1. Назначение и определение сети. Элементы сети.

**Компьютерная сеть** – совокупность узлов (компьютеров, рабочих станций), соединённых коммуникационными каналами, а также набор вспомогательного оборудования, обеспечивающего соединение станций и передачу между ними информации. **Назначение компьютерной сети** заключается в установлении связи между различными компьютерами и устройствами для обмена информацией. **Элементы сети** можно разделить на несколько категорий**: 1. Узлы (Nodes):** Компьютеры, серверы или другие устройства, подключенные к сети и способные обмениваться данными. **2.** **Каналы связи (Communication Channels):** Физические или беспроводные средства передачи данных между узлами. Это могут быть провода, оптоволокно, радиоволны и т.д. **3. Сетевое оборудование (Networking Equipment):** Вспомогательное оборудование, включая маршрутизаторы, коммутаторы, мосты и другие устройства, обеспечивающие стабильное соединение и передачу данных. **4. Программное обеспечение (Software):** Специальные программы и протоколы, используемые для организации обмена информацией в сети. К ним относятся операционные системы, сетевые протоколы (например, TCP/IP), а также прикладное программное обеспечение для работы сети. **Сетевая архитектура** – это совокупность сетевых аппаратных и программных решений, методов доступа и протоколов обмена информацией. Она представляет собой фундаментальный план, определяющий, как устройства в сети взаимодействуют между собой.

1. Классификация вычислительных сетей (по типу среды передачи, по размеру, по технологии)

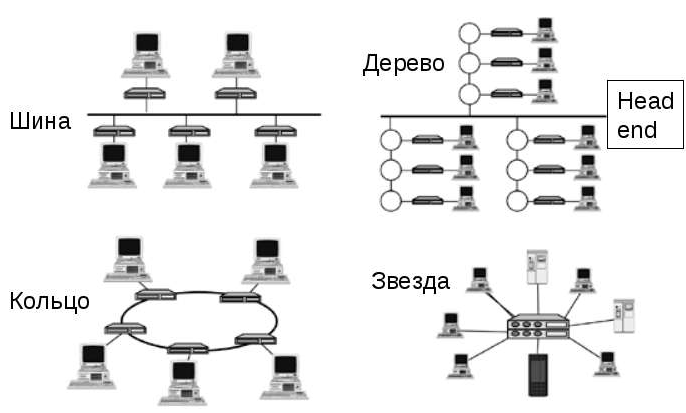
**По технологии передачи:** 1. вещательные, 2. точка-точка (p2p, пиринговые). По принципу организации обмена данными между абонентами: 1. сети на основе коммутации каналов, 2. сети на основе коммутации пакетов, 3. сети на основе коммутации сообщений. **Коммутация** – процесс связывания двух источников обмена информацией. **Коммутация** – технология выбора направления и организации данных в сетях, имеющих несколько альтернативных маршрутов. **Сетевой трафик** – информационные потоки, передаваемые по сети. Сети с коммутацией пакетов основаны на разбиении исходных сообщений на отдельные блоки малых размеров, которые могут передаваться разными маршрутами. Сеть с коммутацией каналов – тип коммутационной сети, в которой каждой паре абонентов в течении сеанса их соединения предоставляется выделенное физическое соединение. Сеть с коммутацией сообщений – передача между абонентами информации в виде логически завершенных частей данных. **По территориальной распространённости:** 1. PAN (personal area network) одно физическое лицо (например наушники). 2. LAN (local area network) включает устройства в пределах одного помещений, зданий, территории. 3. CAN (кампусные сети) состоит из нескольких локальных сетей, принадлежащих одной организации. 4. MAN (городская сеть) набор сетей различных организаций. 5. WAN (world area network) все узлы на планете Земля. 6. DNS (deep space network) обмен между космическими аппаратами. **По скорости передачи:** 1. низкоскоростные, 2. среднескоростные, 3. высокоскоростные. **По типу среды передачи:** проводные и беспроводные. **По принципу организации иерархии компьютеров:** одноранговые (все узлы имеют равные права) и с выделенным сервером (есть сервер, который предоставляет клиентам некоторые услуги).

1. Виды сетей. Одноранговые сети. Сети с выделенным сервером.

**По принципу организации иерархии компьютеров:** одноранговые (все узлы имеют равные права) и с выделенным сервером (есть сервер, который предоставляет клиентам некоторые услуги). **Одноранговые сети:** 1. Каждое устройство может обмениваться ресурсами и информацией непосредственно с другими устройствами 2. Отсутствие центрального сервера, что делает их более децентрализованными. 3. Часто используются в небольших сетях, таких как домашние сети или малые офисы. **Преимущества:** Простота установки и масштабирования. Нет единой точки отказа. **Недостатки:** не всегда эффективны при больших сетях или сетях с высокой нагрузкой. **Сети с выделенным сервером:** 1. Централизованная архитектура, где сервер управляет и распределяет ресурсы. 2. Клиенты обращаются к серверу для запросов и получения услуг. 3. Широко используются в предприятиях, больших офисах и интернет-сервисах. **Преимущества:** Централизованное управление и обслуживание. Эффективное распределение ресурсов. **Недостатки:** есть единая точка отказа – сервер. Больше сложности в установке и обслуживании по сравнению с одноранговыми сетями.

1. Топология сетей. Определение топологии. Физическая и логическая топология.

**Топология компьютерной сети** – конфигурация физических связей компьютеров или других сетевых устройств, количество конфигураций зависит от числа связей. При этом выделяют 2 вида топологий: логическая и физическая. **Физическая топология:** описывает фактическое физическое распределение устройств и кабелей в сети. Включает в себя такие виды топологий, как шина, кольцо, звезда, дерево и другие. **Логическая топология:** определяет способ, которым данные передаются между устройствами в сети. Может отличаться от физической топологии. Обеспечивает абстракцию для управления потоком данных и обменом информации. **Факторы, зависящие от выбора топологии:** надежность, простота подключения новых узлов, экономические соображения. **Классификация топологий:** полносвязные (Каждый узел связан с каждым другим узлом в сети. Обеспечивает высокую надежность, но требует больше ресурсов и дорого в реализации) и неполносвязные (Экономичнее, но с меньшей степенью надежности, наиболее популярные). Первая топология была **общая шина** – все подключены одной линией связи. **Топология кольцо** – соединение компьютеров в кольцо, данные могут передаваться в обе стороны, топология чувствительна к разрывам. **Топология звезда** – один узел ведущий и отвечает за передачу ко всем устройствам, центральный узел – концентратор, не сильно экономичная, но надёжная и масштабируемая (самая популярная технология для дома). **Топология дерево** – топология из нескольких звёзд, объединённых только концентратором.



1. Топология сетей. Топология «Шина»

**Описание:** В топологии "Шина" все устройства подключены к одному центральному каналу (широкополосной линии), который служит основным каналом для передачи данных. Каждое устройство имеет доступ к этому каналу и может слушать или отправлять данные. **Принцип работы:** один канал используется для передачи данных в обе стороны. **Принцип работы:** когда устройство хочет передать данные, оно отправляет их по центральному каналу. Все устройства слушают этот канал, и только устройство, к которому адресованы данные, их принимает. **Преимущества:** Простота установки, так как требуется только один центральный канал. Эффективен для небольших сетей с небольшим числом устройств. **Недостатки:** 1. если центральный канал выходит из строя, вся сеть может быть нарушена. **2.** количество данных, которые могут быть переданы одновременно, ограничено. **Применение:** топология "Шина" редко используется в современных сетях из-за своих ограничений, но может встречаться в небольших офисах или локальных сетях.

1. Топология сетей. Топология «Звезда»

**Описание:** В топологии "Звезда" все устройства подключены к центральному узлу, который служит в качестве центрального хаба или коммутатора. Все данные передаются через центральный узел. Каждое устройство имеет свой собственный канал связи с центральным узлом. **Принцип работы:** когда устройство хочет передать данные, оно отправляет их центральному узлу. Центральный узел передает данные только адресованному устройству. **Преимущества:** 1. легкость управления: (легкость установки и управления, так как центральный узел имеет полный контроль над сетью) 2. отсутствие конфликтов данных (каждое устройство имеет свой собственный канал, что уменьшает возможность конфликтов данных) **Недостатки:** 1. единая точка отказа (если центральный узел выходит из строя, все устройства теряют связь) 2. ограниченная пространственная гибкость (добавление новых устройств требует физического подключения к центральному узлу). **Применение:** 1. широко используется в небольших и средних сетях, таких как офисные или домашние локальные сети. 2. в серверных комнатах для соединения клиентских устройств с серверами.

1. Топология сетей. Топология «Кольцо».

**Описание:** В топологии "Кольцо" все устройства соединены в замкнутый круг, где каждое устройство имеет два соседа, с которыми оно связано. Данные передаются по кольцу от устройства к устройству в одном направлении. **Принцип работы:** когда устройство хочет передать данные, оно отправляет их по кольцу до тех пор, пока не достигнет целевого устройства. **Преимущества:** легко реализуется и понимается. **Недостатки:** 1. если одно устройство выходит из строя, вся сеть может быть нарушена. 2. скорость передачи данных зависит от числа устройств в кольце. **Применение:** редко используется в современных локальных сетях, но может встречаться в телекоммуникационных сетях для передачи данных между городами.

1. Топология сетей. Топология «Дерево».

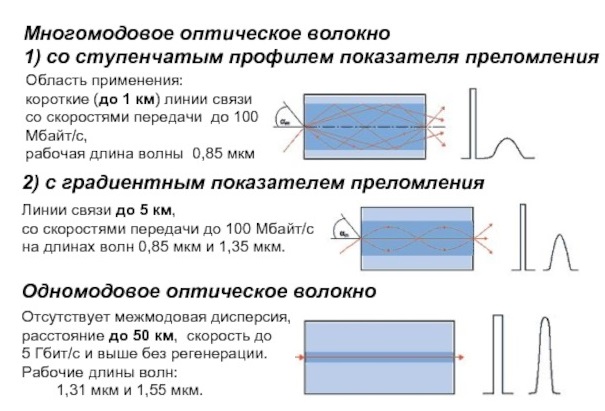
**Описание:** В топологии "Дерево" сеть организована в иерархическую структуру, напоминающую дерево. Центральные узлы (обычно коммутаторы или маршрутизаторы) соединяются между собой, образуя более крупные ветви, к которым подключены более мелкие ветви, представляющие отдельные сегменты сети. Обычно топология дерево выглядит как более мелкие сети с топологией звезда соединены вместе с помощью одного концентратора. **Принцип работы:** Центральные узлы соединены между собой, обеспечивая основные пути передачи данных. Каждый центральный узел может подключать к себе подчиненные узлы, создавая ветви структуры. **Преимущества:** 1. легко масштабируется с добавлением новых сегментов. 2. отказ одного сегмента не обязательно влияет на работу других. **Недостатки:** 1. более сложная структура требует более тщательного управления. 2. отказ центрального узла может повлиять на всю сеть. **Применение:** широко используется в корпоративных сетях, где требуется высокая масштабируемость и структурированность. Может применяться в широкополосных сетях с разветвленной инфраструктурой.

1. Определение и виды сред передачи.

**Среда передачи** – каналы связи, по которым можно обмениваться информацией. Если топология сети не полносвязна, то различные узлы используют одни и теже каналы связи, такие среды называют **разделяемые**. Подключение к разделяемой среде осуществляется с помощью **сетевого адаптора** – программно-аппаратного устройства, которое обеспечивает подключение, передачу и управление информационными потоками. **Виды сред передачи:** 1. проводник (строятся с использованием телефонных или телеграфных проводников. Передача данных осуществляется по проводам, что обеспечивает стабильность и надежность соединения.) 2. кабельная (большая пропускная способность по сравнению с проводниковой средой. Меньше подвержена электромагнитным помехам. Затраты на кабель и оборудование выше. Некоторые виды кабелей могут быть трудными в монтаже) 3. беспроводные (беспроводная мобильность устройств. Отсутствие необходимости в физических кабелях. Более высокая вероятность потери данных или помех. Ограниченная пропускная способность по сравнению с проводными средами).

1. Кабельные среды передачи. Витая пара. Коаксиальный кабель. Оптоволокно.

**Параметры кабелей:** 1. Полоса пропускания – частотный диапазон сигнала. 2. Задержка распространения сигнала, 3. Помехозащищенность кабеля, 4. Затухание – степень потери мощности сигнала относительно входа и выхода. **Три основных типа кабелей:** 1. витая пара, 2. коаксиальный кабель, 3. оптоволоконные. **Витая пара** представляет собой пару проводников, скрученных вместе. Используется для передачи данных в локальных сетях. Широко распространена и легко доступна. Может поддерживать высокие скорости передачи данных. Восприимчива к электромагнитным помехам. Дальность передачи данных ограничена. Есть **два вида витой пары**: UTP (UTP-5 UTP-6 UTP-7) (неэкранированная витая пара) и STP (STP-5 STP-6 STP-7) (экранированная витая пара – это витая пара, где каждая пара проводников экранирована металлической оплеткой или фольгой. Экранирование предназначено для защиты от электромагнитных помех и радиочастотных помех). **Коаксиальный кабель** состоит из центрального проводника, изолированного от внешней оболочки проводящим слоем. Используется для телевидения и кабельного интернета. Обеспечивает лучшую защиту от электромагнитных помех, чем витая пара. Более дорог в установке и обслуживании. Есть **два вида коаксиального кабеля**: толстый коаксиальный кабель RG-8 RG-11 (жила – 2.17мм, весь – 10мм) (Поддерживает длинные расстояния передачи данных и обеспечивает надежное экранирование.) и тонкий коаксиальный кабель RG-58 (жила – 0.89мм, весь – 5мм). **Оптоволоконный кабель** – передает данные в виде световых сигналов через тонкий стеклянный или пластиковый волоконный кабель. Высокая пропускная способность и скорость передачи данных. Устойчиво к электромагнитным помехам. Позволяет передавать данные на большие расстояния. Более дорого в установке и обслуживании по сравнению с другими типами кабелей. Может быть более хрупким и требовать бережного обращения. **Мода луча** – это угол отражения луча в сердцевине оптоволоконного кабеля. **Маркировка оптоволоконного кабеля** 9/125, где 9 – толщина сердцевины, а 11 – толщина наружней трубки.



1. Беспроводные среды передачи. Стандарт 802.11

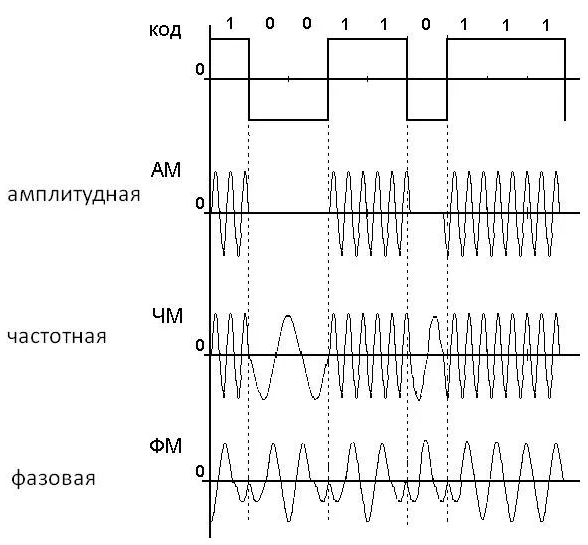
**Беспроводные линии связи** используют радиоволны или инфракрасное излучение, каналы строятся с помощью приёмника и передатчика для соответствующих волн. **Стандарт 802.11** представляет собой семейство стандартов, разработанных Институтом инженеров электротехники и электроники (IEEE) для беспроводных локальных сетей (WLAN). Наиболее известные стандарты из этого семейства включают:

| **Стандарт** | **Частотный диапазон** | **Скорость передачи данных** | **Дальность** |
| --- | --- | --- | --- |
| 802.11a | 5 ГГц | Высокая | Короткая |
| 802.11b | 2.4 ГГц | Низкая | Широкий радиус действия |
| 802.11g | 2.4 ГГц | Умеренная | Средний |
| 802.11n | 2.4 ГГц и 5 ГГц | Высокая | Увеличенная |
| 802.11ac | 5 ГГц | Очень высокая | Увеличенная |
| 802.11ax | 2.4 ГГц и 5 ГГц | Очень высокая | Увеличенная |

Стандарты 802.11 широко применяются в беспроводных сетях, таких как Wi-Fi в домах, офисах и общественных местах. Их выбор зависит от требований к скорости передачи данных, дальности и плотности устройств в сети.

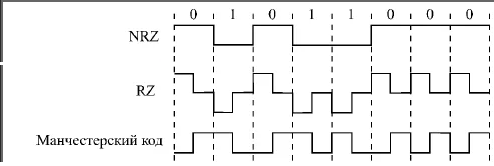
1. Кодирование данных. Понятие модуляции. Виды модуляции.

**Кодирование данных** – представление данных в виде электрического или оптического сигнала. **Модуляция** – способ представления цифрового кода в виде аналогового сигнала. Есть два вида кодирования данных: аналоговое и цифровое. Аналоговое кодирование кодирует информацию непрерывными величинами, в то время как цифровое представляет данные в виде нулей и единиц. **Виды аналоговой модуляции:** 1. амплитудная модуляция (кодируется изменением амплитуды) 2. частотная (кодируется изменением частоты) 3. фазовая: (кодируется изменением фазы). 4. квадратурная амплитудная (комбинирует изменения амплитуды и фазы для эффективного кодирования данных) 5. поляризационная (информация кодируется изменением поляризации электромагнитных волн) 6. амплитудно-фазовая (комбинирует изменения амплитуды и фазы для передачи данных). Цифровой сигнал обладает высокой устойчивостью к помехам и искажениям, так как биты кодируются дискретными уровнями, что делает проще обнаруживать и исправлять ошибки.



1. Цифровое кодирование данных. Способы цифрового кодирования.

**Цифровое кодирование данных** – это метод представления информации в цифровой форме, где данные преобразуются из аналоговой или дискретной формы в последовательность бит (0 и 1). **Способы цифрового кодирования:** **NRZ (Non-Return-to-Zero):** в этом методе бит "1" представлен высоким уровнем напряжения, а бит "0" - низким уровнем напряжения на протяжении всего времени бита. **Применение:** Прост в реализации, но может привести к проблемам синхронизации из-за отсутствия переходов. **RZ (Return-to-Zero):** каждый бит представлен двумя уровнями напряжения. Половина бита - высокий уровень, вторая половина - низкий уровень. В конце каждого бита происходит возврат к нулю. **Применение:** обеспечивает лучшую синхронизацию, но требует больше полосы пропускания из-за высоких частот. **Манчестерский код:** каждый бит разделяется на два временных интервала. Первая половина бита представляет "1" как переход от низкого к высокому уровню напряжения, а "0" как переход от высокого к низкому. Вторая половина бита имеет обратный порядок. **Применение:** обеспечивает постоянные переходы и хорошую синхронизацию, но требует удвоенной полосы пропускания.

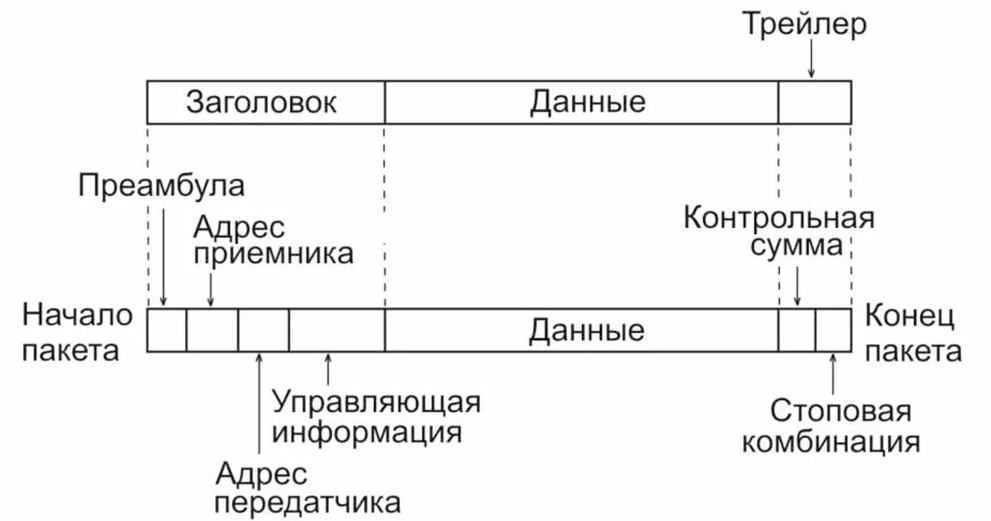


1. Методы логического кодирования данных.

**Методы логического кодирования данных** охватывают различные техники, которые применяются для представления логических значений (0 и 1) в цифровой форме. Вот несколько распространенных методов логического кодирования: 1. **Не инвертированный код (Non-Inverted Code):** 0 представлено низким уровнем напряжения, а 1 - высоким уровнем напряжения. **Применение:** простой и часто используемый метод логического кодирования. 2. **инвертированный код** (Inverted Code): 0 представлено высоким уровнем напряжения, а 1 - низким уровнем напряжения. **Применение:** в некоторых системах использование инвертированного кода может облегчить обнаружение ошибок. 3. **Дополнительный код (Two's Complement):** положительные числа представлены стандартным способом, а отрицательные - с использованием дополнительного кода, который получается инверсией битов и добавлением 1 к результату. **Применение:** широко используется в арифметических операциях с отрицательными числами. 4. **Код с четностью (Parity Code):** Дополнительный бит (бит четности) добавляется к блоку данных для обеспечения четного или нечетного количества единиц в блоке. **Применение:** позволяет обнаруживать ошибки в передаче данных**. 5. Грей-код (Gray Code):** последовательность чисел, где два соседних числа отличаются только одним битом. **Применение:** используется в определенных системах, где важно минимизировать ошибки при изменении состояний. 6. **Шинный код (One-Hot Code):** каждому логическому состоянию соответствует свой собственный бит, и только один из них установлен в 1, остальные - в 0. **Применение:** используется в логических схемах и схемах управления.

1. Сетевые стандарты. Типы пакетов. Структура пакета.

**Сетевые стандарты** – это набор правил и соглашений, которые определяют форматы данных, протоколы и технологии для эффективного обмена информацией в компьютерных сетях. **Пакет** – это блок данных, который передается по сети. Он содержит информацию, необходимую для передачи данных от отправителя к получателю. **Типы пакетов:** **Пакеты данных:** несут в себе фактическую информацию, такую как текст, файлы или мультимедийные данные, для передачи от отправителя к получателю. **Пакеты заголовка:** содержат метаданные о пакете, такие как адрес отправителя и получателя, необходимые для корректной маршрутизации в сети. **Пакеты контрольной суммы:** содержат контрольные данные для обнаружения и, в некоторых случаях, исправления ошибок в передаваемых данных. **Пакеты запросов и ответов:** используются для взаимодействия между клиентами и серверами, где запросы содержат запросы от клиентов, а ответы - соответствующие ответы от серверов. **Пакеты маршрутизации:** переносят информацию о маршрутах в сети, позволяя маршрутизаторам оптимизировать передачу данных. **Пакеты управления:** несут команды и сигналы для управления сетью, включая запросы на установление или разрыв соединения. **Структура пакета:** 1. **Преамбула** (последовательность битов, которая позволяет сетевым устройствам обнаружить присутствие сигнала и провести синхронизацию приёмника 10101010) 2. **Стартовый ограничитель** (специальная последовательность, которая обозначает начало пакета) 3. **Адрес назначения** (адрес узла, которому адресован данный пакет, этот адрес может быть индивидуальным, групповым или обозначать всех абонентов при извещательной передаче) 4. **Адрес отправителя** (адрес узла, сгенерировавшего пакет) 5. **Служебная информация** (содержит характеристики пакета: тип, размер, формат, маршрут доставки) 6. **Пользовательские данные** (информация, которую нужно передать по сети) 7. **Контрольная сумма** (специальное значение, которое используется для выявления ошибок при передаче).



1. Сетевые стандарты. Протоколы.

**Сетевые стандарты** – это набор правил и соглашений, которые определяют форматы данных, протоколы и технологии для эффективного обмена информацией в компьютерных сетях. **OSI (Модель взаимодействия открытых систем):** это сетевая модель, разработанная Международной организацией по стандартизации (ISO), которая описывает, как различные уровни сетевых протоколов взаимодействуют между собой. **TCP/IP (Протокольный стек):** это набор протоколов, который включает в себя Transmission Control Protocol (TCP) и Internet Protocol (IP). TCP/IP широко используется в интернете и является основой современных сетей. **Протоколы** – набор правил, определяющих формат и порядок передачи данных между устройствами в сети. **Основные протоколы:** **TCP (Transmission Control Protocol):** обеспечивает надежную и упорядоченную передачу данных между устройствами в сети. Широко используется для передачи данных, где важна точность и последовательность. **IP (Internet Protocol):** Отвечает за маршрутизацию и адресацию данных в сети. IPv4 и IPv6 - две основные версии протокола IP. **HTTP (Hypertext Transfer Protocol):** используется для передачи гипертекстовых документов в вебе. Браузеры и веб-серверы взаимодействуют с использованием HTTP. **HTTPS (Hypertext Transfer Protocol Secure):** безопасная версия HTTP, использующая шифрование для обеспечения конфиденциальности данных. **FTP (File Transfer Protocol):** используется для передачи файлов между устройствами в сети. **SMTP (Simple Mail Transfer Protocol):** протокол отправки почты, используемый для отправки электронных писем. **DNS (Domain Name System):** отвечает за преобразование доменных имен в IP-адреса, что позволяет устройствам находить друг друга в сети. **SSH (Secure Shell):** предоставляет защищенный канал для удаленного доступа и управления устройствами. **DHCP (Dynamic Host Configuration Protocol):** автоматически назначает IP-адреса и другие сетевые параметры устройствам в сети.

1. Эталонная модель взаимодействия открытых систем (OSI)

**Сетевая модель** устанавливает соглашения, по которым регламентируют взаимодействие передающего и принимающего узла, начиная от передачи битов, заканчивая тем как информация должна быть интерпретирована. **Open System Interconnection (эталонная модель взаимодействия открытых систем)** определяет уровни и их функции в задачах сетевого взаимодействия. ЭМВОС делит процессы сетевого взаимодействия на 7 уровней. Вышестоящие уровни выполняют более глобальные задачи, используя нижестоящие уровни, которые в свою очередь выполняют более конкретные и узкие задачи. Каждый уровень может общаться только с соседними ему уровнями. Только самый нижний уровень может общаться напрямую между узлами сети. Интерфейсы регламентируют общение между соседними уровнями одного узла, а протоколы между одноименными протоколами различных узлов. **Описание уровней:** 1. **Физический уровень:** определяет физические механизмы, электрические характеристики линии связи. Данные кодируются в электрические или световые сигналы. 2. **Канальный уровень:** определяет формат сети: 1) Logic Link Control – предоставление канала связи, 2) Media Access Control – установление адреса узла. 3**. Сетевой уровень –** отвечает за адресацию и маршрутизацию пакета. 4. **Транспортный уровень** – разбиение данных на пакеты, исправление ошибок, сборка принимаемых пакетов. 5. **Сеансовый уровень** – обеспечивает координацию связи между узлами, начало, завершение. 6. **Представительный уровень** – решает задачу преобразования, шифрования данных. 7. **Прикладной уровень** – взаимодействие пользователя с сетью через прикладные программы.



1. Модель и реализация стека TCP\IP

**Модель TCP/IP** представляет собой сетевую модель для управления передачей данных в цифровом виде. Она описывает способы передачи данных от одного устройства к другому и является основой для построения сетей, включая Интернет. Выделяемые уровни модели TCP/IP: 1. **Уровень доступа к сети (Канальный уровень):** описывает способ кодирования данных для передачи на физическом уровне. Включает подуровни Logical Link Control (LLC) и Media Access Control (MAC). Задачи включают управление передачей данных, обеспечение проверки и правильности передачи информации, а также управление доступом к физической среде. 2. **Уровень сети Интернет (Сетевой уровень):** предназначен для передачи пакетов из одной сети в другую. Работают маршрутизаторы, определяющие адреса сетей и перенаправляющие пакеты между ними. 3. **Транспортный уровень:** решает проблемы гарантированной или негарантированной доставки данных, контроля потока и управления соединением. Вводит понятие портов для передачи данных между процессами. 4. **Прикладной уровень:** предназначен для работы сетевых приложений. Реализация стека TCP/IP: стек протоколов TCP/IP представляет собой иерархию протоколов, каждый из которых выполняет свою уникальную функцию. Наиболее часто используемые протоколы включают: 1. **Ethernet (или другие канальные протоколы):** на физическом уровне обеспечивает кадровую передачу данных. 2. **IP (Internet Protocol):** межсетевой протокол, ответственный за адресацию и маршрутизацию пакетов. 3. **TCP (Transmission Control Protocol):** протокол транспортного уровня, предоставляющий надежный и упорядоченный поток данных с установкой соединения. 4. **UDP (User Datagram Protocol):** протокол транспортного уровня, обеспечивающий негарантированную передачу данных без установки соединения. 5. **Протоколы прикладного уровня:** включают HTTP, FTP, SMTP и другие, предназначенные для взаимодействия приложений.

1. Протокол IP.

**Протокол IP (Internet Protocol)** – это межсетевой протокол адресации и маршрутизации, который объединяет отдельные компьютерные сети в единую сеть Интернет, обеспечивая доставку пакетов данных между любыми узлами сети через произвольное число промежуточных узлов, таких как маршрутизаторы. **Свойства протокола IP:** 1. **Недостоверность** **доставки:** Протокол IP не гарантирует доставку пакета до адресата в надлежащем порядке. Пакеты могут приходить в порядке, отличном от отправки, могут прийти несколько раз, поврежденными или вовсе не прийти. Гарантию безошибочной доставки обеспечивают протоколы более высокого уровня, такие как TCP. 2. **Фрагментация:** Протокол предусматривает фрагментацию (дробление) пакетов данных в процессе доставки из-за разнородности по возможностям каналов связи. Фрагменты пакетов собираются воедино на стороне получателя. В IPv6 маршрутизаторы больше не обязаны выполнять фрагментацию, и отправитель должен учитывать минимальный размер 3. **Запрет фрагментации:** Возможность запрета фрагментации конкретного пакета предусмотрена в протоколе. В IPv6 запрет фрагментации включен по умолчанию. Если пакет не может быть передан целиком через сегмент связи, он уничтожается, и отправителю направляется уведомление по протоколу ICMP. **Изменения в IPv6 по сравнению с IPv4:** 1. Размер адреса увеличен с 4 байт до 16 байт. 2. Размер заголовка пакета увеличен с 20 до 40 байт. 3. Максимальный размер пакета увеличен с 65 Кб до 4 Гб. 4. Контрольная сумма: Исчезла излишняя контрольная сумма, что уменьшило необходимость ее пересчета на каждом узле маршрутизации. 4. Метки потоков и классы трафика введены для более эффективной обработки трафика. 5. Добавлена возможность для маршрутизации к нескольким адресатам одновременно. 6. Поддержка шифрования по протоколу IPsec. Протокол IP является основой сети Интернета и объединяет устройства в глобальную сеть, предоставляя им уникальные адреса и маршруты для обмена данными. С переходом к IPv6 решаются проблемы нехватки адресов, а также внедряются улучшения в эффективность и безопасность передачи данных.

1. Протокол TCP.

**Протокол TCP (Transmission Control Protocol)** – это один из ключевых протоколов транспортного уровня в стеке TCP/IP. TCP предоставляет надежное и упорядоченное соединение для передачи данных между узлами в сети. Основные свойства и функции протокола TCP: 1. **Надежность передачи данных:** это достигается с помощью механизмов подтверждения получения данных и повторной передачи в случае потери или повреждения пакетов. 2. **Контроль потока:** TCP контролирует скорость передачи данных, чтобы избежать перегрузки получателя. 3. **Упорядоченная доставка:** данные, передаваемые через TCP, доставляются в том порядке, в котором они были отправлены. 4. **Сегментация данных:** TCP разбивает данные на небольшие части, называемые сегментами, которые затем упаковываются в TCP-пакеты для передачи по сети. 5. **Трихэш-рукопожатие (Three-Way Handshake):** процедура установки соединения в TCP включает три шага: отправление синхронизационного (SYN) пакета, подтверждение (ACK) от получателя и отправление второго синхронизационного пакета. Это устанавливает надежное соединение между отправителем и получателем. 6. **Окно TCP (TCP Window):** механизм, позволяющий отправителю послать несколько пакетов до получения подтверждения, что повышает эффективность передачи данных. 7. **Передача потока данных:** TCP предоставляет поток данных, который абстрагирует приложения от деталей сегментации и передачи по сети. Это обеспечивает прозрачность для приложений, использующих TCP.

1. Протокол RIP.

**Протокол RIP (Routing Information Protocol)** – это внутренний протокол маршрутизации дистанционно-векторного типа, используемый для определения оптимальных маршрутов в компьютерных сетях. Основные этапы работы протокола RIP: 1. **Изучение сети:** Создание минимальной таблицы маршрутизации, учитывая только непосредственно подсоединенные сети. 2. **Рассылка минимальной таблицы соседям:** Маршрутизаторы начинают рассылать сообщения протокола RIP своим соседям через дейтаграммы UDP. Сообщения содержат информацию о каждой сети, её IP-адрес и расстояние от передающего маршрутизатора. 3. **Получение и обработка RIP-сообщений от соседей:** Маршрутизатор увеличивает каждое поле метрики на 1 и сравнивает значения с собственной таблицей маршрутизации. Затем рассылает обновленную таблицу соседям. **Адаптация маршрутизаторов RIP к изменениям в сети:** По истечении 180с если маршрут не поступал в новых таблицах адресов, объявляется недействительным. Обмен таблицами маршрутизации происходит каждые 30 секунд. Протокол RIP, хотя прост в реализации, устарел и редко применяется в современных компаниях. Его особенности, такие как ограниченное количество хопов и низкая сходимость, делают его менее эффективным в крупных сетях.

1. Протокол ICMP.

**Протокол ICMP (Internet Control Message Protocol)** представляет собой вспомогательный протокол в стеке протоколов TCP/IP и используется для передачи сообщений об ошибках и управляющих сообщений в компьютерных сетях. Функкции ICMP: **Обработка ошибок:** когда протокол IP обнаруживает, что дальнейшая передача пакета невозможна из-за ошибки, ICMP генерирует диагностическое сообщение. **Служебные функции:** ICMP выполняет служебные функции, например, при отправке эхо-запросов (ping) для проверки доступности хоста в сети. **Перенаправление маршрута:** ICMP может использоваться для отправки сообщений о перенаправлении маршрута, предлагая более эффективный путь к некоторым узлам. **Структура заголовка ICMP сообщения:** Заголовок ICMP-сообщения состоит из 8 байт: 1. **Тип (1 байт):** тип сообщения (например, 0 для ICMP reply, 8 для ICMP request). 2. **Код (1 байт):** более точно определяет тип ошибки или сообщения. 3. **Контрольная сумма (2 байта). 4. Оставшиеся 4 байта и поле данных:** зависят от значений полей типа и кода.

1. Методы доступа к физической среде. Методы доступа с контролем несущей

При построении сетей необходимо определить методы, при которых рабочие станции получают доступ к среде. Методы доступа бывают **1) централизованные** (всё управление в одном узле) **2) децентрализованные** (центра управления нет. Управление доступом в том числе предотвращение конфликтов осуществляется всеми абонентами сети одновременно). Этот метод делится на **1) детерминированные.** Определяют четкие правила, по которым осуществляется доступ абонента к сети. Абоненты имеют определенную систему приоритетов. Конфликты почти исключены. **2) случайные.** Произвольный порядок получения доступа при этом возможность конфликтов подразумевается, для этого определены способы их разрешения. Один из самых распространённых методов среды передачи является метод **множественного доступа с прослушиванием несущей и разрешением коллизий, сокращенно CSMA/CD.** **Суть метода:** сетевой адаптер прослушивает среду передачи чтобы определить свободна ли она в данный момент. **Если да,** то сетевой адаптер начинает передачу кадра**. Если в среде передачи обнаружен сигнал,** то сетевой адаптер откладывает передачу на некоторый интервал времени после которого снова пробует. После завершения передачи каждого кадра любой узел должен выждать паузу — **межкадровый интервал (9,6нс).** В случае, когда одновременно 2 сетевых адаптера прослушивают среду и обнаруживают, что она не занята и начинают одновременно передачу данных, случается **коллизия**, т.к. скорость света не бесконечна. Коллизия возникает даже, если не совсем одновременно была передача данных. Чем длиннее сеть, тем больше вероятность появления коллизий. При обнаружении коллизий рабочие станции обрабатывают передачу данных и переходят в режим ожидания (у каждой станции выбирается случайным образом и может составлять от 0 до 52,4мс после происходит повторная попытка передачи).

1. Методы доступа к физической среде. Методы доступа с передачей маркера, по приоритету запроса.

При построении сетей необходимо определить методы, при которых рабочие станции получают доступ к среде. Методы доступа бывают **1) централизованные** (всё управление в одном узле) **2) децентрализованные** (центра управления нет. Управление доступом в том числе предотвращение конфликтов осуществляется всеми абонентами сети одновременно). Этот метод делится на **1) детерминированные.** Определяют четкие правила, по которым осуществляется доступ абонента к сети. Абоненты имеют определенную систему приоритетов. Конфликты почти исключены. **2) случайные.** Произвольный порядок получения доступа при этом возможность конфликтов подразумевается, для этого определены способы их разрешения. **Маркерный метод** **доступа** используется с топологией кольцо и имеет детерминированный характер. **Суть метода:** поочередная передача права на пересылку кадров. Передается право с помощью маркера (кадр специального формата). Сеть с маркерным доступом контролируется активным монитором: генерация маркера, удаление, управление. **Метод доступа по приоритету запроса. Суть метода:** в передаче концентратору функций арбитра сети, который предоставляет доступ к сети. Концентратор циклически опрашивает свои порты, если нужно начать передачу, то он формирует очередь. Концентратор ведет таблицу запросов на передачу и ее приоритетов. Если сеть свободна он дает доступ более приоритетному.

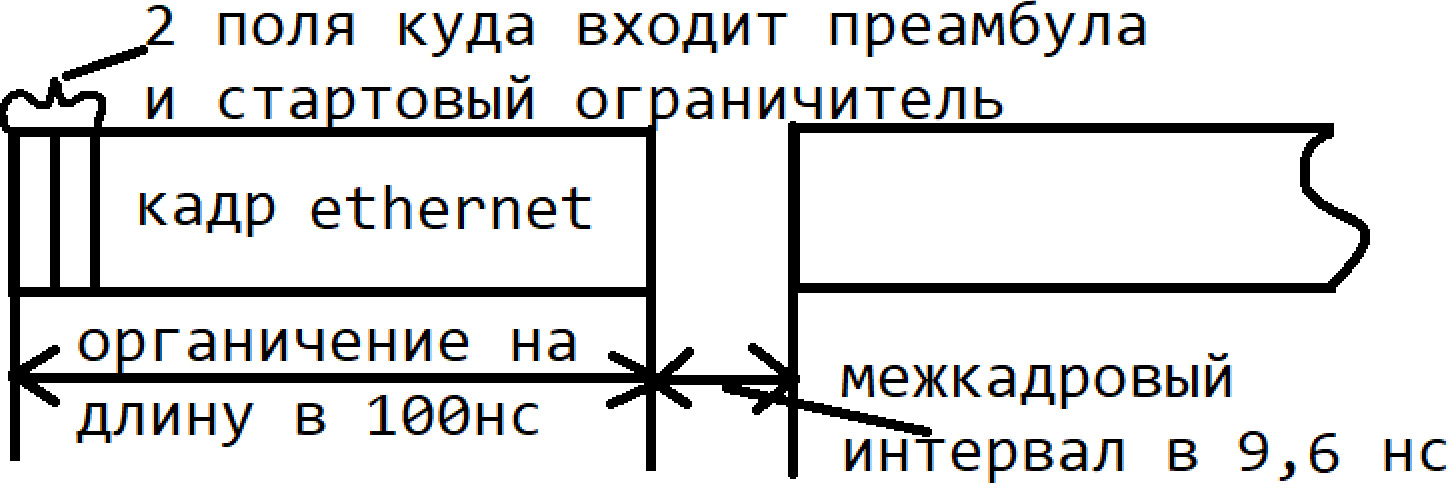
1. Модель IEEE Project 802. Структура комитетов.

**Модель IEEE Project 802** представляет собой серию стандартов, разрабатываемых IEEE (Институт инженеров электротехники и электроники), охватывающих различные аспекты компьютерных сетей, включая локальные и метрополитенские сети. В рамках модели IEEE Project 802 формируются различные комитеты для разработки стандартов и регулирования аспектов сетевых технологий.

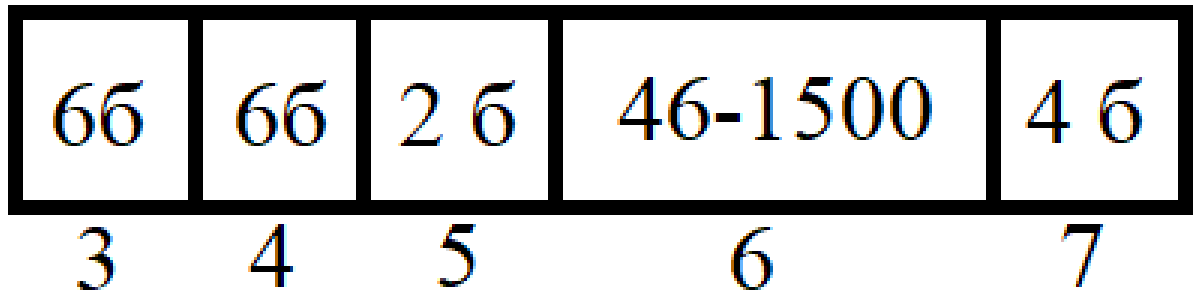
| **№** | **Комитет** | **Описание** |
| --- | --- | --- |
| 1 | IEEE 802 Executive Committee | Исполнительный комитет, общее руководство и управление проектом 802. |
| 2 | IEEE 802.1 Working Group | Архитектурные аспекты и общие стандарты для сетей. |
| 3 | IEEE 802.3 Working Group | Технологии и стандарты для сетей Ethernet. |
| 4 | IEEE 802.11 Working Group | Стандарты для беспроводных локальных сетей (Wi-Fi). |
| 5 | IEEE 802.15 Working Group | Стандарты для беспроводных персональных областных сетей (WPAN). |
| 6 | IEEE 802.16 Working Group | Стандарты для беспроводных метрополитенских областных сетей (WiMAX). |

1. Технология Ethernet. Формат кадра.

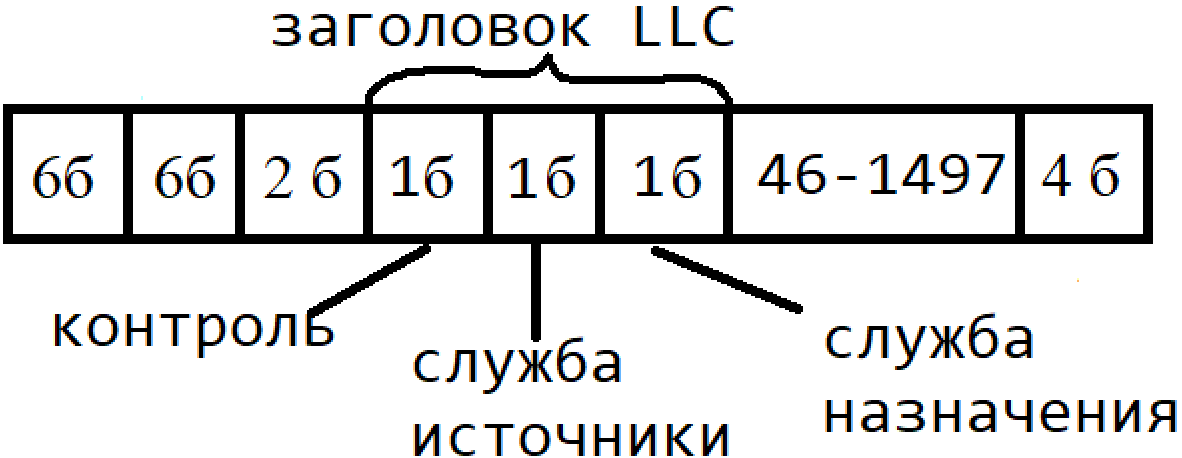
Было разработано базово несколько пакетов Ethernet: **1)** Raw 802.3 **2)** 802.3/LLC **3)** Ethernet ⅠⅠ **4)** Ethernet SNAP. Общий формат кадра начинается с такой информации:



**Формат кадра Raw 802.3:** передача кадров Ethernet любого из этих кадров предшествует преамбуле кадров 10101010 чтобы были одинаковые переходы. Стартовый ограничитель после преамбулы имеет вид: 10101011 показывая конец преамбулы. Ограничитель на длину кадра 100нс и паузы в 9,6нс. Поле данных не должно превышать 1500б, но min для 46б это надо для выравнивания пакета, если меньше 46б, то добавляем псевдоданные.



**Формат 802.3/LLC:** LLC — стандарт управления логическим соединением. Этот заголовок содержит поля службы назначения и службы источника и контроль. Эти службы определяют какие сообщения или данные принадлежат какой службе, пересылаемой в данном кадре и какие службы на другом узле должны эти данные получить.



**Формат кадра Ethernet ⅠⅠ** идентичен **Raw 802.3** с той лишь разницей, что поле идентификатора протокола выполняет аналогичные функции заголовка LLC.

1. Технология Ethernet. Адресация.

**Ethernet** является одним из наиболее широко используемых стандартов локальных сетей (LAN). Она определяет метод передачи данных в сетях с коммутацией пакетов. Протокол Ethernet работает на физическом и канальном уровнях модели OSI. **Адресация в технологии Ethernet:** **MAC-адрес:** Каждое устройство в сети Ethernet имеет уникальный физический адрес, называемый MAC-адресом. MAC-адрес представляет собой 48-битный идентификатор, обычно записываемый в виде шестнадцатеричного числа (например, 00:1A:2B:3C:4D:5E). Производители сетевого оборудования получают уникальные идентификаторы у Альянса IEEE. **Фрейм Ethernet:** Данные в сети Ethernet передаются в виде фреймов. Фрейм Ethernet содержит, среди прочего, MAC-адрес отправителя, MAC-адрес получателя и тип данных. Принимающее устройство сравнивает MAC-адрес получателя с собственным; если они совпадают, устройство принимает фрейм. **Коммутаторы Ethernet:** Коммутаторы являются устройствами на канальном уровне, обеспечивающими коммутацию фреймов на основе MAC-адресов. Когда коммутатор получает фрейм, он определяет порт, на котором находится устройство с соответствующим MAC-адресом, и направляет фрейм только на этот порт. **ARP (Протокол разрешения адресов):** используется для преобразования логических IP-адресов в физические MAC-адреса. Устройства в локальной сети отправляют ARP-запросы для определения MAC-адреса устройства с определенным IP-адресом.

1. Технология Ethernet. Физические реализации.

**Ethernet** является одним из наиболее широко используемых стандартов локальных сетей (LAN). Она определяет метод передачи данных в сетях с коммутацией пакетов. Протокол Ethernet работает на физическом и канальном уровнях модели OSI. **Основные физические реализации Ethernet:**

| **Технология** | **Описание** | **Скорость передачи данных** | **Дистанция** |
| --- | --- | --- | --- |
| 10BASE-T | Одна из самых распространенных реализаций, использующая витую пару (категории 5e или 6). | 10 Мбит/с | До 100 м |
| 100BASE-TX | Использует витую пару для передачи данных с более высокой скоростью. | 100 Мбит/с | До 100 м |
| 1000BASE-T (Gigabit) | Расширенная версия 100BASE-TX, предоставляющая гигабитные скорости. | 1 Гбит/с | До 100 м |
| 1000BASE-SX | Использует оптоволокно для передачи данных на скорости 1 Гбит/с. | 1 Гбит/с | До нескольких сотен м |
| 10GBASE-T (10-Gigabit) | Предназначена для достижения скоростей передачи данных 10 Гбит/с по витой паре. | 10 Гбит/с | До 100 м |
| 100GBASE-SR4 | Версия 100-Gigabit Ethernet для оптоволокна с дистанцией до нескольких сотен метров. | 100 Гбит/с | До нескольких сотен м |

1. Технологии Fast Ethernet, Gigabit Ethernet.

Fast Ethernet описан в 2 документах в 802,3u и изменился метод доступа в 802.12. Скорость этих стандартов 100Мбит/с.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Характеристика** | **100 Base-TX** | **100 Base-T4** | **100 Base-FX** | **100 VG-AnyLan** |
| **Тип кабеля** | UTP-5, STP-1 | UTP-3 | Многомодовое оптоволокно | UTP-3, UTP-4, UTP-5, STP-1, оптоволокно |
| **Метод доступа** | CSML CD | CSML CD | CSML CD | Demand priority |
| **Max число узлов в сети** | 1024 | 1024 | 1024 | 1024 |
| **Max длина сегментов в метрах** | 100м | 100м | 2000м | 225м |
| **Топология** | звезда | звезда | звезда | звезда |
| **Диаметр сети** | 205м | 205м | — | 1100м |

Gigabit Ethernet (скорость 1000Мбит/с) описан в стандарте 802.3z. 4 спецификации: **1) 1000 Base-LX** носитель одномодового оптоволокна с длинноволновым сигналом, длина сегмента до 5000м. **2) 1000 Base-SX** передача по многомодовому оптоволокну, длина волны 700нм, передача до 500м. **3) 1000 Base-T** витая пара категории 5, по каждой отдельной паре передача 250МегаБит в секунду. **4) 1000 Base-CX** в качестве физической среды используется специальная экранированная витая пара с волновым сопротивлением 750м на каждой жиле проводника, длина сегмента 25м.

1. Беспроводные локальные сети. Технология Bluetooth.

**Беспроводные локальные сети (БЛС)** представляют собой сети, в которых устройства связи соединены без использования физических проводов или кабелей. **Bluetooth** – это технология беспроводной связи, предназначенная для обеспечения короткодействующих соединений между устройствами. **Основные характеристики технологии Bluetooth:** 1. Короткодействующая технология: передача на расстояния до 10м. 2. Низкое энергопотребление. 3. Автоматическое подключение. 4. Частотный диапазон: работает в частотном диапазоне 2,4 ГГц, что является общим стандартом для беспроводных технологий. 5. Протоколы и профили: Bluetooth поддерживает различные протоколы и профили, включая для потоковой передачи аудио, подключения клавиатур и мышей. **Этапы работы Bluetooth:** 1. Обнаружение устройств: состояние ожидания запроса на подключение, отправка запроса на подключение. 2. Сопряжение (Pairing): во время сопряжения устройства обмениваются уникальными ключами безопасности, что обеспечивает защиту от несанкционированного доступа. 3. Формирование соединения: может быть одноразовым или постоянным. 4. Каналы связи: для уменьшения конфликтов частоты устройства могут переключаться между различными частотными каналами. 5. Профили и службы: определение девайса, типа передаваемых данных. 6. Мастер и ведомые устройства: в каждом соединении устройства выполняют роли мастера и ведомого. Мастер координирует связь, а ведомое устройство слушает и отвечает на команды мастера. 7. Спаренные устройства: после сопряжения и установления соединения устройства могут обмениваться данными в защищенном режиме.

1. Беспроводные локальные сети. Технология Wi-Fi.

**Беспроводные локальные сети (БЛС)** представляют собой сети, в которых устройства связи соединены без использования физических проводов или кабелей. **Принцип работы:** Wi-Fi, основанный на стандарте IEEE 802.11, представляет собой технологию беспроводной передачи данных по радиоканалам. Он использует различные протоколы, но одним из самых распространенных является 802.11b, работающий в частотном диапазоне 2,4 ГГц и обеспечивающий максимальную скорость 11 Мбит/с. Компоненты Wi-Fi-системы включают в себя точки доступа (Access Points) и беспроводные адаптеры (Wi-Fi Adapters). Точка доступа подключается к проводной сети и служит для передачи данных через радиоканалы. **Преимущества:** 1. Беспроводной доступ: позволяет организовать сеть без прокладки кабеля, что удобно в случаях, когда проводы невозможны или чрезмерно дороги. 2. Мобильность: обеспечивает доступ к сети для мобильных устройств в пределах зоны покрытия, что важно для ноутбуков и других портативных устройств. 3. Широкое распространение. 4. Быстрота развертывания. **Недостатки:** 1. Частотные ограничения: частотные диапазоны и правила использования различаются в разных странах, что может создавать ограничения и проблемы совместимости. 2. Ограниченная дальность: даже при максимальной дальности передачи сигнала (обычно до 100 м) преграды, стены и другие помехи могут снижать качество связи. 3. Безопасность: Беспроводные сети подвержены потенциальным угрозам безопасности, и для обеспечения безопасности часто требуется дополнительная настройка и шифрование.

| **Протокол** | **Частотный диапазон** | **Скорость передачи данных** |
| --- | --- | --- |
| 802.11b | 2,4 ГГц | До 11 Мбит/с |
| 802.11a | 5 ГГц | До 54 Мбит/с |
| 802.11g | 2,4 ГГц | До 54 Мбит/с |
| 802.11n | Различные частоты | До 320 Мбит/с |

1. Технологии глобальных сетей. Сети с коммутацией каналов.

Технологии глобальных сетей часто включают **сети с коммутацией каналов**, которые представляют собой метод организации коммуникации, при котором выделяется постоянный канал связи между двумя конечными пунктами на время их общения. Это отличается от сетей с коммутацией пакетов, где данные разделяются на пакеты и передаются по сети независимо друг от друга, а затем собираются обратно на конечном пункте. **Принцип работы:** 1. Выделение постоянного канала на время соединения. 2. Обеспечение гарантированной полосы пропускания для соединения. **Преимущества:** 1. Гарантированная пропускная способность в течение всего сеанса связи. 2. Подходит для передачи данных в реальном времени, таких как голосовая связь и видеоконференции. **Недостатки:** 1. Неэффективное использование ресурсов в случае неактивного соединения. **Примеры технологий:** ISDN (Integrated Services Digital Network): Интегрированная цифровая сеть, предоставляющая коммутацию каналов для передачи голоса и данных. PSTN (Public Switched Telephone Network): Общественная коммутируемая телефонная сеть, использующая коммутацию каналов для телефонных соединений. **Применение:** используется там, где требуется постоянная и гарантированная пропускная способность, например, в случае видеоконференций и потокового видео.

1. Технологии глобальных сетей. Сети с коммутацией пакетов.

Одной из основных технологий, лежащих в основе глобальных сетей, является **коммутация пакетов**. Суть их заключается в том, что данные разбиваются на небольшие пакеты для передачи по сети, каждый пакет может следовать различными маршрутами к месту назначения, пакеты собираются обратно в исходное сообщение на конечной точке. **Преимущества:** 1. Эффективность использования ресурсов: позволяет эффективно использовать пропускную способность сети, разделяя данные на пакеты. 2. Гибкость: позволяет выбирать оптимальные маршруты в зависимости от текущей загруженности сети. 3. Эффект непрерывной работы. **Самым распространённым стеком протоколов** для организации коммутация пакетов является TCP/IP. **Проблемы и вызовы:** 1. Фрагментация: Возможна разделенная передача пакетов по разным маршрутам, что требует их последующей сборки. 2. Задержки: Возможны небольшие задержки из-за коммутации и передачи каждого пакета.

1. Сетевое оборудование. Концентраторы.

**Концентраторы (hub)** — специальное многопортовое устройство, основная функция — повторение одного кадра на все остальные порты. К портам подключаются узлы сети с помощью различных кабелей. Hub зависит от технологии построения сети. Помимо основных функций может усиливать передаваемые сигналы или отключать неработающие порты. Производят 3 вида hub: **1)** с фиксированным количеством портов. **2)** как модульное устройство на основе шасси. **3)** со стековой конструкцией.

1. Сетевое оборудование. Коммутаторы.

**Коммутаторы** — это многопортовое устройство, выполняющее функции концентратора, моста. Отличительная особенность, является параллельная обработка кадров, позволяющая одновременно продвигать данные между всеми парами своих портов. Работа коммутатора основана на работе одном из 3 принципов: **1) Коммутирующая матрица.** Обеспечивает работу по принципу коммутации каналов, если нужный порт занят, полученный кадр записывается в буфер и ожидает доступности порта. **2) Общая шина.** Коммутаторы на основе общей шины используют аппаратное устройство шину, все видят и получают все, но каждый порт сам фильтрует данные. **3) Разделенная память.** На основе разделенной памяти реализовано несколько очередей данных для каждого порта в общей памяти.

1. Сетевое оборудование. Маршрутизаторы.

**Маршрутизатор (роутер)** — это высокоуровневое сетевое устройство, выполняющее функции концентратора, моста, коммутатора. Отличительная особенность наличие функции маршрутизации. **Функции маршрутизатора:** 1. Определение пути данных, учитывая параметры, такие как задержка и пропускная способность. 2. Пересылка данных по выбранному маршруту. 3. Балансировка нагрузки – распределение данных по разным путям. Алгоритмы определяют, как маршрутизаторы выбирают наилучший маршрут на основе метрик, таких как стоимость пути. **Процесс маршрутизации:** 1. Каждый маршрутизатор анализирует заголовок пакета и принимает решение о передаче по оптимальному пути. 2. Маршрутизаторы создают и обновляют таблицы маршрутизации на основе условий сети.

1. Маршрутизация.

**Маршрутизация** представляет собой процесс выбора оптимального маршрута для передачи данных в компьютерной сети. Сеть состоит из множества маршрутов, и маршрутизаторы принимают решения о передаче данных в зависимости от текущих условий сети. **Маршрутизатор** – сетевое устройство, соединяющее узлы и сети между собой. **Функции маршрутизатора:** 1. Определение пути данных, учитывая параметры, такие как задержка и пропускная способность. 2. Пересылка данных по выбранному маршруту. 3. Балансировка нагрузки – распределение данных по разным путям. Алгоритмы определяют, как маршрутизаторы выбирают наилучший маршрут на основе метрик, таких как стоимость пути. **Процесс маршрутизации:** 1. Каждый маршрутизатор анализирует заголовок пакета и принимает решение о передаче по оптимальному пути. 2. Маршрутизаторы создают и обновляют таблицы маршрутизации на основе условий сети. **Виды маршрутизации:** 1. Статическая маршрутизация: Ручная настройка маршрутов администратором, статичные таблицы. 2. Динамическая маршрутизация: Автоматическое обновление таблиц маршрутизации в реальном времени на основе условий сети. **Протоколы маршрутизации:** Протоколы внутренних шлюзов (IGP) и внешних шлюзов (EGP) определяют, как маршрутизаторы обмениваются информацией о маршрутах. **DNS-маршрутизация:** используется для управления коммуникационной нагрузкой DNS-серверов, оптимизируя связь с учетом задержек и географического распределения.

1. Адресация. Виды адресации и адресных пространств.

При объединении трех и более узлов возникает проблема идентификации конкретного узла. Решением данной проблемы является адресация компьютерных узлов. На практике обычно идентифицируют именно сетевой адаптер, т.к. в одном компьютере может был 1 и более сетевых карт (узел 1, а сетевых адаптеров больше). Множество всех допустимых адресов в какой-либо системе адресации называется **адресным пространством**. **Структура** адресного пространства: **1)** **Линейной (плоской).** Примером является mac адрес или физический адрес — это уникальный идентификатор, однозначно определяющий каждый сетевой интерфейс, запрограммированный в аппаратном обеспечении сетевого адаптера. За распределением диапазоном mac адресов для сетевого оборудования следит организация IEEE. Mac адрес представляет двоичное число длиной 48 бит. Для простоты восприятия и работы mac адреса записывают в виде 12 цифр в 16тиричной системе счисления. Первые 6 цифр определяют производителя сетевого устройства, а оставшиеся идентифицируют само устройство. **2)** **Иерархической.** Примером служат сетевые IP-адреса, которые используют в своей работе стек TCP/IP, т.к. IP-адрес работает на сетевом уровне, поэтому IP-адрес часто называется сетевым адресом. Он представляет собой двоичное число длиной 32 бита. Для удобства чтения и записи он представляется в виде 4 разделенных точками десятичных чисел. При иерархической адресации адресное пространство состоит из вложенных друг в друга подгрупп адресов, последовательно уточняющий конечного адресата. Первая часть IP-адреса уточняет номер сети, в которой находится узел, вторая часть идентифицирует сам узел. Адрес сети может быть выбран администратором самостоятельно, тогда можно использовать любой набор чисел, но если надо чтобы он был виден из интернета, то адрес назначается централизованно и получить его можно у ICANN. **Адреса класса A** предназначены для крупных сетей в масштабе региона или страны. **Адреса класса B** имеют средний размер использования в университетах и крупных компаниях. **Сети класса C** используются в малых сетях имеющие небольшое количество узлов. **Адреса класса D** используются для обращения к группе компьютеров. **Адреса класса E** зарезервированы для будущего использования. **Выделяют 5 диапазонов IP-адресов:**

|  |  |  |  |
| --- | --- | --- | --- |
| **Диапазон** |  | **Количество сетей** | **Количество узлов** |
| **A** | 1-126 | 126 | 16млн |
| **B** | 128-191 | 16382 | 65к |
| **C** | 192-223 | 2млн | 254 |
| **D** | 224-239 |  |  |
| **E** | 240-247 |  |  |