|  |  |  |  |
| --- | --- | --- | --- |
| **1.Определение понятий.**  Телеком. сеть –это совокупность телекоммуникаций, посредством которых обеспечивается информационный обмен между множеством территориально удаленных объектов.  Инф. сеть – сеть, предназначенная для обработки, хранения и передачи данных.  Выч. сеть — система, обеспечивающая обмен данными между выч. устройствами (компьютеры, серверы, маршрутизаторы и др.).  Назначение компьютерных сетей:   * Хранение и обработка данных * Организация доступа пользователей к данным * Передача данных и результатов обработки пользователям   Пакет — это определённым образом оформленный блок данных, передаваемый по сети в пакетном режиме. | **2. Классификация**  **По архитектуре**   * Клиент-сервер * Одноранговая сеть   **По топологии**   * Шина * Кольцо * Двойное кольцо * Звезда * Ячеистая * Решётка * Дерево * Смешанная топология * Fat Tree * **По типу среды передачи** * Проводные (телефонный провод, коаксиальный кабель, витая пара, волоконно-оптический кабель) * Беспроводные (по радиоволнам в определённом частотном диапазоне)   **По функц. назначению**   * Сети хранения данных * Серверные фермы * Сети управления процессом * Сети SOHO, домовые сети   **По скорости передачи**   * низко(< 10 Мбит/с) * сред(< 100 Мбит/с) * выс(> 100 Мбит/с);   **По сетевым ОС:**   * на осн Windows * на осн UNIX * на осн NetWare * на осн Cisco   **По необходимости поддержания пост. соединения**   * Пакетная сеть * Онлайновая сеть | **3. Разновидности по технологии передачи, масштабу**  По технологии передачи:   * Широковещательные сети (передаваемая инф-я доступна всем компьютерным узлам). * Точка-точка (инф-я передается между двумя отдельными компьютерами / через несколько промежуточных машин).   **По масштабу:**   * **PAN** — персональная сеть, для взаимодействия разл. устройств, принадлежащих одному владельцу. * **LAN** — имеющие замкнутую инфраструктуру до выхода на поставщиков услуг. * **CAN** — кампусная, объединяет лок. сети близко расположенных зданий. * **MAN** — городские сети между учреждениями в пределах одного/ нескольких городов, связывающие много ЛВС. * **WAN** — глоб. сеть, покрывающая большие географ.регионы, вкл. в себя лок. сети и прочие телеком. сети и устройства. Пример — сети с коммутацией пакетов (Frame relay), через которую могут «разговаривать» между собой различные компьютерные сети. WAN являются открытыми и ориентированы на обслуживание любых пользователей. | **4. Разновидности по топологии; преимущества и недостатки**  **Шина**:  +1) Отказ 1 рабочей станции не влияет на работу всей сети.  2) Простота и гибкость соединений.  3) Недорогой кабель и разъемы.  4) небольшое количество кабеля  5) его прокладка не сложна.  -1) Разрыв кабеля/ другие неполадки в соединении может исключить нормальную работу всей сети.  2) Ограниченная длина кабеля и количество рабочих станций.  3) Трудно обнаружить дефекты соединений.  4) Невысокая производительность.  5) При большом объеме передаваемых данных главный кабель может не справляться с потоком информации, что приводит к задержкам  **Звезда:**  **+**1) Подключение новых рабочих станций не вызывает особых затруднений.  2) Возможность мониторинга сети и централизованного управления сетью  3) При использовании централизованного управления сетью локализация дефектов соединений максимально упрощается.  4)Хорошая расширяемость и модернизация  -1)Отказ концентратора приводит к отключению от сети всех рабочих станций, подключенных к ней.  2) Достаточно высокая стоимость реализации, т.к. требуется большое количество кабеля.  **Кольцо**  +простота установки;  +практически полное отсутствие +дополнительного оборудования;  +возможность устойчивой работы без +существенного падения скорости передачи данных при интенсивной загрузке сети  -каждая рабочая станция должна активно участвовать в пересылке информации; в случае выхода из строя хотя бы одной из них/ обрыва кабеля – работа всей сети останавливается;  -подключение новой рабочей станции требует краткосрочного выключения сети, поскольку во время установки нового ПК кольцо должно быть разомкнуто; сложность конфигурирования и настройки;  сложность поиска неисправностей. |
| **5. Режимы передачи:**  Последовательная передача осуществляется всего по одному каналу, хотя общее число каналов может быть и больше. В этом случае по доп. каналам передаются сигналы синхронизации и управления.  Параллельная - выполняется последовательно квантами, содержащими т бит. Каждый квант передаётся одновременно по т каналам; величина m наз. шириной интерфейса и обычно соответствует/ кратна байту. Наиболее распространены параллельные интерфейсы, в которых т = 8/ т = 16.  Симплекс, полудуплекс, дуплекс определяют направление передачи сигнала. В симплексном режиме данные передаются по каналу только в одном направлении. В полудуплексном - в течение одного промежутка времени данные передаются в одном направлении, а в течение другого - в обратном. В дуплексном режиме данные передаются одновременно в обоих направлениях. | **6. Клиент-серверная архитектура; горизонтальное и вертикальное разделение компонент**  Модель клиент-сервер: процессы, реализующие некоторую службу (например, службу файловой системы/ БД), называются серверами. Процессы, запрашивающие службы у серверов путем посылки запроса и последующего ожидания ответа от сервера, - клиенты.  Распределение предполагает разбиение компонентов на мелкие части и последующее разнесение этих частей по системе.  При горизонтальном распределении клиент/ сервер могут содержать физически разделённые части логически однородного модуля, причем работа с каждой из частей может происходить независимо. Это делается для выравнивания загрузки.  Вертикальное распределение достигается размещением логически различных компонентов на разных машинах. | **7. Трехзвенная архитектура; одноранговые сети**  Трёху́ровневая - архитектурная модель пр. комплекса, предполагающая наличие в нём 3 компонентов: клиента, промежуточного сервера и агента.  1.клиент системы управления уст. на компьютере оператора, поддерживает пользовательский интерфейс с промежуточным сервером.  2.промежуточный сервер уст. либо на компьютере оператора, либо на специально выделенном компьютере.Он взаимодействует обычно с несколькими клиентами и агентами, обеспечивая диспетчеризацию запросов клиентов к серверам и обрабатывая полученные от агентов данные. Для повышения надежности и производительности в системе управления может быть предусмотрено несколько менеджеров.  3.агент устанавливается на управляемом объекте /связанном с ним компьютере, от него поступает информация о состоянии управляемого объекта, значении его характеристик  В случае одноранговых связей каждый менеджер управляет своей частью сети на основе информации, получаемой от нижележащих агентов. Центральный менеджер отсутствует. Координация их работы достигается за счет обмена информацией между БД менеджеров. Одноранговое построение системы управления сегодня считается  неэффективным и устаревшим. | **8. Эталонная модель ISO/OSI: причины появления, функции уровней.**  В ней было решено разделять задачу передачи информации на 7 проблемных областей, которым соответствуют 7 уровней модели. Модель определяет, как информация от прикладной программы одного компьютера, через среду передачи передается др. прикладной программе, выполняемой в др.компьютере.  **Прикладной**: взаимодействует с прикладными программами (не входят в модель). Определяет доступность партнеров по коммуникации, синхронизирует приложения, уст. соглашения о процедурах коррекции ошибок и целостности данных.  **Уровень представления**: гарантирует, что информация будет читабельной прикладным уровнем др. системы, обеспечивает конвертацию между разл. форматами и структурами данных.  **Сессионный**: Установление, управление и завершение сессий между приложениями. Сессия - диалог между 2< презентационными сущностями, синхронизирует диалог между ними, управляет их обменом данными  **Транспортный**: обеспечивает надежность транспорта, механизмы уст-я, поддержки и завершения виртуальных соединений, опред-е сбоев транспорта и восст-е  **Сетевой**: обеспечивает связь и выбор пути между системами. Поскольку они могут разделяться значительными географ. расст-ми и др. подсетями. Протоколы маршрутизации выбирают опт. путь через последовательность подсетей. Др. протоколы сетевого уровня обеспечивают передачу инф-и по этим путям.  **Канальный**: Предоставляет надежную передачу данных по физ. каналу связи. Отвечает за физ. адресацию, сетевую топологию, порядок доставки фреймов, упр-е потоком данных и т.п.  **Физический**: Электрические, мех., процедурные и функц. спецификации для активации, поддержки и деактивации физ. уровня между конечными системами. Примеры: уровни напряжений, временные параметры, физические скорости передачи данных, разъемы и т.п. |
| **9. Понятие коммутации...**  Коммутация данных - это такая передача, при которой канал передачи может использоваться попеременно для обмена инф-й между разл. пунктами инф. сети.  Некоммутируемые (выделенные) каналы, как правило жестко закрепляются за определенными абонентами.  Коммутируемы каналы: Образование непрерывного физического канала из последовательно соединенных отдельных участков сети. Каналы оказываются недоступными для других передач до их освобождения источником. Отдельные участки сети (каналы) соединяются друг с другом коммутаторами  Коммутация пакетов в дейтаграммном режиме: Дейтаграмма – один пакет данных с сопутствующей информацией о пункте назначения, передаваемый в сети с пакетной коммутацией. Не требует предварительного установления соединения. Маршрутизация каждого пакета независима.  Коммутация пакетов виртуального вызова: Перед тем, как начать передачу пакетов сообщения в сеть, источник посылает пакет «виртуального вызова» (virtual call) с информацией о том, что собирается передать приемнику сообщение с указанием его величины. Приемник резервирует память и посылает подтверждение (или отказ). Источник, получив подтверждение, начинает сеанс связи.  Коммутация пакетов установлением виртуального канала: Кроме резервирования ресурсов приемника, фиксируется маршрут передачи пакетов одного и того же сообщения.  Коммутация пакетов установлением виртуального соединения: в отличие от режима с установкой виртуального канала (ресурсы в линиях и устройствах коммутации не закрепляются за виртуальным каналом), обеспечивает приход пакетов к абоненту в правильной последовательности. | **10. Понятие модуляции, основные принципы и их виды.**  Процесс изменения параметров несущей в соответствии с передаваемым сигналом, называется модуляцией.  Виды модуляции: Амплитудная, Частотная, Фазовая, Широтно-импульсная, Время-импульсная.  Манипуляция. При дискретной модуляции сообщение выступает как последовательность кодовых символов, например, «1» и «0». Дискретная модуляция называется манипуляцией: Амплитудная, Частотная, Фазовая.  Амплитудная модуляция. При АМ символу «1» соответствует передача колебания в течение времени t (посылка), символу «0» - отсутствие колебания (пауза)    Частотная модуляция. При ЧМ символу «1» соответствует передача колебания с частотой ω1, символу «0» - ω0    Фазовая модуляция (1): При ФМ меняется фаза колебания. При двукратной ФМ фаза колебания изменяется на 180° при каждом переходе от символа «1» к «0», и на -180° - от «1» к «0».    Фазовая модуляция (2): Выражение изменения фазы колебания в векторной форме. | **11. Определение канала передачи...**  Каналом передачи информации называют совокупность технических средств, обеспечивающих передачу электрических сигналов от одного пункта к другому. Входы канала подключаются к передатчику, выходы – к приемнику  Амплитудно-частотная характеристика (АЧХ) - Зависимость амплитуды синусоиды на выходе линии связи по сравнению с амплитудой на ее входе для всего диапазона частот передаваемого сигнала  Полоса пропускания - Диапазон частот, для которых отношение амплитуды выходного сигнала к входному превышает некоторый заданный предел. Влияет на максимально возможную скорость передачи информации по линии связи.  Затухание - Относительное уменьшение амплитуды или мощности сигнала при передаче по линии связи сигнала определенной частоты  Обычно измеряется в децибелах (дБ). Вычисляется по формуле: L = 10 log10(Pвых/Pвх), Pвых - мощность сигнала на выходе линии, Pвх - мощность сигнала на входе линии  Емкость канала - предельно допустимое значение скорости передачи информации канала. Формула Хартли-Шеннона для емкости канала, С = F log2 (1 + Pc / Pш), F – максимальная частота в спектре сигнала, Pc - мощность сигнала, Pш - мощность шума  Пропускная способность - Характеризует максимально возможную скорость передачи данных по линии связи и измеряется в бит/с (Кбит/с, Мбит/с, Гбит/с)  Достоверность передачи данных - Характеризует вероятность искажения для каждого передаваемого бита данных | **12. Представление информации при передаче...**  При асинхронной передаче символы передаются в свободном темпе независимо друг от друга, причем каждый символ передается со своими сигналами «Старт» и «Стоп», указывающими на начало и конец передачи символа.  Асинхронная передача: позволяет передавать информацию с устройств, выдающих ее асинхронно во времени; скорость ниже из-за большого числа служебных сигналов.  При синхронной передаче блок символов передается непрерывно в принудительном темпе, синхронизация передающего и принимающего устройств достигается посылкой специальных кодовых комбинаций. Синхронный метод передачи: большая скорость; более сложная реализация.  Синхронизация — процесс установления и поддержания временных соотношений (взятия отсчётов) между двумя и более системами, участвующих в процессе синхронной  передачи цифровых данных. Один из способов синхронизации – посылка передающим узлом сигналов тактовой частоты. Требуется отдельная линия связи.  Самосинхронизирующиеся коды - коды, из которых можно выделить синхроимпульс.  NRZ – Non Return to Zero – «без возврата к нулю». Простейший код. Логическая 1 представляется положительным напряжением высокого уровня, 0 – низкого уровня. Преимущество - простота реализации (не требуется кодировка/декодировка). Недостаток - возможность потери синхронизации приемником при приеме длинного блока. Код NRZ используется только для передачи коротких блоков информации.  RZ – Return to Zero – «возврат к нулю». Трехуровневый код, после значащего уровня сигнала в первой половине передаваемого бита информации следует возврат к нулевому уровню. В середине каждого бита всегда есть переход. Недостаток – требуется вдвое большая полоса пропускания канала, при той же скорости передачи по сравнению с NRZ, т.к. на каждый бит приходится 2 изменения уровня напряжения.  Код Манчестер - ||. В отличие от RZ использует только 2 уровня – выше помехозащищенность. Логическому нулю соответствует положительный переход в центре бита (из низкого уровня в высокий), логической единице – отрицательный переход в центре бита (или наоборот). Преимущество – отсутствие постоянной составляющей сигнала (половину времени сигнал положительный, половину – отрицательный).  Код AMI - «0» соответствует 0 вольт , «1» - попеременно сигналами положительной и отрицательной полярности. Возникает проблема синхронизации при большом количестве нулей подряд.  Код HDB3 - Последовательность из 4 нулей заменяется последовательностью из 3 нулей, за которой следует нарушение последовательности отображения единиц. |
| **13.Проводные и кабельные линии связи..**  Линия связи – физическая среда, обеспечивающая поступление сигналов от передающего устройства к приемнику.  В зависимости от среды передачи линии связи могут быть: Проводные (воздушные), Кабельные (медные и волоконно-оптические), Беспроводные (радиоканалы наземной и спутниковой связи)  Проводные линии – провода без экранирующих или изолирующих оплеток. Обладают низкой помехозащищенностью и низкой скоростью передачи данных. Как правило, применяются для передачи телефонных и телеграфных сигналов.  Кабельные линии связи – пучок проводов, заключенных в одну или несколько защитных трубок  Основные типы кабелей: Витая пара, Коаксиальные кабели с медной жилой, Волоконно-оптические кабели  Витая пара (twisted pair) – скрученная пара проводов. Скручивание снижает влияние внешних помех на передаваемые по кабелю сигналы  Основные виды:  Экранированная (Shielded Twisted Pair, STP) – каждая из витых пар помещается в металлическую оплетку – экран . Уменьшение излучений кабеля, Защита от внешних электромагнитных помех, Снижение взаимного влияния пар проводов друг на друга  Неэкранированная (Unshielded Twisted Pair, UTP) - Простота монтажа и ремонта, Больше затухание сигнала => линии связи, как правило, короче, Ниже помехозащищенность  Категории кабелей на основе неэкранированной витой пары: 1 – не витые провода; 2 – витые пары, полоса частот до 1МГц; 3 – витая пара с 9 витками на 1 метр длины, полоса частот до 16 МГц; 4 – полоса частот до 20 МГц; 5 – полоса частот до 100 МГц, не менее 27 витков на метр длины; 6 – до 200 МГц; 7 – до 600 МГц  Коаксиальный кабель состоит из Внутренней медной жилы (центральный проводник), Слоя изоляции, Внешнего экрана, Внешней защитной оболочки  Основные типы коаксиальных кабелей: Тонкий (Гибкий, диаметр ок.0,5 см.), Толстый (Диаметр ок.1 см., значительно более жесткий). Затухание в тонком кабеле выше. | **14.Волоконно-оптические кабели(ВОК)..**  Состоит из центрального проводника света – стеклянного волокна, окруженного другим слоем стекла – оболочкой, обладающим меньшим показателем преломления, чем сердцевина. Распространяясь по сердцевине, лучи света, отражаясь от оболочки, не выходят из центрального проводника  Защитная оболочка предохраняет оптоволокно от повреждений. «Мода» – режим распространения световых лучей во внутреннем сердечнике кабеля.  Виды  -Многомодовые волокна - это опт. волокна, поддерживающие несколько поперечных мод для данной оптической частоты и поляризации. Число мод опред. длиной волны и показателем преломления материала. Подразделяются на волокна со ступенчатым профилем показателя преломления и градиентные.  Устройство  При ступенчатом изменении показателя преломления свет разных «мод» проходит разное расстояние, что приводит к «модальной дисперсии» и снижению качества сигнала на приемнике  Для снижения влияние этого эффекта существуют волокна с плавным изменением показателя преломления  - Одномодовое волокно - опт. кабель передает одну моду и имеет диаметр сечения ≈ 9,5 нм)  Устройство  Диаметр сердечника одномодового волокна значительно меньше  Только одна «мода» света пропускается сквозь сердечник  Качество сигнала выше  Полное внутреннее отражение:  100% света,попадающего на поверхность, отражается  Зеркало отражает только порядка 90% падающего на него света  Свет, в зависимости от угла падения отражается от поверхности/ преломляется  Полное внутреннее отражение:  Свет поступает от более плотного к менее плотному материалу  Угол падения меньше критического (при кот. свет прекращает преломляться и вместо этого полностью отражается)  Коэффициент преломления сердечника больше, чем у оболочки  Лучи под углом меньше крит.отражаются; под углом больше - преломляются | **15. Передача радиосигнала**….  Радиосвязь - разновидность беспроводной передачи информации, при которой в кач-ве носителя инф-и исп.радиоволны, свободно распространяемые в простр-ве.  Передача радиосигнала  В диапазонах LF и MF можно поймать радиоприемником на расст-и порядка 1000 км; радиоволны проникают сквозь здания; недостаток – низкая пропускная спос-сть.  В диапазонах HF и VHF радиоволны поглощаются землей, однако при достижении ими ионосферы, они отражаются и возвращ. обратно к земле. Исп. для дальней связи.  Особенности связи в разл. диапазонах.  Электромагнитный спектр  Движ-е e порождает эл. маг. волны, кот. могут распростр. в пространстве  В вакууме все эл. маг. волны распр. с одной скоростью, независимо от их частоты  Эта - скоростью света, с = 3 \* 108 м/с  Величины f, λ, c связаны: λ \* f = с  Для передачи информации исп. радио, микроволновый, инфракрасный диапазоны  Ультрафиолетовое, рентгеновское и гамма-излучение сложны для генерации и модулирования и опасны.  Микроволновый диапазон  На частотах выше 100 МГц радиоволны распространяются почти по прямой и могут быть сфокусированы в узкие пучки при помощи параболической антенны  Чем выше ретрансляционные башни, тем большее расстояние между ними может быть  Сложности:  Плохо проходят сквозь здания  Отражение части волн от атмосферы  На частотах > 4 ГГц становится заметным поглощение водой  Преимущества:  Дешевизна  Не требуется прокладка кабелей  Лицензирование частот  Ведется учет владельцев радиопередатч.  Инфракрасные и миллиметровые волны  широко применяется для связи на небольших расстояниях  Пульты ДУ для бытовой техники  ИК порты компьютеров  Не проходит сквозь твердые объекты (и+и-)  Связь в видимом диапазоне  Используется два лазера  Сложность настройки  Не проходит сквозь туман/ дождь  Возможно откл-е луча в завис. от t воздуха | **16. Спутниковые системы связи..**  Спутники связи  -Проще всего представить в виде огромного микроволнового повторителя, включающего в себя несколько транспондеров  -Транспондер (Передатчик-ответчик) – приемо-передающее ус-во, посылающее сигнал в ответ на принятый сигнал  -Каждый транспондер настраивается на опред. часть частотного спектра  -Транспондер принимает, усиливает и передает далее сигнал на др. частоте (чтобы передаваемый сигнал не накладывался на прямой)  Различаются :  - Шириной нисходящего луча  - Высотой орбиты (и периодом обращения)  Геостационарные спутники  -Про спутники, находящие на большой высоте говорят, что они расположены на геостационарной орбиты  -несколько антенн и до 40 транспондеров; нисходящий луч может иметь малые размеры – до сотен километров  Средневысотные спутники  -Полный оборот за 6 часов  -Меньший диаметр луча  -Требуются менее мощные передатчики  Пример – спутники GPS  Низкоорбитальные спутники  -Большое количество спутников  -Высокая скорость движения по орбите  -Низкая мощность наземных передатчиков  -Низкие задержки (несколько миллисекунд)  Преимущества:  -Простота и скорость развертывания  -Зона покрытия  -Широковещательный режим передачи  Недостатки:  -Слабая помехозащищённость.  -Влияние атмосферы.  -Поглощение в тропосфере.  -Задержка распространения сигнала.  -Влияние солнечной интерференции |
| **17. Мобильная связь….**  Мобильная связь 1 поколения  -используется узкодиапазонная аналоговая мобильная сеть, которая позволяет совершать звонки и писать сообщения(предусмотрена система коммутации каналов).  -Скорость передачи 1,9 кбит/с  -связь возможна только в пределах страны  Мобильная связь 2 поколения  -используется узкодиапазонная беспроводная цифровая сеть, что делает связь более четкой  -Цифровое кодирование голоса делало возможным проверку цифровых ошибок, которая позволяла увеличить качество звука за счёт увеличения динамического диапазона и снижения уровня шума.  -Переход к цифровой системе способствовал внедрению цифровых сервисов данных, как SMS и e-mail  -2G телефоны намного более конфиденциальны, чем 1G, которые не имеют защиты от подслушивания.  Мобильная связь 3 поколения  используется система беспроводной сети. Данные передаются с помощью пакетной коммутации. Голосовые звонки интерпретируются через систему коммутации.  широкодиапазонный голосовой канал  3G сети (UMTS FDD and TDD, CDMA2000 1x EVDO и др.) –сотовые сети со скоростью передачи данных от 384 Кб/с до 42 Мб/сек.  Мобильная связь 4 поколения  4G сотовые системы должны иметь макс. скорость передачи данных до 100 Мбит/с для мобильного доступа и до 1 Гбит/с для переменного или местного доступа  Мобильная связь 5 поколения  скорость 100 Мбит/с и более.  Повышение энергоэффективности  Сокращение временной задержки на радиоинтерфейсе  Увеличение общего числа подключенных устройств до 1 млн./км2.  MSC (Mobile Switching Center) - коммутатор мобильных сетей связи 1G и 2G. Гл. ф-я - коммутация (соединение) сигналов подсистемы базовых станций и внешних сетей.  BSS (Base Station System) – система базовых станций сотовой связи стандарта GSM. Задача: уст-е, поддержание и разруш-е соед-я между MS (Mobile station) и NSS (Network Switching System).  Принцип сотовой связи: повторное исп-е частот в несмежных сотах.  Сотовая топология позволяет многократно увеличить абонентскую емкость системы и охватить сколь угодно большую зону обслуживания без ухудшения качества связи. Сложность: определение текущего местоположения мобильного абонента и обеспечение непрерывности связи при перемещении его из одной соты в другую. Соответствующая процедура получила название Handoff. | **18. Представление аналогового сигнала в цифровом виде. ...**  Одной из основных тенденций - передача в одной сети как дискретных, так и аналоговых по своей природе сигналов. Изначально все типы данных передавались сигналами в аналоговой форме; дискретные данные преобразовывались в аналоговую форму при помощи модемов. Передача данных в аналоговой форме не позволяет улучшить качество принятых на другом конце линии данных, если они существенно исказились при передаче; аналоговый сигнал не дает никаких указаний ни о том, что произошло искажение, ни о том, как его исправить  Дискретизация – преобразование функции непрерывного времени в функцию дискретного времени, т.е. замена непрерывной функции ее отдельными значениями  Дискретизация может быть равномерной и неравномерной. Наиболее часто применяется равномерная дискретизация – длительность интервалов между отсчетами постоянна и выбирается в соответствии с теоремой Котельникова (Найквиста-Котельникова): аналоговая непрерывная функция, переданная в виде последовательности ее дискретных по времени значений, может быть точно восстановлена, если частота дискретизации в два или более раз выше, чем частота самой высокой гармоники спектра исходной функции  Квантование – преобразование некоторой величины с непрерывной шкалой значений в величину, имеющую дискретную шкалу значений. Весь диапазон значений сигнала, называемый шкалой, делится на равные части – кванты, h – шаг квантования. Процесс квантования сводится к замене любого мгновенного значения одним из множества разрешенных значений, называемых уровнями квантования  По линии связи передаются не значения амплитуды, а номера уровней сигнала – импульсно-кодовая модуляция, ИКМ. Дискретизированное значение сигнала, находящееся между двумя уровнями квантования, отождествляется либо с ближайшим уровнем квантования, либо с ближайшим меньшим уровнем квантования. Это приводит к ошибкам квантования. Чем меньше шаг квантования, тем меньше ошибки квантования. Преобразование сигнала из аналоговой формы в цифровую форму осуществляется с помощью аналого-цифрового преобразователя, АЦП и обратное преобразование – с помощью цифро-аналогового преобразователя, ЦАП. Для удовлетворительного воспроизведения речи, достаточно 4096 уровней квантования сигнала (12 разрядов АЦП). 12-битные коды преобразуются в 8-битные и формируют поток в 64 Кбит/c с помощью логарифмического преобразования – разборчивость слуха снижается с увеличением громкости | **19. Основные методы повышения достоверности передачи….**  Кодовым расстоянием(d) - называется минимальное количество разрядов в которых одна кодовая комбинация отличается от другой кодовой комбинации.  Для конкретного кода кодовым расстоянием данного кода называется минимальное число элементов, которыми одна кодовая комбинация данного кода отличается от другой кодовой комбинации того же кода.  Иногда кодовое расстояние называется хемминговым расстоянием (по имени Ричарда Хемминга, основателя помехоустойчивых кодов).  Методы повышения верности приема информации  n Многократная передача кодовых комбинаций  n Одновременная передача кодовой комбинации по нескольким параллельно работающим каналам  n Использование корректирующих кодов, т.е. кодов, исправляющих ошибки  В обычном равномерном коде число разрядов в кодовых комбинациях определяется числом сообщений и основанием кода  Если произошла ошибка (даже одна), то принятая комбинация будет интерпретироваться приемником как кодовая комбинация, соответствующая другому символу. Все комбинации (32) являются разрешенными (допустимыми). Ошибки переводят одну разрешенную комбинацию в другую, также разрешенную. При помехоустойчивом кодировании в передаваемую кодовую комбинацию вводится избыточность (признаки разрешенной комбинации). Если на приемной стороне эти признаки в кодовой комбинации не обнаруживаются, то она считается принятой с ошибкой  Внесение избыточности всегда связано с увеличением числа разрядов (длины) кодовой комбинации n  Все множество N0 = 2n комбинаций можно разделить на два подмножества:  n разрешенных  n и запрещенных комбинаций  При использовании корректирующего кода передаются не все кодовые комбинации N0, которые можно сформировать из имеющегося числа разрядов n, а только разрешенные N < N0  n Если в результате искажений кодовая комбинация переходит в подмножество запрещенных, то ошибка будет обнаружена  n Однако если ошибки в кодовой комбинации превращают ее в какую-либо другую разрешенную, то ошибки обнаружены быть не могут  Поскольку любая из N разрешенных комбинаций может превращаться в N0 возможных, общее число таких случаев: N\*N0. Число случаев, в которых ошибка обнаруживается = N\*(N0 – N). Доля обнаруживаемых ошибочных комбинаций составит:  Большинство кодов предназначено для корректирования взаимно независимых ошибок определенной кратности и пачек (пакетов) ошибок. Кратностью ошибки называется количество искаженных символов в кодовой комбинации. При взаимно независимых ошибках наиболее вероятны ошибки низшей кратности. Наиболее вероятен переход в кодовую комбинацию, отличающуюся от данной в наименьшем числе символов  Степень отличия любых двух кодовых комбинаций характеризуется кодовым расстоянием (расстоянием Хемминга). Кодовое расстояние d выражается числом символов, в которых комбинации отличаются одна от другой. Чтобы получить кодовое расстояние между двумя комбинациями двоичного кода, достаточно посчитать число единиц в сумме этих комбинаций по модулю 2  Минимальное расстояние, взятое по всем парам кодовых разрешенных комбинаций кода, называют минимальным кодовым расстоянием  При минимальном кодовом расстоянии d = 1 все комбинации являются разрешенными.  При минимальном кодовом расстоянии = 2 ни одна из разрешенных кодовых комбинаций не переходит в другую разрешенную  Для обнаружения ошибки кратности до r0 включительно должно выполняться условие d>=r0 +1  Для исправления ru – кратной ошибки необходимо, чтобы новая кодовая комбинация не только не совпадала какой-либо разрешенной, но и оставалась ближе к правильной комбинации, чем любой другой разрешенной. | **20. Проверка по четности и код Хемминга**  Самый простой способ обнаружения ошибок – это проверка по чётности. Однако такой код позволяет только констатировать факт ошибки, а не исправлять её. Суть этого кода заключается в следующем: к битам передаваемого или хранимого M-разрядного слова добавляется еще один бит – бит четности, значение которого подбирается так, чтобы среди получившихся N = M + 1 разрядов обязательно было четное число единиц.  Код Хэмминга был один из самых первых обоснованных и использованных на практике корректирующих кодов. Он представляет собой совокупность проверок на чётность и является одной из разновидностей более широкого семейства корректирующих кодов – циклических кодов.  Необходимое число добавочных разрядов определяется из соотношения 2N-M – 1 >= N, где М – количество разрядов в исходном кодовом слове, N – в результирующем; К = N-M – количество дополнительных битов четности. Все биты, номера которых равны степени 2 являются битами четности, остальные – информационными.    Каждый бит четности используется для контроля определенных разрядов. Содержимое бита устанавливается так, чтобы суммарное число единиц было четным. Код, образованный значениями контрольных разрядов, называют дополнительным кодом. Также дополнительный код можно получить инвертированием результата поразрядного сложения (сложения по модулю 2) номеров тех разрядов, значения которых равны 1.  Предположим, один из бит искажен. В таком случае номер искаженного разряда определяется суммой номеров неправильных бит четности. |
|  |  |  |  |
| **21. Алгоритмы сжатия информации; понятие степени сжатия; основные виды алгоритмов: адаптивные и неадаптивные; с потерями и без потерь. Алгоритмы RLE, разностного кодирования, Хаффмена**  Алгоритмы сжатия информации. Алгоритмы сжатия информации подразделяются на два типа: симметричные и ассиметричные. Симметричные алгоритмы используют аналогичные методы для сжатия и распаковки данных. В программах обмена данными, которые осуществляют и сжатие, и распаковку, обычно используются именно эти алгоритмы. Асимметричные алгоритмы используют разные методы для работы в разных направлениях, при сжатии и распаковке.  o Обычно больше времени и ресурсов затрачивается на сжатие для максимально компактного хранения  o При резервном копировании, наоборот, сжатие необходимо осуществлять быстрее, чем распаковку, которую, возможно, вообще не придется производить  Понятие степени сжатия. Степень сжатия – это показатель оценки эффективности методов сжатия, который определяет отношения объёма несжатых данных к объёму сжатых.  Основные виды алгоритмов.  Ø Адаптивные алгоритмы: не зависят от типа обрабатываемых данных и строят словари динамически только на основе поступивших для сжатия данных  Ø Неадаптивные алгоритмы: используют для сжатия данных только определённых типов, они содержат статический словарь предопределенных подстрок, о которых известно, что они встречаются достаточно часто в исходных данных.  Ø Алгоритмы сжатия с потерей информации: (обычно потери малосущественные) они используются для сжатия изображений, звука и т.п.  Ø Алгоритмы сжатия без потери информации: используются для сжатия разнообразных данных, текстов и т.п.  Алгоритм RLE. Алгоритм Run Length Encoding основан на замене цепочки одинаковых символов символом и значением длины цепочки. Например, символьная группа из восьми символов АААААААА, занимающая восемь байт, после RLE кодирования будет представлена двумя символами 8A и занимать два байта. Этот алгоритм может применяться для сжатия изображений. Однако он не эффективен для текста.  Алгоритм разностного кодирования. Разности амплитуд представляются меньшим числом разрядов, чем значения самих амплитуд. Если текущее значение отличается от экстраполированного более, чем на допустимую погрешность, то передатчик это значение передает. В противном случае значение не передается, и приемник использует экстраполированное значение.  Алгоритм Хаффмена.  1) Часто повторяющиеся символы кодируются более короткими цепочками бит, чем редко встречающиеся. 2) Строится двоичное дерево, листья соответствуют кодируемым символам, код символа представляется последовательностью значений ребер (0, 1). Листья символов с высокой вероятностью находятся ближе к корню, чем листья маловероятных символов. 3) Данный алгоритм широко применяется для факсимильной передачи. 4) Неадаптивный метод, как правило, основан на фиксированном словаре. | **22. Управление доступом к общей среде передачи. Преимущества и недостатки широковещательных сетей; чистая и дискретная системы ALOHA, варианты протоколов CSMA, отличия протокола CSMA/CD**  Управление доступом к общей среде передачи. Все сетевые технологии могут быть разделены на соединения от узла к узлу и с применением широковещания. Основная проблема широковещательных сетей – кому предоставить канал. Пользоваться каналом могут одновременно несколько компьютеров.  Преимущества и недостатки широковещательных сетей. Широковещательные каналы также называют каналами с множественным доступом или каналами с произвольным доступом. Множественный доступ преимущественно используется в локальных сетях.  Плюсы: простота и гарантированность доступа. Минусы: неэффективное использования канала  Чистая и дискретная система ALOHA.  Чистая система ALOHA, её отличительные признаки: пользователи могут осуществлять передачу как только у них появляются данные для отправки. При коллизии кадры теряются. Благодаря обратной связи каждый отправитель может установить, дошел ли до получателя его кадр или был потерян. Если же кадр был потерян, отправитель повторяет попытку передачи спустя случайное время. Максимальная производительность – 18% от пропускной способности.  Дискретная система ALOHA, её отличительные признаки: время делится на дискретные интервалы, соответствующие времени одного кадра. Компьютер может передавать данные только в начале нового такта. Максимальная производительность = 1/e = 37% от пропускной способности, т.е. 37% интервалов будут пустыми, 37% - с успешно переданными кадрами, а 26% - коллизий. С увеличением количества попыток передачи в единицу времени количество пустых интервалов уменьшается, но увеличивается количество конфликтов  Варианты протоколов CSMA. CSMA (Carrier Sense Multiple Access) – множественный доступ с контролем несущей.  Ø CSMA с настойчивостью 1: при наличии данных станция сначала прослушивает канал, проверяя, свободен он или нет. Если канал занят, то станция ожидает его освобождения. При освобождении канала станция передает кадр (не начиная прослушивание). Если происходит коллизия, станция ожидает в течение случайного интервала времени, затем снова начинает прослушивать канал. Такой протокол называется CSMA с настойчивостью 1, так как станция посылает кадр с вероятностью 1, как только обнаружит, что канал свободен. Большое влияние оказывает задержка распространения сигнала – если первая станция начала передачу, то вторая тоже может начать, если сигнал не достиг нее.  Ø Ненастойчивый протокол CSMA: прежде чем начать передачу, станция опрашивает канал. Если никто не передает, станция начинает передачу. Если канал занят, станция  не ждет освобождения канала, постоянно его прослушивая и пытаясь сразу захватить, а ждет в течение случайного интервала времени, затем снова прослушивает линию. Такой алгоритм приводит к лучшему использованию канала, но большим задержкам  Ø Протокол CSMA с настойчивостью p: применяется в дискретных каналах. Когда станция готова, она опрашивает канал. Если канал свободен, то с вероятностью p она начинает передачу. С вероятностью (1-p) она отказывается от передачи и ждет начала следующего такта. Этот процесс повторяется до тех пор, пока кадр не будет передан или какая-либо другая станция не начнет передачу  Отличия протокола CSMA/CD CSMA/CD (Carrier Sense Multiple Access with Collision Detection – множественный доступ с контролем несущей и обнаружением конфликтов)  Следующим шагом является прекращение передачи станцией при обнаружении конфликта. То есть, если две станции, обнаружив, что канал свободен, одновременно начали передачу, они практически немедленно обнаруживают коллизию. Вместо того, чтобы продолжать передачу кадра, которые уже не могут быть приняты получателем, они прекращают передачу. Таким образом, экономится время и улучшается производительность каналов. | **27.Протоколы ARP и RARP**  Для определения локального адреса по IP-адресу используется протокол разрешения адресов (Address Resolution Protocol, ARP).  Для того, чтобы 2 машины в какой-либо сети могли обмениваться данными, им необходимо знать физические (MAC) адреса другой машины  •Посылая широковещательный запрос ARP, устройство может динамически определять соответствие адресов MAC уровня IP адресам  •Полученные MAC адреса сохраняются в ARP кэше во избежание повторных широковещательных ARP запросов  В ARP-таблицах существуют два типа записей: динамические и статические. Статические записи создаются вручную с помощью утилиты агр и не имеют срока устаревания, точнее, они существуют до тех пор, пока компьютер или маршрутизатор остается включенным. Динамические записи должны периодически обновляться. Если запись не обновлялась в течение определенного времени (порядка нескольких минут), то она исключается из таблицы. Таким образом, в ARP-таблице содержатся записи не обо всех узлах сети, а только о тех, которые активно участвуют в сетевых операциях. Поскольку такой способ хранения информации называют кэшированием, ARP-таблицы иногда называют ARP-кэшем.  •Протокол RARP (Reverse ARP) позволяет по MAC адресу определить IP адрес  В некоторых случаях возникает обратная задача — нахождение IP-адреса по известному локальному адресу. Тогда в действие вступает реверсивный протокол разрешения адресов (Reverse Address Resolution Protocol, RARP). Этот протокол используется, например, при старте бездисковых станций, не знающих в начальный момент времени своего 1Р-адреса, но знающих МАС-адрес своего сетевого адаптера. | **28. Протокол ICMP, основные команды**  · Протокол ICMP (IP Control Message Protocol) – протокол сетевого уровня, позволяющий передавать сообщения об ошибках и другую информацию, связанную с обработкой IP пакетов  Задача ICMP другая — он является средством оповещения отправителя о «несчастных случаях», произошедших с его пакетами. Пусть, например, протокол IP, работающий на каком-либо маршрутизаторе, обнаружил, что пакет для дальнейшей передачи по маршруту необходимо фрагментировать, но в пакете установлен признак DF (не фрагментировать). Протокол IP, обнаруживший, что не может передать IP-пакет далее по сети, прежде чем отбросить пакет, должен отправить диагностическое ICM P-сообщение конечному узлу-источнику.  · ICMP описан в RFC 792  Протокол ICMP определяет несколько типов сообщений: •Destination Unreachable •Echo Request / Echo Reply •Redirect •Time Exceeded •Router-Advertisement / Router Solicitation  CMP Destination Unreachable  •Посылается маршрутизатором если тот не может послать пакет по назначению -Либо указан несуществующий адрес -Либо у маршрутизатора нет маршрута к получателю •ICMP Echo Request / Echo Reply -Echo request генерируется командой ping -Echo reply посылается в ответ на Echo request и является признаком того, что узел доступен •ICMP Time-exceeded -Поле Time-to-live (предохраняет от бесконечного зацикливания пакетов) достигло нуля; пакет был отброшен |
| **29. Протокол TCP….**  Transmission Control Protocol (TCP)  •Обеспечивает надежную передачу данных в IP среде  •Соответствует 4-му уровню модели OSI  •Обеспечивает  •Потоковую передачу данных  •Надежность  •Эффективное управление потоком  •Полнодуплексный режим работы  •Мультиплексирование  Потоковая передача данных (stream data transfer) обеспечивает неструктурированный поток байт, идентифицируемых номером последовательности•При этом приложение не должно разбивать данные на блоки перед передачей их TCP, - TCP объединяет байты в сегменты и передает их IP для доставки  1.Надежность обеспечивается ориентированной на соединение, надежной из конца в конец передачей пакетов по сети•Это решается нумерацией передаваемых байт и передачей прямого номера подтверждения, показывающего получателю номер следующего байта, который источник ожидает получить.  2. Управление потоком (flow control) – при отправке подтверждений, принимающий TCP процесс показывает максимальный порядковый номер, который он может получить без переполнения его внутренних буферов  3.Полнодуплексная передача – TCP процесс может одновременно отправлять и получать данные  4.Мультиплексирование – множественные потоки данных верхних уровней могут передаваться по одному соединению  Для надежного транспортного сервиса TCP узлы должны установить ориентированный на соединение сеанс друг с другом  •Выполняется с помощью механизма «тройного рукопожатия» («three-way handshake»)  •Предназначен для выбора обеими сторонами начальных порядковых номеров  •Также гарантирует что обе стороны готовы к передаче данных и уведомлены о готовности другой стороны  •Исключает возможность передачи данных во время установления соединения или после его завершения  Заголовок TCP  •Порядковый номер – номер первого байта данных в текущем сообщении  •Номер подтверждения – порядковый номер следующего байта, который ожидает получить отправитель сообщения  Заголовок TCP  •Длина заголовка (смещение данных) – количество 32-битных слов в TCP заголовке  •Флаги – управляющая информация, в том числе SYN и ACK биты, необходимые для установления соединения, FIN – для его завершения, RST – для сброса  •Окно – определяет размер окна отправителя (т.е.размер его буфера)  •Контрольная сумма – показывает, не было ли ошибок при передаче  •Указатель на срочные данные – указатель на первый байт срочных данных в пакете  •Параметры – различные дополнительные параметры TCP  •Данные – информация верхних уровней  Протокол UDP (User Datagram Protocol) – протокол транспортного (4-го) уровня без установления соединения из семейства интернет-протоколов  •Порты UDP протокола позволяют различать несколько программ, выполняемых на одном узле друг от друга  •В отличие от TCP, UDP не обеспечивает надежности, управления потоком или восстановления после ошибок  •Заголовок UDP содержит меньше байт и расходует меньшую полосу, чем TCP  •Применяется когда нет необходимости в механизмах надежности TCP, например, когда они обеспечены протоколами верхних уровней  Заголовок UDP содержит 4 поля:  •Порты отправителя и получателя  •Аналогично TCP, но независимы  •Длина – длина заголовка и данных  •Контрольная сумма – контроль целостности заголовка и данных | **23. Сети Ethernet; управление доступом к среде CSMA/CD, формат MAC адреса; основные поля пакета Ethernet; обозначения сетей Ethernet, причины популярностиЛокальная сеть** — семейство технологий [пакетной](https://ru.wikipedia.org/wiki/%D0%9F%D0%B0%D0%BA%D0%B5%D1%82_(%D1%81%D0%B5%D1%82%D0%B5%D0%B2%D1%8B%D0%B5_%D1%82%D0%B5%D1%85%D0%BD%D0%BE%D0%BB%D0%BE%D0%B3%D0%B8%D0%B8)) передачи данных между устройствами для [компьютерных](https://ru.wikipedia.org/wiki/%D0%9A%D0%BE%D0%BC%D0%BF%D1%8C%D1%8E%D1%82%D0%B5%D1%80%D0%BD%D0%B0%D1%8F_%D1%81%D0%B5%D1%82%D1%8C) и [промышленных](https://ru.wikipedia.org/wiki/%D0%9F%D1%80%D0%BE%D0%BC%D1%8B%D1%88%D0%BB%D0%B5%D0%BD%D0%BD%D0%B0%D1%8F_%D1%81%D0%B5%D1%82%D1%8C) сетей. Стандарты Ethernet определяют проводные соединения и электрические сигналы на [физическом уровне](https://ru.wikipedia.org/wiki/%D0%A4%D0%B8%D0%B7%D0%B8%D1%87%D0%B5%D1%81%D0%BA%D0%B8%D0%B9_%D1%83%D1%80%D0%BE%D0%B2%D0%B5%D0%BD%D1%8C), формат [кадров](https://ru.wikipedia.org/wiki/%D0%9A%D0%B0%D0%B4%D1%80_(%D1%82%D0%B5%D0%BB%D0%B5%D0%BA%D0%BE%D0%BC%D0%BC%D1%83%D0%BD%D0%B8%D0%BA%D0%B0%D1%86%D0%B8%D0%B8)) и протоколы управления доступом к среде — на [канальном уровне](https://ru.wikipedia.org/wiki/%D0%9A%D0%B0%D0%BD%D0%B0%D0%BB%D1%8C%D0%BD%D1%8B%D0%B9_%D1%83%D1%80%D0%BE%D0%B2%D0%B5%D0%BD%D1%8C) [модели OSI](https://ru.wikipedia.org/wiki/%D0%A1%D0%B5%D1%82%D0%B5%D0%B2%D0%B0%D1%8F_%D0%BC%D0%BE%D0%B4%D0%B5%D0%BB%D1%8C_OSI). Ethernet в основном описывается стандартами [IEEE](https://ru.wikipedia.org/wiki/%D0%98%D0%BD%D1%81%D1%82%D0%B8%D1%82%D1%83%D1%82_%D0%B8%D0%BD%D0%B6%D0%B5%D0%BD%D0%B5%D1%80%D0%BE%D0%B2_%D1%8D%D0%BB%D0%B5%D0%BA%D1%82%D1%80%D0%BE%D1%82%D0%B5%D1%85%D0%BD%D0%B8%D0%BA%D0%B8_%D0%B8_%D1%8D%D0%BB%D0%B5%D0%BA%D1%82%D1%80%D0%BE%D0%BD%D0%B8%D0%BA%D0%B8) [группы 802.3](https://ru.wikipedia.org/wiki/IEEE_802.3)  *Ether – эфир, среда*  *1970-е годы, Xerox*  Определен в стандарте IEEE 802.3 (и дополнениях)  IEEE – Institute of Electrical and Electronic Engineers  Скорости передачи  10 Мб/c  100 Мб/с – Fast Ethernet  1000 Мб/с – Gigabit Ethernet – IEEE 802.3z  *10-Gigabit Ethernet – IEEE 802.3ae*  **Управление доступом к среде CSMA/CD**  Метод CSMA/CD доступа:  Carrier Sense  Multiple Access  Collision Detect  **CSMA/CD**  — технология (IEEE 802.3) множественного доступа к общей передающей среде в [локальной компьютерной сети](https://ru.wikipedia.org/wiki/%D0%9B%D0%92%D0%A1) с контролем [коллизий](https://ru.wikipedia.org/wiki/%D0%9A%D0%BE%D0%BB%D0%BB%D0%B8%D0%B7%D0%B8%D1%8F_%D0%BA%D0%B0%D0%B4%D1%80%D0%BE%D0%B2). CSMA/CD относится к децентрализованным случайным (точнее, квазислучайным) методам. Он используется как в обычных сетях типа [Ethernet](https://ru.wikipedia.org/wiki/Ethernet" \o "Ethernet), так и в высокоскоростных сетях ([Fast Ethernet](https://ru.wikipedia.org/wiki/Fast_Ethernet" \o "Fast Ethernet), [Gigabit Ethernet](https://ru.wikipedia.org/wiki/Gigabit_Ethernet" \o "Gigabit Ethernet)). Так же называют [сетевой протокол](https://ru.wikipedia.org/wiki/%D0%A1%D0%B5%D1%82%D0%B5%D0%B2%D0%BE%D0%B9_%D0%BF%D1%80%D0%BE%D1%82%D0%BE%D0%BA%D0%BE%D0%BB), в котором используется схема CSMA/CD. Протокол CSMA/CD работает на [канальном уровне](https://ru.wikipedia.org/wiki/%D0%9A%D0%B0%D0%BD%D0%B0%D0%BB%D1%8C%D0%BD%D1%8B%D0%B9_%D1%83%D1%80%D0%BE%D0%B2%D0%B5%D0%BD%D1%8C) в модели [OSI](https://ru.wikipedia.org/wiki/Open_Systems_Interconnection). Характеристики и области применения этих популярных на практике сетей связаны именно с особенностями используемого метода доступа.  Если во время передачи кадра рабочая станция обнаруживает другой сигнал, занимающий передающую среду, она останавливает передачу, посылает [сигнал преднамеренной помехи](https://ru.wikipedia.org/wiki/Jam_signal) и ждёт в течение случайного промежутка [времени](https://ru.wikipedia.org/wiki/%D0%92%D1%80%D0%B5%D0%BC%D1%8F) (известного как «backoff delay» и находимого с помощью [экспоненциального двоичного алгоритма выдержки](https://ru.wikipedia.org/wiki/%D0%AD%D0%BA%D1%81%D0%BF%D0%BE%D0%BD%D0%B5%D0%BD%D1%86%D0%B8%D0%B0%D0%BB%D1%8C%D0%BD%D0%B0%D1%8F_%D0%B2%D1%8B%D0%B4%D0%B5%D1%80%D0%B6%D0%BA%D0%B0)), перед тем как снова отправить кадр.  Обнаружение коллизий используется для улучшения производительности CSMA с помощью прерывания передачи сразу после обнаружения коллизии и снижения вероятности второй коллизии во время повторной передачи.  Методы обнаружения коллизий зависят от используемого оборудования, но на электрических шинах, таких как Ethernet, коллизии могут быть обнаружены сравнением передаваемой и получаемой информации. Если она различается, то другая передача накладывается на текущую (возникла коллизия) и передача прерывается немедленно. Посылается сигнал преднамеренной помехи, что вызывает задержку передачи всех передатчиков на произвольный интервал времени, снижая вероятность коллизии во время повторной попытки.  [Ethernet](https://ru.wikipedia.org/wiki/Ethernet) является классическим примером протокола CSMA/CD.  **Формат МАС адреса**  **MAC-адрес** — уникальный идентификатор, присваиваемый каждой [единице активного оборудования](https://ru.wikipedia.org/wiki/%D0%9E%D0%BA%D0%BE%D0%BD%D0%B5%D1%87%D0%BD%D0%BE%D0%B5_%D0%BE%D0%B1%D0%BE%D1%80%D1%83%D0%B4%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5_%D0%B4%D0%B0%D0%BD%D0%BD%D1%8B%D1%85) или некоторым их интерфейсам в [компьютерных сетях](https://ru.wikipedia.org/wiki/%D0%9A%D0%BE%D0%BC%D0%BF%D1%8C%D1%8E%D1%82%D0%B5%D1%80%D0%BD%D0%B0%D1%8F_%D1%81%D0%B5%D1%82%D1%8C) [Ethernet](https://ru.wikipedia.org/wiki/Ethernet" \o "Ethernet).  В широковещательных сетях (таких, как сети на основе [Ethernet](https://ru.wikipedia.org/wiki/Ethernet" \o "Ethernet)) MAC-адрес позволяет уникально идентифицировать каждый [узел сети](https://ru.wikipedia.org/wiki/%D0%A3%D0%B7%D0%B5%D0%BB_%D1%81%D0%B5%D1%82%D0%B8) и доставлять данные только этому узлу. Таким образом, MAC-адреса формируют основу сетей на [канальном уровне](https://ru.wikipedia.org/wiki/%D0%9A%D0%B0%D0%BD%D0%B0%D0%BB%D1%8C%D0%BD%D1%8B%D0%B9_%D1%83%D1%80%D0%BE%D0%B2%D0%B5%D0%BD%D1%8C) модели [OSI](https://ru.wikipedia.org/wiki/%D0%A1%D0%B5%D1%82%D0%B5%D0%B2%D0%B0%D1%8F_%D0%BC%D0%BE%D0%B4%D0%B5%D0%BB%D1%8C_OSI), которую используют протоколы более высокого ([сетевого](https://ru.wikipedia.org/wiki/%D0%A1%D0%B5%D1%82%D0%B5%D0%B2%D0%BE%D0%B9_%D1%83%D1%80%D0%BE%D0%B2%D0%B5%D0%BD%D1%8C)) уровня. Для преобразования MAC-адресов в адреса сетевого уровня и обратно применяются специальные протоколы (например, [ARP](https://ru.wikipedia.org/wiki/ARP) и [RARP](https://ru.wikipedia.org/wiki/RARP) в сетях [IPv4](https://ru.wikipedia.org/wiki/IPv4), и [NDP](https://ru.wikipedia.org/wiki/Neighbor_Discovery_Protocol) в сетях на основе [IPv6](https://ru.wikipedia.org/wiki/IPv6)).  **Преамбула** – 7 байт, содержащих последовательность «10101010»  -Манчестерское кодирование такой последовательности дает прямоугольные импульсы с частотой 10 МГц и длительностью 6,4 мкс, что позволяет получателю синхронизировать часы  **Разграничитель начала кадра** – 1 байт, определяет завершение преамбулы и начало кадра  -Как и преамбула, состоит из чередующихся «1» и «0», но завершается «11»  -Необходим для совместимости с другим стандартами  **Длина/тип** – 2 байта  -либо количество байт данных, содержащихся в поле данных (если значение <=1500)  -Либо тип кадра (для специальных форматов, если значение > 1536  **Данные** – n байт, n <=1500: Если длина < 46, до дополняется до 46 байт  **Контрольная сумма** – 4 байта  -32-битный циклический код  -Создается отправителем  -Проверяется получателем для обнаружения поврежденных фреймов  Основные поля пакета:  В пакет Ethernet входят следующие поля: Преамбула состоит из 8 байт, первые семь из которых представляют собой код 10101010, а последний восьмой – код 10101011. В стандарте IEEE 802.3 этот последний байт называется признаком начала кадра (SFD – Start of Frame Delimiter) и образует отдельное поле пакета. Адрес получателя (приемника) и адрес отправителя (передатчика) включают по 6 байт и строятся по стандарту, описанному в разделе 3.2. Эти адресные поля обрабатываются аппаратурой абонентов. Поле управления (L/T – Length/Type) содержит информацию о длине поля данных. Оно может также определять тип используемого протокола. Принято считать, что если значение этого поля не больше 1500, то оно определяет длину поля данных. Если же его значение больше 1500, то оно определяет тип кадра. Поле управления обрабатывается программно. Поле данных должно включать в себя от 46 до 1500 байт данных. Если пакет должен содержать менее 46 байт данных, то поле данных дополняется байтами заполнения. Согласно стандарту IEEE 802.3, в структуре пакета выделяется специальное поле заполнения (pad data – незначащие данные), которое может иметь нулевую длину, когда данных достаточно (больше 46 байт). Поле контрольной суммы (FCS – Frame Check Sequence) содержит 32-разрядную циклическую контрольную сумму пакета (CRC) и служит для проверки правильности передачи пакета.  Причины популярности Ethernet   * Простота * Надежность * Невысокая цена * Легкость обслуживания * Хорошее взаимодействие с TCP/IP – доминирующем протоколом Интернет * Нет установления соединения (в отличие от АТМ) | **24. Стек протоколов TCP/IP; соответствие протоколов TCP/IP уровням модели ISO/OSI**  Стек TCP/IP – это набор иерархически упорядоченных сетевых протоколов. Название стек получил по двум важнейшим протоколам – TCP (Transmission Control Protocol) и IP (Internet Protocol). Помимо них в стек входят ещё несколько десятков различных протоколов. В настоящее время протоколы TCP/IP являются основными для Интернета, а также для большинства корпоративных и локальных сетей.  Стек протоколов сети TCP/IP имеет 4 уровня:  Канальный (Link).  Сетевой (Internet).  Транспортный (Transport).  Прикладной (Application).  **Прикладной уровень:**  Прикладной уровень обеспечивает возможность взаимодействия между приложением и другими уровнями стека протоколов, анализирует и преобразовывает поступающую информацию в формат, подходящий для программного обеспечения. Является ближайшим к пользователю и взаимодействует с ним напрямую.  Самые распространенные протоколы: HTTP; FTP; SMTP; DNS. Каждый протокол определяет собственный порядок и принципы работы с данными.  HTTP (HyperText Transfer Protocol) предназначен для передачи данных. По нему отправляются, например, документы в формате HTML, которые служат основой веб-страницы. Упрощенно схема работы представляется как «клиент – сервер». Клиент отправляет запрос, сервер его принимает, должным образом обрабатывает и возвращает конечный результат.  FTP (File Transfer Protocol) служит стандартом передачи файлов в сети. Клиент посылает запрос на некий файл, сервер ищет этот файл в своей базе и при успешном обнаружении отправляет его как ответ.  SMTP (Simple Mail Transfer Protocol) используется для передачи электронной почты. SMTP-операция включает в себя три последовательных шага: Определение адреса отправителя. Это необходимо для возвращения писем. Определение получателя. Этот шаг может повторяться некоторое количество раз при указании нескольких адресатов. Определение содержимого сообщения и отправка. В качестве служебной информации передаются данные о типе сообщения. Если сервер подтверждает готовность принять пакет, то совершается сама транзакция  **Транспортный уровень**  На транспортном уровне полученная информация обрабатывается как единый блок, вне зависимости от содержимого. Полученные сообщения делятся на сегменты, к ним добавляется заголовок, и все это отправляется ниже. Протоколы передачи данных: TCP; UDP.  TCP (Transmission Control Protocol) - самый распространенный протокол. Он отвечает за гарантированную передачу данных. При отправке пакетов контролируется их контрольная сумма, процесс транзакции. Это значит, что информация дойдет «в целости и сохранности» независимо от условий.  UDP (User Datagram Protocol) - второй по популярности протокол. Он также отвечает за передачу данных. Отличительное свойство кроется в его простоте. Пакеты просто отправляются, не создавая особенной связи.  **Сетевой уровень**  Сетевой уровень из полученной информации образует пакеты и добавляет заголовок. Наиболее важной частью данных являются IP и MAC-адреса отправителей и получателей.  IP-адрес (Internet Protocol address) – логический адрес устройства. Содержит информацию о местоположении устройства в сети. Пример записи: [192.168.33.4]. MAC-адрес (Media Access Control address) – физический адрес устройства. Используется для идентификации. Присваивается сетевому оборудованию на этапе изготовления. Представлен как шестибайтный номер. Например: [08-00-27-AB-0E-25]. Сетевой уровень отвечает за: Определение маршрутов доставки. Передачу пакетов между сетями. Присвоение уникальных адресов.  Маршрутизаторы - устройства сетевого уровня. Они прокладывают путь между компьютером и сервером на основе полученных данных.  Самый популярный протокол этого уровня – IP.  IP (Internet Protocol) - интернет-протокол, предназначенный для адресации в сети. Используется для построения маршрутов, по которым происходит обмен пакетами. Не обладает никакими средствами проверки и подтверждения целостности. Для обеспечения гарантий доставки используется TCP, который использует IP в качестве транспортного протокола. Понимание принципов этой транзакции во многом объясняет основу того, как работает стек протоколов TCP/IP.  **Канальный уровень**  На канальном уровне определяется взаимосвязь между устройством и физической средой передачи, добавляется заголовок. Отвечает за кодировку данных и подготовку фреймов для передачи по физической среде. На этом уровне работают сетевые коммутаторы. Самые распространенные протоколы: Ethernet. WLAN.  Ethernet – наиболее распространенная технология проводных локальных сетей.  WLAN – локальная сеть на основе беспроводных технологий. Взаимодействие устройств происходит без физических кабельных соединений. Пример самого распространенного метода – Wi-Fi. | **25. Протокол IP. Назначение, основные задачи; уровень модели ISO/OSI; фрагментация и сборка пакетов, основные поля заголовка IP**  Протокол сетевого (3-го) уровня, содержащий информацию об адресации и управляющую информацию, необходимую для маршрутизации пакетов.  Протокол IP описан в RFC 791 и является основным протоколом сетевого уровня в стеке TCP/IP.  Вместе с протоколом TCP (Transmission Control Protocol), IP представляет основу всех Интернет протоколов.  Основные задачи:  -Доставка дейтаграмм без установления соединения  -Фрагментация и сборка дейтаграмм для поддержки каналов с различным MTU  -MTU – Maximum Transmission Unit, максимальная единица передачи  IP объединяет сегменты сети в единую сеть, обеспечивая доставку пакетов данных между любыми узлами сети через произвольное число промежуточных узлов ([маршрутизаторов](https://ru.wikipedia.org/wiki/%D0%9C%D0%B0%D1%80%D1%88%D1%80%D1%83%D1%82%D0%B8%D0%B7%D0%B0%D1%82%D0%BE%D1%80)). Он классифицируется как протокол [сетевого](https://ru.wikipedia.org/wiki/%D0%9F%D1%80%D0%BE%D1%82%D0%BE%D0%BA%D0%BE%D0%BB%D1%8B_%D1%81%D0%B5%D1%82%D0%B5%D0%B2%D0%BE%D0%B3%D0%BE_%D1%83%D1%80%D0%BE%D0%B2%D0%BD%D1%8F) уровня по [сетевой модели OSI](https://ru.wikipedia.org/wiki/%D0%A1%D0%B5%D1%82%D0%B5%D0%B2%D0%B0%D1%8F_%D0%BC%D0%BE%D0%B4%D0%B5%D0%BB%D1%8C_OSI). IP не гарантирует надёжной доставки пакета до адресата — в частности, пакеты могут прийти не в том порядке, в котором были отправлены, продублироваться (приходят две копии одного пакета), оказаться повреждёнными (обычно повреждённые пакеты уничтожаются) или не прийти вовсе.  А вот при необходимости передать пакет в следующую сеть, для которой размер пакета является слишком большим, IP-фрагментация становится необходимой. В функции уровня IP входит разбиение слишком длинного для конкретного типа составляющей сети сообщения на более короткие пакеты с созданием соответствующих служебных полей, нужных для последующей сборки фрагментов в исходное сообщение.  -При фрагментации дейтаграмма разделяется на несколько частей  -Заголовок каждой из них содержит большую часть полей заголовка оригинальной дейтаграммы  -Поле данных – столько данных, чтобы общая длина дейтаграммы была < MTU и она могла быть передана по сети  -После того, как была произведена фрагментация, пакеты передаются как отдельные дейтаграммы на всём пути от точки фрагментации до получателя  IP-пакет состоит из заголовка и поля данных. Заголовок, как правило, имеющий длину 20 байт, имеет следующую структуру (рис. 14.1).  Поле *Номер версии (Version)*, занимающее 4 бит, указывает версию протокола IP. Сейчас повсеместно используется версия 4 (IPv4), и готовится переход на версию 6 (IPv6).  Поле *Длина заголовка (IHL)* IP-пакета занимает 4 бит и указывает значение длины заголовка, измеренное в 32-битовых словах. Обычно заголовок имеет длину в 20 байт (пять 32-битовых слов), но при увеличении объема служебной информации эта длина может быть увеличена за счет использования дополнительных байт в поле *Опции (IP Options)*. Наибольший заголовок занимает 60 октетов.  Поле *Тип сервиса (Type of Service)* занимает один байт и задает приоритетность пакета и вид критерия выбора маршрута. Первые три бита этого поля образуют подполе *приоритета* пакета *(Precedence)*. Приоритет может иметь значения от самого низкого - 0 (нормальный пакет) до самого высокого - 7 (пакет управляющей информации). Маршрутизаторы и компьютеры могут принимать во внимание приоритет пакета и обрабатывать более важные пакеты в первую очередь. Поле *Тип сервиса* содержит также три бита, определяющие критерий выбора маршрута. Реально выбор осуществляется между тремя альтернативами: малой задержкой, высокой достоверностью и высокой пропускной способностью. Установленный бит D (delay) говорит о том, что маршрут должен выбираться для минимизации задержки доставки данного пакета, бит Т - для максимизации пропускной способности, а бит R - для максимизации надежности доставки. Во многих сетях улучшение одного из этих параметров связано с ухудшением другого, кроме того, обработка каждого из них требует дополнительных вычислительных затрат. Поэтому редко, когда имеет смысл устанавливать одновременно хотя бы два из этих трех критериев выбора маршрута. Зарезервированные биты имеют нулевое значение.  Поле *Общая длина (Total Length)* занимает 2 байта и означает общую длину пакета с учетом заголовка и поля данных. Максимальная длина пакета ограничена разрядностью поля, определяющего эту величину, и составляет 65 535 байт, однако в большинстве хост-компьютеров и сетей столь большие пакеты не используются. При передаче по сетям различного типа длина пакета выбирается с учетом максимальной длины пакета протокола нижнего уровня, несущего IP-пакеты. Если это кадры Ethernet, то выбираются пакеты с максимальной длиной в 1500 байт, умещающиеся в поле данных кадра Ethernet. В стандарте предусматривается, что все хосты должны быть готовы принимать пакеты вплоть до 576 байт длиной (приходят ли они целиком или по фрагментам). Хостам рекомендуется отправлять пакеты размером более чем 576 байт, только если они уверены, что принимающий хост или промежуточная сеть готовы обслуживать пакеты такого размера.  Поле *Идентификатор пакета (Identification)* занимает 2 байта и используется для распознавания пакетов, образовавшихся путем фрагментации исходного пакета. Все фрагменты должны иметь одинаковое значение этого поля.  Поле *Флаги (Flags)* занимает 3 бита и содержит признаки, связанные с фрагментацией. Установленный бит DF (Do not Fragment) запрещает маршрутизатору фрагментировать данный пакет, а установленный бит MF (More Fragments) говорит о том, что данный пакет является промежуточным (не последним) фрагментом. Оставшийся бит зарезервирован.  Поле *Смещение фрагмента (Fragment Offset)* занимает 13 бит и задает смещение в байтах поля данных этого пакета от начала общего поля данных исходного пакета, подвергнутого фрагментации. Используется при сборке/разборке фрагментов пакетов при передачах их между сетями с различными величинами MTU. Смещение должно быть кратно 8 байт.  Поле *Время жизни (Time to Live)* занимает один байт и означает предельный срок, в течение которого пакет может перемещаться по сети. Время жизни данного пакета измеряется в секундах и задается источником передачи. На маршрутизаторах и в других узлах сети по истечении каждой секунды из текущего времени жизни вычитается единица; единица вычитается и в том случае, когда время задержки меньше секунды. Поскольку современные маршрутизаторы редко обрабатывают пакет дольше, чем за одну секунду, то время жизни можно считать равным максимальному числу узлов, которые разрешено пройти данному пакету до того сак он достигнет места назначения. Если параметр времени жизни станет нулевым до того, как пакет достигнет получателя, этот пакет будет уничтожен. Время жизни можно рассматривать как часовой механизм самоуничтожения. Значение этого поля изменяется при обработке заголовка IP-пакета.  Идентификатор *Протокол верхнего уровня (Protocol)* занимает один байт и указывает, какому протоколу верхнего уровня принадлежит информация, размещения в поле данных пакета (например, это могут быть сегменты протокола TCP (дейтаграммы UDP, пакеты ICMP или OSPF). Значения идентификаторов для различных протоколов приводятся в документе RFC “Assigned Numbers”.  *Контрольная сумма (Header Checksum)* занимает 2 байта и рассчитывается только по заголовку. Поскольку некоторые поля заголовка меняют свое значение в процессе передачи пакета по сети (например, время жизни), контрольная сумма проверяется и повторно рассчитывается при каждой обработке IP-заголовка. Контрольная сумма - 16 бит - подсчитывается как дополнение к сумме всех 16-битовых слов заголовка. При вычислении контрольной суммы значение самого поля “контрольная сумма” устанавливается в нуль. Если контрольная сумма неверна, о пакет будет отброшен, как только ошибка будет обнаружена.  Поля *IP-адрес источника (Source IP Address)* и *IP-адрес назначения (Destination Address)* имеют одинаковую длину - 32 бита - и одинаковую структуру.  Поле *Опции (IP Options)* является необязательным и используется обычно только при отладке сети. Механизм опций предоставляет функции управления, которые необходимы или просто полезны при определенных ситуациях, однако он не нужен при обычных коммуникациях. Это поле состоит из нескольких подполей, каждое из которых может быть одного из восьми предопределенных типов. В этих подполях можно указывать точный маршрут прохождения маршрутизаторов, регистрировать проходимые пакетом маршрутизаторы, помещать данные системы безопасности, а также временные отметки. Так как число подполей может быть произвольным, то в конце поля *Опции* должно быть добавлено несколько байт для выравнивания заголовка пакета по 32-битной границе.  Поле *Выравнивание (Padding)* используется для того, чтобы убедиться в том, то IP-заголовок заканчивается на 32-битной границе. Выравнивание осуществляется нулями. |
| **26. IP адресация, классы адресов, адреса хоста, сети, широковещательный. Формат адресов IPv6, причины появления IPv6**  Каждому устройству (хосту) в сети TCP/IP присваивается уникальный 32-битный логический адрес, состоящий из 2 частей:  -Адрес сети  -Адрес хоста  Номер сети уникально идентифицирует сеть и если сеть подключается к интернет, то этот номер должен присваиваться Internet Network Information Center (InterNIC)  Интернет-провайдеры получают блоки сетевых адресов и затем самостоятельно выделяют адресное пространство  Адрес хоста идентифицирует сетевое устройство (хост) и присваивается местным сетевым администратором  32 бита IP адреса группируются по 8 бит, разделенных точками и представляются в десятичной форме  В IP адресации выделяются классы IP адресов: A, B, C, D, E  Для коммерческого использования доступны классы A, B, C  Наиболее значащие биты (крайние левые) определяют класс сети  Классы IP адресов  IP сети могут делиться на меньшие сети, называемые подсетями. Это дает большую гибкость, более эффективное использование сетевых адресов и ограничение широковещательного трафика. Адреса подсетей получаются «отсечением» бит от поля хоста и добавлением их в поле подсети.  Адрес 127.0.0.1 и имя хоста localhost зарезервированы. Они указывают на виртуальный интерфейс, loopback. Все пакеты, отправленные на этот интерфейс, возвращаются назад, как будто были отправлены снаружи. *Wireshark перехватывает и отображает данные только на физических интерфейсах; пакеты, передающиеся по интерфейсу loopback, не будут в нем видны.*  Маршрутизатор для определения адреса сети:  -Выделяет IP адрес из поступившего пакета  -Получает внутреннюю сетевую маску интерфейса  -Выполняет логическое «И» для получения адреса сети. При этом адрес хоста удаляется, а адрес сети остается  -Сравнивает полученный адрес сети назначения и определяет исходящий интерфейс  -Направляет пакет получателю  IPv6 ([англ.](https://ru.wikipedia.org/wiki/%D0%90%D0%BD%D0%B3%D0%BB%D0%B8%D0%B9%D1%81%D0%BA%D0%B8%D0%B9_%D1%8F%D0%B7%D1%8B%D0%BA) *Internet Protocol version 6*) — новая версия интернет [протокола](https://ru.wikipedia.org/wiki/%D0%A1%D0%B5%D1%82%D0%B5%D0%B2%D0%BE%D0%B9_%D0%BF%D1%80%D0%BE%D1%82%D0%BE%D0%BA%D0%BE%D0%BB) ([IP](https://ru.wikipedia.org/wiki/IP)), призванная решить проблемы, с которыми столкнулась предыдущая версия ([IPv4](https://ru.wikipedia.org/wiki/IPv4)) при её использовании в [Интернете](https://ru.wikipedia.org/wiki/%D0%98%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82), за счёт использования длины адреса 128 [бит](https://ru.wikipedia.org/wiki/%D0%91%D0%B8%D1%82) вместо 32. Протокол был разработан [IETF](https://ru.wikipedia.org/wiki/IETF).  В 6-й версии IP-адрес ([IPv6](https://ru.wikipedia.org/wiki/IPv6)) является 128-[битовым](https://ru.wikipedia.org/wiki/%D0%91%D0%B8%D1%82). Внутри адреса разделителем является двоеточие (напр. 2001:0db8:85a3:0000:0000:8a2e:0370:7334)[[1]](https://ru.wikipedia.org/wiki/IP-%D0%B0%D0%B4%D1%80%D0%B5%D1%81#cite_note-:0-1). Ведущие нули допускается в записи опускать. Нулевые группы, идущие подряд, могут быть опущены, вместо них ставится двойное двоеточие (fe80:0:0:0:0:0:0:1 можно записать как fe80::1). Более одного такого пропуска в адресе не допускается.  Размер и формат адреса IPv6 расширяют возможности адресации.  В протоколе IPv6 размер адреса составляет 128 бит. Предпочтительным является следующее представление адреса IPv6: x:x:x:x:x:x:x:x, где каждая буква x - это шестнадцатиричные значения шести 16-битных элементов адреса. Диапазон адресов IPv6 составляет от 0000:0000:0000:0000:0000:0000:0000:0000 до ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff.  Помимо обычного формата, адреса IPv6 могут быть представлены в двух других форматах:  С пропуском начальных нулей  Адрес IPv6 записывается с пропуском начальных нулей. Например, адрес IPv6 1050:0000:0000:0000:0005:0600:300c:326b можно записать как 1050:0:0:0:5:600:300c:326b.  Двойное двоеточие  В адресе IPv6 на месте нескольких нулей ставится двойное двоеточие (::). Например, адрес IPv6 ff06:0:0:0:0:0:0:c3 можно записать как ff06::c3. В одном IP-адресе двойное двоеточие может использоваться только один раз.  В альтернативном формате адреса IPv6 совмещаются формат с двоеточиями и формат с точками, поэтому адреса IPv4 можно вставлять в адреса IPv6. В первых 96 битах указываются шестнадцатиричные значения, а в последних 32 битах указываются десятичные значения, задающие адрес IPv4. Такой формат обеспечивает совместимость между узлами IPv6 и IPv4.  Адрес IPv6, преобразованный для IPv4, использует альтернативный формат. Такие адреса представляют узлы IPv4 в сети IPv6. С их помощью приложение IPv6 может напрямую взаимодействовать с приложением IPv4. Например, 0:0:0:0:0:ffff:192.1.56.10 и ::ffff:192.1.56.10/96 (сокращенный формат). | **30. Механизм установления TCP соединения; механизм скользящего окна**  Transmission Control Protocol (TCP)  Обеспечивает надежную передачу данных в IP среде  Соответствует 4-му уровню модели OSI  Обеспечивает:  Потоковую передачу данных  Надежность  Эффективное управление потоком  Полнодуплексный режим работы  Мультиплексирование  Установление TCP соединения  Для надежного транспортного сервиса TCP узлы должны установить ориентированный на соединение сеанс друг с другом  Выполняется с помощью механизма «тройного рукопожатия» («three-way handshake»)  - Предназначен для выбора обеими сторонами начальных порядковых номеров  - Также гарантирует что обе стороны готовы к передаче данных и уведомлены о готовности другой стороны  - Исключает возможность передачи данных во время установления соединения или после его завершения  Последовательность операций:  Каждый узел случайно выбирает порядковый номер  Узел 1 инициирует соединение передачей пакета с начальным порядковым номером (x) и установленным битом SYN для индикации запроса на соединение  Узел 2 подтверждает SYN с значением ACK = x+1 и своим порядковым номером (y)  ACK = 20 означает, что узел получил байты с 0 по 19 и ожидает байт 20 следующим – это называется прямым подтверждением  Узел 1 подтверждает посланные узлом 2 байты прямым подтверждением с ACK = y+1  Передача данных может начинаться  Одновременная попытка установления соединения с обеих сторон: (картинка)    Позитивное подтверждение и повторная передача:  Позитивное подтверждение и повторная передача (Positive Acknowledgement and Retransmission)  Отправитель посылает пакет, стартует таймер и ожидает подтверждения до отправки нового пакета  Если подтверждение не получено до того, как истечет время таймера, отправитель повторяет передачу пакета  Присвоив каждому пакету порядковый номер, можно отслеживать потерянные и дублированные пакеты  Неэффективно, т.к.отправитель должен ожидать подтверждения до отправки последующего пакета, и отправка может осуществляться только по одному пакету  Скользящее окно TCP  Скользящее окно более эффективно использует сеть поскольку позволяет узлу отправлять более одного байта или пакета до получения подтверждения  Получатель сообщает отправителю текущий размер окна (в байтах) в каждом пакете  Размер окна – количество байт данных, которые отправитель может послать без подтверждения  Начальный размер окна определяется при установлении соединения  Окно определяет какое количество информации м.б. передано отправителем без ожидания подтверждения. При этом передаваемая информация представляется в виде потока сообщений, для которого транспортная служба гарантирует сохранение на стороне получателя порядка следования сообщений. | **31. Протокол UDP. Назначение, характеристики и задачи; уровень модели ISO/OSI. В каких случаях используется и почему?**  n Протокол UDP (User Datagram Protocol) – протокол транспортного (4-го) уровня без установления соединения из семейства интернет-протоколов. Порты UDP протокола позволяют различать несколько программ, выполняемых на одном узле друг от друга  Протокол UDP, подобно IP, является дейтаграммным протоколом. В отличие от TCP, UDP не обеспечивает надежности, управления потоком или восстановления после ошибок, он реализует так называемый ненадежный сервис по возможности, который не гарантирует доставку сообщений адресату.  При работе на хосте-отправителе данные от приложений поступают протоколу UDP через порт в виде сообщений. Протокол UDP добавляет к каждому отдельному сообщению свой 8-байтный заголовок, формируя из этих сообщений собственные протокольные единицы, называемые UDP-дейтаграммами, и передает их нижележащему протоколу IP. В этом и заключаются его функции по мультиплексированию данных.  n Заголовок UDP содержит меньше байт и расходует меньшую полосу, чем TCP  n Применяется, когда нет необходимости в механизмах надежности TCP, например, когда они обеспечены протоколами верхних уровней Пример – передача голоса по I | **32. Задачи маршрутизации. Понятие метрики. Отличие статических и динамических алгоритмов, одноуровневой и иерархической маршрутизации. Дистанционно-векторные алгоритмы и алгоритмы состояния связей**  **Маршрутизация включает в себя две основных задачи:**  Определение оптимального маршрута Передача информационных блоков (пакетов) по сети  Алгоритмы маршрутизации используют ***метрики*** для оценки того, какой путь будет наилучшим для доставки пакета до узла назначения например:  Длина пути (цена или количество промежуточных узлов) Полоса пропускания Надежность Задержка  Стоимость, ….  Алгоритмы маршрутизации поддерживают таблицы маршрутизации, содержащие информации о маршрутах  Маршрутизаторы взаимодействуют друг с другом для построения таблиц маршрутизации  ***Статические алгоритмы*** – не совсем корректно называть алгоритмами – это таблицы, определенные администратором Просты для дизайна Подходят для ситуации, когда сетевой трафик относительно предсказуем, а структура сети относительно проста Не могут реагировать на изменения в сети и не подходят для современных больших и постоянно изменяющихся сетей  ***Динамические алгоритмы*** – реагируют на изменения в сети, анализируя поступающие сообщения об изменении маршрутов и перестраивая таблицы маршрутизации  При **плоской, одноуровневой** маршрутизации все маршрутизаторы равнозначны  При иерархической маршрутизации часть маршрутизаторов является магистральными (backbone), остальные – второстепенными  Пакеты от второстепенных маршрутизаторов передаются магистральным, они пересылают их по магистрали до магистрального маршрутизатора, ближайшего к получателю; затем пакет передается второстепенными маршутизаторами до точки назначения  При иерархической маршрутизации часто выделяются группы узлов, называемые доменами, автономными системами или областями  Только часть маршрутизаторов в домене может взаимодействовать с маршрутизаторами другого домена; остальные взаимодействуют только с маршрутизаторами своего домена  Основное преимущество – построение иерархии, аналогичной организационной; домены соответствуют организационным единицам, большая часть сетевых взаимодействий осуществляется в пределах домена  **Алгоритмы дистанционно-векторные (Distance vector)**  каждый маршрутизатор периодически и широковещательно рассылает по сети вектор расстояний от себя до всех известных ему сетей.  Под расстоянием обычно понимают число промежуточных маршрутизаторов через которые пакет должен пройти прежде, чем попадет в соответствующую сеть.  Могут использоваться и другие метрики, учитывающая не только число транзитных пунктов, но и время прохождения пакетов по связи между соседними маршрутизаторами.  Получив вектор от соседнего маршрутизатора, каждый маршрутизатор добавляет к нему информацию об известных ему других сетях  В результате каждый маршрутизатор узнает информацию об имеющихся сетях и о расстоянии до них хорошо работают только в небольших сетях; в больших сетях они генерируют интенсивный широковещательный трафик;  изменения конфигурации отрабатываются по этому алгоритму не всегда корректно, так как маршрутизаторы не имеют точного представления о топологии связей в сети, а располагают только обобщенной информацией - вектором дистанций, к тому же полученной через посредников.  **Алгоритмы состояния связей (Link-state)**  обеспечивают каждый маршрутизатор информацией, достаточной для построения точного графа связей сети  Все маршрутизаторы работают на основании одинаковых графов  Это делает процесс маршрутизации более устойчивым к изменениям конфигурации  Широковещательная рассылка используется только при изменениях состояния связей, что происходит в надежных сетях не так часто  Для того чтобы понять, в каком состоянии находятся линии связи, подключенные к его портам, маршрутизатор периодически обменивается короткими пакетами со своими ближайшими соседями. Этот трафик также широковещательный, но он циркулирует только между соседями и поэтому не так загружает сеть. |
| **33. Протокол RIP, основные принципы, преимущества и**  **Недостатки(c518)**  ПО ЛЕКЦИИ  Протокол RIP(Routing Information Protocol) предназначен для сравнительно небольших и однородных сетей  · Сообщения передаются в UDP дейтаграммах, порт 520  · Метрика – число хопов (промежуточных узлов)  · Таблица маршрутизации содержит по одной записи на каждую обслуживаемую машину, например:IP адрес сети, Расстояние до этой сети, IP адрес следующего маршрутизатора по пути к месту назначения, Таймеры.  · Каждый маршрутизатор RIP периодически рассылает свой вектор RIP (набор пар IP адрес сети и расстояние до сети)  · Построение таблицы маршрутизации – итеративное  · Для предотвращения зацикливания предусмотрены дополнительные правила  · Малое значение бесконечности = 16 (из-за эффекта «счет до бесконечности») ограничивает размер RIP-системы.  · Широковещательная рассылка векторов расстояний каждые 30 с ухудшает пропускную способность сети;  · Время схождения алгоритма при создании маршрутных таблиц сравнительно велико  · Иногда (например, после включения), все маршрутизаторы рассылают свои вектора одновременно, что приводит к пикам трафика  · В таблице маршрутизации каждой записи о маршруте, полученном по RIP, назначен 3-минутный тайм-аут, по истечение которого не обновленные записи удаляются. Если маршрутизатор выходит из строя, распространение изменений по объединенной сети может занять несколько минут. Возникает проблема медленной конвергенции.  Недостатки протокола маршрутизации RIP  1)малое значение бесконечности ограничивает размер RIP-системы. Кроме того, по той же причине весьма затруднительно использование сложных метрик, учитывающих не просто количество промежуточных маршрутизаторов, но и скорость и качество канала связи (чем хуже (медленнее) канал, тем больше метрика).  2) само явление счета до бесконечности вызывает сбои в маршрутизации.  3), время схождения алгоритма при создании маршрутных таблиц достаточно велико (по крайней мере, по сравнению с протоколами состояния связей).  4), несмотря на то, что каждый маршрутизатор начинает периодическую рассылку своих векторов, вообще говоря, в случайный момент времени (например, после включения), через некоторое время в системе наблюдается эффект синхронизации маршрутизаторов, сходный с  эффектом синхронизации аплодисментов. Все маршрутизаторы рассылают свои вектора в один и тот же момент времени, что приводит к большим пикам трафика и отказам в маршрутизации дейтаграмм во время обработки большого количества одновременно полученных векторов | **34. Протокол OSPF, основные принципы, преимущества и Недостатки**  Протокол OSPF (Open Shortest Path First)-протокол состояния связей. Использует алгоритм поиска кратчайшего пути в графе.Применяют для внутренней маршрутизации в системах сетей любой сложности  Метрика –оценка качества связи данного канала (сети):  · Метрика маршрута – сумма метрик каналов (сетей)  · В простейшем случае, по аналогии с RIP, метрика каждой сети =1, метрика маршрута = количеству хопов (промежуточных узлов)  · Поддерживает множественные маршруты: Балансировка трафика, Дублирование  · Внешние маршруты:  o Для достижения сетей, не входящих в OSPF-систему (в автономную систему), используют пограничные маршрутизаторы автономной системы (ASBR - Autonomous System Border Router)  o ASBR вносят в базу данных состояния связей данные о сетях за пределами системы, достижимых через тот или иной маршрутизатор ASBR  o Такие сети, а также ведущие к ним маршруты называются внешними (external).  Построение базы данных состояния связей:  Протокол Hello. После инициализации OSPF маршрутизатор начинает рассылаться Hello-сообщения.  · Задача Hello-протокола - обнаружение соседей и установлении с ними отношений смежности  o Соседями называют OSPF-маршрутизаторы, подключенные к одной сети (к одной линии связи) и обменивающиеся Hello-сообщениями  o Смежными называют соседние OSPF- маршрутизаторы, которые приняли решение обмениваться друг с другом информацией, необходимой для синхронизации базы данных состояния связей построения маршрутов  · Hello-пакеты периодически рассылаются и после того, как соседи обнаружены.  · Контролируется состояние связей с соседями  Протокол обмена:  · После установления отношений смежности для каждой пары смежных маршрутизаторов осуществляется синхронизация их баз данных  · Также при восстановлении разорванного соединения  Протокол затопления (Flooding Protocol):  · Каждый маршрутизатор отвечает за те записи в базе данных состояния связей, которые описывают связи, исходящие от данного маршрутизатора  · При образовании новой связи, изменении в состоянии связи или ее исчезновении (обрыве), маршрутизатор, ответственный за эту связь, должен изменить свою копию базы данных и известить все остальные маршрутизаторы  · Сообщение не должны передаваться слишком часто; но каждые 30 минут происходит принудительное обновление всех записей  Преимущества:  1. Для каждого адреса может быть несколько маршрутных таблиц, по одной на каждый вид IP–операции (TOS).  2. Каждому интерфейсу присваивается безразмерная цена, учитывающая пропускную способность, время транспортировки сообщения. Для каждой IP–операции может быть присвоена своя цена (коэффициент качества).  3. При существовании эквивалентных маршрутов OSFP распределяет поток равномерно по этим маршрутам.  4. Поддерживается адресация субсетей (разные маски для разных маршрутов).  5. При связи точка–точка не требуется IP–адрес для каждого из концов. (Экономия адресов)  6. Применение мультикастинга вместо широковещательных сообщений снижает загрузку не вовлеченных сегментов.  Недостатки:  1. Трудно получить информацию о предпочтительности каналов для узлов, поддерживающих другие протоколы, или со статической маршрутизацией.  2. OSPF является лишь внутренним протоколом. | **35. Прикладные протоколы TCP/IP, их назначение: HTTP, FTP,**  **Telnet, SMTP/POP**  Протокол пересылки файлов FTP (File Transfer Protocol) реализует удаленный доступ к файлам. RFC 959 – основная спецификация FTP.  · Используется протокол с установлением соединений – TCP  · Аутентификация пользователей:1)Прежде чем получить доступ к файлу, в соответствии с протоколом пользователи должны сообщить свое имя и пароль2)Для доступа к  публичным каталогам FTP-архивов Internet используют т.н.анонимный доступ с именем пользователя anonymous  · В стеке ТСР/IР протокол FTP предлагает наиболее широкий набор услуг для работы с файлами, однако он является и самым сложным для программирования.  · Порты: 20 – передача данных; 21 – передача команд  · Пассивный режим  · Изначально протокол предполагал встречное TCP-соединение от сервера к клиенту для передачи файла или содержимого каталога.  · Если клиент находится за NAT, то такое соединение невозможно. Также, зачастую, сетевые экраны блокируют входящие соединения  · Чтобы этого избежать, было разработан режим passive mode, когда соединение для передачи данных также устанавливается от клиента к серверу  Telnet обеспечивает передачу потока байтов между процессами, а также между процессом и терминалом  · Наиболее часто этот протокол применяют для эмуляции терминала удаленного компьютера (удаленного доступа к текстовому интерфейсу командной строки или псевдографическому)  · Не предусматривает шифрование, поэтому в настоящее время обычно используется протокол SSH (Secure Shell)  HTTP – протокол прикладного уровня, разработанный для обмена гипертекстовой информацией в сети Internet  · Для HTTP-запросов обычно используется 80 порт TCP/IP  · Клиент устанавливает соединение, посылает запрос и ждет ответа сервера  · После отправки ответа сервер инициирует разрыв соединения: При передаче сложных гипертекстовых страниц соединение может устанавливаться несколько раз  · Основным объектом манипуляции в HTTP является ресурс, на который указывает URI (Uniform Resource Identifier) в запросе клиента.  · Каждое HTTP-сообщение состоит из трёх частей, которые передаются в указанном порядке: 1)Стартовая строка (Starting line)-определяет тип сообщения; Заголовки (Headers)- характеризуют тело сообщения, параметры передачи и прочие сведения; Тело сообщения (Message Body)-непосредственно данные сообщения; обязательно должно отделяться от заголовков пустой строкой.  · Наиболее часто используются следующие методы:  o GET - метод, позволяющий получить данные ресурса, заданные в форме URI; при использовании метода GET в поле тела ресурса возвращается запрошенная информация (например, HTML-документ).  o HEAD - метод, аналогичный GET, возвращает только заголовок  o POST - этот метод используется для передачи информации на сервер  SMTP (Simple Mail Transfer Protocol) – отправка почты от пользователей к серверам и между серверами для дальнейшей пересылки к получателю, RFC 2821  · Протокол был разработан для передачи только текста в кодировке ASCII:  o Это не даёт возможности отсылать текст на национальных языках (например, кириллице), а также отправлять двоичные файлы  o Для снятия этого ограничения был разработан стандарт MIME, который описывает способ преобразования двоичных файлов в текстовые.  o Почтовый адрес записывают в виде mailbox@domain,  n mailbox - символическое имя почтового ящика пользователя (до 63 символов)  n domain - уникальное имя (почтовый домен) системы, в которой зарегистрирован упомянутый пользователь (до 255 символов)  POP3 (Post Office Protocol Version 3 — протокол почтового отделения, версия 3) используется почтовым клиентом для получения сообщений электронной почты с сервера.  · Обычно используется в паре с протоколом SMTP.  · В протоколе POP3 предусмотрено 3 состояния сеанса:  o Авторизация – клиент проходит процедуру Аутентификации  o Транзакция – клиент получает информацию о состоянии почтового ящика, принимает и удаляет почту  o Обновление – сервер удаляет выбранные письма и закрывает соединение | **36. Frame Relay. Понятия PVC, SVC; адресация во Frame Relay**  Frame Relay  -Начало работ по созданию стандарта – 1984 г  - В 1990 Cisco, DEC, Northern Telecom и StrataCom сформировали консорциум, разработавший спецификации  -Существует несколько вариантов (ITU-T и CCITT), различающихся спецификациями дополнительных функций Local Management Interface (LMI)  Все устройства подразделяются на:  -DTE (Data Terminal Equipment) – оконечное (terminal) пользовательское оборудование, подключаемое к сети  - DCE (Data circuit-terminating Equipment) – оконечное сетевое оборудование  n Работает в режиме коммутации пакетов с установлением соединения  n Такие соединения называются виртуальными каналами (Virtual Circuit) – двунаправленные логические связи, создаваемыми между двумя терминальными устройствами (DTE)  n Виртуальные каналы устанавливаются через произвольное количество устройств DCE сети Frame Relay  n Каждый виртуальный канал уникально идентифицируется номером DLCI – Data Link Connection Identifier  n DLCI уникален только в пределах физического канала между DTE и DCE  n Каналы подразделяются на 2 категории:  n PVC (Permanent Virtual Circuits) – постоянные виртуальные каналы  n SVC (Switched Virtual Circuits) – коммутируемые виртуальные каналы  Frame Relay SVC  n Коммутируемые виртуальные каналы SVC – временные соединения, используются для разового обмена данными  n Существует 4 состояния:  n Call Setup – установление соединения  n Data Transfer – передача данных между устройствами DTE по виртуальному каналу  n Idle – соединение активно, передачи данных нет  n Call Termination – разъединение виртуального канала  Frame Relay PVC  n Обычно используются PVC – постоянные соединения, используемые для частого обмена данными  n Не требуют установления и завершения соединения  Для каждого виртуального соединения в технологии Frame Relay определяется несколько параметров, связанных со скоростью передачи данных. □ Согласованная скорость передачи данных (Committed Information Rate, CIR) — гарантированная пропускная способность соединения; фактически сеть гарантирует передачу данных пользователя со скоростью предложенной нагрузки, если эта скорость не превосходит CIR. □ Согласованная величина пульсации (Committed Burst Size, Вс) — максимальное количество байтов, которое сеть будет передавать от данного пользователя за интервал времени Т, называемый временем пульсации, соблюдая согласованную скорость CIR. □ Дополнительная величина пульсации (Excess Burst Size, Be) — максимальное количество байтов, которое сеть будет пытаться передать сверх установленного значения Вс за интервал времени Т.  Второй параметр пульсации (Be) позволяет оператору сети дифференцированно обрабатывать кадры, которые не укладываются в профиль CIR. Обычно кадры, которые приводят  к превышению пульсации Вс, но не превышают пульсацию Вс + Be, сетью не отбрасываются, а обслуживаются, но без гарантий по скорости CIR. Для запоминания факта нарушения  в кадрах Frame Realy имеется специальное поле DE (Discard Eligibility — возможность  отбрасывания). В том случае, когда это поле кадра содержит значение 1, последующие  коммутаторы данного виртуального канала отбрасывают такой кадр, если испытывают  перегрузку И только если превышен порог Вс + Be, кадры отбрасываются сразу  Если приведенные величины определены, то время Т определяется следующей формулой:  Т = Bc/CIR. |
| **37. Управление перегрузками во Frame Relay, биты FECN, BECN, DE; качество обслуживания во Frame Relay: Committed Burst Rate, Committed Burst Size, Excess Burst Size**  FECN, BECN  n В Frame Relay существует механизм оповещения конечных пользователей о том, что в коммутаторах сети возникли перегрузки  n Бит FECN (Forward Explicit Congestion Bit) кадра извещает об этом принимающую сторону  n На основании значения этого бита принимающая сторона должна с помощью протоколов более высоких уровней (TCP/IP, SPX и т. п.) известить передающую сторону о том, что та должна снизить интенсивность отправки пакетов в сеть.  n Бит BECN (Backward Explicit Congestion Bit) извещает о переполнении передающую сторону и является требованием немедленного снижения темпа передачи  n Эти биты служат указанием для протоколов более высоких уровней (TCP, SPX, NCP и т. п.) о необходимости снизить скорость  Discard Eligibility  n Бит DE (Discard Eligibility) кадра используется для пометки кадров с более низким приоритетом  n При перегрузке сети в первую очередь начинают отбрасываться кадры, помеченные этим битом  n Это снижает вероятность потери важных данных при перегрузках  Качество обслуживания  n Для каждого виртуального соединения определено несколько характеристик качества обслуживания  n CIR (Committed Information Rate) – согласованная скорость передачи пользовательских данных – определяется в договоре с абонентом сети  n Committed Burst Size – «согласованный объем пульсации», Bc, максимальное количество байт, которые сеть будет пытаться передать за интервал времени T  n Excess Burst Size – «дополнительный объем пульсации», Be, максимальное количество байт, которые сеть будет пытаться передать сверх установленного значения за интервал времени T  n Обычно доступ к сети осуществляются по каналы с большей скоростью, чем CIR | **38. Технология ATM. Назначение. Понятие ячейки. Понятие уровня адаптации ATM, классов служб.**  **Технология АТМ**  n ATM (Asynchronous Transfer Mode) – асинхронный режим передачи  n Ориентирована на работу с информацией различного типа:  n Данные  n Мультимедиа  n статические изображения,  n аудио,  n видео,  n голос, традиционно передаваемый по телефонными сетями;  n Технология пакетной коммутации ATM применяет короткие пакеты фиксированной длины, называемые ячейками (cell)  n Ячейка ATM имеет размер 53 байт  n 5 – составляют заголовок,  n 48 – собственно информацию  n Благодаря фиксированной длине, конструкция АТМ-коммутатора более проста, задержки и их дисперсия ниже  n Существенно для таких чувствительных к задержкам видам коммуникационного обслуживания, как передача голосовых сообщений и видео  n В сетях ATM «выделенные» соединения называют постоянными виртуальными устройствами (PVC), создаваемыми по соглашению между пользователем и оператором (подобно выделенной телефонной линии)  n Коммутируемые соединения ATM используют коммутируемые виртуальные устройства (SVC), устанавливаемые путем передачи специальных сигналов между пользователем и сетью  n Основной функцией уровня ATM является коммутация ячеек  Устройство ATM принимает ячейки, поступающие по пути передачи данных, определяет путь дальнейшей пересылки, по которому эти ячейки следует ретранслировать, и форматирует заголовок каждой отправляемой ячейки  Ур. адаптации  Уровень адаптации ATM (AAL) предлагает интерфейс между сетью ATM и пользовательским программным обеспечением ATM, обычно реализуемым в подсистеме сетевого ПО  n AAL применяется только в оконечных устройствах, но не в коммутаторах ATM  n В оконечном устройстве, играющем роль отправителя, AAL принимает битовый поток от пользовательского программного обеспечения ATM и структурирует его в виде ячеек, подходящих для транспортировки по сети ATM  n В принимающем оконечном устройстве ATM соответствующий уровень AAL получает ячейки из сети, воссоздает исходный битовый поток и передает его принимающему пользовательскому ПО.  Для уровня адаптации ATM определены четыре класса служб  n Класс А (эмуляция цепей)  n ориентирована на создание соединения  n поддерживает постоянную скорость передачи битов и временные соотношения между отправлением и получением информации  n Таким образом, адресат получает поток данных с постоянной скоростью (с какой ее передает отправитель)  n Службу этого класса можно использовать для передачи аудио- и видеоданных вместо обычной телекоммуникационной связи с коммутацией цепей (т. е. вместо аналогового канала)  n Класс В (переменная скорость передачи)  n во многом аналогична службе класса А  n ориентирована на соединение  n имеет переменную скорость передачи и поддерживает временные соотношения между отправлением и получением данных  n предусматривает передачу уплотненной (сжатой) аудио- и видеоинформации и может использоваться, например, в видеоконференциях, где при ограниченных задержках изменяющаяся скорость передачи данных считается допустимой.  n Класс С (передача данных, ориентированная на создание соединения).  n ориентирована на создание соединения,  n не поддерживает временные соотношения. Служба этого класса требует создания двухточечного соединения между отправителем и получателем. Пользователь-  отправитель передает информацию в сеть в виде пакетов переменного размера, которые получает целевое программное обеспечение пользователя ATM. Поступающие к целевому пользователю пакеты могут приходить с отличной от исходной скоростью. Эта служба обеспечивает обмен данными подобно обычным компьютерным сетям.  n Класс D (передача данных, не ориентированная на создание соединения).  n предназначена для передачи данных без создания соединения  n информация передается по сети ATM в виде пакетов переменного размера, которые поступают к получателю с переменной скоростью.  n пакеты могут адресоваться как одному получателю, так и нескольким одновременно (многоадресная рассылка). |  |  |