МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Юго-Западный государственный университет»
(ЮЗГУ)

Кафедра вычислительной техники

УТВЕРЖДАЮ
Проректор по учебной работе
_____ О.Г. Локтионова
«20» 02 2026 г.

ТЕХНОЛОГИИ БЕСПРОВОДНОЙ СВЯЗИ

Методические указания по практическим занятиям и лабораторным работам для студентов направления подготовки «Информатика и вычислительная техника»

Курск 2026

УДК 004.7

Составитель Д.О. Бобынцев

Рецензент: к.т.н., доцент Конаныхина Т.Н.

Технологии беспроводной связи: методические указания к практическим занятиям и лабораторным работам / Юго-Зап. гос. ун-т; сост.: Д.О. Бобынцев. Курск, 2026. – 44 с.

Содержит методические указания по практическим и лабораторным занятиям дисциплины «Технологии беспроводной связи». Даны теоретические материалы, описание порядка выполнения работ, контрольные вопросы, список литературы. Предназначено для студентов направления подготовки «Информатика и вычислительная техника».

Текст печатается в авторской редакции

Подписано в печать 20.02.26. Формат 60x84 1/16.
Усл.печ. л. 2,56. Уч.-изд. л. 2,32. Тираж 100 экз. Заказ. 188 Бесплатно.
Юго-Западный государственный университет.
305040, г. Курск, ул. 50 лет Октября, 94.

Лабораторные работы

Все лабораторные работы выполняются в виртуальной лаборатории при помощи специализированного программного обеспечения – Cisco Packet Tracer. Это свободно доступный программный продукт, разработанный и выпускаемый фирмой Cisco Systems в учебных целях.

Cisco Packet Tracer – это симулятор телекоммуникационных сетей, он позволяет строить работоспособные модели сети, настраивать маршрутизаторы и коммутаторы (преимущественно производства фирмы Cisco Systems), в произвольных топологиях с поддержкой разных протоколов. В симуляторе реализованы серии маршрутизаторов Cisco 800, 1800, 1900, 2600, 2800, 2900 и коммутаторов Cisco Catalyst 2950, 2960, 3560, а также межсетевой экран ASA 5505. Беспроводные устройства представлены маршрутизатором Linksys WRT300N, точками доступа и сотовыми вышками. Кроме того, есть серверы DHCP, HTTP, TFTP, FTP, DNS, AAA, SYSLOG, NTP и EMAIL, рабочие станции, различные модули к компьютерам и маршрутизаторам, IP-фоны, смартфоны, хабы, а также облако, эмулирующее глобальные сети. Объединять сетевые устройства можно с помощью различных типов кабелей, таких как прямые и обратные патч-корды, оптические и коаксиальные кабели, последовательные кабели и телефонные пары.

Cisco Packet Tracer позволяет создавать довольно сложные макеты сетей, что зачастую нереально сделать на реальном оборудовании, проверять на работоспособность топологии. Однако, реализованная функциональность устройств ограничена и не предоставляет всех возможностей реального оборудования, но зато приспособлена для понимания основных концепций устройства вычислительных сетей.

Организация сети с помощью коммутатора

Цель работы: смоделировать сеть на основе концентраторов и коммутаторов Ethernet.

Если в сети появляется более двух компьютеров, то необходимы следующие устройства:

- сетевой концентратор (hub);
- коммутатор (switch).

Для организации сети с помощью коммутатора с использованием Cisco Packet Tracer необходимо:

1. Запустить Cisco Packet Tracer;
2. Пусть в сети будет 4 компьютера. Перетаскиваем 1 компьютер, кликом по нему вызываем мастер настроек и в разделе Desktop – IP Configuration задаём IP адрес вида 192.168.1.N, где N – ваш номер по списку. Аналогично создаем 2-4 компьютеры, которым задаём IP-адреса, отличающиеся только последним числом: N+1, N+2 и N+3 соответственно. В результате должно получиться, как на рис. 1.

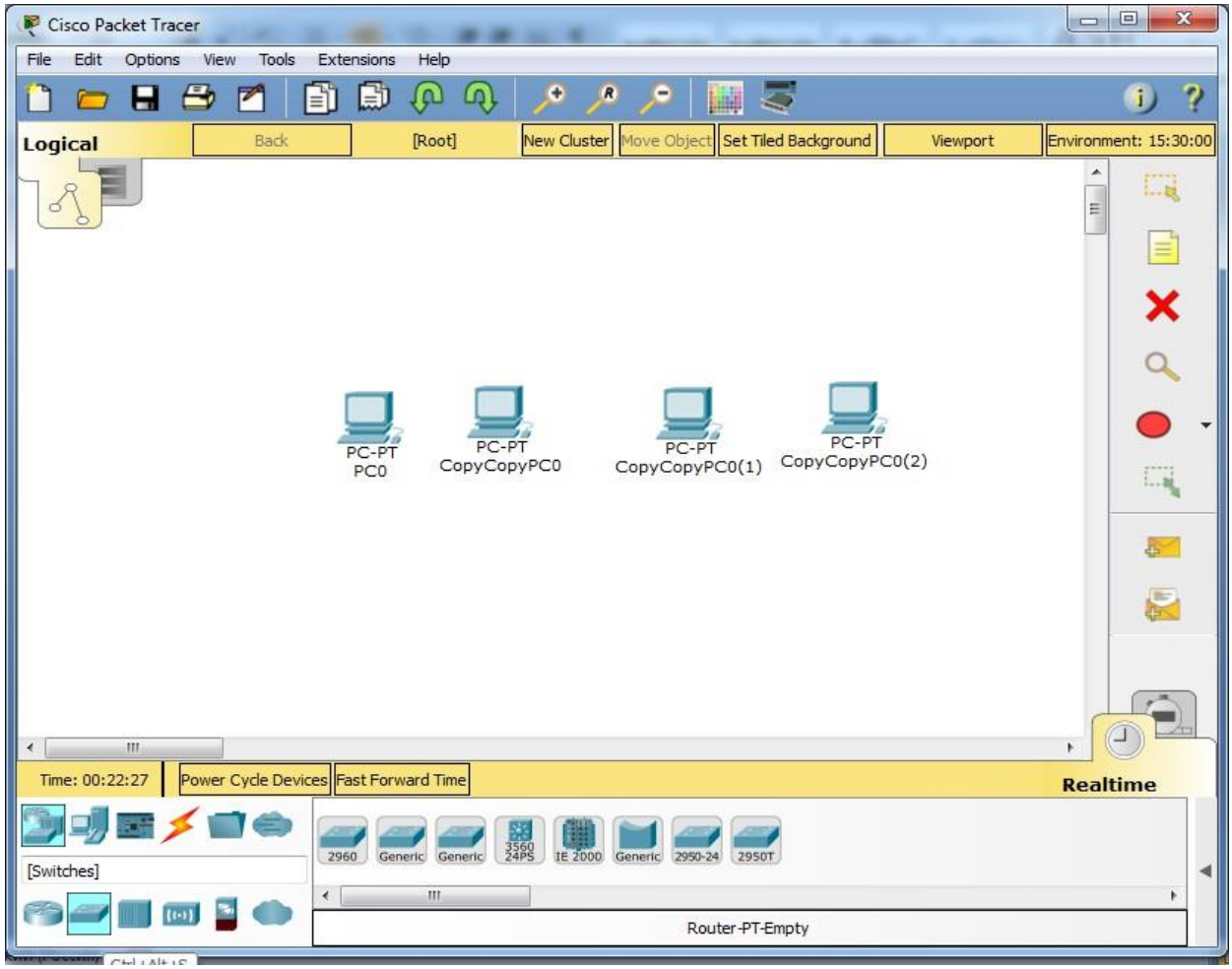


Рисунок 1 – Создание 4 компьютеров

3. Рассмотрим 2 случая.

3.1. В первом выбираем Switches – коммутатор 2960 (рис. 1).

- переходим на вкладку Connections в нижнем левом меню. Выбираем тип кабеля (в нашем случае прямой). И подключаем Fast Ethernet – Fast Ethernet (рис. 2). Если link загорелся зелёным (это может произойти не сразу), значит, наша сеть функционирует;

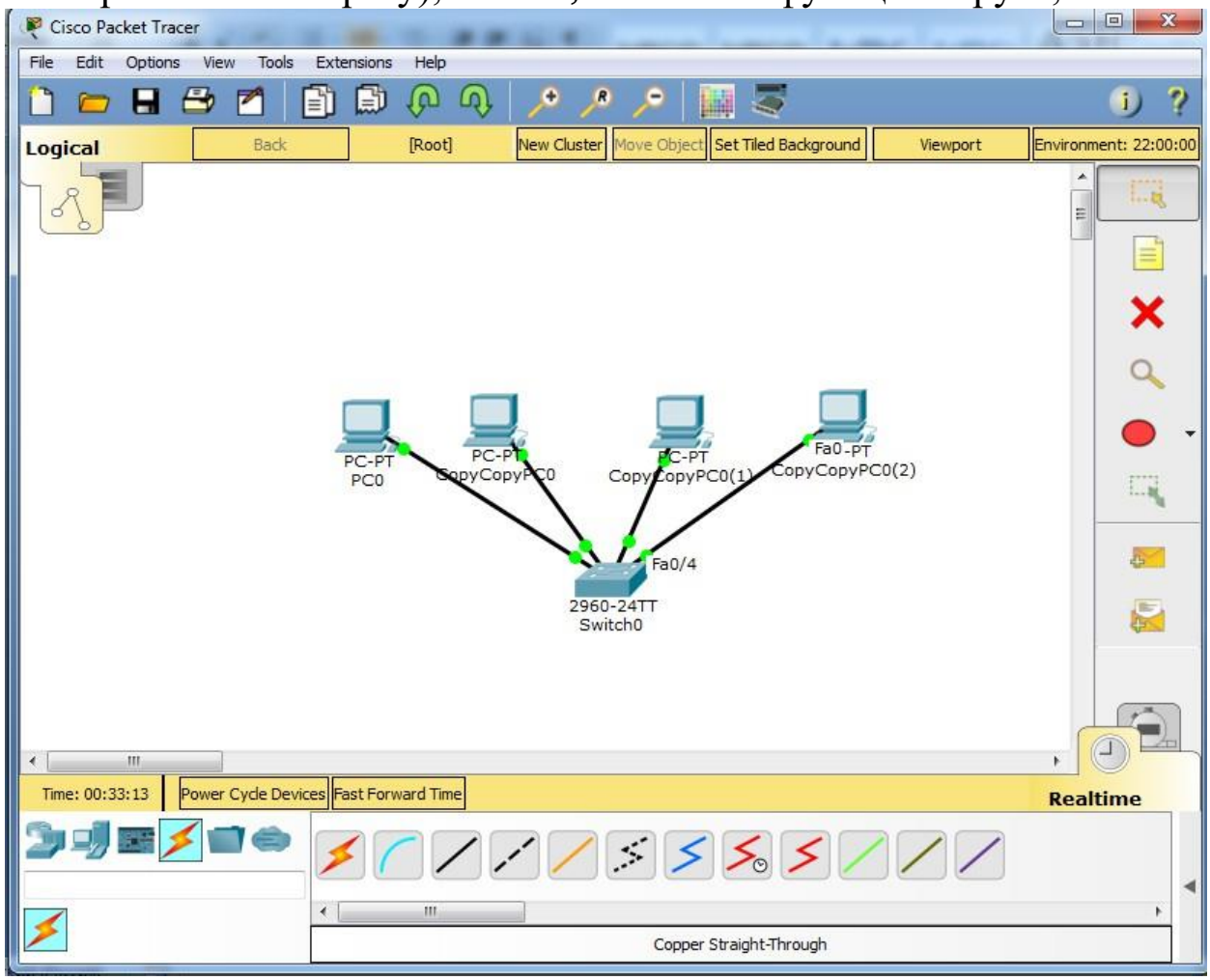


Рисунок 2 – Сеть из 4 компьютеров, соединённая коммутатором

- проверим работоспособность сети: выбираем в мастере настройки любого из компьютеров Desktop – Command Prompt, и прозваниваем остальные компьютеры по их IP-адресам командой ping <IP-адрес вызываемого компьютера>. Если результат, как на рис. 3, значит, связь работает.

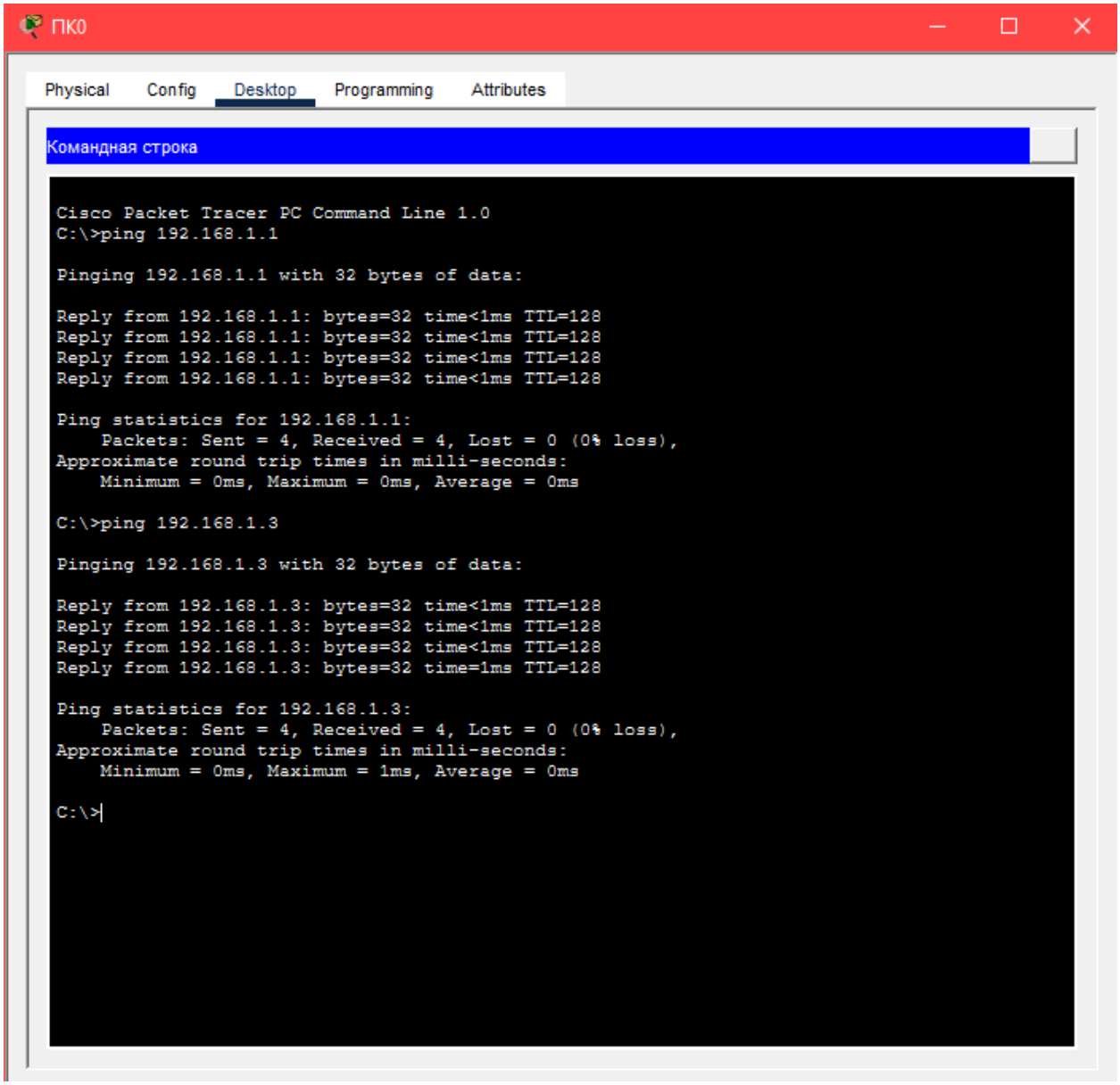


Рисунок 3 – Успешный результат прозвона

3.2. Во втором случае выбираем Hubs вместо Switch.

- переходим на вкладку Connections, выбираем тип кабеля (в этом случае прямой) и подключаем;
- проверяем работоспособность сети.

4. Воспользуемся визуализацией прохождения пакета с помощью функции Add Simple PDU (P). Например, с компьютера 2 передаем пакет на компьютер 3.

5. Затем переходим во вкладку Simulation – Capture/Forward. Результат передачи приведен на рис. 4.

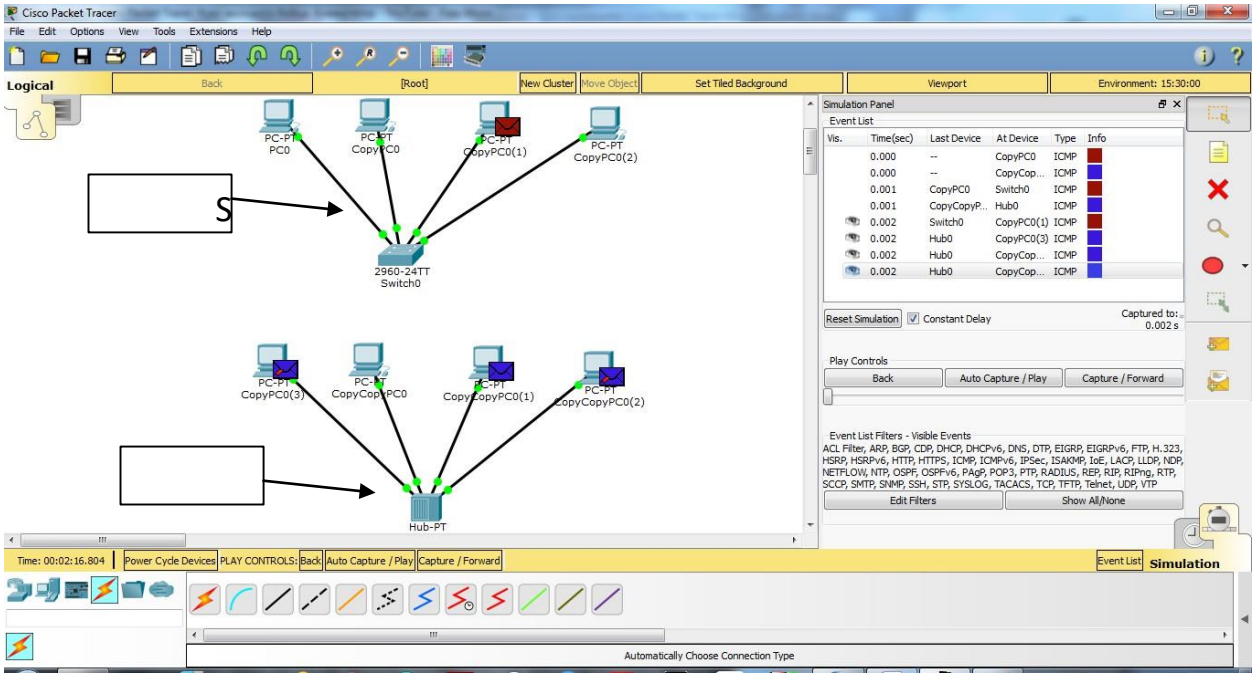


Рисунок 4 – Результат передачи пакета с компьютера 2 на компьютер 3

Результаты работы покажите преподавателю.

Контрольные вопросы

1. Что такое концентратор?
2. Что такое коммутатор?
3. На каких уровнях ЭМВОС работают концентратор и коммутатор?
4. Чем отличается IP-адрес от MAC-адреса?
5. Что такое маска подсети?
6. Что делает команда ping?

Подключение к сетевому оборудованию

Цель работы: познакомиться с методами управления активным сетевым оборудованием.

Ход работы

Известные следующие способы подключения сетевого оборудования:

1. С помощью консольного кабеля.
2. По Telnet/SSH.
3. Web-интерфейс.
4. Специализированное ПО (SDM, IME, CSM).

Для подключения необходимо:

1. Компьютер.
2. Консольный кабель;
3. Переходник USB-to-Com.
4. ПО (Putty/SecureCRT).

Рассмотрим процесс подключения коммутатора в Cisco Packet Tracer:

1. Подключаемся по консоли:

1.1. Запускаем Cisco Packet Tracer.

1.2. В рабочую область добавляем компьютер и коммутатор (2960). И соединяем консольным кабелем (Console) RS 232-Console. В конфигурации компьютера выбираем Terminal.

1.3. В Terminal заходим в привилегированный режим с помощью команды enable.

1.4. Перед настройкой необходимо войти в режим «глобального конфигурирования» с помощью команды configure terminal.

1.5. Для безопасности создадим пароль на вход в привилегированный режим. Набираем enable password parol. Вместо parol вводим свой пароль.

1.6. Однако применение enable password не совсем безопасно. Если ввести show run, то мы увидим строку enable password parol. Для того чтобы это скрыть сделаем следующее:

- набираем команду configure terminal. Затем вводим команду service password-encryption.
- выходим из режима конфигурации и вводим команду show run. Как видно из рис.1, пароль зашифрован

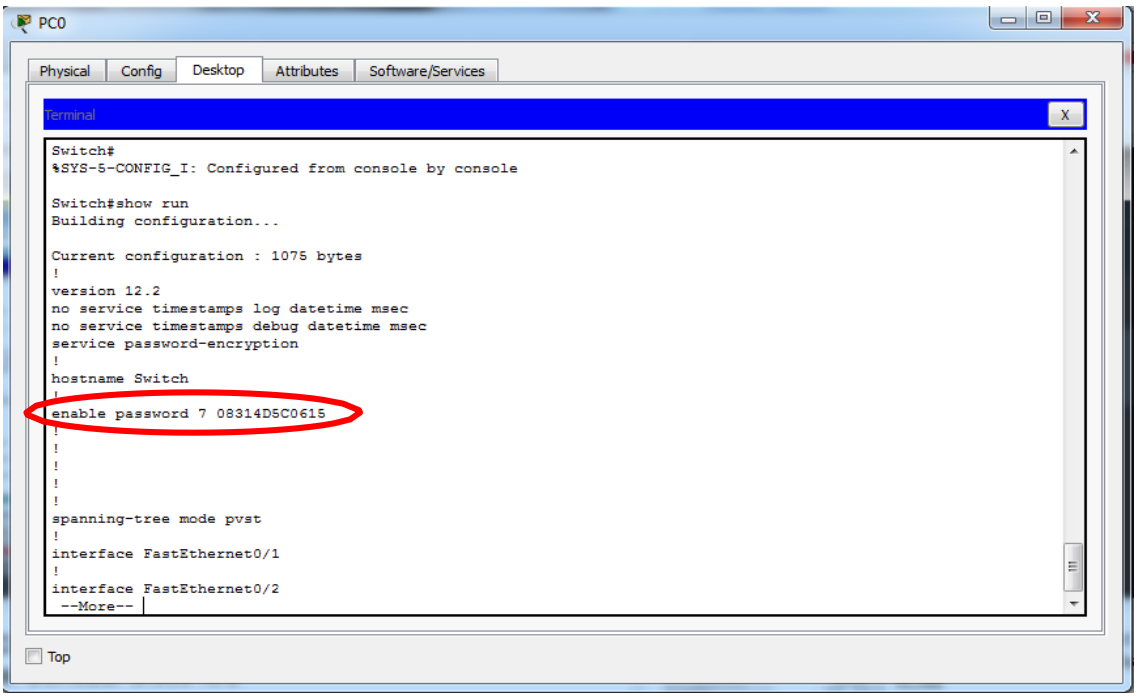


Рисунок 1 – Пароль на привилегированный режим с помощью команды enable secret

1.7. Второй способ задания пароля:

- заходим в режим «глобального конфигурирования», вводим команду enable secret parol2;
- затем выходим из режима конфигурации и вводим команду show run, на рис. 2 видно, что наш второй пароль также зашифрован. При этом приоритет имеет именно этот пароль.

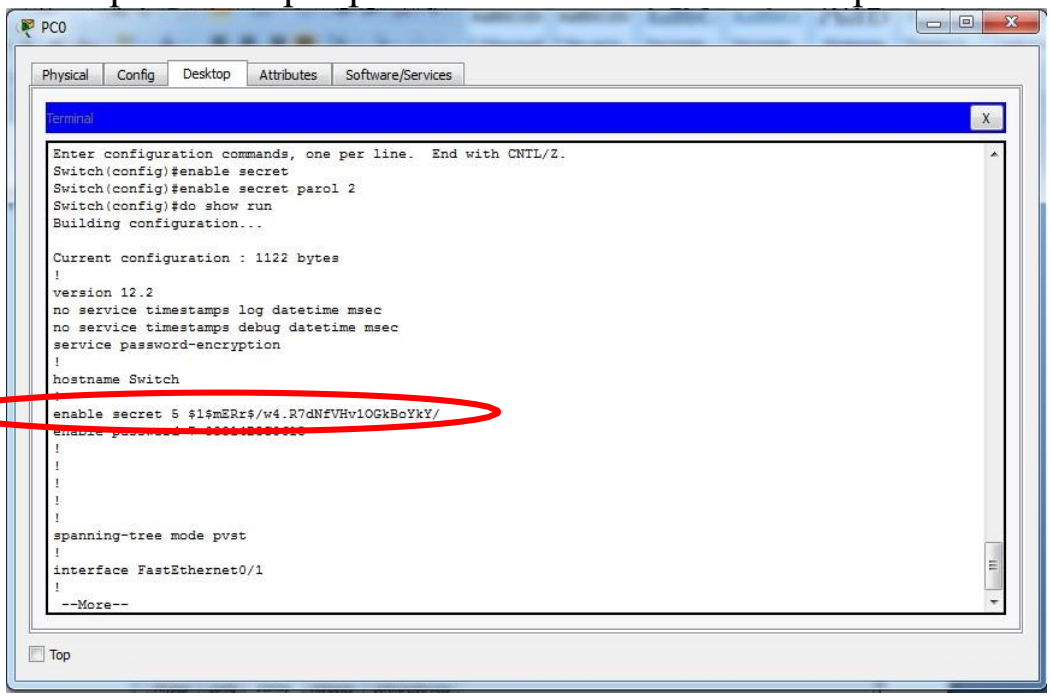


Рисунок 2 – Пароль на привилегированный режим с помощью команды enable password

2. Создадим пользователя.

2.1. Заходим в привилегированный режим «глобального конфигурирования».

2.2. Вводим команду username admin privilege. Выводится значение от 0 до 15. При 15 пользователю доступны все команды. Здесь admin – имя пользователя. Затем вводим команду username admin 15 password parol. Здесь parol – пароль. Локальный пользователь создан;

3. Установим авторизацию на подключение к консоли:

3.1. Заходим в режим «конфигурирования терминальных линий». В режиме «глобального конфигурирования» набираем команду line console 0.

3.2. Набираем команду login local.

3.3. Выходим из всех режимов конфигурации с помощью команды end. Теперь при попытке входа в консоль требуется ввести имя пользователя и пароль, вводим их. Доступ к консоли защищен.

4. Задаем IP адрес устройства.

4.1. Заходим в режим «глобального конфигурирования». Вводим команду interface Vlan1.

4.2. Набираем команду ip address 192.168.1.1 255.255.255.0. Здесь 192.168.1.1 – IP адрес, 255.255.255.0 – маска подсети для того, чтобы убедиться, что интерфейс поднят набираем команду no shutdown.

4.3. Выходим из режима конфигурирования интерфейса с помощью команды end.

5. Настроим виртуальные терминальные линии;

5.1. Заходим в режим глобального конфигурирования. Набираем команду line vty 0 4.

5.2. Определим транспортный протокол. Введем команду transport input telnet;

Создадим пароль на вход с помощью команды login local.

5.3. Выходим из режима конфигурирования и сохраняем конфигурации write memory.

6. Конфигурация сохранена. Чтобы проверить выполним следующие действия:

6.1. Для этого в Cisco Packet Tracer подключим компьютер прямым кабелем с коммутатором по FastEthernet.

6.2. Сконфигурируем IP адрес из той же сети, что и IP адрес нашего коммутатора. В настройках компьютера в IP адресе введем 192.168.1.2.

6.3. В командной строке вызовем команду telnet 192.168.1.1 с адресом коммутатора.

6.4. Коммутатор запросил имя пользователя и пароль (Username – admin, password – parol). Таким образом, мы зашли удаленно на наш коммутатор.

Контрольные вопросы

1. Какие вы знаете способы подключения сетевого оборудования?
2. Что понимается под привилегированным режимом терминала в Cisco Packet Tracer?
3. Что делает команда service password-encryption?
4. Что делает команда enable password?
5. Что делает команда line vty?

Протокол DHCP

Цель работы: освоить управление службой автоматической раздачи и учёта IP-адресов.

О службе DHCP

В современном мире сетевых технологий важно понимать основные протоколы, обеспечивающие стабильную работу сети. Один из таких протоколов — DHCP. В этой статье мы подробно рассмотрим, что такое DHCP, как он работает, и почему он необходим для эффективного управления сетями.

DHCP (от англ. *Dynamic Host Configuration Protocol*) – это протокол динамической конфигурации узла. Он автоматически назначает IP-адреса и другие сетевые параметры устройствам в сети, что позволяет им быстро и безошибочно подключаться к локальной сети или интернету.

Основное назначение DHCP заключается в автоматизации процесса настройки сетевых параметров устройств в сети. Это избавляет от необходимости вручную присваивать каждому устройству уникальный IP-адрес и другие параметры. Использование DHCP позволяет:

- Упростить управление сетью, особенно при большом количестве устройств.
- Снизить вероятность ошибок, связанных с дублированием IP-адресов.
- Ускорить подключение новых устройств к сети.
- Облегчить администрирование сетевых настроек.

Работа DHCP основана на взаимодействии между DHCP-клиентом (устройство, подключающееся к сети) и DHCP-сервером (устройство или сервис, управляющий распределением IP-адресов). Процесс состоит из четырех основных этапов:

1. DHCP Discover (Обнаружение): Когда устройство подключается к сети, DHCP-клиент отправляет широковещательный запрос, пытаясь найти DHCP-сервер. Это сообщение называется DHCP Discover.
2. DHCP Offer (Предложение): DHCP-сервер получает запрос и отвечает пакетом DHCP Offer, предлагая свободный IP-адрес из своего пула адресов вместе с другими сетевыми параметрами.

3. DHCP Request (Запрос): Клиент получает предложение и отвечает серверу сообщением DHCP Request, подтверждая готовность принять предложенные параметры.

4. DHCP Acknowledgment (Подтверждение): Сервер подтверждает назначение IP-адреса и отправляет клиенту окончательные параметры. После этого устройство может полноценно работать в сети.

DHCP-сервер автоматически предоставляет клиенту следующие сетевые параметры:

- IP-адрес: Уникальный адрес устройства в сети.
- Маска подсети: Определяет диапазон адресов в локальной сети.
- Основной шлюз: Адрес устройства, через которое осуществляется выход в другие сети или интернет.
- DNS-серверы: Адреса серверов доменных имен для преобразования URL в IP-адреса.
- Время аренды IP-адреса: Период, на который назначается IP-адрес клиенту.
- Другие параметры: Например, параметры прокси-сервера, домена и т.д.

Преимущества использования DHCP

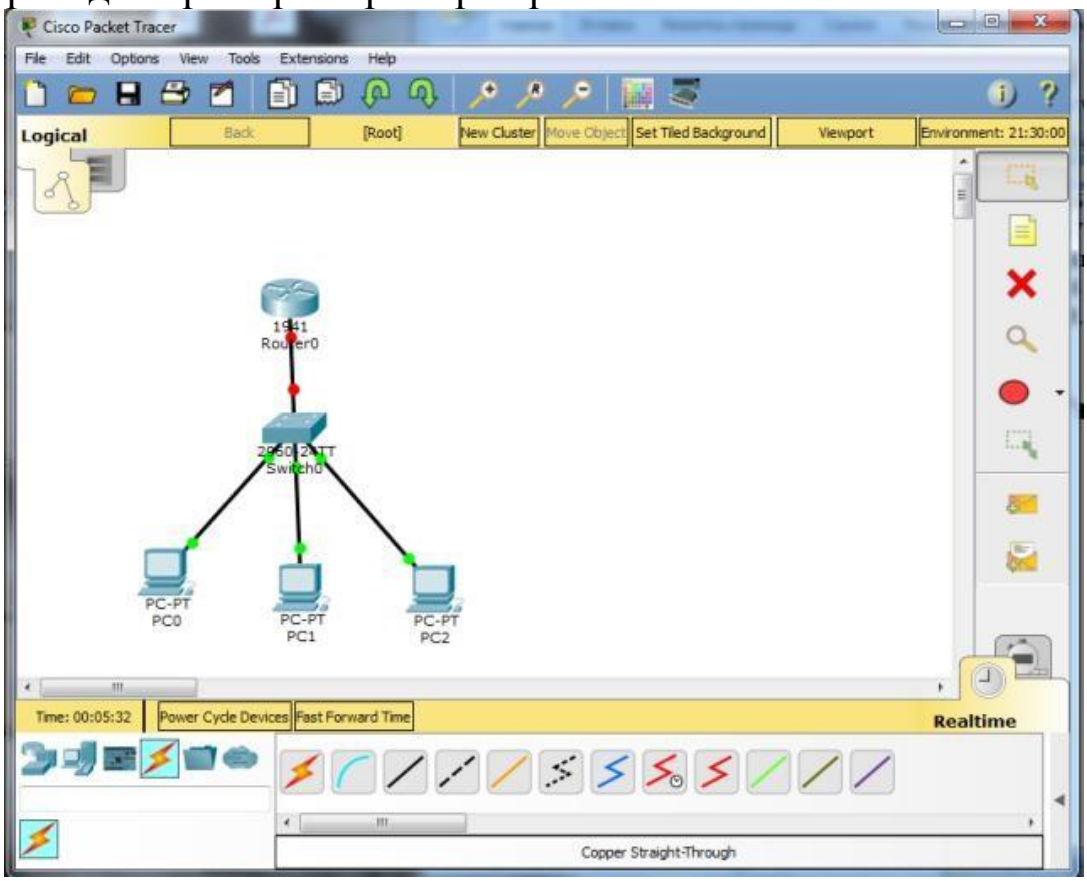
- Автоматизация процесса настройки: нет необходимости вручную настраивать сетевые параметры на каждом устройстве.
- Гибкость: легкое добавление и удаление устройств из сети.
- Эффективное использование адресного пространства: DHCP-сервер управляет пулом адресов, избегая конфликтов.
- Облегчение администрирования: централизованное управление сетевыми настройками.

В некоторых случаях может потребоваться отключить DHCP и настроить сетевые параметры вручную:

- Статические IP-адреса: Для серверов, принтеров и других устройств, которым требуется постоянный адрес.
- Безопасность: В сетях с высоким уровнем безопасности ручная настройка может снизить риски несанкционированного доступа.
- Особые настройки: При необходимости специфических сетевых конфигураций.

Применение DHCP особенно актуально в беспроводных общественных сетях, где администратор не может себе позволить брать у каждого гостя его мобильное устройство и назначать ему вручную параметры сетевого подключения.

Опробуем работу с DHCP при помощи Cisco Packet Tracer. Рассмотрим два примера. Пример первый:



1. Запускаем Cisco Packet Tracer.

2. Настроим маршрутизатор:

2.1. Подключение осуществляется к порту fastEthernet 0/1. Настройте интерфейс и присвойте IP адрес 192.168.1.1 255.255.255.0.

2.2. Создадим пространство IP адресов с помощью команд ip dhcp pool DHCP, network 192.168.1.0 255.255.255.0.

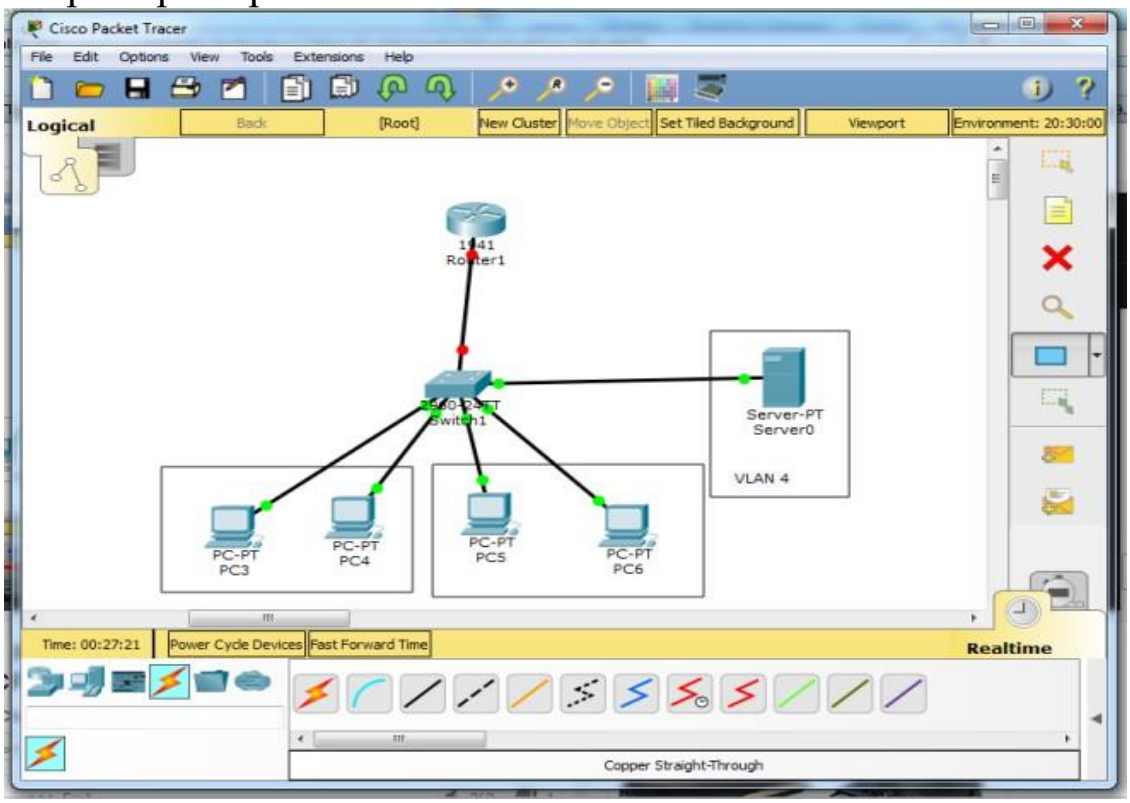
2.3. Выдаем компьютеру IP адрес и маршрут default-router 192.168.1.1, dns –server 0.0.0.0.

2.4. Исключим некоторые IP адреса и DHCP протокола (например, при подключении к сети сервера) с помощью команд ip dhcp excluded- adresses 192.168.1.99 и исключим IP адрес роутера ip dhcp excluded-adresses 192.168.1.1.

3. Настроим компьютеры. Ставим галочку на DHCP вместо Static. IP адрес присвоится автоматически.

4. Проверьте сеть.

Пример второй:



1. Настроим коммутатор.

1.1. Создайте VLAN 2,3 и 4.

1.2. Настройте порты, к которым подключены компьютеры.

1.3. Настройте порт, к которым подключен сервер.

1.4. Соединим все VLAN с маршрутизатором с помощью команд (в нашем случае порт fastEthernet 0/1) interface fastEthernet 0/1, switchport mode trunk, switchport trunk allowed vlan 2, 3, 4. Сохраните.

2. Настроим маршрутизатор:

2.1. Настройте порт и задайте IP адрес (например, с VLAN 2 IP адрес 192.168.2.1, с VLAN 3 IP адрес 192.168.3.1, с VLAN 4 IP адрес 192.168.4.1).

2.2. Проверьте.

3. Настроим DHCP сервер:

3.1. Зададим статический IP адрес 192.168.4.2 и шлюз 192.168.4.1.

3.2. Проверьте взаимодействие с маршрутизатором.

3.3. Перейдите во вкладку Config/DHCP. Создадим сервер с именем DHCPvlan2, IP адрес 192.168.2.0. Шлюз 192.168.2.1 и DNS Server 0.0.0.0.

Включаем его (On) и добавляем (Add); Аналогично создайте для VLAN 3.

4. Переадресуем запросы с компьютеров на DHCP сервер:

4.1. Заходим в настройки маршретизатора. С помощью команд interface gigabitEthernet 0/0.2, ip helper-adress 192.168.1.2. Аналогично выполните для VLAN 3. Сохраните.

5. Попробуйте получить IP адреса компьютеров (IP Configuration).

6. Проверьте взаимодействие.

Контрольные вопросы

1. Что такое DHCP?
2. Почему DHCP актуален для беспроводных сетей?
3. Опишите формат работы DHCP?
4. Какие настройки выдаёт DHCP?
5. Какими способами выполняется раздача адресов?

Технология WiFi

Цель работы: настроить беспроводной доступ доверенных конечных устройств в локальную сеть.

Wi-Fi передаёт данные от одного устройства к другому с помощью радиоволн в определённом частотном диапазоне – 2,4, 5 или 6 ГГц.

Для создания сети обычно используют роутеры или маршрутизаторы с беспроводными адаптерами. Их главное различие заключается в способе подключения к кабелю интернет-провайдера: роутер – напрямую, маршрутизатор – через модем.

На любом из этих устройств есть антенны для передачи сигнала. Они могут находиться внутри корпуса модема или маршрутизатора, а могут быть внешними. В последнем случае антенны можно направлять в сторону подключаемых устройств для улучшения сигнала.

На устройстве-получателе, например, ноутбуке или смартфоне, тоже есть антенна, которая обычно находится внутри корпуса. Её размер и форма зависят от конкретного гаджета.

Если говорить просто, то передача данных с помощью Wi-Fi работает следующим образом:

1. На антенны роутера или маршрутизатора подаётся ток, который используется для генерации радиоволн.

2. Здесь происходит модулирование сигнала. Это означает, что его характеристики, такие как амплитуда, частота или фаза, изменяются в соответствии с битами информации, которые требуется передать. Модуляция «упаковывает» передаваемые данные (набор нулей и единиц) в форму радиоволны, пригодную для беспроводной передачи.

3. На компьютере или другом гаджете приёмник демодулирует сигнал, переводя радиоволну в исходные данные, то есть в набор нулей и единиц, с которыми способны работать устройства.

Радиосигналы проходят через стены и другие преграды – это обеспечивает связь внутри помещений и на небольших расстояниях. Общая зона покрытия Wi-Fi – несколько десятков метров внутри зданий и около 100 метров у уличных точек доступа. Она зависит от

мощности роутера, диапазона частот и версии стандарта. Стены, мебель, металлические объекты и другие препятствия уменьшают зону покрытия.

Для беспроводной связи используются радиоволны в диапазоне частот 2,4, 5 и 6 ГГц. Внутри диапазона есть отдельные каналы для подключения:

- Для Wi-Fi с частотой 2,4 ГГц используется три непересекающихся канала с шириной 20 МГц каждый.
- Для частоты 5 ГГц используются 33 канала, 19 из которых не пересекаются. При этом каналы имеют ширину 40 МГц, то есть в два раза больше, чем у Wi-Fi с частотой 2,4.
- Для стандарта с частотой 6 ГГц используется уже 59 каналов различной ширины. В нём появляются 14 дополнительных каналов шириной 80 МГц и семь дополнительных каналов шириной 160 МГц.

Звучит сложно, но здесь работает простое правило: чем больше непересекающихся каналов и чем больше их ширина, тем меньше помех будет возникать из-за одновременной работы нескольких сетей. Поэтому в многоквартирных домах или в бизнес-центрах, где одновременно существуют десятки или сотни беспроводных сетей, лучше использовать Wi-Fi с частотой 5 ГГц, а не 2,4 ГГц. В последнем случае они будут пересекаться, снижая стабильность друг друга.

Для безопасности передачи данных по Wi-Fi используются различные методы шифрования, например WPA (Wi-Fi Protected Access) и WPA2. Это стандарты безопасности, которые защищают беспроводные сети от взлома.

Wi-Fi – основной протокол беспроводной связи, используемый в квартирах, офисах и на производственных объектах. Его широкое распространение связано с преимуществами стандарта:

1. При перемещении устройств в пространстве сохраняется стабильность соединения и высокая скорость передачи данных.

2. Одна беспроводная сеть может обслуживать несколько десятков устройств одновременно. Максимальное количество гаджетов зависит от стандарта Wi-Fi, типа роутера и пропускной способности сети.

3. Можно подключать к Wi-Fi разнообразные умные устройства и датчики, создать сеть для управления умным домом, медиацентром, системой безопасности и другими приложениями IoT.

4. Wi-Fi можно использовать для создания локальных беспроводных сетей. Устройства внутри дома или офиса смогут обмениваться данными между собой без проводов и подключаться к общим ресурсам: принтеру, сканеру и так далее.

5. Возможность настроить меш-сеть с несколькими маршрутизаторами. Она обеспечивает «бесшовное» подключение устройств к интернету даже в помещениях с большим количеством экранирующих объектов – например, с толстыми стенами или промышленным оборудованием.

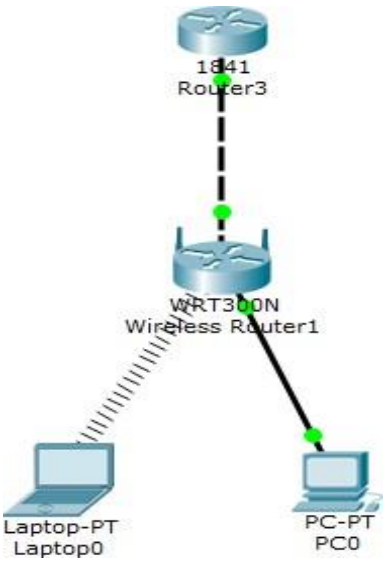
Но есть и минусы, которые стоит учитывать при работе с Wi-Fi:

1. Сигнал ограничен пределами определённой зоны покрытия. Как правило, в помещениях это 50–70 метров в зависимости от типа роутера или маршрутизатора. Стены, особенно железобетонные, массивная мебель и другие преграды ухудшают качество сигнала. Эту проблему можно решить с помощью репитеров и меш-сетей, но это требует дополнительных затрат.

2. На стабильность соединения влияют электромагнитные помехи от других беспроводных гаджетов и электроники. Их создают, например, флуоресцентные лампы, электронагреватели или вентиляторы. То же самое делают микроволновые печи, беспроводные телефоны, Bluetooth, охранные и беспроводные системы и другие устройства, использующие тот же частотный диапазон, что и у Wi-Fi, — 2.4 ГГц. Решение — использовать сеть с частотой 5 ГГц.

3. Один и тот же канал могут использовать сети, расположенные рядом, что приводит к его перегрузке. Снижается стабильность соединения и скорость передачи данных. Это стоит учитывать при расположении квартиры или офиса в плотно населённых районах или местах с высокой концентрацией беспроводных устройств. Справиться с перегрузкой канала поможет использование сетей с частотным диапазоном 5 ГГц, так как в них больше каналов с большей шириной, которые не перекрываются друг другом.

Рассмотрим пример WiFi роутера в Cisco Packet Tracer:



1. На интерфейсе Router3 настройте IP адрес 210.210. 0.1.

2. Настроим WiFi Router1:

2.1. Во вкладке GUI настроем IP адрес, используя Static IP 210.210.0.2, 255.255.255.255.252, маршрутом будет 210.210.0.1.

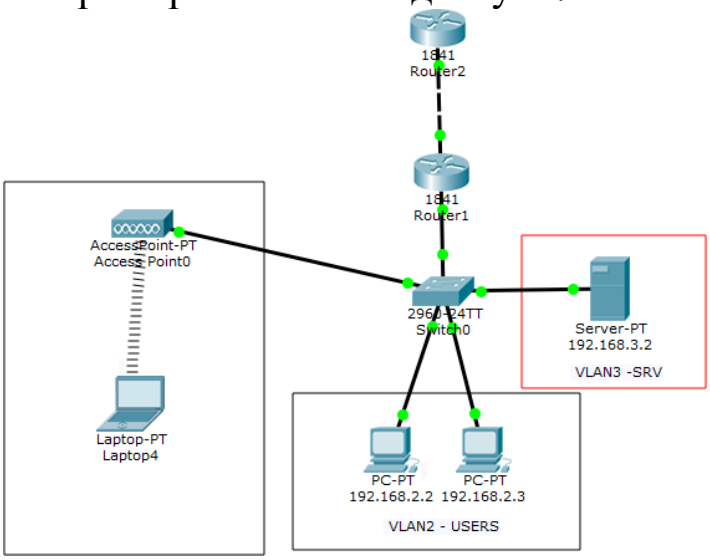
2.2. Во вкладке Wireless можно выбрать настройки WiFi.

2.3. Во вкладке Wireless Security можно выбрать режим, выбрать режим шифрования и задать ключевое слово. Сохраните.

3. Настроим ноутбук. Wireless, вкладка Desktop, вкладка Connect, где видим доступные сети. Подключитесь к созданному нами WiFi и введите пароль. На рисунке видно, что подключение успешное (пунктирная линия). Проверьте выход в интернет.

4. В настройках компьютера проверьте IP адрес, выход в интернет и доступность ноутбука.

Рассмотрим пример WiFi точка доступа:



1. Настройте порты на коммутаторе Switch0 в соответствующие VLAN.

2. На Router1 настройте интерфейс на подключение к интернет провайдеру, настройте sub интерфейсы, которые соответствуют VLAN 2 и 3, настройте NAT.

3. Проверьте сеть.

4. Настроим точку доступа, вкладка Config, вкладка Port 1, задайте идентификатор сети, тип аутентификации и задайте пароль.

5. Пусть WiFi сегмент будет во VLAN 4. Создайте VLAN 4 и настройте интерфейс в Switch0.

6. Создайте sub интерфейсы на Router1 и добавьте IP адрес 192.168.4.1 255.255.255.0.

7. Настроим раздачу IP адресов пользователям на Router1:

7.1. Создадим ip dhcp pool WiFi-pool, network 192.168.4.0. 255.255.255.0, default router 192.168.4.1;

7.2. Необходимо исключить IP адрес маршрутизатора из DHCP с помощью команды ip dhsp excluded-addresses 192.168.4.1.

7.3. Настроим NAT, отредактировав созданный access list - ip access- list standard FOR-NAT, permit 192.168.4.0 0.0.0.255.

7.4. В нашем случае fa0/1.4 определим как ip nat inside. Сохраните.

8. Настроим ноутбук аналогично предыдущей схеме с маршрутизатором и определим точку доступа в VLAN 4 на маршрутизаторе с помощью команд swichport mode access, switchport access vlan 4 description WiFi-AP.

9. Проверьте работоспособность сети

Контрольные вопросы

1. Какие частотные диапазоны использует WiFi?
2. Что является носителем сигнала в WiFi?
3. Опишите передачу данных при помощи WiFi.
4. Назовите достоинства и недостатки технологии.
5. Приведите примеры методов шифрования в WiFi.

Практические занятия

Монтаж кабеля для подключения устройств к WiFi-роутеру на основе витой пары

Цель работы: подготовить кабель на основе витой пары к эксплуатации в компьютерных сетях.

Для кого-то будет открытием, что по кабелю передаются не биты и байты, хотя технику мы называем цифровой. На самом деле, в проводе нет никакой информации, а только напряжение. Один компьютер задает вопрос, другой отвечает, и все это происходит с помощью передачи вольтажа через витые пары.

Для передачи информации компьютер делит ее на биты. Затем они шифруются в двоичную систему и передаются по кабелю. В это время информация выглядит как простые электрические импульсы разной длительности (частоты) и с разным вольтажом. При этом, передаются два сигнала: один с положительным напряжением, другой – с отрицательным. Принимая сигнал, дешифратор складывает напряжения и в сумме получает ноль. Таким образом, зная вольтаж, длительность импульса и разницу напряжений, сетевая карта понимает, какой код ей посылает собеседница.

Кабель витой пары применяется для передачи цифрового сигнала в IP-сетях, телекоммуникациях, системах видеонаблюдения. Скрученные попарно жилы обеспечивают дополнительную защиту данных от электромагнитных помех и перекрёстных наводок.

Различают два типа витых пар в структурированных сетях – FTP и UTP. Разберем особенности, преимущества и недостатки каждого типа, чтобы помочь вам сделать выбор.

Foiled Twisted Pair (FTP) – это кабель с фольгированным экраном, применяемый в условиях с сильными помехами. Он особенно актуален в промышленности, на объектах с повышенным электромагнитным фоном и при высоких требованиях к скорости передачи данных.

Экранирование уменьшает затухание сигнала и защищает его от искажений. Существует несколько вариантов конструкции:

- U – экранирование каждой пары;

- F – фольга вокруг каждой пары и общий экран;

- S – общая оплётка и фольга на каждой паре.

Важно обеспечить надёжное заземление через коннекторы или патч-панели, чтобы сохранить эффективность защиты.

FTP чаще всего используется в категориях 6, 7 и 8 — для высокочастотных сигналов и скорости передачи до 40 Гбит/с.

Преимущества:

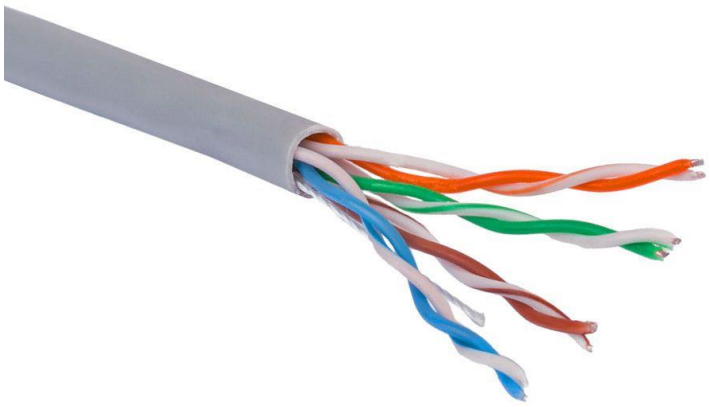
- высокая степень защиты;
- поддержка частот до 2000 МГц;
- стабильная работа в сложных условиях;
- подходит для сетей защиты и промышленных объектов.

Недостатки:

- высокая стоимость;

- меньшая гибкость;
- чувствительность к повреждениям;
- необходимость соблюдения условий монтажа.

Unshielded Twisted Pair – это неэкранированный кабель, который часто применяется в жилых и офисных помещениях. Его используют при организации Ethernet-сетей внутри зданий, видеонаблюдения и связи.



Из-за отсутствия экрана он более подвержен внешним помехам и ограничен по дальности и частоте сигнала. Обычно встречается в категориях от 1 до 5.

Преимущества:

- низкая цена;
- простота установки;
- высокая гибкость;
- небольшой вес.

Недостатки:

- отсутствие экранирования;
- меньшая устойчивость к помехам;
- ограниченные технические характеристики.

FTP или UTP? Выбор зависит от условий эксплуатации. При сильных помехах и высоких скоростях лучше использовать FTP. Если задача не требует высокой защиты и важна экономия, подойдёт UTP.

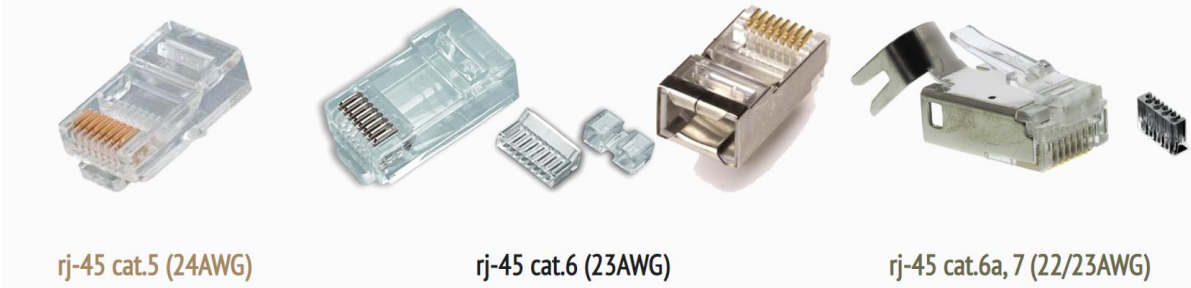
Витая пара бывает одножильная и многожильная. Провод с цельными жилами подходит для разводки сети по стенам, в кабель-каналах или для организации длинных трасс. Физические и электрические свойства цельного медного провода лучше, чем у много-

жилки. В основном это прочность и помехоустойчивость. Многожильный провод применяется для сборки заводских патч-кордов. Его свойств достаточно для передачи информации между устройствами на небольшом (до 5 м) расстоянии. Он хорошо принимает форму и устойчив к изломам.

Несмотря на стандарты в Cat. 5e, производители могут выпускать провода с **двумя парами** вместо четырех. Количество пар играет роль в сетях со скоростью выше 100 Мбит/с. Учитываем этот момент и берем полноценный кабель со всеми парами, чтобы потом спокойно переключиться на высокоскоростной тариф, подключить видеонаблюдение и смотреть фильмы в 4К без проблем с пропускной способностью.

Качественная витая пара должна защищаться толстой, но мягкой оболочкой. Тогда провод будет легче свернуть, направить в кабель-канале, а еще он не перетрется и будет уверенно держаться в клипсе сетевого разъема. Хорошая изоляция — это также защита от потери сигнала на больших расстояниях, где полимерное покрытие проводника работает как электромагнитный диэлектрик.

Registered Jack — стандартизированный разъем. Как и витая пара, коннектор имеет разные категории и уровни качества.



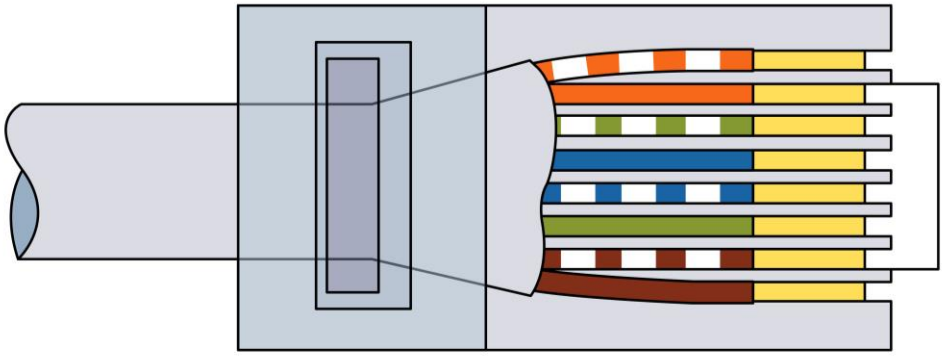
Для каждого типа витой пары применяется свой разъем. Для проводов **Cat. 5** и **5e** используют первый вариант (см. изображение выше). Он знаком каждому пользователю и способен переварить толщину проводников до 24 AWG. Более ничем не примечателен.

`Для построения экранированных сетей используется джек **Cat. 6**. Он может зажимать провода до 23 AWG, а также имеет металлический корпус, который соединяется с фольгой в проводе и создает единый помехоустойчивый контур между устройствами.

Соответственно, для проводов высших категорий есть другие коннекторы. Но это серверный уровень и домашний пользователь вряд ли столкнется даже с коннекторами типа **6а**.

Пригодность разъема для разного типа проводов диктуется не только размерами клипсы, что удерживает провод в разъеме, но и типами ножей, которые пробивают оболочку каждого провода в паре и соединяются с медью. А еще качеством позолоты контактов.

Для приема и передачи данных в проводе используется два способа расположения витых пар в коннекторах. Это прямой и перекрестный обжим. Для современных сетевых устройств нет разницы в распиновке, потому что устройства умеют делать это автоматически на уровне разъема. Поэтому в основном используется прямой обжим и соответствующая ему распиновка пар:



В соединениях до 100 Мбит/с данные передаются только двумя парами: одна занимается отправкой сигнала (называют TX), другая приемом (RX). То есть, Transfer и Receive. Причем в каждой паре оба провода работают в одном направлении. Только по одному бежит положительное напряжение, а в другом — отрицательное. Это мы разобрали в начале статьи. Остальные пары задействуются под нужды PoE (подключение IP-камер), телевидения или телефонии. Для работы высокоскоростных линий задействуют все четыре пары.

Провода обозначают стандартными цветами, где каждая пара имеет свой основной цвет. Это сделано для удобства, так как прозванивать восемь одноликих проводов при каждом обжиме —занятие утомительное. Физической разницы между парами нет, главное, чтобы провод был обжат одинаково с обоих концов.

По проводу передаются электрические импульсы с высокой частотой. В самом начале эти импульсы сильные и отчетливые, а к

концу провода их амплитуда снижается. Это называется затуханием сигнала или «вносимыми потерями». Отношение силы выходного сигнала в начале провода к силе входного сигнала в конце измеряют в децибелах. Чем выше разница, тем хуже качество сигнала. Обычно сигнал портится на больших расстояниях, если спецификации витой пары не соответствуют заявленным или нарушаются правила построения сетей. Немалую роль в качестве сигнала играет материал проводников, их правильный обжим в коннекторе, а также защита от собственных и внешних наводок.

Как сократить потери сигнала на длинных трассах:

- Использовать провод с медными парами большого диаметра (AWG 22-23);
- Подобрать провод с толстой оболочкой, которая обладает лучшими диэлектрическими свойствами;
- Использовать провода из серебра (да, такое тоже бывает);
- Включить в трассу усилитель сигнала.

То есть, если нужно передать сигнал на очень большое расстояние, то без репитера это не получится. Принцип работы такой же, как и у повторителя для WiFi: берется редуцированный сигнал, преобразуется в исходный по мощности и отправляется следующей станции или адресату. Для этого есть специальные устройства — экстендеры Ethernet. Или роутер (он же свитч). То есть, если сигнал тухнет через каждые 100 метров, то можно переподключать линию на свитчах и передавать сигнал дальше. Но это в теории.

На практике сигнал в витой паре перемешивается с различными помехами. Это сигналы сотовой сети, радиосигнал роутера, высокочастотные волны от микроволновой печи и даже низкочастотный шум от двигателя автомобиля. Помимо этих явлений есть и внутренние, когда одна пара вносит паразитные сигналы в другую пару и возникают перекрестные помехи.

От внешних воздействий на сигнал провод защищают алюминиевой фольгой. В зависимости от типа и категории провода, такая фольга может защищать каждую пару отдельно или весь провод целиком. Для защиты от сильных помех также используют металлическую оплетку.

Порядок обжима витой пары

Для того, чтобы обжать витую пару, необходимо срезать внешнюю изоляцию примерно на 1 см – обычно этого достаточно, чтобы

довести её провода до конца коннектора, и при этом внешняя изоляция частично входила в коннектор, защищая провода от повреждений о края коннектора.

Всю работу можно сделать при помощи специальных обжимных клещей, которые имеют не только гнёзда для непосредственно обжатия коннекторов, но и специальные лезвия для работы с проводами.

После того, как провода будут освобождены от внешней изоляции, их необходимо расплести, выровнять и расположить в ряд в соответствии с приведенной выше распиновкой. Собственную изоляцию проводов резать не нужно – медные контакты, торчащие из кончика коннектора, выполнены в виде зубчатых ножей, которые при обжатии сами прорежут изоляцию проводов и установят физический контакт с медными жилками.

Удерживая провода в построенном в ряд состоянии одной рукой, вставьте их в коннектор. Если вы перед этим свели провода максимально плотно друг к другу, то они должны свободно войти в предназначенные им дорожки коннектора. Убедитесь, что все провода достали до конца коннектора.

Пока вы не сделали обжатие, то есть не продавили контакты внутрь коннектора, провода ещё можно вытащить, если какой-то провод оказался не в своей дорожке. Внимательно проверьте ещё раз соответствие распиновке. Если всё верно, вставляйте коннектор в соответствующее гнездо обжимных клещей до установленного с одной стороны упора, после чего резко сжимайте клещи до конца. После этого можно вынимать коннектор и проверить, не выпадают ли провода из него? Если провода держатся крепко, и все контакты провалились внутрь, обжатие состоялось.

Чтобы проверить работоспособность провода, его нужно обжать и с другой стороны. При этом необходимо определить правую и левую сторону коннектора, так как теперь будет иметь значение, с какой стороны будет находиться оранжевая пара, с какой коричневая – должно быть одинаково на обоих концах.

Когда провод обжат с обеих сторон, его работоспособность можно проверить специальным LAN-тестером

Тестер последовательно «прозвонит» каждый провод витой пары, в результате чего на обеих секциях индикаторы должны загореться так же последовательно. Если какой-то индикатор на приёмнике не загорелся, значит, физический контакт отсутствует в одном из коннекторов. Если индикаторы загораются одновременно, значит, между соответствующими проводами короткое замыкание. Если порядок загорания нарушен, значит, нарушена распиновка в одном из коннекторов. Во всех трёх случаях провод можно забраковывать. Для этого дефектный коннектор придётся отрезать и обжимать заново.

Задание: получить у преподавателя витую пару, коннекторы, обжимные клещи и LAN-тестер, подготовить провод к эксплуатации и проверить его работоспособность.

Контрольные вопросы

1. Почему провода витой пары попарно скручены?
2. Почему в настоящее для обжима практически всегда подходит прямая схема?
3. Какие вы знаете коннекторы для витой пары?
4. Каковы преимущества и недостатки экранированной витой пары?
5. Какие вы знаете знаки признаки ошибок обжима витой пары, в результате которых провод можно считать непригодным?

Статическая маршрутизация в IP-сетях

Цель работы: освоить построение таблицы маршрутизации.

В процессе организации межсетевого взаимодействия важное место занимает маршрутизация сообщений между отдельными подсетями. При этом под маршрутизацией понимается процесс доставки сообщения из одной подсети в другую. Данная задача может решаться различными способами. При этом, чем сложнее рассматриваемая система, чем больше подсетей ее образуют, тем более нетривиальным является решение задачи доставки сообщений.

Сетевой компонент, выполняющий маршрутизацию пакетов, называется маршрутизатором (**router**). Маршрутизатор может быть реализован на базе компьютера с несколькими сетевыми интерфейсами, на котором установлено специальное программное обеспечение. В этом случае говорят о программном маршрутизаторе. В другом случае маршрутизатор может быть выполнен в виде отдельного сетевого устройства. Разумеется, наиболее эффективным решением является использование специальных аппаратных маршрутизаторов.

В настоящее время лидером на рынке корпоративных маршрутизаторов является компания **Cisco**, предлагающая высокопроизводительные и надежные устройства. В небольших сетях (таких как сеть небольшого офиса или домашняя сеть), использование аппаратного маршрутизатора может быть экономически необоснованно.

Системы Windows Server включают в себя механизмы, позволяющие серверу, находящемуся под ее управлением, выступать в качестве программного маршрутизатора. Эти механизмы реализованы в составе Службы маршрутизации и удаленного доступа (**Routing and Remote Access Service**, RRAS).

Хотя в архитектуре Windows Server основной упор делается на стек протоколов TCP/IP, в состав указанной службы также включена поддержка механизмов маршрутизации стека протоколов **AppleTalk**.

Реализованный в Windows Server механизм маршрутизации может с успехом использоваться для организации межсетевого взаимодействия в вычислительных сетях любого масштаба (в том числе и

для интеграции корпоративной сети в Интернет), а также для организации виртуальных частных сетей (**Virtual Private Network**, VPN).

В межсетевой среде каждая подсеть может быть соединена с произвольным количеством других подсетей посредством маршрутизаторов. Суть процесса маршрутизации сводится к тому, что два хоста, разделенных друг с другом любым произвольным количеством маршрутизаторов (другими словами, находящиеся в разных подсетях), могут взаимодействовать друг с другом.

Всю организацию процесса доставки пакета от одного хоста другому берут на себя маршрутизаторы. Рассмотрим основные принципы, лежащие в основе процесса маршрутизации сообщений.

Сразу оговоримся, что разговор будет идти, прежде всего, о маршрутизации IP-трафика. Подавляющее большинство сетевых служб Windows Server функционирует на базе стека протоколов TCP/IP, получившего широкое распространение именно благодаря простоте организации межсетевого взаимодействия (как известно, самое большое объединение сетей – Интернет, тоже основывается на этом стеке протоколов). Тем не менее, заметим, что в своей основе принципы маршрутизации являются общими для большинства стеков протоколов.

В зависимости от количества вовлеченных получателей стек протоколов TCP/IP поддерживает два способа маршрутизации: одноадресная и многоадресная маршрутизация.

Под одноадресной маршрутизацией понимается процесс передачи сообщений между подсетями, в котором сообщение адресовано только одному заданному получателю. Вся задача маршрутизации в этом случае сводится к доставке пакета получателю и выбору оптимального маршрута из множества возможных.

Понятие таблицы маршрутизации

Отправителя и получателя может разделять произвольное количество маршрутизаторов. При этом процесс передачи сообщения от одного маршрутизатора другому называется "прыжком" (**hop**). Каждый маршрутизатор обладает информацией о структуре сети на расстоянии одного прыжка. Другими словами, маршрутизатор не обладает информацией о точном местоположении требуемого хоста.

В большой сети, да еще и с интенсивно меняющейся структурой (как, например, Интернет), это было бы невозможно. Вместо

этого, маршрутизатор обладает информацией о соседних маршрутизаторах и о том, кому из них необходимо передать сообщение для последующей доставки в той или иной ситуации. Эта информация хранится в специальной таблице, которая носит название таблицы маршрутизации (**routing table**).

Таблицы маршрутизации используются для принятия решения о том, как именно будет доставлено то или иное сообщение. Наличие этих таблиц не является исключительным свойством маршрутизатора. В сети TCP/IP любой хост (даже не являющийся маршрутизатором) может также располагать таблицей маршрутизации, которая используется с целью определения оптимального маршрута передачи сообщений. Так, скажем, если в подсети имеется три маршрутизатора, хост использует таблицу маршрутизации для того, чтобы выбрать из них наиболее оптимальный для доставки сообщения.

Типы записей в таблице маршрутизации

Записи в таблице маршрутизации называются маршрутами. При этом существует три типа маршрутов.

- **Маршрут к хосту, или узловой маршрут** (Host Route). Этот тип маршрута определяет путь доставки пакета, адресованного хосту с конкретным сетевым адресом. Маршруты к хостам обычно используются для создания настраиваемых маршрутов к определенным компьютерам, а также для управления или оптимизации сетевого трафика.
- **Маршрут к сети, или сетевой маршрут** (Network Route). Данный тип маршрута используется для определения способа доставки пакета в подсеть с определенным адресом. Большую часть содержимого таблицы маршрутизации представляют собой маршруты данного типа.
- **Маршрут по умолчанию** (Default Route). Маршрут по умолчанию используется, когда не найдены никакие другие маршруты в таблице маршрутизации. Маршрут по умолчанию используется в ситуации, когда в таблице маршрутизации отсутствует соответствующий маршрут по идентификатору сети или маршрут к хосту по адресу получателя. Маршрут по умолчанию упрощает конфигурацию компьютеров. Вместо конфигурирования компьютера и настройки маршрутов для всех идентификаторов сетей в межсетевой

среде используется одиночный маршрут по умолчанию для пересылки всех пакетов в сеть получателя или по адресу в межсетевой среде, который не был найден в таблице маршрутизации.

Рассмотрим структуру таблицы маршрутизации на следующем примере:

Сеть назначения	**Маска подсети**	**Шлюз**	**Интерфейс**	**Метрика**
0.0.0.0	0.0.0.0	0.0.0.0	fffffffff	1
10.0.0.0	255.255.255.0	10.0.0.1	10.0.0.1	30
10.0.0.1	255.255.255.255	127.0.0.1	127.0.0.1	30
10.255.255.255	255.255.255.255	10.0.0.1	10.0.0.1	30
127.0.0.0	255.0.0.0	127.0.0.1	127.0.0.1	1
224.0.0.0	240.0.0.0	10.0.0.1	10.0.0.1	30
255.255.255.255	255.255.255.255	10.0.0.1	10.0.0.1	1

Каждая запись в таблице маршрутизации (представляющая собой информацию о маршруте) состоит из информационных полей, перечисленных ниже.

- **Сеть назначения** (Network Destination). Данное поле содержит сведения об адресе хоста-получателя пакета или сети, в которой этот хост располагается. Принимая решение о маршрутизации пакета, система просматривает именно это поле. Если в данном поле не будет найдено записи о конкретном адресе сети или хоста, маршрутизатором будет использован маршрут по умолчанию, который обычно отмечается адресом 0.0.0.0.
- **Маска подсети** (Netmask). Это поле в сочетании с предыдущим полем используется для вычисления идентификатора IP-сети.
- **Шлюз** (Gateway). В этом поле указывается адрес, по которому будет должен быть передан согласно данному маршруту. Адрес пересылки может быть аппаратным адресом или адресом в межсетевой среде. В большинстве случаев в этом поле указывается следующий в цепочке маршрутизатор, который должен будет принять решение о дальнейшей маршрутизации сообщения.
- **Интерфейс** (Interface). В этом поле указывается сетевой интерфейс, с которого будет осуществляться передача сообщения согласно данному маршруту. Данное поле необходимо в ситуации,

когда маршрутизатор имеет множество сетевых интерфейсов, подключенных к разным подсетям. Фактически данное поле указывает, в какую именно подсеть необходимо передать сообщение.

- **Метрика** (Metric). Стоимость маршрута, характеризующая меру его предпочтения. Из множества альтернативных маршрутов будет выбран тот, что обладает наименьшей стоимостью (т. е. меньшим значением метрики). Некоторые алгоритмы маршрутизации сохраняют только один маршрут для любого идентификатора сети в таблице маршрутизации, даже когда существует несколько маршрутов. В этом случае метрика используется маршрутизатором, чтобы определить какой именно маршрут необходимо сохранить в таблице маршрутизации.

В зависимости от способа формирования содержимого таблицы маршрутизации различают два вида маршрутизации.

Статическая маршрутизация

Все маршруты прописываются и изменяются администратором системы вручную. Это самый простой способ организации маршрутизации. Однако он подходит только для небольших сетей, изменения в структуре которых происходят достаточно редко. Кроме того, данный способ маршрутизации не годится в случае, когда важно обеспечить высокую надежность межсетевого взаимодействия.

Если один из маршрутов окажется по каким-либо причинам недоступен, администратору необходимо будет вручную изменить таблицу маршрутизации на всех маршрутизаторах в сети. До этого момента межсетевое взаимодействие на отдельных участках сети будет невозможно.

Динамическая маршрутизация

Построение таблицы маршрутизации осуществляется посредством специальных протоколов маршрутизации. Участие администратора в этом процессе минимально и сводится к изначальной конфигурации маршрутизаторов. Два наиболее распространенных протокола IP-маршрутизации, используемых в интрасетях, – протоколы **RIP** (Routing Information Protocol) и **OSPF** (Open Shortest Path First).

Посредством указанных протоколов маршрутизаторы способны информировать друг друга об изменениях в структуре сети. В

случае недоступности одного из маршрутов, маршрутизаторы автоматически перестроят свои таблицы маршрутизации и, при возможности, выберут другой маршрут доставки сообщений.

Статическая маршрутизируемая IP-сеть не использует протоколы маршрутизации, поскольку вся информация о маршрутизации хранится в статической таблице на каждом маршрутизаторе. Чтобы любые два произвольных хоста в сети могли взаимодействовать между собой, каждый маршрутизатор должен иметь такую таблицу маршрутов.

Статическая маршрутизируемая IP-среда лучше всего подходит для небольшой сети с редко изменяющейся структурой, в которой отсутствуют альтернативные маршруты. Статическая маршрутизируемая среда может применяться для:

- сети малого предприятия;
- сети домашнего офиса;
- филиала с одной сетью.

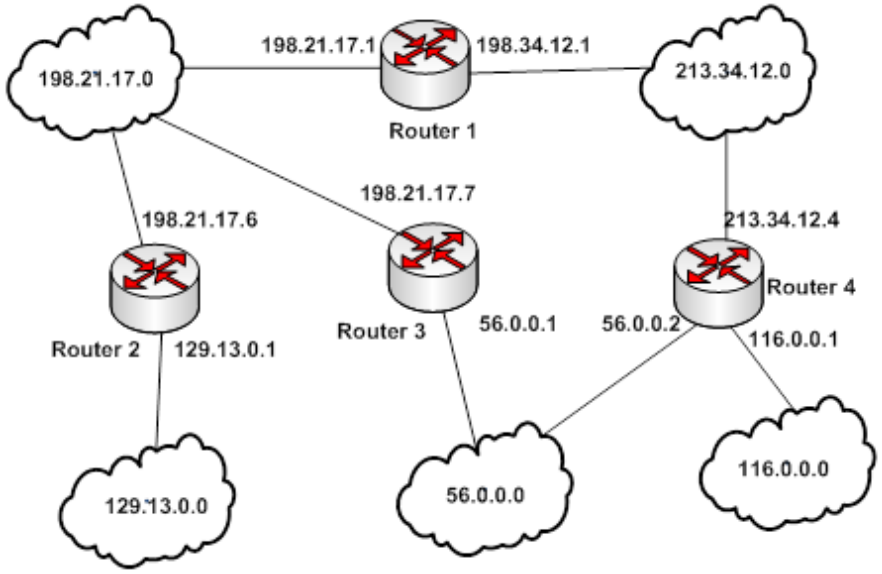
Вместо реализации протокола маршрутизации через узкополосный канал связи, одиночный маршрут по умолчанию на маршрутизаторе филиала гарантирует, что весь трафик, не предназначенный для компьютера в сети филиала, будет направлен в основной офис.

Недостатки статической маршрутизации:

- **Отсутствие отказоустойчивости**. Если в силу каких-либо причин один из маршрутизаторов выходит из строя или становится недоступным коммуникационный канал, статический маршрутизатор не сможет как-то отреагировать на неисправность. Более того, другие маршрутизаторы в сети не будут знать о неисправности и будут продолжать передавать данные по недоступному маршруту. В сетях малого офиса (например, с двумя маршрутизаторами и тремя сетями, соединенными в ЛВС) подобные ситуации могут решаться администратором оперативно. В крупных сетях более предпочтительным оказывается использование специальных протоколов маршрутизации;
- **Непроизводительные административные затраты**. Если добавляется новая подсеть или удаляется из межсетевой среды существующая, маршруты к ней должны быть вручную добавлены или удалены. Если добавляется новый маршрутизатор, то он должен быть правильно сконфигурирован для маршрутизации в межсетевой среде.

Пример построения таблицы маршрутизации

Рассмотрим структуру компьютерной сети, состоящей из 5 подсетей и 4 маршрутизаторов:



Каждая подсеть имеет свой адрес. Маршрутизаторы 1, 2 и 3 имеют подключения к двум подсетям каждый, маршрутизатор 4 подключен к трём подсетям. Рассмотрим маршрутизатор 2. У него задействованы два сетевых интерфейса, имеющие адреса 129.13.0.1 и 198.21.17.6. Как нетрудно заметить по рисунку, первый из них входит в диапазон адресов сети 129.13.0.0, с которой маршрутизатор соединён через этот интерфейс, а второй – в диапазон сети 198.21.17.0. К этим двум подсетям маршрутизатор подключен напрямую, поэтому для них ему не требуется никакой шлюз, поэтому соответствующее поле будет пустым, а вместо метрики будет установлено «Подключен».

В сеть 213.34.12.0 маршрутизатор 2 может послать пакет только через другие маршрутизаторы. Кратчайшим будет путь через маршрутизатор 1. Отправку в этом случае необходимо выполнить с интерфейса 198.21.17.6, и послать на тот интерфейс маршрутизатора 1, которым он подключен к общей с маршрутизатором 2 подсети 198.21.17.0. Поэтому адрес шлюза будет 198.21.17.1, а метрика равна 1, то есть достаточно пройти один маршрутизатор.

Аналогично выбираются интерфейсы и шлюзы для подсетей 56.0.0.0 и 116.0.0.0. Обратите внимание, что маршрутизатор может передать пакет для дальнейшей пересылки только своим соседям, с которыми он подключен к одной подсети – это маршрутизаторы 1 и 3. Поэтому в данном случае есть только 2 варианта адреса шлюза –

198.21.17.1 и 198.21.17.7. В результате получится следующая таблица:

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

Одношаговая маршрутизация обладает еще одним преимуществом – она позволяет сократить объем таблиц маршрутизации в конечных узлах и маршрутизаторах за счет использования в качестве номера сети назначения так называемого маршрута по умолчанию – default (0.0.0.0), который обычно занимает в таблице маршрутизации последнюю строку. Если в таблице маршрутизации есть такая запись, то все пакеты с номерами сетей, которые отсутствуют в таблице маршрутизации, передаются маршрутизатору, указанному в строке default. В нашем случае им назначен маршрутизатор 3, которому принадлежит интерфейс 198.21.17.7. Поэтому маршрутизаторы часто хранят в своих таблицах ограниченную информацию о сетях интерсети, пересылая пакеты для остальных сетей в порт и маршрутизатор, используемые по умолчанию. Подразумевается, что маршрутизатор, используемый по умолчанию, передаст пакет на магистральную сеть, а маршрутизаторы, подключенные к магистрали, имеют полную информацию о составе интерсети.

Задание: составить таблицу маршрутизации для заданных топологий корпоративной сети. Рисунок и маршрутизатор, для которого необходимо составить таблицу, определяется вариантом задания.

Вариант	Рисунок	Номер маршрутизатора
1	1	1
2	1	2
3	1	3
4	1	4
5	1	5
6	2	1
7	2	2
8	2	3
9	2	4

10	2	5
11	2	6
12	2	7
13	3	4
14	3	3
15	3	1

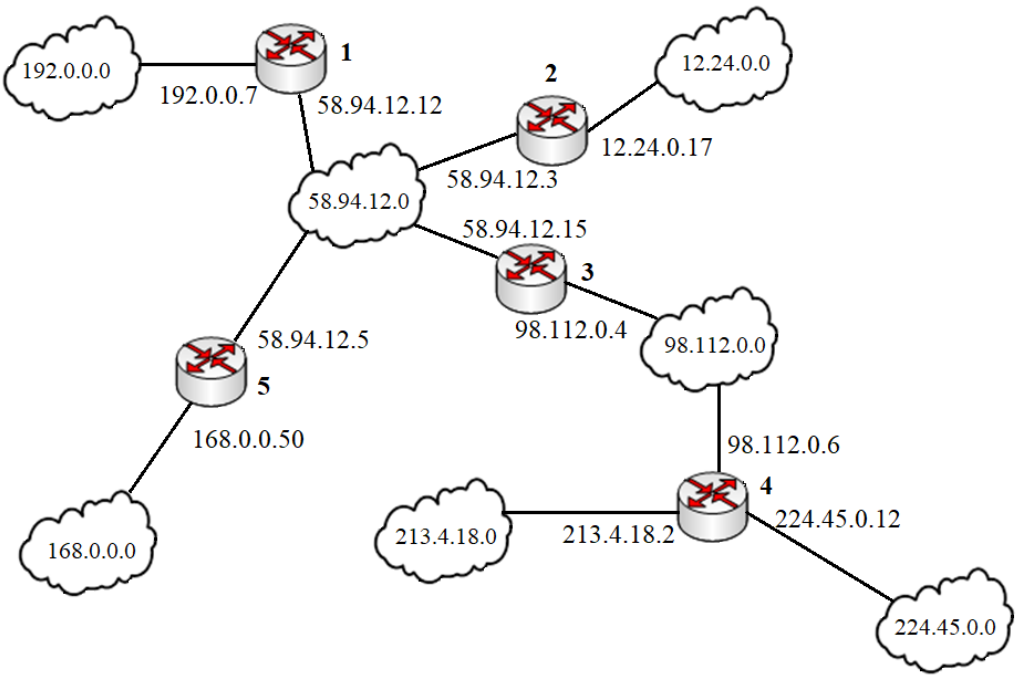


Рисунок 1

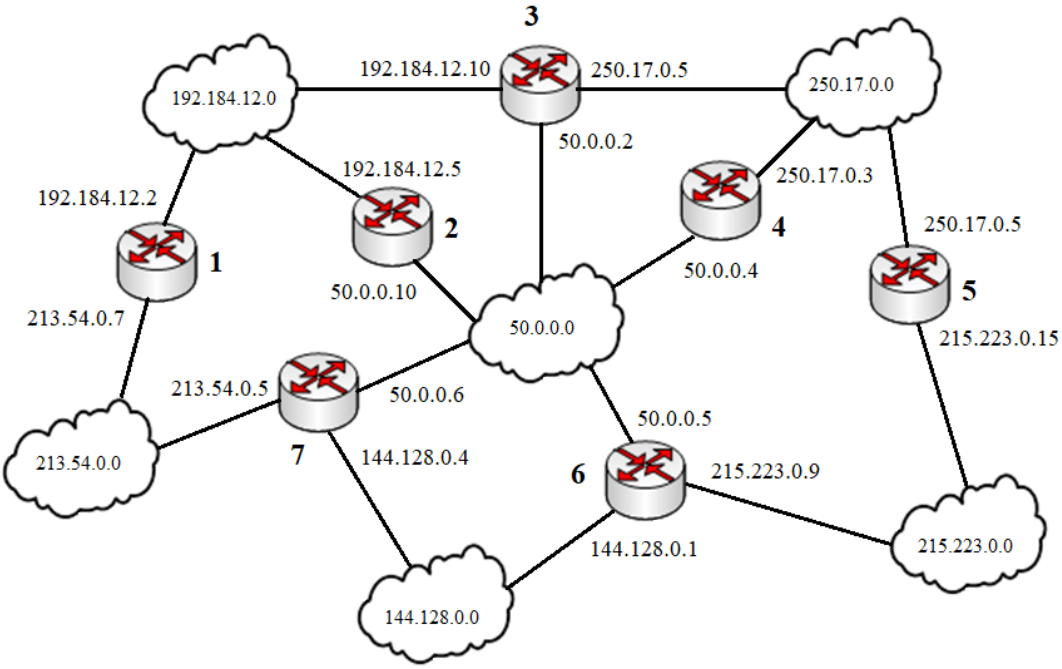


Рисунок 2

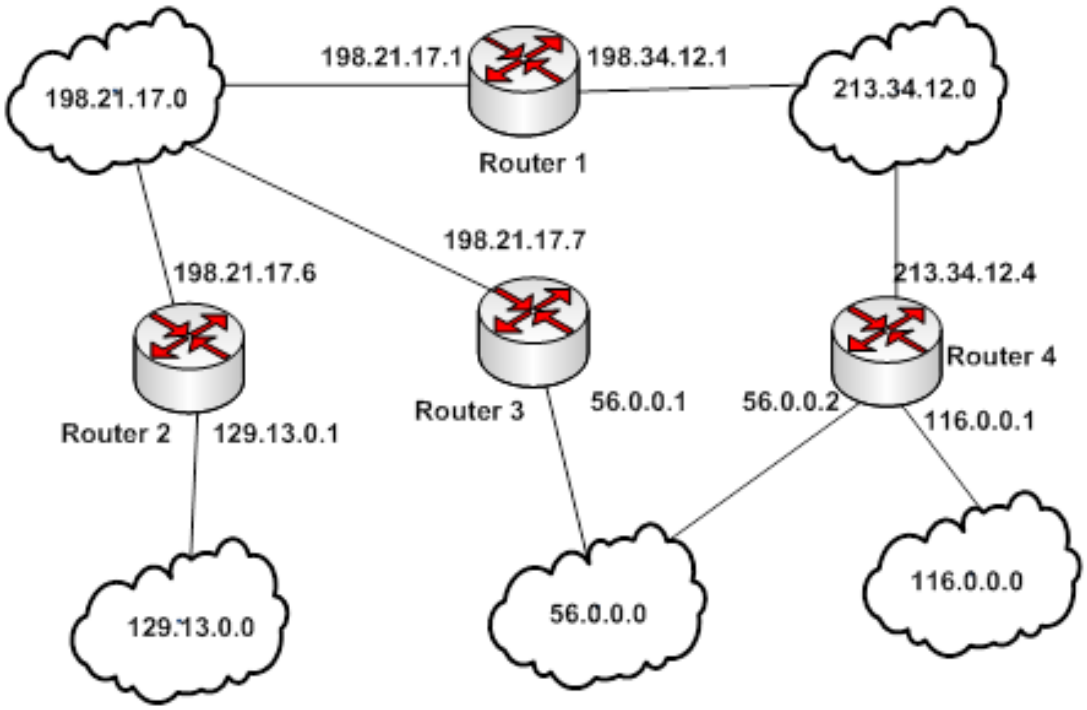


Рисунок 3

Контрольные вопросы

1. Что такое маршрутизация?
2. Чем отличается статическая маршрутизация и от динамической?
3. Поясните физический смысл записи в таблице маршрутизации?
4. Что такое интерфейс в таблице маршрутизации?
5. Что такое адрес шлюза в таблице маршрутизации?
6. Что такое метрика в таблице маршрутизации?

Составление технико-экономического обоснования построения локальной сети предприятия

Цель работы: научиться планировать прокладку сетевой инфраструктуры широкополосного доступа с серверной комнатой по архитектурному плану помещений.

В организациях чаще всего локальные сети прокладываются по проводной технологии с подключением инфраструктуры к магистральным сетям с целью обеспечения широкополосного доступа в Интернет и применением беспроводных технологий.

Для соединения компьютеров в сеть в рамках одного помещения, как правило, используется звездообразная топология сети, предполагающая наличие центрального устройства – коммутатора, к которому подключаются рабочие станции при помощи витой пары.

Подсеть каждого помещения может быть подключена к общему маршрутизатору. Провода при этом для поддержания порядка обычно укладываются в кабельные каналы, которые могут содержаться в плинтусах, либо быть монтированы на стенах. Патч-корды рабочих станций могут подключаться не напрямую к коммутатору, а через специальные розетки, от которых прокладываются провода к центральному устройству.

При проектировании стоит учитывать, что активное сетевое оборудование сейчас, как правило, представляет собой многофункциональные устройства, которые официально называются маршрутизаторами, но могут работать также и коммутаторами, шлюзами, сетевыми экранами и DHCP-серверами, при этом функцию шлюза устройство выполняет, поскольку обладает электромагнитным излучателем и антенной, что позволяет реализовать беспроводное подключение мобильных устройств по технологии WiFi.

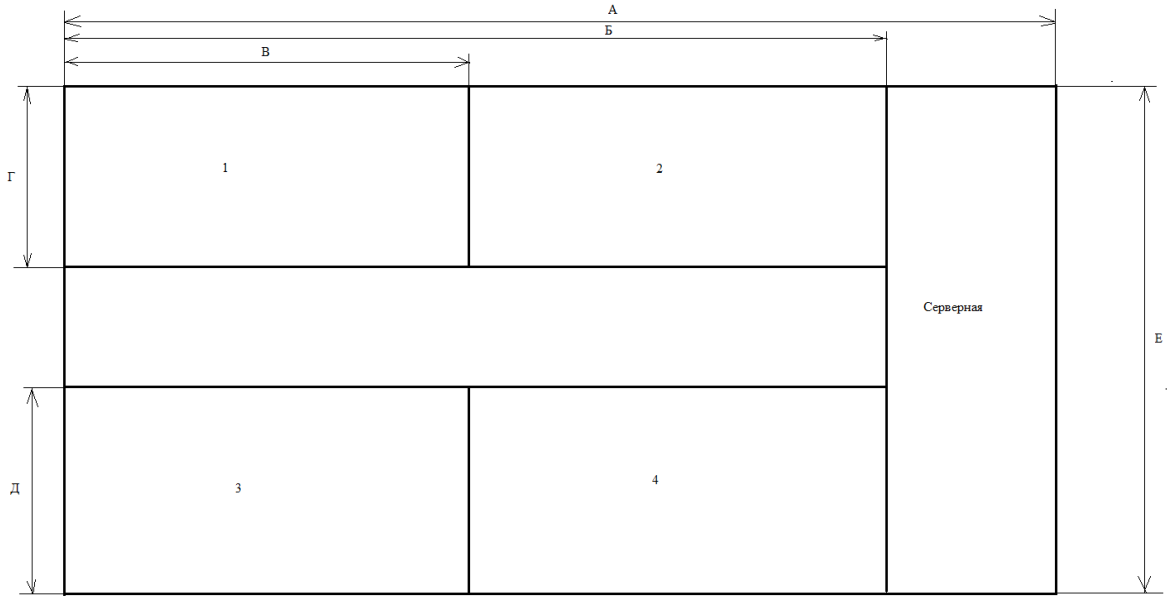
Для подключения серверов необходима максимальная пропускная способность активного сетевого оборудования, то есть маршрутизатор должен обладать высокоскоростными гигабитными портами.

Для того, чтобы провести подбор активного и пассивного сетевого оборудования и расчёт стоимости, необходимо составить примерный план сети:

1. Определить, исходя из планируемого количества рабочих станций в каждой комнате, примерную схему прокладки проводов с учётом геометрических размеров помещения, количество розеток при необходимости, а также коннекторов.
2. Исходя из примерной схемы прокладки проводов и геометрических размеров рассчитать метраж проводов, необходимый для подключения каждой рабочей станции к коммутатору, а также метраж кабельных каналов.
3. Добавить к метражу проводов в помещениях провода для подключения каждого помещения к центральному маршрутизатору.
4. Выбрать коммутаторы и маршрутизатор, исходя из необходимого количества портов.

Выбирая активное сетевое оборудование, необходимо иметь в виду, что оборудование имеет широкой ценовой диапазон, и не всегда выбор дорогого оборудования является технически обоснованным, поэтому внимательно анализируйте технические характеристики устройства и сравнивайте с другими, прежде чем останавливаться на дорогих аппаратах.

Задание: дан план помещений организации. В таблице приведены варианты геометрических размеров в метрах и количество рабочих станций в помещениях 1 – 4. Серверная содержит 2 вычислительные установки. Составить список активного и пассивного сетевого оборудования, необходимого для построения компьютерной сети, с указанием стоимости каждого пункта и общей стоимости оборудования. *Учитывается только сетевое оборудование, стоимость рабочих станций и серверов, а также стоимость работ не рассматривается.*



Варианты

Вариант	Размер А	Размер Б	Размер В	Размер Г	Размер Д	Размер Е	Количество 1	Количество 2	Количество 3	Количество 4
1	15	11	5	4	3	10	5	5	4	4
2	15	10	4	3	3	10	4	6	3	5
3	20	15	7	4	5	12	7	7	6	6
4	20	16	8	5	4	12	8	8	5	6
5	25	22	12	5	5	13	10	8	7	7
6	24	21	11	5	4	12	9	9	6	6
7	20	17	10	4	4	11	12	10	7	7
8	15	12	6	5	4	12	8	8	6	6
9	19	15	8	4	3	10	10	8	7	7
10	18	15	7	4	4	11	8	9	5	6
11	17	14	7	3	4	10	7	7	5	5
12	16	13	6	4	4	11	5	7	4	5
13	21	18	10	3	4	10	10	7	7	5

14	22	19	10	3	3	9	12	8	7	7
15	23	20	12	5	3	11	12	10	8	6
16	24	21	12	3	3	9	10	10	7	8
17	25	21	14	4	4	12	15	12	10	10
18	25	22	12	5	5	13	10	8	7	7
19	24	21	11	5	4	12	9	9	6	6
20	20	16	8	5	4	12	8	8	5	6
21	20	17	10	4	4	11	12	10	7	7
22	15	11	5	4	3	10	5	5	4	4
23	17	14	7	3	4	10	7	7	5	5
24	21	18	10	3	4	10	10	7	7	5
25	23	20	12	5	3	11	12	10	8	6
26	19	15	8	4	3	10	10	8	7	7
27	24	21	12	3	3	9	10	10	7	8
28	18	15	7	4	4	11	8	9	5	6
29	15	10	4	3	3	10	4	6	3	5
30	20	15	7	4	5	12	7	7	6	6

Контрольные вопросы

1. Что такое коммутатор?
2. Что такое маршрутизатор?
3. Что такое шлюз?
4. Какая беспроводная технология используется в современных маршрутизаторах?
5. Что такое шлюз?
6. Какая топология преимущественно используется в современных локальных сетях?

Литература

1. Берлин, А. Н. Абонентские сети доступа и технологии высокоскоростных сетей : учебное пособие / А. Н. Берлин. — 4-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2025. — 276 с. — Текст : электронный // Цифровой образовательный ресурс IPR SMART. — URL: https://www.iprbookshop.ru/146320.html (дата обращения: 16.02.2026).
2. Морозова, Е. И. Технологии предоставления широкополосного доступа : учебное пособие / Е. И. Морозова. — Новосибирск : Сибирский государственный университет телекоммуникаций и информатики, 2019. — 57 с. — Текст : электронный // Цифровой образовательный ресурс IPR SMART. — URL: https://www.iprbookshop.ru/102140.html (дата обращения: 16.02.2026).
3. Маглицкий, Б. Н. Основы технологий множественного доступа в сетях сотовой связи : учебное пособие / Б. Н. Маглицкий. — Новосибирск : Сибирский государственный университет телекоммуникаций и информатики, 2011. — 140 с. — Текст : электронный // Цифровой образовательный ресурс IPR SMART. — URL: https://www.iprbookshop.ru/45496.html (дата обращения: 16.02.2026).