ТРАНСПОРТНЫЕ ТЕХНОЛОГИИ ГЛОБАЛЬНЫХ СЕТЕЙ

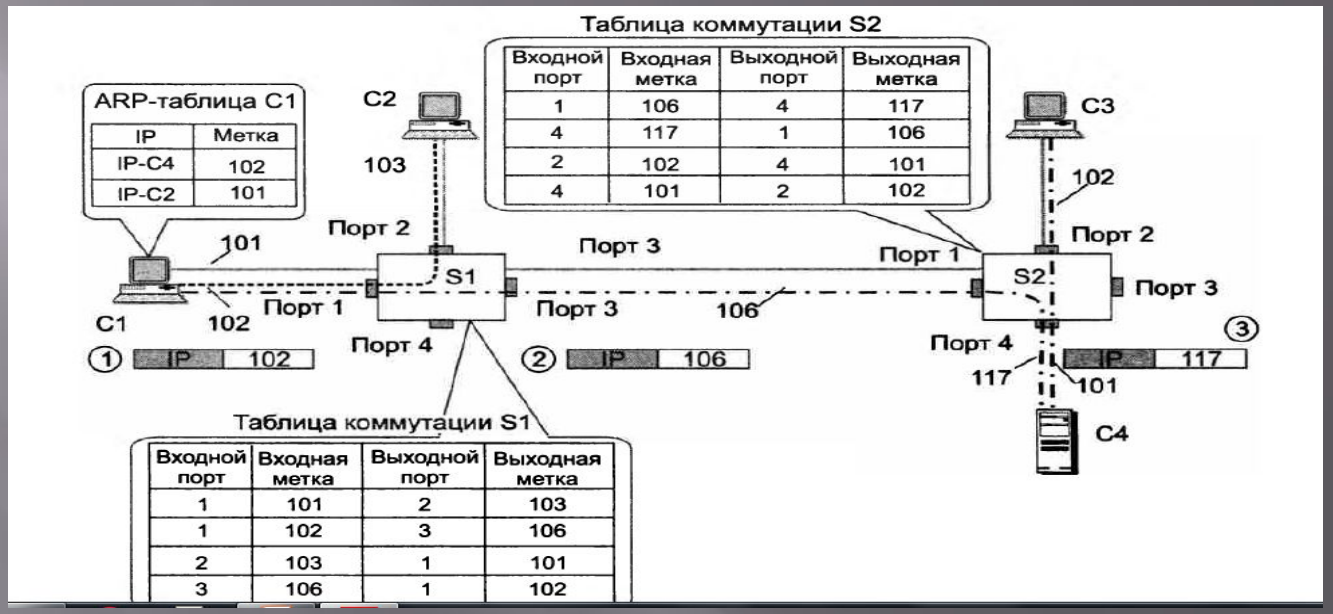
Технологии виртуальных каналов — от X .25 к M PLS

Глобальные компьютерные сети объединяют Интернет и протокол IP . В глобальных сетях протокол IP работает поверх специфических технологий канального уровня, разработанных с учетом характеристик глобальных линий связи и транспортных услуг, предоставляемых этим видом сетей. На протяжении всего времени существования глобальных компьютерных сетей важную роль в них играли транспортные технологии, основанные на технике виртуальных каналов. Мы рассмотрим, каким образом происходила эволюция технологий этого типа, от X.25 через frame relay и ATM к MPLS — технологии, которая смогла объединить технику виртуальных каналов с протоколами управляющего слоя стека TCP/IP.

Принципы работы виртуального канала

В сети с виртуальными каналами два узла могут начать обмен данными только после того, как между ними будет установлено логическое соединение — виртуальный канал. Виртуальный канал лучше защищает пользователей от внешних атак, поскольку у злоумышленника нет возможности посылать пакеты данных от одного произвольного узла к другому, что вполне можно сделать в сети, построенной на транспортной технологии дейтаграммного типа, такой как IP или Ethernet. Продвижение кадров вдоль виртуального канала происходит не на основе адресов конечных узлов, а на основе метки, которая позволяет коммутаторам сети определять принадлежность кадров тому или иному виртуальному каналу и продвигать их соответственно. Значение метки потока изменяется в каждом коммутаторе при передаче кадра с входного интерфейса на выходной, — в этом случае говорят, что происходит коммутация по меткам. Коммутация по меткам позволяет избавиться от требования уникальности их значений в пределах сети, которую обеспечить сложно; для того, чтобы кадры различных виртуальных каналов не смешивались, достаточно обеспечить уникальность значений меток только в пределах отдельного интерфейса. Из-за того, что коммутация по меткам является неотъемлемым атрибутом технологий виртуальных каналов, у них есть и второе название — технологии коммутации по меткам. Технически установление виртуального канала означает формирование записей в таблицах продвижения кадров на каждом коммутаторе вдоль виртуального канала. Такая таблица включает информацию о продвижении: на какой выходной порт нужно передать кадр с данной меткой, какое новое значение нужно присвоить метке после передачи кадра на выходной интерфейс.

На рисунке показан фрагмент сети, состоящей из двух коммутаторов S1 и S2 и четырех конечных узлов C1-C4. Через эти коммутаторы проложено три виртуальных канала: C1-C2, C1-C4 и C3-C4.



Эти каналы являются двунаправленными, а это означает, что кадры по ним могут передаваться в любом из двух направлений. Для каждого виртуального канала в таблице продвижения имеется две записи — по одной для каждого направления. Например, первая запись в таблице коммутации коммутатора S1 (запись 1-101-2-103) определяет работу коммутатора по продвижению кадров виртуального канала C1-C2 в направлении от C1 к C2; она предписывает коммутатору S1 передать кадр, принятый на порт 1 со значением метки 101, на порт 2 и поменять значение метки (скоммутировать метку) на 103. Третья запись (2-103-1-101) означает, что все пакеты, которые поступят на порт 2 со значением метки 102, будут продвигаться на порт 3, а ее значение поменяется

Существуют также однонаправленные виртуальные каналы. В случае их использования для дуплексного обмена информацией нужно установить два независимых виртуальных канала между конечными узлами, по одному для каждого направления.

Виртуальные каналы делится на два класса.

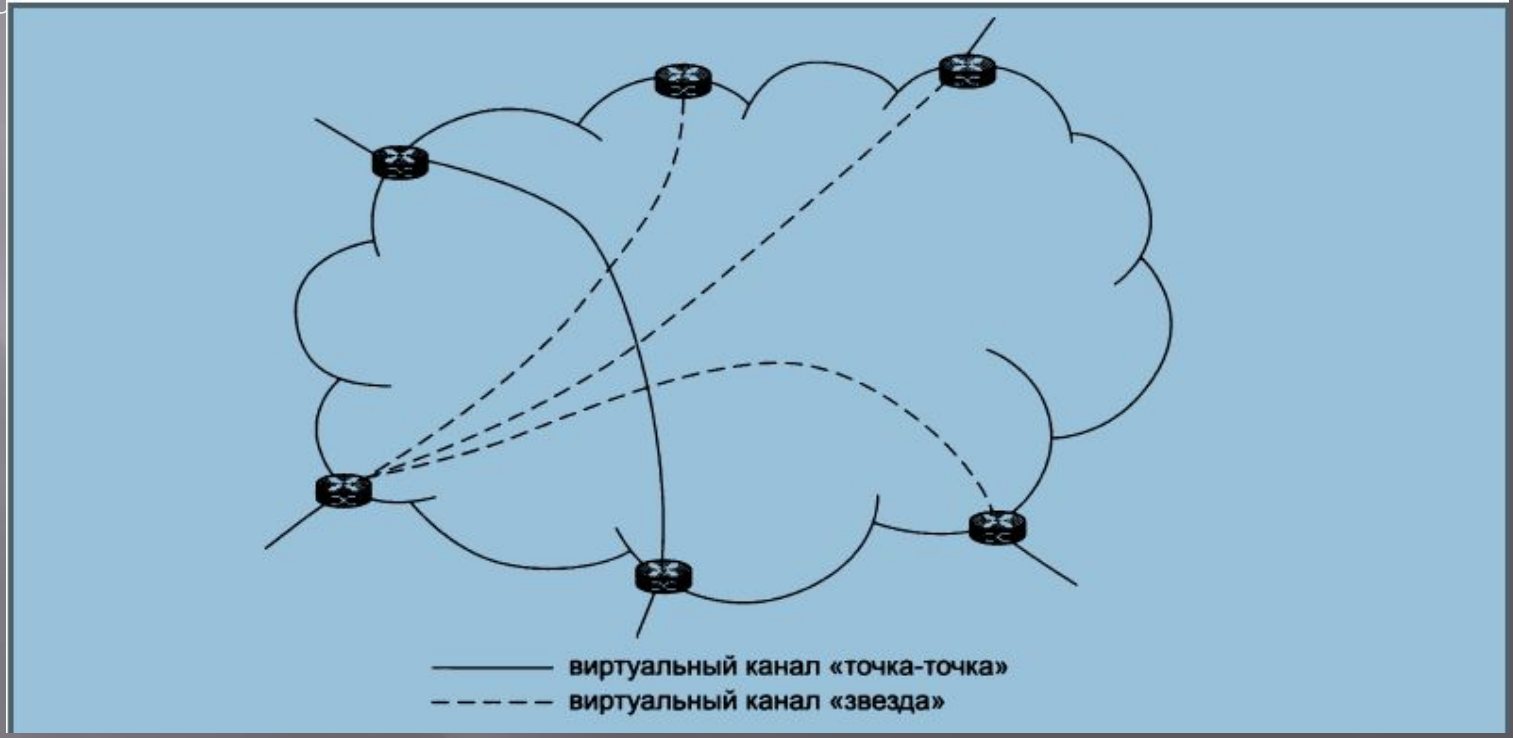
-коммутируемые виртуальные каналы (Switched Virtual Circuit, SVC); □

-постоянные виртуальные каналы (Permanent Virtual Circuit, PVC).

Для поддержания режима SVC в сети должны существовать таблицы маршрутизации, в соответствии с которыми продвигается пакет с запросом соединения. По отношению к пакету с запросом соединения сеть работает в дейтаграммном режиме, и такой пакет должен содержать адрес назначения конечного узла, а не метку.

Постоянный виртуальный канал устанавливается вручную, администратор создает его на достаточно длительное время (отсюда название), возможно, с привлечением централизованной системы управления сетью. Виртуальные каналы чаще всего имеют двухточечную топологию. Однако существуют каналы и с другим типом топологии — звезда (рис. 19.2). В канале с такой топологией один и тот же кадр передается от источника — центра звезды, называемого также концентратором, — вдоль ее лучей всем конечным узлам. Конечные узлы не могут использовать виртуальный канал звездообразной топологии для обмена кадрами между собой, он передает кадры в обратном направлении только от конечного узла к центральному узлу. Виртуальные каналы со звездообразной топологией рассчитаны на эффективную поддержку группового вещания.

Виртуальный канал является удобным инструментом для инжиниринга трафика. Это объясняется тем, что он может быть установлен независимо в каждом промежуточном коммутаторе путем соответствующего назначения локальных меток, выполняемого администратором сети или внешней программной системой. Поток пакетов, который должен быть передан по виртуальному каналу, может быть определен гибко и с любой степенью детализации, в этом определении могут использоваться не только IP-адреса назначения, как это происходит в IP-сетях, но и любые признаки: IP-адреса источника, TC P/U D P-порты назначения, поле DSCP и т. п., что также повышает эффективность инжиниринга трафика



Сети, работающие на основе техники виртуальных каналов, относятся к типу **сетей, не поддерживающих широковещание с множественным доступом (Non Broadcast Multiple Access, NBMA).** Действительно, у такой сети существует произвольное количество конечных узлов, но отсутствует возможность послать кадр сразу всем узлам — ни двухточечный, ни звездообразный виртуальный канал этого не позволяет. В сетях NBMA протокол IP не может воспользоваться услугами протокола ARP для автоматического построения ARP-таблицы, так как эти услуги основаны на широковещательных запросах. Так что в тех случаях, когда входящий поток отображается на виртуальный канал на основе IP- адреса, таблицу отображения, которая является здесь ARP-таблицей, приходится строить вручную или же с помощью некоторого дополнительного протокола, не использующего широковещание.

Эффективность виртуальных каналов.

Сравнение эффективности виртуальных каналов мы проведем отдельно для коммутируемых и постоянных виртуальных каналов, сравнивая первые с дейтаграммными технологиями, а вторые — с выделенными физическими каналами.

Применение *коммутируемых виртуальных каналов* *требует предварительного установления соединения, что вносит дополнительную задержку перед передачей данных по сравнению с применением дейтаграммных протоколов. Эта задержка особенно сказывается при передаче небольшого объема данных, когда время установления виртуального канала может быть соизмеримым со временем передачи данных. Кроме того, дейтаграммный метод быстрее адаптируется к изменениям в сети. При отказе коммутатора или линии связи вдоль виртуального канала соединение разрывается, и виртуальный канал нужно прокладывать заново, обходя отказавшие участки сети.*

Маршрутизация пакетов в сети с поддержкой виртуальных каналов ускоряется за счет двух факторов. Первый состоит в том, что решение о продвижении пакета принимается быстрее, так как таблица коммутации, в которой есть информация только об установленных виртуальных каналах, чаще всего существенно меньше таблицы маршрутизации, в которой число записей определяется количеством сетей назначения (размер таблицы маршрутизации магистральных IP-маршрутизаторов провайдеров Интернета составлял весной 2015 года около 550 ООО записей).

Вторым фактором является уменьшение доли служебной информации в пакетах. Адреса конечных узлов в глобальных сетях обычно имеют достаточно большую длину — 4 байта в версии IP v4,16 байт в версии IPv6, MAC- адрес имеет длину 6 байт. Номер же виртуального канала обычно занимает 10-12 бит, так что накладные расходы на адресную часть существенно сокращаются, а значит, полезная скорость передачи данных возрастает.

Постоянные виртуальные каналы являются гораздо более эффективными в отношении производительности передачи данных, чем коммутируемые. Значительную часть работы по маршрутизации пакетов сети выполняет администратор, вручную прокладывая постоянные виртуальные каналы и оставляя коммутаторам только продвижение пакетов на основе готовых таблиц коммутации портов.

Постоянные виртуальные каналы выгодно использовать для передачи агрегированных потоков трафика, состоящих из большого количества индивидуальных потоков абонентов сети. В этом случае виртуальный канал прокладывается не между конечными абонентами, а между участком магистрали сети, на котором данный агрегированный поток существует, например от одного пограничного маршрутизатора сети оператора связи до другого. В силу закона больших чисел агрегированные потоки обладают высокой степенью устойчивости, так что для них нет смысла динамически создавать коммутируемые виртуальные каналы — лучше эффективно использовать постоянные, которые при хорошем планировании (методами инжиниринга трафика) оказываются достаточно загруженными. Подводя итог, можно сказать, что виртуальные каналы более эффективны при передаче долговременных, чем кратковременных, потоков, так как в этом случае

Технология X.25

Технология виртуальных каналов X.25 появилась на заре эры компьютерных сетей, практически одновременно с сетью ARPANET, давшей начало Интернету и дейтаграммному протоколу IP. Долгое время, до середины 1980-х, X.25 была основной технологией для построения как сетей операторов связи, так и корпоративных сетей.

Технология X.25 оказалась хорошо приспособленной для построения глобальной всемирной сети благодаря тому, что была масштабируемой — в ней был определен протокол межсетевого взаимодействия, позволяющий объединять сети разных провайдеров, а также поддерживалась международная система иерархической адресации X.121, включающая код страны, номер сети и номер терминала в сети. Сети X.25 используют трехуровневый стек протоколов. Физический уровень в то время чаще всего был представлен модемами, работающими на коммутируемых и выделенных телефонных линиях со скоростями 2400-9600 Кбит/с. Как на канальном (LAP-B), так и на сетевом (X.25/3) уровне протоколы стека X.25 поддерживают установление соединений и коррекцию ошибок на основе метода скользящего окна. Такая избыточность функций, направленных на обеспечение надежности передачи данных, объясняется ориентацией технологии на ненадежные аналоговые каналы. Распространение высокоскоростных и надежных цифровых оптических каналов в середине 80-х годов привело к тому, что функции технологии X.25 по обеспечению надежной передачи данных превратились из достоинства технологии в ее недостаток, так как лишь замедляли скорость передачи пользовательских данных. Результатом этой революции стало появление

Технология Frame Relay

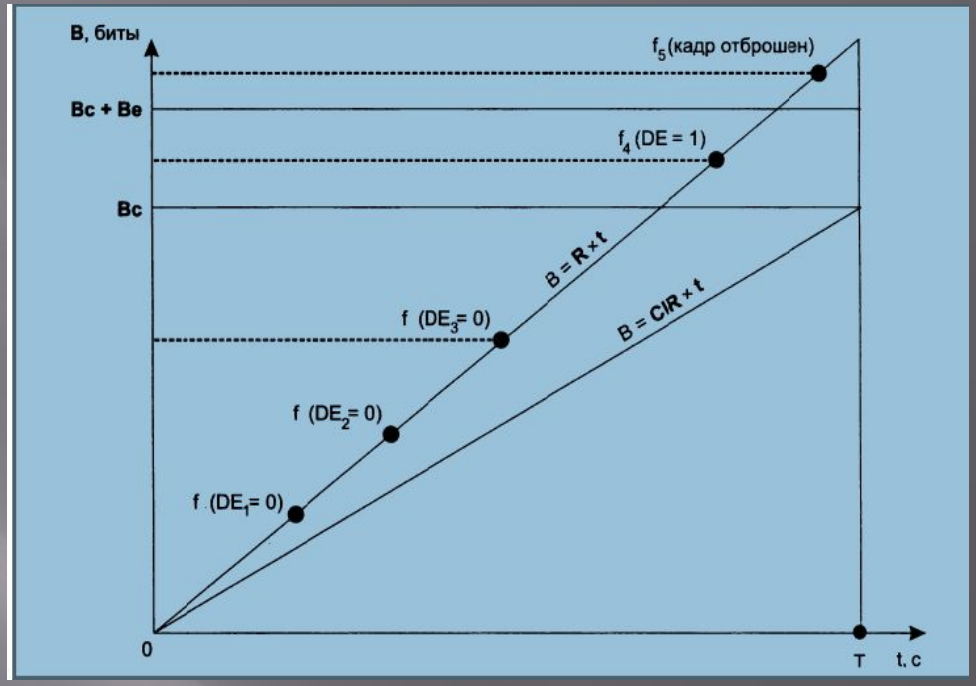
Главным достоинством Frame Relay является простота; освободившись от многих ненужных в условиях существования надежных оптических каналов связи функций, эта технология предлагает только тот минимум услуг, который необходим для быстрой доставки кадров адресату. В соответствии с этой концепцией протокол Frame Relay работает в режиме передачи данных по «возможности», то есть не поддерживает процедуры надежной передачи кадров, оставляя повторную передачу искаженных и потерянных данных протоколам более высоких уровней, например TCP. В сетях Frame Relay имеются только постоянные виртуальные каналы, что также упрощает их организацию.

Разработчики технологии Frame Relay сделали важный шаг вперед, предоставив пользователям сети гарантию пропускной способности сетевых соединений — свойство, которое до появления Frame Relay не поддерживалось ни одной технологией глобальных сетей с коммутацией пакетов.

Для каждого виртуального соединения в технологии Frame Relay определяется несколько параметров, связанных со скоростью передачи данных. 1.Согласованная скорость передачи данных (Committed Information Rate, CIR) — гарантированная пропускная способность соединения; фактически сеть гарантирует передачу данных пользователя со скоростью предложенной нагрузки, если эта скорость не превосходит CIR. 2.Согласованная величина пульсации (Committed Burst Size, Bc) — максимальное количество байтов, которое сеть будет передавать от данного пользователя за интервал времени T, называемый временем пульсации, соблюдая согласованную скорость CIR. 3.Дополнительная величина пульсации (Excess Burst Size, Be) — максимальное количество байтов, которое сеть будет пытаться передать сверх установленного значения Bc за интервал времени T.

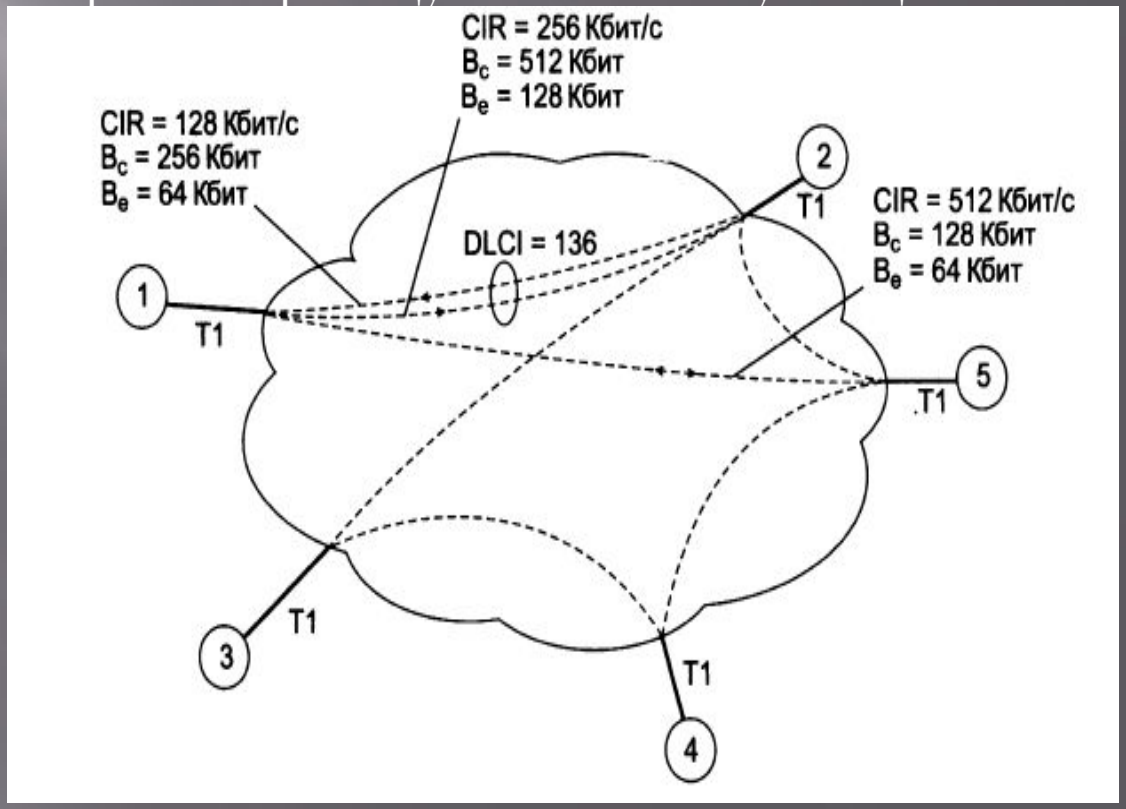
Второй параметр пульсации (Be) позволяет оператору сети дифференцированно обрабатывать кадры, которые не укладываются в профиль CIR. Обычно кадры, которые приводят к превышению пульсации Bc, но не превышают пульсацию Bc + Be, сетью не отбрасываются, а обслуживаются, но без гарантий по скорости CIR. Для запоминания факта нарушения в кадрах Frame Realy имеется специальное поле DE (Discard Eligibility — возможность отбрасывания). В том случае, когда это поле кадра содержит значение 1, последующие коммутаторы данного виртуального канала отбрасывают такой кадр, если испытывают перегрузку И только если превышен порог Bc + Be, кадры отбрасываются сразу Если приведенные величины определены, то время T определяется следующей формулой: $T = Bc/CIR$.
Можно рассматривать значения CIR и T в качестве варьируемых параметров, тогда производной величиной станет пульсация Bc. Обычно для контроля пульсаций трафика выбирается время T, равное 1-2 секунды при передаче компьютерных данных и в диапазоне десятков-сотен миллисекунд при передаче голоса.
Соотношение между параметрами CIR, Bc, Be и T иллюстрирует рис. 19.3 (R — скорость в канале доступа; fi-fs — кадры).

Работа сети описывается двумя линейными функциями, показывающими зависимость количества переданных битов от времени: B = RxtHB = CIRxt. Средняя скорость поступления данных в сеть составила на этом интервале R бит/с, и она оказалась выше CIR. На рисунке представлен случай, когда за интервал времени T в сеть по виртуальному каналу поступило 5 кадров.



Кадры fi, f2 и f3 доставили в сеть данные, суммарный объем которых не превысил порог Bc, поэтому эти кадры ушли дальше транзитом с признаком DE = 0. Данные кадра *U, прибавленные к данным кадров fi, f2 и f3, уже превысили порог Bc, но еще не достигли порога Bc + Be, поэтому кадр {4 также ушел дальше, но уже с признаком DE = 1 (возможно, его удалят последующие коммутаторы). Данные кадра fs, прибавленные к данным предыдущих кадров, превысили порог Bc + Be, поэтому этот кадр был удален из сети.*

На рис. 19.4 приведен пример сети Frame Relay с пятью удаленными региональными отделениями корпорации. Обычно доступ к сети осуществляется по каналам с пропускной способностью, большей чем CIR. Однако при этом пользователь платит не за пропускную способность канала, а за заказанные величины CIR, Bc и Be. Так, при применении в качестве линии доступа канала T-1 и заказа обслуживания со скоростью CIR, равной 128 Кбит/с, пользователь будет платить только за скорость 128 Кбит/с, а скорость канала T-1 в 1,5 Мбит/с окажет влияние на верхнюю границу возможной пульсации Bc + Be.



Параметры качества обслуживания могут быть разными для разных направлений виртуального канала. Так, на рисунке абонент 1 соединен с абонентом 2 виртуальным каналом с меткой 136. При направлении от абонента 1 к абоненту 2 канал имеет среднюю скорость 128 Кбит/с с пульсациями Bc = 256 Кбит (интервал T составил 1 с) и Be = 64 Кбит. А при передаче кадров в обратном направлении средняя скорость уже может достигать значения 256 Кбит/с с пульсациями Bc = 512 Кбит и Be = 128 Кбит.

Сети Frame Relay получили большое распространение в 1980-е и в первой половине 1990-х годов. Их услуги с предоставлением гарантий пропускной способности являлись в то время наиболее качественными услугами VPN, и многие корпоративные сети их использовали.

Однако постепенно скорость доступа 2 Мбит/с, которую предоставляли эти сети, становилась явно недостаточной для корпоративных пользователей. К тому же мультимедийный трафик начал все больше интересовать как пользователей, так и провайдеров Интернета, а сети Frame Relay были рассчитаны только на передачу *компьютерного трафика. В результате в начале 1990-х годов была начата разработка новой технологии глобальных сетей, получившей название асинхронного режима передачи.*

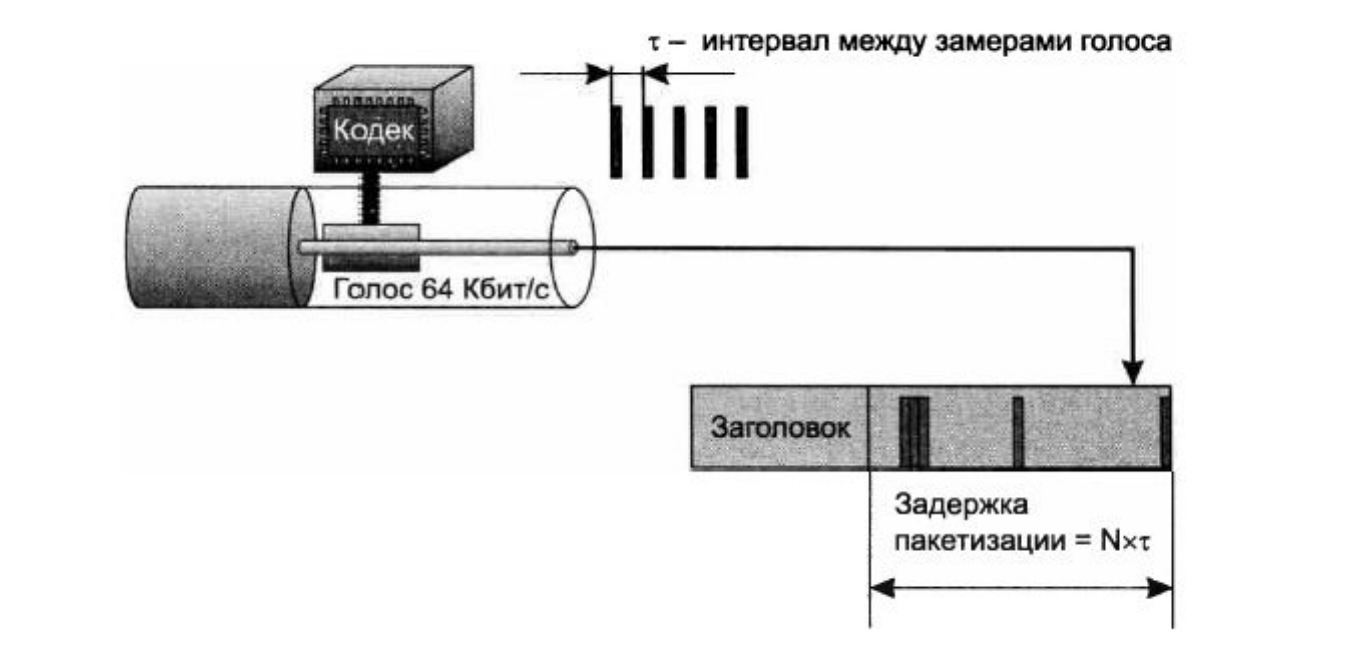
Технология ATM (асинхронный режим передачи)

Асинхронный режим передачи (Asynchronous Transfer Mode, ATM) — это технология, основанная на технике ***виртуальных каналов и предназначенная для использования в качестве единого универсального транспорта сетей с интегрированным обслуживанием. ATM может передавать трафик разного типа, чувствительный к задержкам,(голосовой) эластичным(просмотр веб-страницы). И этим самым технология ATM отличается от Frame Relay .*** Цель технологии ATM обеспечение многоуровневой иерархии скоростей и возможности использования первичных сетей SDH для соединения коммутаторов ATM.

В технологии ATM для переноса данных применяются **ячейки. Принципиально ячейка отличается от кадра только тем, что имеет, во-первых,** ***фиксированный, во-вторых, небольшой размер.*** Длина ячейки составляет 53 байта, а поля данных — 48 байт. Именно такие размеры позволяют сети ATM передавать чувствительный к задержкам аудио- и видеотрафик с необходимым уровнем качества. Небольшой размер ячейки снижает две составляющие задержки: задержку пакетизации и время нахождения ячейки в очереди.

Задержка пакетизации связана с процессом оцифровывания аналоговой (например, голосовой) информации и помещения ее в пакет компьютерной сети. Эту операцию должны выполнять интерфейсные модули коммутаторов ATM, к которым подключены в качестве абонентских устройств обычные аналоговые телефоны. Задержка пакетизации зависит только от размера пакета, так как кодек — устройство, которое выполняет оцифровывание голоса, — работает с постоянной частотой 8 КГц, требуемой для качественного представления голоса в

На рисунке показан голосовой кодек — устройство, которое представляет голос в цифровой форме. Пусть он выполняет замеры голоса в соответствии со стандартной частотой 8 КГц (то есть через каждые 125 мкс), кодируя каждый замер одним байтом данных. Если мы используем для передачи голоса кадры Ethernet максимального размера, то в один кадр поместится 1500 замеров голоса. В результате первый замер, помещенный в кадр Ethernet, вынужден будет ждать отправки кадра в сеть (1500 - 1) x 125 = 187 375 мкс, или около 187 мс. Это весьма большая задержка для голосового трафика. Рекомендации стандартов говорят о величине 150 мс как о максимально допустимой *суммарной задержке голоса, в которую задержка пакетизации входит как одно из слагаемых.*



Задержка пакетизации не зависит от битовой скорости протокола, она зависит только от быстродействия кодека и размера поля данных кадра.

Классы трафика различаются в зависимости от следующих критериев:

- является ли скорость трафика постоянной (как у голосового трафика) или переменной (как у трафика данных) трафик с постоянной скоростью не может не требовать гарантий средней скорости.
- является ли трафик чувствительным к задержкам;
- нужны ли гарантии средней скорости передачи.

Сети ATM отличаются от сетей Frame Relay в сетях ATM нужный уровень обслуживания задается не только численными значениями параметров, гарантирующих среднюю скорость передачи данных, но и самой категорией услуги. Категорий услуг для наиболее важных классов трафика, таких как чувствительный к задержкам голосовой трафик с постоянной битовой скоростью и чувствительный к задержкам компрессированный видеотрафик с переменной битовой скоростью, сделало ATM гораздо более эффективной технологией мультисервисных сетей. Frame Relay, может эффективно передавать только нечувствительный к задержкам трафик данных с переменной битовой скоростью. Технология ATM , пережил свой пик до 1990годов. Одна из причин появление сетей DWDM и рост скорости сетей Ethernet до 10Гбит/с. Кроме того, оборудование ATM не смогло перейти порог скорости 622 Мбит/с. Ограничением стал маленький размер ячеек — на высоких скоростях коммутаторы с трудом справляются с обработкой интенсивных потоков таких ячеек.

Технологии двухточечных каналов

Технологии двухточечных каналов или протоколы «точка-точка», отражает топологию связей между маршрутизаторами.

Протокол HDLC (High-level Data Link Control — высокоуровневое управление линией связи) представляет целое семейство протоколов, реализующих функции канального уровня. Важным свойством HDLC является его функциональное разнообразие. HDLC поддерживает двухточечные соединения, и соединения с одним источником и несколькими приемниками, а кроме того, предусматривает различные функциональные роли взаимодействующих станций. HDLC является старым каналом разработан 70-годов. В IP-маршрутизаторах чаще всего используется версия протокола HDLC Cisco. HDLC стала стандартом де-факто для IP-маршрутизаторов. Версия Cisco HDLC работает только в дейтаграммном режиме, что соответствует современной ситуации с незашумленными надежными каналами. Cisco HDLC включает несколько расширений, главным из которых является многопротокольная поддержка. В заголовок кадра Cisco HDLC добавлено поле типа протокола, подобное полю EtherType в кадре Ethernet. Это поле содержит код протокола, данные которого переносит кадр Cisco HDLC.

Протокол PPP

Протокол PPP (Point-to-Point Protocol — протокол двухточечной связи) является стандартным протоколом Интернета. Протокол PPP так же, как и HDLC, представляет собой целое семейство протоколов, в которое, в частности, входят:

- протокол управления линией связи (Link Control Protocol, LCP); Протокол, в соответствии с которым принимаются параметры соединения, называется протоколом управления линией связи (LCP).
- протокол управления сетью (Network Control Protocol,); Каждый протокол сетевого уровня конфигурируется отдельно с помощью соответствующего протокола управления сетью (NCP).
- многоканальный протокол PPP (Multi Link PPP, MLPPP); Многопротокольная поддержка — способность протокола PPP поддерживать несколько протоколов сетевого уровня — обусловила распространение PPP как стандарта де-факто.
- протокол аутентификации по паролю (Password Authentication Protocol, PAP);
- протокол аутентификации по квитированию вызова (C hallenge H andshake Authentication Protocol, CHAP).

Особенностью протокола PPP, отличается от других протоколов канального уровня, сложная переговорная процедура принятия параметров соединения. Стороны обмениваются различными параметрами, такими как качество линии, размер кадров, тип протокола аутентификации и тип инкапсулируемых протоколов сетевого уровня.

Технологии доступа

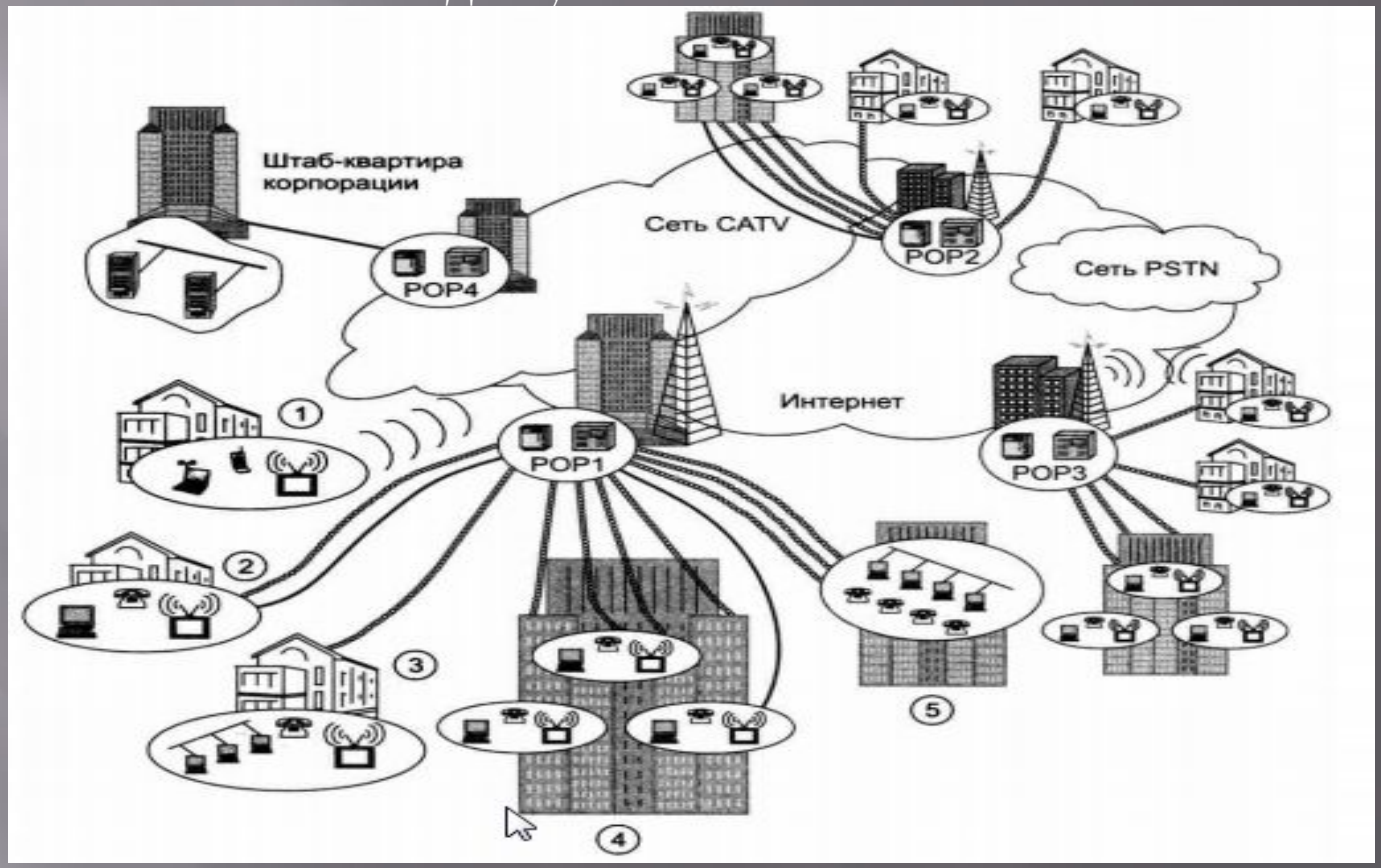
Проблема последней мили. Наиболее острых проблем компьютерных сетей является удаленный доступ, и получил название проблемы последней мили, где под последней милей подразумевается расстояние от точки присутствия (POP) оператора связи до помещений клиентов. Определяется следующими факторами:

1.Современным пользователям необходим высокоскоростной доступ, обеспечивающий качественную передачу трафика любого типа, в том числе данных, голоса, видео.

2.Подавляющее большинство домов в больших и малых городах и особенно в сельской местности по-прежнему соединены с POP абонентскими окончаниями телефонной сети, которые не были рассчитаны на передачу компьютерного трафика.

Сегодня существует ряд технологий, способных предоставлять услуги скоростного удаленного доступа на основе существующей инфраструктуры абонентских окончаний телефонных сетей или сетей кабельного телевидения. Наиболее популярными технологиями являются технология ADSL, использующая телефонные абонентские окончания, и кабельные модемы, работающие поверх сети кабельного телевидения.

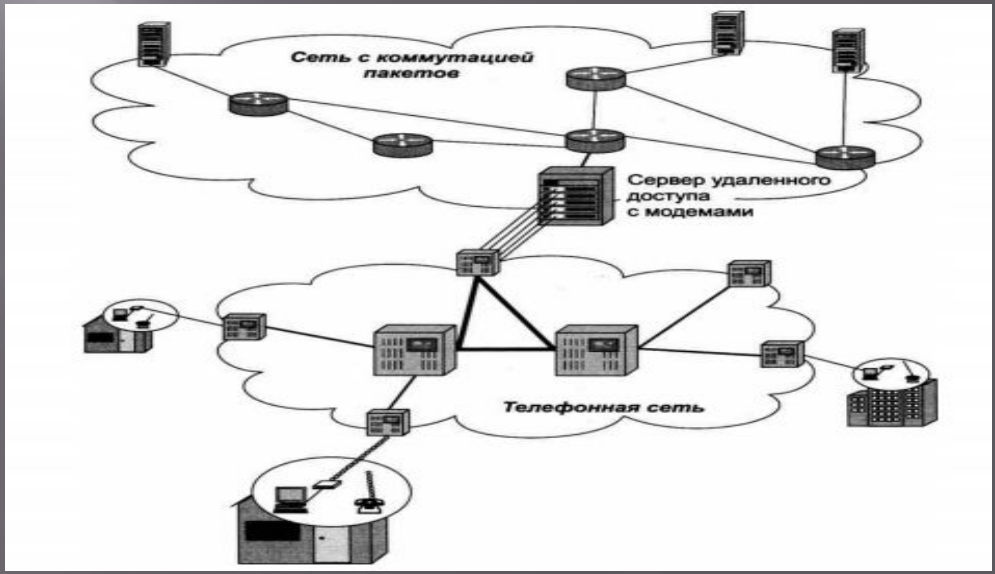
Рисунок 19.6 иллюстрирует разнообразный и пестрый мир удаленного доступа.



Коммутируемый аналоговый доступ

Основная идея коммутируемого доступа состоит в том, чтобы использовать имеющуюся телефонную сеть для организации коммутируемого соединения между компьютером домашнего пользователя и сервером удаленного доступа (Remote Access Server, RAS), установленным на границе телефонной и компьютерной сетей. Компьютер пользователя подключается к телефонной сети с помощью коммутируемого модема, который поддерживает стандартные процедуры набора номера и имитирует работу телефонного аппарата для установления соединения с RAS.

Схема организации доступа через аналоговую телефонную сеть показана на рис. 19.7.



Сервер RAS имеет два типа соединений: с телефонной сетью через пул модемов и с локальной IP-сетью, соединенной с Интернетом

Сервер RAS имеет два типа соединений: с телефонной сетью через пул модемов и с локальной IP-сетью, соединенной с Интернетом
Существует двухточечный протокол туннелирования (Point-to-Point Tunneling Protocol, PPTP). При работе PPTP сервер удаленного доступа поставщика услуг передает транзитом запрос пользователя серверу аутентификации предприятия и в случае положительного ответа соединяет пользователя через Интернет с корпоративной сетью.
Сервер RAS обслуживает подключенные к нему клиентские компьютеры, используя протокол Proxy-ARP . Это означает, что клиентский компьютер работает в режиме удаленного узла локальной IP-сети, с которой соединен сервер RAS, получая на время соединения один из IP-адресов этой сети.

Модемы.

Реализует функции физический и канальный уровень.

Канальный уровень нужен , выявлять и исправлять ошибки, появляющиеся из-за искажений битов. Функция исправления ошибок является очень важной для модема. Для протокола, который работает поверх модемного соединения между удаленным компьютером и RAS, канальный протокол модема прозрачен, его работа проявляется только в том, что интенсивность битовых ошибок (BER) снижается до приемлемого уровня. В качестве канального протокола между компьютером и RAS в основном используется протокол PPP, который не занимается восстановлением искаженных и потерянных кадров, способность модема исправлять ошибки оказывается весьма полезной.

Протоколы и стандарты модемов определены в рекомендациях ITU-T серии V и делятся на три группы:

- стандарты, определяющие скорость передачи данных и метод кодирования, модемы являются одними из наиболее старых и заслуженных устройств передачи данных в процессе своего развития они прошли долгий путь, прежде чем научились работать на скоростях до 56 Кбит/с. Первые модемы работали со скоростью 300 бит/с и исправлять ошибки не умели.
- стандарты исправления ошибок V.34, повысил максимальную скорость передачи данных в два раза, с 14 до 28 Кбит/с по сравнению со своим предшественником — стандартом V.32. Особенностью стандарта V.34 являются процедуры динамической адаптации к изменениям характеристик канала во время обмена информацией .

- стандарты сжатия данных.

Стандарт V.90 описывает технологию недорогого и быстрого доступа пользователей к сетям поставщиков услуг.

В стандарте V.92 учитывается возможность принятия модемом второго вызова во время соединения.

Коррекция ошибок. Для модемов, работающих с DTE по асинхронному интерфейсу, комитет ITU-T разработал протокол коррекции ошибок V.42. В стандарте V.42 основным является протокол доступа к линии связи для модемов (Link Access Protocol for Modems, LAP-M). Рекомендации V.42 позволяют устанавливать связь без ошибок с любым модемом, поддерживающим этот стандарт, а также с любым MNPсовместимым модемом.

Сжатие данных. Почти все современные модемы при работе по асинхронному интерфейсу поддерживают стандарты сжатия данных ITU-T V.42bis и MNP-5 (обычно с коэффициентом 1:4, некоторые модели — до 1:8). При работе модемов по синхронному интерфейсу наиболее популярным является протокол сжатия синхронных потоков данных (Synchronous Data Compression, SDC) компании Motorola.

Коммутируемый доступ через сеть ISDN