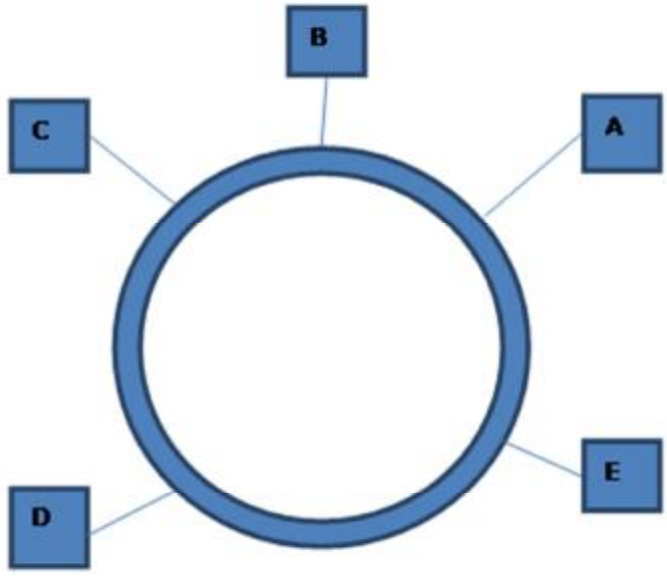
Тема 9. Методы доступа к среде передачи: конфликтные и бесконфликтные. Основные принципы организации и передачи данных.

Классификация методов доступа к среде передачи. Метод доступа CSMA/CD. Метод доступа CSMA/CA. Метод доступа приоритету. Маркерные методы доступа. Передача данных по сети. Инкапсуляция пакетов. Виртуальные каналы.

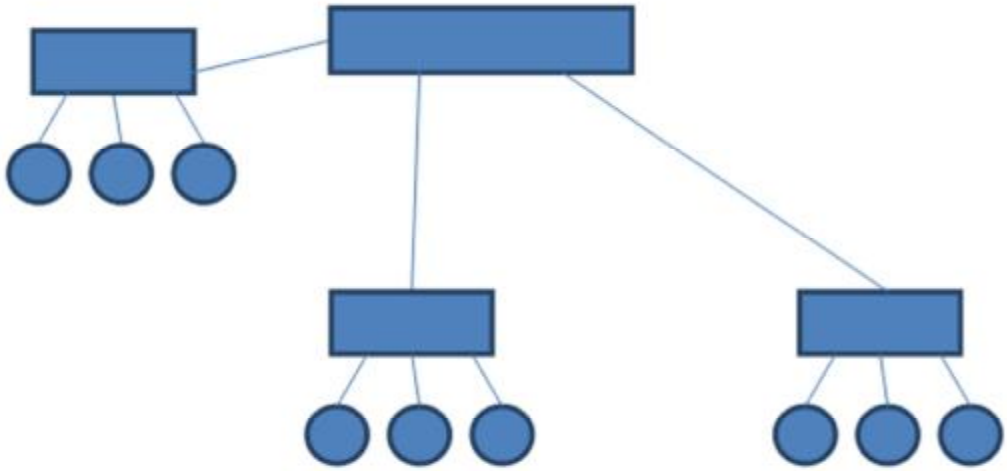
Кольцевая сеть

В данном случае имеется замкнутая проводящая среда, по которой информация распространяется в одном направлении.

Если станция А отправляет информацию станции С, она движется по кольцу через адаптеры других станций, эти станции ее не воспринимают. Когда кадр данных доходит до станции получателя получатель считывает эту информацию. Делает пометку что информация считана правильно и информация следует далее по кольцу до получателя, и тот удаляет этот кадр из сети.



В настоящее время наиболее широко используется древовидные сети. Ветвления в такой сети используются при помощи высокоскоростных концентраторов (хабах). В отличии от кольцевых сетей, шинной топологии, звездообразных, древовидные сети обладают высокой живучестью. При нарушении функционирования какой либо ветки дерева оставшаяся часть сети продолжает функционировать.



Классификация методов доступа к среде передачи данных

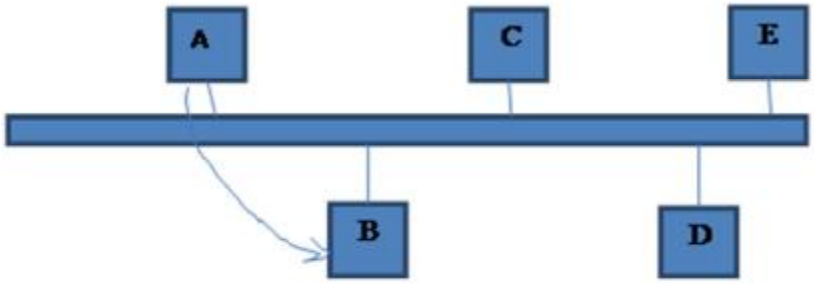
Если станция обращается к среде передачи данных, как только у нее есть информация для передачи это **случайный метод доступа.** Случайный метод ведет свое происхождение от радиосетей со случайным методом доступа пользователей к компьютеру, которая была впервые использована в Гавайском университете и называлась «Aloha». «Алоха» - это метод доступа, когда станция сразу отправляет данные в сеть, не прослушивая свободна ли среда передачи данных. В сетях используется модификация случайного метода доступа (в сетях шинной топологии или древовидных сетях)

Станция перед началом передачи всегда прослушивает среду, и начинает передачу только если среда свободна (контроль несущей частоты). Но и в этом случае возможно наложение сообщений одно на другое.

Пусть в момент т1 станция А прослушивает среду, а станция В уже начала передачу. Однако из за конечной скорости распространения информации по сети этот сигнал не достиг станции А, она начинает передачу, и происходит наложение сообщений. Дальнейшая передача бессмыслена. Чтобы прекратить передачу предусмотрен следующий механизм: станция не только передает информацию в сеть, но и принимает информацию из сети. Если то, что она принимает - совпадает, с тем, что она передает, это означает, что столкновения нет. При наложении информации станция будет считывать искаженную информацию, станция обнаружившая столкновение прекращает передачу, и будет делать попытку передать информацию через случайные промежутки времени, которые подобраны так, чтобы избежать столкновения. Описанный метод доступа называется**случайным методом доступа с контролем несущей частоты и обнаружением столкновений**.

Детерминированные методы доступа представляют собой такие методы, когда станции получают доступ к среде на основе некоторого правила (алгоритма). В сетях шинной топологии (и древовидных) могут использоваться детерминированные методы доступа двух видов:

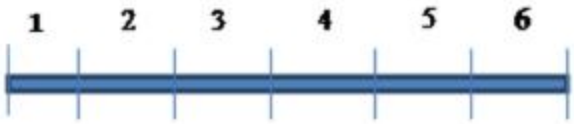
1.Метод передачи полномочий (маркерный метод доступа)



Используется специальный служебный кадр (маркер) станция может передавать информацию в сеть, если она получила этот кадр-маркер. Пусть маркер у станции А, когда она заканчивает передачу данных, она передает маркер станции В, если у станции В нет информации для передачи, она передает маркер следующей станции С. Таким образом маркер переходит от станции к станции и каждая по очереди получает право передачи данных. Последняя станция Е передает маркер станции А, тем самым замыкая логическое кольцо.

Случайный метод доступа эффективно использовать при небольшой нагрузке на сеть, когда станции редко обращаются к сети. Если станции активно обращаются к сети, и сеть практически не пустует, предпочтителен маркерный метод. В случае малой нагрузки на сеть, маркер циркулирует по сети, которая пуста.

2.Метод разделения времени



Интервал времени длительностью T, разделяется на n отрезков времени, где n – число станций в сети. Каждый j из отрезков времени отведен для того, чтобы соответствующие в частности j станция осуществляла передачу в течение этого отрезка времени. Этот метод эффективен, когда нагрузка от станции поступает высокая (все станции активны) и активность их относительно равномерная. В случае неравномерной активности станций станция имеющая большой объем информации активно обращается к сети, но только в свои интервалы времени, и не может использовать другие, которые простаивают, что снижает эффективность работы сети.

Методы доступа к среде передачи (media access method) делятся на конфликтные и неконфликтные.

Конфликтные методы доступа предполагают возможность конфликта (коллизии) – одновременной передачи по одной линии двумя или более компами

При этом методе доступа узел, желающий послать кадр в сеть, прослушивает линию. Если линия занята или обнаружена коллизия, попытка передачи отклады-вается на некоторое время. Основные разновидности:

CSMA/CA - множественный доступ с прослушиванием несущей и избежанием коллизий

CSMA/CD - множественный доступ с опознаванием несущей и обнаружением коллизий

2. При неконфликтном методе узлы получают доступ к среде в предопределенном порядке. Последовательность определяется контроллером сети, который может быть централизованным (его функции может выполнять, например, сервер) или/и распреде-ленным (функции выполняются оборудованием всех узлов).

Основные типы:

-доступ с передачей маркера (token passing), применяемый в сетях ARCnet, Token Ring, FDDI;

-доступ по приоритету

поллинг (polling) — опрос готовности, применяемый в больших машинах (mainframes) и технологии 100VG-AnyLAN, так же polling применяется в широкополосных беспроводных технологиях (WiMax, фирменные решения). Основное преимущество метода — ограниченное время прохождения кадра, мало зависящее от нагрузки.

Метод доступа к среде CSMA/CD. Этапы доступа к среде.

В сетях Ethernet используется метод доступа к среде передачи данных, называемый методом коллективного доступа с опознаванием несущей и обнаружением коллизий (carrier-sense-multiply-access with collision detection, CSMA/CD).

Этот метод используется исключительно в сетях с общей шиной (к которым относятся и радиосети, породившие этот метод). Все компьютеры такой сети имеют непосредственный доступ к общей шине, поэтому она может быть использована для передачи данных между любыми двумя узлами сети. Простота схемы подключения - это один из факторов, определивших успех стандарта Ethernet. Говорят, что кабель, к которому подключены все станции, работает в режиме коллективного доступа (multiply-access,MA).

Алгоритм работы: Узел, готовый послать кадр, прослушивает линию. При отсутствии несущей он начинает передачу кадра, одновременно контролируя состояние линии При обнаружении коллизии передача прекращается и повторная попытка откладывается на случайное время. Коллизии — нормальное, хотя и не очень частое явление для CSMA/CD. Их частота связана с количеством и активностью подключенных узлов. Нормально коллизии могут начинаться в определенном временном окне кадра, запоздалые коллизии сигнализируют об аппаратных неполадках в кабеле или узлах. Метод эффективнее, чем CSMA/CA, но требует более

сложных и дорогих схем цепей доступа Применяется во многих сетевых архитектурах: Ethernet, EtherTalk (реализация Ethernet фирмы Apple), G-Net, IBM PC Network, AT&T StarLAN.

Csma/ca

CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance) — множественный доступ с прослушиванием несущей и избежанием коллизий Узел, готовый послать кадр, прослушивает линию. При отсутствии несущей он посылает короткий сигнал запроса па передачу (RTS) и определенное время ожидает ответа (CTS) от адресата назначения. При отсутствии ответа (подразумевается возможность коллизии) попытка передачи откла¬дывается, при получении ответа в линию посылается кадр. При запросе на широковещательную передачу (RTS содержит адрес 255) CTS не ожидается. Метод не позволяет полностью избежать коллизий, но они обрабатываются на вышестоящих уровнях протокола Метод применяется в сети Apple LocalTalk, характерен простотой и низкой стоимостью цепей доступа.

Метод доступа с маркером

Для обеспечения доступа станций к физической среде по кольцу циркулирует кадр специального формата и назначения — маркер.

Получив маркер, станция анализирует его и при отсутствии у нее данных для передачи обеспечивает его продвижение к следующей станции. Станция, которая имеет данные для передачи, при получении маркера изымает его из кольца, что дает ей право доступа к физической среде для передачи своих данных.

Затем эта станция выдает в кольцо кадр данных установленного формата последовательно по битам. Переданные данные проходят по кольцу всегда в одном направлении от одной станции к другой. Кадр снабжен адресом назначения и адресом источника.

Все станции кольца ретранслируют кадр побитно, как повторители. Если кадр проходит через станцию назначения, то, распознав свой адрес, эта станция копирует кадр в свой внутренний буфер и вставляет в кадр признак подтверждения приема. Станция, выдавшая кадр данных в кольцо, при обратном его получении с подтверждением приема изымает этот кадр из кольца и передает в сеть новый маркер, давая другим станциям сети возможность передавать данные.

Метод доступа по приоритету

Каждый кадр данных или маркер имеет приоритет, устанавливаемый битами приоритета (значение от 0 до 7, причем 7 — наивысший приоритет), Станция может воспользоваться маркером, только если у нее есть кадры для передачи с приоритетом равным или большим, чем приоритет маркера.

Сетевой адаптер станции с кадрами, у которых приоритет ниже, чем приоритет маркера, не может захватить маркер, но может поместить наибольший приоритет своих ожидающих передачи кадров в резервные биты маркера, но только в том случае, если записанный в резервных битах приоритет ниже его собственного. В результате в резервных битах приоритета устанавливается наивысший приоритет станции, которая

пытается получить доступ к кольцу, но не может этого сделать из-за высокого приоритета маркера. Станция, сумевшая захватить маркер, передает свои кадры с приоритетом маркера, а затем передает маркер следующему соседу. При этом она переписывает значение резервного приоритета в поле приоритета маркера, а резервный приоритет обнуляется. Поэтому при следующем проходе маркера по кольцу его захватит станция, имеющая наивысший приоритет.

Информация в локальных сетях, как правило, передается отдельными порциями, кусками, называемыми в различных источниках пакетами, кадрами или блоками. Использование пакетов связано с тем, что в сети, как правило, одновременно может происходить несколько сеансов связи, то есть в течение одного и того же интервала времени могут идти два или больше процессов передачи данных между различными парами абонентов. Пакеты как раз и позволяют разделить во времени сеть между передающими информацию абонентами.

Если бы вся требуемая информация передавалась сразу, непрерывно, без разделения на пакеты, то это привело бы к монопольному захвату сети одним из абонентов на довольно продолжительное время. Все остальные абоненты вынуждены были бы ждать окончания передачи всей информации, что в ряде случаев могло бы потребовать десятков секунд и даже минут (например, при копировании содержимого целого жесткого диска). Чтобы уравнять в правах всех абонентов, а также примерно уравнять время доступа к сети и интегральную скорость передачи информации для всех абонентов, как раз и используются пакеты (кадры). Длина пакета зависит от типа сети, но обычно она составляет от нескольких десятков байт до нескольких килобайт.

Структура пакета определяется прежде всего аппаратными особенностями данной сети, выбранной топологией и типом среды передачи информации, а также существенно зависит от используемого протокола (порядка обмена информацией). Строго говоря, в каждой сети структура пакета индивидуальна. Но существуют некоторые общие принципы формирования пакета, определяемые характерными особенностями обмена информацией по любым локальным сетям.

Модель OSI описывает только системные средства взаимодействия, реализуемые операционной системой, системными утилитами, системными аппаратными средствами. Модель не включает средства взаимодействия приложений конечных пользователей. Свои собственные протоколы взаимодействия приложения реализуют, обращаясь к системным средствам. Поэтому необходимо различать уровень взаимодействия приложений и прикладной уровень.

Следует также иметь в виду, что приложение может взять на себя функции некоторых верхних уровней модели OSI. Например, некоторые СУБД имеют встроенные средства удаленного доступа к файлам. В этом случае приложение, выполняя доступ к удаленным ресурсам, не использует системную файловую службу; оно обходит верхние уровни модели OSI и обращается напрямую к системным средствам, ответственным за транспортировку сообщений по сети, которые располагаются на нижних уровнях модели OSI.

Итак, пусть приложение обращается с запросом к прикладному уровню, например к файловой службе. На основании этого запроса программное обеспечение прикладного уровня формирует сообщение стандартного формата. Обычное сообщение состоит из заголовка и поля данных. Заголовок содержит служебную информацию, которую необходимо передать через сеть прикладному уровню машины-адресата, чтобы сообщить ему, какую работу надо выполнить. В нашем случае заголовок, очевидно, должен содержать информацию о месте нахождения файла и о типе операции, которую необходимо над ним выполнить. Поле данных сообщения может быть пустым или содержать какие-либо данные, например те, которые необходимо записать в удаленный

файл. Но для того чтобы доставить эту информацию по назначению, предстоит решить еще много задач, ответственность за которые несут нижележащие уровни.
После формирования сообщения прикладной уровень направляет его вниз по стеку представительному уровню. Протокол представительного уровня на основании информации, полученной из заголовка прикладного уровня, выполняет требуемые действия и добавляет к сообщению собственную служебную информацию - заголовок представительного уровня, в котором содержатся указания для протокола представительного уровня машины-адресата. Полученное в результате сообщение передается вниз сеансовому уровню, который в свою очередь добавляет свой заголовок, и т. д. (Некоторые реализации протоколов помещают служебную информацию не только в начале сообщения в виде заголовка, но и в конце, в виде так называемого «концевика».) Наконец, сообщение достигает нижнего, физического уровня, который собственно и передает его по линиям связи машине-адресату. К этому моменту сообщение «обрастает» заголовками всех уровней (рис. 13).

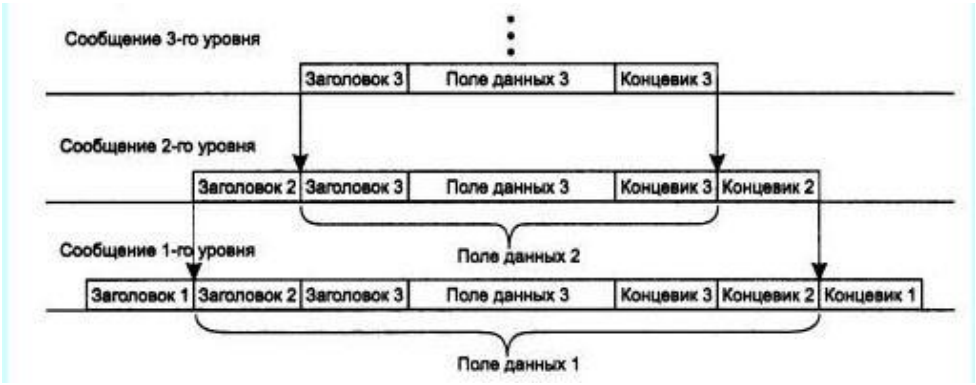


Рисунок 13 – Вложенность сообщений различных уровней

Когда сообщение по сети поступает на машину - адресат, оно принимается ее физическим уровнем и последовательно перемещается вверх с уровня на уровень. Каждый уровень анализирует и обрабатывает заголовок своего уровня, выполняя соответствующие данному уровню функции, а затем удаляет этот заголовок и передает сообщение вышележащему уровню.
Наряду с термином *сообщение (message)* существуют и другие термины, применяемые сетевыми специалистами для обозначения единиц данных в процедурах обмена. В стандартах ISO для обозначения единиц данных, с которыми имеют дело протоколы разных уровней, используется общее название *протокольный блок данных (Protocol Data Unit, PDU)*. Для обозначения блоков данных определенных уровней часто используются специальные названия: кадр (frame), пакет (packet), дейтаграмма (datagram), сегмент (segment).
В модели OSI различаются два основных типа протоколов. В протоколах с *установлением соединения (connection-oriented)* перед обменом данными отправитель и получатель должны сначала установить соединение и, возможно, выбрать некоторые параметры протокола, которые они будут использовать при обмене данными. После завершения диалога они должны разорвать это соединение. Телефон - это пример взаимодействия, основанного на установлении соединения.
Вторая группа протоколов - протоколы *без предварительного установления соединения (connectionless)*. Такие протоколы называются также *дейтаграммными* протоколами. Отправитель просто передает сообщение, когда оно готово. Опускание письма в почтовый ящик - это пример связи без предварительного установления соединения. При взаимодействии компьютеров используются протоколы обоих типов.
Инкапсуля́ция в компью́терных сетя́х — это метод построения модульных сетевых протоколов, при котором логически независимые функции сети абстрагируются от

нижележащих механизмов путём включения или инкапсулирования этих механизмов в более высокоуровневые объекты. Например, когда приложению требуется послать сообщение с помощью UDP, то производится последовательность действий:

– в первую очередь приложение заполняет специальную структуру данных, в которой указывает информацию о получателе (сетевой протокол, IP-адрес, порт UDP);

– передаёт сообщение, его длину и структуру с информацией о получателе обработчику протокола UDP (транспортный уровень);

– обработчик UDP формирует датаграмму, в которой в качестве данных выступает сообщение, а в заголовках находится UDP-порт получателя (а также другие данные);

– обработчик UDP передаёт сформированную датаграмму обработчику IP (сетевой уровень);

– обработчик IP рассматривает переданную UDP датаграмму как данные и предваряет их своим заголовком (в котором, в частности, находится IP-адрес получателя, взятый из той же структуры данных приложения, и номер верхнего протокола);

– полученный пакет обработчик IP передаёт на канальный уровень, который опять-таки рассматривает данный пакет как «сырые» данные;

– обработчик канального уровня, аналогично предыдущим обработчикам, добавляет в начало свой заголовок (в котором так же указывается номер протокола верхнего уровня, в нашем случае это 0x0800(IP)) и, в большинстве случаев, добавляет конечную контрольную сумму, тем самым формируя кадр;

– далее полученный кадр передаётся на физический уровень, который осуществляет преобразование битов в электрические или оптические сигналы и посылает их в среду передачи.

То есть, говоря более простым языком, инкапсуляция — упаковка пакетов (возможно, разного протокола) в пакеты одного протокола, включая адрес.

Типичная структура пакета:

– *стартовая комбинация*, или *преамбула*, которая обеспечивает настройку аппаратуры адаптера или другого сетевого устройства на прием и обработку пакета. Это поле может отсутствовать или сводиться к одному-единственному стартовому биту.

– *сетевой адрес (идентификатор) принимающего абонента*, то есть индивидуальный или групповой номер, присвоенный каждому принимающему абоненту в сети. Этот адрес позволяет приемнику распознать пакет, адресованный ему лично, группе, в которую он входит, или всем абонентам сети одновременно.

– *сетевой адрес (идентификатор) передающего абонента*, то есть индивидуальный или групповой номер, присвоенный каждому передающему абоненту. Этот адрес информирует принимающего абонента, откуда пришел данный пакет. Включение в пакет адреса передатчика необходимо в том случае, когда одному приемнику могут попеременно приходить пакеты от разных передатчиков.

– *служебная информация*, которая указывает на тип пакета, его номер, размер, формат, маршрут его доставки, на то, что с ним надо делать приемнику и т.д.

– *данные* - та информация, ради передачи которой используется данный пакет. Правда, существуют специальные управляющие пакеты, которые не имеют поля данных. Их можно рассматривать как сетевые команды. Пакеты, включающие поле данных, называются информационными пакетами. Управляющие пакеты могут выполнять функцию начала сеанса связи, конца сеанса связи, подтверждения приема информационного пакета, запроса информационного пакета и т.д.

– *контрольная сумма пакета* - это числовой код, формируемый передатчиком по определенным правилам и содержащий в свернутом виде информацию обо всем пакете. Приемник, повторяя вычисления, сделанные передатчиком, с принятым пакетом, сравнивает их результат с контрольной суммой и делает вывод о правильности или ошибочности передачи пакета. Если пакет ошибочен, то приемник запрашивает его повторную передачу.

– стоповая комбинация служит для информирования аппаратуры принимающего абонента об окончании пакета, обеспечивает выход аппаратуры приемника из состояния приема. Это поле может отсутствовать, если используется самосинхронизирующийся код, позволяющий детектировать факт передачи пакета.

– В сетях с коммутацией пакетов сегодня применяется два класса механизмов передачи пакетов:

– дейтаграммная передача;

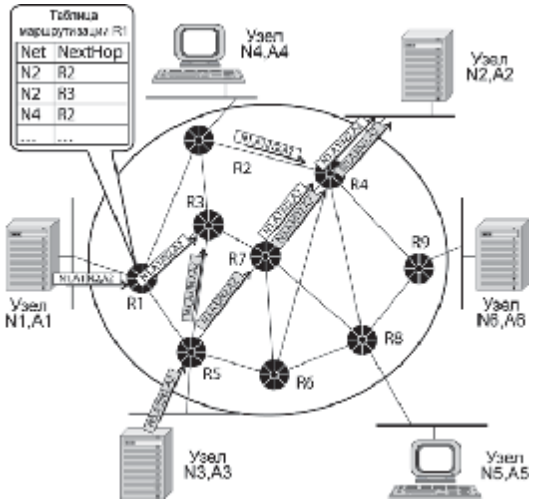
– виртуальные каналы.

– Примерами сетей, реализующих дейтаграммный механизм передачи, являются сети Ethernet, IP и IPX. С помощью виртуальных каналов передают данные сети X.25, frame relay и ATM. Сначала мы рассмотрим базовые принципы дейтаграммного подхода.

– Дейтаграммный способ передачи данных основан на том, что все передаваемые пакеты обрабатываются независимо друг от друга, пакет за пакетом. Принадлежность пакета к определенному потоку между двумя

конечными узлами и двумя приложениями, работающими на этих узлах, никак не учитывается.

– Выбор следующего узла — например, коммутатора Ethernet или маршрутизатора IP/IPX — происходит только на основании адреса узла назначения, содержащегося в заголовке пакета. Решение о том, какому узлу передать пришедший пакет, принимается на основе таблицы, содержащей набор адресов назначения и адресную информацию, однозначно определяющую следующий (транзитный или конечный) узел. Такие таблицы имеют разные названия — например, для сетей Ethernet они обычно называются таблицей продвижения (forwarding table), а для сетевых протоколов, таких как IP и IPX, — таблицами маршрутизации (routing table). Далее для простоты будем пользоваться термином "таблица маршрутизации" в качестве обобщенного названия такого рода таблиц, используемых для дейтаграммной передачи на основании только адреса назначения конечного узла.



– Рисунок 14 – Дейтаграммный принцип передачи пакетов

– В таблице маршрутизации для одного и того же адреса назначения может содержаться несколько записей, указывающих, соответственно, на различные адреса следующего маршрутизатора. Такой подход используется для повышения производительности и надежности сети. В примере на рис. 14 пакеты, поступающие в маршрутизатор R1 для узла назначения с адресом N2, A2, в целях баланса нагрузки распределяются между двумя следующими маршрутизаторами — R2 и R3, что снижает нагрузку на каждый из них, а значит, уменьшает очереди и ускоряет доставку. Некоторая "размытость" путей следования пакетов с одним и тем же адресом назначения через сеть является прямым следствием принципа независимой обработки каждого пакета, присущего дейтаграммным протоколам. Пакеты, следующие по одному и тому же адресу назначения, могут добираться до него разными

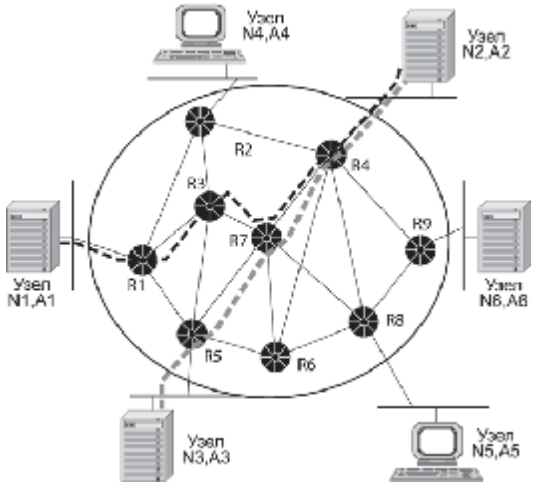
путями и вследствие изменения состояния сети, например отказа промежуточных маршрутизаторов.

– Такая особенность дейтаграммного механизма как размытость путей следования трафика через сеть также в некоторых случаях является недостатком. Например, если пакетам определенной сессии между двумя конечными узлами сети необходимо обеспечить заданное качество обслуживания. Современные методы поддержки QoS работают эффективней, когда трафик, которому нужно обеспечить гарантии обслуживания, всегда проходит через одни и те же промежуточные узлы.

– Виртуальные каналы в сетях с коммутацией пакетов

– Механизм виртуальных каналов (virtual circuit или virtual channel) создает в сети устойчивые пути следования трафика через сеть с коммутацией пакетов. Этот механизм учитывает существование в сети потоков данных.

–



– Рисунок 15 – Принцип работы виртуального канала.

– Если целью является прокладка для всех пакетов потока единого пути через сеть, то необходимым (но не всегда единственным) признаком такого потока должно быть наличие для всех его пакетов общих точек входа и выхода из сети. Именно для передачи таких потоков в сети создаются виртуальные каналы. На рисунке 15 показан фрагмент сети, в которой проложены два виртуальных канала. Первый проходит от конечного узла с адресом N1, A1 до конечного узла с адресом N2, A2 через промежуточные коммутаторы сети R1, R3, R7 и R4. Второй обеспечивает продвижение данных по пути N3, A3 — R5 — R7 — R4 — N2, A2. Между двумя конечными узлами может быть проложено несколько виртуальных каналов, как полностью совпадающих в отношении пути следования через транзитные узлы, так и отличающихся.

– Сеть только обеспечивает возможность передачи трафика вдоль виртуального канала, а какие именно потоки будут передаваться по этим

каналам, решают сами конечные узлы. Узел может использовать один и тот же виртуальный канал для передачи всех потоков, которые имеют общие с данным виртуальным каналом конечные точки, или же только части из них. Например, для потока реального времени можно использовать один виртуальный канал, а для трафика электронной почты — другой. В последнем случае разные виртуальные каналы будут предъявлять разные требования к качеству обслуживания, и удовлетворить их будет проще, чем в том случае, когда по одному виртуальному каналу передается трафик с разными требованиями к параметрам QoS.

– Важной особенностью сетей с виртуальными каналами является использование локальных адресов пакетов при принятии решения о передаче. Вместо достаточно длинного адреса узла назначения (его длина должна позволять уникально идентифицировать все узлы и подсети в сети, например технология ATM оперирует адресами длиной в 20 байт) применяется локальная, то есть меняющаяся от узла к узлу, метка, которой помечаются все пакеты, перемещаемые по определенному виртуальному каналу. Эта метка в различных технологиях называется по-разному: в технологии X.25 — номер логического канала (Logical Channel number, LCN), в технологии frame relay — идентификатор соединения уровня канала данных (Data Link Connection Identifier, DLCI), в технологии ATM — идентификатор виртуального канала (Virtual Channel Identifier, VCI). Однако назначение ее везде одинаково — промежуточный узел, называемый в этих технологиях коммутатором, читает значение метки из заголовка пришедшего пакета и просматривает свою таблицу коммутации, в которой указывается, на какой выходной порт нужно передать пакет. Таблица коммутации содержит записи только о проходящих через данный коммутатор виртуальных каналах, а не обо всех имеющихся в сети узлах (или подсетях, если применяется иерархический способ адресации). Обычно в крупной сети количество проложенных через узел виртуальных каналов существенно меньше количества узлов и подсетей, поэтому по размерам таблица коммутации намного меньше таблицы маршрутизации, а, следовательно, просмотр занимает гораздо меньше времени и не требует от коммутатора большой вычислительной мощности.

– Идентификатор виртуального канала (именно такое название метки будет использоваться далее) также намного короче адреса конечного узла (по той же причине), поэтому и избыточность заголовка пакета, который теперь не содержит длинного адреса, а переносит по сети только идентификатор, существенно меньше.

– Виртуальный путь – это соединение между двумя коммутаторами сети ATM, описанные в таблицах коммутации соответствующих коммутаторов. Виртуальные пути применяются для наиболее часто используемых направлений. По одному виртуальному пути могут передаваться несколько виртуальных каналов. Виртуальный путь существует независимо от того, идет по нему передача данных или нет. Всего виртуальных путей в рамках сети может быть 256. В каждом виртуальном пути м.б. до 65 000 соединений.

– Виртуальный канал – это соединение между двумя конечными станциями сети ATM. Виртуальный канал является двунаправленным.

– Имеются три вида виртуальных каналов:

– 1) постоянные виртуальные каналы (PVC). PVC устанавливается вручную в процессе конфигурирования сети.

– 2) коммутируемые виртуальные каналы (SVC). SVC устанавливается по мере необходимости всякий раз, когда конечная станция пытается передать данные другой станции. Это наиболее часто используемый тип каналов.

– 3) интеллектуальные постоянные виртуальные каналы (SPVC). SPVC представляет собой гибрид двух предыдущих типов каналов. Данное соединение устанавливается вручную на этапе конфигурирования сети, однако провайдер ATM знает только конечные станции.

– Преимущества PVC:

– 1) не тратится время на установление соединения, поэтому обеспечивается более высокая производительность сети.

– 2) обеспечивается лучший контроль над сетью.

– Недостаток: они должны формироваться вручную

–

– Преимущества SVC:

– 1) данный вид соединения лучше установить или устранить, нежели PVC.

– 2) с помощью SVC могут эмулироваться каналы без установления соединения.

– 3) SVC требует меньше затрат на обслуживание, т.к. данное соединение проводится автоматически, а не вручную.

– 4) данный вид соединения имеет более высокую отказоустойчивость.

– Преимущества SPVC:

– 1) Позволяет заранее задать конечные станции, поэтому не приходится тратить время на установление соединения.

– 2) Имеет более высокую отказоустойчивость подобно SVC.