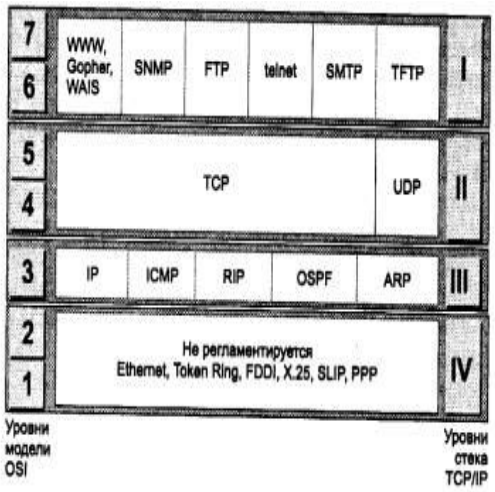
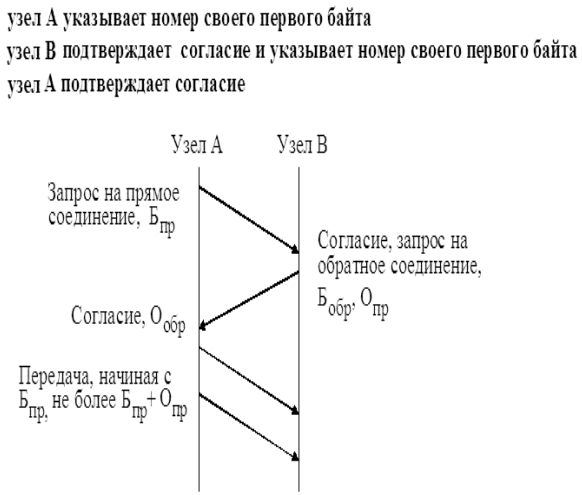
Лекция ТО САПР (продолжение).

Протокол TCP/IP - это средство обмена информацией между компьютерами, объединенными в сеть. Не имеет значения, составляют ли они часть одной и той же сети или подключены к отдельным сетям. Не играет роли и то, что один из них может быть компьютером Cray, а другой Macintosh. **TCP/IP - это не зависящий от платформы стандарт**, который перекидывает мосты через пропасть, лежащую между разнородными компьютерами, операционными системами и сетями. Благодаря программному обеспечению TCP/IP все компьютеры, подключенные к вычислительной сети, становятся "близкими родственниками".



Структура протоколов TCP/IP



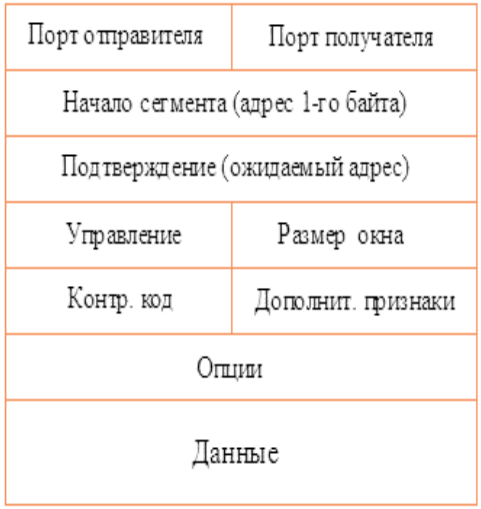
Трехшаговая процедура установления соединения

Стек TCP/IP был разработан до появления модели взаимодействия открытых систем ЭМВОС, он также имеет многоуровневую структуру, соответствие уровней стека TCP/IP уровням модели OSI достаточно условно. Сеть TCP/IP поддерживает все популярные стандарты физического и канального уровней: для локальных сетей это Ethernet, Token Ring, FDDI, Fast Ethernet, Gigabit Ethernet, ATM. Специально для TCP/IP разработан протокол канального уровня PPP (Point to Point Protocol).

TCP — дуплексный транспортный протокол с установлением логического соединения. TCP обеспечивает верхним уровням стека, прикладному и сеансовому, заданный **уровень сервиса** - передачу данных с той степенью надежности, которая им требуется, делит поток байт на части - **сегменты**, и передает их ниже лежащему уровню межсетевого взаимодействия. После того как эти сегменты будут доставлены средствами уровня межсетевого взаимодействия в пункт назначения, протокол TCP снова соберет их в непрерывный поток байт.

Функции протокола: **установление виртуального канала** путем обмена запросом и согласием на соединение, **упаковка и распаковка сообщений** на концах транспортного соединения, **контроль правильности передачи пакетов** (получатель подтверждает правильность полученных данных), **управление потоком** (получатель сообщает размер окна, т.е. диапазон номеров пакетов, которые получатель готов принять), **управление скоростью передачи**.

Схема установления соединения при дуплексной передаче такова: инициатор соединения обращается к своей ОС, которая в ответ выдает номер протокольного порта и посылает сегмент получателю. Номера протокольных портов включаются в заголовок пакета. Получатель должен подтвердить получение запроса и послать свой сегмент-запрос на создание обратного соединения (так как соединение дуплексное). Инициатор должен подтвердить создание обратного соединения. Получается **трехшаговая процедура** установления соединения. Во время этих обменов партнеры сообщают номера байтов $Б_{пр}$ и $Б_{обр}$ в потоках данных, с которых начинаются сообщения и обеспечивают механизм синхронизации в дейтаграммной передаче, реализуемой на сетевом уровне.



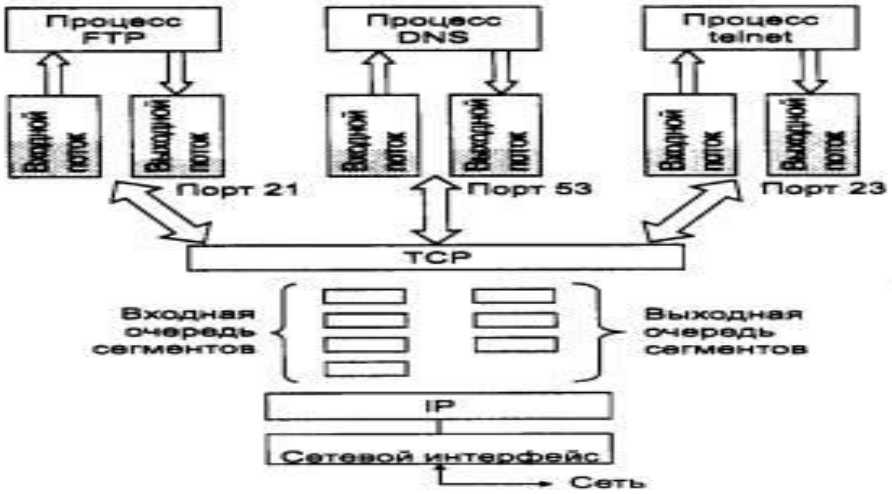
Протокол TCP является **байтовым**, т.е. каждый байт в передаваемых сегментах конкретного сообщения имеет уникальный порядковый номер.
Структура TCP-пакета (в скобках указано число битов) показана рис.2 и представлена следующим списком:
- порт отправителя (16);
- порт получателя (16);
- порядковый номер первого байта в поле данных сегмента (32);
- подтверждение в виде номера первого байта (32) из числа еще не подтвержденных байтов;
- управление (16);
- размер окна (16), т.е. число байт, которое можно послать до получения подтверждения (размер окна указывает получатель в сегментах подтверждения приема);
- контрольная сумма (16);
- дополнительные признаки, например срочность передачи (16);
- опции (24);
- заполнитель (8);
- данные.

Рис. Структура протокола TCP

Порты

Пакеты, поступающие на транспортный уровень, организуются операционной системой в виде множества очередей к точкам входа различных прикладных процессов, называемых **портами.** Адресом назначения, который используется протоколом TCP, является номер порта прикладной службы. Централизованное присвоение сервисам номеров портов выполняется организацией **I**nternet **A**ssigned **N**umbers **A**uthority. Эти номера затем закрепляются и опубликовываются в стандартах Internet. Например, порт http -80, https - 443, FTP - 21, Telnet -23. При локальном присвоении номера порта некоторому приложению, ОС связывает с ним любой доступный числовой идентификатор, так чтобы он не входил в число зарезервированных ISNA номеров портов.

Номер порта в совокупности с номером сети и номером конечного узла однозначно определяют прикладной процесс в сети. Этот набор идентифицирующих параметров имеет название **сокет.** Источник запроса, например, идентифицируется сокетом, образованным IP-адресом и номером порта - **10.0.118.52**:**1244**. Протокол TCP ведет для каждого порта **две очереди**: очередь пакетов, **поступающих в данный порт** из сети, и очередь пакетов, **отправляемых данным портом** в сеть. Процедура обслуживания протоколом TCP запросов, поступающих от нескольких различных прикладных служб, **называется мультиплексированием**. Обратная процедура распределения протоколом TCP поступающих от сетевого уровня пакетов между набором высокоуровневых служб, идентифицированных номерами портов, называется **демультиплексированием**.



Когда требования высокой скорости передачи данных, минимизации задержек превалируют над надежностью и гарантией доставки сообщения, то используется более простой и быстрый **протокол UDP**. Он рассчитан на короткие сообщения, является протоколом дейтаграммного типа, его скорость передачи данных выше, чем TCP, поэтому он используется для передачи, например, аудио и видеоинформации.

Сетевой уровень.

Стержнем всей архитектуры является **уровень межсетевого взаимодействия, уровень IP,** который реализует концепцию передачи пакетов в режиме **без установления соединений**, то есть **дейтаграммным** способом. Этот уровень обеспечивает возможность перемещения пакетов по сети, используя тот маршрут, который в данный момент является наиболее рациональным. Уровень также называют **уровнем internet**, указывая тем самым на основную его функцию - передачу данных через составную сеть.

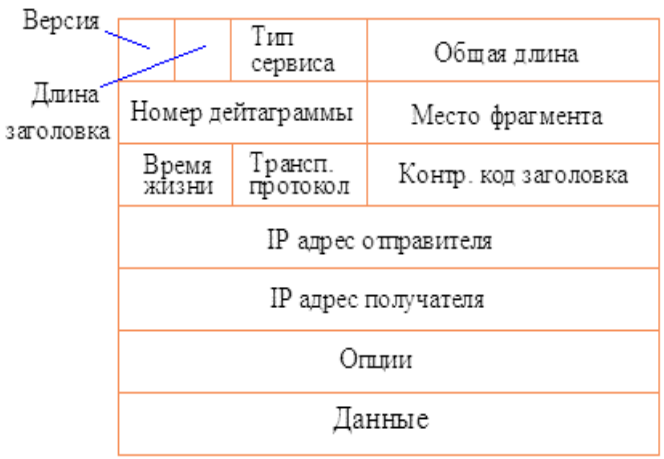


Рис. Структура IP-пакета (соответствует версии IPv4)

Протокол IP — дейтаграммный протокол сетевого уровня без установления соединения отправляет дейтаграммы от одного IP-адреса к другому. Его функции: **фрагментация и сборка пакетов** при прохождении через объединенную систему компьютерных сетей имеющих разные протоколы, **маршрутизация**, **проверка контрольной суммы заголовка** пакета (правильность передачи всего пакета проверяется на транспортном уровне с помощью TCP в оконечном узле), **управление потоком** — сброс дейтаграмм при превышении заданного времени жизни.
Структура дейтаграммы в IP (в скобках указано число бит) показана на рис. 1 и представлена следующим списком:
- версия протокола IP (4) (сейчас практически используются четвертая IPv4 и шестая IPv6 версии);
- длина заголовка (4байт= 32битному слову),
- тип сервиса (8), включает трехбитовое поле приоритета пакета (большее значение кода означает больший приоритет) и 4 признака, соответствующие требованиям к задержке, пропускной способности, надежности и стоимости передачи пакета, лишь один из этих признаков может быть равен 1, т.е. активизирован;

- общая длина (16 байт) информационной части пакета;
- идентификация (16 бит) — порядковый номер дейтаграммы, он используется, если из-за особенностей промежуточных сетей при маршрутизации требуется разделение дейтаграммы на несколько частей, тогда номер дейтаграммы идентифицирует принадлежность фрагмента к определенной дейтаграмме;
- место фрагмента в дейтаграмме (16 бит), номер фрагмента, который используется при восстановлении дейтаграммы из фрагментов;
- время жизни дейтаграммы в сети (8 бит);
- тип протокола (8 бит), который должен использоваться на транспортном уровне для обработки сегмента (TCP, UDP и т.п.);
- контрольный код (CRC) заголовка (16);
- адрес источника (32 бит);
- адрес назначения (32 бит); IP-адрес имеет длину 4 байта и обычно записывается в виде четырех чисел, представляющих значения каждого байта в десятичной форме и разделенных точками, например, 128.10.2.30 - традиционная десятичная форма представления адреса, а 10000000 00001010 00000010 00011110 - двоичная форма представления этого же адреса.
- опции (32);
- данные (не более 65536 бит).

Важной особенностью протокола IP, отличающей его от других сетевых протоколов (например, от сетевого протокола IPX), является его способность выполнять **динамическую фрагментацию пакетов** при передаче их между сетями с различными, максимально допустимыми значениями поля данных кадров MTU. Свойство фрагментации во многом способствовало тому, что протокол IP смог занять доминирующие позиции в сложных составных сетях.

Среди недостатков — 32-битный размер адреса, который соответствуют $2^{32} \approx 4{,}3$ миллиардам адресов, что вызывает затруднения с распределением адресного пространства. Поэтому разработана версия IPv6, в которой применена другая структура заголовка и адресации. В протоколе IPv6 размер адреса увеличен до 128 бит. В структуре IPv6-адреса можно разместить IPv4-адрес, т.е. сети с протоколами этих версий могут работать совместно. Пока (к 2015 г.) большинство доменов Internet работает по протоколу IPv4.

IP-Телефония - это технология, которая использует IP-протокол для передачи голоса и данных. Речевой сигнал от абонентов оцифровывается с использованием современных алгоритмов, которые обеспечивают сжатие голоса без потери качества и с одновременным подавлением пауз, свойственных любому разговору. Полученный цифровой поток разбивается на пакеты протокола IP, при необходимости шифруется и передаётся по сети к заданным шлюзам. Маршрутизация пакетов осуществляется согласно алгоритмам работы сетей IP по наикратчайшему пути и с наименьшими задержками.

Адресация в сетях TCP/IP.

В вычислительных сетях используют как **индивидуальные линии** связи между компьютерами, так и **разделяемые** *(***shared),** когда одна линия связи попеременно используется несколькими компьютерами. В случае применения разделяемых линий связи возникают **электрические проблемы** обеспечения нужного качества сигналов при подключении к одному и тому же проводу нескольких приемников и передатчиков, и **логические проблемы** разделения во времени доступа к этим линиям (шина общая). Еще одной проблемой, которую нужно учитывать при объединении трех и более компьютеров, является **проблема их адресации**. К адресу узла сети и схеме его назначения можно предъявить несколько требований:

-адрес должен уникально идентифицировать компьютер в сети любого масштаба. Схема назначения адресов должна сводить к минимуму ручной труд администратора и вероятность дублирования адресов.

-адрес должен иметь иерархическую структуру, удобную для построения больших сетей. Эту проблему хорошо иллюстрируют международные почтовые адреса, которые позволяют почтовой службе, организующей доставку писем между странами, пользоваться сначала названием страны адресата, потом названием его города, улицы.

-адрес должен быть удобен для пользователей сети, а это значит, что он должен иметь символьное представление, например, www.cisco.com.

-адрес должен иметь по возможности компактное представление, чтобы не перегружать память коммуникационной аппаратуры - сетевых адаптеров, маршрутизаторов и т. п. Так как все перечисленные требования трудно совместить в рамках какой-либо одной схемы адресации, то на практике обычно используется сразу несколько схем, так что компьютер одновременно имеет несколько адресов-имен.

Различают три типа адресов:

- **на канальном уровне** используют адреса, называемые **физическими, локальными или MAC-адресами**. Это **шестибайтовые адреса** (**48 бит**) сетевых плат, присваиваемые изготовителем контроллеров (каждый изготовитель вместе с лицензией на изготовление получает уникальный диапазон адресов).

Два старших бита MAC-адреса используются для идентификации типа адреса: первый бит - одиночный (0) или групповой (1) адрес; второй бит - признак универсального (0) или локально администрируемого (1) адреса. Следующие 22 бита адреса содержат специальный код производителя (OUI - универсальный код организации - это централизованно выделяемая каждому производителю старшая часть MAC – адреса). Например, 00:E0:4C используется для сетевых устройств REALTEK SEMICONDUCTOR CORP, 00:00:01 - для XEROX CORPORATION. Младшая часть MAC-адреса формируется при производстве оборудования и уникальна для каждого экземпляра устройства. В сетях Ethernet передаваемые и принимаемые данные всегда содержат MAC-адрес источника (Source MAC) и MAC-адрес приемника (Destination MAC). MAC - адреса компактны, но неудобны для восприятия человеком. Кроме того при смене сетевой платы меняется и MAC- адрес. Одному и тому же производителю может принадлежать несколько кодов OUI.

- **на сетевом уровне** используют адреса, называемые **виртуальными или логическими**. Кадр, поступивший на сетевой уровень, инкапсулируется в пакет с заголовком, в котором указываются сетевые адреса отправителя и получателя. Эти адреса имеют иерархическую структуру, для них существует цифровое и буквенное выражение. В сетях TCP/IP (в интернет) эти выражения называют **IP-адресом и IP-именем** соответственно.

IP-адрес в четвертой версии протокола (IPv4) – уникальная совокупность чисел, адреса сети и адреса хоста (узла в сети с которым связаны компьютеры). Записывается в виде четырех частей (побайтно), разделенных точками. IP-адрес имеет длину 4 байта и обычно записывается в виде четырех чисел, представляющих значения каждого байта в десятичной форме и разделенных точками, например, **128.10.2.30** - традиционная десятичная форма представления адреса, а **10000000 00001010 00000010 00011110** - двоичная форма представления этого же адреса.

Для указания номера сети (192.168.100.1) может использоваться от одного до трех старших байтов, остальные – для номера узла. Классы адресов A,B,C,D, различают значения старших битов. Младшие биты используются для адресации подсетей и узлов в подсетях. Какая **часть IP-адреса относится к подсети** и **какая к узлу - определяется маской**, выделяющей соответствующие биты в IP-адресе. Маска - это число, которое используется в паре с IP-адресом. Двоичная запись маски содержит единицы в тех разрядах, которые должны в IP-адресе интерпретироваться как номер сети. Маску подсети часто записывают вместе с IP-адресом в формате «IP-

адрес/количество единичных бит в маске». Например, IP-адрес 12.34.56.78 с маской 255.255.224.0 (то есть состоящей из 19 единичных и 13 нулевых бит) можно записать как 12.34.56.78/19.

Адреса при включении новых хостов в сеть выдает провайдер. Он же обеспечивает включение IP- адреса и соответствующего ему IP-имени в сервер службы адресов DNS.

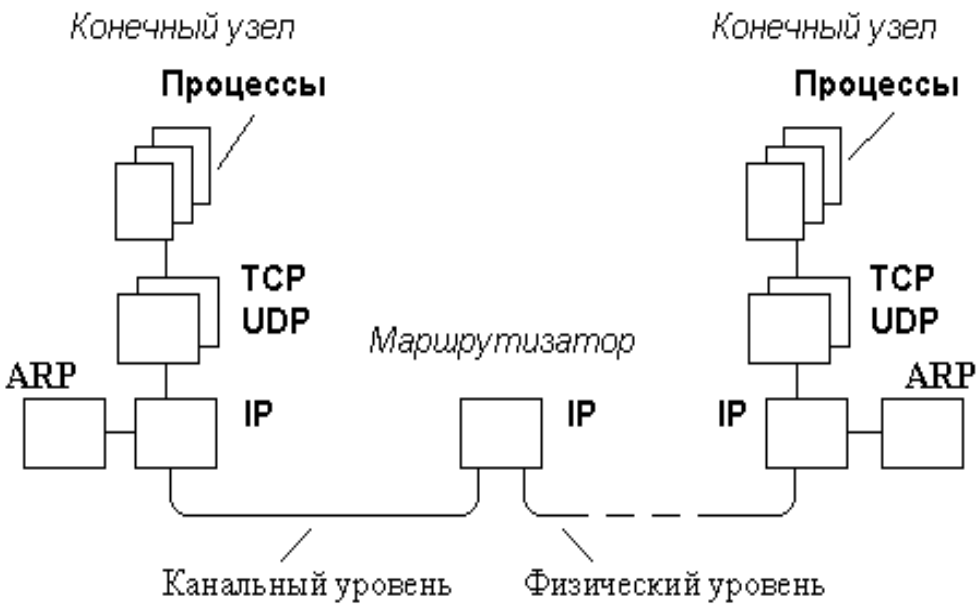
IP-имя (доменное имя) – удобное для человека название узла или сети. Оно отражает иерархическое построение сети Internet и поэтому состоит из нескольких частей, аналогично почтовым адресам. Корень иерархии означает страну либо отрасль знаний, например: ru –Россия, de –Германия, uk –Великобритания, edu –образование, com –коммерческие организации, org –некоммерческие, gov –правительсвенные, mil – военные, net – служба поддержки Internet. Корень занимает в IP-имени правую позицию, левее записываются локальные части адреса. Так, запись **norenkov@rk6.bmstu.ru** расшифровывается как пользователь Норенков в подразделении rk6, организации bmstu, в стране ru.

При маршрутизации **имя переводится в адрес с помощью серверов DNS**. Этот перевод обязателен, поскольку маршрутизация в сети осуществляется по IP-адресам. При обращении из одного узла в другой IP-имя переводится в IP-адрес обращением к местному серверу DNS. Если там сведений о сети назначения нет, то осуществляется переход к серверу более высокого уровня (ru) и далее вниз до получения IP-адреса места назначения. Узел отправителя сравнивает номер своей сети (подсети) с номером сети IP-адреса получателя в заголовке пакета. Если номера совпадают, то узел-отправитель с помощью его ARP-таблицы переводит IP-адрес в MAC-адрес, по которому и доставляется пакет. Если в ARP-таблице MAC-адреса не оказалось, то по сети широковещательно рассылается ARP-запрос, на который нужный узел откликается своим MAC-адресом. Если номера сетей не совпадают, пакет пересылается маршрутизатору, который ищет доступ к нужной сети через один из своих портов.

Работа программного обеспечения, реализующего взаимодействие процессов в сетях TCP/IP**,** кратко может быть охарактеризована следующим образом:

- при установлении соединения **прикладной процесс ОС** в узле - отправителе получает **номер порта** и передает **IP-имя** получателя на уровень TCP. С помощью обращения к службе DNS IP-имя переводится в **IP-адрес.**
- на сетевом уровне IP-адрес определяет номер сети и номер хоста (ведущего компьютера в подсети, где находится адресат). Для получения MAC-адреса получателя используется **ARP-таблица** хоста. Если в таблице есть строка с данным IP-адресом, то формируется заголовок пакета и дейтаграмма отправляется в сеть. Если искомой строки в таблице не оказалось, то формируется ARP-запрос, который широковещательно рассылается по подсети. Получатель откликается на запрос, посылая ARP-ответ с указанием своего MAC-адреса.

Если узла с запрошенным IP-адресом в данной сети нет, то пакет направляется по **MAC-адресу порта маршрутизатора**, который пересылает пакет с IP-адресом в следующую сеть и т.д., пока пакет не достигнет сети, в которой найдется MAC-адрес, соответствующий искомому IP-адресу. Аналогичные действия выполняются при установлении обратного соединения. Передача пакетов по установленным соединениям происходит более быстро, так как теперь не нужно обращаться к DNS и использовать ARP-запросы.



Получение: Сетевая карта сервера принимает биты (на физическом уровне) и преобразует их в кадры (канального уровня). Канальный уровень сначала смотрит на MAC-адрес (физический) получателя, он должен совпадать с MAC-адресом сетевой карты, иначе кадр будет уничтожен. Затем канальный уровень высчитывает сумму полученных данных и сравнивает полученное значение со значением трейлера (КС). Если они совпадают, кадр преобразуется в пакет, иначе уничтожается. На сетевом уровне происходит проверка логического адреса (IP-адреса), в случае успешной проверки пакет преобразуется в сегмент, попадая на транспортный уровень. На транспортном уровне проверяется информация из заголовка, что это за сегмент, какой протокол, для какого логического порта предназначается и на сервер посылается уведомление о прибытии сегмента. На верхних уровнях проверяется, доступна ли запрашиваемая веб-страничка на сервере - это **декапсуляция** (запроса).

Отправление: Найденная страница на сервере (текст, изображения, музыка) преобразуется в цифровой код, делится на части (сегменты) и поступает транспортный уровень с портом назначения, с которого вы посылали запрос. Сегмент преобразуется в пакет, в заголовке которого содержится IP-адрес вашего компьютера и переходит на канальный уровень, преобразуется в кадры, добавляется заголовок и трейлер. В заголовок помещается MAC-адрес назначения, а в трейлер (КС) проверочный код на целостность данных. Сетевая карта посылает кадры по кабелю по направлению к Вашему компьютеру – это **инкапсуляция** (ответа).

http://www.deti.ru/skazki/kolobok.txt

протокол доменное имя путь к файлу

URL – универсальный указатель на ресурс в Интернете. Как каждый компьютер в Интернете имеет уникальный адрес, то любой файл на компьютере может быть точно указан через структуру папок и имя файла. Для каждого файла можно записать точный универсальный **указатель ресурса**– адрес **URL** (Uniform Resourse Locator).

Протоколы ARP, IGP, EGP, RTP, UDP в стеке TCP/IP. ***Стек***... в первую очередь ассоциируется со способом организации памяти. Что же такое стек TCP/IP? Это все протоколы семейства TCP/IP, действующие на разных иерархических уровнях. Это также некоторый набор программ, библиотек, модулей, интегрированных в ОС и отвечающих за создание, отправку, прием и обработку информации по стандартам TCP/IP.

В состав протокола IP входит ряд частных протоколов. Так, протоколы **ARP, IGP, EGP, RIP** относятся к **маршрутизации** на разных иерархических уровнях в архитектуре сети.

На одном уровне с IP находится **протокол управления сетью - ICMP** (Internet Control Message Protocol), котоый реализуется путем предоставления приоритета внутренних потоков перед внешними, ограничением числа пакетов в сети (пакет принимается, если у узла есть соответствующее разрешение), посылкой предупредительных пакетов-заглушек в адрес источника от которого идут пакеты в перегруженную линию связи. ICMP-пакеты вкладываются в IP-дейтаграммы.

В TCP/IP входит **протокол UDP** (User Datagram Protocol) — транспортный протокол без установления соединения, он значительно проще TCP и используется чаще всего для сообщений, умещающихся **в один пакет**. После оформления UDP -пакета, он передается с помощью средств IP к адресату, который по заголовку IP-пакета определяет тип протокола и передает пакет не агенту TCP, а агенту UDP. В UDP служебная часть дейтаграммы короче, чем в TCP (8 байт вместо 20), не требуется предварительного установления соединения или подтверждения правильности передачи, как это делается в TCP, что и обеспечивает большую скорость за счет снижения надежности доставки.

Протокол RTP — транспортный протокол реального времени, используемый вместо протокола TCP, например, для передачи видео, обеспечивая синхронность передачи компонентов видео (задержка < 6мс).

В сети Internet для **файлового** обмена используется прикладной **протокол FTP** (FTPS = FTP + SSL(TLS)). Его особенность в том, что он использует двойное подключение. Одно используется для передачи команд серверу и происходит по умолчанию через TCP-порт 21 и существует все время, пока клиент общается с сервером. Через второе происходит непосредственная передача данных. Оно открывается каждый раз, когда осуществляется передача файла между клиентом и сервером. Если одновременно передаётся несколько файлов, для каждого из них открывается свой канал передачи. Передача данных может осуществляться в поточном, блочном режимах, режиме сжатия. FTP client – это программа (браузер), позволяющая подключиться к удаленному серверу по FTP и выполнить на нем необходимые действия с элементами файловой системы.

PPP (Point-to-Point Protocol) — двухточечный протокол канального уровня, разработан специально для стека TCP/IP . Используется для установления прямой связи между двумя узлами сложной сети. Он может обеспечить полнодуплексное одновременное двунаправленное функционирование, аутентификацию соединения, шифрование и сжатие данных. Используется на всех типах физических сетей: нуль-модемный кабель (соединяет порты двух компьютеров), телефонная линия, сотовая связь и т. д. Его функции: присвоение и управление адресами IP, асинхронное (старт-стопное) и синхронное (бит-ориентированное) формирование пакета данных, конфигурация и проверка качества канала связи, обнаружение ошибок, согласование способа сжатия информации и т.д. PPP представляет собой целое семейство протоколов: протокол управления линией связи (LCP), протокол управления сетью (NCP), протоколы аутентификации (PAP, CHAP), многоканальный протокол MLPPP для параллельной передачи информации.

GPRS - протокол пакетной передачи данных в технологии мобильной связи GSM. Мобильные системы GSM используют принцип временного кодирования сигналов с множественным доступом (TDMA). Аналоговые сигналы перед подачей их на модулятор должны быть оцифрованы, и все сигналы обработаны процессором, чтобы занять свое определенное для них в пакете место. GPRS по принципу работы аналогичен TCP/IP: данные разбиваются на пакеты и отправляются получателю (необязательно одним и тем же маршрутом), где происходит их сборка. Поэтому интеграция GPRS с интернетом незаметна конечному пользователю. GPRS поддерживает протоколы IP и PPP и позволяя пользователю мобильного телефона говорить, работать в Интернете и пересылать сообщения электронной почты. Мобильный телефон выступает как клиент внешней сети и ему присваивается динамический IP-адрес. Скоростной предел передачи GPRS до 171,2 Кбит/с на канал. Применение:

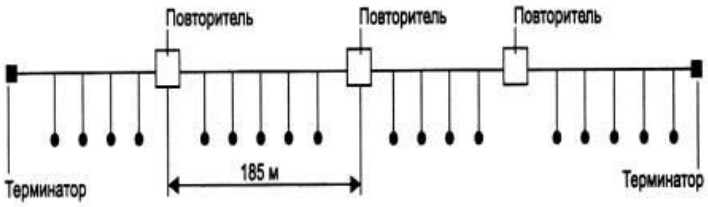
- Мобильный доступ в Интернет, к корпоративным сетям, удалённым базам данных, почтовым и информационным серверам.

- Телеметрия. Устройство может оставаться в подключённом состоянии, не занимая при этом отдельный канал, что востребовано службами охраны (сигнализация), банками и платёжными системами (банкоматы), в промышленности (датчики и счётчики различного рода, например по ходу нефте- и газопроводов).

Базовое оборудование ЛВС

В подсеть каждого из отделов должны попадать только те кадры, которые адресованы узлам этой сети. При такой организации работы сети ее производительность существенно повыситься, так как компьютеры одного отдела не будут простаивать в то время, когда обмениваются данными компьютеры других отделов. Распространение трафика, предназначенного для компьютеров некоторого сегмента сети, только в пределах этого сегмента, называется **локализацией трафика.** Для логической структуризации сети используются **мосты, коммутаторы, маршрутизаторы и шлюзы**, которые составляют базовое оборудование ЛВС.

Сетевой контроллер сервера и **сетевые платы** компьютеров относятся к **средствам канального уровня** и реализуют принятый метод доступа. В случае **МДКН/ОК** в блоке вырабатывается сигнал затора, величина задержки в передаче при наличии конфликта или при занятом канале, происходит формирование данных в кадры, кодированию (декодированию) сигналов, распознавание MAC-адреса в принимаемых из сети сообщений, буферизация, преобразование параллельного кода в последовательный, избыточное кодирование данных.



Простейшее из коммуникационных устройств - **повторитель (repeater)** - используется для физического соединения различных сегментов кабеля локальной сети с целью увеличения общей длины сети. Повторитель восстанавливает амплитуды сигналов и качество фронтов, передавая их побитно. Многопортовый повторитель называется **концентратором.**

Концентраторы (хабы) имеют ряд портов для подключения компьютеров и порт для внешнего управления с целью отключение некорректно работающих узлов, передачи данных о состоянии соответствующего участка сети менеджеру. протокола управления.

Мост (bridge) — блок взаимодействия разных подсетей, который разделяет трафик. Если отправитель и получатель некоторого сообщения находятся в одной и той же подсети, то это сообщение не пропускается в другую подсеть. Мосты имеют по два или более портов. Каждый порт может оказаться входным или выходным. Управление передачей пакетов выполняется с помощью **маршрутной таблицы** моста, в которой строки содержат соответствующие друг другу значения **MAC-адреса** узла, а столбцы - номера порта моста, на который следует отправить принятый кадр.

Мост передает кадр не побитно, а с буферизацией кадра. Если компьютеры с адресами источника и адресом назначения находятся в разных сегментах, то мост выполняет операцию продвижения кадра. Если компьютеры принадлежат одному сегменту, то кадр просто удаляется из буфера. Такая операция называется **фильтрацией.** Администратор может удалять пакеты с определенными адресами или запретить доступ к некоторым ресурсам.

Коммутатор (switch, switching hub) по принципу обработки кадров ничем не отличается от моста. Основное его отличие от моста состоит в том, что он является **коммуникационным мультипроцессором**, так как каждый его порт оснащен специализированным процессором, который обрабатывает кадры по алгоритму моста независимо от процессоров других портов. Имеется центральный

процессор, координирующий работу остальных устройств. За счет этого общая производительность коммутатора намного выше производительности традиционного моста, имеющего один процессорный блок. Коммутаторы - это мосты нового поколения, которые обрабатывают кадры в параллельном режиме.

Протокол случайного доступа МДКН/ОК делает сеть малоэффективной при большом количестве пользователей, поскольку он приводит к росту задержек в сети (столкнувшиеся кадры уничтожаются, и их приходится пересылать повторно), время ожидания растет. Часть этих проблем решается разделением сложной сети на подсети с применением **коммутаторов**. Кадры передаются только в подсети с нужными MAC-адресами. Поэтому не происходит коллизий и нет необходимости в повторной трансляции утерянных по этой причине кадров, а пользовательские устройства не тратят времени на ожидание освобождения среды передачи.

Коммутаторы и мосты, работают с MAC-адресами и локализуют значительную часть трафика внутри соединяемых подсетей, группируя сегменты для различных подсетей (Ethernet, Token Ring, FDDI). Процессоры внутри коммутатора соединяются посредством высокоскоростной **общей шины, многовходовой памяти** или **коммутирующей матрицы**, в которой одновременно может быть создано много соединений. Основными характеристиками коммутаторов являются пропускная способность, измеряемая количеством информации, переданной через порты коммутатора в единицу времени, скорость фильтрации и скорость продвижения пакетов через коммутатор и задержка кадра в коммутаторе. В небольших сетях возможна коммутация "на лету", когда передача пакета начинается сразу после расшифровки его заголовка, в магистральных узлах коммутация происходит после полного получением пакета (промежуточная буферизация). Сети с мостами или с коммутаторами подвержены так называемому широковещательному шторму, когда пакеты направляются во все подсети.

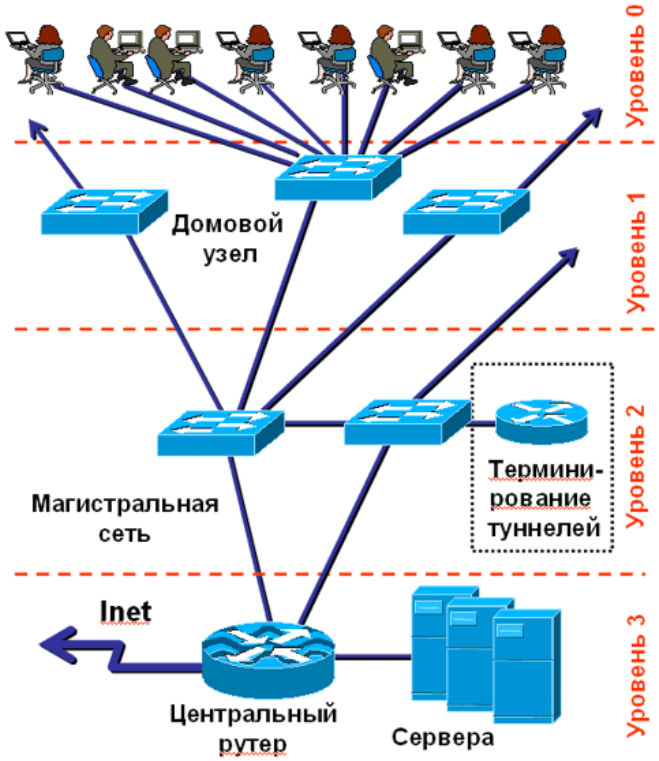
Маршрутизаторы более надежно и более эффективно, чем мосты, изолируют трафик отдельных частей сети (сегментов) друг от друга посредством явной адресации, используя номера сети, так что все компьютеры, у которых значение этого поля одинаково, принадлежат к одному сегменту, называемому подсетью. Маршрутизаторы связаны между собой и обрабатывает с помощью алгоритмов маршрутизации информацию о текущем состоянии сети, фиксируя в памяти ее состояние в виде **таблицы маршрутизации**. Маршрутизатор также имеет несколько портов, центральный процессор, контроллеры и буферные накопители портов. Маршрутизатор определяет на основании таблицы маршрутизации выходной порт, на который нужно направить дейтаграмму, на что тратится некоторое время и увеличиваются задержки в передаче данных. Цель **маршрутизации** — доставка пакетов по назначению с максимальной эффективностью, выраженной взвешенной суммой времен доставки сообщений по маршруту. Маршрутизация сводится к определению направлений движения пакетов от порта в порт внутри устройства, зависит от текущей топологии сети, длин очередей в узлах коммутации, интенсивности входных потоков и т.п. Алгоритмы **адаптивной маршрутизации** выбирают нужное направление передачи кадров на основе информации о загрузке устройств смежных сетей. В **фиксированных** алгоритмах информация о маршрутах составляется и заносится в память маршрутизатора администратором сети. В **случайных алгоритмах** выбор выходного порта случаен. В алгоритмах **лавинной маршрутизации** пакет передается во всех возможных направлениях, что ускоряет доставку данного пакета, но лишь в условиях малой нагрузки.

Шлюз (gateway) — блок взаимодействия, служащий для соединения информационных сетей различной архитектуры и с неодинаковыми протоколами. Часто под шлюзом понимают сервер, имеющий внешний канал передачи данных. В шлюзах предусматривается согласование протоколов всех семи уровней ЭМВОС.

К блокам взаимодействия относят также модемы, конверторы, преобразующие потоки в пакеты промежуточных сетей, многопротокольные переключатели (например, из X.25 в Frame Relay и обратно), мультиплексоры и демультиплексоры — устройства для преобразования сообщений в кадры TDM и обратно.

Каковы критерии оценки сетевого оборудования? Это производительность и стандартность, латентность коммутации, совместимость с гетерогенными сетями, возможность работы с разными протоколами (в случае Ethernet таким протоколом является SDH), перспективная поддержка стандартов будущего (таких как 100Gig Ethernet), насыщенность портами, маршрутная емкость, отказоустойчивость, время восстановления канала передачи, обеспечение параметров качества обслуживания, стоимость внедрения, возможность и простота удаленного обслуживания.

Абонентские линии «последней мили» (непосредственно к потребителю).



Для подключения клиентов к узлам магистральной сети применяют **модемы** и **цифровые абонентские линии** (xDSL) на основе обычного телефонного кабеля, пакетные каналы провайдера, радиоканалы **WiMAX и Wi-Fi** и технологии **LTE.**

- **Коммутируемый** доступ является - один из первых общедоступных способов удаленного подключения к сетям передачи данных. Пользователи используют единый телефонный номер для доступа в свои корпоративные сети (или доступ через GPRS в Internet), а определение их принадлежности к той или иной компании осуществляется на основе уникального имени и пароля.

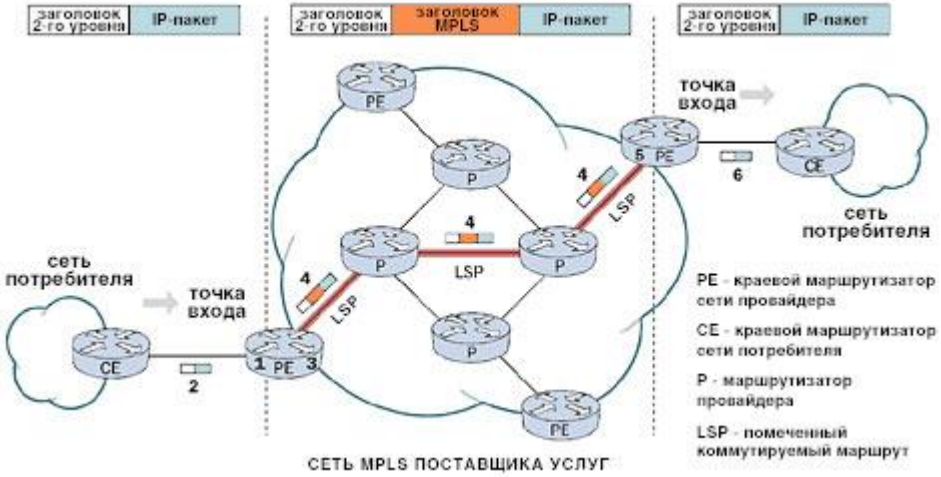
- Для связи офисов всегда использовались **выделенные линии** связи. Скорости, обеспечиваемые на телефонных каналах, колебались от 9,6 кбит/с (модемы) до 8 Мбит/с при появлении xDSL-технологий. Все это - временные решения, на смену которым пришло оптическое волокно со скоростью 10/100/1000 Мбит/с.

Организация связи ЛВС через Интернет. Клиентский компьютер устанавливает с провайдером стандартное соединение типа «точка - точка» (по протоколу PPP), после чего подключается через Интернет к центральному узлу. При этом формируется **канал VPN**, представляющий собой «туннель», по которому можно производить обмен данными между двумя конечными узлами. В действительности данные передаются через Интернет, как и любые другие пакеты, но с использованием дополнительных меток. Каналы VPN могут быть защищены алгоритмами шифрования, заложенными в стандарты протокола безопасности **Internet Protocol Security (IPSec**).

Выбирая **сервис IP VPN (webvpn.bmstu.ru)**, потребитель получает комплекс услуг – доступ в Интернет, видеоконфенцсвязь, передачу данных и доступ к базам внутри корпоративной информационной системы, экономичную внутреннюю телефонию. Клиент арендует подходящий порт и в нужный момент заказывает нужную услугу, оплачивая реальный трафик. Заботу об организации и поддержке всех сервисов IP VPN берет на себя провайдер. **VPN канал** обычно представляется в виде подключения к порту Ethernet (на скорости от 10 до 100 Мбит/с).

Канал в пакетной сети оператора (Frame Relay, ATM). Каждый офис подключается одним (или несколькими) портами к сети передачи данных заказчика. После этого в пределах сети заказчика организуются виртуальные каналы, которые связывают его офисы. Виртуальные каналы настраиваются программно и для каждого устанавливается собственная гарантированная скорость передачи

данных – до 2 Мбит/с. Часто этих скоростей уже недостаточно для современных приложений. ATM – от 2 до 155 Мбит/с, однако такие подключения распространены относительно мало, а стоимость порта и канала ATM превышает стоимости IP/MPLS - каналов аналогичной скорости. По уровню безопасности виртуальные FR/ATM каналы уступают выделенным линиям. Трафик одного клиента, передаваемый по сети Frame Relay, отделен от трафика другого клиента и не может попасть в его сеть. Однако данное разделение – программное и может быть нарушено незаметно для пользователя.



IP/ MPLS (Multiprotocol Label Switching = IP + VPN)
- сеть, организованная на базе технологии многопротокольной коммутации меток (способ распознавания пакетов с одинаковым маршрутом путем присваивания им меток, с помощью которых эти пакеты коммутируются в сетевых узлах) построена по иерархической двухуровневой архитектуре, включающей **опорный слой (ядро)** MPLS-коммутации IP-трафика и **пограничный слой**, несущий основную нагрузку по обслуживанию абонентов. Во время установления соединения между абонентами **формируется программно обособленный виртуальный канал связи**, по которому передаются данные с номером канала в заголовке (как номер троллейбуса). Все промежуточные устройства сети коммутируют сообщение по этому номеру с высокой скоростью.

Технология MPLS строится на технологии IP, объединяя интеллект процесса маршрутизации современных IP-сетей (пограничный слой), с **высокой производительностью процесса коммутации каналов** (ядро).

MPLS функционирует как поверх существующей сети SDH(SONET), инфраструктуры (10/100/1000/10G Ethernet) и сетей (IP, ATM, Ethernet). При разработке MPLS пришло понимание того, что на уровне ядра современной сети нет необходимости в ячейках ATM маленького фиксированного размера (53 байта), так как современные оптические сети обладают такой большой скоростью передачи данных (на 2011 г. пропускная способность магистралей большинства провайдеров составляет от 40 Гбит/с до 100 Гбит/с), что даже Ethernet- пакет данных максимальной длины в 1500 байт испытывает незначительную задержку в очередях буферов устройств коммутации.

Из современных технологий **беспроводной** передачи информации наибольшее распространение получили **Wi-Fi** и **WiMAX** и технологии **LTE**. Мобильные системы **GSM, 3G, LTE** полностью основаны на IP-протоколе и поддерживают передачу данных только в цифровой форме. По сравнению с WiMAX, **LTE на современном этапе** не требует освоения новых частотных диапазонов, а идет по пути ускорения обмена информацией за счет использования сложных сигналов и цифровых методов фильтрации, обеспечивая межсетевое взаимодействие 2G/3G /4G (GSM, UMTS/HSPA, TD-SCDMA, CDMA2000) со скоростью передачи данных до 100 Мбит/с.

Технология **WiMAX** предназначена для организации широкополосной связи вне помещений и для организации крупномасштабных сетей. Это технология быстрого беспроводного интернета, которая обеспечивает высокую скорость доступа в сеть — до 75 Мбит/с в теории (10 Мбит/с на практике), в любое время, в любом месте зоны покрытия и поддерживает соединение даже в движении, на

скорости до 120 км/ч. WiMAX разрабатывался как **городская вычислительная сеть** (MAN). У WiMAX лучше качество связи, чем у WiFi. Когда несколько пользователей подключены к точке доступа Wi-Fi, они буквально «дерутся» за доступ к каналу связи. Технология WiMAX обеспечивает каждому пользователю постоянный доступ. Когда базовая станция WiMAX приближается к максимуму своего потенциала, она автоматически перенаправляет «избыточных» пользователей на другую базовую станцию.

Принцип действия сети на базе WiMAX очень похож на принцип работы сотовой связи. Существуют абонентские станции, то есть базовые станции, пользовательское и прочее коммуникационное оборудование оператора, связанное с Интернетом. Базовые станции установлены на расстоянии нескольких (а то и десятков) километров друг от друга. Одна «перекидывает» сигнал другой в условиях прямой видимости **в частотных диапазонах 2.4- 3.5 -5.8 ГГц** (скорость передачи данных может быть очень высокой). По крайней мере одна базовая станция должна соединяться с сетью провайдера при помощи проводов. На практике же к проводной сети подсоединяют довольно много передатчиков, что позволяет повысить скорость прохождения данных и надежность всей системы. Максимальная скорость - до 1 Гбит/сек. Структура сетей WiMax схожа с традиционными GSM сетями (базовые станции действуют на расстояниях до десятков километров), для их установки не обязательно строить вышки — допускается установка на крышах домов при соблюдении условия прямой видимости между станциями.

Однако, внедрение **WiMAX** требует создание **новой сети** приемопередатчиков в новом, более высокочастотном диапазоне, при наличии сотовой структуры GSM в диапазоне 890-1800 МГц. (**Yota** - провайдер беспроводного интернета по технологии Mobile WiMAX в Москве).

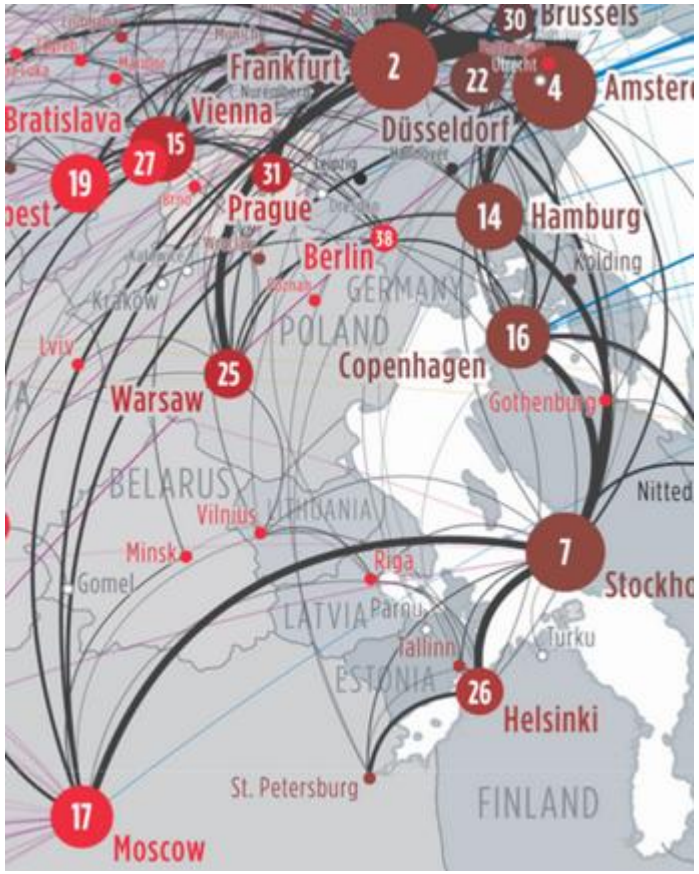
Wi-Fi это система более короткого действия, обычно покрывающая десятки метров, которая использует нелицензированные диапазоны частот для обеспечения доступа к сети. Обычно Wi-Fi используется пользователями для доступа к их собственной локальной сети, которая может быть и не подключена к Интернету. Если WiMAX и LTE можно сравнить с мобильной связью, то **Wi-Fi** скорее похож на **стационарный беспроводной телефон**. Из-за дешевизны и простоты установки, Wi-Fi часто используется для предоставления клиентам быстрого доступа в Интернет различными организациями. Например, в некоторых кафе, отелях, вокзалах и аэропортах можно обнаружить бесплатную точку доступа Wi-Fi.

WiMAX и Wi-Fi имеют совершенно разный механизм **Quality of Service** (QoS). WiMAX использует механизм, основанный на установлении соединения между базовой станцией и устройством пользователя. Каждое соединение основано на специальном алгоритме планирования, который может гарантировать приоритет для каждого соединения. Wi-Fi, в свою очередь, использует механизм QoS подобный тому, что используется в Ethernet, при котором пакеты получают различный приоритет (как получится).

Bluetooth

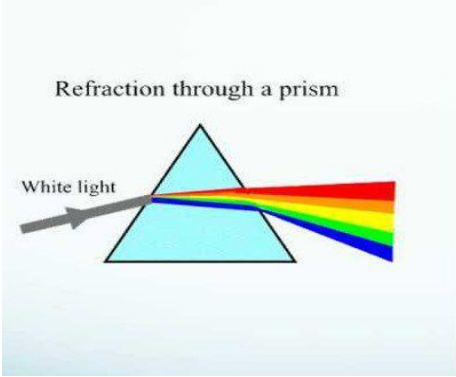
Технология Bluetooth реализована в диапазоне 2,4—2,48 ГГц с использованием метода частотных скачков FHSS (Frequency Hopping Spread Spectrum) по строго заданному алгоритму для каждого приемника. В соответствии с методом FHSS в Bluetooth несущая частота сигнала скачкообразно меняется 1600 раз в секунду (всего выделяется 79 рабочих частот). Рабочая частота каждые 625 мкс (один временной слот) синхронно перестраивается с одной несущей на другую. Последовательность переключения между частотами для каждого соединения является псевдослучайной и известна только передатчику и приёмнику. При этом возможна одновременная передача данных нескольким приемникам в одном и том же диапазоне.

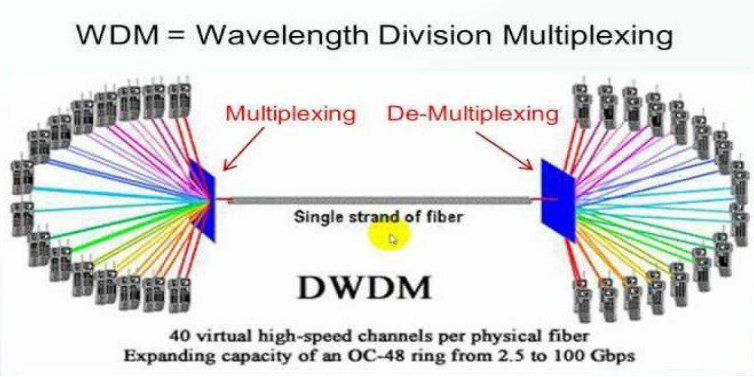
Магистральные линии связи. На физическом уровне интернет представляет **сеть хабов** (точек обмена трафиком), связанных **магистральными каналами**, в том числе подводными. В точках обмена трафиком концентрируется не только трафик, но и сетевая инфраструктура (дата-центры, хостинг и т.д). Крупнейшие точки обмена находятся во Франкфурте (5178 Гбит/с), Амстердаме (4270 Гбит/с), Лондоне, Париже, Нью-Йорке. Москва занимает 5 место в Европе. Трансатлантическая информационная магистраль: в 2003-2014годы не проложено ни одного нового кабеля, зато пропускная способность действующих каналов увеличилась в 2,4 раза исключительно за счёт уплотнения каналов и апгрейда оборудования. Серверы размещают внутри национальных границ той страны, где находится основная аудитория. Сейчас не только Россия, но и другие страны рассматривают законы, обязывающие хранить конфиденциальную информацию (в том числе финансового и медицинского характера) только внутри страны.



Оптическая транспортная платформа, состоящая из оптического волокна, систем разделения полос передачи (DWDM) и устройств передачи (лазеров и светодиодов), является основой для различных технологий передачи данных - **PDH/SDH/SONET, ATM, PON, Ethernet и семейства протоколов IP (TCP/IP).**

Ключевой технологией для интегрированных телекоммуникационных сетей и высокоскоростных сетей оптической передачи данных является **технология спектрального уплотнения (Wavelength Division Multiplexing, WDM**). В рекомендациях Международного телекоммуникационного союза G.692 в области 1550 нм предусматривается **40 каналов DWDM** (плотное спектральное уплотнение), ширина полосы каждого из них составляет 100 ГГц (приблизительно 0,8 нм). Каждая длина волны несет нагрузку в 2,5 либо 10 Гбит/с. Так как оптическое волокно имеет свойство поглощать оптические сигналы, без регенерации или усиления они передаются только на ограниченное расстояние (обычно от 5 до 300 км). При использовании волоконно-оптических каналов связи выделенная линия перестает быть узким местом корпоративной сети передачи данных.





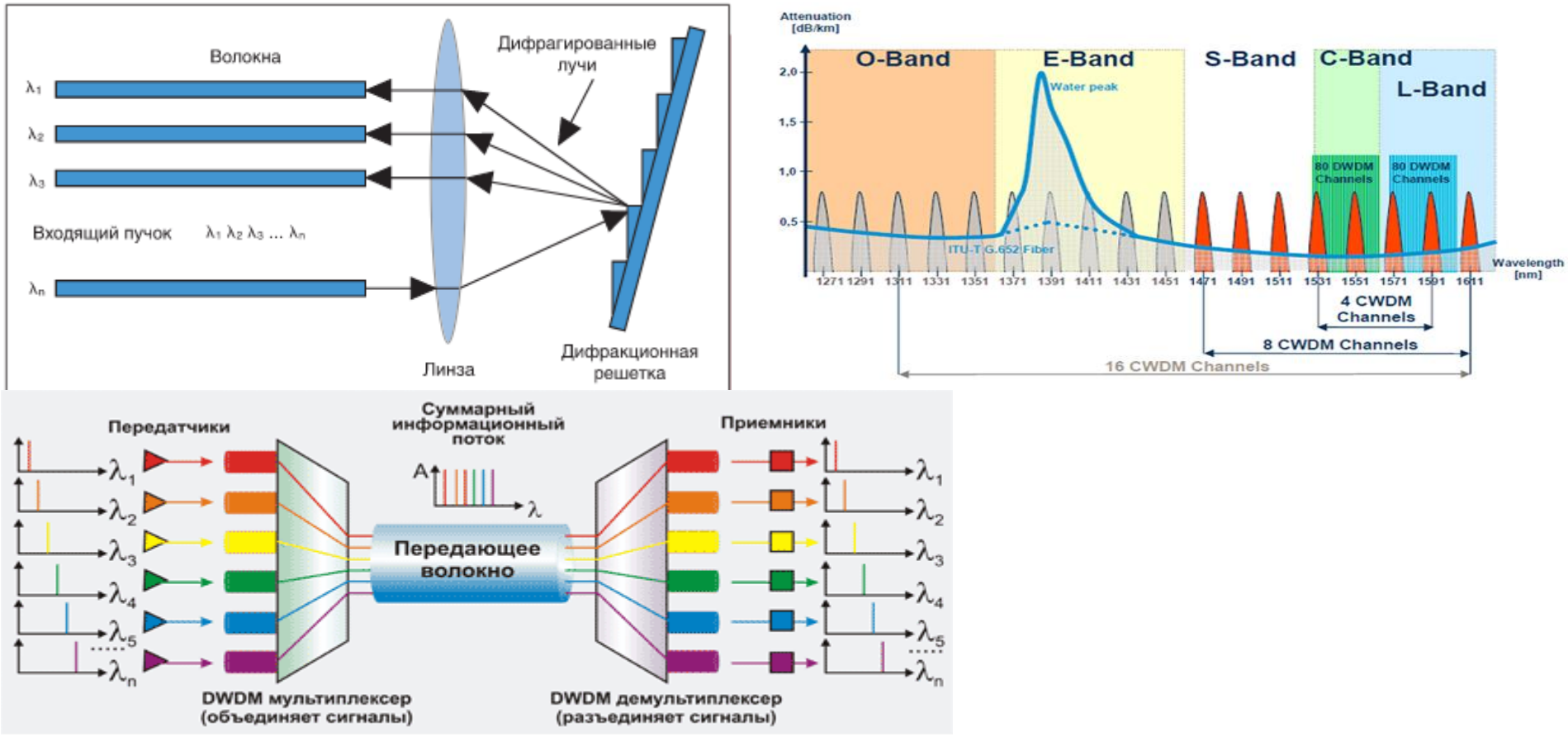
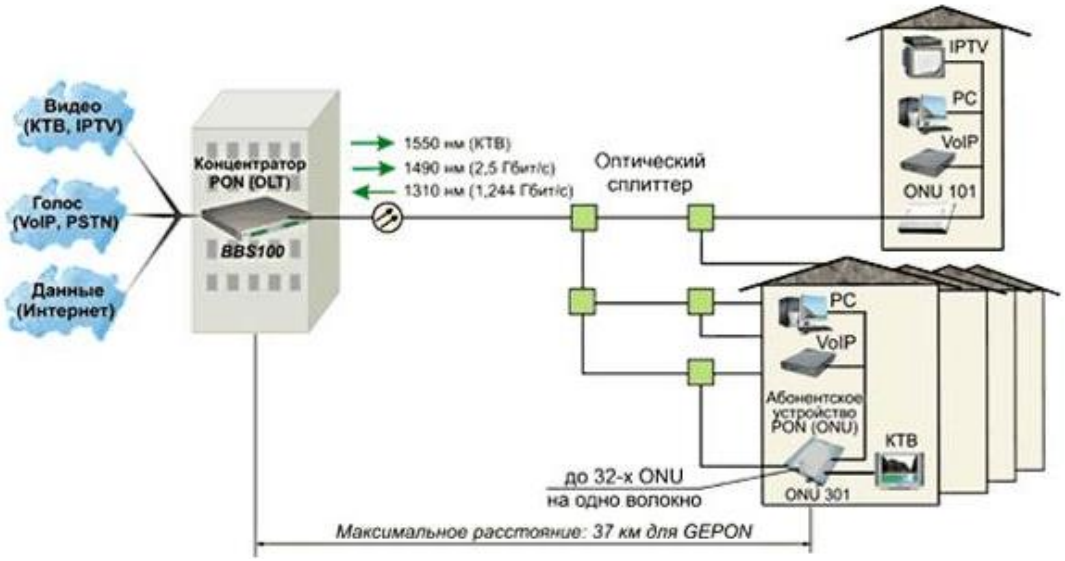


Рис.6

В технологии **PON** (A,B,E,G,GE – от 155 Мбит/с до 10 Гбит/с) при построении оптической сети используются два метода мультиплексирования: **WDM** мультиплексирование/демультиплексирование и **TDMA** (метод множественного доступа с разделением по времени).

WDM - это волновое спектральное уплотнение потока инфракрасных волн в одном волокне.

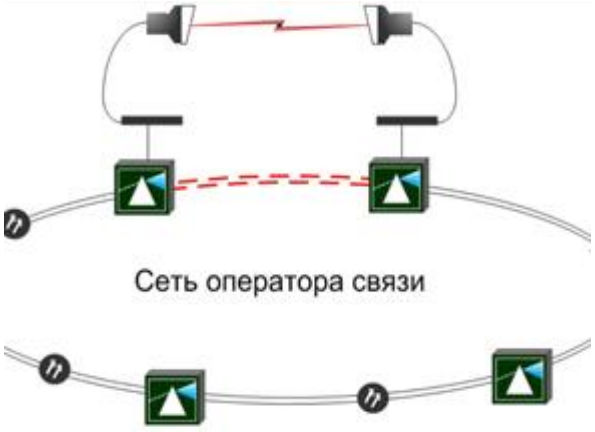
TDMA (метод множественного (коллективного) доступа с временным разделением) использует специальный механизм арбитража, исключающего случаи столкновения информационных потоков в общем канале передачи данных. Стандартно сети PON работают в интерфейсе с форматами Ethernet, обеспечивая на абонентском тракте "последняя миля" эффективное распределение пользовательских услуг по принципу "оптика в дом" со скоростью 10 Мбит/с.

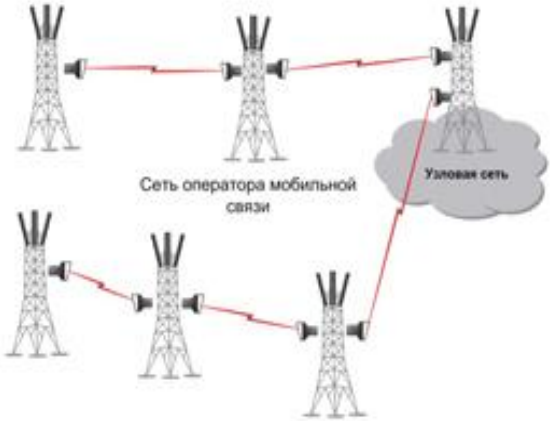


Архитектура PON достаточно тривиальная. Имеется один активный центральный узел OLT (optical line terminal) с лазерным приемопередающим модулем (трансивером) и множество активных удаленных абонентских узлов ONT (optical network terminal) со своими светодиодными приемопередающими модулями. Между устройствами расположена **полностью пассивная оптическая среда**, не требующая электроэнергии и технического обслуживания и состоящая из оптических кабелей и оптических разветвителей. Внешним источником информации для OLT является Интернет-провайдер и кабельное телевидение. Для деления мощности сигнала используется сплиттер 1:32 или 1:64, который разделяет всю мощность входящего сигнала поровну между абонентами.

Альтернативные сети.

Цифровые радиорелейные линии связи. Радиорелейная связь первоначально применялась для организации многоканальных линий телефонной связи. Первая такая линия с 5 телефонными каналами (аналоговыми) появилась в США в 1935 году. Она соединяла города Нью-Йорк и Филадельфию и имела протяженность 200 км. Суммарная протяженность цифровых РРЛ в СССР превысила к середине 70-х годов 100 тыс. км.





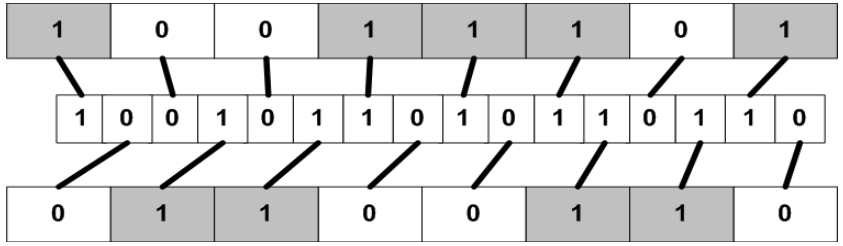
В зависимости от назначения связь производится с помощью радиоволн длиной от дециметров до миллиметров. Частотные диапазоны от 2 ГГц до 38 ГГц относятся к «классическим» радиорелейным частотным диапазонам. Наземные радиорелейные линии связи строят с пролётами между ретрансляторами 30–50 км, возможно увеличение этого расстояния до 100–120 км за счёт увеличения высоты подвеса антенн и усложнения оборудования. В городах расстояние между станциями значительно

меньше – 4–7 км. Межстанционные пролёты тропосферных линий связи (использующих эффект отражения от тропосферных неоднородностей) могут превышать 400 км.

Основное назначение цифровых радиорелейных линий связи - построение технологических линий связи, соединение скоростных сетей LAN, резервирование оптоволоконных линий связи. Для обеспечения высокой пропускной способности и отказоустойчивой передачи данных организуется несколько радиостволов. В случаях невозможности прокладки оптоволоконных линий, операторы связи используют радиорелейные станции для объединения своих региональных сетей, создавая беспроводные магистральные линии связи большой протяженности с несколькими транзитными пунктами.

Абонент может арендовать до 30 каналов DS-0, до 120 каналов DS-1 и т.д., пригодных как для передачи голоса, так и цифры (со скоростью 64 кбит/с в каждом канале). **Ethernet–over-PDH** – набор технологий и стандартов, которые позволяют передавать потоки (фреймы) цифровой информации Ethernet через существующие сети PDH.

Цифровая выделенная линия - несинхронный **PDH** (плезиохронная, почти синхронная двоичная иерархия) канал или синхронный **SDH** (синхронная двоичная иерархия, американское название – SONET) в ТДМ-сети оператора связи. Базовой скоростью или нулевым уровнем в обоих типах иерархии (PDH и SDH) является скорость 64 кбит/с, с которой передается один стандартный телефонных канал.



Эта скорость есть результат ИКМ в звуковом канале с отсчетами 4 кГц х 2 = 8 кГц (по теореме Котельникова) и представления полученных отсчетов в байтах со скоростью 8 х 8 = 64 кбит/с в канале DS-0 (Digital Signal-0) и 2048 кБит/с на канал аппаратуры E1, состоящей из 32 цифровых каналов DS-0. Эти каналы были разработаны для передачи голосовых сигналов по технологии TDM (мультиплексная передача с временным разделением и коммутацией каналов) - PDH в Европе и США.

В канале E1 все 32 канала DS-0 передают в мультиплексор по одному байту, образуя 32 байтный (256-битный) суперкадр с добавлением контрольного кода и синхронизирующей комбинации.

Длительность кадра не изменяется, поэтому каждый бит ужимается по времени также в 32 раза и скорость передачи возрастает по сравнению с первоначальной в 32 раза. Каждый из 32 каналов имеет пропускную способность 64 кбит/с, таким образом, общая пропускная способность E1 — 2048 кбит/с. Параллельные 32 потока байт превращаются в последовательный поток. Объединение потоков выполняется по **принципу чередования,** что называется **мультиплексированием**.

В кадре PDH положение данных канала жестко фиксировано (первый байт – первый канал, второй байт – второй канал, и т.д.), что приводит к нерациональному использованию кадра. Так если в кадре из 30 каналов данные передаются только по одному каналу, то мультиплексор все равно заполняет весь кадр, 1 байт данных канала, а остальные 29 байт кадра просто заполняются нулями. Чтобы выделить из кадра данные только одного канала, придется полностью «разобрать» (демультиплексировать) весь кадр. Недостатками плезиохронной цифровой иерархии являются невозможность прямого доступа к каналам, без процедур демультиплексирования/ мультиплексирования всего линейного сигнала, и практическое отсутствие средств сетевого мониторинга и управления.

Следующие уровни в иерархии E1/E4 представлены каналами E2(8448 кбит/с), E3(34368 кбит/с), E4(139364 кбит/с) (DS-2, DS-3 и DS-4), каждый канал последующего уровня объединяет 4 канала предыдущего уровня, разделенных несколькими служебными битами. Средой передачи таких сложных сигналов являются радиорелейные линии на частоте от 5 ГГЦ или ВОЛС. Радиорелейные линии используют воздушную среду и антенны в пределах прямой видимости.

На практике используется **синхронная двоичная иерархия** - **SDH**. Помимо значительно более высокой скорости передачи данных, технология SDH позволяет извлекать (добавлять) отдельные пользовательские данные канала из/в кадра SDH, не производя его полное демультиплексирование («разборку»). Данный способ объединения ЛВС удобен пользователям, поскольку практически не зависит от расстояния между офисами, отличается крайне малыми задержками (обычно в пределах сотни микросекунд, т.е. на 2-3 порядка меньше, чем в пакетных сетях передачи данных) и выбором пропускной способности.

Сеть SDH может быть использована для передачи услуг PDH, а также сигналов других иерархий, таких как ATM, Ethernet и FDDI. В октябре 2000 года ITU - T принял Рекомендацию G .707/ Y .1322 по использованию сигнала 256-го уровня иерархии, т. е. сигнала STM - 256 со скоростью передачи 39813,12 Мбит/с (40 Гбит/с).

В Москве имеется несколько сетей с **каналами SDH**, например, сети компании МТУ-Информ. Фрейм STM-1 рассчитан на передачу данных со скоростью 155,52 Мбит/с., по каждому из них может передаваться 63, 252 или 1008 потоков E1 соответственно. Имеются кольца STM-1, STM-4, STM-16, обладающие высокой надежностью передачи данных, поскольку для каждого потока данных образуется два канала — основной и дублирующий, по которым одна и та же информация передается параллельно. Подключение к сети SDH происходит через сети Frame Relay или ATM на расстояниях до 3 км. Однако, стоимость синхронного порта FR или ATM 2 Мбит/с превосходит стоимость 100-мегабитного порта Ethernet.

Достоинства SDH/SONET состоят в предоставлении гарантированной пропускной способности, функций мультиплексирования и масштабирования скорости передачи от 155 Мбит/с до 40 Гбит/с. Недостаток состоит в необходимости оптимизации работы с Ethernet и IP/MPLS с большими пульсациями трафика.

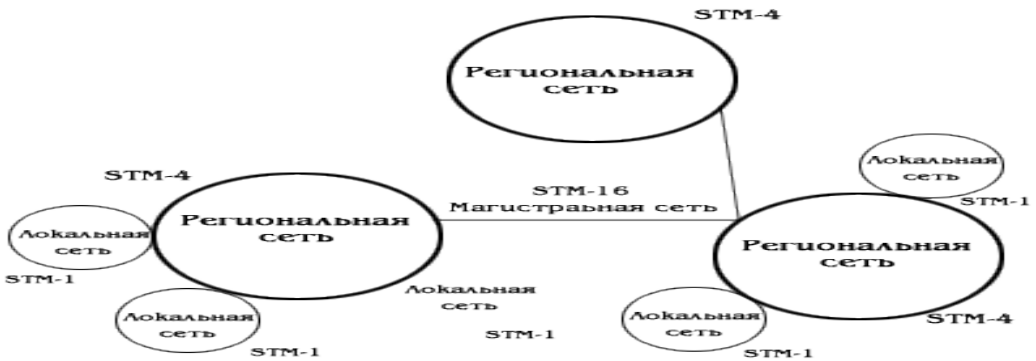


Рис. Пример первичной сети, построенной на технологии SDH

SDH	SONET	Скорость
—	STS-1, OC-1	51,840 Мбит/с
STM-1	STS-3, OC-3	155,520 Мбит/с
STM-3	STS-9, OC-9	466,560 Мбит/с
STM-4	STS-12, OC-12	622,080 Мбит/с
STM-6	STS-18, OC-18	933,120 Мбит/с
STM-8	STS-24, OC-24	1,244 Гбит/с
STM-12	STS-36, OC-36	1,866 Гбит/с
STM-16	STS-48, OC-48	2,488 Гбит/с

Сети X.25 относятся к первому поколению сетей коммутации пакетов.

Протоколы X.25 разработаны ITU еще в 1974 г. В России их популярность остается значительной до настоящего времени, поскольку эти сети хорошо работают на ненадежных линиях благодаря протоколам с установлением соединения и коррекцией ошибок на двух уровнях - канальном и сетевом. Технология сетей X.25 имеет несколько существенных признаков, отличающих ее от других технологий.

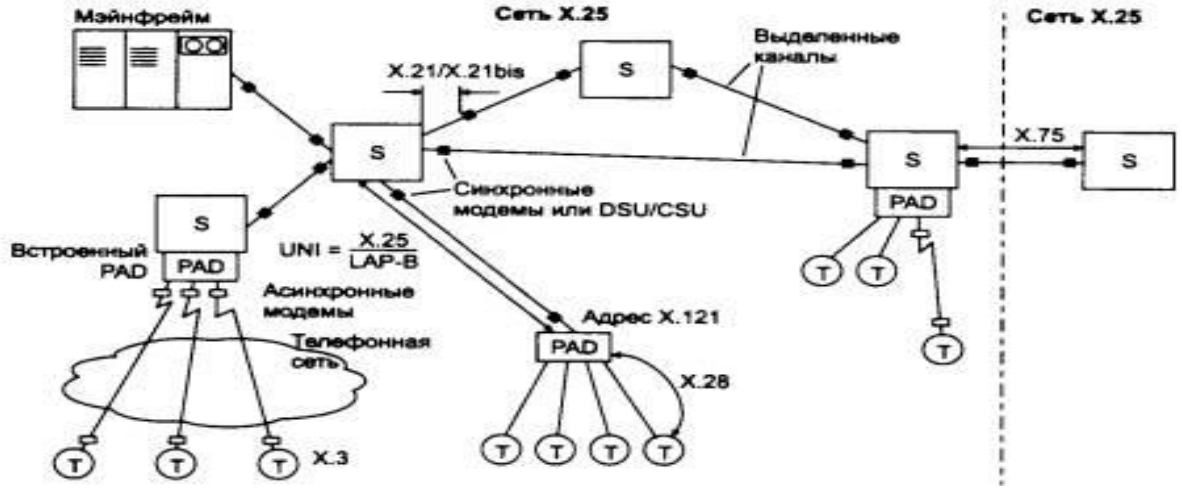
1. Наличие в структуре сети специального устройства - **PAD (Packet Assembler Disassembler) «Сборщик-разборщик пакетов»**, предназначенного для выполнения операции сборки нескольких низкоскоростных потоков байт от терминалов в пакеты, передаваемые по сети и направляемые компьютерам для обработки. К удаленному устройству PAD терминалы подключаются по асинхронному интерфейсу, обычно для этой цели используется интерфейс RS-232C. Один PAD обычно обеспечивает доступ для 8, 16 или 24 асинхронных терминалов. Устройства PAD часто используются для подключения к сетям X.25 кассовых терминалов и банкоматов, имеющих асинхронный интерфейс RS-232.

2. Наличие трехуровневого стека протоколов с использованием на канальном и сетевом уровнях протоколов с установлением соединения, управляющих потоками данных и исправляющих ошибки.

3. Ориентация на однородные стеки транспортных протоколов во всех узлах сети - сетевой уровень рассчитан на работу только с одним протоколом канального уровня и не может подобно протоколу IP объединять разнородные сети. Сеть X.25 состоит из коммутаторов (Switches, S), называемых **также центрами коммутации пакетов (ЦКП)**, расположенных в различных географических точках и соединенных высокоскоростными выделенными каналами (рис.). Выделенные каналы могут быть как цифровыми, так и аналоговыми.

Взаимодействие двух сетей X.25 определяет стандарт X.75.

Компьютеры и локальные сети обычно подключаются к сети X.25 непосредственно через адаптер X.25 или маршрутизатор, поддерживающий на своих интерфейсах протоколы X.25. Для управления устройствами PAD в сети существует протокол X.29, с помощью которого узел сети может управлять и конфигурировать PAD удаленно, по сети. Стандарт X.25 относится к трем нижним уровням ЭМВОС, т.е. включает протоколы физического, канального и сетевого уровней. На сетевом уровне используется коммутация пакетов.



Структура сети X.25 (64 кбит/с – 2 Мбит/с)

Характеристики сети:

- **пакет** размером до одного **килобайта** содержит адресную, управляющую, информационную и контрольную части, т.е. в его заголовке имеются флаг, адреса отправителя и получателя, тип кадра (служебный или информационный), номер кадра (используется для правильной сборки сообщения из пакетов);

- на канальном уровне применено оконное управление, размер окна задает число кадров, которые можно передать до получения подтверждения (это число равно 8 или 128);
- передача данных по виртуальным (логическим) каналам, т.е. это сети с установлением соединения;
- узлы на маршруте, обнаружив ошибку, ликвидируют ошибочный пакет и запрашивает повторную передачу пакета. В сетевом протоколе X.25 значительное внимание уделено контролю ошибок (в отличие, например, от протокола IP, в котором обеспечение надежности передается на транспортный уровень). Эта особенность приводит к уменьшению скорости передачи, т.е. **сети X.25 низкоскоростные** (обычно обеспечивается скорость **64 кбит/с**), но зато эти сети можно реализовать на каналах связи с невысокой помехоустойчивостью. Контроль ошибок производится при инкапсуляции и восстановлении пакетов во всех коммутаторах, а не только в оконечном узле. Типичная АКД в X.25 — синхронный модем с дуплексным бит-ориентированным протоколом. Скорости от 9,6 до 64 кбит/с. На физическом уровне для связи с цифровыми каналами передачи данных используется протокол X.21, а с аналоговыми каналами — протокол X.21bis.

Сети Frame Relay (FR) как и сети **X.25**, — это сети пакетной коммутации. В них в отличие от сетей X.25 обеспечивается большая скорость до 2 Мбит/с за счет исключения контроля ошибок в промежуточных узлах, так как контроль, адресация, инкапсуляция и восстановление выполняются в оконечных пунктах, т.е. на транспортном уровне.

Сети ATM

Перспективными являются технологии передачи информации в вычислительных сетях, обеспечивающие высокие скорости передачи **разнородной информации** (данных, речевых и видеосигналов) на значительные расстояния. Передача голосовой и видеоинформации обычно требуется в режиме реального времени и задержки должны быть только малыми (так, для голосовой связи — около 6 мс).
К числу таких технологий, прежде всего, относится **технология ATM** (Asynchronous Transfer Mode), которая кратко формулируется, как **быстрая коммутация коротких пакетов фиксированной длины 53 байт**, называемых **ячейками**. По этой причине и саму технологию ATM иногда называют **коммутацией ячеек**. На сегодняшний день технология ATM обеспечивает наиболее высокую эффективность и качество передачи голосового трафика на низкоскоростных каналах (NxE1) за счет совершенных механизмов качества обслуживания (QoS).
Сети ATM относят к сетям с установлением соединения. Соединения могут быть постоянными и коммутируемыми (динамическими). Первые устанавливаются и разрываются администратором сети, их действие продолжительно, для каждого нового обмена данными между абонентами постоянного соединения не нужно тратить время на его установление. Вторые устанавливаются и ликвидируются автоматически для каждого нового сеанса связи.
Каждое соединение получает свой идентификатор, который указывается в заголовке ячеек (как номер троллейбуса). При установлении соединения каждому коммутатору на выбранном пути следования данных передаются данные о соответствии идентификаторов и портов коммутаторов. Коммутатор, распознав идентификатор, направляет ячейку в нужный порт. Непосредственное указание в заголовке адресов получателя и отправителя не требуется, **заголовок** короткий — **всего 5 байтов**.
Высокие скорости в ATM обеспечиваются рядом технических решений:
Во-первых, физической основой для ATM служат высокоскоростные каналы передачи данных. Так, при применении технологии SONET в ATM предусматриваются каналы OC-1, OC-3, OC-12 и OC-48 на ВОЛС со скоростями соответственно 52, 155, 622 и 2488 Мбит/с. Большое число каналов с временным мультиплексированием (TDM) можно использовать для параллельной передачи частей одного и того же "объемного" сообщения, что соответствует понятию "статистическое мультиплексирование"

Во-вторых, Для контроля правильности заголовков используется один байт в заголовке ячейки, в котором размещается контрольный код Хемминга для заголовка. Искаженные и не восстановленные по Хеммингу ячейки отбрасываются.

В-третьих, упрощена маршрутизация. Собственно установление соединения выполняется аналогично этой процедуре в TCP/IP. Однако далее номер рассчитанного маршрута помещается в заголовок каждого пакета, и для них не нужно заново определять маршрут по таблицам маршрутизаторов при прохождении через сеть. Другими словами, осуществляется передача с установлением соединения (в отличие, например, от IP). При этом клиент направляет серверу запрос в виде специального управляющего кадра. Кадр проходит через промежуточные маршрутизаторы и/или коммутаторы, в которых соединению (каналу) присваивается идентификаторы виртуальных пути и канала VPI/VCI.

В-четвертых, фиксированная длина пакетов (кадров) упрощает алгоритмы управления и буферизации данных, исключает необходимость инкапсуляции или конвертирования пакетов при смене форматов в промежуточных сетях (если они соответствуют формату ячейки ATM). Применяемый подход позволяет в дальнейшем перевести сеть с технологии ATM на технологию IP с полным сохранением первоначальных инвестиций.

ATM использовался в WAN-сетях, в оборудовании для передачи аудио/видео потоков, как промежуточный слой между физическим и вышележащим уровнем **в устройствах ADSL** для каналов не более 2 Мбит/с. Но в конце десятилетия ATM начинает вытесняться новой технологией IP-VPN, связанной с технология Gigabit Ethernet, которая начинает конкурировать с ATM. Главными достоинствами последней является значительно более низкая стоимость, преемственность, простота, легкость в настройке и эксплуатации. **Переход** с Ethernet или Fast Ethernet на Gigabit Ethernet можно было осуществить значительно легче и дешевле. Проблему качества обслуживания Gigabit Ethernet решил за счет скорости и более дешевой полосы пропускания, нежели за счет умного оборудования. Свитчи ATM стали вытесняться маршрутизаторами IP/MPLS. По прогнозу компании Uvum от 2009г., к 2015г. Новые **ATM и Frame relay** должны почти полностью исчезнуть, в то время как рынки Ethernet и IP-VPN будут продолжать расти с хорошим темпом.

.