) по сети, заполните таблицы 1 и 2.

Таблица 1 – Адреса интерфейсов отправителя и получателя

Рабочая станция	MAC	IP
PC «Отправитель»	*00:00:00:00:00:00*	0001.9754.79B2 или 192.168.1.1
PC «Получатель»	*11:11:11:11:11:11*	192.168.1.1

Таблица 2 – Адресная информация передачи ARP-запроса

Рабочая станция	MAC адрес		IP адрес	
	Отправитель	Получатель	Отправитель	Получатель
PC «Отправитель»	*00:00:00:00:00:00*	*00:00:00:00:00:00*	*192.168.1.1*	
Коммутационный узел (hub/switch)				
PC «Получатель»				

7. После моделирования просмотрите ARP таблицу компьютера-отправителя (команда `arp -a`).

8. Продолжите моделирование передачи ICMP-запроса и заполните таблицу 3.

Таблица 3 – Адресная информация передачи ICMP-пакета

Рабочая станция	MAC адрес		IP адрес	
	Отправитель	Получатель	Отправитель	Получатель
PC «Отправитель»	*00:00:00:00:00:00*	*00:00:00:00:00:00*	*192.168.1.1*	
Коммутационный узел (hub/switch)				
PC «Получатель»				

9. Проанализируйте заполненные таблицы. Обратите внимание на адресацию ARP-пакета. Выделите цветом особенности адресации в таблицах 1-3.

Выполните исследование работы протокола ARP в случае взаимодействия сетевых интерфейсов компьютеров различных сетей по предложенной методике. Заполните таблицы 4-6 адресной информации передачи icmp и arp –пакетов.

Таблица 4 – Адресная информация передачи ARP-запроса

Рабочая станция	MAC	IP
PC «Отправитель»		
PC «Получатель»		
Маршрутизатор (шлюз)		

Таблица 5 – Адресная информация передачи ARP-запроса

Рабочая станция	MAC адрес		IP адрес	
	Отправитель	Получатель	Отправитель	Получатель
PC «Отправитель»	*00:00:00:00:00:00*	*00:00:00:00:00:00*	*192.168.1.1*	*192.168.2.1*
Маршрутизатор(вх)				
Маршрутизатор(вых)				
PC «Получатель»				

Таблица 6 – Адресная информация передачи ICMP-пакета

Рабочая станция	MAC адрес		IP адрес	
	Отправитель	Получатель	Отправитель	Получатель
PC «Отправитель»	*00:00:00:00:00:00*	*00:00:00:00:00:00*	*192.168.1.1*	*192.168.2.1*
Маршрутизатор(вх)				
Маршрутизатор(вых)				
PC «Получатель»				

3. Динамическая адресация на основе протокола DHCP

DHCP (Dynamic Host Configuration Protocol – протокол динамической настройки узла) – сетевой протокол, позволяющий компьютерам автоматически получать IP-адрес и другие параметры, необходимые для работы в сети TCP/IP.

Данный протокол работает по модели «клиент-сервер». Для автоматической конфигурации компьютер-клиент на этапе конфигурации сетевого устройства обращается к так называемому серверу DHCP, и получает от него нужные параметры. Сетевой администратор может задать диапазон адресов, распределяемых сервером среди компьютеров. Это позволяет избежать ручной настройки компьютеров сети и уменьшает количество ошибок. Протокол DHCP используется в большинстве сетей

TCP/IP. В домашней сети в качестве DHCP-сервера наиболее часто выступает точка доступа (маршрутизатор).

Последовательность построения и конфигурации сегмента сети:

1. Удалите все сетевые сценарии передачи данных в сети.
2. Перейдите в режим симуляции и настройте фильтр на захват только DHCP трафика.
3. Добавьте 3 персональных компьютера PC-PT из типа – End devices.

4. В настройках IP Configuration компьютеров выберите DHCP.

5. Добавьте Server-PT из типа – End devices.

6. Добавьте еще один коммутатор – 2950-24. Подключите узлы третьей сети к коммутатору.

7. Задайте статический IP-адрес сервера и шлюза по умолчанию из сети 192.168.200.0\21.

8. Настройте сервер динамической адресации на вкладке Services-DHCP. Включите сервис. Задайте значения адреса Default Gateway, диапазон IP-адресов для хостов сети, задав начальный IP-адрес (Start IP Address) и количество хостов в сети. Нажмите кнопку Save для сохранения конфигурации.

9. Создайте Icmp пакет в третьей сети и проанализируйте созданный DHCP-пакет. Откройте пакет и заполните таблицу 7. Проанализируйте и словесно опишите принцип работы протокола DHCP. Какому хосту адресуется DHCP-запрос (IP, MAC) от интерфейса устройства желающего получить динамический адрес, опишите принцип получения IP-адреса.

Таблица 7 – Уровневая модель DHCP-пакета

Уровень OSI	**Данные**
7. Application	
6. Presentation	
5. Session	
4. Transport	
3. Network	
2. Data link	
1. Physical	

4. Протокол преобразования символьных имён DNS

DNS (Domain Name System) – протокол прикладного уровня модели OSI, выполняющий преобразование символьных имён в IP-адреса.

Протоколы DNS разработаны как приложение сервер-клиент. Хост – «распознаватель», который нуждается в отображении адреса в имя или имени в адрес, последовательно (до получения результата) обращается в:

1. Локальную базу приоритетных доменных имён и трансляции их в сетевые адреса хостов. База данных в ОС Windows представлена специальным файлом hosts. Путь к файлу: C:\WINDOWS\system32\drivers\etc\
2. Локальную базу кэш записей DNS. Для вывода на экран записей базы перейдите в командную строку (cmd) и используйте команду ipconfig /displaydns, используйте команду /flushdns когда необходимо очистить базу данных.
3. DNS-сервер, указанный в настройках сетевого соединения. Если сервер имеет информацию, он выполняет запрос распознавателя; в противном случае он либо отсылает распознаватель к другим серверам (итерационное распознавание адреса распознавателем), либо сам запрашивает другие сервера для того, чтобы обеспечить эту информацию (рекурсивное распознавание).

Рассмотрим работу с каждым из источников DNS данных.

Откройте файл **hosts** ОС и внесите изменения таким образом, чтобы **IP** адрес сервера **rambler.ru** соответствовал сетевому имени **mail.ru**. Проверьте результат используя браузер. Верните файл в исходное состояние.

Будьте внимательны, записи с подменой IP-адресов в файле hosts для блокирования доступа к ресурсам или перенаправления на поддельные и посторонние сайты могут производиться и вредоносными программами запущенными на локальном компьютере!

Вредоносные программы могут не только внести изменения в файл hosts, но и совершить его подмену. Подмена может быть осуществлена:

- скрытым файлом hosts, с переименовыванием оригинала в hosts.txt;

- произвольным файлом, путь к которому указан в реестре операционной системы (HKEY_LOCAL_MACHINE - SYSTEM - CurrentControlSet - services – Tcpip – Parameters – DataBasePath).

Проверим работу с локальной базой кэш записей и сервером DNS:

1. Запустите Wireshark в режиме захвата трафика сетевого подключения 192.168.28.N.
2. Настройте фильтр на захват DNS трафика.
3. Перейдите в командную строку операционной системы и выведите на экран локальную базу кэш записей DNS.
4. Используйте команду nslookup сетевоеИмя для получения IP адреса по известному в кэше сетевому имени. Проанализируйте результат (от кого получен DNS ответ).
5. Перейдите в WireShark и проанализируйет сетевой трафик. Сделайте выводы.
6. Используйте команду nslookup сетевоеИмя для получения IP адреса узла, которого нет в локальной базе кэш записей (можно прежде очистить кэш DNS).
7. Перейдите в WireShark и проанализируйте сетевой трафик. Откройте пакет DNS-запрос (query) и перейдите в поле данных протокола DNS, раздел Queries и Flags. Сделайте выводы об используемом режиме работы DNS. Откройте полученный ответ (response), раздел Answers поля данных DNS. Проанализируйте результаты.

Задание

Научиться конфигурировать различные виды адресации и коммутации в локальной вычислительной сети, работающей под управлением коммуникационного стека протоколов TCP/IP.

Содержание отчета:

- формулировка задачи;
- схемы сети связи в cisco Packet Tracer 7.2.1.

Указания к выполнению работы:

1. Изучить теоретический материал.

2. Составить схемы сети связи в cisco Packet Tracer 7.2.1.

3. Настроить сетевое оборудование.

Контрольные вопросы:

1. Как производится коммутация кадров, на основе каких правил?
2. В каком случае коммутатор рассылает принимаемый кадр широковещательно?
3. На каком уровне модели OSI работает маршрутизатор и с какими адресами, с какими блоками данных?

Литература

3. Работа с литературными источниками:

Олифер В.Г., Олифер Н.А. - Компьютерные сети. Принципы, технологии, протоколы (4-ое изд.) - 2010.

ЧАСТЬ I. ОСНОВЫ СЕТЕЙ ПЕРЕДАЧИ ДАННЫХ

Глава 2. Общие принципы построения сетей. Коммутация.

Обобщённая задача коммутации

4. Работа с мультимедийными источниками:
   a. Простейшая сеть https://www.youtube.com/watch?v=c9TMXiRk3E8
   b. Коммутатор и концентратор https://www.youtube.com/watch?v=VZDvaleQB0s
   c. Протокол ARP https://www.youtube.com/watch?v=0UbLESURFwQ
   d. Анализ протокола DHCP в WireShark https://www.youtube.com/watch?v=WaP4SZY0GJQ
   e. Кратко о работе службы DNS https://www.youtube.com/watch?v=m6-9fgmbfzg
   f. DNS: итеративный и рекурсивный режим https://www.youtube.com/watch?v=no9yc-BHaFA&t=1s

Практическая работа №3

Стек протоколов TCP/IP. Протоколы транспортного уровня OSI: TCP, UDP**.**

Цель работы:

получение общих знаний о многоуровневом стеке протоколов TCP/IP и протоколах обеспечения надёжности передачи данных UDP, TCP.

Формируемые компетенции: ПК1.1, ПК1.2, ПК1.3, ПК1.4, ОК1-ОК10.

Оборудование:

персональный компьютер, операционная система Windows, приложения MS Office, WireShark.

Пояснения к работе

Теоретический материал.

Протоколы транспортного уровня стека протоколов выполняют следующие основные функции по обработке данных при передаче потока данных от приложения удалённому сетевому интерфейсу и при приёме данных:

- Адресация.

  Каждая программа должна получить предназначаемые для неё данные – для этого на транспортном уровне стека протоколов используется третья ступень адресации в ЛВС. Каждая сетевая программа на компьютере использует индивидуальный(е) закреплённый за ней в операционной системе номер логического порта. Указание информации в заголовке TPDU позволяет идентифицировать программу, которой предназначаются данные на компьютере.

  Все порты разделены на три диапазона — общеизвестные (или системные, 0—1023), зарегистрированные (или пользовательские, 1024—49151) и динамические (или частные, 49152—65535).

- Сегментация.

  Для того чтобы снизить объём потери данных передаваемых по сети, а также не монополизировать канал передачей одного приложения в сети поток данных от приложения операционной

системы делится на протокольные единицы данных – сегменты (протокол TCP) или дейтаграммы (UDP). Учитывая максимальный размер кадра сети Ethernet 1518 байт, а также размеры заголовков вложенных в него протокольных единиц данных определить максимальный размер сегмента.

– Надёжная доставка (для протокола TCP).

Для надёжной доставки данных производится нумерация сегментов, а также используется механизм квитирования (подтверждения) принятых сегментов данных получателем. Нумерация производится с целью восстановления данных на стороне получателя в необходимой для этого последовательности. Нарушение последовательности доставки возможно в случае использования различных маршрутов передачи, либо неуспешной доставки сегмента(ов). Подтверждение позволяет убедиться в успешной доставке сегмента. В случае если подтверждение не получено за установленное таймером время, то узел предпринимает некоторое конечное число повторных попыток передачи.

1. Протокол ненадёжной доставки UDP

UDP (User Datagram Protocol — протокол пользовательских датаграмм) – один из ключевых протоколов TCP/IP, используя который компьютерные приложения могут посылать сообщения (в данном случае называемые датаграммами) другим хостам по IP-сети без необходимости предварительной установки соединения.

UDP является протоколом, не обеспечивающим надежность доставки. Изучите структуру дейтаграммы:

1. Запустите анализатор сетевого трафика WireShark в режиме захвата сообщений протокола DNS (Фильтр **dns**). Этот прикладной протокол использует в качестве транспорта протокол ненадежной доставки UDP.

2. Откройте браузер и сформируйте DNS запрос к web-сайту по доменному имени, которого нет в кэш компьютера (например, http://www.comnews.ru/).

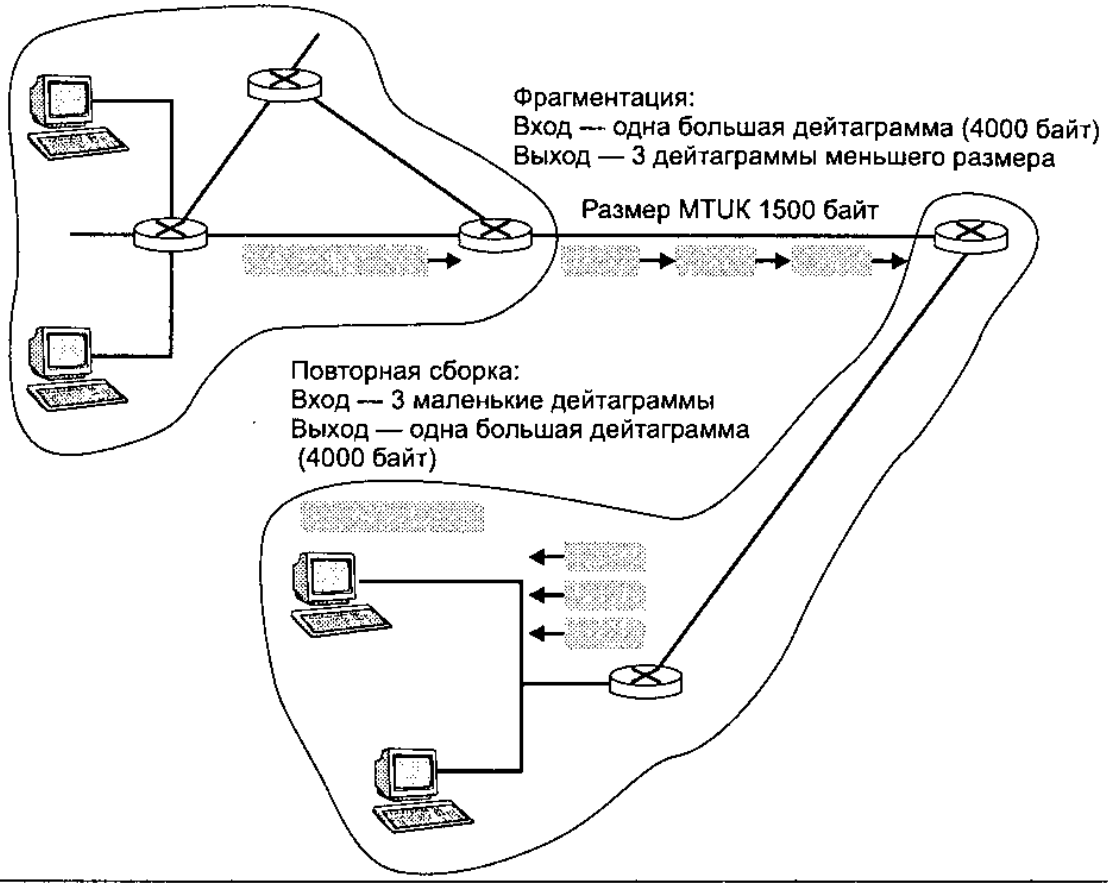
3. Перейдите в WireShark и откройте перехваченное DNS сообщение. Проанализируйте заголовок UDP. Заполните таблицу 2.

Таблица 2 – Формат дейтаграммы

Биты	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0-31																																
32-63																																
63- **?**																																

4. Определите максимальный размер поля полезных данных дейтаграммы (Maximum datagram size). Для этого учитывайте максимальный размер поля данных кадра (Maximum transmission unit, MTU) 1500 байт, а также размеры заголовков сетевого и транспортного уровней OSI. Таким образом, протокол UDP используется в том случае, когда передаваемые данные могут быть переданы в одном сообщении.

Однако, указанная особенность не исключает возможность фрагментации передаваемой по сети дейтаграммы. Это возможно в случае, когда MTU передаваемого кадра, с содержащейся в нём дейтаграммой, превышает максимальный размер блока данных MTU для используемой технологии передачи. На рисунке 1 показан пример фрагментации дейтаграммы 4000 байт, проходящей через сеть с максимальным размером поля данных кадра MTU=1500 байт (Ethernet). При этом происходит фрагментация сообщения, с указанием в IP-заголовке служебной информации для его сборки на стороне получателя: идентификатор (ID) смещения, смещение данных, флаг.



Фрагмент	Байты	ID	Смещение	Флаг
1	1480	777	0	1
2	1480	777	1480	1
3	1020 = 3980 – 1480 – 1480	777	2960	0

Рисунок 1 – Фрагментация дейтаграммы

Полезная нагрузка дейтаграммы передается транспортному уровню получателя только после того, как IP-уровень полностью восстановит оригинальную дейтаграмму. Если один или несколько фрагментов не сумеют достичь адресата, вся дейтаграмма отбрасывается и не передается транспортному уровню. Фрагментация и повторная сборка накладывают дополнительную нагрузку на интернет-маршрутизаторы (фрагментация) и на хосты-адресаты (повторная сборка). Поэтому желательно свести фрагментацию к минимуму. Для этого часто ограничиваются размеры TCP-сегментов и UDP-дейтаграмм, что снижает вероятность фрагментации. Поскольку все протоколы передачи данных, поддерживаемые протоколом IP, должны обеспечивать транспортировку пакетов данных размером, по меньшей мере, 576 байт, фрагментации можно полностью избежать, если использовать максимальный размер сегмента (MSS), равный 536 байт, что вместе с двумя 20-разрядными IP- и TCP-заголовками составит 576 байт. По

этой причине размер большинства TCP-сегментов для передачи данных больших объемов (например, HTTP-данных) находится в пределах от 512 до 536 байт.

2. Протокол надёжной доставки TCP

TCP (Transmission Control Protocol – протокол управления передачей) – основной протокол надежной передачи данных в ЛВС. Механизм TCP предоставляет поток данных с предварительной установкой соединения, осуществляет повторный запрос данных в случае потери и устраняет дублирование при получении копий одного пакета, гарантируя тем самым, в отличие от UDP, целостность передаваемых данных и уведомление отправителя о результатах передачи.

При передаче данных с использованием протокола TCP взаимодействие хостов проходит в три фазы: установление соединения, передача данных, разрыв соединения.

Установление соединения

Все TCP-соединения начинаются с тройного рукопожатия (рис. 2). Прежде чем хосты смогут обменяться любыми данными приложений, они должны «договориться» о начальном случайном числе последовательности пакетов, а также о ряде других переменных, связанных с этим соединением. Числа последовательностей выбираются случайно на обоих сторонах ради безопасности. Процедура установления соединения выглядит следующим образом (рис. 2):

- Хост1-инициатор передачи выбирает случайное число X и отправляет SYN-пакет, который может также содержать дополнительные флаги TCP и значения опций. Хост открывает порт для передачи.
- Хост2 выбирает свое собственное случайное число Y, прибавляет 1 к значению X, добавляет свои флаги и опции и отправляет ответ. Хост открывает порт для приёма и передачи данных.
- Хост1 прибавляет 1 к значениям X и Y и завершает хэндшейк, отправляя ACK-пакет. Инициатор открывает порт для приема данных.

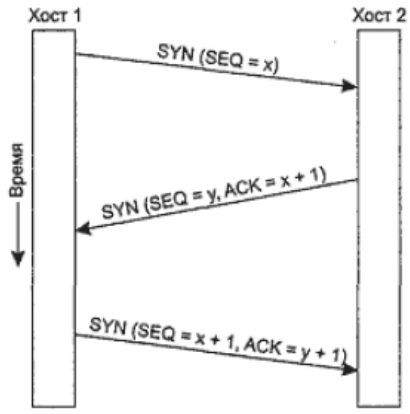


Рисунок 2 – Тройное рукопожатие

Перехватите сетевой трафик установления соединения в ЛВС. Для этого:

1. Запустите анализатор сетевого трафика WireShark в режиме захвата сообщений протокола TCP: tcp && ip.addr == 192.168.28.10. Рассмотрим пример удалённого доступа к файлам компьютера с интерфейсом 192.168.28.10. Удалённый доступ к файлам в ОС Windows осуществляется с помощью протокола прикладного уровня SMB (Server Message Block), использующего TCP в качестве транспорта данных.

2. Перейдите с рабочего стола ОС в сетевую папку «Лабораторные работы» расположенную на компьютере с IP-адресом интерфейса 192.168.28.10. (Win+R «\\328-10\"Лабораторные работы"»).

3. Перейдите в WireShark и проанализируйте сообщения установления соединения (рис. 3).

No.	Time	Source	Destination	Protocol	Length	Info
83617	8.828000	192.168.28.28	192.168.28.10	TCP	66	58757 → 445 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
83618	8.828708	192.168.28.10	192.168.28.28	TCP	66	445 → 58757 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=1 SACK_PERM=1
83619	8.828778	192.168.28.28	192.168.28.10	TCP	54	58757 → 445 [ACK] Seq=1 Ack=1 Win=65700 Len=0

Рисунок3 – Установление TCP-соединения

Передача данных с квитированием

В рамках соединения правильность передачи каждого сегмента должна подтверждаться квитанцией получателя. Квитирование - это один из традиционных методов обеспечения надежной связи. Идея квитирования состоит в следующем.

Для того чтобы можно было организовать повторную передачу искаженных данных отправитель нумерует отправляемые сообщения. Для каждого кадра отправитель ожидает от приемника так называемую

положительную квитанцию - служебное сообщение, извещающее о том, что исходный кадр был получен и данные в нем оказались корректными. Время этого ожидания ограничено - при отправке каждого кадра передатчик запускает таймер, и если по его истечению положительная квитанция не получена, то кадр считается утерянным. В некоторых протоколах приемник, в случае получения кадра с искаженными данными, должен отправить отрицательную квитанцию - явное указание того, что данный кадр нужно передать повторно.

Изучите механизм квитирования и структуру TCP-сегмента:

1. Перейдите в анализатор трафика WireShark
2. Выполните анализ перехваченного ранее трафика – TCP-сегментов и соответствующих им квитанций (ACK).
3. Изучите структуру TCP-сегмента в WireShark. Заполните таблицу 3.

Таблица 3 – Формат сегмента

Биты	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0-31																																
32-63																																
64-95																																
96-127																																
128-159																																
160-191																																
192-**?**																																

Продолжите описание полей заголовка сегмента.

4. Определите размер заголовка TCP-сегмента. Из-за столь большого объёма заголовка и дополнительного установления и завершения соединения, передачи с квитированием (см. ниже) – TCP протокол называется протоколом с высокими накладными расходами, что значительно снижает полезную скорость передачи данных, которая не может сравняться с пропускной способностью канала передачи.

5. Определите максимальный размер поля данных сегмента (Maximum segment size, MSS) учитывая MTU, а также размеры заголовков сетевого и транспортного уровней.

Задание

Изучить функции транспортного уровня стека протоколов TCP/IP.

Содержание отчета:

- формулировка задачи;
- заполненные таблицы в формате MS Word.

Указания к выполнению работы:

1. Изучить теоретический материал.

2. Изучить принципы работы протоколов: UDP, TCP.

Контрольные вопросы:

1. Назовите структуру стека протоколов TCP/IP.
2. В чем различия протоколов UDP, TCP?
3. Назовите функции транспортного уровня стека протоколов.

Литература

1. Работа с литературными источниками:

Олифер В.Г., Олифер Н.А. - Компьютерные сети. Принципы, технологии, протоколы (4-ое изд.) - 2010.

ЧАСТЬ IV. СЕТИ TCP/IP

Глава 15. Адресация в стеке протоколов TCP/IP. Стек протоколов TCP/IP

Глава 17. Базовые протоколы TCP/IP. Протоколы транспортного уровня TCP и UDP

2. Работа с мультимедийными источниками:

a. Углублённый урок о TCP и UDP

https://www.youtube.com/watch?v=K3iE-wiyFQU

b. Протокол UDP

https://www.youtube.com/watch?v=GBrLfZvRrd8

c. Протокол TCP

https://www.youtube.com/watch?v=CKUOb4htnB4

d. Протокол TCP: скользящее окно

https://www.youtube.com/watch?v=hd6QNXK5rPk

Практическая работа №4

Изучение технологии VLAN. Настройка VLAN.

Цель работы:

Получение знаний и умений настройки технологий VLAN.

Формируемые компетенции: ПК1.1, ПК1.2, ПК1.3, ПК1.4, ОК1-ОК10.

Оборудование:

персональный компьютер, операционная система Windows, приложения MS Office, Cisco Packet Tracer.

Пояснения к работе

Теоретический материал.

1. Изучение технологии VLAN.

VLAN (Virtual Local Area Network) – логическая («виртуальная») локальная компьютерная сеть. В зависимости от назначения выделяют два основных вида виртуальной локальной сети: сеть на основе одного и нескольких коммутаторов.

Технология VLAN на коммутаторе позволяет разделить сеть на канальном уровне на несколько независимых подсетей (VLAN 1 и 2, рис. 1) или же наоборот объединить компьютеры, расположенные удаленно друг от друга, подключенные к различным коммутаторам, в одну сеть (рис. 2). Таким образом, технология VLAN позволяет организовать коммутатор внутри коммутатора.

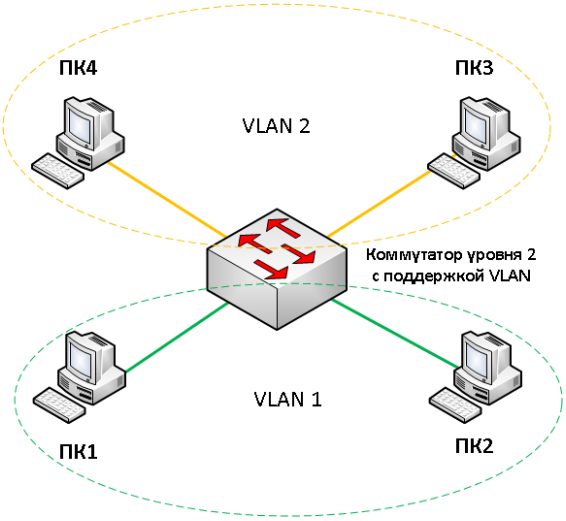


Рисунок 1 – Локальная VLAN-сеть на коммутаторе

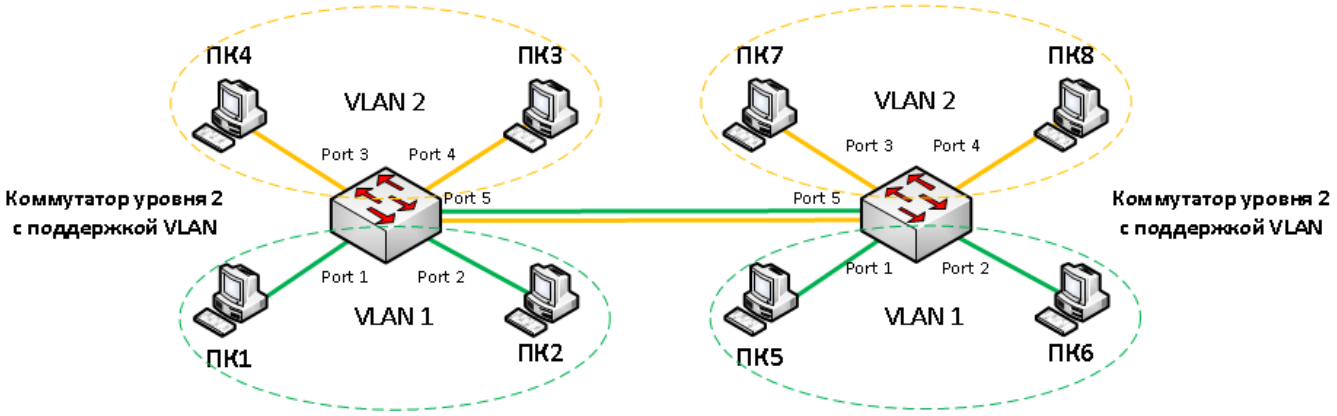


Рисунок 2 – Распределенная VLAN-сеть

Основные преимущества технологии VLAN:

- Структурирование сети. Возможность разделения портов коммутатора для различных отделов компании, сегментов серверов, пользователей, ip-камер и др. Пример показан на рисунке 1.
- Обеспечение безопасности. VLAN позволяет разделить сети на логические «подсети», тем самым ограничить доступ пользователей одной VLAN сети к пользователям другой VLAN сети (VLAN 1 и 2, рис. 1). Взаимодействие хостов из разных подсетей становится ограниченным в виду отсутствия между этими подсетями коммутационного оборудования третьего (сетевого) уровня OSI.
- Объединение пользователей сети, подключенных к различным физическим коммутаторам (пользователи VLAN 1 и VLAN 2, рис. 2). В таком случае отсутствует необходимость непосредственного подключения удаленных пользователей подсети к удаленному коммутатору. Вместо этого может быть настроена VLAN конфигурация.
- Уменьшение широковещательного трафика ARP, DHCP и др. Каждый VLAN образует широковещательный домен, то есть сегмент сети, внутри которого передаются широковещательные кадры (кадры передаваемые на всю сеть передаются на каждый порт вложенного коммутатора).

Настройка VLAN предполагает выделение двух типов портов коммутатора:

- Access port – порт для подключения конечных устройств (рис. 1).

- Trunk port – порт для соединения между коммутаторами (рис. 2).

Для изучения технологии VLAN откройте программное обеспечение Cisco Packet Tracer. Решим рассмотренные ранее две задачи конфигурации VLAN (рис. 1 и 2). Для этого следуйте нижеследующим инструкциям:

1. Постройте модель сегмента сети (рис. 1) и настройте статическую адресацию. Адреса для компьютеров выберите из пространства одной сети класса С (при настройке различных VLAN на практике IP-адреса хостам назначаются из различных сетей). В качестве коммутационного оборудования используйте коммутатор Cisco 2960.
2. Разделим сегменты как это показано на рисунке 1. Для этого зайдите в командную строку коммутатора и примените следующие команды:
   - Вход в привилегированный режим

     Switch>enable
   - Переход в режим глобального конфигурирования

     Switch#configure terminal
   - По умолчанию все порты коммутатора объединены в VLAN 1. Создадим VLAN 2 для IT-отдела и VLAN 3 для пользователей users.

     Switch(config)#vlan 2

     Switch(config-vlan)#name IT

     Switch(config-vlan)#exit
   - Настройка интерфейсов коммутатора. Определите порты коммутатора к которым подключены хосты планируемых VLAN 1 и VLAN2. Для примера ниже рассматривается работа с портом Fa0/1 и добавление его в VLAN2. Выполните добавление двух соответствующих портов коммутатора в vlan 2 и двух других портов к vlan 3.

     Switch(config)#interface fastEthernet 0/1

     Switch(config-if)#switchport mode access

     Switch(config-if)#switchport access vlan2

     Switch(config-if)#exit

– Проверьте настройку vlan (рис. 3).

Switch#show vlan

```
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                                Gig0/1, Gig0/2
2    IT                               active    Fa0/1, Fa0/2
3    users                            active    Fa0/3, Fa0/4
```

Рисунок 3 – Настройка VLAN коммутатора

– Проверьте настройку vlan коммутатора с помощью программной утилиты ping анализа связи между компьютерами в сети. Компьютеры одной виртуальной подсети должны быть доступны, а связь между компьютерами различных подсетей должна отсутствовать.

– После обмена кадрами через коммутатор проверим MAC-таблицу коммутатора и VLAN (рис. 4).

Switch#show mac address-table

```
Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

   2    0003.e4b6.6b82    DYNAMIC     Fa0/2
   2    0060.3ea2.250c    DYNAMIC     Fa0/1
   3    000b.beda.770e    DYNAMIC     Fa0/4
   3    00d0.9759.428c    DYNAMIC     Fa0/3
```

Рисунок 4 – MAC-table коммутатора

Пример настройки VLAN между коммутаторами сети продемонстрирован в мультимедиа-формате в ресурсах рекомендуемых к самостоятельному изучению. Основное отличие настройки заключается в необходимости конфигурирования Trunk-портов и демонстрируется ниже.

Задание

Изучить технологии VLAN. Настроить VLAN.

Содержание отчета:

– формулировка задачи;

– схема сети связи в Cisco Packet Tracer с настроенными VLAN.

Указания к выполнению работы:

1. Изучить теоретический материал.

2. Построить схему сети связи в Cisco Packet Tracer с настроенными VLAN.

Контрольные вопросы:

1. Что такое VLAN? Для чего нужен VLAN?
2. На каком оборудовании можно настроить VLAN?
3. Какие достоинства в настройке VLAN?

Литература

1. Работа с литературными источниками:
2. Олифер В.Г., Олифер Н.А. - Компьютерные сети. Принципы, технологии, протоколы (4-ое изд.) - 2010.
    1) ЧАСТЬ IV. СЕТИ TCP/IP
    2) Глава 18. Дополнительные функции маршрутизаторов IP-сетей. Трансляция сетевых адресов
3. Работа с мультимедийными источниками:
    a. Cisco Packet Tracer. VLAN https://www.youtube.com/watch?v=b51lvU6tV_Y
    b. Cisco Packet Tracer. NAT https://www.youtube.com/watch?v=6d2kvuWuyI0

Практическая работа №5

Маршрутизация в локальной вычислительной сети. Протоколы сетевого уровня OSI: RIP, OSPF.

Цель работы:

Получение знаний и умений настройки динамической маршрутизации в ЛВС с помощью протоколов RIP и OSPF.

Формируемые компетенции: ПК1.1, ПК1.2, ПК1.3, ПК1.4, ОК1-ОК10.

Оборудование:

персональный компьютер, операционная система Windows, приложения MS Office, Cisco Packet Tracer.

Пояснения к работе

Теоретический материал.

Для построения сети выполните следующие шаги:

1. Откройте среду моделирования Cisco Packet Tracer.
2. Создайте проект сети, предложенный на рисунке 1.
3. Сконфигурируйте устройства в подсетях 1-3 назначив сетевым адаптерам IP-адреса из адресного пространства сети класса С. В сети №3 используйте сервис динамического назначения IP адресов.
4. Проверьте наличие связи между устройствами подсетей 1 и 2, а также устройствами в сети 3. В случае неработоспособности сети исправьте ошибки.

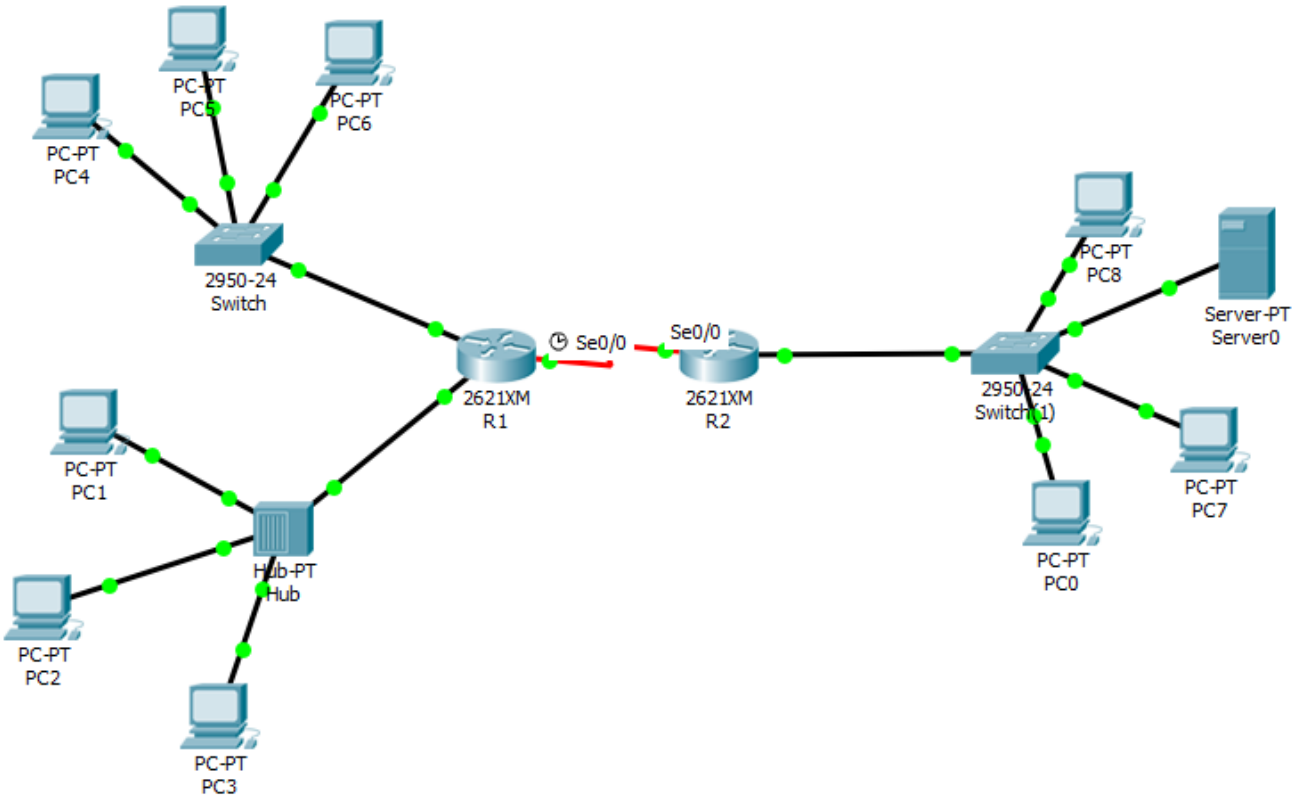


Рисунок 1 – Модель анализируемой сети

5. Соедините два маршрутизатора.

   a. Перед изменением конфигурации маршрутизаторов сохраните текущие настройки в энергонезависимой памяти (Config/Global Settings/NVRAM/Save).

   b. Имеющиеся в наличии маршрутизаторы имеют лишь по два сетевых интерфейса, поэтому мы не можем использовать стандартные типы витой пары с разъемами 8P8C. Для того чтобы не производить замену ранее выбранных устройств, для соединения маршрутизаторов будем использовать последовательное соединение Serial. На выбранных маршрутизаторах (по умолчанию) отсутствуют соответствующие активные порты, поэтому подключите к каждому маршрутизатору по одному последовательному порту с модулем —WIC-1T. Для этого на вкладке Physical выключите устройство, разместите модуль и включите питание. Дождитесь загрузки (для этого может потребоваться переход в режим реального времени).

c. Соедините последовательные порты маршрутизаторов кабелем —Serial DCE от первого маршрутизатора ко второму.

d. Для соединения маршрутизаторов в единую сеть, настройте IP-адреса последовательных интерфейсов роутеров из диапазона 100.0.0.0.

e. Наведите курсор на последовательное соединение. Для порта последовательного соединения маршрутизатора, около которого появится значок часов, установите параметр – Clock Rate в 56000.

f. После физического соединения для подключения локальных сетей в единую информационную сеть необходимо задать соответствующие параметры маршрутизации. Без настройки маршрутизации устройства подсетей 1 и 2 не смогут осуществлять информационный обмен с устройствами подсетиЗ.

3. Динамическая маршрутизация в ЛВС

Динамическая маршрутизация – вид маршрутизации, при котором таблица маршрутизации редактируется программно. При динамической маршрутизации происходит **обмен служебной маршрутной информацией** между соседними маршрутизаторами, в ходе которого они сообщают друг другу, какие сети в данный момент доступны через них, а также метрику (стоимость) маршрута. Информация обрабатывается и помещается в таблицу маршрутизации. На основе стоимости маршрута до сети назначения определяется маршрут следования пакета на каждом маршрутизаторе. К наиболее распространенным внутренним протоколам маршрутизации относятся протоколы RIP и OSPF.

4. Настройка динамической маршрутизации RIP

Протокол RIP (Routing Information Protocol) является внутренним протоколом маршрутизации **дистанционно-векторного типа**, он представляет собой один из наиболее ранних протоколов обмена

маршрутной информацией и до сих пор чрезвычайно распространен в вычислительных сетях ввиду простоты реализации.

Для IP имеются две версии протокола RIP: первая и вторая. Протокол RIPvl не поддерживает масок, то есть он распространяет между маршрутизаторами только информацию о номерах сетей и расстояниях до них, а информацию о масках этих сетей не распространяет, считая, что все адреса принадлежат к стандартными классам A, B или C. Протокол RIPv2 передает информацию о масках сетей, поэтому он в большей степени соответствует требованиям сегодняшнего дня. Так как при построении таблиц маршрутизации работа версии 2 принципиально не отличается от версии 1, то в дальнейшем для упрощения записей будет описываться работа первой версии.

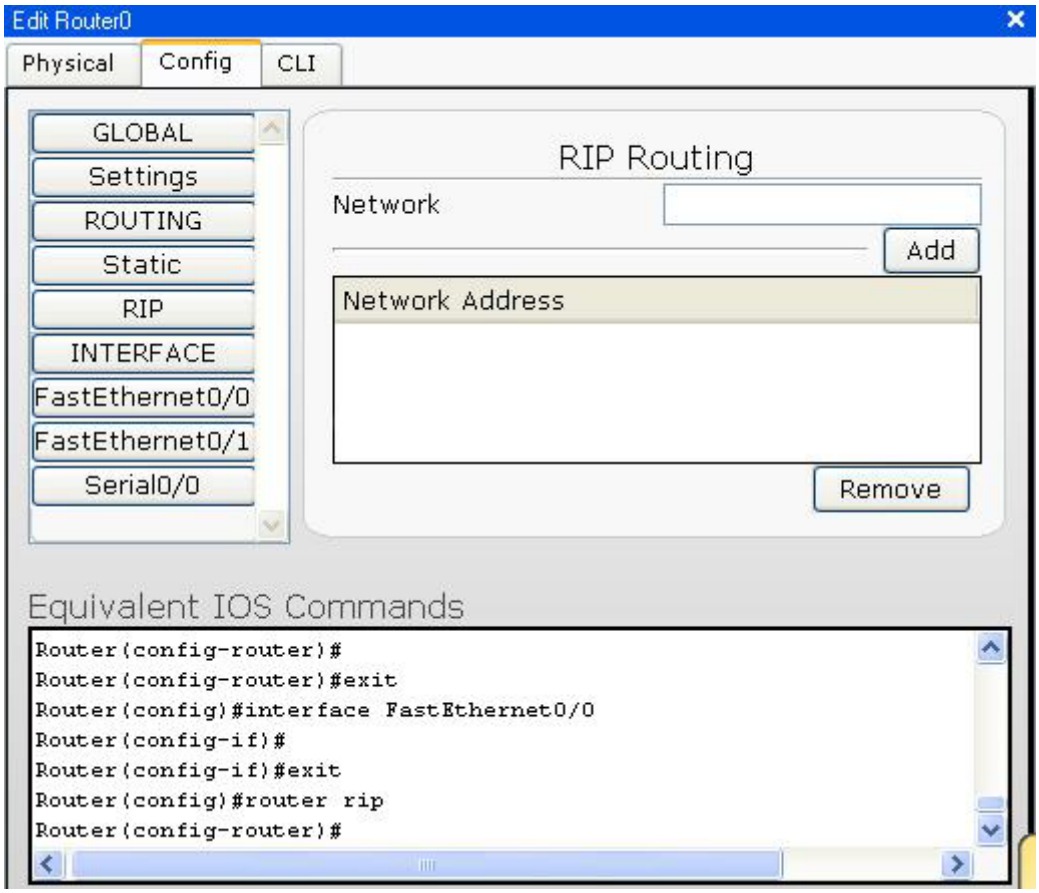


Рисунок 2 – Окно настроек протокола RIP маршрутизатора

Для измерения расстояния до сети стандарты протокола RIP допускают различные виды метрик: хопы, значения пропускной способности, вносимые задержки, надежность сетей (то есть соответствующие признакам D, T и R в **поле качества сервиса IP-пакета**), а также любые комбинации этих метрик.

Метрика должна обладать свойством аддитивности – метрика составного пути должна быть равна сумме метрик составляющих этого пути. В большинстве реализаций RIP используется простейшая метрика – **количество хопов**, то есть количество промежуточных маршрутизаторов, которые нужно преодолеть пакету до сети назначения.

Для исследования сконфигурируйте RIP протокол на маршрутизаторах сети:

1. Переведите модель в режим моделирования
2. Настройте фильтры трафика на пакеты RIP
3. Зайдите в настройки маршрутизатора R1 на закладку – Config (рис. 2).
4. В поле – Network введите адрес сети, непосредственно подключенной к порту маршрутизатора. Нажмите кнопку Add чтобы добавить введенный адрес в список сетей.
5. Повторите операцию 4 пока для добавления в список роутера R1 всех непосредственно подключенных к нему сетей.
6. После добавления сети в список роутером будут сформированы RIP-пакеты с информацией о известных ему сетях.
7. Откройте пакеты и проанализируйте кому они предназначаются и какую информацию содержат в поле данных RIP.
8. Последовательно промоделируйте передачу пакетов. Ответьте на вопрос – почему пакеты передаваемые в различные сети содержат различную информацию о сетях подключенных к маршрутизатору.

Более гибкая настройка всех параметров возможна при настройке динамической маршрутизации RIP с помощью командной строки Cisco IOS (консоли).

Порядок выполнения действий

1. Зайдите в настройки маршрутизатора на закладку – CLI .

2. Для удаления предыдущих настроек маршрутизации необходимо последовательно прописать следующие команды в консоли:

Router>enable

Router#configure terminal

Router(config)#no router rip

Router(config)#exit

Router#

Убедитесь в графическом интерфейсе настройки RIP что удалены все записи о подключенных к маршрутизатору сетях

3. Для настройки маршрутизации RIP необходимо прописать следующие команды:

Router#configure terminal

Router(config)#router rip

Router(config-router)#network *ip-address*

Router(config-router)#exit

Router(config)#exit

Router#

Описание: ip-address : адрес сети, подключенной к порту маршрутизатора.

4. Проверьте работоспособность сети. Зафиксируйте и объясните маршрут прохождения пакетов между разными сетями.

5. **Настройка динамической маршрутизации OSPF**

OSPF (англ. Open Shortest Path First) — протокол динамической маршрутизации, основанный на технологии отслеживания состояния канала (link-state technology) и использующий для нахождения кратчайшего пути Алгоритм Дейкстры (Dijkstra’s algorithm).

В отличие от протоколов RIP протоколы маршрутизации на основании состояния связей (метрика – свойство канала связи, например, пропускная способность) могут масштабироваться и обслуживать очень большие сети, кроме того можно создать области (areas) внутри зоны действия протокола OSFP. Каждая область выступает как объект маршрутизации, внутри которого маршрутизаторы обмениваются информацией между собой.

Расширим сеть, добавив в неё еще нескольких маршрутизаторов:

1. Для соединения с дополнительными устройствами по витой паре добавьте к каждому из двух существующих маршрутизаторов по плате – NM-2FE2W.
2. Добавьте 2 дополнительных маршрутизатора Cisco 2621XM.
3. Соедините маршрутизаторы с помощью кабеля – Copper Cross-Over через интерфейсы FastEthernet.
4. Настройте IP-адреса соответствующих интерфейсов из диапазона сети класса A.

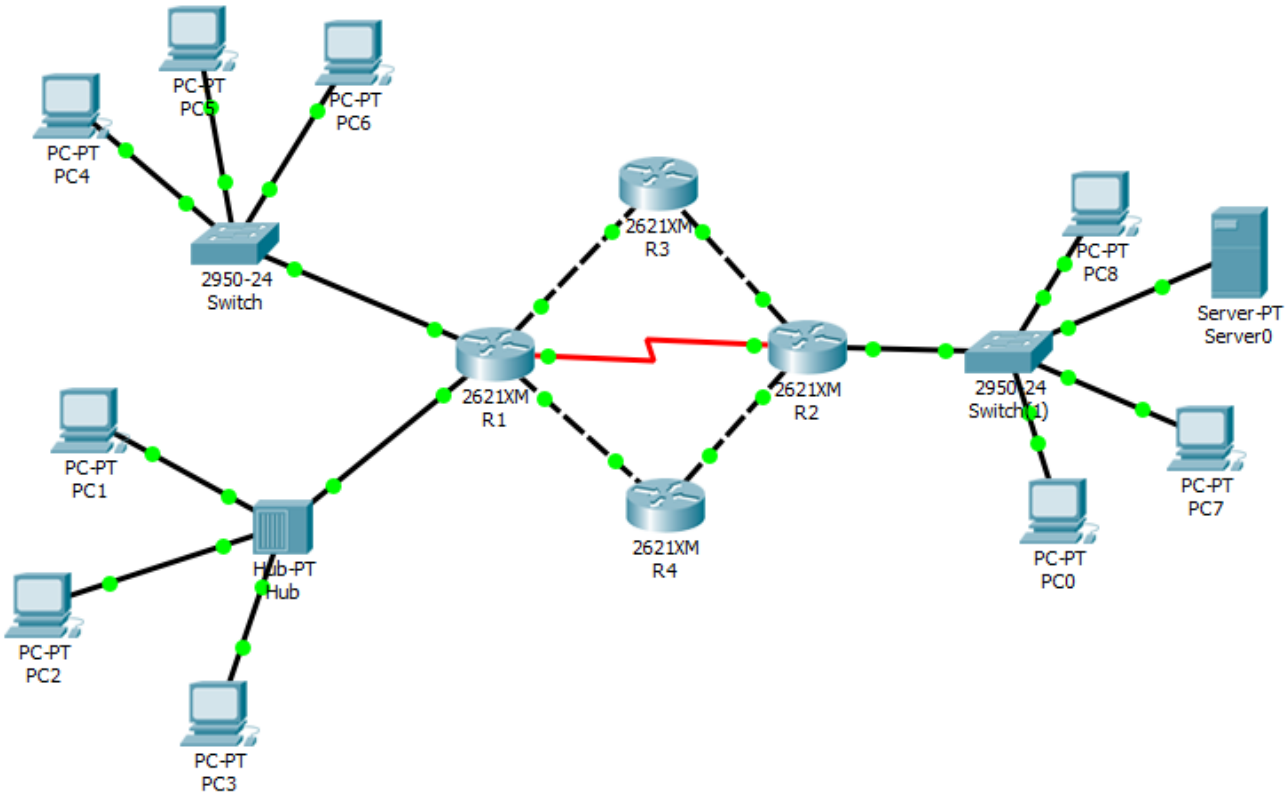


Рисунок 3 – Модель сети с дополнительными маршрутизаторами

Порядок настройки динамической маршрутизации OSPF с помощью командной строки Cisco IOS (консоли).

1. Очищаем настройки сделанные ранее на маршрутизаторах.

Router>enable

Router#configure terminal

Router(config)#no router rip

Router(config)#exit

Router#

2. Запуск процесса OSPF:

Router#configure terminal

Router(config)#router ospf *process-id*

Router(config-router)# network *address wildcard-mask area area-id*

Router(config-router)#exit

Router(config)#exit

Router#

Описание:

process-id : Номер процесса OSPF (любое число > 0, можно запустить несколько процессов).

address wildcard-mask : Адрес и wild-card маска сети (маска записывается в обратной форме, например 0.0.0.255), которая будет участвовать в OSPF маршрутизации (также определяет интерфейс на котором будет запущен OSPF).

area-id : Номер зоны действия протокола OSPF (в данной лабораторной работе сети должны находится в одной зоне).

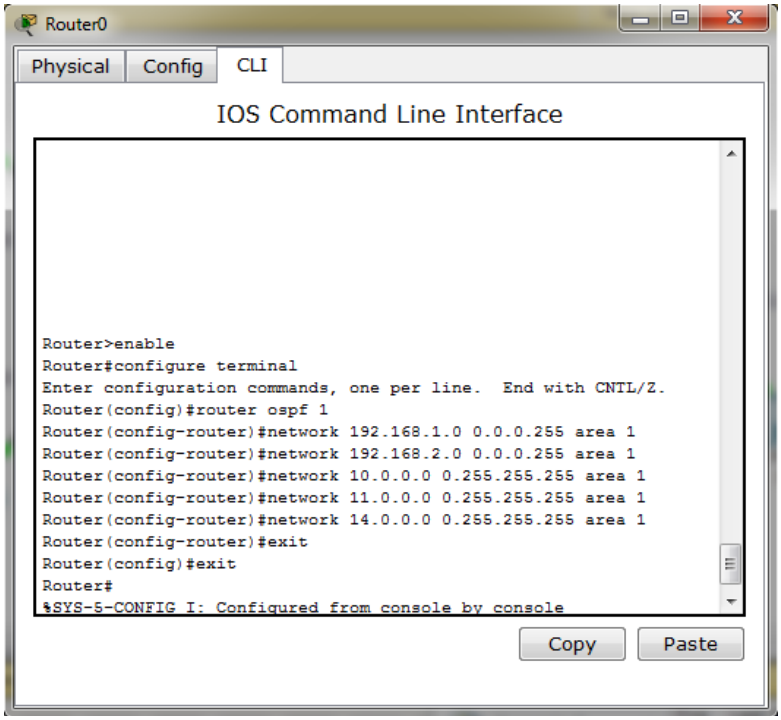


Рисунок 4 – Пример результата работы командной строки по настройке OSPF

Задание

Настроить динамическую маршрутизацию в ЛВС с помощью протоколов RIP и OSPF.

Содержание отчета:

- формулировка задачи;
- схема сети связи в Cisco Packet Tracer с настроенной динамической маршрутизацией.

Указания к выполнению работы:

1. Изучить теоретический материал.

2. Построить схему сети связи в Cisco Packet Tracer с настроенной динамической маршрутизацией.

Контрольные вопросы:

1. Что такое динамическая маршрутизация? Для чего она нужна?
2. Какие протоколы динамической маршрутизации существуют?
3. Какие достоинства динамической маршрутизации?

Литература

1. Работа с литературными источниками:

Олифер В.Г., Олифер Н.А. - Компьютерные сети. Принципы, технологии, протоколы (4-ое изд.) - 2010.

ЧАСТЬ IV. СЕТИ TCP/IP

Глава 17. Базовые протоколы TCP/IP. Общие свойства и классификация протоколов маршрутизации. Протокол RIP. Протокол OSPF

2. Работа с мультимедийными источниками:

a. Маршрутизация

https://www.youtube.com/watch?v=7cIiK3jbK0s

b. Протоколы маршрутизации

https://www.youtube.com/watch?v=MSg8gx3wnfQ

Практическая работа №6

Статическая маршрутизация в локальной вычислительной сети.

Цель работы:

Получение знаний и умений настройки статической маршрутизации в локальной вычислительной сети.

Формируемые компетенции: ПК1.1, ПК1.2, ПК1.3, ПК1.4, ОК1-ОК10.

Оборудование:

персональный компьютер, операционная система Windows, приложения MS Office, Cisco Packet Tracer.

Пояснения к работе

Теоретический материал.

1. **Построение модели сети**

Для построения сети выполните следующие шаги:

1. Откройте среду моделирования Cisco Packet Tracer.
2. Создайте проект сети по электрической структурной схеме предложенной на рисунке 1.
3. Сконфигурируйте устройства в подсетях 1-4 назначив сетевым адаптерам IP-адреса из указанных адресных пространств. В сети с наличием DHCP сервера настройте динамическую адресацию.
4. Проверьте с использованием командной строки правильность конфигурирования сетевых интерфейсов и наличие связи между интерфейсами устройств в подсетях. В случае неработоспособности сети исправьте ошибки.

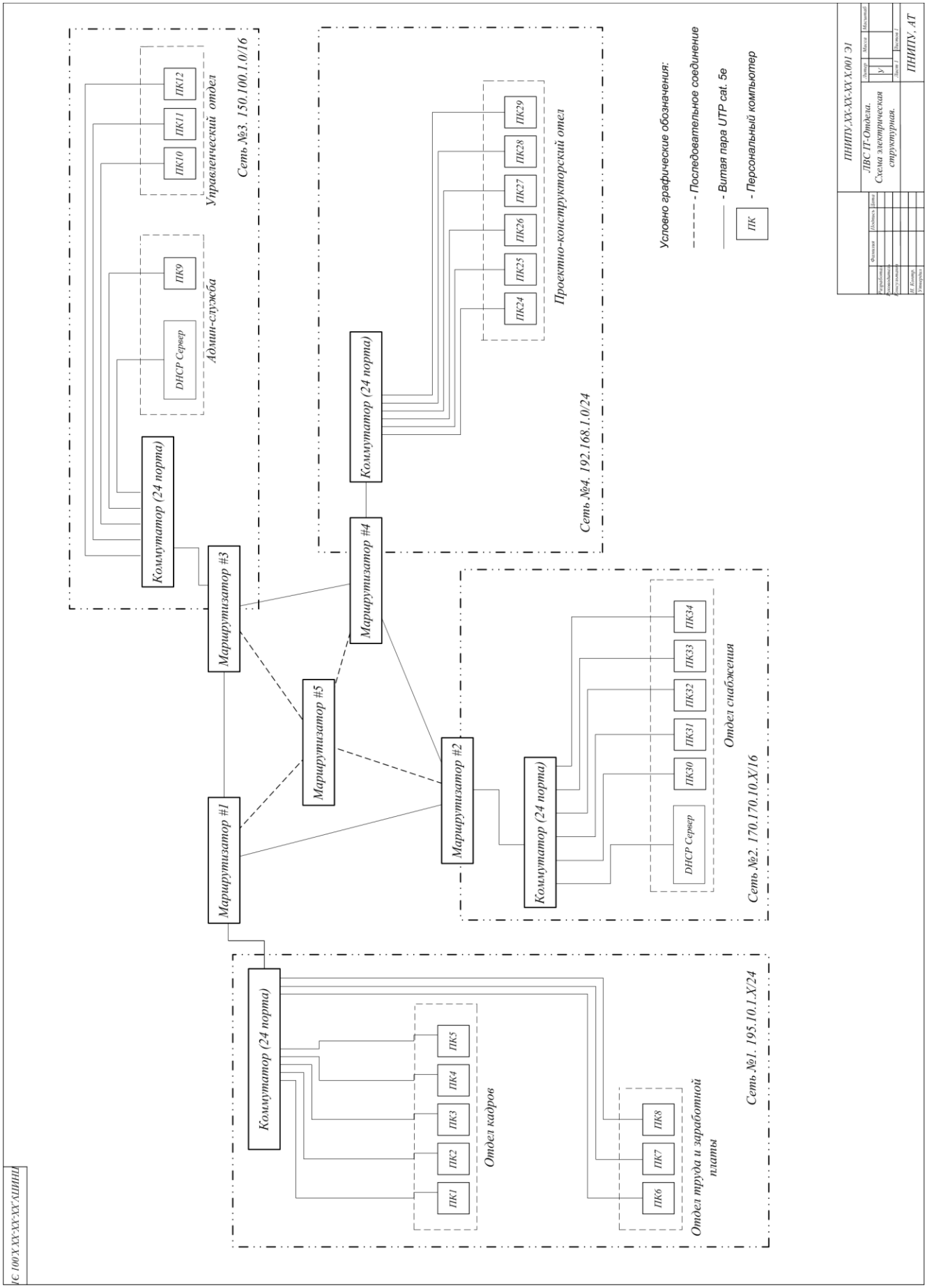


Рисунок 1 – Модель анализируемой сети

2. Конфигурация маршрутизаторов

Для настройки маршрутизаторов выполните следующие шаги:

1. Добавьте необходимые модульные платы в маршрутизаторы сети для организации необходимых последовательных соединений и соединений типа Fast Ethernet.
2. Сконфигурируйте интерфейсы маршрутизаторов. IP-адреса интерфейсов выбирайте из адресного пространства класса А. Для удобства настройки номера сетям выбирайте исходя из номеров соединяемых маршрутизаторов. Например, номер сети между маршрутизаторами 3 и 4 можно обозначить как 34 (меньшая цифра на первом месте).

3. Настройка статической маршрутизации

Правила статической маршрутизации сходны с динамической и содержат:

- Адрес сети назначения пакета (Network destination)
- Маска сети назначения (Mask network)
- Адрес следующего сетевого интерфейса (Next hop) куда требуется передать пакет.

Рассмотрим пример настройки маршрутизации пакетов от узлов сети №3 в сеть №1 по прямому соединению (рис. 1).

Настройка статической маршрутизации может выполняться с помощью графического интерфейса пользователя (graphical user interface, GUI) или с помощью командной строки (Command Line Interface, CLI).

Настройка статической маршрутизации из графического интерфейса:

9. Зайдите в настройки маршрутизатора #3 на закладку – Config (рис. 2).
10. Перейдите в раздел Routing и выберите настройка статической маршрутизации «Static».
11. Заполните поля статической маршрутизации. Для рассматриваемого примера:
    - Сеть назначения: 195.10.1.0

- Маска сети назначения: 255.255.255.0
- Адрес следующего интерфейса: 13.0.0.1

Нажмите кнопку Add для добавления правила маршрутизации в таблицу маршрутов. Не забывайте сохранять настройки маршрутизатора. Откройте таблицу маршрутов с помощью элемента «Увеличительное стекло» и убедитесь в наличии маршрута.

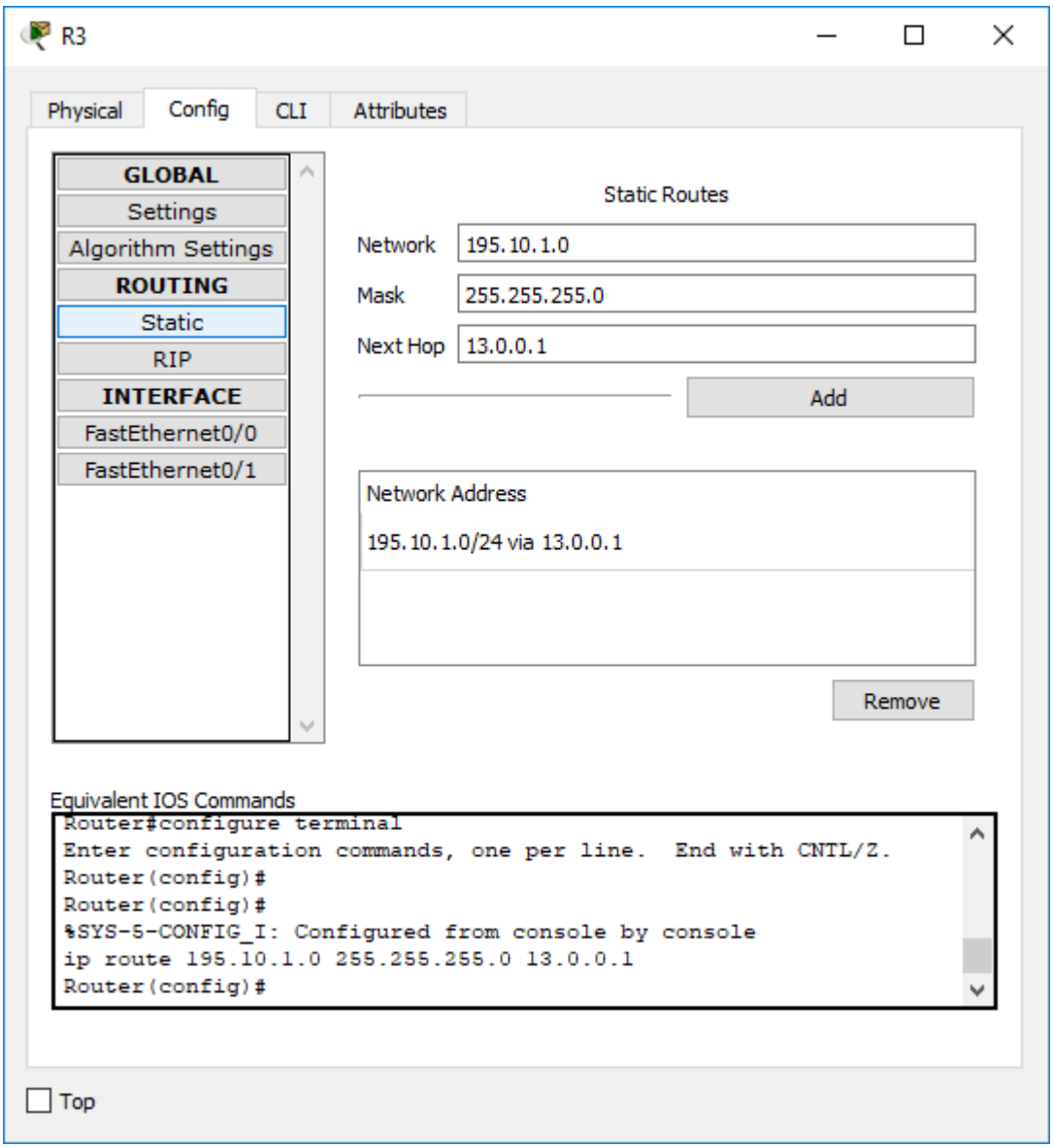


Рисунок 2 – Графический интерфейс настройки статической маршрутизации

Настройка статической маршрутизации из командной строки (консоли, рис. 2):

1. Router>enable
2. Router#configure terminal
3. ip route *ip_network mask next_hop*

Проверьте работоспособность сети выполнив трассировку маршрутов следования пакетов в сети.

Задание

Настроить статическую маршрутизацию в распределенной сети.

Содержание отчета:

- формулировка задачи;
- схема сети связи в Cisco Packet Tracer с настроенной статической маршрутизацией.

Указания к выполнению работы:

1. Изучить теоретический материал.

2. Построить схему сети связи в Cisco Packet Tracer с настроенной статической маршрутизацией.

Контрольные вопросы:

1. Что такое статическая маршрутизация? Для чего нужна?
2. Какие достоинства статической маршрутизации?

Литература

1. Работа с литературными источниками:

Олифер В.Г., Олифер Н.А. - Компьютерные сети. Принципы, технологии, протоколы (4-ое изд.) - 2010.

ЧАСТЬ IV. СЕТИ TCP/IP

Глава 17. Базовые протоколы TCP/IP. Общие свойства и классификация протоколов маршрутизации

2. Работа с мультимедийными источниками:

a. Статическая маршрутизация

https://www.youtube.com/watch?v=dp1IM4gor40