

Лабораторная работа № 1

Построение простой сети с использованием симулятора компьютерных сетей

2.1. Цель работы

Изучить принципы построения простейших сетей и их настройки с использованием симулятора компьютерных сетей.

Собрать в соответствии с заданием топологии сетей, запустить и настроить виртуальное оборудование.

Согласно пунктам выполнения лабораторной работы, сделать необходимые снимки экрана. Изучить полученную информацию и оформить ее в соответствии с требованиями раздела 5 (Содержание отчета).

2.2. Лабораторное задание

Организовать простейшие сети:

- компьютер-коммутатор-маршрутизатор-коммутатор-компьютер.

Запустить и настроить виртуальное оборудование.

Изучить полученную информацию и оформить ее в соответствии с требованиями раздела 2.5 (Содержание отчета).

2.3. Краткие теоретические сведения

Объединяя в сеть несколько (больше двух) компьютеров, необходимо решить, каким образом соединить их друг с другом, другими словами, выбрать конфигурацию физических связей, или топологию. Под топологией понимается граф, отдельным узлам которого соответствуют точки подключения активного сетевого терминального и группового оборудования, а ребрам – физические связи между этими узлами по кабельным линиям.

От выбора топологии связей существенно зависят характеристики сети. Например, наличие между узлами нескольких путей повышает надежность сети и делает возможным распределение загрузки между отдельными каналами. Экономические соображения часто приводят к выбору топологий, для которых характерна минимальная суммарная длина линий связи.

Среди множества возможных конфигураций различают полносвязные и неполносвязные.

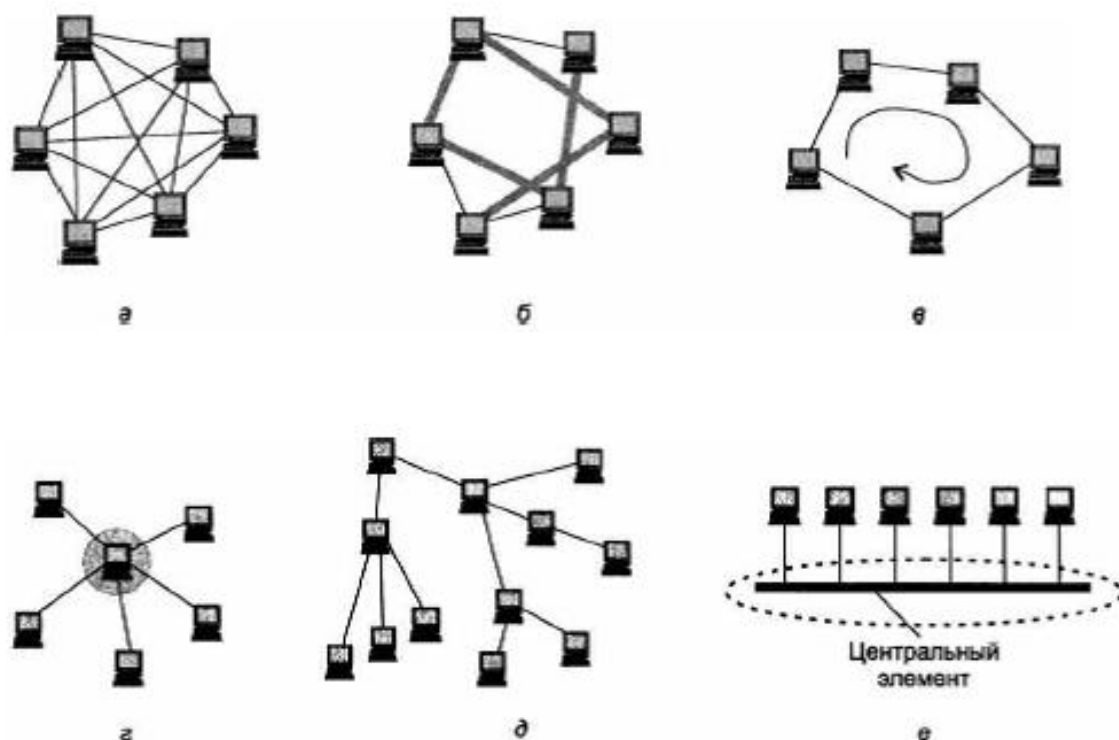


Рисунок 2.3.1 – Типовые топологии сетей

а) полносвязная; б) ячеистая; в) кольцевая; г) звездообразная;
д) иерархическая звезда (дерево); е) общая шина

Полносвязная топология (рис. 2.3.1, а) соответствует сети, в которой каждый компьютер непосредственно связан со всеми остальными. Несмотря на логическую простоту, этот вариант оказывается громоздким и неэффективным: каждый компьютер в сети должен иметь большое количество коммуникационных портов, достаточное для связи с каждым из остальных компьютеров сети. Для каждой пары компьютеров должна быть выделена отдельная физическая линия связи.

Все другие варианты основаны на **неполносвязных топологиях**, когда для обмена данными между двумя компьютерами может потребоваться транзитная передача данных через другие узлы сети.

Ячеистая топология (рис. 2.3.1, б) получается из полносвязной путем удаления некоторых связей. Она допускает соединение большого количества компьютеров и характерна, как правило, для крупных сетей.

В сетях с **кольцевой топологией** (рис. 2.3.1, в) данные передаются по кольцу от одного компьютера к другому. Главным достоинством кольца является то, что оно по своей природе обеспечивает резервирование связей: любая пара узлов соединена здесь двумя путями — по часовой стрелке и против нее. Кроме того, кольцо представляет собой очень удобную конфигурацию для организации обратной связи - данные, сделав полный оборот, возвращаются к узлу-источнику. Поэтому источник может контролировать процесс доставки данных адресату. Часто это свойство кольца используется для тестирования связности сети и поиска узла, работающего некорректно. В то же время в сетях с кольцевой топологией необходимо принимать специальные меры, чтобы в случае выхода из строя или

отключения какого-либо компьютера не прерывался канал связи между остальными узлами кольца.

Звездообразная топология (рис. 2.3.1, г) образуется в случае, когда каждый компьютер подключается непосредственно к общему центральному устройству, называемому **концентратором**. В функции концентратора входит направление передаваемой компьютером информации одному или всем остальным компьютерам сети. В качестве концентратора может выступать как универсальный компьютер, так и специализированное устройство. К недостаткам звездообразной топологии относится более высокая стоимость сетевого оборудования из-за необходимости приобретения специализированного центрального устройства. Кроме того, возможности по наращиванию количества узлов в сети ограничиваются количеством портов концентратора.

При создании сети с использованием нескольких концентраторов, иерархически соединенных между собой звездообразными связями, получаемую в результате структуру называют **иерархической звездой**, или **деревом** ((рис. 2.3.1, д). В настоящее время дерево является самой распространенной топологией связей как в локальных, так и глобальных сетях.

Особым частным случаем звезды является **общая шина** ((рис. 2.3.1, е). Здесь в качестве центрального элемента выступает пассивный кабель, к которому по схеме «монтажного ИЛИ» подключается несколько компьютеров (такую же топологию имеют многие сети, использующие беспроводную связь, - роль общей шины здесь играет общая радиосреда). Передаваемая информация распространяется по кабелю и доступна одновременно всем компьютерам, присоединенным к этому кабелю. Основными преимуществами такой схемы являются ее дешевизна и простота присоединения новых узлов к сети, а недостатками — низкая надежность (любой дефект кабеля полностью парализует всю сеть) и невысокая производительность (в каждый момент времени только один компьютер может передавать данные по сети, поэтому пропускная способность делится здесь между всеми узлами сети).

К техническим средствам, обеспечивающие функционирование высокоскоростных сетей передачи данных относятся концентраторы (или хабы), мосты, коммутаторы, маршрутизаторы.

Сетевой концентратор или **хаб** — сетевое устройство для объединения нескольких устройств Ethernet в общий сегмент. Все порты концентратора равноправны. Получив сигнал от одной из подключенных к нему станций, концентратор транслирует его на все свои активные порты. Устройства подключаются при помощи витой пары, коаксиального кабеля или оптоволокну. Термин концентратор используется вместо термина «повторитель», когда речь идет об устройстве, которое служит центром сети

Наиболее важные особенности концентраторов:

- усиливают сигналы;
- распространяют сигналы в сети;
- используются как точки концентрации в сети.

К дополнительным функциям концентратора относят: отключение некорректно работающего порта. и поддержку резервных связей.

Недостатком использования концентратора является то, что он не может фильтровать сетевой трафик (то есть принимать решение – пропускать трафик или игнорировать его) на основании определённых критериев, например, адресу источника, адресу получателя или протоколу и т.п.

Мосты предназначены для соединения сетевых сегментов, имеющих различные физические среды. Мосты также могут быть использованы для связи сегментов, имеющих различные протоколы низкого уровня (физического и канального). Возможно применение мостов для связи сегментов локально-вычислительных сетей (ЛВС), как с одинаковыми протоколами, так и для связи сегментов, осуществляющих соединение с различными протоколами. Задачи мостов:

- передача пакетов из одной сети в другую и наоборот. В процессе передачи мост регенерирует пакет, что позволяет передавать данные вдоль сети на значительное расстояние;
- просмотр каждого пакета и принятие решения, какой из двух сетей принадлежит тот или иной пакет;
- отслеживание адреса приемника и передатчика информации в процессе передачи какого-либо пакета;
- определение, какой сети принадлежит тот или иной пакет благодаря просмотру информации уровня управления доступом к среде передачи.

Коммутатор — это устройство, конструктивно выполненное в виде сетевого концентратора и действующего как высокоскоростной много портовый мост. Коммутаторы обеспечивают широковещательное сегментирование локальных сетей и выделение полосы пропускания к рабочим станциям. Коммутаторы устраняют физические ограничения, возникающие вследствие совместного использования концентратора, поскольку они логически группируют пользователей и порты всего предприятия. Коммутаторы могут быть использованы для создания виртуальных сетей, осуществляющих сегментацию. В традиционных конфигурациях локальных сетей сегментация осуществляется **маршрутизаторами**. Коммутаторы являются основными компонентами, обеспечивающими обмен данными в виртуальных сетях, в которых они выполняют жизненно важные функции, являясь для устройств конечной станции точкой входа в среду коммутации, а также обеспечивают обмен данными в рамках всего предприятия. Каждый коммутатор обладает способностью принимать решения о фильтрации и отправке фреймов (frame) на основе метрики виртуальной сети, определяемой сетевыми администраторами, а также способностью передавать эту информацию другим коммутаторам и маршрутизатором сети.

Коммутаторы ЛВС поддерживают два режима работы:

- полудуплексный режим — это режим, при котором только одно устройство может передавать данные в любой момент времени в одном домене коллизии;
- дуплексный режим — это режим работы, который обеспечивает одновременную двустороннюю передачу данных между станцией отправителем и станцией получателем на MAC-уровне.

Существует разделение коммутаторов по уровням.

К коммутаторам 2 уровня (Layer 2) относят все устройства, которые работают на 2 уровне сетевой модели OSI — канальном уровне. К таким устройствам можно отнести все неуправляемые коммутаторы и часть управляемых. Коммутаторы 2 уровня работают с данными не как с непрерывным потоком информации (коммутаторы 1 уровня), а как с отдельными порциями информации — кадрами. Они умеют анализировать получаемые кадры и работать с MAC-адресами устройств отправителей и получателей кадра. Такие коммутаторы «не понимают» IP-адреса компьютеров, для них все устройства имеют названия в виде MAC-адресов. Коммутаторы 2 уровня составляют коммутационные

таблицы, в которых соотносят MAC-адреса встречающихся сетевых устройств с конкретными портами коммутатора.

К коммутаторам 3 уровня (Layer 3) относятся все устройства, которые работают на 3 уровне сетевой модели OSI — сетевом уровне. Данные коммутаторы управляемые. Коммутаторы 3 уровня целесообразнее отнести уже не к разряду коммутаторов, а к разряду маршрутизаторов, так как эти устройства уже полноценно могут маршрутизировать проходящий трафик между разными сетями. Коммутаторы 3 уровня полностью поддерживают все функции и стандарты коммутаторов 2 уровня. С сетевыми устройствами они могут работать по IP-адресам. Коммутатор 3 уровня поддерживает установку различных соединений: VPN, PPP и т.д.

Коммутатор 4 уровня (Layer 4) работает на транспортном уровне, умеет работать с приложениями. Коммутаторы 4 уровня используют информацию, которая содержится в заголовках пакетов и относится к уровню 3 и 4 стека протоколов, такую как IP-адреса источника и приемника, номер портов TCP/UDP для идентификации принадлежности трафика к различным приложениям. На основании этой информации коммутаторы 4 уровня могут принимать интеллектуальные решения о перенаправлении трафика того или иного сеанса.

Маршрутизаторы — это устройства третьего уровня эталонной модели OSI использующие один или более метрик для определения оптимального пути передачи трафика на основе информации сетевого уровня. По определению, основное назначение маршрутизаторов — это маршрутизация трафика сети. Процесс маршрутизации можно разделить на два иерархически связанных уровня:

1. Уровень маршрутизации. На этом уровне происходит работа с таблицей маршрутизации. Таблица маршрутизации служит для определения адреса (сетевого уровня) следующего маршрутизатора или непосредственно получателя по имеющемуся адресу (сетевого уровня) и получателя после определения адреса передачи выбирается определенный выходной физический порт маршрутизатора. Этот процесс называется определением маршрута перемещения пакета. Настройка таблицы маршрутизации ведется протоколами маршрутизации. Этот уровень часто называют уровнем управления (control plain).

2. Уровень передачи пакетов. Перед тем, как передать пакет, необходимо проверить контрольную сумму заголовка пакета, определить адрес (канального уровня) получателя пакета и произвести непосредственно отправку пакета с учетом очередности, фрагментации, фильтрации и т.д. Эти действия выполняются на основании команд, поступающих с уровня маршрутизации. Этот уровень часто называют уровнем данных (data plain).

Основные достоинства маршрутизаторов:

- можно вносить изменения в программную конфигурацию во время работы маршрутизатора, без его перезагрузки и прерывания выполнения сетевых приложений и услуг;
- возможность установки и удаления модулей во время работы маршрутизатора без перезагрузки или выключения системы. Требуется минимальное вмешательство оператора, так как адаптеры порта реконфигурируются автоматически;
- быстрая начальная загрузка (как правило, 35 секунд) обеспечивает быстрый ввод системы в рабочий режим после обновлений операционной системы, сводя к минимуму воздействие на работу сети;

- мониторинг параметров окружающей среды: выдача тревожных сообщений об отклонениях рабочих параметров от нормальных значений;
- самодиагностика и инструментальные средства контроля гарантируют работоспособность модулей перед их включением в работу;
- использование факультативного блока питания повышает отказоустойчивость и позволяет выравнивать нагрузку;
- flash-память обеспечивает быструю, надежную модернизацию программного обеспечения и микрокода с центрального пункта управления сети.

Маршрутизаторы обеспечивают сквозную маршрутизацию при прохождении пакетов данных и маршрутизацию трафика между различными сетями на основании информации сетевого протокола или уровня и способны принимать решение о выборе оптимального маршрута движения данных в сети. С помощью маршрутизаторов также может быть решена проблема чрезмерного широкополосного трафика, так как они не переадресовывают дальше широкополосные кадры, если им это не предписано. Маршрутизаторы и коммутаторы отличаются друг от друга в нескольких аспектах. Во-первых, коммутаторные соединения осуществляются на канальном уровне, в то время как маршрутизация выполняется на сетевом уровне эталонной модели OSI. Во-вторых, коммутаторы используют физические или MAC-адреса для принятия решения о передаче данных. Маршрутизаторы для принятия решения используют различные схемы адресации, существующие на уровне 3. Они используют адреса сетевого уровня, также называемые логическими или IP-адресами (Internet Protocol).

Межсетевой протокол IP (Internet Protocol) — маршрутизируемый сетевой протокол семейства TCP/IP. Протокол IP используется для доставки данных, разделяемых на пакеты, от одного узла сети к другому. Протокол не гарантирует надежной доставки пакета до адресата. В частности, пакеты могут прийти не в том порядке, в котором были отправлены, продублироваться (например, когда приходят две копии одного пакета), оказаться поврежденными (обычно поврежденные пакеты уничтожаются) или вообще не прибыть. В этом случае, отправителю посылается соответствующее ICMP-сообщение (или не посылается ничего). Обеспечение же надежности возлагается на более высокий уровень (UDP или TCP). На сегодняшний день на сети внедрены две версии протокола IPv4 и IPv6. Протокол IPv4. Формат IP-пакетов показан на рис. 2.3.2.

| | | | | | | |
|-------------------------|------|-------------------|-----------------------------|---------------------|-------------|----|
| 0 | 4 | 8 | 16 | 19 | 24 | 31 |
| Версия | Нлеп | Тип сервиса (TOS) | Полная длина | | | |
| Идентификатор | | | Флаги | Указатель фрагмента | | |
| Время жизни | | Протокол | Контрольная сумма заголовка | | | |
| IP-адрес отправителя | | | | | | |
| IP-адрес получателя | | | | | | |
| IP-опции (если имеются) | | | | | Заполнитель | |
| Данные | | | | | | |
| | | | | | | |

Рисунок 2.3.2 - Формат дейтаграммы Интернет протокола версии 4

Поле «Версия» (4 бита) определяет версию IP-протокола (например, 4 или 6). Формат пакета определяется программой.

«Длина заголовка» (Hlen) пакета IP занимает 4 бита и указывает значение длины заголовка, измеренное в 32-битовых словах. Поле «Полная длина» определяет полную длину IP-дейтаграммы (до 65535 октетов), включая заголовок и данные.

«Тип сервиса» TOS (Type Of Service) определяет, порядок обработки дейтаграмм. Это поле делится на 6 субполей.

Субполе «приоритет» (3 бита) предоставляет возможность присвоить код приоритета каждой дейтаграмме.

Биты D, T, R, C характеризуют способы доставки дейтаграммы. Так, D = 1 требует минимальной задержки, T = 1 — высокую пропускную способность, R = 1 — высокую надежность, а C = 1 — низкую стоимость. Интернет не гарантирует запрашиваемый TOS, но многие маршрутизаторы учитывают эти запросы при выборе маршрута (например, протоколы OSPF и IGRP).

Поле «полная длина» (2 байта) задает размер списка адресов, а «указатель фрагмента» отмечает адрес очередного маршрутизатора на пути дейтаграммы.

Существует две формы маршрутизации: свободная маршрутизация и жесткая маршрутизация.

Жесткая маршрутизация означает, что адреса определяют точный маршрут дейтаграммы. Путь от одного адреса к другому может включать только одну сеть.

Свободная маршрутизация отличается от предшествующей возможностью пересылки между двумя адресами списка более чем через одну сеть. Маршрутизаторы имеют маршрутные таблицы, которые просматриваются каждый раз, когда маршрутизаторы получают IP дейтаграмму для отправки. Когда дейтаграмма приходит от сетевого интерфейса, по маршрутной таблице проверяется, принадлежит ли IP-адрес места назначения к списку локальных адресов или является ширококвещательным адресом. Если имеет место один из этих вариантов, дейтаграмма передается программному модулю в соответствии с кодом в поле протокола. IP-процессор может быть сконфигурирован как маршрутизатор, в этом случае дейтаграмма может быть переадресована в другой узел сети. Маршрутизация на IP-уровне носит пошаговый характер. Протокол IP не знает всего пути, он владеет лишь информацией о том, какому маршрутизатору послать дейтаграмму с конкретным адресом места назначения.

При просмотре маршрутной таблицы возможны варианты:

- IP-адрес назначения совпал с IP-адресами, находящимися в маршрутной таблице. В этом случае пакет будет передан соответствующему маршрутизатору или непосредственно интерфейсу адресата. Связь «точка–точка» выявляются именно на этом этапе.

- IP-адрес назначения не совпал с IP-адресами, находящимися в маршрутной таблице. В этом случае система пересылает пакет всем узлам в сети, исключая тот, откуда пришел пакет.

- Осуществляется поиск маршрута по умолчанию и, если он найден, дейтаграмма посылается к соответствующему маршрутизатору.

«Идентификатор», «флаги» и «указатель фрагмента». Данные поля управляют процессом фрагментации и последующей «сборки» дейтаграммы. Идентификатор представляет собой уникальный код дейтаграммы, позволяющий идентифицировать принадлежность фрагментов и исключить ошибки при «сборке» дейтаграмм. Бит 0 поля «флаги» является резервным, бит 1 служит для управления фрагментацией пакетов (0 —

фрагментация разрешена; 1 — запрещена), бит 2 определяет, является ли данный фрагмент последним (0 — последний фрагмент; 1 — следует ожидать продолжения).

«Указатель фрагмента» отмечает первую свободную позицию в списке IP-адресов (куда можно произвести запись очередного адреса).

«Время жизни пакетов в сети» TTL (Time To Life). Задаёт время жизни дейтаграммы в секундах, то есть предельно допустимое время пребывания дейтаграммы в системе. Проходя через несколько маршрутизаторов, это время уменьшается в соответствии со временем пребывания в данном устройстве или согласно протоколу обработки. Если TTL = 0, дейтаграмма из системы удаляется.

Поле «Протокол» определяет структуру поля «данные».

Поле «Контрольная сумма заголовка» вычисляется с использованием операций сложения 16-разрядных слов заголовка по модулю 1. Сама контрольная сумма является дополнением по модулю 1 полученного результата сложения. В пакете осуществляется контрольное суммирование заголовка, а не всей дейтаграммы.

Поле «IP-опции» не обязательно присутствует в каждой дейтаграмме. Размер поля опции зависит от того, какие опции применены. Если используется несколько опций, они записываются подряд без каких-либо разделителей. Каждая опция содержит один байт кода опции, за которым может следовать байт длины и серия байтов данных. Если место, занятое опциями, не кратно 4 байтам, используется заполнитель.

IP-адрес представляет собой уникальную четырехбайтовую (32-битовую) величину, выраженную в десятичных числах, разделённых точками в форме W.X.Y.Z, где точки используются для отделения байтов (например, 10.12.10.1). Поле адреса размером 32 бита состоит из двух частей: адрес сети или связи, который представляет собой сетевую часть адреса, и адрес хоста, идентифицирующий рабочую станцию в сетевом сегменте. Разграничение сетей по количеству хостов в них традиционно осуществляется на основе так называемых классов IP-адресов. Сегодня существует 5 классов IP-адресов: А, В, С, D и Е. Распределение битов в IP-адресе сети представлены в табл. 2.3.1.

Таблица 2.3.1 – Распределение бит в IP-адресе сети

| | 0 | 7 8 | | | 15 16 | | 23 24 | | 31 |
|---------|---|------------|------------|------------|-----------------|-----------------|-------|-------------|----|
| Класс А | 1 | номер сети | | | номер хоста | | | | |
| Класс В | 1 | 0 | номер сети | | | номер хоста | | | |
| Класс С | 1 | 1 | 0 | номер сети | | | | номер хоста | |
| Класс D | 1 | 1 | 1 | 0 | групповой адрес | | | | |
| Класс E | 1 | 1 | 1 | 1 | 0 | зарезервировано | | | |

Опираясь на эту структуру, можно подсчитать число сетей и число хостов в каждой сети (табл. 2.3.2)

Таблица 2.3.2 – Диапазон значения сетей

| Класс | Диапазон значений первого байта | Возможное количество сетей | Возможное количество хостов в сетях |
|-------|---------------------------------|----------------------------|-------------------------------------|
| A | 1 – 127 | 127 | 16 777 216 |
| B | 128 – 191 | 16 384 | 65 534 |
| C | 192 – 223 | 2 097 152 | 254 |
| D | 224 – 239 | – | – |
| E | 240 – 247 | – | – |

Только адреса классов А, В и С могут использоваться как уникальные. Адреса класса D применяются для обращения к набору узлов, а адреса класса Е зарезервированы для исследовательских целей.

Возьмем для примера адрес в сети класса А 124.0.0.1. Здесь 124.0.0.0 представляет собой адрес сети, а единица в конце адреса обозначает первый хост в этой сети [2]. Первый и последний адреса хостов выполняют специальные функции. Так, первый адрес 124.0.0.0 (из приведенного выше примера) используется в качестве адреса сети, а последний адрес (124.255.255.255) представляет собой широковещательный адрес для этой сети. Таким образом, с помощью адресов класса А можно представить только 16 777 216 хостов в каждой сети.

Сети класса В определяются значениями 1 и 0 в старших битах адреса. Первые два байта в адресе (биты с 0 по 15) служат для представления адресов сетей, а оставшиеся два байта представляют номера хостов в этих сетях. В результате мы получим $2^{14} = 16\,384$ адреса сетей и 65 534 количество хостов в каждой сети (табл. 5.2) [2]. Сети класса С определяются значениями 110 в старших битах адреса. Первые три байта в адресе (биты с 0 по 23) служат для представления адресов сетей, а оставшийся один байт представляет номера хостов в этих сетях. В результате мы получим $2^{21} = 2\,097\,150$ адреса сетей и $[(2^8 - 2)]$ хостов в каждой сети (табл. 2.3.2).

Сети класса D определяются значениями 1, 1, 1 и 0 в первых четырех битах IP-адреса. Адресное пространство класса D зарезервировано для представления групповых IP-адресов, которые используются для адресации набора узлов. Это означает, что данный пакет должен быть доставлен сразу нескольким узлам, которые образуют группу с номером, указанным в поле адреса.

Сети класса Е определяются значениями 1, 1, 1 и 1 в старших четырех битах IP-адреса. Адреса этого диапазона зарезервированы для экспериментальных целей.

Важным элементом адресного пространства Internet являются подсети.

Подсеть — это подмножество сети или фрагменты сети, которые не пересекаются с другими подсетями. Это означает, что сеть организации (например, сеть класса В) может быть разбита на фрагменты, каждый из которых будет составлять подсеть. Реально, каждая подсеть соответствует физической локальной сети (например, сегменту Ethernet).

Таким образом, подсети придуманы для того, чтобы обойти ограничения физических сетей на число узлов в них.

При использовании шлюза сеть разбивается на подсети.

Как и номера хост-машин в сетях класса А, класса В и класса С, адреса подсетей задаются локально. Обычно это выполняет сетевой администратор. Так же, как и другие IP-адреса, каждый адрес подсети является уникальным. Использование подсети никак не

отражается на том, как внешний мир видит эту сеть, но в пределах организации подсети рассматриваются как дополнительные структуры.

Адрес подсети включает номер сети, подсети и номер хост-машины внутри подсети. Благодаря этим трем уровням адресации подсети обеспечивают сетевым администраторам повышенную гибкость настройки.

При разбивке сетей на подсети используют ту часть IP-адреса, которая закреплена за номерами хостов (узлов).

Таким образом, чтобы создать адрес подсети, сетевой администратор «заимствует» биты из поля хост-машин и перераспределяет их в качестве поля подсетей. Количество «заимствованных» битов можно увеличивать до тех пор, пока не останется 2 бита. Поскольку в поле хостов сетей класса В имеются только 2 октета, для создания подсетей можно заимствовать до 14 бит. Сети класса С имеют только один октет в поле хостов. Следовательно, в сетях класса С для создания подсетей можно заимствовать до 6 бит (рис. 2.3.3).

| | | | |
|-----------------------------------|-----------------------------------|-----------------------------------|-----------------------------------|
| $2^7 2^6 2^5 2^4 2^3 2^2 2^1 2^0$ | $2^7 2^6 2^5 2^4 2^3 2^2 2^1 2^0$ | $2^7 2^6 2^5 2^4 2^3 2^2 2^1 2^0$ | $2^7 2^6 2^5 2^4 2^3 2^2 2^1 2^0$ |
| 11111111 | 11111111 | 11111111 | 11111100 |
| Сеть | Сеть | Сеть | Поле подсети хосты |

Рисунок 2.3.3 - Биты заимствуются из поля хост-машины и переопределяются в качестве поля подсети

Чем больше бит заимствуется из поля хоста, тем меньше бит в октете можно использовать для задания номера хоста. Таким образом, каждый раз, когда заимствуется 1 бит из поля хоста, число адресов хостов, которые могут быть заданы, уменьшается на степень числа 2.

Чтобы понять смысл вышесказанного, рассмотрим сеть класса С. Все 8 бит в последнем октете используются для поля хостов. Следовательно, возможное количество адресов равно 28 или 256.

Представим, что эту сеть разделили на подсети. Если из поля хостов заимствовать 1 бит, количество бит, которое можно использовать для адресации хостов, уменьшится до 7. Если записать все возможные комбинации нулей и единиц, можно убедиться, что число хостов, которые можно адресовать, стало равно 27 или 128.

Если в сети класса С из поля хостов заимствовать 2 бита, то количество бит, которое можно использовать для адресации хостов, уменьшится до 6. Общее число хостов, которое можно адресовать, станет равным 26 или 64.

IP-адреса, которые заканчиваются всеми двоичными единицами, зарезервированы для широковещания. Это утверждение справедливо и для подсетей.

Для увеличения адресного пространства в сети и создания подсетей часть IP-адреса можно замаскировать. Для этого используется «маска». **Маска подсети** — это 4 байта, которые накладываются на IP-адрес для получения номера подсети; она разделена на 4 октета. Маски подсетей имеют все единицы в части, отвечающей за сети и подсети, и все нули в части, отвечающей за хост-машины. По умолчанию, если нет заимствованных битов, маска подсети сети класса В будет иметь вид 255.255.0.0 (рис. 2.3.4). Если же заимствовано 8 бит, маской подсети той же сети класса В будет 255.255.255.0. Поскольку для сетей класса

В только 2 октета относится к полю хост-машин, то для создания подсетей может быть задействовано до 14 бит. В сетях класса С только один байт относится к полю хост-машин, поэтому для создания подсетей может быть заимствовано до 6 бит.

Маски подсети также используют 32-битовые IP-адреса, которые содержат все двоичные единицы в сетевой и подсетевой части адреса, и все двоичные нули в хостовой части адреса. Таким образом, адрес маски подсети класса В с 8 заимствованными битами из поля хостов будет иметь вид 255.255.255.0 (рис. 2.3.4). Это уже маска для сети класса С.

| 2 ⁷ 2 ⁶ 2 ⁵ 2 ⁴ 2 ³ 2 ² 2 ¹ 2 ⁰ | 2 ⁷ 2 ⁶ 2 ⁵ 2 ⁴ 2 ³ 2 ² 2 ¹ 2 ⁰ | 2 ⁷ 2 ⁶ 2 ⁵ 2 ⁴ 2 ³ 2 ² 2 ¹ 2 ⁰ | 2 ⁷ 2 ⁶ 2 ⁵ 2 ⁴ 2 ³ 2 ² 2 ¹ 2 ⁰ |
|---|---|---|---|
| 183 | 205 | 0 | 0 |
| 10110111 | 11001101 | 00000000 | 00000000 |
| 255 | 255 | 0 | 0 |
| 11111111 | 11111111 | 11111111 | 00000000 |
| 255 | 255 | 255 | 0 |

Рисунок 2.3.4. - Биты для создания подсети заимствуются из поля хост-машин, начиная со старших позиций

Для создания подсети в классе В вместо 8 бит в третьем октете заимствуются только 7. В двоичном представлении маска подсети в этом случае будет иметь вид 11111111.11111111.11111110.00000000. Следовательно, 255.255.255.0 не может больше использоваться в качестве маски подсети, в данном случае маска подсети будет 255.255.254.0.

Таким образом, стандартные маски без разбивки на подсети следующие:

класс А — 255.0.0.0;

класс В — 255.255.0.0;

класс С — 255.255.255.0.

2.4. Порядок выполнения работы

2.4.1. Предварительная настройка сетевого оборудования

Соберите сетевую топологию согласно рисунку 2.4.1. Топология содержит 6 ПК, 2 коммутатора (Cisco 2960), маршрутизатор (Cisco 2811).

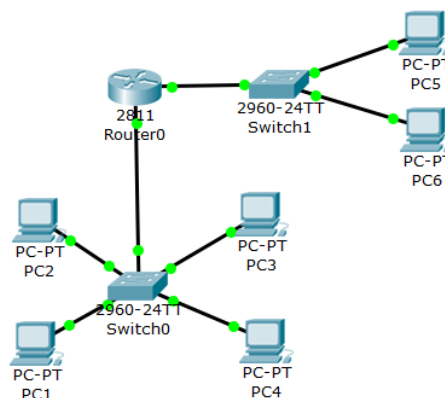


Рисунок 2.4.1 – Топология сети

Назначьте всем устройствам сетевые адреса согласно таблице 2.4.1. N- номер по журналу.

Таблица №2.4.1. Сетевые адреса устройств

| Сетевой элемент | Интерфейс | IP-адрес | Маска подсети |
|-----------------|-----------------|-----------------|---------------|
| PC1 | FastEthernet0 | 192.168.N.1 | 255.255.255.0 |
| PC2 | FastEthernet0 | 192.168.N.2 | 255.255.255.0 |
| PC3 | FastEthernet0 | 192.168.N.3 | 255.255.255.0 |
| PC4 | FastEthernet0 | 192.168.N.4 | 255.255.255.0 |
| PC5 | FastEthernet0 | 192.168.N+1.1 | 255.255.255.0 |
| PC6 | FastEthernet0 | 192.168.N+1.2 | 255.255.255.0 |
| Router0 | FastEthernet0/0 | 192.168.N.254 | 255.255.255.0 |
| | FastEthernet0/1 | 192.168.N+1.254 | 255.255.255.0 |

После соединения компьютеров и сетевых устройств необходимо настроить их конфигурацию (Для 1 варианта). Для этого сначала кликаем мышью по пиктограмме компьютера для вызова меню. В появившемся окне переходим на вкладку «Desktop» и активируем «IP Configuration», где настраиваем конфигурацию первого компьютера (PC1): IP-адрес 192.168.1.1, маска подсети 255.255.255.0 (рис. 2.4.3).

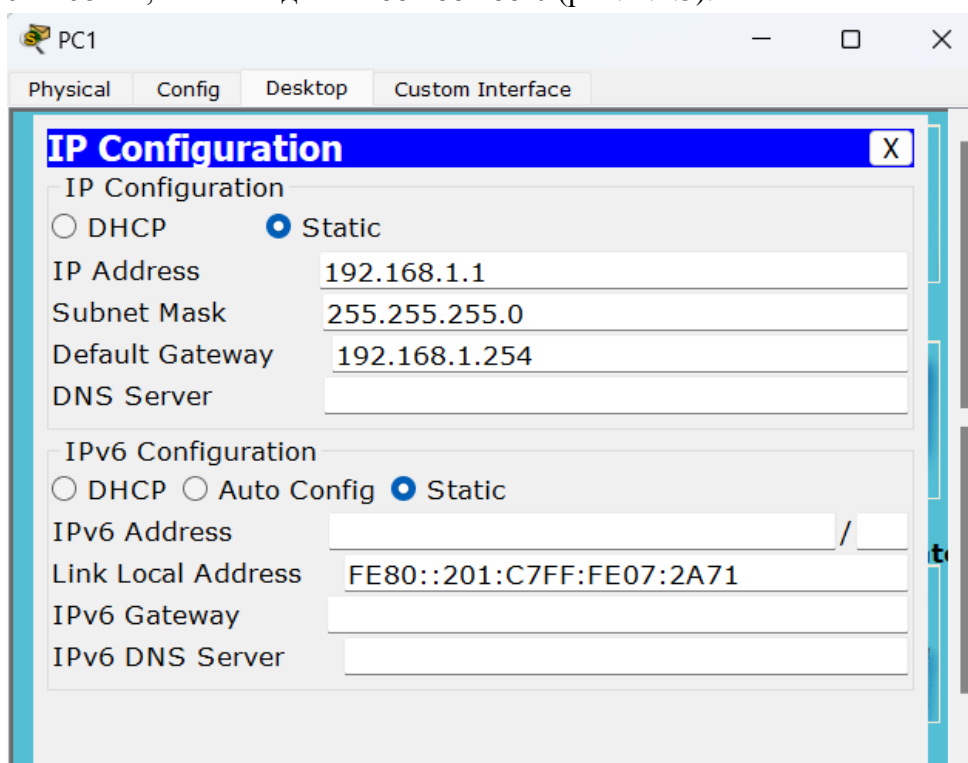


Рисунок 2.4.3 – Конфигурирование левого компьютера (PC1)

Аналогично настраиваем правый по схеме компьютер (PC5): IP-адрес 192.168.2.1, маска подсети 255.255.255.0 (рис. 2.4.4).

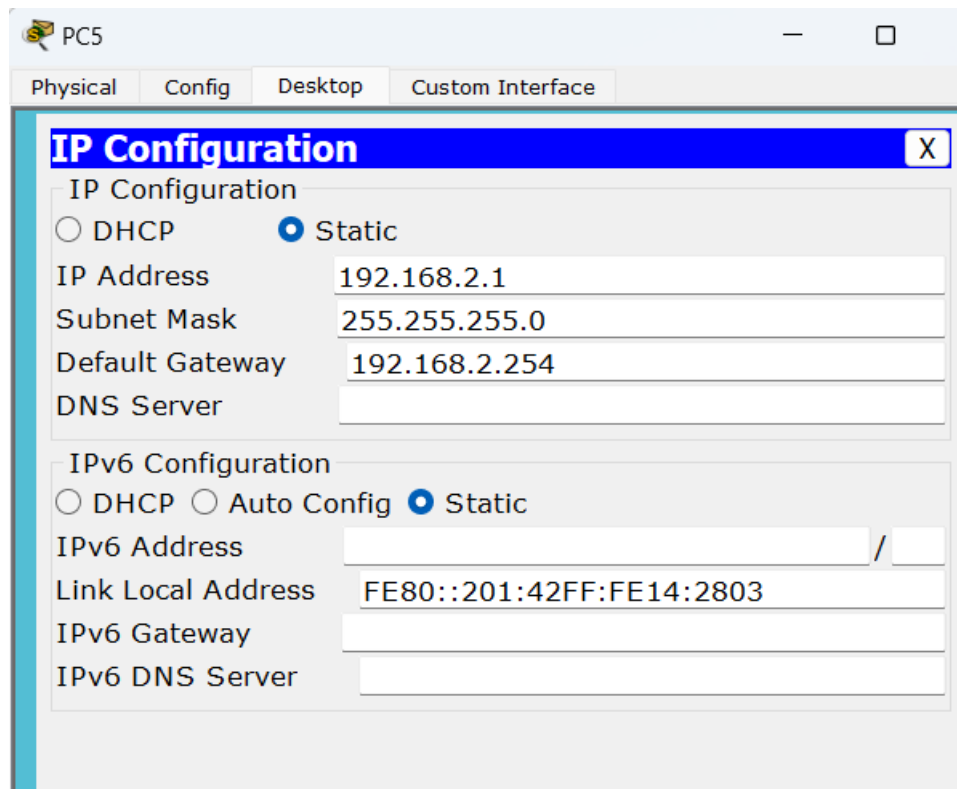


Рисунок 2.4.4 – Конфигурирование правого компьютера (PC5)

Аналогичным образом производим настройку остальных компьютеров первого и второго сегмента сети.

Настройка Router0 осуществляется подобным образом. Кликаем мышью по пиктограмме маршрутизатора (Router0) для вызова меню. В появившемся окне переходим на вкладку «Config» и в поле «Interface» поочередно настраиваем FastEthernet0/0 и FastEthernet0/1. Вначале необходимо включить интерфейс, для этого переводим его в режим «On». В поле адрес настраиваем адресацию и маску подсети.

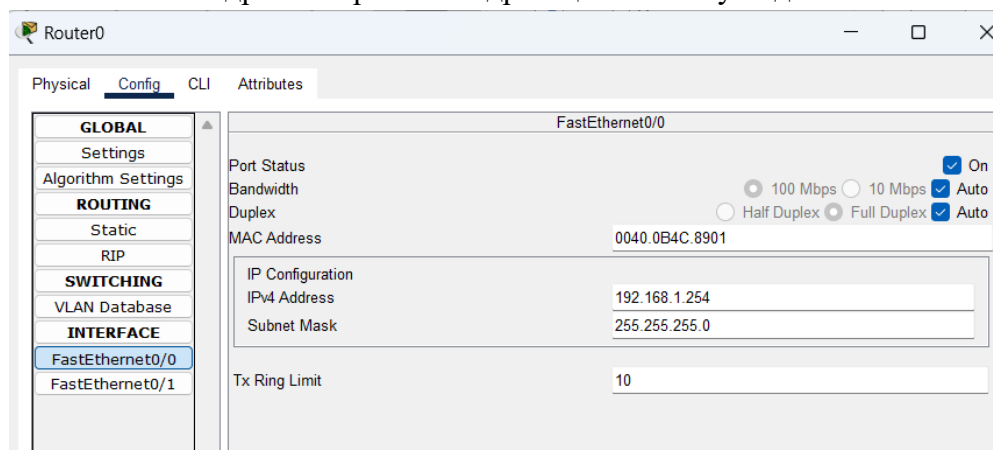


Рисунок 2.4.5 Настройка маршрутизатора

Повторить действия для второго интерфейса и прописать соответствующий адрес.

Настроить на компьютерах каждого сегмента сети шлюз по умолчанию, которым является адрес роутера в этом сегменте сети.

Проверку наличия связи между двумя компьютерами можно осуществить, если ввести команду «ping» перейдя на вкладке «Desktop» в поле «Command Prompt» и указать IP-адрес соседнего компьютера. Как видно из рисунка 2.4.6, связь между компьютерами существует и настроена.

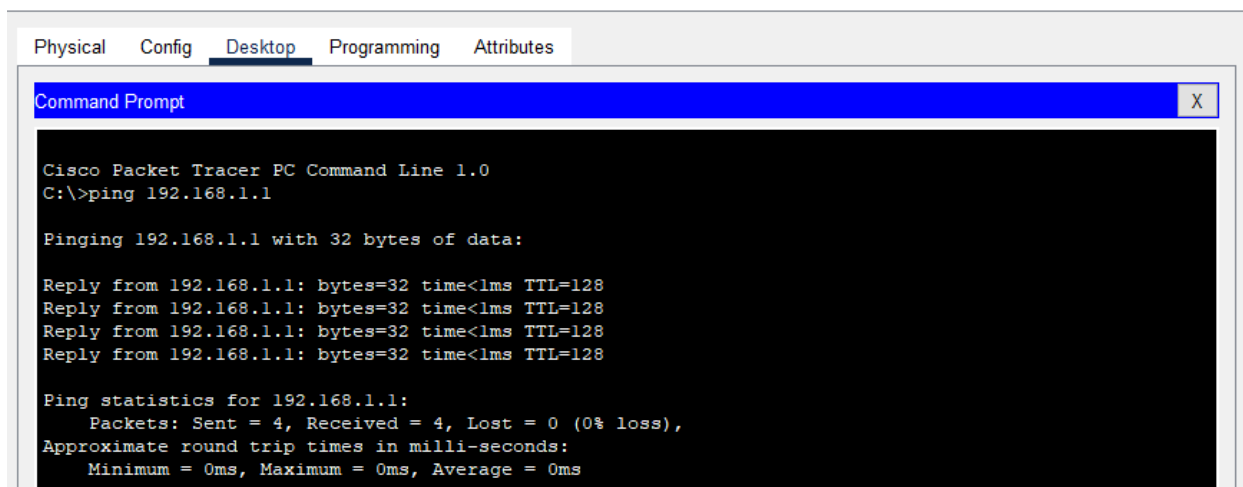


Рисунок 2.4.6 – Подтверждение наличия связи между двум компьютерами

Проверить связи между другими устройствами одного и разных сегментов сети с помощью команды «ping», а также с помощью простого PDU.

2.5. Содержание отчёта

В индивидуальном отчёте должны быть указаны цель, задание, краткое описание лабораторного стенда, представлены необходимые снимки экрана и пояснения к ним. Следует проанализировать полученные данные и дать ответы на контрольные вопросы.

2.6. Контрольные вопросы

1. Какие типовые топологии сетей вам известны?
2. Каковы достоинства и недостатки известных типовых топологий сетей?
3. Опишите принцип действия сетевого концентратора (хаба)
4. Опишите принцип действия сетевого моста
5. Опишите принцип действия коммутатора
6. Опишите принцип действия маршрутизатора
7. В чем отличие между коммутатором и маршрутизатором?
8. Какие формы маршрутизации вам известны?
9. Что такое IP-адрес, какие функции он выполняет? Из каких частей состоит? Какие классы IP-адресов вы знаете?
10. Что такое подсеть и для чего она создаётся?
11. Что такое маска подсети? Какие функции она выполняет?
12. Что такое команда ping? Зачем она нужна?