МЕЖГОСУДАРСТВЕННОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ОБРАЗОВАНИЯ
«БЕЛОРУССКО-РОССИЙСКИЙ УНИВЕРСИТЕТ»

Кафедра «Автоматизированные системы управления»

# КОМПЬЮТЕРНЫЕ СЕТИ

***Методические рекомендации к лабораторным работам для студентов специальности 6-05-0611-01 «Информационные системы и технологии» очной и заочной форм обучения***

Могилев 2025

УДК 004.7
ББК 32.971.35
К56

Рекомендовано к изданию
учебно-методическим отделом
Белорусско-Российского университета

Одобрено кафедрой «Автоматизированные системы управления» «29» августа 2025 г., протокол № 1

Составители: канд. техн. наук, доц. В. М. Ковальчук;
канд. техн. наук, доц. Ю. Д. Столяров

Рецензент канд. техн. наук, доц. С. К. Крутолевич

Методические рекомендации предназначены для студентов специальности 6-05-0611-01 «Информационные системы и технологии» очной и заочной форм обучения.

Учебное издание

КОМПЬЮТЕРНЫЕ СЕТИ

| | |
|---|---|
| Ответственный за выпуск | А. И. Якимов |
| Корректор | И. В. Голубцова |
| Компьютерная верстка | Н. П. Полевничая |

Подписано в печать . Формат 60 × 84/16. Бумага офсетная. Гарнитура Таймс.
Печать трафаретная. Усл. печ. л. . Уч.-изд. л. . Тираж 21 экз. Заказ №

Издатель и полиграфическое исполнение:
Межгосударственное образовательное учреждение высшего образования
«Белорусско-Российский университет».
Свидетельство о государственной регистрации издателя,
изготовителя, распространителя печатных изданий
№ 1/156 от 07.03.2019.
Пр-т Мира, 43, 212022, г. Могилев.

# Содержание

# Введение

Цель методических рекомендаций к лабораторным работам по дисциплине «Компьютерные сети» заключается в овладении и закреплении студентами практических навыков работы в компьютерных сетях.

Целью преподавания дисциплины является теоретическая и практическая подготовка специалистов по специальности «Информационные системы и технологии», обеспечивающая получение знаний по основам компьютерных сетей.

Дисциплина «Компьютерные сети» является неотъемлемой частью современных инженерных знаний и относится к модулю «Инструментальные средства разработки программ» (Государственной компоненты).

Полученные при изучении дисциплины знания и навыки будут востребованы при изучении специальных дисциплин инженерной направленности и станут инструментом для разрабатки модели компьютерных сетей, программы сетевого взаимодействия, использования аппаратных и программных компонентов компьютерных сетей при решении задач по направлениям деятельности, работы с сетевыми протоколами разных уровней.

# 1 Лабораторная работа № 1. Топология компьютерной сети

**Цель работы**: изучить топологии вычислительных сетей.

***Методические указания***

Сетевая топология – это способ описания конфигурации сети: схема расположения и соединения сетевых устройств, или/и схема прохождения электрических сигналов, или/и описание направления потоков информации.

Сетевая топология может быть:

– физической, которая описывает реальное расположение и связи между узлами сети и способ физического соединения компьютеров с помощью среды передачи, например, участками кабеля;

– логической, которая описывает пути и направление передачи потоков данных между сетевыми устройствами в рамках физической топологии и подразделяется на информационную, которая описывает направление потоков информации, передаваемых по сети, и управление обменом – это принцип передачи права на пользование сетью.

Выделяют три базовые топологии и ряд дополнительных производных типовых сетевых топологий, объединяющих компьютеры в единую сеть (таблица 1.1).

Таблица 1.1 – Типы сетевых топологий

| Базовый тип сетевых топологий | Производный (дополнительный) тип сетевых топологий | |
|---|---|---|
| Шина | Дерево | Двойное кольцо |
| Звезда | Ячеистая топология | Fat Tree |
| Кольцо | Полносвязная | Решётка |

***Порядок выполнения работы***

1 Изучить основные теоретические положения, сделав необходимые выписки в конспект.

2 Зарисовать расположение компьютеров в классе и определить тип топологии локальной сети.

3 Описать преимущества и недостатки каждого из базовых типов топологии.

4 Оформить отчет.

***Контрольные вопросы***

1 Дайте определение таким понятиям, как топология, Абонент, Сервер, Клиент.

2 Опираясь на определение топологии, назовите, что может описывать (отображать) топология сети.

3 Назовите базовые и дополнительные типы топологий.

4 Какие факторы, связанные с понятием «топология», могут повлиять на работоспособность сети?

5 Как влияет затухание сигнала на работоспособность сети.

6 Какие типы кабеля применяются при шинной топологии (тип коннектора, терминатор)?

7 Для каких целей применяется терминатор?

8 Преимущества и недостатки шинной топологии.

9 Для чего применяется «Репитер» в сети с шинной топологией?

10 Топология «Звезда». Нарисуйте схему и расскажите о принципе движения сигналов. Преимущества и недостатки данной топологии.

11 Активная и пассивная топология «Звезда».

12 Предельная длина сети с применением топологии «Звезда».

13 Топология «Кольцо». Нарисуйте схему и расскажите о принципе движения сигналов. Преимущества и недостатки данной топологии.

14 Топологии активное и пассивное дерево, особенности и отличия.

15 Другие типы топологий: звездно-шинная, звездно-кольцевая.

16 Сеточная топология: разновидности (названия), особенности, где и как применяются.

17 Назовите четыре разных понятия, относящихся к различным уровням сетевой архитектуры, связанных с топологией.

18 Какие факторы, параметры, требования влияют на выбор топологии реальной сети?

# 2 Лабораторная работа № 2. Моделирование различных топологий с использованием Packet Tracer (PT)

**Цель работы**: изучить принципы построения компьютерных сетей базовой топологии базовым набором аппаратных средств с применением симулятора сетей Packet Tracer.

***Методические указания***

Программный продукт Packet Tracer (PT) является симулятором сети передачи данных. Разработан фирмой Cisco Systems в рамках программы Сетевых академий Cisco. Packet Tracer позволяет имитировать работу различных сетевых устройств: маршрутизаторов, коммутаторов, точек беспроводного доступа, персональных компьютеров, сетевых принтеров, IP-телефонов и т. д.

С помощью Packet Tracer можно создавать работоспособные модели сети, настраивать (командами Cisco IOS) маршрутизаторы и коммутаторы, взаимодействовать между несколькими пользователями (через облако). Включает в себя серии маршрутизаторов Cisco 1800, 2600, 2800 и коммутаторов 2950, 2960, 3650. Кроме того, есть серверы DHCP, HTTP, TFTP, FTP, рабочие станции,

различные модули к компьютерам и маршрутизаторам, устройства Wi-Fi, различные кабели.

Cisco Packet Tracer (PT) является удобным средством моделирования сетей передачи данных различной топологии и сложности. Основные инструменты его интерфейса расположены и организованы вполне логично, что упрощает процесс освоения программы PT.

Основное окно программы одержит шесть основным меню, четыре из которых используются наиболее часто.

Стандартное программное меню мало чем отличается от подобного меню в других программах операционной системы Windows. Исключение составляют два инструмента на графической панели: Drawing Palette и Custom Device Dialog. В процессе выполнения лабораторных работ курса нет острой необходимости для использования этих инструментов. Остальные пункты меню вполне можно освоить самостоятельно.

***Порядок выполнения работы***

С помощью программного симулятора Packet Tracer необходимо построить простую сеть физической топологией «Звезда» и логической «Шина».

1 Выбираем тип оборудования «Концентраторы» (Hub’s) (рисунок 2.1).


Рисунок 2.1 – Выбор Hub's

2 В обновившемся меню «Список устройств данного типа оборудования» выбираем конкретный концентратор Hub-PT и перетаскиваем его в рабочую область «Логическое пространство» (рисунок 2.2).

3 Далее выбираем тип устройства «Конечные устройства», в дополнительном меню выбираем настольный компьютер PC-PT и также перетаскиваем в рабочую область. Таким образом, устанавливаем ещё три компьютера и один сервер. Используя инструмент Place Note (клавиша N), подписываем все устройства, а вверху рабочей области создаем заголовок проекта «Л.Р. №_2 Изучение топологии «Шина№ № Гр. Ф.И.О. », где указываем номер группы, фамилию, имя, отчество.

4 С целью исключения нагромождения рабочей области надписями уби-

раем надписи (метки) типов устройств: открываем меню Options в верхней части окна Packet Tracer, в ниспадающем списке выбираем Preferens и в диалоговом окне снимем галочку Show device model labels.

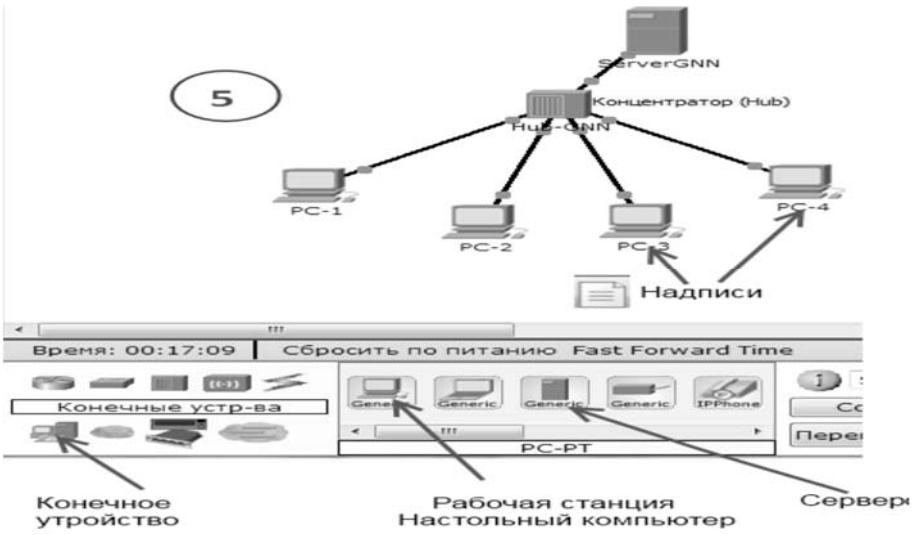


Рисунок 2.2 – Установка компьютеров и Hub's в рабочую область

5 Для подключения компьютеров и сервера к концентратору выбираем новый тип устройств «Соединения», т. е. линии связи, и далее выбираем «медный прямой» тип кабеля. Чтобы соединить сетевую карту компьютера (Рабочей станции) с портом Hub-a, щелкним левой клавишей мыши по нужному компьютеру. В открывшемся графическом меню выбираем порт FastEthernet0. Протягиваем кабель к концентратору, где в аналогичном меню выбираем любой свободный порт FastEthernet концентратора. Лучше придерживаться следующего правила: для сервера выбираем «0-й» порт, для PC-1 – «1-й» порт и т. д. Выполняем конфигурацию устройств в данной сети. Каждому компьютеру в сети присваиваем IP-адрес. Для этого двойным щелчком открываем нужный компьютер, далее – «Конфигурация» и в левой части окна – «Интерфейс» → FastEthetnet0. В группе параметров «Настройка IP» должно быть выбрано «Статический». В поле IP-адрес необходимо ввести IP-адрес компьютера. Состояние порта «Вкл.» (рисунок 2.3).

При вводе IP-адресов следует выполнять следующее правило. Для сервера вводим IP-адрес: 192.GGG.NN.10, где GGG – номер группы (только цифры), NN – порядковый номер по журналу группы, например 192.101.12.10.

Для компьютера PC-1 IP-адрес 192.GGG.NN.1 , PC-2: 192.GGG.NN.2 и т. д.

Маска подсети для всех компьютеров 255.255.255.0.

Обращайте внимание на установку всех остальных параметров.

6 Возле каждого компьютера создаем дополнительную надпись, содержащую IP- и MAC- адрес компьютера. Эти параметры следует скопировать с окна «Конфигурация».

7 При построении модели сети в данном случае лучше отключить отобра-

жение моделей устройств в рабочем окне программы. Для этого открываем последовательно меню Options → Preferences и снимаем галочку → Show Device Model Labels.

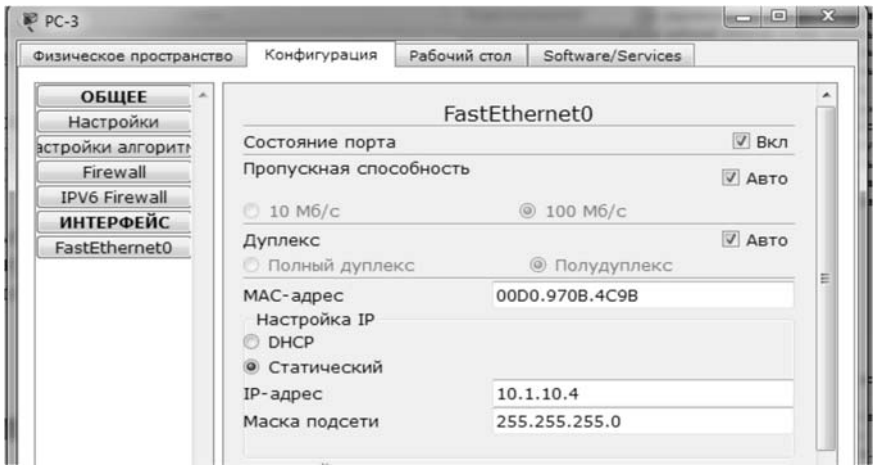


Рисунок 2.3 – Конфигурация компьютера PC-4

8 Для проверки работоспособности сети пробуем послать с компьютера на другой тестовый сигнал ping. Для этого открываем, например, компьютер PC-2, вкладку «Рабочий стол» → «Командную строку», в появившемся окне вводим команду ping 192.GGG.NN.10, нажимам Enter. Должны появиться сообщения об успешном прохождении сигнала ping до места назначения и обратно (рисунок 2.4).

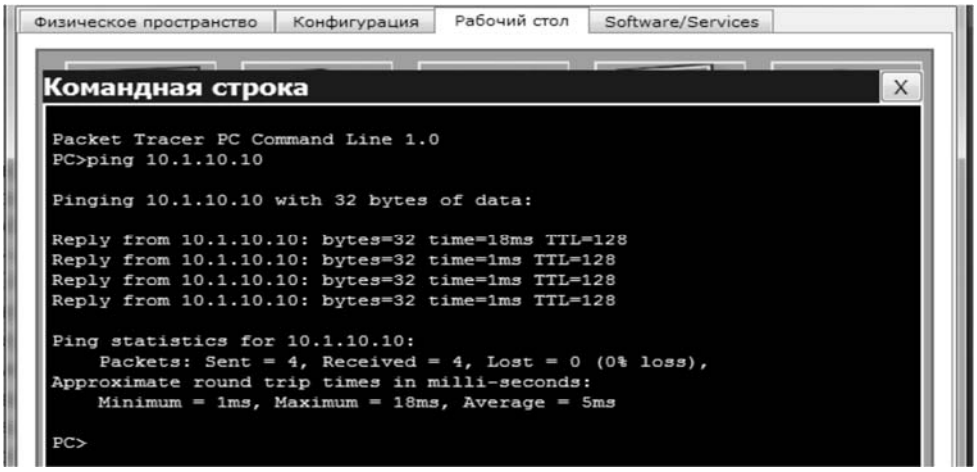


Рисунок 2.4 – Проверка связи командой ping

9 Посылаем тестовый сигнал ping от каждого компьютера к серверу, результаты фиксируем в Screen Shot's и вкладываем в отчет.

10 Для моделирования сети топологии «Звезда» будем использовать коммутатор CISCO 2960-24TT. Коммутатор является более сложным, интеллектуальным и функциональным сетевым устройством, чем концентратор.

11 Необходимо смоделировать локальную сеть (LAN) с использованием

коммутатора в качестве центрального коммутирующего сетевого устройства и концентратора как устройства для расширения сети (рисунок 2.5).

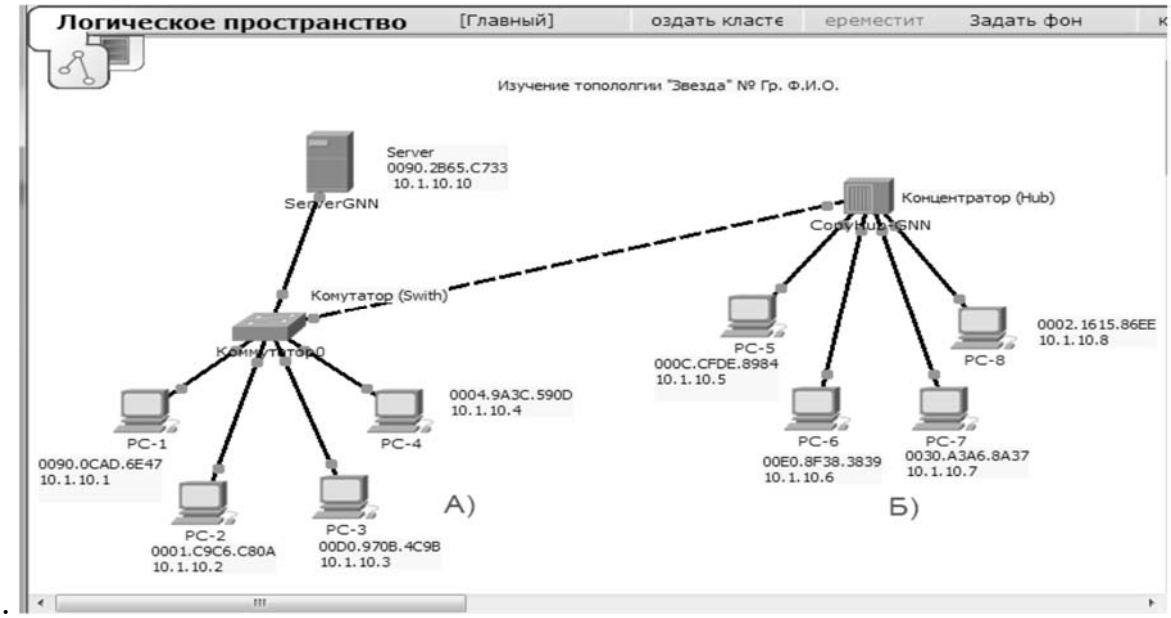


Рисунок 2.5 – Модель сети с использованием коммутатора и концентратора

12 Для создания модели новой сети открываем ранее созданный файл #LR2-Bus-Hub_FIO.pkt, сохраняем его под именем #LR2-Swith&Hub-Star_FIO.pkt.

13 Выделяем с помощью графического меню все элементы первого проекта. Копируем и вставляем. Далее перемещаем полученные копии на свободное пространство рабочего окна. Удаляем элемент CopyServer из скопированной подсети с помощью меню. В данной подсети сконфигурируем компьютеры в соответствии с рисунком 2.5 и вариантами, как в п. 5. При назначении новых IP-адресов 192.GGG.NN.XX необходимо также контролировать значения, используя альтернативный способ конфигурации IP-протокола. На каждом компьютере открываем вкладку «Рабочий стол» меню «Настройка IP» и проверяем значения IP-протокола, при необходимости корректируем.

14 В подсети А (см. рисунок 2.5) удаляем концентратор, на его место устанавливаем коммутатор Switch-2960-24TT, используя меню «Тип устройств» и «Модель сетевого устройства». Создаем надпись данного устройства.

15 Соединяем все компьютеры подсети А с портами коммутатора. Подключаем к коммутатору подсеть Б, при этом используем тип соединения – кабель «медный кроссовер». Результат зафиксируем в Screen Shot's.

16 Проверяем работоспособность всей сети с помощью команды ping с компьютеров PC-1…PC4 к Server и с компьютеров PC-5…PC8 к Server. Результат сохраняем в отчете ввиде Screen Shot's с пояснениями.

***Контрольные вопросы***

1 Назовите международный широко известный стандартизирующий институт по локальным вычислительным сетям и серию его стандартов.

2 Какие три группы аппаратного обеспечения являются составляющими компьютерных сетей и из каких компонентов они состоят?

3 Назовите основные программные компоненты и службы сетей.

4 Назовите разновидности сетевых карт в зависимости от технологий и стандартов.

5 Чем различаются сетевые карты для клиентских компьютеров и серверов?

6 Какие сетевые кабели применяются для локальных вычислительных сетей?

7 Разновидности коаксиальных кабелей, топология сетей и особенности подключения компьютеров при использовании данного типа кабеля.

8 Неэкранированная витая пара и особенности построения сетей с использованием кабеля UTP.

9 Концентратор, назначение, основные и дополнительные функции. Какой кабель применяется для подключения к концентратору? «Диаметр» сети (максимальная длина от одного компьютера к другому) с одним концентратором.

10 Дайте подробное объяснение: продвижение пакетов/кадров концентратором.

11 Какая топология (физическая и логическая) сети с концентратором?

12 Коммутаторы – основной «алгоритм прозрачного моста» – стандарт. Формат записи таблицы коммутации коммутатора.

13 Какие основные операции выполняют коммутатор и мост?

14 Коммутатор и классический мост. В чем их отличие и схожесть?

15 Основные отличия коммутатора и концентратора.

16 Маршрутизатор – назначение, протокол обмена данными.

17 Какие интерфейсы могут быть использованы в маршрутизаторах?

18 Что использует маршрутизатор для доставки пакетов данных?

19 Какие таблицы маршрутизации применяются маршрутизатором?

20 Старые и новые форматы IP-адреса. Формат адреса IPv4.

21 Как продвигаются данные (пакеты) при выходе с порта маршрутизатора в граничную локальную сеть?

22 С какими типами топологий можно строить сети на маршрутизаторах и почему?

23 Назовите основные полезные функции маршрутизаторов.

24 Что такое модель OSI? Базовая структура.

25 Что описывается в модели OSI?

26 Назовите назначение и основные функции двух нижних уровней модели OSI.

27 Назовите подуровни канального уровня.

28 Что означает PDU?

# 3 Лабораторная работа № 3. Изучение протоколов доступа к среде передачи LAN

**Цель работы**: изучить протоколы доступа к среде передачи LAN, метод случайного доступа, детерминированный доступ, канальный уровень, подуровни LLC и MAC, MAC-адрес, формат кадра Ethernet.

***Методические указания***

Существуют различные методы, способы и порядок доступа к физической среде, обеспечивающей передачу дискретной информации между компьютерами. По порядку доступа среда передачи может быть индивидуальной или разделяемой. Индивидуальной средой передачи является линия связи, к каждому окончанию которой подключено только одно устройство. Устройство единолично владеет линией все время и получает всю ее пропускную способность в свое распоряжение. Например, в топологии «Ззвезда» каждый компьютер связан с центральным узлом по индивидуальной линии. Но в сети, где устройства сети включены физически по схеме «Звезда», могут использовать способы передачи сигнала топологий «Шина» или «Кольцо». Сеть, построенная «Линейная сеть» либо «Полносвязанная сеть», где все компьютеры связаны между собой, представляет собой индивидуальную среду.

Разделяемой средой передачи (shared media) называется линия, которая используется попеременно несколькими (более чем двумя) устройствами, подключенными к ней.

Примерами связи компьютеров посредством разделяемой среды являются системы с топологией «Общая шина» и «Кольцо». В связи с совместным использованием разделяемых линий возникают проблемы как электрического характера (обеспечение нужного уровня сигнала при подключении к одному кабелю нескольких приемников и передатчиков), так и логического (разделение доступа к кабелю во времени между всеми устройствами). Система с разделяемой средой при увеличении количества подключенных к ней компьютеров будет работать все медленнее, поскольку пропускная способность линии делится между всеми компьютерами. То есть в этом случае за экономичность структуры локального сегмента приходится расплачиваться его производительностью. Несмотря на эти проблемы, подключение к сети посредством разделяемой среды применяется очень часто. Этот подход реализован в широко распространенных классических технологиях Ethernet (для общей шины) и Token Ring (для кольца).

В технологиях Token Ring и FDDI тот факт, что компьютеры используют разделяемую среду, не так очевиден, как в случае Ethernet. Физическая топология этих сетей – кольцо, каждый узел соединяется кабелем с двумя соседними узлами. Однако эти отрезки кабеля также являются разделяемыми, т. к. в каждый момент времени только один компьютер может использовать кольцо для передачи своих пакетов.

Существуют два основных метода доступа к разделяемой физической среде:

1) метод случайного доступа;

2) детерминированный доступ.

Метод случайного доступа является одним из основных методов захвата разделяемой среды. Он основан на том, что узел, у которого есть кадр для передачи, пытается его отправить без какой бы то ни было предварительной процедуры согласования времени использования разделяемой среды с другими узлами сети.

Метод случайного доступа является децентрализованным, он не требует наличия в сети специального узла, который играл бы роль арбитра, регулирующего доступ к среде. Результатом этого является высокая вероятность коллизий, т. е. случаев одновременной передачи кадра несколькими станциями. Во время коллизии происходит наложение сигналов нескольких передатчиков, из-за чего информация всех передаваемых на периоде коллизии кадров искажается.

Детерминированный доступ – это другой популярный подход к обеспечению доступа к разделяемой среде. Он получил свое название благодаря тому, что максимальное время ожидания доступа к среде всегда известно. Алгоритмы детерминированного доступа используют два механизма – передачу токена и опрос.

Передача токена обычно реализуется децентрализовано. Каждый компьютер, получивший токен, имеет право на использование разделяемой среды в течение фиксированного промежутка времени – времени удержания токена. В это время компьютер передает свои кадры. После истечения этого промежутка компьютер обязан передать токен другому компьютеру. Таким образом, если знаем количество компьютеров в сети, то максимальное время ожидания доступа равно произведению времени удержания токена на это число. Время ожидания может быть и меньше, поскольку если компьютер, получивший токен, не имеет кадров для передачи, то он передает его следующему компьютеру, не дожидаясь истечения времени удержания. Последовательность передачи токена от компьютера к компьютеру может определяться разными способами. В сетях Token Ring и FDDI она определяется топологией связей. Компьютер в кольце получает токен от предыдущего соседа, а передает токен следующему.

Алгоритмы опроса чаще всего основаны на централизованной схеме. В сети существует выделенный узел, который играет роль арбитра в споре узлов за разделяемую среду. Арбитр периодически опрашивает узлы сети на наличие кадров для передачи. Собрав заявки на передачу, арбитр решает, какому узлу он предоставит право использования разделяемой среды, сообщая свое решение выбранному узлу. После завершения передачи кадра фаза опроса повторяется.

Алгоритм детерминированного доступа более эффективен алгоритма случайного доступа при большой загрузке сети, когда коэффициент использования приближается к единице. В то же время при небольшой загрузке сети более

эффективными являются алгоритмы случайного доступа, т. к они позволяют передать кадр немедленно.

Разработано достаточно много различных протоколов доступа, использующих тот или иной порядок, метод доступа к физической среде.

При случайном (вероятностном – probabilistic) методе доступа узел, желающий послать кадр в сеть, прослушивает линию. Если линия занята или обнаружена коллизия (столкновение сигналов от двух передатчиков), попытка передачи откладывается на некоторое время. К этим методам относятся следующие.

CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance**)** – множественный доступ с прослушиванием несущей и избежанием коллизий. Узел, готовый послать кадр, прослушивает линию. При отсутствии несущей он посылает короткий сигнал запроса на передачу (RTS) и определенное время ожидает ответа (CTS) от адресата назначения. При отсутствии ответа (подразумевается возможность коллизии) попытка передачи откладывается, при получении ответа в линию посылается кадр. При запросе на широковещательную передачу (RTS содержит адрес 255) CTS не ожидается. Метод не позволяет полностью избежать коллизий, но они обрабатываются на вышестоящих уровнях протокола. Метод применяется в сети Apple Local-Talk, характеризуется простотой и низкой стоимостью цепей доступа.

CSMA/CD (Carrier Sense Multiple Access/Collision Detect**)** – множественный доступ с прослушиванием несущей и обнаружением коллизий. Узел, готовый послать кадр, прослушивает линию. При отсутствии несущей он начинает передачу кадра, одновременно контролируя состояние линии. При обнаружении коллизии передача прекращается, и повторная попытка откладывается на случайное время. Коллизии – нормальное, хотя и не очень частое явление для CSMA/CD. Их частота связана с количеством и активностью подключенных узлов. Нормально коллизии могут начинаться в определенном временном окне кадра, запоздалые коллизии сигнализируют об аппаратных неполадках в кабеле или узлах. Метод эффективнее, чем CSMA/CA, но требует более сложных и дорогих схем цепей доступа. Применяется во многих сетевых архитектурах: Ethernet, EtherTalk (реализация Ethernet фирмы Apple), G-Net, IBM PC Network, AT&T Star LAN.

При детерминированным методе доступа применяются следующие.

TPMA (Token Passing Multiple Access) – множественный доступ с передачей полномочия, или метод с передачей маркера.

Метод с передачей маркера – это метод доступа к среде, в котором от рабочей станции к рабочей станции передается маркер, дающий разрешение на передачу сообщения. При получении маркера рабочая станция может передавать сообщение, присоединяя его к маркеру, который переносит это сообщение по сети. Каждая станция между передающей станцией и принимающей видит это сообщение, но только станция- адресат принимает его. При этом она создает новый маркер. Маркер (token), или полномочие, – уникальная комбинация битов, позволяющая начать передачу данных.

Каждый узел принимает пакет от предыдущего, восстанавливает уровни сигналов до номинального уровня и передает дальше. Передаваемый пакет может содержать данные или являться маркером. Когда рабочей станции необходимо передать пакет, ее адаптер дожидается поступления маркера, а затем преобразует его в пакет, содержащий данные, отформатированные по протоколу соответствующего уровня, и передает результат далее по ЛВС.

Пакет распространяется по ЛВС от адаптера к адаптеру, пока не найдет своего адресата, который установит в нем определенные биты для подтверждения того, что данные достигли адресата, и ретранслирует его вновь в ЛВС. После чего пакет возвращается в узел, из которого был отправлен. Здесь после проверки безошибочной передачи пакета узел освобождает ЛВС, выпуская новый маркер. Таким образом, в ЛВС с передачей маркера невозможны коллизии (конфликты). Метод с передачей маркера в основном используется в кольцевой топологии.

TDMA (Time Division Multiple Access) – множественный доступ с разделением во времени, основан на распределении работы канала между системами.

Доступ TDMA основан на использовании специального устройства, называемого тактовым генератором. Этот генератор делит время канала на повторяющиеся циклы. Каждый из циклов начинается сигналом-разграничителем (сигнал синхронизации). Цикл включает *n* (обычно 30) пронумерованных временных интервалов, называемых ячейками. Интервалы предоставляются для загрузки в них блоков данных.

### *Порядок выполнения работы*

1 Изучить основные теоретические положения, сделав необходимые выписки в конспект.

2 Письмено ответить на контрольные вопросы.

3 Оформить отчет.

### *Контрольные вопросы*

1 Порядок доступа к физической среде.

2 Что означает индивидуальная среда и разделяемая?

3 Какие топологии могут использовать индивидуальную среду и разделяемую и в каких технологиях они используются?

4 Два основных метода доступа к разделяемой физической среде.

5 При каком методе доступа используются передача токена, алгоритм опроса и множественный доступ с прослушиванием несущей?

6 Общие принципы и различия методов доступа CSMA/CA и CSMA/CD.

7 Принципы работы методов доступа TPMA, TDMA, FDMA.

8 Уровень MAC. Передача, формирование и прием кадра.

9 MAC-адреса.

10 Алгоритм CSMA/CD. Что означает Multiply Access-MA, Carrier Sense-CS?

11 Алгоритм CSMA/CD. Доступ к среде и передача данных. Для чего нужны преамбула, ограничитель начала кадров, межпакетный интервал IGP?

12 Возникновение коллизии. В каких буквах название CSMA/CD отражается обнаружение коллизий?

13 Что такое jam-последовательность, интервал отсрочки?

14 Как вычисляется пауза для повторной передачи кадра после обнаружения коллизий?

15 Время оборота PDV (RTT) и распознавание коллизий.

16 Определите максимальное количество кадров минимальной и максимальной длины, проходящих по стандартному сегменту Ethernet (10Base-5).

17 Определите максимальную пропускную способность сегмента 10Base 5 в Мбит/с для кадров максимальной длины, усредненной и минимальной.

18 Изобразите схематично в виде стандартных блоков алгоритм передачи кадра MAC-уровня с доступом CSMA/CD с объяснением принципа работы (согласовать с преподавателем).

# 4 Лабораторная работа № 4. Базовые настройки коммутатора CISCO Packet Tracer

**Цель работы**: изучить базовую настройку коммутатора Cisco.

***Методические указания***

Базовая настройка одинакова для всех устройств Cisco, будь то коммутатор, маршрутизатор, IP-телефон либо точка доступа.

Первое, о чём хотелось бы сказать, – это что такое коммутатор и принцип его действия. Коммутатор – это сетевое устройство, которое объединяет оконечное устройство в локальную сеть. Оконечными устройствами в данном случае выступают персональные компьютеры (ПК), принтеры и др.

На сетевых устройствах, как и на компьютерах, есть операционная система. В данном случае это сетевая ОС Cisco IOS, которая обладает одной особенностью – для повышения производительности устройства она из флэш-памяти выгружается в ОЗУ. Но есть один нюанс: ОЗУ – это энергозависимая память, поэтому если не сохраните настройки, то они попросту слетят, ввиду чего всегда необходимо сохранять настройки, которые были совершены.

Способы подключения к коммутатору:

– через консоль, т. е. по внеполосному доступу, в обход всех проводных подключений;

– удалённо через telnet;

– удалённо через SSH.

Для подключения через консоль потребуется консольный кабель. Преимущество использования консоли в том, что если нет никаких настроек, то с использованием консольного кабеля это можно всё произвести с нуля.

Следующий способ подключения к коммутатору – удалённое подключение через telnet. Это достаточно удобный способ, т. к. можно с любого компьютера подключиться на коммутатор и зайти в командную строку. Но есть один нюанс: там должны быть уже настроены виртуальный интерфейс, IP-адрес, маска подсети и на самом коммутаторе шлюз подсети, а также коммутатор должен быть уже подключён к маршрутизатору для того, чтобы трафик мог выходить в сеть и была возможность зайти на свой коммутатор.

Следующий способ подключения – подключение через SSH. По сути, это подключение такое же, как и через telnet, но с одним нюансом: все пароли шифруются, соответственно, данный протокол является более защищённым.

Для того чтобы начать базовую настройку, необходимо получить доступ к командной строке. Чтобы это сделать, существуют специальные программы – эмуляторы терминала: для Windows – HyperTerminal и PuTTY, для Linux – Minicom.

Коммутатор подключён по консольному соединению, также подключён к стойке. Хотелось бы отметить, что идёт во время загрузки: сначала коммутатор делает Power-On-Self-Test (POST), подгружает Bootstrap, после этого ищет образ Cisco IOS, загружает его и после этого можно начинать работу. С помощью команды show можно просмотреть всё, что угодно. Также из данного режима можно перезагрузить коммутатор с помощью команды reload. Попадаем в командную строку. На устройствах Cisco существует несколько разных режимов конфигурации: пользовательский, привилегированный, глобальной конфигурации и несколько режимов тонкой настройки. Конкретно тот режим, в котором сейчас находимся, – пользовательский (режим просмотра). С этого режима можно пропинговать и ограниченно просмотреть некоторые моменты. Для того чтобы попасть в следующий режим, а именно в привилегированный, пропишем команду enable: Switch>enable.

После выполнения данной команды попадаем в привилегированный режим, об этом сигнализирует запись Switch#. Из данного режима можно прописать в следующий режим. Прописываем команду configure terminal: Switch# configure terminal. После выполнения данной команды попадаем в режим глобальной конфигурации Switch(config)#. Этот режим и всё, что в нём будет сделано, влияют на коммутатор, т. е. именно из этого режима будем изменять настройки.

Первое, что можем сделать, – задать имя устройству с помощью команды hostname s1, где s1 – имя устройства. Хотелось бы отметить то, что название должно быть логичным, понятным и легко запоминающимся. Есть ещё некоторые требования к названиям: они могут состоять из цифр, букв, но не должны содержать пробелов, т. к. данное имя устройства попросту не сохранится.

Следующее, что хотелось бы сделать, – это обезопасить все виды подключений, чтобы к консоли не было доступа посторонних лиц. В первую очередь обезопасим переход к привилегированному режиму. Это можно сделать двумя способами: есть команда enable password, где выбирается определённый пароль, и команда enable secret, где также можно задать определённый пароль. Их отличие состоит в том, что если прописывается команда enable

secret, то пароль будет зашифрован. При установке паролей необходимо учитывать то, что пароль должен быть таким, чтобы его было сложно подобрать. В связи с тем, что нас консольное соединение, его также лучше защитить. Чтобы это сделать, надо зайти в более тонкий режим настройки с помощью команды line console 0. О переходе в более тонкий режим свидетельствует запись S1(config-line)#. Устанавливаем на него пароль с помощью команды password. Далее необходимо запустить процесс аутентификации, прописав команду login, а затем выйти из данного режима настройки с помощью команды exit. Следующий раз, когда человек захочет подключиться по консольному подключению, ему будет выдано сообщение, что ему необходимо ввести пароль. Далее, если захотим удалённо работать с коммутатором, необходимо защитить терминальное соединение. По умолчанию на коммутаторах Cisco существует 16 линий VTY от 0 до 15. Поэтому команда, чтобы перейти в более тонкий режим, будет выглядеть следующим образом: line vty 0 15. Далее проводим те же операции, что и с консольным соединением: устанавливаем на него пароль с помощью команды password, затем необходимо запустить процесс аутентификации, прописав команду login, и в завершение выйти из данного режима настройки с помощью команды exit. Для того чтобы зашифровать все пароли, нужна такая функция, как service password-encryption. На этом работа с защитой заканчивается.

Также есть такая функция, как баннерное сообщение. Баннерное сообщение – это сообщение о том, что неавторизованный пользователь не имеет права входить в систему. Это существует для судебных исков, очень распространено в США, Европе, поэтому также можно организовать при настройке коммутатора. Это делается с помощью команды banner notd #AUTHORIZED ACCESS ONLY#, где сообщение начинается и заканчивается со знака #, но эти символы могут быть другими, главное – они должны быть совпадать. После выполнения данной команды баннер настроен. Теперь, если кто-то попытается войти в систему, ему высветится сообщение, что заходить может только авторизованный пользователь.

Ранее упоминалось про подключение через telnet и SSH. Для подключения через telnet необходимо настроить виртуальный интерфейс. Это производится с помощью команды interface vlan1. После выполнения данной команды попадаем в следующий режим: S1(config-if)#. Для виртуального интерфейса необходимо настроить IP-адрес. Это делается с помощью команды ip address, которая в консоли прописывается следующим образом: S1(config-if)#ip address 192.168.29.43 255.255.255.0, где 192.168.29.43 – IP-адрес интерфейса, а 255.255.255.0 – маска подсети. Также необходимо запустить данный интерфейс с помощью команды no shutdown. После этого выходим из режима интерфейса с помощью команды exit. После выполнения данной команды видим строку в консоли S1(config)#. Следующее, что необходимо настроить, – это адрес шлюза по умолчанию. Это делается с помощью команды ip default-gateway 192.168.29.1, где 192.168.29.1 – IP-адрес шлюза. После этого настройка интерфейса окончена. Имеется возможность удалённого доступа на коммутатор.

Теперь важный момент. Необходимо сохранить настройки. Это делается с помощью команды copy running-config startup-config, которая выглядит следующим образом в консоли: S1# copy running-config startup-config. После чего билдится конфигурация и сохраняются настройки.

***Порядок выполнения работы***

1 Изучить основные теоретические положения, сделав необходимые выписки в конспект.
2 Письмено ответить на контрольные вопросы.
3 Оформить отчет.

***Контрольные вопросы***

1 Что такое коммутатор? Принцип его действия.
2 Назовите способы подключения к коммутатору.
3 Назовите несколько разных режимов конфигурации Cisco.

# 5 Лабораторная работа № 5. Изучение локальных сетей (VLAN) Packet Tracer

**Цель работы**: изучить общие принципы работы виртуальных сетей VLAN, назначение и особенности построения VLAN на одном коммутаторе при помощи эмулятора CISCO Packet Tracer.

***Методические указания***

Виртуальная локальная сеть (Virtual Local Area Network, VLAN) представляет собой коммутируемый сегмент сети, который логически выделен по выполняемым функциям, рабочим группам или приложениям вне зависимости от физического расположения пользователей. Виртуальные локальные сети обладают всеми свойствами физических локальных сетей, но рабочие станции можно группировать, даже если они физически расположены не в одном сегменте, т. к. любой порт коммутатора можно настроить на принадлежность определенной VLAN. При этом одноадресный, многоадресный и широковещательный трафик будет передаваться только между рабочими станциями, принадлежащими одной VLAN. Каждая VLAN рассматривается как логическая сеть, т. е. пакеты для данной VLAN будут коммутироваться коммутатором только в пределах этой VLAN.

Для того чтобы трафик одной VLAN попадал в другую, применяются сетевые устройства третьего уровня OSI, а именно маршрутизаторы.

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 VLAN-сетей может осуществляться различными способоми. В основном применяются три типа VLAN:

1) VLAN на базе портов;

2) VLAN на базе MAC-адресов;

3) VLAN на основе меток в дополнительном поле кадра (стандарт IEEE 802.1Q).

При использовании VLAN на базе портов каждый порт назначается в определенную VLAN независимо от того, какой пользователь, или компьютер, или Hub подключены к этому порту. Это означает, что все пользователи, подключенные к этому порту, будут членами одной VLAN. Конфигурация портов статическая и может быть изменена только вручную.

Основные характеристики VLAN на базе портов:

– применяются в пределах одного коммутатора – если необходимо организовать несколько рабочих групп в пределах небольшой сети на основе одного коммутатора, например, разнести технический отдел и отдел продаж, то решение VLAN на базе портов оптимально подходит для данной задачи;

– простота настройки – создание виртуальных сетей на основе группирования портов не требует от администратора большого объема ручной работы, достаточно каждому порту, находящемуся в одной VLAN, присвоить один и тот же идентификатор VLAN (VLAN ID);

– возможность изменения логической топологии сети без физического перемещения станций – достаточно всего лишь изменить настройки порта с одной VLAN (например, VLAN технического отдела) на другую (VLAN отдела продаж), как рабочая станция сразу же получает возможность совместно использовать ресурсы с членами новой VLAN. Таким образом, VLAN обеспечивают гибкость при перемещениях, изменениях и наращивании сети.

Каждый порт может входить только в один VLAN. Поэтому для объединения виртуальных подсетей как внутри одного коммутатора, так и между двумя коммутаторами нужно использовать сетевой уровень (третий уровень модели ISO/OSI). Один из портов каждой VLAN подключается к интерфейсу маршрутизатора, который создает таблицу маршрутизации для пересылки пакетов из одной подсети в другую, при этом IP-адреса подсетей должны быть разными.

### *Порядок выполнения работы*

1 Для создания сети, согласно рисунку 5.1, используем коммутатор cisco 2960-24PT, девять компьютеров PC-PT, один сервер Server-PT.

2 Первые три PC-PT (ПК-0-ПК-2) будем считать как хосты бухгалтерии – buh, следующие три компьютера (ПК-3-ПК-5) – компьютеры отдела продаж – Sales, остальные компьютеры и сервер отнесем к отделу маркетинга – Market.

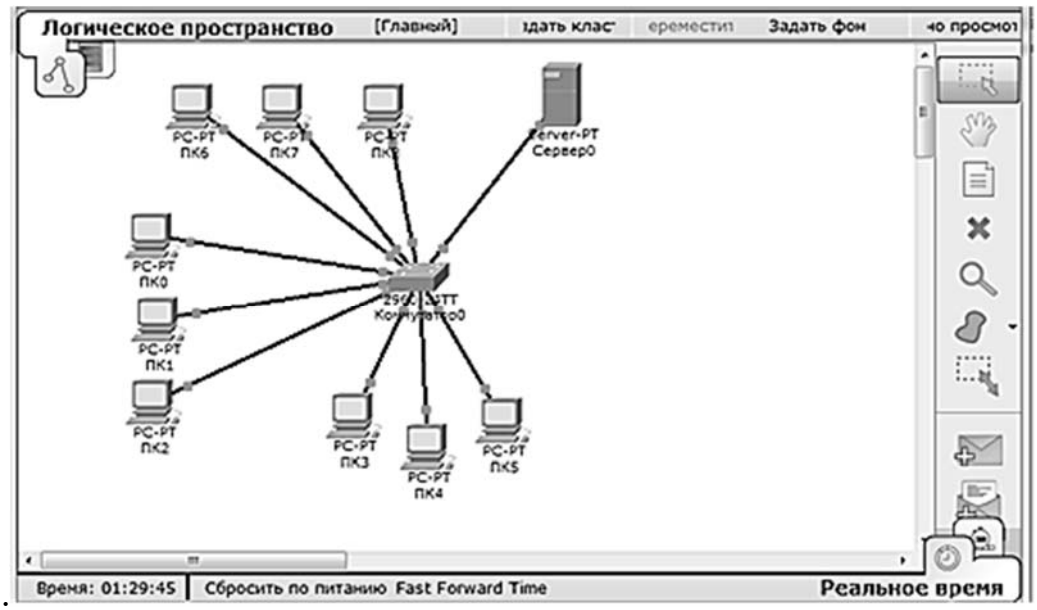


Рисунок 5.1 – Топология сети с одним коммутатором

3 Присвоим IP-адреса каждому хосту и серверу согласно следующему правилу:

– для ПК-0 IP adress 10.10.NN.G01;

– для ПК-1 IP adress 10.10.NN.G02 и т. д.;

– для Sever-PT IP adress 10.10.NN.G10 (где NN – порядковый номер в журнале группы, G – порядковый номер группы («1» – для первой группы «2» для второй группы).

4 Данные компьютеры соединим с портами коммутатора согласно таблице 5.1, приведённой ниже (в отчёте создать аналогичную таблицу 5.1 с конкретными данными согласно вариантам). Маска на каждом из компьютеров должна соответствовать 255.255.255.0.

Таблица 5.1 – Первоначальная конфигурация сети LAN

| Отдел | Компьютер | IP-адрес | Номер порта коммутатора |
|---|---|---|---|
| Бухгалтерия (Buh) | ПК-0 | 10.10.12.101 | Fa 0/1 |
| | ПК-1 | 10.10.12.102 | Fa 0/2 |
| | ПК-2 | 10.10.12.103 | Fa 0/3 |
| Отдел продаж (Sales) | ПК-3 | 10.10.12.104 | Fa 0/4 |
| | ПК-4 | 10.10.12.105 | Fa 0/5 |
| | ПК-5 | 10.10.12.106 | Fa 0/6 |
| Отдел маркетинга (Market) | ПК-6 | 10.10.12.107 | Fa 0/7 |
| | ПК-7 | 10.10.12.108 | Fa 0/8 |
| | ПК-8 | 10.10.12.109 | Fa 0/9 |
| | Server | 10.10.12.110 | Fa 0/10 |

5 Проверим прохождение пакетов каждого из компьютеров к серверу и между собой. Результат зафиксируем в отчете (рисунок 5.2).

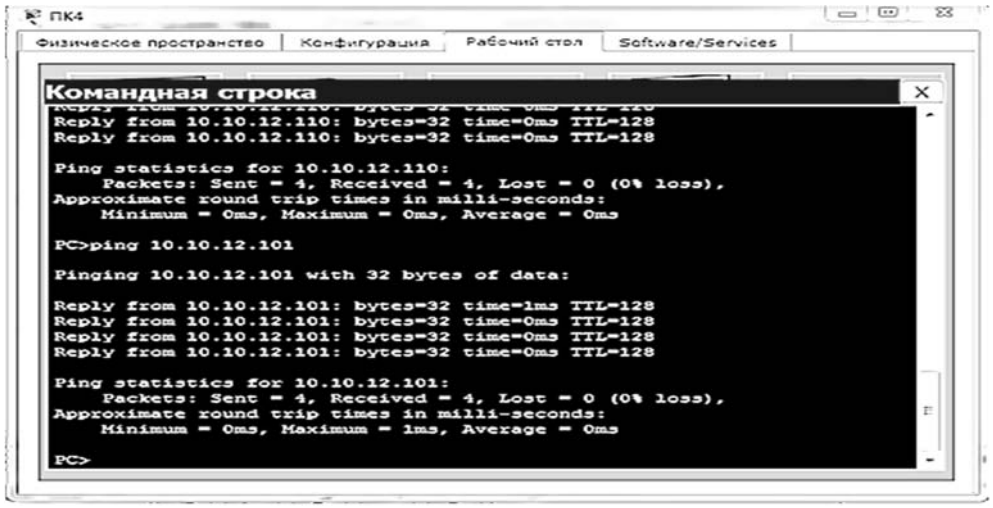


Рисунок 5.2 – Прохождение тестовых пакетов между ПК-4, Server, ПК-4 и ПК-0

6 Данная сеть являтся сетью одного адресного пространства IP-адресов и одного широковещательного домена. Проверим данное утверждение. Переключимся в режим симуляции и создадим комплексный PDU: щёлкнув по элементу меню «Комплексное PDU», с помощью мышки перенесём его на любой компьютер. Откроется диалоговое окно с параметрами IP-пакета, заполним поля диалогового окна, как показано на рисунке 5.3, в соответствии со своими вариантами, нажимаем кнопку «Создать PDU». IP-адрес назначения и источника заполняется в соответствии с IP-номерами варианта и используемого компьютера (в данном случае представлен 12 вариант первой группы и ПК-5). Последний октед IP-адреса назначения должен равняться значению 255, т. е. широковещательная рассылка с использованием IP-протокола.

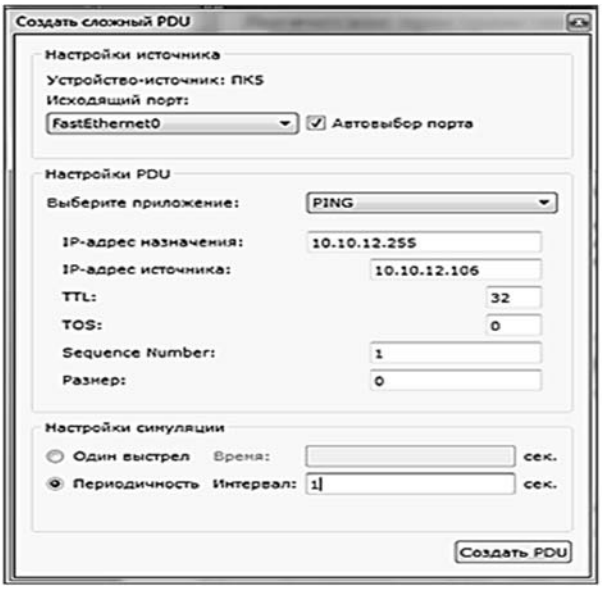


Рисунок 5.3 – Диалоговое окно «Создание комплексного PDU»

На выбранном компьютере появится сохраненный пакет, дважды щёлкнув по нему откроем информационное окно (рисунок 5.4). Проанализируем его и сделаем Screen Shot's, сохранив в отчете. Обращаем внимание на выделенные желтым цветом параметы пакета.

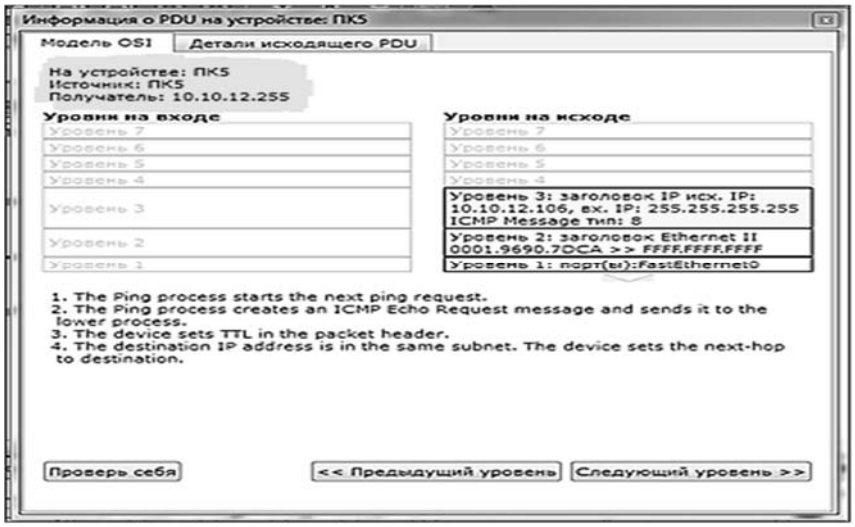


Рисунок 5.4 – Информационное окно «Комплексный PDU»

Используя кнопки «Захват/Вперед», проследим прохождение пакета по сети. Здесь видно сразу, что созданный пакет распространяется на все компьютеры сети (рисунок 5.5). Таким образом, данная сеть является сетью с единым широковещательным доменом. Сохраним файл для отчета.

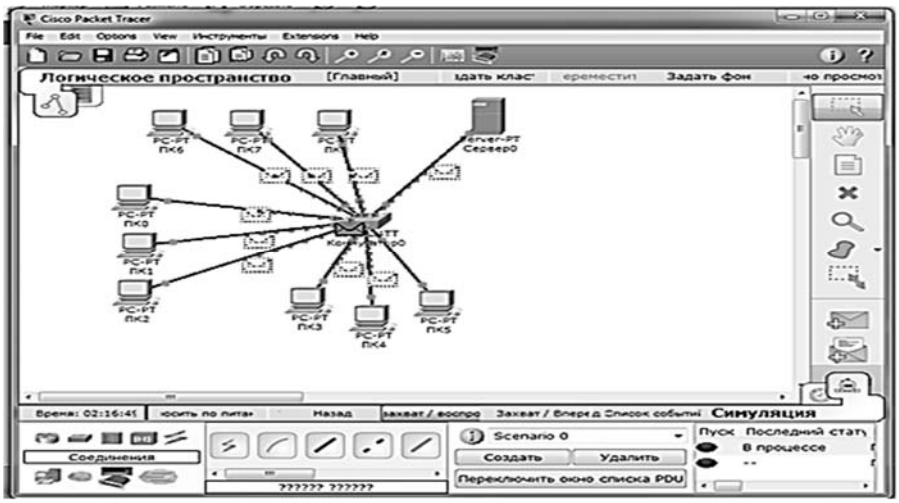


Рисунок 5.5 – Передача широковещательного пакета/кадра на все задействованные порты коммутатора

7 Используя возможность конфигурации коммутатора cisco 2960, разделим сеть на три виртуалные локальные сети VLAN.

8 Каждая VLAN имеет свой индентификатор – диапазон номеров 1–4096, который условно делится на «нормальный диапазон»: 1–1005 и «расширен-

ный» 1006–4094. Номера 1002–1005 назначаются для виртуальных сетей технологий Token Ring и FDDI.

9 Создадим три VLAN для одного коммутатора, используя статическое конфигурирование. Создание виртуальных сетей может производиться двумя способами:

1) в режиме глобального конфигурирования;

2) из привилегированного режима конфигурирования по команде vlan database.

Корпорация Cisco рекомендует использовать первый способ создания VLAN’s. Создаём VLAN, используя первый способ, в режиме глобального конфигурирования:

– используя CLI, входим в привеллегированный режим Switch>enable;

– переходим в режим глобального конфигурирования командами Switch#conf term, Switch(config)#;

– создаём первую VLAN по правилу для выбора VLAN IDVLAN =NN*10+NumVLAN (NN – порядковый номер по журналу) командами Switch(config)#vlan 121, Switch(config-vlan)#;

– аналогично создаем вторую и третью VLAN’s Switch(config)#vlan 122, Switch(config-vlan)#vlan 123;

– присвоим имена созданым VLAN's, согласно таблице 5.1, с помощью команд Switch(config)#vlan 121, Switch(config-vlan)#name Buh, Switch(config-vlan)#vlan 122, Switch(config-vlan)#name Sales, Switch(config-vlan)#vlan 123, Switch(config-vlan)#name Market;

– с помощью команды Switch(config-vlan)#do show vlan brief посмотрим состояние виртуальных сетей и интерфейсов коммутатора Cisco на данном этапе. Аналогичную команду можно использовать в глобальном режиме;

– для перехода в глобальный режим (рисунок 5.6) используем дважды команду exit и далее Switch(config)#show vlan brief или sh vlan brief.


Рисунок 5.6 – Состояние VLAN после первоначальной конфигурации

10 Следует обратить внимание, что все порты принадлежат VLAN 1 по умолчанию. В соответствии с исходным заданием дополняем таблицу 5.1 значениями IDVLAN и получаем таблицу 5.2.

11 Сконфигурируем порты коммутатора в соответствии с таблицей 5.2. Порты в коммутаторах Cisco назначаются одной из сетей VLAN. Такие порты обеспечивают соединение для конечных компьютеров пользователей или узловых устройств, таких как маршрутизатор и сервер, и называются портами доступа к сети (access ports). Стандартно все устройства назначаются сети VLAN 1, которая называется стандартной сетью VLAN (default VLAN).

Таблица 5.2 – Конфигурация VLAN коммутатора Cisco 2960

| Отдел | Компьютер | IP-адрес | Номер порта коммутатора | IDVLAN |
|---|---|---|---|---|
| Бухгалтерия (Buh) | ПК-0 | 10.10.12.101 | Fa 0/1 | 121 |
| | ПК-1 | 10.10.12.102 | Fa 0/2 | |
| | ПК-2 | 10.10.12.103 | Fa 0/3 | |
| Отдел продаж (Sales) | ПК-3 | 10.10.12.104 | Fa 0/4 | 122 |
| | ПК-4 | 10.10.12.105 | Fa 0/5 | |
| | ПК-5 | 10.10.12.106 | Fa 0/6 | |
| Отдел маркетинга (Market) | ПК-6 | 10.10.12.107 | Fa 0/7 | 123 |
| | ПК-7 | 10.10.12.108 | Fa 0/8 | |
| | ПК-8 | 10.10.12.109 | Fa 0/9 | |
| | Server | 10.10.12.110 | Fa 0/10 | |

После создания VLAN-сети можно вручную назначить ей порт, который сможет обмениваться данными только с другими устройствами в ней, используя пару команд switchport mode access и switchport access vlan №.

Далее описаны необходимые действия по конфигурированию портов коммутатора для включения в состав определенной VLAN-сети.

Выбираем порт или диапазон портов командами Switch(config)#int range fa0/1-3, Switch(config-if-range)#switchport mode access, Switch(config-if-range)#switchport access vlan 121, Switch(config-if-range)#end, Switch#.

Выполним дальнейшую конфигурацию для остальных портов. Командой CLI отобразим в отчете в виде Screen Shot’s.

12 С помощью команды Switch#show vlan brief из глобального режима посмотрим конфигурацию vlan (рисунок 5.7). Проанализируем результат и зафиксируем в отчете в виде Screen Shot’s и анализа.

13 С помощью команды ping проверим доступность компьютеров в одной и в разных Vlan, результат представим в виде Screen Shot's (рисунок 5.8).

14 В режиме симуляции воспроизведем продвижение широковещательного пакета в пределах одной из сетей и просмотрим «Информацию PDU на устройствах: коммутатор, компьютер» (рисунок 5.9). Результат с помощью Screen shot's сохраняем в отчете.

15 В результате создания vlan's и их конфигурации получены три изолированные локальные сети. Как правило, в таких сетях IP-адреса назначаются из разных подсетей. Часто придерживаются следующего правила: один из октедов

IP-адреса назначают равным или визуально похожим на IDVLAN. Выполним данную рекомендацию:

– в адресное пространство подсети «Бухгалтерия» установим второй октед IP-адреса равным IDVLAN =NN*10+1. Таким образом, IP-адреса для VLAN «buh» будут иметь значения (10. VLAN_1.12.XX) 10.121.12.XX;

– адресное пространство подсети «Отдел продаж (Sales)» будет равным (10. VLAN_2.12.XX) 10.122.12.XX;

–в адресном пространстве подсети «Отдел маркетинга (Market)» также поменяем второй октед (10. VLAN_3.12.XX) 10.123.12.XX.

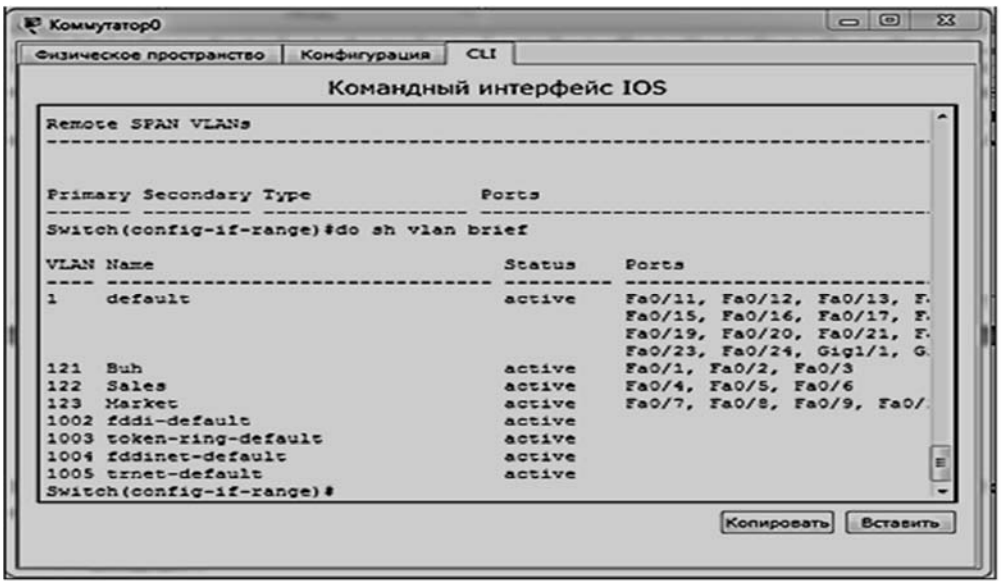


Рисунок 5.7 – Состояние VLAN's после «привязки» портов

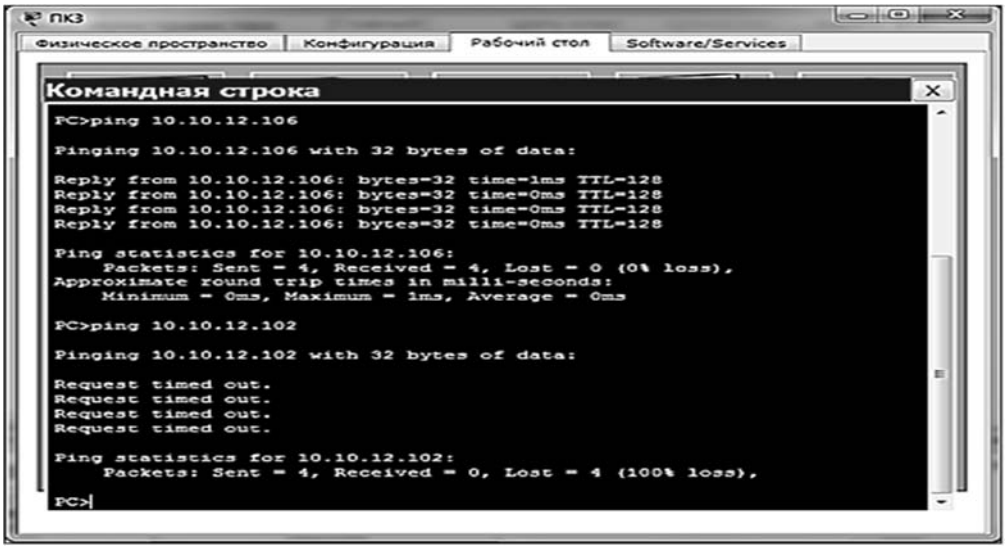


Рисунок 5.8 – Проверка доступности компьютеров

При необходимости соединить три независимые VLAN's в одну сеть можно, используя сетевое устройство третьего уровня: более мощный коммутатор с функциями третьего уровня или маршрутизатор. В этом случае преиму-

щества сетей с VLAN сохраняются: уменьшаются широковещательные домены до масштабов VLAN's, гибкое разделение хостов на функциональные группы независимо от местоположения, более высокое обеспечение безопасности и управляемости сети.

16 Сохраним файл для отчета LR_5_FIO.pkt.

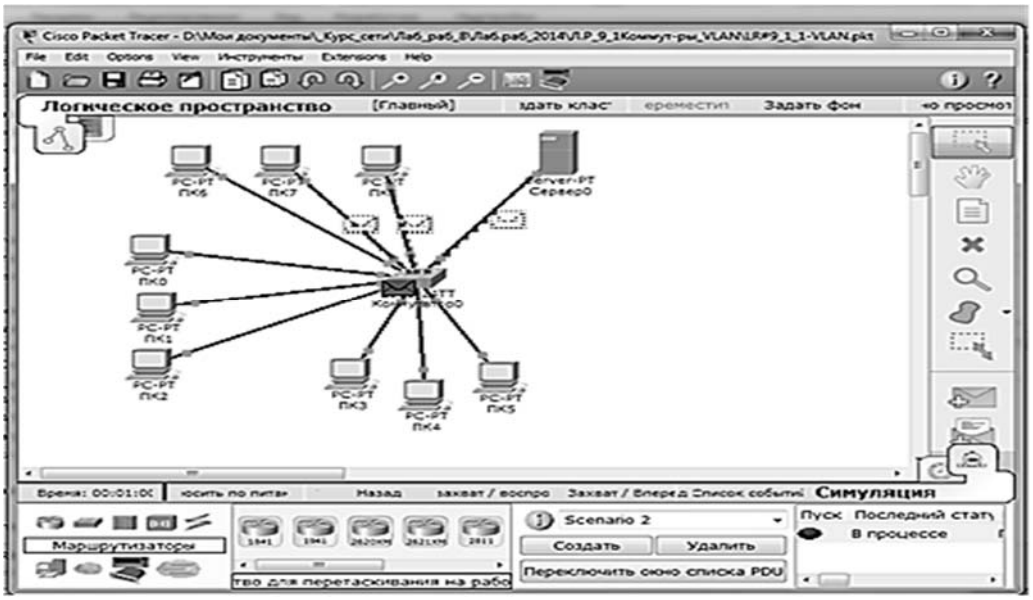


Рисунок 5.9 – Продвижение широковещательного трафика в пределах одной VLAN

***Контрольные вопросы***

1 Назовите и кратко объясните основные алгоритмы коммутаторов Ethernet.

2 Что такое «широковещательный шторм» и в каких ситуациях он возникает?

3 Что представляет собой виртуальная локальная сеть VLAN?

4 Назначение, функции и преимущества сетей VLAN.

5 Расскажите подробно создание виртуальных сетей на базе одного коммутатора.

6 Покажите на примере конфигурацию VLAN на базе портов одного коммутатора.

# 6 Лабораторная работа № 6. Изучение правил адресации сетевого уровня

**Цель работы**: изучить правила адресации сетевого уровня; научиться распределять адреса между участниками сети передачи данных.

***Методические указания***

В технологии TCP/IP сетевой адрес называют IP-адрес.

Адреса получателя и отправителя должны содержать в себе:

– номер (адрес) подсети;

– номер (адрес) участника (хоста) внутри подсети.

IP-адреса представляют собой 32-разрядные двоичные числа. Для удобства их записывают в виде четырех десятичных чисел, разделенных точками. Каждое число является десятичным эквивалентом соответствующего байта адреса 192.168.200.47 и десятичным эквивалентом двоичного адреса 11000000.10101000.11001000.00101111 (точки оставлены для удобства).

IP-адрес содержит информацию адреса подсети и адреса узла в ней.

Запись адреса не предусматривает специального разграничительного знака между номером сети и номером узла, но необходимость в этом, несомненно, есть. Для решения данной проблемы используются несколько вариантов.

Первоначально использовался простой способ: адрес фиксировано, жестко разбивался на две части (RFC 760). Очевидно, что такой жесткий подход не позволяет дифференцированно удовлетворять потребности отдельных предприятий и организаций. Он не нашел широкого применения.

Второй подход, распространенный до недавнего времени, заключается в использовании классов адресов (RFC 791). Вводится пять классов адресов: A, B, C, D, E. Три из них – A, B и C – используются для адресации сетей, а два – D и E – имеют специальное назначение. Для каждого класса сетевых адресов определено собственное положение границы между номером сети и номером узла.

И, наконец, третий способ (RFC 950, RFC 1518) основан на использовании маски, которая позволяет максимально гибко устанавливать границу между номером сети и номером узла. При таком подходе адресное пространство можно использовать для создания множества сетей разного размера. Для этих целей, наряду с IP-адресом, введено такое понятие, как маска.

Практический интерес представляют два последних способа построения адреса IP.

Существуют ограничения при назначении IP-адресов интерфейсам сети. Следующие адреса не назначаются сетевым интерфейсам (но используются для других целей).

1 Содержащие 0 во всех двоичных разрядах поля номера узла; такие IP-адреса используются для записи адресов сетей в целом.

2 Содержащие 1 во всех двоичных разрядах поля номера узла; такие IP-адреса являются широковещательными адресами для сетей, номера которых определяются этими адресами, а именно номера сетей и номера узлов не могут состоять из одних двоичных нулей или единиц. Отсюда следует, что максимальное количество узлов для сетей каждого класса должно быть уменьшено на 2. Например, в адресах класса C под номер узла отводится 8 бит, которые позволяют задавать 256 номеров: от 0 до 255. Однако в действительности максимальное число узлов в сети класса C не может превышать 254, т. к. адреса 0 и 255 запрещены для адресации сетевых интерфейсов.

3 Все поля IP-адреса состоят из двоичных нулей (0.0.0.0). Такой адрес называется неопределенным адресом и обозначает адрес того узла, который

сгенерировал этот пакет. Адрес такого вида в особых случаях помещается в заголовок IP-пакета в поле адреса отправителя.

4 Содержащие в поле номера сети только нули (0.0.X.X). Такой адрес обозначает адрес назначения узла сети, в которой находится узел, отправивший данный пакет. Такой адрес также может быть использован только в качестве адреса отправителя.

5 Все поля IP-адреса состоят из двоичных 1 (255.255.255.255). Пакет с таким адресом назначения должен рассылаться всем узлам, находящимся в той же сети, что и источник этого пакета. Такой адрес называется ограниченным широковещательным (limited broadcast). Ограниченность в данном случае означает, что пакет не выйдет за границы данной сети ни при каких условиях (маршрутизаторы этого не допустят).

6 Поле адреса назначения в разрядах, соответствующих номеру узла, стоят только единицы, то пакет, имеющий такой адрес, рассылается всем узлам сети, номер которой указан в адресе назначения. Например, пакет с адресом 192.190.21.255 будет направлен всем узлам сети 192.190.21.0. Такой тип адреса называется широковещательным (broadcast).

Схема разделения IP-адреса на номер сети и номер узла, основанная на понятии класса адреса, не является эффективной. Для более гибкого определения границ между разрядами номеров сети и узла внутри IP-адреса используются так называемые маски подсети. Маска подсети – это 4-байтовое число специального вида, которое используется совместно с IP-адресом. Специальный вид маски подсети заключается в следующем: двоичные разряды маски, соответствующие разрядам IP-адреса, отведенным под номер сети, содержат единицы, а в разрядах, соответствующих разрядам номера узла, – нули. Количество разрядов адреса подсети может быть различным и определяется маской сети.

Все единичные разряды маски (если они есть) находятся в старшей (левой) части маски, а нулевые (если они есть) – в правой (младшей). Для определения адреса сети на 32-разрядный двоичный IP-адрес накладывается 32-разрядная двоичная маска и выполняется побитно логическая операция & (И).

В компьютере каждая маска адреса хранится в виде 32-битового значения. Однако для записи префикса и маски адреса неудобно пользоваться двоичным представлением. Вместо этого применяется формат в виде десятичных чисел, разделенных точками, или новая синтаксическая форма, которая была разработана для адресации CIDR (технология бесклассовой междоменной маршрутизации – Classless Inter-Domain Routing, CIDR). Эта новая форма определяет, что маска, связанная с адресом, добавляется через косую черту; размер маски указывается в виде десятичного числа. Например, в первоначальной схеме на основе классов адрес 128.10.0.17 состоит из 16-битового префикса сети и 16-битового суффикса хоста. Маска сети в этом случае 255.255.0.0. С использованием адресации CIDR IP-адрес в месте с маской запишется более компактно: 128.10.0.17/16.

Исходя из вышесказанного, маску часто записывают в виде числа единиц, в ней содержащихся. 255.255.248.0 (11111111.11111111.11111000.00000000) –

является правильной маской подсети (/21), а 255.255.250.0 (11111111.11111111.11111010.00000000) – неправильной, недопустимой. Нетрудно увидеть, что максимальный размер подсети может быть только степенью двойки (двойку надо возвести в степень, равную количеству нулей в маске).

Определение диапазона адресов подсети можно произвести из определения понятия маски:

– разряды, которые относятся к адресу подсети, у всех хостов подсети должны быть одинаковы;

– адреса хостов в подсети могут быть любыми.

То есть если наш адрес 192.168.200.47 и маска равна /20, то диапазон можно посчитать:

– адрес 11000000.10101000.11001000.00101111;

– маска 11111111.11111111.11110000.00000000;

– диапазон адресов 11000000.10101000.1100XXXX.XXXXXXXX.

Здесь 0,1 – определенные значения разрядов, а X – любое значение, что приводит к диапазону адресов от 11000000.10101000.11000000.00000000 (192.168.192.0) до 11000000.10101000.11001111.11111111 (192.168.207.255).

Следует учитывать, что некоторые адреса являются запрещенными или служебными и их нельзя использовать для адресов хостов или подсетей. Это адреса, содержащие 0 в первом или последнем байте, 255 в любом байте (это широковещательные адреса), 127 в первом байте (внутренняя петля – этот адрес имеется в каждом хосте и служит для связывания компонентов сетевого уровня).

### *Порядок выполнения работы*

1 По данным IP-адресам (таблица 6.2) определить, к сети какого класса они принадлежат, получить IP-адрес сети, маску сети и IP-адрес широковещательной рассылки в данной сети.

Таблица 6.2 – Варианты задания

| Вариант | Задание 1 | Задание 2 | Задание 3 | Задание 4 |
|---|---|---|---|---|
| 1 | 36.24.212.27 | 151.204.234.208 | 167.143.166.151 | 81.207.5.124 |
| 2 | 187.196.89.86 | 37.38.56.94 | 194.3.50.241 | 35.42.64.114 |
| 3 | 42.160.157.215 | 75.59.233.215 | 163.143.246.230 | 218.161.0.172 |
| 4 | 45.45.183.158 | 10.128.217.44 | 56.86.29.157 | 186.113.68.173 |
| 5 | 65.72.172.57 | 191.194.186.67 | 117.39.255.239 | 203.80.81.87 |
| 6 | 98.152.43.182 | 19.160.138.248 | 78.123.49.191 | 205.44.61.253 |
| 7 | 182.76.142.213 | 80.117.227.93 | 137.225.232.195 | 160.22.40.236 |
| 8 | 168.173.44.192 | 37.73.200.123 | 213.180.159.172 | 20.55.186.108 |
| 9 | 56.99.61.195 | 49.229.236.82 | 55.23.59.226 | 4.6.214.143 |
| 10 | 110.157.233.184 | 159.57.141.205 | 195.137.48.42 | 190.30.134.79 |

Окончание таблицы 6.2

| Вариант | Задание 1 | Задание 2 | Задание 3 | Задание 4 |
|---|---|---|---|---|
| 11 | 209.91.67.50 | 158.133.84.236 | 168.168.105.250 | 37.108.141.213 |
| 12 | 7.138.74.144 | 59.27.242.99 | 132.219.211.86 | 54.157.52.232 |
| 13 | 136.203.39.139 | 3.155.81.90 | 213.255.238.108 | 105.243.46.212 |
| 14 | 103.250.75.224 | 83.252.152.35 | 208.90.192.85 | 18.245.178.92 |
| 15 | 167.212.40.42 | 116.199.97.6 | 144.104.247.170 | 1.160.40.122 |

2 Используя IP-адреса из задания 1 и нижеуказанную длину маски сети (таблица 6.3), необходимо получить IP-адрес сети, маску сети и IP-адрес широковещательной рассылки в данной сети.

Таблица 6.3 – Варианты задания

| Вариант | Задание 1 | Задание 2 | Задание 3 | Задание 4 |
|---|---|---|---|---|
| 1 | /30 | /18 | /20 | /28 |
| 2 | /6 | /21 | /26 | /10 |
| 3 | /12 | /7 | /17 | /15 |
| 4 | /24 | /3 | /23 | /8 |
| 5 | /26 | /13 | /20 | /27 |
| 6 | /4 | /10 | /25 | /28 |
| 7 | /28 | /24 | /18 | /3 |
| 8 | /10 | /14 | /20 | /9 |
| 9 | /11 | /4 | /23 | /14 |
| 10 | /17 | /25 | /26 | /20 |
| 11 | /10 | /27 | /29 | /11 |
| 12 | /27 | /14 | /21 | /15 |
| 13 | /15 | /29 | /14 | /19 |
| 14 | /17 | /10 | /21 | /13 |
| 15 | /13 | /30 | /27 | /7 |

3 Определить, является ли данная маска сети (таблица 6.4) правильной и какова ее длина в битах.

4 Определить, является ли данный IP-адрес (таблица 6.5) адресом сети с указанной длиной маски сети (необходимо вычислить по данному IP-адресу адрес сети и сравнить с исходным адресом, указанным в задании).

5 Определить, принадлежат ли указанные IP-адреса (таблица 6.6) к одной подсети (чтобы узнать, принадлежат ли адреса к одной подсети, необходимо получить адрес сети для каждого из адресов и сравнить адреса сетей).

Таблица 6.4 – Варианты задания

| Вариант | Задание 1 | Задание 2 | Задание 3 | Задание 4 |
|---|---|---|---|---|
| 1 | 255.254.0.0 | 255.255.255.214 | 255.255.255.248 | 255.255.248.0 |
| 2 | 255.255.255.0 | 255.255.255.240 | 255.253.0.0 | 255.255.252.0 |
| 3 | 255.255.252.0 | 255.255.255.192 | 255.7.0.0 | 248.0.0.0 |
| 4 | 255.254.0.0 | 255.255.248.0 | 240.0.3.0 | 255.255.255.248 |
| 5 | 248.0.0.0 | 255.249.0.0 | 255.255.255.240 | 224.0.0.0 |
| 6 | 255.255.0.0 | 252.253.0.0 | 255.124.0.0 | 65.255.0.0 |
| 7 | 255.248.0.0 | 255.255.240.0 | 255.255.254.0 | 255.255.255.254 |
| 8 | 255.224.0.0 | 252.2.0.0 | 255.240.0.0 | 255.255.255.240 |
| 9 | 255.255.255.248 | 255.255.255.252 | 255.255.248.0 | 192.0.0.0 |
| 10 | 255.248.9.0 | 255.255.255.0 | 255.248.0.0 | 254.0.0.0 |
| 11 | 255.255.225.255 | 255.255.193.0 | 255.255.0.0 | 255.255.255.128 |
| 12 | 255.255.255.252 | 255.255.255.128 | 255.255.255.248 | 255.192.0.0 |
| 13 | 255.224.0.0 | 250.0.0.0 | 255.255.254.0 | 192.0.0.0 |
| 14 | 255.240.0.0 | 255.255.192.0 | 255.255.255.252 | 255.240.0.0 |
| 15 | 255.255.255.128 | 255.240.0.0 | 224.0.0.0 | 255.224.224.0 |

Таблица 6.5 – Варианты задания

| Вариант | Задание 1 | Задание 2 | Задание 3 | Задание 4 |
|---|---|---|---|---|
| 1 | 185.129.0.0/9 | 80.0.0.0/5 | 100.241.96.0/22 | 129.199.93.82/31 |
| 2 | 185.214.114.0/22 | 85.0.0.0/7 | 157.143.151.177/29 | 58.189.128.0/17 |
| 3 | 128.0.0.0/2 | 1.193.76.0/24 | 127.12.0.0/14 | 134.0.0.0/6 |
| 4 | 120.118.0.0/12 | 195.165.102.0/18 | 184.98.36.0/24 | 200.0.0.0/5 |
| 5 | 32.0.0.0/3 | 15.53.210.202/30 | 240.97.66.0/18 | 189.66.194.64/26 |
| 6 | 152.228.0.0/14 | 229.0.0.0/3 | 126.17.238.0/23 | 66.37.0.0/16 |
| 7 | 146.0.0.0/11 | 88.142.0.0/14 | 107.212.0.0/14 | 202.58.239.204/31 |
| 8 | 65.0.0.0/7 | 73.100.0.0/17 | 105.213.190.0/23 | 169.22.0.0/15 |
| 9 | 80.243.8.200/31 | 7.81.247.0/21 | 40.127.40.54/31 | 222.117.148.0/22 |
| 10 | 32.10.0.0/9 | 95.81.1-8.0/18 | 68.111.8.0/22 | 52.96.0.0/11 |
| 11 | 43.51.83.162/27 | 21.96.100.0/11 | 105.49.54.226/31 | 164.0.0.0/7 |
| 12 | 122.0.0.0/5 | 67.109.141.105/30 | 161.249.88.0/25 | 104.184.0.0/13 |
| 13 | 33.245.254.0/22 | 152.0.0.0/6 | 46.126.200.209/30 | 155.80.0.0/18 |
| 14 | 147.0.0.0/8 | 138.182.0.0/14 | 7.117.120.60/32 | 112.0.0.0/6 |
| 15 | 127.160.0.0/11 | 27.100.136.87/29 | 17.91.200.10/21 | 166.51.64.0/19 |

Таблица 6.6 – Варианты задания

| Вариант | Задание 1 | Задание 2 |
|---|---|---|
| 1 | 229.52.17.190 – 229.50.17.191/30 | 226.144.183.64 – 226.128.186.152/9 |
| 2 | 223.62.19.244 – 223.67.176.98/14 | 67.50.242.243 – 67.50.200.172/18 |
| 3 | 127.73.18.240 – 137.114.177.17/9 | 195.94.59.188 – 195.94.59.191/30 |
| 4 | 185.63.56.182 – 85.63.239.16/16 | 199.57.36.63 – 199.57.5.169/15 |
| 5 | 136.61.83.119 -– 111.181.218.52/5 | 125.60.255.103 – 125.34.169.199/9 |
| 6 | 133.206.62.249 – 133.105.92.88/11 | 192.243.42.162 – 192.243.42.246/25 |
| 7 | 94.176.91.111 – 94.176.92.80/20 | 4.244.159.102 – 4.246.125.165/12 |
| 8 | 47.88.172.145 – 47.88.178.192/21 | 203.40.171.158 – 203.40.141.180/18 |
| 9 | 244.23.38.153 – 244.23.78.154/29 | 28.3.34.25 – 19.109.158.253/4 |
| 10 | 123.65.168.74 – 123.65.164.72/27 | 110.71.140.119 – 110.67.85.239/9 |
| 11 | 116.75.124.87 – 116.75.124.85/20 | 135.143.91.179 – 135.143.87.229/20 |
| 12 | 253.130.198.145 – 253.130.198.145/22 | 37.125.13.168 – 37.125.15.13/21 |
| 13 | 108.11.214.167 – 108.11.223.5/19 | 246.235.45.207 – 246.235.45.215/29 |
| 14 | 74.28.237.200 -– 74.28.237.203/25 | 181.84.249.67 – 181.65.130.204/9 |
| 15 | 199.123.3.50 – 199.123.3.101/23 | 100.101.216.145 – 100.182.234.25/5 |

***Контрольные вопросы***

1 Что такое маска подсети?
2 Какова структура IP-адреса?
3 Чем определяется размер подсети?
4 Как определить диапазон адресов в подсети?
5 Как определить размер подсети?

# 7 Лабораторная работа № 7. Изучение принципов статической маршрутизации IP-сетей

**Цель работы**: изучить принципы маршрутизации IP сетей на примере протоколов статической маршрутизации с использованием программного обеспечения построения виртуальных сетей Packet Tracer 6.0; получить практические навыки по настройке маршрутизаторов Cisco 2811-28xx.

***Методические указания***

Протокол маршрутизации – это сетевой протокол, используемый маршрутизаторами для определения возможных маршрутов следования данных в составной компьютерной сети.

Статическая маршрутизация – вид маршрутизации, при котором информация о маршрутах заносится в таблицы маршрутизации каждого маршру-

тизатора вручную администратором сети. Статические маршруты не изменяются до тех пор, пока администратор не перенастроит их вручную. В таблице маршрутизации эти маршруты обозначаются буквой S. Символом C в таблице маршрутизации помечены непосредственно присоединенные к маршрутизатору сети. Маршрутизатор задействует административное расстояние каждого маршрута, чтобы определить лучший путь к адресату. Меньшее административное расстояние означает более надежный источник.

### *Порядок выполнения работы*

1 Базовая настройка маршрутизации и устройств сети. В области «Логическое пространство» создаем иерархическое дерево сети, аналогичное дереву на рисунке 7.1.

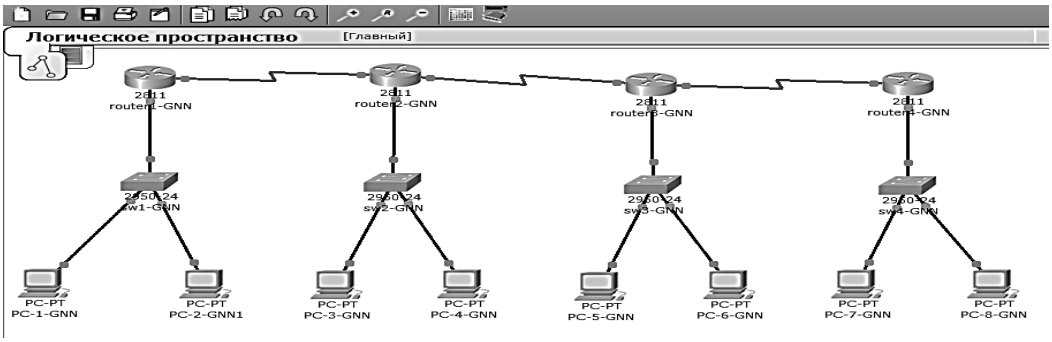


Рисунок 7.1 – Конфигурация сети

2 При обозначении коммутаторов, маршрутизаторов, компьютеров выполняем следующее правило: например, коммутатор SW-1 обозначается как SW-1-GNN, G – номер группы, NN – порядковый номер в журнале группы (ведущий ноль в данном случае пишется), например, G – 2, порядковый № 13, запишется как SW-1-213; router1 обозначится как R1-GNN.

3 Конструкция выбранного маршрутизатора (2811) предусматривает наличие двух интерфейсов Fast Ethernet, для увеличения количества интерфейсов надо установить плату расширения. Выбираем из списка сетевой модуль Cisco NM-4A/S на четыре асинхронных/синхронных последовательных порта.

Модуль Cisco NM-4A/S позволяет иметь четыре низкоскоростных последовательных соединений через DB-60 коннекторы, поддерживающие пять типов интерфейсов (RS-232, RS-449, RS-530, V.35, X.21) и в режиме DTE, и в DCE. Такие соединения могут быть сконфигурированы вплоть до 115.2 kbps на асинхронный трафик или 128 kbps на синхронный.

Для этого нужно выключить маршрутизатор, выбрать плату и установить ее в свободный разъем. После установки необходимо включить маршрутизатор. На рисунках 7.2 и 7.3 показан пример добавления платы NM-4A-S в router1-GNN.

Из имеющегося списка можно выбрать более скоростную плату (модуль), например NM-1FE-FX. Данный модуль предоставляет один интерфейс

Fast-Ethernet для подключения оптического кабеля. В этом случае можно достичь скорости 100 М/с, но придется использовать оптический кабель. Cisco 2811 поддерживает множество других модулей. Так, например, WIC-2A/S поддерживает два последовательных соединения T1/E1, асинхронный и синхронный трафик. Подключается напрямую к слоту WIC.

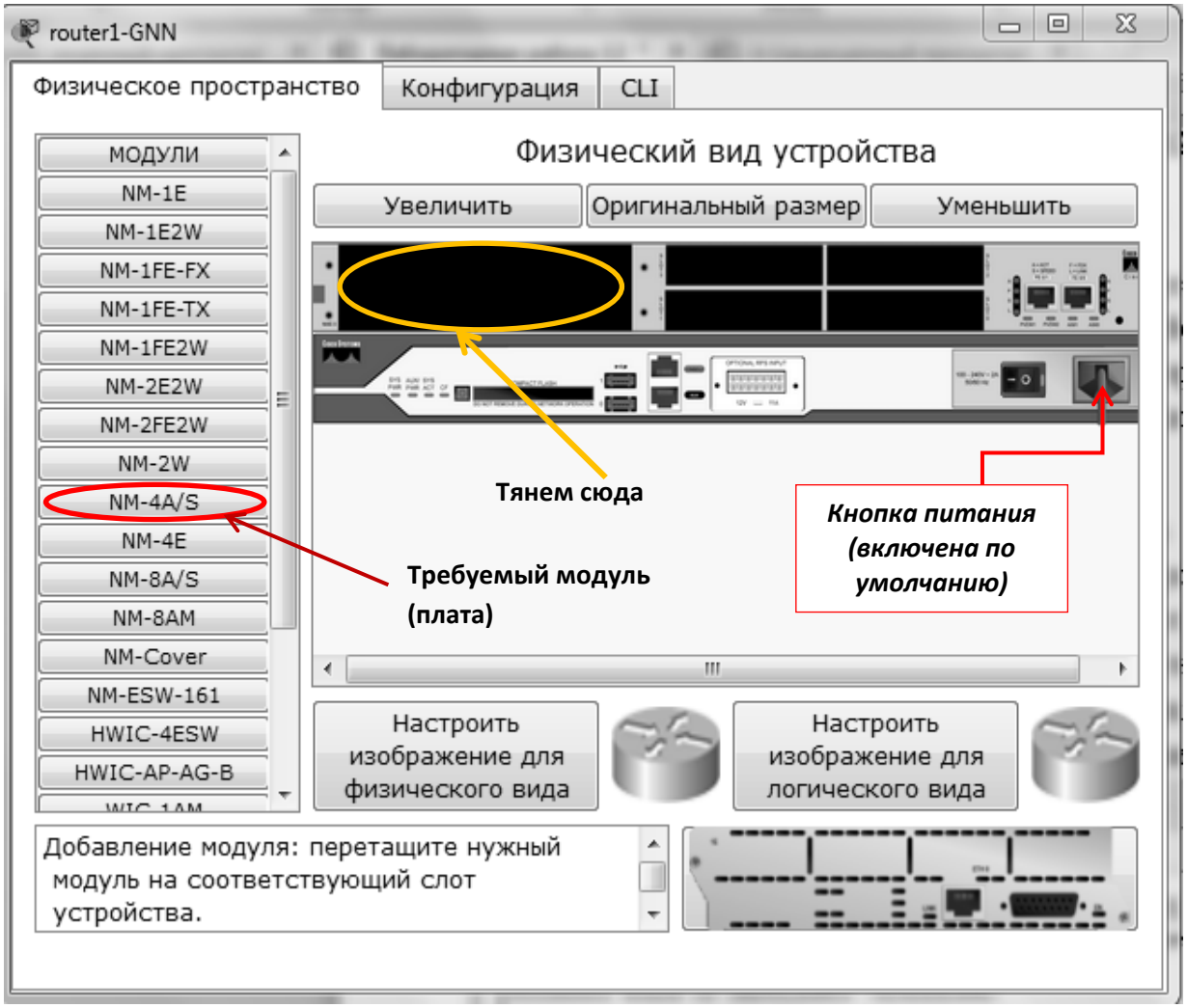


Рисунок 7.2 – Добавление модуля NM-4A/S

Аналогичные действия повторяем для остальных маршрутизаторов (рисунок 7.4).

4 Конфигурирование интерфейсов маршрутизаторов. Настройку IP-адресов интерфейсов проводим в соответствии с таблицей 7.1.

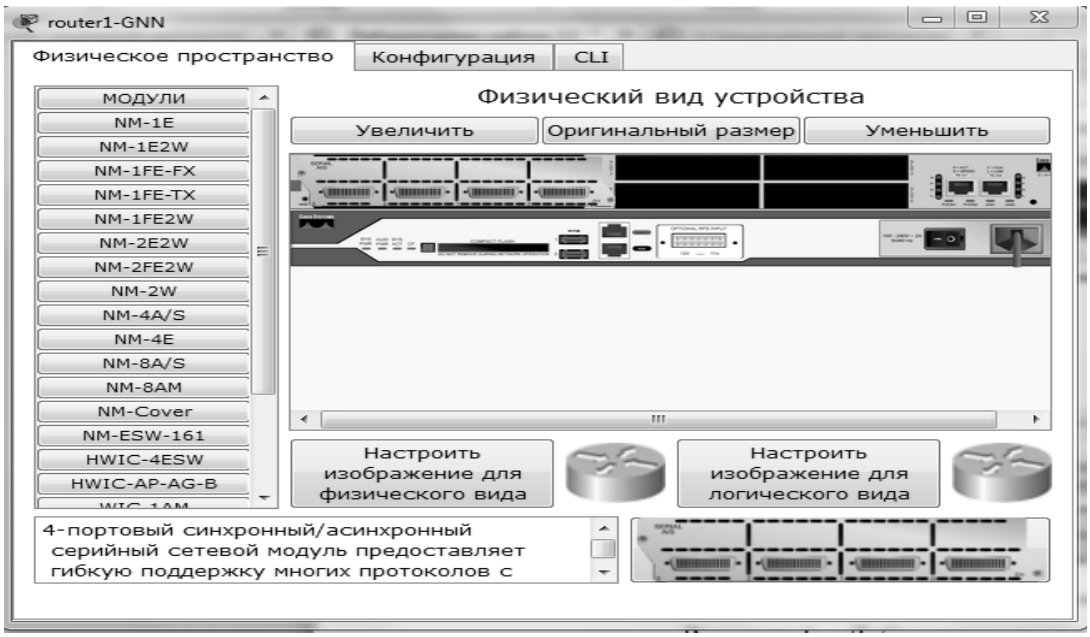


Рисунок 7.3 – Установленная плата NM-4A/S

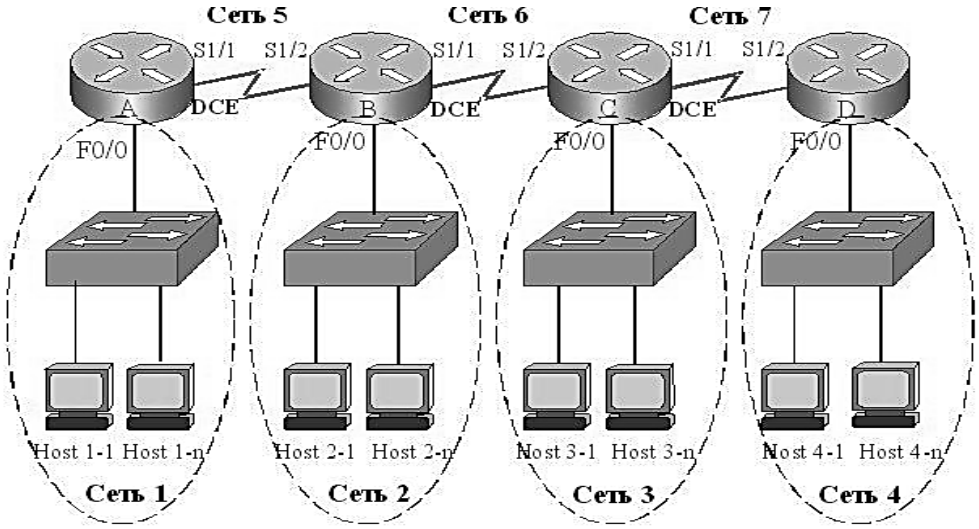


Рисунок 7.4 – Упрощенная схема сети с указанием портов и разбиением на подсети

Таблица 7.1 – Адреса сетей и интерфейсов маршрутизаторов

| Номер сети | IP-адрес сети | Интерфейс | IP-адрес интерфейса |
|---|---|---|---|
| Сеть 1 | 192.100 + G.NN.0/24 | F0/0 R1-GNN | 192.100 + G.NN.1 |
| Сеть 2 | 192.100 + G.10 + NN.0/24 | F0/0 R2-GNN | 192.100 + G.10 + NN.1 |
| Сеть 3 | 192.100 + G.20 + NN.0/24 | F0/0 R3-GNN | 192.100 + G.20 + NN.1 |
| Сеть 4 | 192.100 + G.30 + NN.0/24 | F0/0 R4-GNN | 192.100 + G.30 + NN.1 |
| Сеть 5 | 200.50.50.0/30 | S1/1 R1-GNN | 200.50.50.11 |
| | 200.50.50.0/30 | S1/2 R2-GNN | 200.50.50.12 |
| Сеть 6 | 200.60.60.0/30 | S1/1 R2-GNN | 200.60.60.11 |
| | 200.60.60.0/30 | S1/2 R3-GNN | 200.60.60.12 |
| Сеть 7 | 200.70.70.0/30 | S1/1 R3-GNN | 200.70.70.11 |
| | 200.70.70.0/30 | S1/2 R4-GNN | 200.70.70.12 |

5 После начальной загрузки маршрутизатора операционная система предложит продолжить конфигурирование в диалоговом режиме (рисунок 7.5), от которого следует отказаться (Continue with configuration dialog? [yes/no]:no). Аналогичная запись появляется и при работе с реальными устройствами. В некоторых версиях операционных систем затем необходимо подтвердить завершение диалогового режима.

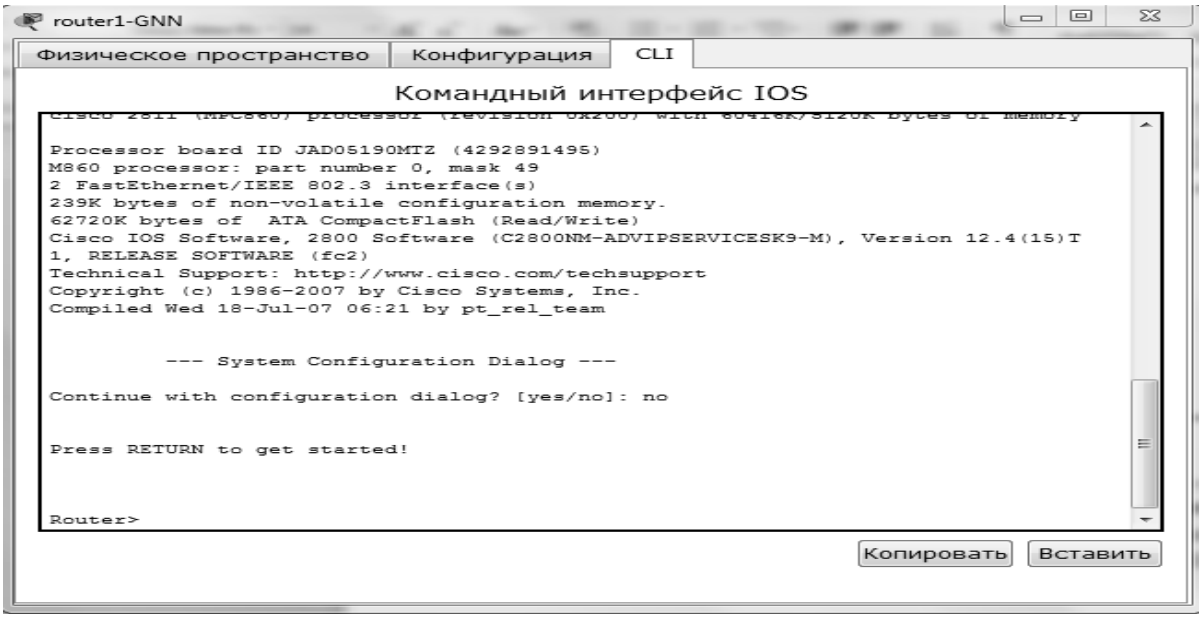


Рисунок 7.5 – Диалоговый режим конфигурирования

6 Для входа в привилегированный режим (рисунок 7.6) вводим команду enable,а затем для входа в глобальный режим – команду config terminal (conf term).

```
Router>enable
Router#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#
```

Рисунок 7.6 – Вход в привелигированный режим кофигурирования

7 Для того чтобы войти в режим детального конфигурирования интерфейса, используем команду interface (либо сокращенный ее вариант int) в глобальном режиме конфигурации. Например, при конфигурировании интерфейса Fast Ethernet с номером 0, входящим в состав слота 0, используем команду

```
R1-213(cnfig-if)#int f0/0
R1-213(cnfig-if)#
```

8 Установка IP-адреса интерфейса 192.102.13.1 с маской 24 производится следующей командой: R1-213(cnfig-if)#ip address 192.102.13.1 255.255.255.0.

9 По умолчанию все интерфейсы выключены. Включение интерфейса производится по команде no shutdown, а выключение – командой shutdown (рисунок 7.7).

```
R1-213(config-if)#no shutdown

%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state t
o up
```

Рисунок 7.7 – Команда включения интерфейса

10 Конфигурацию интерфейса можно просмотреть по командам show interfaces и show running-config (сокращенно sh int и sh run). По команде sh int производится верификация всех интерфейсов маршрутизатора.

Верификация одного конкретного интерфейса производится по команде sh int с указанием проверяемого устройства. Далее приведена часть распечатки команды sh int f0/0, по которой проводится проверка конфигурации интерфейса Fast Ethernet 0/0: R1-213>sh int f0/0.

Результат выполнения данной команды представлен на рисунке 7.8.

```
R1-213(config-if)#int f0/0
R1-213(config-if)#exit
R1-213(config)#exit

%SYS-5-CONFIG_I: Configured from console by console
R1-213#show int f0/0
FastEthernet0/0 is up, line protocol is up (connected)
  Hardware is Lance, address is 0001.c7bb.7e01 (bia 0001.c7bb.7e01)
  Internet address is 192.102.13.1/24
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  ARP type: ARPA, ARP Timeout 04:00:00,
  Last input 00:00:08, output 00:00:05, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0 (size/max/drops); Total output drops: 0
  Queueing strategy: fifo
  Output queue :0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     0 input packets with dribble condition detected
     0 packets output, 0 bytes, 0 underruns
     0 output errors, 0 collisions, 1 interface resets
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
R1-213#
```

Рисунок 7.8 – Результат выполнения команды R1-213>sh int f0/0

Из распечатки следует, что:

– интерфейс включен (Fast Ethernet 0/0 is up) и протокол на нем тоже (line protocol is up);

– MAC-адрес интерфейса Fast Ethernet0/0 будет 0001.c7bb.7e01;

– IP-адрес – 192.102.13.1/24, где число 24 означает маску 255.255.255.0;

– максимальный размер кадра MT – 1500 байт;

– ширина полосы – 100 Мбит/с (BW 100000 Kbit);

– задержка – 100 мкс (DLY 100 usec);

– надежность – максимальная (reliability 255/255);

– передача и прием – txtload 1/255 и rxload 1/255.

11 При конфигурировании последовательного интерфейса, имеющего DCE-подключение, например интерфейса s1/1 маршрутизатора R1-GNN, задается не только IP-адрес, но и скорость передачи данных в битах в секунду с помощью команды clock rate (рисунок 7.9).

```
R1-213#conf term
Enter configuration commands, one per line.  End with CNTL/Z.
R1-213(config)#int s1/1
R1-213(config-if)#ip address 200.50.50.11 255.255.255.248
R1-213(config-if)#clock rate 128000
R1-213(config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial1/1, changed state to down
R1-213(config-if)#
```

Рисунок 7.9 – Исполнение команды clock rate

Команда clock rate определяет, что интерфейс s1/1 маршрутизатора R1_GNN является ведущим (DCE) в соединении «точка – точка» с интерфейсом s1/2 маршрутизатора R2_GNN. Конфигурация остальных маршрутизаторов аналогична.

12 Просматриваем конфигурацию сконфигурированных интерфейсов f0/0, s1/1, s1/2 и других с помощью команды show running-config.

13 Повторяем пп. 1–13 для остальных маршрутизаторов, установив для них IP-адреса в соответствии с таблицей 7.1 Для маршрутизаторов R2-GNN, R3-GNN конфигурируются два последовательных интерфейса: s1/2 и s1/2, для маршрутизатора R1 – интерфейс s1/1, для R4 – s1/2, т. к. они пограничные (см. рисунок 7.4). Каждый шаг по пп. 1–13 сохраняем в отчете с помошью ScreenShot's.

14 Устанавливаем IP-адрес для всех конечных устройств (Host). При работе с пакетом Packet Tracer задание параметров узла производится следующим образом:

– «кликнуть» конфигурируемый узел, например, первый узел Сети 1;

– во всплывшем окне выбрать опцию Desktop, затем – IP Configuration и в новом окне установить IP-адрес узла, маску подсети и адрес шлюза в соответствии с таблицей 7.2.

Таблица 7.2 – Адреса составной сети

| Сеть | Адрес сети | Шлюз по умолчанию | IP-адрес узла 1 | IP-адрес узла 2 |
|---|---|---|---|---|
| Сеть 1 | 192.100 + + G.NN.0/24 | 192.100 +G.NN.1 | 192.100 + G.NN.2 | 192.100 + G.NN.3 |
| Сеть 2 | 192.100 + G.10 + + NN.0/24 | 192.100 + G.10 + + NN.1 | 192.100 + G.10 + + NN.2 | 192.100 + G.10 + + NN.3 |
| Сеть 3 | 192.100 + G.20 + + NN.0/24 | 192.100 + G.20 + + NN.1 | 192.100 + G.20 + + NN.2 | 192.100 + G.20 + +NN.3 |
| Сеть 4 | 192.100 + G.30 + + NN.0/24 | 192.100 + G.30 + + NN.1 | 192.100 + G.30 + + NN.2 | 192.100 + G.30 + +NN.3 |

15 Конфигурирование статической маршрутизации проводим самостоятельно. При защите работы имеем полностью оформленный отчет и рабочий файл PacketTracer с именем LR#7-GNN.pkt.

***Контрольные вопросы***

1 В чем заключается задача маршрутизации?

2 Какие технологии используются маршрутизатором на физическом и канальном уровне? Дайте краткую характеристику вышеперечисленным технологиям.

3 Перечислите основные компоненты маршрута.

4 С помощью каких команд можно сконфигурировать маршрут по умолчанию?

5 Что такое административное расстояние? Перечислите его значения для нескольких видов маршрутизации.

6 Что такое петля маршрутизации? Как с ней бороться?

7 Что такое статическая маршрутизация? Что в ней обозначается буквами C и S?

8 Назовите шесть признаков, относящихся к недостаткам статической маршрутизации.

9 Назовите три положительных признака, относящихся к статической маршрутизации.

# 8 Лабораторная работа № 8. Изучение принципов динамической маршрутизации IP-сетей

**Цель работы**: изучить принципы динамической маршрутизации IP-сетей на примере протоколов динамической маршрутизации RIP и OSPF.

***Методические указания***

Динамическая маршрутизация (dynamic routing) или адаптивная маршрутизация, когда записи в таблице обновляются автоматически при помощи одного или нескольких протоколов маршрутизации – RIP, OSPF, IGRP, EIGRP, IS-IS, BGP и др. Кроме того, маршрутизатор строит таблицу оптимальных путей к сетям назначения на основе различных критериев: количества промежуточных узлов, пропускной способности каналов, задержки передачи данных. Критерии вычисления оптимальных маршрутов чаще всего зависят от протокола маршрутизации, а также задаются конфигурацией маршрутизатора. Такой способ построения таблицы позволяет автоматически поддерживать таблицу маршрутизации в актуальном состоянии и вычислять оптимальные маршруты на основе текущей топологии сети. Однако динамическая маршрутизация оказывает дополнительную нагрузку на устройства, а высокая нестабильность сети может приводить к ситуациям, когда маршрутизаторы не успевают синхронизировать свои таблицы, что приводит к противоречивым сведениям о топологии сети в различных её частях и потере передаваемых данных. Зачастую для построения таблиц маршрутизации используют теорию графов.

***Порядок выполнения работы***

1 Изучить основные теоретические положения, сделав необходимые выписки в конспект.

2 Письмено ответить на контрольные вопросы.

3 Оформить отчет.

***Контрольные вопросы***

1 В чем заключается задача маршрутизации? Что такое протокол маршрутизации?

2 Специальные термины и понятия: метрика, Автономная система, Административное расстояние, Алгоритм выбора SPF, шлюз по умолчанию.

3 Протоколы маршрутизации. Классы, автономные системы AS. Какие протоколы применяются между AS и внутри AS? Дайте краткие характеристики.

4 Какие протоколы относятся к дистанционно-векторной маршрутизации?

5 Какие протоколы относятся к протоколам, использующим алгоритмы состояния связи?

6 Принцип дистанционно-векторного протокола поэтапно.

7 Основные ограничения протокола RIP. Какие методы применялись для устранения этих ограничений? Расскажите подробно о каждом.

8 Как образуются петли в сети с применением протокола RIP?

9 Таймеры RIP Cisco, функции и назначение, команды конфигурации.

10 Нежелательные анонсы RIP. Какой командой можно их устранить с привязкой к конкретному интерфейсу?

11 Какие версии RIP знаете? Совместимость версий RIP. С помощью какой команды можно инициализировать ту или иную версию и для чего она нужна?

12 Таблица маршрутизации протокола RIP. Поля таблицы, поэтапное построение таблицы маршрутизации.

13 Назовите три основных события обновления таблицы. Расскажите о каждом подробно.

14 Какой тип IP-адресации используется в RIP ver.1 и ver.2?

15 Какие дополнительные функции включает протокол RIPv2?

16 Где лучше применять протокол RIP?

17 На каком алгоритме основан протокол OSPF?

18 Что является метрикой OSPF и как она вычисляется?

19 Что такое LSA, для чего используются и как часто они появляются в сети?

20 На какие подразделы и области делится AS с OSPF?

21 Какие типы зон Вы знаете?

22 Как делятся по типам маршрутизаторы зон?

23 Какой идентификатор присваивается основной или единственной зоне?

24 На основе каких данных создают таблицы-протоколы Link-state?

25 Назовите пять типов пакетов для обмена маршрутной информацией между устройствами OSPF.

26 Какие типы сетей различают в протоколе OSPF?

27 Поэтапное описание работы протокола OSPF.

28 Протокол BGP, назначение, функции.

29 Какую информацию формирует и переносит протокол BGP?

30 Какой тип IP-адресов использует протокол BGP?

31 К какому уровню OSI относится BGP-протокол?

## Список литературы

1 **Гулай, А. В.** Построение интеллектуальных систем : учеб. пособие / А. В. Гулай, В. М. Зайцев. – Мн. : ИВЦ Минфина, 2022. – 368 с.

2 **Грохова, Т. А**. Информатика для инженера : учеб. пособие / Т. А. Грохова, Е. И. Гридина. – Мн. : РИВШ. 2022. – 156 с.

3 **Скитер, Н. Н**. Информационные технологии : учеб. пособие / Н. Н. Скитер, А. В. Костикова. – Волгоград : ВолгГТУ, 2019. – 96 с.

4 **Олифер, В. Г.** Компьютерные сети. Принципы, технологии, протоколы: учеб. пособие / В. Г. Олифер, Н. А. Олифер. – 6-е изд. – СПб. : Питер, 2016. – 992 с. : ил.