КОМПЬЮТЕРНЫЕ СЕТИ ‘18

1. Базовая эталонная модель взаимодействия открытых систем

Модель OSI – это модель, принятия ISO для описания общих принципов взаимодействия информационных систем. OSI признана всеми международными организациями как основа для стандартизации протоколов информационных сетей. В OSI информационная сеть рассматривается как совокупность функций, которые делятся на группы, называемые уровнями.

Модель OSI имеет 7 уровней, описывает только системные средства взаимодействия и не включает средства взаимодействия конечных пользователей. Не является сетевой архитектурой, поскольку не описывает службы и протоколы.

Каждый следующий уровень вкладывается в секцию данных предыдущего. Для обработки следующего уровня не должна быть задействована информация с другого (хорошо для распараллеливания работы над уровнями).

Интерфейс взаимодействия между двумя уровнями называется **точкой доступа**. Инициатор взаимодействия – **клиент**, предоставляющий ресурсы уровень – **провайдер**.

Уровень	**Тип данных**	**Функции**	**Примеры**
Приложения	Сообщение	Обеспечивает сетевой сервис пользователей – набор разнообразных протоколов для доступа к разделяемым ресурсам сети	HTTP, SMTP, FTP, DHCP
Представления		Представление, шифрование и сжатие данных	ASCII, EBCDIC
Сеансовый		Позволяет пользователям различных узлов устанавливать сеансы связи друг с другом; предоставляет средства синхронизации	RPC, PAP
Транспортный (промежуточный, скрывает функционирование верхних от нижних)	Сегменты	Обеспечивает доставку пакетов от приложения на одном узле к приложению на другом. Отвечает за надежность передачи данных	TCP, UDP
Сетевой	Пакеты/ Дейтаграммы	Определение маршрута и логическая адресация. Не несет ответственности за передачу сигнала	IP, IPX
Канальный	Биты/Кадры	Физическая адресация. На основе интерфейсов физического уровня определяет принципы кодирования. Реализация механизмов обнаружения и коррекции ошибок	Ethernet, FDDI
Физический	Кадры	Работа со средой передачи и сигналами	USB, кабель («витая пара», коаксиальный, оптоволоконный), радиоканал

2. Виды каналов связи: оптический, медный, беспроводной

Работа любой КС основана на эффективной передаче **информации** (совокупность данных об окружающем мире, являющихся объектом хранения, передачи и преобразования). Информация передается в виде **сообщений** (совокупность первичных сигналов, содержащих информацию). **Сигнал** – изменяющийся по времени физический процесс, отражающий передаваемое сообщение. В зависимости от значений сигналы делятся на: *непрерывные*(аналоговые) и *дискретные*.

Каналом связи называется комплекс технических устройств, обеспечивающих передачу сигналов от передатчика к приемнику. В зависимости от типа сигнала подразделяются на *аналоговые* и *дискретные*.

МЕДНЫЕ КАБЕЛЬНЫЕ СИСТЕМЫ.

В качестве линии связи используются, по крайней мере, два медных проводника, по которым информация передается с помощью электрических сигналов. Для передачи сигналов используются два основные разновидности кабеля: коаксиальный и витая пары проводников. Медные кабельные системы характеризуются набором параметров, распределенных по всей длине: *емкостью, сопротивлением изоляции между проводниками, индуктивностью и активным сопротивлением.* Важным комплексным параметром кабеля является *волновое сопротивление* – полное сопротивление, которое встречает электромагнитная волна при распространении вдоль однородной цепи.

Витая пара (twisted pair) представляет собой витую пару медных проводов (или несколько пар проводов), заключенных в экранированную оболочку. При скручивании проводники идут под некоторым углом друг к другу, что снижает емкостную и индуктивную связь между ними, также кабель становится симметричным для внешних помех, что снижает его чувствительность к разлтичным наводкам. Существует два типа этого кабеля: неэкранированная витая пара **UTP** и экранированная витая пара **STP** (имеет дополнительный элемент с оплеткой).

Кабель используется для передачи данных на скорости 10 Мбит/с и 100 Мбит/с. Витая пара обычно используется для связи на расстояние не более нескольких сот метров. К недостаткам кабеля "витая пара" можно отнести возможность простого несанкционированного подключения к сети.

Коаксиальный кабель (coaxial cable) - это кабель с центральным медным проводом, который окружен слоем изолирующего материала (диэлектрика). Затем идет проводник-экран. Внешний проводящий экран кабеля покрывается изоляцией.

Является прототипом Ethernet. Коаксиальный кабель более помехозащищенный, чем витая пара. Допустимая длина линии связи – несколько километров. Несанкционированное подключение к коаксиальному кабелю сложнее, чем к витой паре.

ОПТИЧЕСКИЕ

В *волоконно-оптических* кабельных системах сигналы передаются несущей оптического диапазона волн по световодам. Принцип действия волоконного световода основан на использовании процессов отражения и преломления оптической волны на границе раздела двух сред с различными показателями преломления. Типичные волокна имеют строение (изнутри наружу): сердечник, оболочка, защитное покрытие.

Излучение внешнего источника возбуждает в световоде несколько типов волн, которые называются **модами**. В зависимости от распределения показателя преломления и от величины диаметра сердечника различают **многомодовые** и **одномодовые волокна.** В одномодовых сигнал распространяется параллельно оси симметрии (оптической оси). В многомодовых запускаются несколько сигналов под различными углами.

БЕСПРОВОДНЫЕ

Радиоканал использует передачу информации по радиоволнам. Плюсы: большое расстояние, высокая скорость передачи. Классифицируют по распространению волн, объему передачи и чувствительности точек.

Инфракрасный канал использует для связи инфракрасное излучение. Главное его преимущество по сравнению с радиоканалом - нечувствительность к электромагнитным помехам, что позволяет применять его, например, в производственных условиях.

Рентгеновское и ультрафиолетовое излучение.

3. Методы передачи данных

Работа любой КС основана на эффективной передаче **информации** (совокупность данных об окружающем мире, являющихся объектом хранения, передачи и преобразования). Информация передается в виде **сообщений** (совокупность первичных сигналов, содержащих информацию). **Сигнал** – изменяющийся по времени физический процесс, отражающий передаваемое сообщение. В зависимости от значений сигналы делятся на: *непрерывные*(аналоговые) и *дискретные*. Периодический информационный сигнал, имеющий конечную длительность, может быть представлен в виде ряда Фурье:

$$s(t) = \sum_{i=0}^{\infty} A_i \sin(2\pi\vartheta_i + \varphi_i),\ A_i - \text{амплитуда}, \varphi_i - \text{фаза}, \varphi_i - \text{частота}$$

Каждая составляющая синусоида называется также **гармоникой**, а набор всех гармоник – **спектральным разложением** исходного сигнала.

В связи с тем, что физические параметры линий связи отличаются от идеальных, при передаче происходит искажение гармоник сигнала. Существуют также внешние помехи, создающиеся электрическими и электронными устройствами, атмосферными явлениями. Степень искажения синусоидальных сигналов каналами связи может быть оценена с помощью **амплитудно-частотной характеристики**, **полосы пропускания** и **затухания** на определенной частоте.

Амплитудно-частотная характеристика показывает затухание (относительное уменьшение мощности амплитуды сигнала при передаче, децибел) амплитуды синусоиды на выходе канала связи по сравнению с ее амплитудой на входе для всех возможных частот передаваемого сигнала. Можно также использовать фазово-частотную зависимость.

Полоса пропускания – непрерывный диапазон частот, для которого отношение амплитуды выходного сигнала к входному превышает некоторый заранее заданный предел. Полоса пропускания определяет диапазон частот синусоидального сигнала, при которых этот сигнал передается по каналу без значительных искажений. Ширина полосы пропускания в наибольшей степени влияет на максимально возможную скорость передачи информации по линии связи.

Выбор способа представления дискретной информации в виде сигналов, подаваемых на линию связи, называется **физическим** или **линейным кодированием** (аналоговое – на основе синусоидального несущего сигнала, и

цифровое – на основе последовательности прямоугольных импульсов). Периодический сигнал, параметры которого изменяются, называют *несущим сигналом* или *несущей частотой*, если в качестве такого сигнала используется синусоида.

Количество изменений информационного параметра несущего периодического сигнала измеряется в *бодах*.

Процесс представления аналоговой информации в дискретной форме называется **дискретной модуляцией** и включает этапы: дискретизации по времени, оцифровывания, передачи битовой последовательности по каналам связи с использованием методов цифрового кодирования.

4. Цифровое кодирование

При цифровом кодировании дискретной информации на основе прямоугольных импульсов применяют следующие коды:

1) **потенциальные** – для представления двоичных данных используется только значение потенциала сигнала;
2) **импульсные** – двоичные данные представляются либо импульсами определенной плотности, либо частью импульса – перепадом потенциала определенного направления.

Выбор способа кодирования требует достижения целей:

1) иметь меньшую ширину спектра результирующего сигнала при одной и той же битовой скорости;
2) обеспечить синхронизацию между передатчиком и приемником;
3) обладать способностью распознавать ошибки;
4) обладать низкой стоимостью реализации.

В КС используются так называемые *самосинхронизирующиеся коды*, сигналы которых несут для приемника указания на моменты времени считывания очередного бита (бит), например любой резкий перепад сигнала, так называемый фронт. (*Прикол рассинхронизации в том, что если отправляется большая последовательность одинаковых бит, то получатель может неправильно определить количество этих бит, например отправили 100, а полчатель понял, что 101Ю потому что частоту по-другому считал*)

ПОТЕНЦИАЛЬНЫЕ

NRZ – без возврата к нулю

Обычная схема: бит «1» предстальвяется напряжением +V, бит «0» - нулевым напряжением. Дифференциальная схема: состояние меняется в начале битового интервала «1» и не меняется для «0». Нет привязки «1» и «0» к определенному состоянию. Метод прост в реализации, обладает хорошей распознаваемостью ошибок, но не обладает свойством самосинхронизации – возможны постоянные составляющие из 0 и 1.

AMI (Alternate Mask Inversion) - биполярное кодирование с альтернативной инверсией

«0» кодируется потенциалом 0, а «1» - либо +V, либо -V, при этом потенциал каждой новой «1» противоположен потенциалу предыдущей. Метод частично решает проблему постоянной составляющей и не является полностью самосинхронизирующимся. По сравнению с NRZ имеет более узкий спектр.

MLT-3 – несамосинхронизирующее 3-уровневое кодирование

«0» не меняет значение, а при «1» значения меняются по цепочке +V, 0, -V, 0, +V.

ИМПУЛЬСНЫЕ

Манчестерский код

Текущий бит определяется по направлению смены состояния в середине битового интервала: от -V к +V – “1”, от +V к -V – «0». То есть если возрастает, то 1, убывает – 0. Относится к самосинхронизирующимся, так как изменение на середине интервала.

Длинная последовательность из 1 или 0 с помощью служебных перехоов(как будто не вовремя)

В дифференциальном текущий бит определяется по наличию перехода в начале битового интервала: «0» - есть переход, «1» - нет перехода. Среди минусов кода: сложная реализация; из-за того, что на каждом такте сигнал меняет свое состояние, то для передачи одного бита треубет удвоенная частота тактового генератора (2 бод/1 бит); тяжело оцифровывается.

RZ

В определенный момент битового интервала состояние всегда возвращается к нулю. Имеет обычный вариант и дифференциальный, в котором нет привязки «0» и «1» к определенному состоянию.

Для улучшения ряда свойств потенциальных кодов кодирование данныз на физическом уровне строится по двухступенчатой схеме – физическое кодирование дополняется логическим. **Логическое кодирование** преобразует входной поток бит перед физическим кодированием. Позволяет избавиться от нежелательных последовательностей (например много «1» или «0» подряд).

1) *Избыточные коды.* Основаны на разбиении исходной последовательности бит на части, которые называют символами. Затем каждый исходный символ заменяется на новый, имеющий большее кол-во бит.

1.1) **4B/5B**. Каждые 4 бита входнго потока кодируются 5-битными символами. Двухкратная избыточность. Позволяет преобразовать исходный поток бит в последовательность, в которой содержится не более 3 «0» подряд.

1.2) **8B/10B**. Каждый 8 бит входного потока кодируются 10-битными символами с 4-кратной избыточностью. Не более 5 подряд идущих «0».

2) *Скрэмблирование*. Позволяет на физическом уровне подавлять слишком сильные гармоники сигнала, распределяя их по некоторой полосе спектра.

5. Управление каналом связи

Управление каналами связи осуществляется с помощью протоколов канального уровня. Протоколы канального уровня оперируют с блоками данных, которые называются кадрами. Основные задачи протоколов канального уровня:

1) формирование кадров для передачи пакетов данных между физически связанными узлами КС;
2) нахождение границ кадра в потоке бит, передаваемых на физическом уровне;
3) обработка ошибок передачи и управление потоком кадров.

В завимисоти от метода передачи протоколы, работающие на канальном уровне, могут быть разделены на **асинхронные** и **синхронные.**

Асинхронные протоколы

Оперируют на кадрами, а символами (байт данных, сопровождаемый специальными сигналами «Start», «Stop», необходимыми для синхронизации передатчика и приемника). Такой метод передачи пригоден для связи низкоскоростных устройств на небольших расстояних (клавиатур, дисплеев с компьютером).

Синхронные протоколы

Синхробиты (преамбула)	Служебная информация (заголовок)	Данные	Служебная информация (концевик)

Обмен осуществляется кадрами. Для надежной синхронизации приемника и передатчика используются один или несколько байтов синхронизации. Однако при передаче больших кадров могут возникнуть проблемы и необходимо применение на физическом уровне самосинхронизирующихся кодов.

Выделяют два типа синхронныз протоколов:

1) *символьно-ориентированные*. Используют символы SYN (0010 110 синхробит), STX (0000 010 граница начала кадра), ETX (0000 011 окончание кадра). Недостаток подхода в том, что внутри кадра возможно появление символов STX, ETX. Кодопрозрачность протокола, т.е. его способность отличать граничные символы от символов данных кадра, достигается байт-стаффингом – вставка экранирующего символа DLE. Это сильно увеличивает избыточность.

2) *бит-ориентированные.*
СХЕМА 1: Принимаемый поток бит сканируется приемником на побитовой основе для обнаружения начального и конечного флагов.

1111 1111	0111 1110	Данные	0111 1110	1111 1111
Преамбула	Начальный флаг		Конечный флаг	

← *направление передачи*

Длина кадров не обязательно кратна 8 бит.

Для синхронизации используется преамбула – байты простоя. Кодопрозрачность протокола обеспечивается бит-стаффингом (вставка 0 бита), которая применяется только во время передачи поля данных кадра.

- если передатчик обнаруживает, что подряд передано 5 «1», то он автоматически вставляет «0». Поэтому флаговая последовательность 0111 1110 никогда не появится в поле данных.
- приемник выполняет обратную функцию – если после 5 «1» обнаруживает «0», то автоматически удаляет его из поля данных кадра.

Бит-стаффинг является менее избыточным, чем байт-стаффинг.

СХЕМА 2: Для обозначения начала кадра имеется только начальный флаг, а для определения конца кадра используется поле длины кадра (длины поля данных кадра).

1010 1010	1010 1011	Фикс. заголовок	Длина поля данных (байт)	Поле данных	Фиксированный концевик
Преамбула	Нач. флаг				

СХЕМА 3: Для обозначения начала и конца кадра используются флаги, которые включают запрещенные для данного кода сигналы (code violations). Схема экономична: не требует байт/бит-стаффинга либо поля длины данных.

Существует ряд протоколов, в которых кадры имеют более гибкую структуру. Кадры таких протоколов состоят из неопределенного количества полей, каждое из которых может иметь переменную длину. Способ представления данных в таких протоколах называется TLV (Type, Length, Value). Каждому полю кадра (Value) предшествуют два дополнительных поля фиксированного размера: Type, Length.

При передаче кадров данных на канальном уровне могут быть предоставлены различные службы, подразделяющиеся на:

1) *службы без установления соединения (дейтаграммные*). Работает быстро, но не гарантирует доставку кадров. Восстановление потерянных или ошибочных кадров возлагается на протоколы верхних уровней. В некоторых протоколах дейтаграммный методдополняется средствами подтверждения, что повышает его надежность.
2) *службы с установлением соединения.* Является надежной, но требует больше вычислительных затрат от узлов. Состоит из трех фаз:
   a. *установление логического соединения.* С помощью обмена служебными кадрами обе стороны подтверждают установление соединения.
   b. *передача данных.* С помощью информационных кадров передаются пользовательские данные, при этом отслеживается корректность последовательности их передачи.
   c. *Разрыв логического соединения.* С помощью служебных кадров партнеры извещают друг друга о закрытии логического соединения.

Процедура установления соединения позволяет достичь: взаимной аутентификации пользователей и оборудования; согласования изменяемых параметров протокола; обнаружения и коррекции ошибок.

6. Обнаружение и коррекция ошибок

Каканльный уровень должен обнаруживать ошибки передачи данных, связанные с искажением бит в принятом кадре или с потерей кадра, и по возможности его корректировать.

ОБНАРУЖЕНИЕ ОШИБОК

Все методы обнаружения ошибок основаны на передаче в составе кадра служебной избыточной информации. Эту служебную информацию принято называть контрольной суммой или последовательностью контроля кадра FCS (Frame Check Sequence).

1) ***Контроль по паритету***. Все биты контролируемого блока данных суммируются по модулю 2. Результат суммирования (бит паритета) пересылается вместе с контролируемой информацией. Такой код позволяет обнаруживать только одиночные ошибки. Модификацией данного метода является *вертикальный* и *горизонтальный контроль по паритету*. Контролируемый блок данных рассматривается как матрица n*k. Затем биты паритета рассчитываются отдельно для каждых строки и столбца. Однако большая избыточность кода ограничивает его применение на практике.
2) ***Циклический избыточный контроль CRC (Cyclic Redundancy Check)***. В основу положено представление битовых строк в виде полиномов с коэффициентами 0 или 1. Кадр из k бит – полином степени k-1. Отправитель и получатель определяют $G(x), \deg G(x) = r$ – образующий полином, старший и младший биты которого 1.
   Алгоритм вычисления контрольной суммы $M(x), degM(x) = m$:
   1) $M_1(x) = x^r M(x)$ #соответствует контролируемому кадру, дополненному справа r нулями.
   2) $R(x) = M_1(x)\ mod\ G(x),\ degR(x) \le r$ #остаток от деления $M_1(x)$ на G(x)
   3) $T(x) = M_1(x) + R(x)$ #соответствует передаваемому кадру
   4) $R_1(x) = T(x)\ mod\ G(x) = \begin{cases} 0, \text{успешно} \\ \text{другое, ошибка!} \end{cases}$ #это получаетель вычисляет, получив кадр

   Суммирование производится без переноса в следующий разряд. Есть только опреации сдвига и xor. Работает только если известен вид полинома (должен быть неприводимым). Минус метода в высокой вычислительной сложности. Для повышения производительности метода Питерсон и Браун предложили простую схему для аппаратного подсчета и проверки контрольной суммы на основе сдвигового регистра, которая применяется почти во всей аппаратуре. Метод обладает невысокой степенью избыточности.

КОРРЕКЦИЯ ОШИБОК

Методы коррекции ошибок в КС основаны на повторной передаче кадра в случае его потери или искажения информации в нем. Для коррекции ошибок необходимо ввести: нумерацию отправляемых кадров, служебные таймеры для подтверждения приема кадров, таймер для ограничения ожидания приема.

Служебные кадры, подтверждающие прием кадров данных, называются квитанциями (могут быть «+» (**ACK** - acknowledgment) или «-» (**NAK –** not acknowledgment)). При отправке каждого кадра передатчик запускает таймер, и если по его истечении квитанция не получена, то кадр считается утерянным. Однако если квитанция запаздывает, то возникает проблема дублирования передаваемых кадров.

1) ***Метод с простоями.*** Источник, пославший кадр, ожидает получения квитанции от приемника и только после этого посылает следующий кадр.Метод имеет низкую производительность обмена данными за счет простоев на ожидание подтверждений.
2) ***Метод «скользящего окна».*** Каждый передаваемый кадр имеет порядковый номер $S \in [0,\ 2^{n-1}]$, где n – кол-во бит, отводимых под номер. Для передачи и приема кадров используются посылающее и принимающее окна. Окна можно представить как циклический буфер, позволяющий разместить $M = 2^n$ кадров. Тогда будем говорить, что задано окно по модулю M. Квитанция посылается только при получения последнего кадра в окне.
   СТРАТЕГИЯ 1: Возврат на n. Получатель игнориуретт все кадры, полученные вслед за ошибочным, и требует повторить все кадры, начиная с ошибочного.
   СТРАТЕГИЯ 2: С выборочным повтором. Делаем квитанцию с номерами пакетов, дошедших успешно. Получатель запрашивает потворить передачу ошибочных и потерянных кадров, сохраняя в буфере последующие, правильно полученные кадры.

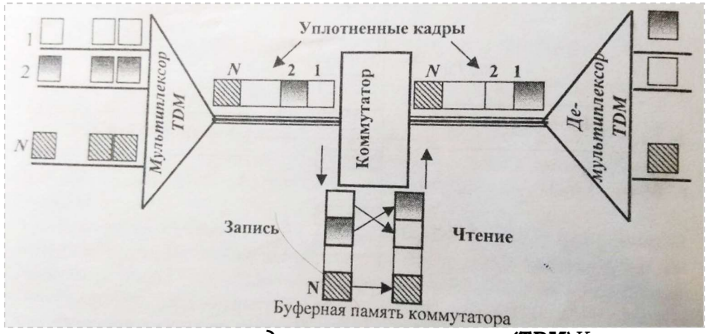
7. Коммутация и мультиплексирование

Коммутация каналов подразумевает образование непрерывного составного физического канала из последовательно соединенных отдельных канальных участков для прямой передачи данных между узлами. Отдельные каналы соединяются между собой коммутаторами, которые могут устанавливать связи между любыми конечными узлами сети.

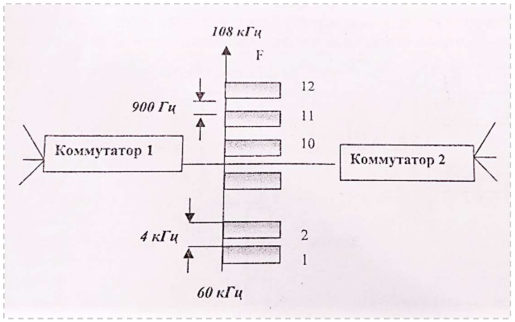
Сети с коммутацией каналов могут быть разделены на: ***сети с динамической коммутацией*** (коммутация происходит во время сеанса связи, по инициативе одного из взаимодействующих пользователей – передача файла, просмотр страницы) и ***сети со статической коммутацией*** (паре пользователей разрешается запросить соединение на длительный период времени, которое устанавливается персоналом, обслуживающим сеть. Режим постоянной коммутации называется *сервисом выделенных или арендуемых каналов*).

Коммутаторы, а также соединяющие их каналы должны обеспечивать одновременную передачу данных нескольких абонентских каналов или нескольких сеансов связи. Эта задача решается с помощью техники **мультиплексирования**.

1) ***Частотное мультиплексирование (FDM).*** (разрабатывалась в расчете на передачу непрерывных сигналов, представляющих голос). При частотном мультиплексировании полоса частот выходного канала делится на некоторое число полос (подканалов) n, соответствующих по ширине основной полосе стандартного телефонного канала 4 кГц, оставляя между ними промежуток в 900Гц. В канале между двумя FDM-коммутаторами одновременно передаются сигналы всех абонентских каналов. Такой канал азывают *уплотненным*. Коммутаторы FDM могут выполнять как *динамическую*, так и *постоянную* коммутацию. При динамической коммутации коммутатор выделяет данному абоненту одну из свободных полос своего уплотненного канала. При постоянной коммутации за абонентом полоса в 4 кГц закрепляется на длительный срок.



2) ***Мультиплексирование с разделением по времени (TDM)*** Каждому соединению выделяется один квант времени цикла работы аппаратуры, называемый **тайм-слотом** (длительность зависит от числа обслуживающих абонентских каналов). Мультиплексор TDM принимает информацию по N входным каналам от конечных абонентов (абоненты передают данные по каналу со скоростью 64 Кбит/с).
   В каждом цикле мультиплексор выполняет следующие действия:
   1) прием от каждого канала очередного байта данных;
   2) составление из прирятых байтов уплотненного кадра
   3) передача уплотненного кадра на выходной канал со скоростью N*64 Кбит/с



   Порядок байт в уплотненном кадре соответствует номеру входного канала, от которого этот байт получен. Кол-во обслуживаемых мультиплексором абонентских каналов зависит от его быстродействия.
   Демультиплексор выполняет обратную задачу – байты уплотненного кадра распределяет по своим выходным каналам, считая, что порядковый номер байта в кадре соответствует номеру выходного канала.
   Соединение в сети TDM обладает фиксированной пропускной способностью, кратной 64 Кбит/с. *Сети, использующие TDM, требуют синхронной работы всего оборудования!*

3) ***Мультиплексирование по длине волны (WDM).*** Технология передачи в системе в оптических системах, где различные источники *используют разную длину волны.* Оптические сигналы объединяются и передаются по одному общему оптическому пути. Эта технология позволяет объединение передачи нескольких потоков данных по одному физическому волконно-оптическому кабелю. Это работает потому, что *лучи света с разными длинами волн не взаимодействуют между собой* (из физики). Из плюсов: высокая скорость, широкая полоса пропускания.

8. Основы Ethernet (локальная сеть)

Общая формула для спецификации классов сетей Ethernet имеет вид **xBase-y**, где x – скорость технологии данного класса в Мбит/с, y – тип физической среды. **Base** означает, что все классы сетей используют немодулированную передачу в цифровой форме по каналу без частотного разделения. В зависимости от значения x существуют:

1) базовые технологии Ethernet (x = 10 Мбит/с);
2) высокоскоростные технологии Ethernet (Fast Ethernet: x = 100 Мбит/с; Gigabit Ethernet: x = 1000 Мбит/с)

Преимущества Ethernet:

1) простота реализации, управления и обслуживания сетей
2) дешево
3) топологическая гибкость при установке сетей (много вариантов расположения узлов в сети)
4) довольно высокая надежность
5) большая помехоустойчивость

Для доступа к среде передачи данных используется **протокол множественного доступа с прослушиванием несущей и обнаружением коллизий** (**CSMA/CD**). Этапы доступа к среде передачи данных:

1) данные передаются в виде кадров определенной структуры (содержит MAC-адреса узла-отправителя и узла-получателя)
2) узел-отправитель прослушивает основную гармонику сигнала (несущую частоту), чтобы определить, свободна ли разделяемая среда
3) если среда свободна, узел может начать передачу
4) все станции, подключенные к кабелю, могут распознать передачу кадра, синхронизируясь по преамбуле кадра. Узел-получатель, распознавший свой адрес, буферизирует кадр. Кадр проверяется на отсутствие ошибок с помощью контрольной последовательности и по длине кадра.
5) если среда занята, то узел ждет освобождения
6) после передачи кадра все узлы сети должны выдержать технологическую паузу – междкадровый интервал. (для приведения сетевых адаптеров в исходное состояние, а также для предотвращения монопольного захватывания среды одним узлом)

Могут возникать **коллизии** – нежелательное наложение двух или более сигналов в общей шине, приводящие к искажению информации (если два узла одновременно определили среду свободной).

Есть 4 основных типа кадров Ethernet: Ethernet II, Ethernet 802.3, Ethernet 802.2, Ethernet SNAP.

МОДИФИКАЦИИ ETHERNET

1) **10Base-5.** В качестве среды передачи данных – коаксиальный кабель с волновым сопротивлением 50 Ом, диаметром медного провода 2.17 мм и внешним диаметром 10 мм.

2) **10Base-2**. В качестве среды передачи данных – коаксиальный кабель с волновым сопротивлением 50 Ом, диаметром медного провода 0.89 мм и внешним диаметром 5 мм.
3) **10Base-T.** В качестве среды передачи данных – UTP-кабель (неэкранированная витая пара) категории 3.
4) **Оптоволоконный Ethernet.** В качестве среды передачи данных – многомодовое оптическое волокно.
5) **10Base-F** – обобщенное название 10Base-FL, 10Base-FB, 10Base-FP, все используют оптический кабель.

9. Logical Link Control protocol

В локальных сетях канальный уровень делится на два подуровня: **логической передачи данных (LLC**) и **управления доступом к среде (MAC**). Уровень LLC отвечает за передачу кадров данных между узлами с различной степенью надежности, а также реализует функции интерфейса с прилегающим к нему сетевым уровнем.

Протокол LLC уровня LLC обеспечивает для технологий локальных сетей требуемое качество услуг транспортной службы. Протоколы сетевого уровня (они выше в OSI модели) передают LLC протоколу информацию, на базе которой LLCP формирует кадр:

- данные;
- адресную информацию об узле назначения;
- требования к качеству транспортных услуг.

Для реализации качества транспортных услуг LLC предоставляет верхним уровням три типа служб:

1) **LLC1**. Без установления соединения и без подтверждения (ненадежный, верхние уровни занимаются обеспечением корректности передачи данных)
2) **LLC2**. С установлением соединения и подтверждеинем (позволяет восстанавливать данные после ошибок)
3) **LLC3**. Без установления соединения, но с подтверждением (когда нужно быстро, но с подтверждением корректности)

Формат кадров LLCP имеет следующий вид:

0111 1110	DSAP(1 байт)	SSAP(1 байт)	Control(1/2 байт)	Data	0111 1110

DSAP (адрес точки входа службы назначения), **SSAP** (адрес точки входа службы источника), **Control** (управляющее поле) обзрают **заголовок**. Поле данных кадра предназначено для передачи по сети пакетов протокола вышележащих уровней.

10. VLAN

Виртуальной локальной сетью VLAN называется группа узлов сети, трафик которой на канальном уровне полностью изолирован от других узлов сети. Технология VLAN позволяет создавать изолированные сети, которые затем связываются с помощью маршрутизаторов.

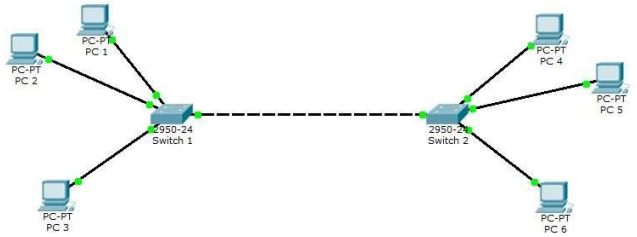
VLAN могут быть построены *только на основе коммутаторов,* правила ее построения определены стандартом IEEE 802.1Q

Возможности, предоставляемые VLAN:

- упрощение управления сетью
- повышение надежности и безопасности сети
- объединение участников обмена в логическую группу
- оптимизация трафика
- организация приоритезации

Основные методы построения VLAN:

1) **По портам**. Сеть строится на основе одного или нескольких коммутаторов, порты коммутаторов приписываются некоторой виртуальной сети. Статическое конфигурирование выполняется администратором. (в cisco packet tracer так делали)



2) **По спискам MAC-адресов.** Каждый MAC-адрес, известный коммутатору, приписывается некоторой виртуальной сети. Это более гибкий метод, чем предыдущий, но все равно администратору надо вручную маркировать MAC-адреса на каждом коммутаторе сети.

Для идентификации **принадлежности кадров** к конкретной VLAN применяется **маркировка** кадров. Маркерный тег (2 байта) вставляется в кадр Ethernet после поля SA (при этом поле данных кадра Ethernet уменьшено на 2 байта, чтобы длина кадра осталась такая же) и имеет структуру:

Ptr (3 бит)	CFI (1 бит)	VID (12 бит)

Ptr – приоритет кадра, **CFI** (Canonical Format Identifier) – бит-идентификатор канонического формата заголовка, **VID** – VLAN ID. Коммутатор, поддерживающий приоритезацию, создает для каждого порта несколько очередей, в которые помещаются кадры в зависимости от приоритета. Что будет происходить дальше с очередями конфигурируется на коммутаторе.

Маркировку кадра выолняет либо сетевой адаптер конечного узла, либо коммутатор, первый получивший кадр, они же и удаляют маркерный тег (при этом пересчитывается контрольная последовательность кадра).

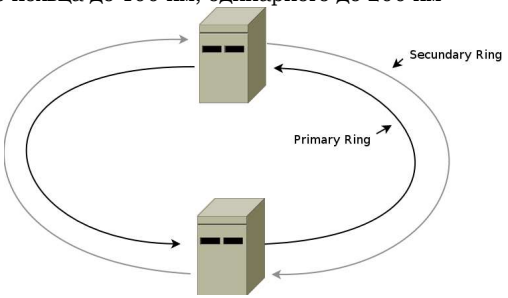
Портам коммутатора, участвующим в формировании VLAN, назначаются атрибуты:

1) PVID (Port VLAN Identifier)
2) P_Ptr (приоритет)
3) T/U/- (tagged member/ untagged member – все проходящие кадры выпускает без тега/ not in VLAN)

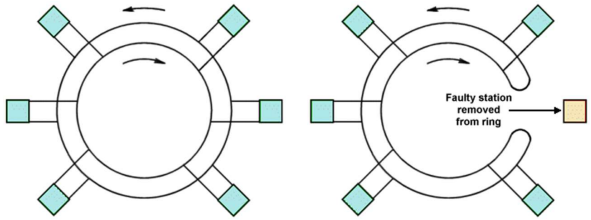
11. FDDI

Технология FDDI – распределенный интерфейс передачи данных по оптоволоконным каналам. Основные характеристики технологии:

- логическая топология – двойное кольцо (*для повышения отказоустойчивости*)
- метод доступа – детерминированный с передачей маркера
- скорость перадачи данных до 100 Мбит/с
- максимальное число станций в сети до 500 с двойным кольцом, до 1000 с одинарным
- длина двойного кольца до 100 км, одинарного до 200 км



Сеть FDDI строится на основе двух оптоволоконных колец, которые образуют основной и резервный пути передачи данных между узлами сети. В нормальном режиме работы сети данные проходят *только через первичное кольцо*. В случае отказа (обрыва кабеля, отказа узла) первичное кольцо объединяется со вторичным, что называется wrap (**свертывание**) колец. Операция свертывания производится средствами концентраторов и/или сетевых адаптеров FDDI.



Модель сети FDDI имеет следующие компоненты:

1) **PMD (Physical Medium Dependent)** – определяет параметры кабельной системы
2) **PHY (Physical) –** определяют методы кодирования и синхронизации сигналов (1 + 2 соответствуют физическому уровню модели OSI)
3) **SMT (Station Management)** – выполняет фунции по управлению кольцом:
   - Инициализация кольца
   - передача управляющих кадров, связывающих все станции
   - координация управления включением станций в кольцо
   - управление физическим соединением
   - самодиагностика станций
   - контроль за состоянием маркера
4) **MAC** – реализует протокол маркерного метода доступа к среде.

В стандарте FDDI допускается два вида подключения:

1) Dual Attachment (DA) – двойное подключение: одновременное подключение к первичному и вторичному кольцам
2) Single Attachment (SA) – одиночное подключение: только к первичному кольцу

Станции могут быть двух классов:

1) Класса A – станции DAS двойного подключения (два трансивера)
2) Класса B – станции SAS одиночного подключения (один трансивер)

Концентраторы (выполняют функцию поддержки целостности логического кольца) также могут быть SAC, DAC (одинарного и двойного типов).

Кадры двух типов: маркер, команда/данные.

Маркер:

Preamble	SD (start delimiter)	FC (признак маркера)	ED (end delimiter)
≥ 16	2	2	2

Команда/данные:

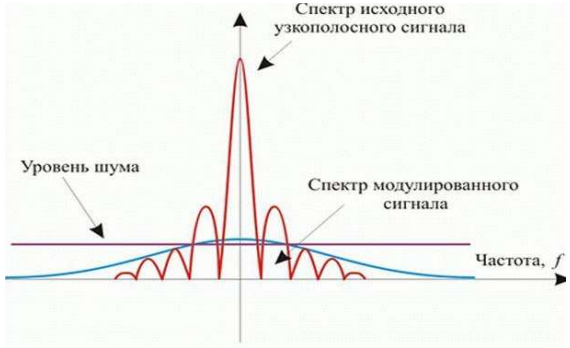
Pre	SD	FC	DA (dest addr)	SA (src addr)	Info	FSC (контрольная сумма)	ED	FS (frame status)
≥ 16	2	2	12	12	≥ 0 пар	8	1	≥ 3

12. Беспроводные сети

Беспроводные сети – сети- позволяющие организовывать передачу данных без использования кабельных систем. Беспроводная связь осуществляется в радиочастотнм диапазоне 0.9 – 7 ГГц электромагнитных волн. Стандарт беспроводных сетей – IEEE 802.11 (aka WiFi; частотный диапазон от 2400 до 2483.5 МГц шириной 83.5 МГц).

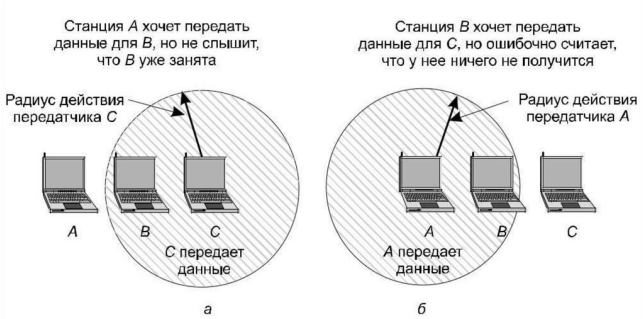
Для беспроводных сетей характерны два основных типа архитектуры: **Ad Hoc** (Independent Basic Service Set/Peer to Peer (точка-точка) *станции непосредственно взаимодействуют друг с другом*), **Infrastructure Mode** (станции взаимодействуют через точку доступа (AP – Access Point)). В Infrastructure Mode разделяют два режима взаимодействия с точками доступа – BSS (Basic – все станции связываются только через точку доступа), ESS (Extended – инфрструктура нескольких BSS, связанных точками доступа).

В основе всех беспроводных протоколов семейства WiFi лежит **технология уширения спектра** SS (чтобы все поместились). Главная идея в том, что для кодирования сигнала при передаче используется более широкий частотный диапазон.



В основе управления доступом к среде алгоритма CSMA/CA (В обычном CSMA/CD отправитель убеждается, что среда свободна, отправляет кадр, приемник с нужным адресом забирает. Если среда занята, то отправитель ждет освобождения). Особенность беспроводных сетей в том, что при передаче важна интерференция сигналов на приемнике, а не передатчике. Можно выделить две проблемы:

1) **Проблема скрытой станции (а)** Такая передача будет интерферировать на В и исказит кадры, передаваемые С
2) **Проблема засвеченной станции (б)** Такая передача создала бы помехи только в зоне А, но не в С

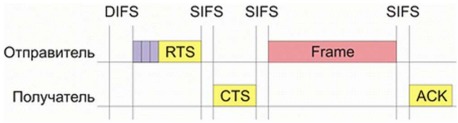


На MAC-уровне протокола WiFi определяются два типа коллективного доступа к среде передачи данных:

- **функция распределенной координации** (**DCF** – Distributed Coordination Function). Основана на методве коллективного доступа с обнаружением несущей и механизмом избежания коллизий CSMA/CD:
    1) каждый узел «прослушивает» среду, пытаясь обнаружить несущий сигнал, и если среда свободна, то может начать передачу
    2) чтобы избежать коллизий, каждый узел перед началом передачи выжидает случайный промежуток времени (обязательный промежуток **DIFS** + случайный промежуток обратного отсчета **backoff time**). Если за время ожидания другой узел начал передачу, то ждем пока освободится

  Для минимизации коллизий в методе DCF использует алгоритм:
    1) после успешного приема кадра принимающая сторона через короткий промежуток времени SIFS подтверждает успешный прием, посылая ACK
    2) если в процессе передачи данных вощникла коллизия, то передающая сторона не получает ACK. В этом случае размер CW-окна для передающего узла увеличивается для каждой i-ой перадчи $CW_i = 2CW_{i-1} + 1$. Это позволяет уменьшить временные задержки и снизить вероятность возникновения коллизий.

  Для решения проблемы скрытой станции используется алгоритм **RTS/CTS (Ready To Send/Clear To Send**). Перед тем, как послать данные, каждый узел сети:
    1) отправляет короткое сообщение RTS, содержащее информацию о продолжительности предстоящей передачи и адресате. Оно доступно всем узлам сети.
    2) приемная станция, получив RTS, отвечает посылкой сигнала CTS, который говорит о готовности станции к приему информации
    3) передающая станция посылает пакет данных, а приемная должна ответить квитанцией ACK, подтверждающей бехошибочный прием

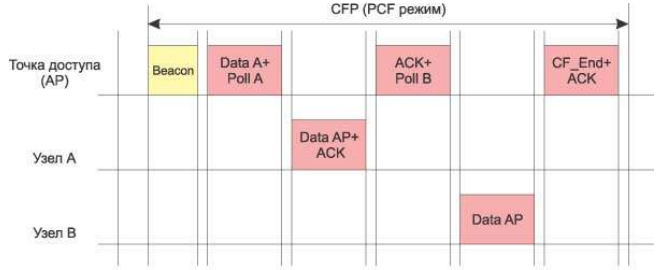


Недостаток RTS/CTS в возможности ложных блокировок станций, что может привести к снижению эффективности использования среды передачи данных.

- **функция централизованной координации** (**PCF** – Point Coordination Function). Применяется только в сетях с точкой доступа, которая выступает в качестве **центра координации** (PC – Point Coordinator). На него возлагается задача управления коллективным доступом для всех остальных узлов сети к среде передачи данных. Фактически PCF реализуется совместно с DCF. Для чередования режимов PCF, DCF необходимо,чтобы центр координации имел приоритетный доступ к среде передачи данных. Для этого интервал ожидания PIFS удовлетворяет условию: SIFS < PIFS < DIFS.
  Режимы PCF и DCF объединяются в **суперфрейме**, который образуется из промежутка бесконкурентного доступа к среде **CFP**, и следующего за ним промежутка конкурентного доступа к среде **CP**.

<---------- CFP ---------->		<----------CP---------->
Beacon	PCF	DCF
<---------- Суперфрейм ---------->		

Суперфреймы несут служебную информацию о продолжительности CFP-интервала и позволяют синхронизировать работу всех узлов сети. Во время режима PCF точка доступа опрашивает все узлы о кадрах, которые стоят в очереди на передачу, посылая им служебные кадры **CF_Poll**, те в ответ посылают **CF_Ack**.Чтобы иметь возможность передавать данные между всеми узлами сети, точка доступа может передавать кадр данных (Data) и отправлять вместе с CF_Poll. Узлы сети могут посылать данные вместе с CF_Ack.



13. Структуризация сети: мосты и коммутаторы. Их виды

Под **логической структуризацией сети** понимается разбиение общей разделяемой среды на логические сегменты, которые представляют самостоятельные разделяемые среды с меньшим кол-вом узлов. Зачем надо? Построение сетей на основе одной разделяемой среды имеет ограничения:

- почти все технологии ЛС ограничивают кол-во узлов в разделяемой среде
- *перегрузка разделяемой среды*

Разделение на логические сегменты:

- повышает производительность сети за счет разгрузки сегментов
- повышает гибкость построения сети, увеличивая степень защиты данных
- облегчает управление сетью

Сеть разделяется на логические сегменты с помощью устройств двух типов – **мостов** и **коммутаторов** (switch), работающий на *канальном уровне* стека протоколов. Также могут использоваться **маршрутизаторы** (router), которые работают на *сетевом уровне.*

МОСТЫ

Алгоритм прозрачного моста. Основан на использовании **адресной таблицы** (АТ/ **таблица маршрутизации/фильтрации**), содержащей поля: MAC-адрес узла; номер порта, через который доступен узел; тип записи. Записи в АТ могут быть динамическими (создаются в процессе самообучение моста, имеют срок жизни) и статическими. Алгоритм:

1) АТ пуста, любой буферизированный кадр мост передает на все свио порты, за исключением того, от которого кадр получен. Одновременно мост анализирует адрес источника кадра и делает новую запись в АТ.
2) АТ не пуста, при получении кадра мост находит номер порта, к которому подсоединен сегмент с узлом назначения.
   2.1) Если узел-источник и узел-получатель в разных сегментах, то мост выполняет операцию **продвижения** (forwarding) кадра: передает кадр на порт назначения, прдеварительно получив доступ к этому сегменту.
   2.2) Если узлы принадлежат одному сегменту, то кадр удаляется из буфера, что называется **фильтрацией**.
   2.3) Если адрес узла-получателя неизвестен, то мост передает кадр на все порты, кроме порта-источника кадра.
   2.4) Кадры с широковещательными MAC-адресами передаются на все его порты, что называется **затоплением сети**.

Типы мостов: **прозрачные** (объединяются сети с едиными протоколами канального и физического уровней), **транслирующие** (объединяются сети с различными протоколами канального и физического уровней), **инкапсулирующие** (соединяют сети с едиными протоколами канального и физического уровня через сети с другими протоколами)

КОММУТАТОРЫ

Рассмотрим коммутатор EtherSwitch на 8 портов. Каждый порт коммутатора обслуживается процессором пакетов **EPP** (Ethernet Packet Processor – специализированные микросхемы). *Системный модуль* координирует работу всех процессоров EPP. Кроме того, он ведет адресную таблицу коммутатора (по структуре такая же, как у моста); обеспечивает управление коммутатором по протоколу SNMP (сетевой уровень). *Коммутационная матрица* – это аппаратная схема, позволяющая организовать цепь передачи логического сигнала между любой парой портов. Недостаток коммутационных матриц в отсутствии буферизации внутри матрицы в случае невозможности построения канала из-за занятости выходного порта или промежуточных элементов.

Плюсы использования коммутаторов:

- не нужна замена установленного в сетях оборудования – сетевых адаптеров и кабельной системы
- коммутаторы не оказывают никакого влияния на имеющиеся в сети маршрутизаторы (они прозрачны для протоколов сетевого уровня)
- коммутатор самообучается и не требует конфигурирования

На производительность коммутатора влияют:

- скорость фильтрации кадров (как быстро буферизирует кадр и определяет по АТ порт назначения либо уничтожает кадр, если в одном сегменте отправитель и получатель)
- скорость продвижения кадров (как быстро передает кадр в сеть через выходной порт, определенныый по АТ)
- пропускная способность (сколько данных может передать в единицу времени через свои порты)
- задержка передачи кадра ($t_{появления\_на\_выходном\_порту} - t_{появления\_на\_входном\_порту}$)

ВИДЫ КОММУТАТОРОВ

На сегодняшний день существует большое разнообразие коммутаторов, отличающихся как внутренней организацией, так и набором выполняемых дополнительных функций (например *трансляция протоколов, приоритезация трафика, поддержка алгоритма покрывающего дерева, образование виртуальных логических сетей*). По конструкции коммутаторы делятся на:

1) **Автономные**. Фиксированное количество портов
2) **Модульные**. Выполняются на основе комбинированных схем, в которых взаимодействие модулей реализуется на высокоскоростной шине или на основе быстрой разделяемой памяти большого объема. Модули такого коммутатора выполняются на основе технологии “hot swap”, т.е. допускают замену на ходу, без выключения.

3) **Стековые**. Образуются на базе автономно работающих коммутаторов, имеющих специальные интерфейсы (высокоскоростную шину) для их *объединения в общую систему* (**стек**), работающую как единый коммутатор.

Разница между мостом и коммутатором состоит в том, что мост в каждый момент времени может осуществлять передачу только одного потока кадров и только между двумя портами, а коммутатор способен одновременно передавать несколько потоков данных между любыми своими портами. Другими словами, мост передает кадры последовательно, а коммутатор параллельно.

Мосты используются только *для связи локальных сетей с глобальными*, то есть как средства удаленного доступа, поскольку в этом случае необходимость в параллельной передаче между несколькими парами портов просто не возникает.

14. Коммутация с полной буферизацией и «на лету». Spanning Tree Protocol

Есть два подхода к коммутации:

1) **С полной буферизацией**. Предполагает, что EPP полностью буферизирует поступивший на порт кадр. Затем EPP анализирует заголовок, занося адрес отправителя в AT. По адресу назначения EPP определяет выходной порт, в который будет передаваться кадр (если не может найти, то обращается к системному модулю). Если надо, то EPP отфильтровывает кадр, очищает буфер и ждет следующего кадра. Если же надо передать кадр на другой порт, то EPP обращается к коммутационной матрице для построения канала к порту назначения (если занято, подождет).
   После построения канала в него сразу направляются буферизованные байты кадра, которые принимаются EPP выходного порта. Как только EPP выходного порта получает доступ к подключенному к нему сегменту Ethernet по протоколу CSMA/CD, байты кадра сразу же начинают передаваться в сеть.

2) **Коммутация «на лету»**. Представляет собой конвейерную обработку кадра, совмещая по времени несколько этапов его передачи. После принятия первых 6 байт (там содержится адрес получателя) EPP может уже начать пересылку кадра в выходной порт, если коммутационная матрица разрешает, при этом продолжая прием оставшихся байт кадра. Хотелось бы без буферизации, но если порт занят, то по-другому никак.

Тогда основным методом повышения производительности коммутаторов является параллельная обработка кадров. В идеальном случае коммутатор с N портами обеспечивает N/2 независимых путей. Общая производительность тогда (N/2)*C, где C – пропускная способность протокола доступа к среде. В ЛС обычно используются ***неблокирующие коммутаторы***, которые могут передавать кадры с такой же скоростью, с которой они на них поступают.

При объединении коммутаторов для их нормальной работы не должно быть замкнутых маршрутов. Однако администратор может их специально создавать для образования резервных связей. Чтобы все работало, коммутатор должен поддерживать **алгоритм покрывающего дерева** (Spanning Tree Algorithm), позволяющие автоматически создавать активную древовидную конфигурацию связей без петель на множестве всех связей сети. Такая конфигурация называется **покрывающим деревом**.

Коммутаторы определяют оптимальное покрывающее дерево с помощью обмена служебными пакетами, называемыми протокольными блоками данных моста **BPDU** (Bridge Protocol Data Unit). Пакеты BDPU помещаются в поле данных кажров канального уровня, которые рассылаются широковещательно.

Алгоритм:

1) Определение **корневого коммутатора** RS (root switch) – корня покрывающего дерева. Определяется либо автоматически (с минимальным MAC-адресом блока управления), либо администратором.
2) Определение для каждого коммутатора **корневого порта** RP (root port), имеющего кратчайшее расстояние до любого из портов корневого коммутатора.
3) Выбор для каждого сегмента сети **назначенного порта** DP (designated port), имеющего кратчайшее расстояние от данного сегмента до корневого коммутатора.
4) Блокировка портов, не попавших в RS, RP, DP

Расстояние до RS определяется как *суммарное условное время* на передачу одного бита данных от порта данного коммутатора до порта RS.

15. Идея Internetworking. Маршрутизация и функции маршрутизатора

Создание сложной, структурированной сети, интегрирующей различные базовые технологии, может осуществляться средствами канального уровня с использованием некоторых типов местов и коммутаторов. Однако построение сложных сетей только на основе повторителей, мостов и коммутаторов имеет существенные ограничения и недостатки. Для решения этой проблемы привлекаются средства более высокого, сетевого уровня. Основная идея введения сетевого уровня состоит в следующем:

- сеть рассматривается как совокупность нескольких сетей и называется **составной сетью** или **интерсетью** (internetwork/internet)
- сети, входящие в составную сеть, называются **подсетями** (subnet), составляющими сетями либо просто сетями
- подсети соединяются между собой **маршрутизаторами**

Компонентами составной сети могут быть как **локальные**, так и **глобальные** сети. Режим взаимодействия, когда две или более сети организуют совместную транспортную службу, называется **межсетевым взаимодействием** (internetworking).

Сетевой уровень выступает в качестве **координатора**, организующего работу всех подсетей по обеспечению транспортировки данных между любой произвольной парой узлов этой составно сети. Система адресации сетевого уровня не должна зависеть от локальной адресации в отдельных подсетях. Используется двухуровневая адресация, т.е. положение устройства в сети задается парой (номер сети, номер узла). Номер узла - либо локальный адрес узла (в стеке IPX/SPX), либо любое уникально определяющее в подсети узел число (в стеке TCP/IP).

Сетевой уровень оперирует **пакетами** с заголовком, содержащем *номер сети, нумерацию фрамментов пакета (*для сборки-разборки пакета при транспортировке*), время жизни пакета, качество услуги.*

Сетевой уровень отвечает за **маршрутизацию** – выбор пути передачи пакетов между двумя конечными узлами в составной сети. **Маршрут** – последовательность маршрутизаторов, которые должен пройти пакет от узла-отправителя до узла-получателя. Маршрутизаторы имеют по крайней мере 2 порта, которые выступают

как отдельные узлы сети (имеют собственный сетевой и локальный адреса). То есть маршрутизатор можно рассматривать как совокупность нескольких узлов, принадлежащих разным подсетям. Сам маршрутизатор как устройство не имеет ни локального, ни сетевого адреса.

Задачу выбора маршрута из нескольких возможных решают маршрутизаторы, а также конечные узлы. Маршрут выбирается на основе **таблицы маршрутизации** (ТМ), которая содержит информацию о текущей конфигурации сети, а также указание на критерий выбора маршрута. Структура таблицы:

№ сети назначения	Сетевой адрес входного порта следующего маршрутизатора	Сетевой адрес выходного порта маршрутизатора	Метрика

Алгоритм выбора маршрута является частью ПО сетевого уровня и должен обладать свойствами *корректности, простоты, надежности, устойчивости, справедливости и оптимальности.*

Общий подход к выбору маршрута:

1) когда на маршрутизатор поступает новый пакет, № сети назначения сравнивается с № сетей в ТМ. Строка с совпавшим № указывает на сетевой адрес ближайшего маршрутизатора, куда следует направить пакет.
2) далее из этой строки текущий маршрутизатор определяет сетевой адрес порта, через который может быть осуществлена передача пакета.
3) если ТМ содержит несколько вариантов маршрутов, то принимается во внимание метрика маршрута, используемая по-разному в зависимости от ***класса сервиса*** (например, задержка прохождения маршрута отдельным пакетом; средняя пропускная способность маршрута для последовательности пакетов; количество пройденных в маршруте промежуточных маршрутизаторов (hops)).

Число записей в ТМ часто уменьшают за счет использования специальной записи – **маршрута по умолчанию**.

МЕТОДЫ МАРШРУТИЗАЦИИ

1) Одношаговые алгоритмы
Каждый маршрутизатор определяет только следующий (ближайший) маршрутизатор, лежащий на оптимальном пути к конечному узлу. Существует три класса таких алгоритмов:

1.1) **фиксированная** (статическая) маршрутизации. Все записи в ТМ статические, обычно задаются администратором. При этом может быть задано несколько путей, а может один. Приемлем только в небольших сетях с простой топологией, либо на магистралях крупных сетей, если магистраль имеет простую структуру.

1.2) **простая** маршрутизация. ТМ вообще не используется. Существует три типа: случайная («+»: равномерная загрузка линий связи, «-»: высокая вероятность зацикливания маршрута), лавинная («-»: большое количество дублей пакетов, зато высокая надежность), по предыдущему опыту.

1.3) **адаптивная** (динамическая) маршрутизация. Динамическая маршрутизация должны *обеспечивать рациональность маршрута*; быть *достаточно простой*, чтобы не использовать много сетевых ресурсов; обладать *свойством сходимости* – всегда приходить к однозначному результату за приемлемое время. Такие алгоритмы делятся на ***дистанционно-векторные (DVA)*** и ***алгоритмы состояния связей (LSA)***.
При **DVA** каждый маршрутизатор периодически и широковещательно рассылает по сети вектор с расстояниями от данного маршрутизатора до всех известных ему сетей. Каждый следующий маршрутизатор добавляет расстояния до известных ему сетей.
LSA обеспечивает маршрутизаторы информацией, достаточной для построения точного графа связей сети. При этом все маршрутизаторы работают на основании одинаковых графов, что делает процесс маршрутизации устойчивым к изменениям.

2) Многошаговые алгоритмы
Предполагает, что узел-источник задает в отправляемом в сеть пакете полный маршрут. При таком методе маршрутизации нет необходимоти в ТМ, что ускоряет прохождение пакета по сети и разгружает маршрутизаторы, при этом основная нагрузка ложится на конечные узлы

ФУНКЦИИ МАРШРУТИЗАТОРА

- прием и распределение данных по портам
- выделение/инкапсуляция данных сетевого уровня
- обработка и принятие решения по пакету сетевого уровня
- ведение таблиц маршрутизации

16. Модель DOD (TCP/IP). Классовая и бесклассовая адресации

В отличие от 7-уровневой модели OSI имеет 4-уровня:

OSI	DOD	Протоколы
Приложения	Приложения	HTTP, FTP, SNMP, SMTP, DNS
Представления		
Сеансовый		
Транспортный	Транспортный	TCP, UDP
Сетевой	Межсетевой	IP, ICMP, RIP, OSPF, ARP
Канальный	Сетевого доступа	Ethernet, Token Ring, FDDI, ATM
Физический		

Основой всей архитектуры является **уровень межсетевого взаимодействия** (уровень internet), который реализует концепцию передачи пакетов в режиме без установления соединений, т.е. дейтаграммным способом. Отвечает за передачу данных через составную сеть. **Транспортный уровень** отвечает за надежность информационной связи между двумя конечными узлами. **Уровень приложения** объединяет все службы, предоставляемые системой пользовательским приложениям. **Уровень сетевых интерфейсов** не регламентируется в протоколах TCP/IP, но поддерживает все популярные стандарты физического и канального уровней для глобальных и локальных сетей.

<u>АДРЕСАЦИЯ</u>

В стеке TCP/IP используется три типа адресов: локальные; сетевые IP-адреса; символьные имена.

Локальный адрес узла определяется технологией, с помощью которой построена отдельная сеть, в которую входит данный узел. Для узла, входящего в локальные

сети, - это MAC-адрес сетевого адаптера или порта маршрутизатора. Для узлов, входящих в глобальные сети, локальные адреса назначаются администратором глобальной сети. **IP-адреса** представляют собой основной тип адреса, которые используются на сетевом уровне для передачи пакетов между сетями. Назначается администратором во время конфигурирования компьютеров и маршрутизаторов.

IP-адрес состоит из двух частей: номер сети, номер узла. Номер узла в протоколе IP не зависит от локального адреса узла. Узел может входить в несколько IP-сетей, т.е. IP-адрес характеризует не отдельный компьютер или маршрутизатор, а одно сетевое соединение. **Символьные адреса** удобны для пользователей, поскольку имеют смысловую нагрузку.

Классовая IP адресация — это метод IP-адресации, который не позволяет рационально использовать ограниченный ресурс уникальных IP-адресов, т.к. не возможно использование различных масок подсетей. Использовалась в период с 19821 по 1993 гг., до введения CIDR (см. ниже). Этот метод адресации делит адресное пространство протокола IPv4 на 5 классов адресов: A, B, C, D, E, при этом принадлежность адреса к конкретному классу задается первыми битами адреса.

	0	8	16	24 31
Класс A	0 № сети	№ узла		
Класс B	10 № сети		№ узла	
Класс C	110 № сети			№ узла
Класс D	1110 Адрес многоадресной рассылки			
Класс E	1111 0 Зарезервирован			

Применение такого типа адресации не позволяет экономно использовать ограниченный ресурс адресов IPv4, поскольку *невозможно применение произвольных масок подсетей.* Количество адресов в подсети не равно количеству возможных узлов. Нулевой адрес IP резервируется для идентификации подсети, последний — в качестве широковещательного адреса, таким образом в реально действующих сетях возможно количество узлов на два меньшее количества адресов.

Класс	Начальный адрес	Наибольший адрес	Max число узлов в сети	Маска
A	1.0.0.0	126.0.0.0	2^{24}	255.0.0.0
B	128.0.0.0	191.255.0.0	2^{16}	255.255.0.0
C	192.0.0.0	223.255.255.0	2^{8}	255.255.255.0
D	224.0.0.0	239.255.255.255	multicast	
E	240.0.0.0	247.255.255.255	зарезервирован	

Маска – 32-битовое число, двоичная запись которого содержит единицы в тех разрядах, которые должны быть интерпретироваться как номер сети.

При проектировании составной сети основной задачей администратора является распределение IP-адресов и их назначение узлам сети. При выборе диапазона IP-адресов обычно принимается во внимание следующее:

- если сеть работает автономно, то назначение IP-адресов произвольно. Но чтобы избежать каких-либо коллизий, в стандартах Internet определено несколько диапазонов адресов, рекомендуемых для локального применения (A – из сети 10.0.0.0, B – из сетей 172.16.0.0 – 172.31.0.0, C – из сетей 192.168.0.0 – 192.168.255.0).
- если сеть является частью глобальной сети Internet, номера сетей назначаются централизованно. Возникает проблема дефицита IP-адресов.

Для смягчения проблемы дефицита IP-адресов существуют разные подходы. Кардинальное решение – переход на новую версию протокола IPv6, в которой адресное пространство резко расширяется за счет использования 16-байтных адресов.

В рамках версии IPv4 поддерживаются некоторые технологии, направленные на более экономное расходование IP-адресов. Одной из таких технологий является технология масок и ее развитие – технология **бесклассовой междоменной адресации** CIDR. Это метод IP-адресации, который позволяет рационально управлять пространством IP адресов. *Бесклассовая адресация основывается на переменной длине маски подсети (VLSM), в то время, как в классовой адресации длина маски строго фиксирована 0, 1, 2 или 3 установленными октетами.*

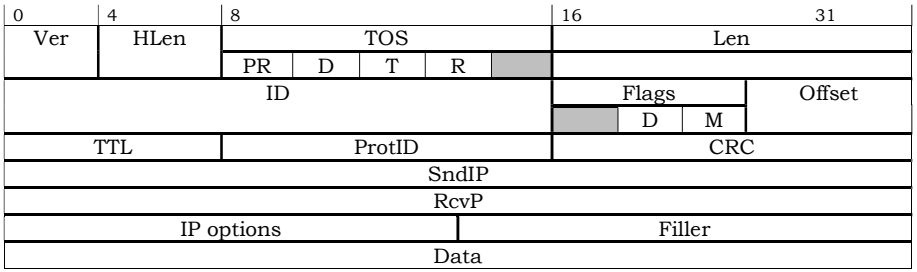
17. Протоколы IPv4, IPv6, ARP

Протокол IP составляет основу транспортных средств стека протоколов TCP/IP. Протокол IP относится к протоколам без установления соединений. Его основные функции:

- обеспечение передачи IP-дейтаграмм или IP-пакетов от отправителя к получателям через объединенную систему КС.
- выполнение динамической фрагментации пакетов при передаче их между сетями с различными максимально допустимыми значениями поля данных кадров (MTU)

В IPv4 используется классовая схема адресации (см. предыдущий вопрос). Использует 4-байтные адреса, ограничивающие адресное пространство 2^{32} возможными адресами. Традиционной формой записи IPv4 адреса является запись в виде четырех десятичных чисел от 0 до 255, разделенных точками. Через дробь указывается длина маски подсети. Некоторые адреса IPv4 зарезервированы для специальных целей и не предназначены для глобальной маршрутизации.

IP-пакет имеет следующую структуру:



Ver – номер версии протокола IP (пока что идет переход от IPv4 к IPv6, поэтому нужно это поле)

HLen – длина заголовка в 32-битных словах

TOS – тип сервиса, задает приоритетность пакета и вид критерия выбора маршрута: PR (priority, от 0 до 7 (обычный < приоритетный < немедленный < срочный < экстренный < critical emergency signal < межсетевое управление < сетевое управление)), D (delay - минимизация задержки доставки пакета), T (transmission - максимизация пропускной способности), R (reliability - максимизация надежности).

Len – длина пакета с учетом заголовка и поля данных.
TTL – сколько времени может пройти от отправления до получения.
ProtID – указывает, какому протокола верхнего уровня принадлежит информация в поле данных. (1 – CMP, 2 - IGMP, 4 – IP over IP, 6 – TCP, 17 UDP)
CRC – контрольная сумма пакета, рассчитывается только по заголовку.
Flags содержит признаки, связанные с фрагментацией (фрагментация IP-пакетов связана с тем, что их размер может превышать MTU технологии, через которую он продвигается). Фрагментация – это деление пакета на части, кратный 8 байтам, за исключением последней. Каждая из них помещается в новый пакет. Получатель использует поле ID для распознавания пакетов, образовавшихся путем фрагментации исходного пакета. Все фрагменты должны иметь одинаковое уникальное значение этого поля для каждой пары отправитель-получатель. Значения флагов: D (do not fragment – запрещает маршрутизатору фрагментировать данный пакет), M (more fragments – говорит, что данный пакет является промежуточным фрагментом).
Offset – смещение поля данных этого пакета от начала общего поля данных исходного пакета, подвергнутого фрагментации.

IPv6 (2^{128} адресов)

Целями создания IPv6 были:

- увеличение пространства IP-адресов
- уменьшение размера таблиц маршрутизации
- упрощение протокола для ускорения обработки пакетов маршрутизаторами
- улучшение безопасности
- указание типа сервиса, в частности при передаче данных реального времени
- добавление многоадресной рассылки с помощью указания области рассылки
- возможность изменение положения хоста без изменения адреса

В общем случае протокол IPv6 несовместим с IPv4, но зато совместим с остальными протоколами Internet, включая TCP, UDP, ICMP, IGMP, OSPF, BGP, DNS. Структура заколовка протокола IPv6:

<table>
<tr><td>0</td><td>4</td><td colspan="3">8 16 31</td></tr>
<tr><td>Ver</td><td>Priority</td><td colspan="3">Flow label</td></tr>
<tr><td colspan="3">Payload Length</td><td>Next Header</td><td>Hop Limit</td></tr>
<tr><td colspan="5">IP-адрес отправителя</td></tr>
<tr><td colspan="5">IP-адрес получателя</td></tr>
</table>

Priority – используется, чтобы отличать пакеты, к отправителям которых может быть применено управление потоком.
Flow label – метка потока, является экспериментальной, но будет применяться для установки между отправителем и получателем псевдосоединения с особыми свойствами и требованиями к передаваемому потоку.
Payload length – длина полезной нагрузки, длина жданных за 40-байтовым заголовком.
Next Header – следующий заголовок указывает на наличие дополнительных заголовков.
Hop length – максимальное число транзитных участков (как TTL, только не по времени).

Разделение адресного пространства IPv6 основано на использовании **префикса** (первый байт адреса). При этом реализуется идея использования раздельных префиксов для адресов провайдеров и географических адресов. Каждому провайдеру будет выделена некоторая доля адресного пространства. Префикс имеет вид (реестр обозначает принадлежность поставщика услуг):

010	Реестр (5 бит)

Географическая модель соответствует сегодняшнему Internet, в котором поставщики не играют большой роли.
Для написания 16-байтных адресов используется новая нотация: адреса записываются в виде 8 групп по 4 шестнадцатеричные цифры, разделенные двоеточиями, например 8000::123:4567:89AB:CDEF (два двоеточия – это нули опускаются)

ARP

Протокол ARP используется для определения локального адреса по IP-адресу, обратную задачу решает протокол RARP. Работа ARP основана на использовании ARP-таблицы, в которой каждая строка устанавливает соответствие между IP и MAC адресами. Она строится для каждой сети, подключенной к сетевому адаптеру или порту маршрутизатора. Структура таблицы:

IP-адрес	MAC-адрес	Тип записи

Тип записи: *статический* или *динамический*. Статические записи создаются вручную, динамические – модулем протокола ARP и имеют время жизни (несколько минут), после которого удаляются. Таким образом, в таблице хранятся только активные участники сетевых операций, поэтому таблицу часто называют ARP-кэшем.

18. Протокол DHCP

Протокол DHCP предназначен для динамического назначения IP-адресов, хотя и не исключает более простого ручного и автоматического назначения адресов.

- При **ручной процедуре назначения адресов** администратор предоставляет DHCP-серверу информацию о соответствии IP-адресов физическим адресам или другим идентификаторам клиентов. Эти адреса сообщаются клиентам в ответ на их запросы к DHCP-серверу.
- При **автоматическом статическом способе** DHCP-сервер присваивает IP-адрес из пула наличных IP_адресов без вмешательства оператора. Границы пула задает администратор при конфигурировании DHCP-сервера. *Между идентификатором клиента и его IP-адресом существует постоянное соответствие*, которое устанавливается в момент первичного назначения сервером DHCP IP-адреса клиенту. Т.е. если отправить запрос еще раз, выдаст тот же IP-адрес.
- При **динамическом распределении адресов** DHCP-сервер выдает адрес клиенту на ограниченное время – *продолжительность аренды*, что дает впоследствии повторно использовать IP-адрес другими компьютерами. Динамическое распределение адресов позволяет строить IP-сеть, количество узлов в которой намного превышает количество имеющихся в распоряжении администратора IP-адресов.

Использование DHCP *освобождает администратора сети от конфигурирования сети* и обеспечивает надежный и простой способ конфигурации сети TCP/IP,

гарантируя отсутствие конфликтов адресов за счет централизованного управления их распределением.

Протокол DHCP использует модель «клиент-сервер».

1) При старте компьютер-клиент DHCP, находящийся в стадии **инициализация**, посылает сообщение **discover**, которое широковещательно распространяется по локальной сети и передается всем DHCP-серверам сети.
2) Каждый DHCP-сервер, получивший это сообщение, отвечает на него сообщением **offer**, которое содержит IP-адрес и конфигурационную информацию.
3) Компьютер-клиент DHCP переходит в состояние **выбор** и собирает конфигурационные предложения от DHCP-всерверов. Затем он выбирает одно из предложений, переходит в состояние **запрос** и отправляет сообщение **request** тому DHCP-сервеу, чье предложение выбрал.
4) Выбранный DHCP-сервер посылает сообщение DHCP **acknowledgement,** содержащее IP-адрес, который был послан ранее. Кроме того, он посылает параметры сетевой конфигурации.
5) После того как клиент получил подтверждение, он переходит в состояние **связь,** находясь в котором, он может принимать участие в работе сети.

Проблемы, возникающие при исполльзовании DHCP:

- Необходимо согласовывать информационную адресную базу в службах DHCP и DNS
- Нестабильность IP-адресов усложняет процесс управления сетью (системы управления, основанные на SNMP, например, расчитывают на статичность IP-адресов; при конфигурации фильтров маршрутизаторов тоже проблемы)
- При отказе DHCP-сервера снижается надежность системы – все его клиенты оказываются не в состоянии получит IP-адрес.

19. Методы маршрутизации. Функции маршрутизатора

Маршрутизация – выбор пути передачи пакетов между двумя конечными узлами в составной сети. **Маршрут** – последовательность маршрутизаторов, которые должен пройти пакет от узла-отправителя до узла-получателя. Маршрутизаторы имеют по крайней мере 2 порта, которые выступают как отдельные узлы сети (имеют собственный сетевой и локальный адреса). То есть маршрутизатор можно рассматривать как совокупность нескольких узлов, принадлежащих разным подсетям. Сам маршрутизатор как устройство не имеет ни локального, ни сетевого адреса.

1) Одношаговые алгоритмы маршрутизации

Каждый маршрутизатор определяет только следующий (ближайший) маршрутизатор, лежащий на оптимальном пути к конечному узлу. Существует три класса таких алгоритмов:

1.4) **фиксированная** (статическая) маршрутизации. Все записи в ТМ статические, обычно задаются администратором. При этом может быть задано несколько путей, а может один. Приемлем только в небольших сетях с простой топологией, либо на магистралях крупных сетей, если магистраль имеет простую структуру.

1.5) **простая** маршрутизация. ТМ вообще не используется. Существует три типа: случайная («+»: равномерная загрузка линий связи, «-»: высокая вероятность зацикливания маршрута), лавинная («-»: большое количество дублей пакетов, зато высокая надежность), по предыдущему опыту.

1.6) **адаптивная** (динамическая) маршрутизация. Динамическая маршрутизация должны *обеспечивать рациональность маршрута*; быть *достаточно простой*, чтобы не использовать много сетевых ресурсов; обладать *свойством сходимости* – всегда приходить к однозначному результату за приемлемое время. Такие алгоритмы делятся на ***дистанционно-векторные (DVA)*** и ***алгоритмы состояния связей (LSA)***.
При **DVA** каждый маршрутизатор периодически и широковещательно рассылает по сети вектор с расстояниями от данного маршрутизатора до всех известных ему сетей. Каждый следующий маршрутизатор добавляет расстояния до известных ему сетей.
LSA обеспечивает маршрутизаторы информацией, достаточной для построения точного графа связей сети. При этом все маршрутизаторы работают на основании одинаковых графов, что делает процесс маршрутизации устойчивым к изменениям.

2) Многошаговые алгоритмы маршрутизации

Предполагает, что узел-источник задает в отправляемом в сеть пакете полный маршрут. При таком методе маршрутизации нет необходимоти в ТМ, что ускоряет прохождение пакета по сети и разгружает маршрутизаторы, при этом основная нагрузка ложится на конечные узлы

ФУНКЦИИ МАРШРУТИЗАТОРА

- прием и распределение данных по портам
- выделение/инкапсуляция данных сетевого уровня
- обработка и принятие решения по пакету сетевого уровня
- ведение таблиц маршрутизации

20. Динамическая маршрутизация. Протокол RIP

Динамическая (адаптивная) маршрутирация обеспечивает автоматическое обновление **таблицы маршрутизации** (ТМ) после изменения конфигурации сети. Динамическая маршрутизация должны обеспечивать *рациональность маршрута*; *быть достаточно простой*, чтобы не использовать много сетевых ресурсов; обладать *свойством сходимости* – всегда приходить к однозначному результату за приемлемое время. Основное преимущество динамической маршрутизации в том, что она позволяет автоматичски обнаруживать вышедшие из строя каналы связи и маршрутизаторы, а также корректировать в связи с этим маршруты передачи данных.

Такие протоколы делятся на **дистанционно-векторные** (**DVA**) и протоколы маршрутизации по **состоянию каналов связи** (**LSRP**), а также протоколы смешанного типа.

Работа **DVRP** основана на рассылке **векторов расстояний** (V_p – набор пар (сеть, расстояние до сети), извлеченный из ТМ). Каждый маршрутизатор периодически и широковещательно рассылает по сети V_p. Вектор распространяется через все интерфейсы маршрутизатора, подключенные к сети. В качестве **метрики** маршута протоколы этого типа используют количество **транзитов** (маршрутизаторов), которые необходимо преодолеть на пути к адресату, иногда время задержки. Каждый маршрутизатор также периодически получает V_p от других

маршрутизаторов, увеличивает расстояния на 1, после чего сравнивается со значением в ТМ (если получилось меньше, заменяем). НЕДОСТАТКИ: избыточный трафик в сети из-за широковещательной рассылки; при изменении топологии не факт что будет работать.

LSRP прооколы используют для оценки маршрута параметр(ы), описывающий состояние канала связи:

- производительность полосы пропускания
- задержка
- нагрузка
- максимальный модуль пересылки

LSRP протоколам свойственны следующие характеристики:

- работа протоколов построена на основе рассылки многоадресных сообщений
- триггерное обновление ТМ инициируется автоматически каким-то событием и только в том случае, когда в сети происходят реальные изменения (и обновления содержат только изменения)
- обеспечивают бесклассовую маршрутизацию: в сообщение об обновлении включена маска подсети
- учитывают параметры ToS в заголовке IP-пакета.

Протоколы **смешанного типа** разрабатываются на основе DVRP-протоколов путем расширения их возможностей через включение различных параметров состояния канала связи. Например, EIGRP.

ПРОТОКОЛ RIP

Routing Information Protocol – протокол внутренней маршрутизации класса **DVRP,** в настоящее время используется две версии RIPv1, RIPv2. Рассчет оптимальных маршрутов основан на алгоритмах *Беллмана-Форда* и *Форда-Фалкерсона*. Основная метрика маршрута – число транзитных участков. Информацию о маршрутах и их обновлении протокол получает через широковещательные рассылки: используют UDP.

Узел в сети, использующий протокол RIP, может работать в **активном** (вектор расстояний передается остальным маршрутизаторам периодически) либо **пассивном** (векторы расстояний не передается маршрутизаторами, но передаются и принимаются сообщения, влияющие на них) режиме.

Формат RIP-сообщения (где * - это есть только в RIPv2):

0	8	16 31
Команда	Версия	ID RIP-системы *
Идентификатор семейства адресов		Метка для внешних маршрутов *
IP-адрес		
Маска сети *		
Адрес следующего маррутизатора *		
DIST		

Команда – задает вид сообщения, обозначающее запрос (код 1) или ответ (код 2). Запрос обычно отправляется маршрутизатором, которому надо обновить ТМ.

Идентификатор семейства адресов (AFI) определяет конкретный используемый стек протоколов.

Для предотвращения петель и для улучшения времени сходимости используются дополнительные механизмы:

- **Split horizon** — запрещает маршрутизатору возвращаться на интерфейс, с которого он пришел;
- **Route poisoning** — принудительное удаление маршрута и перевод в состояние удержания.

21. Протокол OSPF

Протокол маршрутизации **OSPF** (Open Shortest Path First) – открытый алгоритм предпочтительного выбора кратчайшего маршрута, принадлежит классу LSRP (маршрутизация на основе состояния каналов связи). В настоящее время является основным протоколом внутреннего шлюза. Если используется как протокол внешнего шлюза, то есть два варианта:

- Внешний маршрут расчитывается по тому же алгоритму, что и внутренний
- Алгоритм OSPF вычисляет маршрут только до входного шлюза AS-получателя.

Основные свойства протокола:

- в основу работы положен открытый алгоритм
- учитывает весь спектр различных метрик маршрутов, свойственных классу LSRP
- алгоритм является динамическим, автоматически и быстро адаптирующимся к изменениям топологии сети
- поддерживает выбор маршрутов, основываясь на типе сервиса ToS
- обеспечивает бесклассовую маршрутизацию данныз с испльзованием масок подсетей переменной длины
- поддерживает иерархические системы
- обеспечивает необходимый минимум безопасности, защищающий маршрутизаторы
- поддержка маршрутизаторов, соединенных с Internet по туннелю

В OSPF AS представляется *ориентированным графом* с двумя типами вершин: маршрутизаторы и сети (узлы). Дуги соответствуют связи между маршрутизатором и маршрутизатором, узлом или сетью, у дуг есть стоимости. Полное описание графа OSPF-системы хранится в **базе данных состояния связей LSDB** – таблица, где для каждой пары смежных вершин указана дуга и стоимость дуги.

Для расчета оптимальных путей в графе используется алгоритм SPF, предложенный Дейкстрой. Результат работы алгоритма – таблица, где для каждой вершины V графа указан список дуг, соединяющих заданную вершину S с V по кратчайшему пути.

Протокол OSPF позволяет разделить AS на **непересекающиеся пронумерованные области**.

Типы маршрутов при использовании OSPF:

1) **внутриобластные** (уже посчитан Дейкстрой)
2) **межобластные**, три этапа: источник $\xrightarrow{1}$ магистраль $\xrightarrow{2}$ область назначения $\xrightarrow{3}$ адресат. Получается конфигурация звезда

3) **между AS**

Классы маршрутизаторов OSPF:

1) **внутренние**, расположены внутри области
2) **границы област**и, соединяют две и более областей
3) **магистральные**, находятся на магистрали
4) **границы автономной системы**, общаются с маршрутизаторами других AS

Работа OSPF основана на обмене между маршрутизаторами следующими типами сообщений:

1) HELLO-сообщения
2) описание базы данных DD
3) запрос состояния связзи LSR
4) обновление состояния связя LSU
5) подтверждение состояния связей LSack

Структура пакета OSPF:

0	8	16 31
Version	Type	Len
Router ID		
Area ID		
CRC	AuthID	
Auth		
Data		

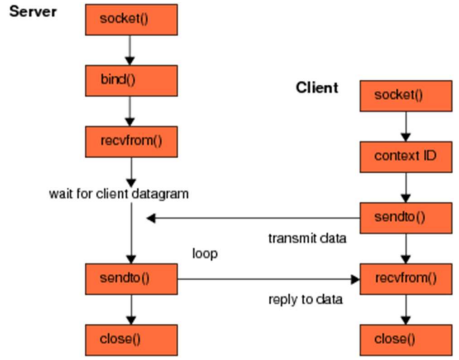
22. Протокол UDP. Передача данных без установления соединения

Протокол UDP (User Datagram Protocol) проектировался для создания в объединенной сети режима передачи дейтаграмм клиента. Протокол UDP **ориентирован на транзакции**, *не гарантирует получение дейтаграмм и защиту от дублирования.* Особенностью данного протокола является возможность широковещательной рассылки данных. Формат UDP-дейтаграммы:

SndPort	RcvPort
Len (и заголовок, и данные)	CRC (охватывает заголовок, данные и псевдозаголовок (берется из заголовка IP))
Data	

Данные, отправляемые прикладным процессом через модуль UDP, достигают места назначения как единое целое. Протокол UDP сохраняет границы сообщений, определяемые прикладным процессом. Он не объединяет несоклько сообщений в одно и не делит одно сообщение на части.

При передаче данных без установления соединения предполагается, что сеть всегда готова принять кадр от конечного узла. Такой метод работает быстро, так как никаких предварительных действий перед отправкой данных не выполняется. Однако трудно организовать отслеживание факта доставки кадра узлу назначения в рамках протокола. Этот метод не гарантирует доставку пакета.



socket() – заявляем системе, «что мы такие есть».
bind() – производит связывание абстрактного порта с конкретным приложением, которая будет обслуживать порт.
close() – освободить связанный с приложением ресурс.

23. Протокол TCP. Потоковая передача данных

В основе TCP-службы лежит модель **сокетов**. Данные, поступающие на транспортный уровень, организованы ОС в виде множества очередей в точках входов прикладных процессов. Такие системные очереди называются **портами** (TSAP-адресами).

Сокет имеет номер, состоящий из *IP-адреса хоста* и *номера порта*. Сокет однозначно определяет прикладной процесс в сети. Номер порта является локальным по отношению к хосту. Назначение номеров прикладных процессов осуществляется:

1) **централизованно**, если процессы представляют общедоступные службы Internet, например, порт 25 закреплен за эл. почтой SMTP;
2) **локально**, если он задается разработчиком приложения;

Для обращения к службе TCO между отправителем и получателем должны установить соединение – образовать информацию состояния (адреса сокетов; последовательные номера передаваемых байтов; размер окна) на каждой из взаимодействующих сторон. Информацию состояния также называют б**локом управления сообщением**.

Один сокет одновременно может участвовать в нескольких соединениях. Все соединения TCP дуплексные и двухточечные. Широковещательная и групповая рассылка протоколом не поддерживается.

Плюсы TCP:

- протокол с установлением соединения: пока узел-отправитель не убедился, что узел-получатель готов принимать данные, ничего не будет
- передает байт за байтом по мере поступления
- гарантирует доставку сообщения и его целостность

Пакет TCP-протокола имеет структуру:

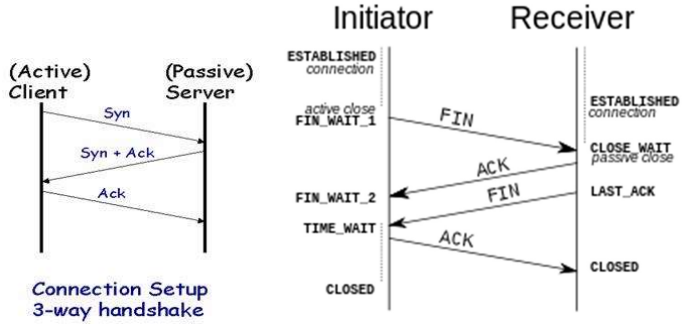
0	16 31
Src Port	DstPort

SeqNum			
AckNum			
HLen		Flags	WinSize
CRC			UrgentInfo(вместе с флагом URG)
Options			Filler
Data			

Flags: URG (urgent), ACK, PSH (отправить данные сразу после получения), RST (сброс соединения), SYN (инициализация соединения), FIN (завершение соединения).
SeqNum, **AckNum** – начальный порядковый номер и номер подтверждения. Обеспечивают корректный порядок пакетов и сообщения о доставке.
WinSize – коичество информации в байтах, которое готов принять отправитель пакета.

ЭТАПЫ ЖИЗНИ СОЕДИНЕНИЯ:

1) установление. Кто ожидает и обрабатывает соединение – сервер, кто устанавливает – клиент.
2) Отправка информации
3) Закрытие соединения. Инициатором закрытия соединения может быть как клиент, так и сервер.



24. Глобальные сети

Глобальные сети (ГС, WAN – Wide Area Network) – компьютерные сети, использующие средства связи дальнего действия для представления сетевых сервисов большому количеству конечных абонентов, расположенных на большой территории.

Существует два типа ГС: **публичные** (например, телефонная связь) и **частные**. Вводятся понятия **владельца сети**, **оператора сети** (компания, обеспечивающая нормальную работу сети), **поставщика услуг** (провайдер – компания, оказывающая платные услуги абонентам сети).

Особенности WAN:

- используются в основном для предоставления конечным пользователям транзитных транспортных механизмов, реализуемых нижними уровнями модели OSI;
- основные прикладыне услуги предоставляются в основном локальными сетями (доступ к данным, проеобразование, защита информации).

Структура ГС вкладывается в общую схему передачи данных. Основу ГС составляют каналы связи и коммутационное оборудование (коммутаторы, соединенные *выделенными* или *коммутируемыми* каналами связи).

По назначению можно выделить **магистральные сети** и **сети доступа**. **Магистральные сети** используются для образования одноранговых связей между ЛС, принадлежащим крупным подразделениям. Магистральные сети должны обеспечивать: высокую пропускную способность; высокий коэффициент готовности.
Под **сетями доступа** понимаются сети, обеспечивающие связи большого кол-ва небольших ЛС и отдельных удаленных компьютеров с магистральной сетью. Должны иметь разветвленную инфраструктуру доступа, быть довольно дешевыми.

В зависимости от способа построения ГС делятс на:

- сети на основе **выделенных каналов**; выделенный канал – канал с фиксированной пропускной способностью, постоянно соединяющий двух абонентов.
- сети на основе **коммутации каналов**; аналоговые или цифровые телефонные сети и цифровые сети с интеграцией услуг ISDN
- сети на основе **коммутации пакетов**.

Пример WAN: **Frame Relay** – общественная сеть, предназначенная для объединения частных ЛС, обеспечивает скорость передачи данных до 2 Мбит/с. Технология **frame relay** в сетях ISDN стандартизирована как сжуба. Преимущество таких сетей в низкой избыточности и дейтаграммном режиме работы, что обеспечивает высокую пропускную способность и небольшие задержки кадров. Надежности, правда, нет.
Работает на основе формирования кадров переменной длины и статическом мультиплексировании TimeDM