Сети

Эволюция компьютерных сетей

Компьютерные сети, преимущества и недостатки

Сеть -- это взаимодействующая совокупность объектов, образуемых устройствами передачи и обработки данных.

Основные преимущества сетей:

1. Возможность совместного использования периферийных устройств.
2. Повышение эффективности и скорости обработки информации в группе сотрудников.
3. Обеспечение совместного доступа к сети интернет.
4. Быстрое получение доступа к корпоративным хранилищам информации.

Недостатки:

1. Всегда существует потенциальная угроза безопасности данных, передаваемых по сетям.
2. Существует опасность паралича деятельности организации при нарушении работоспособности сети.

Однако, в настоящее время сетевые технологии исключительно надёжны, а угроза безопасности возникает лишь в том случае, если компьютеры подключены к интернету. Но и в этом случае есть решение -- брандмауэр, лучше всего аппаратный.

Локальные сети

В начале 70-х годов появились большие интегральные схемы и основанные на них миникомпьютеры. Необходимость их объединения для совместной работы привела к появлению первых локальных вычислительных сетей.

Локальная сеть -- это объединение компьютеров, сосредоточенных на небольшой территории, обычно в радиусе 1-2 км. В общем случае локальная сеть представляет собой коммуникационную систему, принадлежащую одной организации.

В начале для соединения компьютеров друг с другом использовались нестандартные программно-аппаратные средства. Они могли соединять только те конкретные модели компьютеров, для которых были разработаны.

В середине 80-х годов постепенно сложились стандартные технологии объединения компьютеров в сеть. Это Ethernet, Arcnet, Token-link, token-bus и FDDI. Мощным стимулом для их появления послужили персональные компьютеры. С одной стороны они были достаточно мощными для работы сетевого ПО, а с другой стороны нуждались в объединении своей вычислительной мощности для решения сложных задач, а также разделения дорогих периферийных устройств и дисковых массивов. Поэтому ПК стали преобладать в локальных сетях, причем не только в качестве клиентских компьютеров, но и в качестве центров хранения и обработки данных.

В конце 90-х годов в лидеры вышла технология Ethernet. К этому семейству относятся: классическая технология Ethernet (10 мб/с), а также Fast Ethernet (100 мб/с) и Gigabit Ethernet (1000 мб/с).

Простые алгоритмы работы предопределили низкую стоимость оборудования Ethernet. Широкий диапазон иерархий скоростей позволяет рационально строить локальную сеть, применяя ту технологию семейства, которая в наибольшей степени отвечает задачам предприятия и потребностям пользователя.

Все технологии Ethernet очень близки друг к другу по принципам работы, что упрощает обслуживание и интеграцию этих сетей.

Глобальные сети

Развитие глобальных сетей началось в 60-х годах с решения простой задачи -- доступа к компьютеру с терминалов удаленных от него на большие расстояния. Терминалы соединялись с компьютерами через телефонные сети с помощью модемов. Затем появились системы в которых на ряду с соединениями типа терминал-компьютер были реализованы удаленные связи типа компьютер-компьютер.

Глобальные сети -- это сети, которые объединяют территориально рассредоточенные компьютеры, находящиеся в разных городах и странах. Именно при построении глобальных сетей впервые были предложены и отработаны многие основные идеи и концепции современных вычислительных сетей.

Глобальные компьютерные сети очень многое унаследовали от других, более старых и распространенных глобальных сетей (телефонных). Основным отличием глобальных компьютерных сетей от телефонных стал переход от принципа коммутации каналов к принципу коммутации пакетов. Прогресс глобальных компьютерных сетей во многом определялся прогрессом телефонных сетей.

С конца 60-х годов в телефонных сетях стала применяться передача голоса в цифровой форме. Была разработана специальная технология плезиохронной цифровой иерархии,

которая предназначена для первичных сетей. Такие сети не предоставляют услуг конечным пользователям, они являются фундаментом, на котором строятся скоростные цифровые каналы точка-точка.

В конце 80-х годов появилась технология синхронно-цифровой иерархии. Она расширила диапазон скоростей до 10 Гбит/с, а следующая технология спектрального мультиплексирования до сотен гигабит и даже нескольких терабит в секунду.

Сближение глобальных и локальных сетей

В конце 80-х появились отличия между глобальными и локальными сетями. Это протяженность и качество линий связи, сложность методов передачи данных, скорость обмена данными, разнообразие услуг и масштабируемость.

Постепенно различия между локальными и глобальными типами сетевых технологий стали сглаживаться. Их тесная интеграция привела к значительному взаимопроникновению соответствующих технологий. Сближение в методах передачи данных происходит на платформе цифровой передачи данных по волоконно-оптическим линиям связи.

Высокое качество цифровых каналов привело к тому, что на первый план в глобальных сетях вместо процедур обеспечения надежности вышли процедуры обеспечения гарантированной средней скорости доставки данных. Большой вклад в сближение локальных и глобальных сетей внесло доминирование протокола IP.

Компьютерные глобальные сети существенно расширили набор своих услуг и догнали в этом отношении локальную сеть. В локальных сетях защите информации от несанкционированного доступа стало уделяться такое же большое значение как и в глобальных сетях.

Появляются новые технологии, изначально предназначенные как для локальных, так и для глобальных сетей. Например, технология ATM или Ethernet 10G.

Сближение компьютерных и телекоммуникационных (ТК) сетей

К ТК-сетям относятся компьютерные сети, телефонные сети, радио-сети и телевизионные сети. Во всех этих сетях в качестве ресурса предоставляемого клиентам выступает информация.

Сближение компьютерных и ТК-сетей происходит по многим направлениям. Прежде всего наблюдается сближение видов услуг предоставляемых клиентам.

Первая попытка создания универсальной т. н. мультисервисной сети, способной оказывать различные услуги, привела к появлению технологии цифровых сетей с интегральными услугами -- ISDN. В настоящее время на роль глобальной мультисервисной сети нового поколения претендует интернет. В конечном результате он должен с одинаковым успехом поддерживать услуги WWW, телефонии, архивов данных, видеоданных, аудио- и видео-новостей и мультимедийной почты.

Технологическое сближение сетей происходит на основе цифровой передачи информации различного типа, методов коммутации пакетов и программирования услуг. Дополнительные услуги телефонных сетей, такие как переадресация вызова, телеголосование могут создаваться с помощью интеллектуальной сети, которая по своей сути является компьютерной сетью с сервером, на котором программируется логика услуг.

Пакетные методы коммутации постепенно вытесняют традиционные для телефонных сетей методы коммутации каналов даже при передаче голосом. Использование коммутации пакетов для одновременной передачи разнородного трафика сделало актуальным разработку новых методов обеспечения требуемого качества обслуживания. Эти методы призваны минимизировать уровень задержек для чувствительного трафика и одновременно гарантировать среднюю скорость и динамичную передачу трафика данных.

Компьютерные сети используют транспортную инфраструктуру, созданную в рамках тех или иных ТК-сетей.

Особенности сетевых ОС

В вычислительных сетях связь между компьютерами осуществляется с помощью специальных периферийных устройств — сетевых адаптеров, которые соединяются каналами связи. Каждый компьютер работает под управлением собственной ОС. Взаимодействие между компьютерами сети происходит путем передачи сообщений через сетевые адаптеры и каналы связи. В качестве совместно используемых ресурсов выступают данные, хранящиеся на дисках, а также разнообразные периферийные устройства. Разделение локальных ресурсов компьютера между всеми пользователями сети — основная цель создания вычислительной сети. Для этого недостаточно снабдить компьютеры сетевыми адаптерами и соединить кабельной системой. Необходимы некоторые добавления к их ОС. На тех компьютерах, которые должны быть доступны всем пользователям сети, необходимо добавить некоторые модули, которые постоянно будут находиться в режиме ожидания запросов, поступающих по сети от других компьютеров. Такие модули называют программными серверами. Их главная задача обслуживать запросы на доступ к ресурсам своего компьютера. На компьютерах, пользователи которых хотят получить доступ к ресурсам других компьютеров, нужно добавить также специальные модули, которые должны вырабатывать запросы на доступ к

удаденным ресурсам и передавать их по сети на нужный компьютер. Такие модули называют программами-клиентами.
Пара модулей клиент-сервер обеспечивает совместный доступ пользователей к определенному типу ресурсов. Обычно сетевая ОС поддерживает несколько видов сетевых служб для своих пользователей. Это файловая служба, служба печати, служба электронной почты, служба удаленного доступа. Термины клиент и сервер используются и для обозначения соответствующих компьютеров в сети.

Распределенные программы.

Распределенная программа — программа, которая состоит из нескольких взаимодействующих частей. Причем каждая часть, как правило, выполняется на отдельном компьютере сети. Сетевые службы относятся к системным распределенным программам. Кроме того, в сети могут выполняться распределенные пользовательские программы(приложения). Распределенное приложение также состоит из нескольких частей. Каждая из этих частей выполняет какую-то определенную законченную работу по решению прикладной задачи. Распределенные приложения в полной мере используют потенциальные возможности распределённой обработки. И поэтому часто называются сетевыми приложениями. Не всякое приложение, выполняемое в сети, является сетевым. Существует большое количество приложений, которые не являются распределенными, и целиком выполняются на одном компьютере сети. Тем не менее, такие приложения могут использовать преимущества сети засчет встроенных в ОС сетевых служб. Создание распределенных приложений имеет много преимуществ, но является делом сложным. Нужно решить множество дополнительных проблем: на сколько частей разбить приложение, какие функции возложить на каждую часть, как организовать взаимодействие этих частей и тд. Поэтому до сих пор далеко не все приложения являются распределенными.

Простейшая логическая схема взаимодействия двух компьютеров

Здесь происходит взаимодействие двух программ, выполняемых на каждом из компьютеров. Программа, работающая на одном компьютере не может получить непосредственный доступ к ресурсам другого компьютера. Она может только «попросить» об этом другую программу, выполняемую на том компьютере, которому принадлежат эти ресурсы. Эти «просьбы» выражаются в виде сообщений, передаваемых по каналам связи между компьютерами. Сообщения могут содержать не только команды, но и данные. Рассмотрим случай, когда пользователю, который работает с текстовым редактором на компьютере А нужно прочитать часть некоторого файла, расположенного на диске компьютера В. Функции побайтовый передачи данных между компьютерами по линиям связи выполняют сетевые адаптеры и их драйверы. Приложение А формирует сообщение-запрос для приложения В. В запросе указывается имя файла, тип операции, смещение и размер области файла, содержащие нужные данные. Приложение В, получив сообщение, обращается к периферийному устройству, в данном случае к диску. Считанные с диска данные приложение В помещает в буферную область оперативной памяти и затем передает их по каналу связи в компьютер А, где они попадают в

приложение А. Описанные функции приложения А могла бы выполнять сама программа текстового редактора. Но включать все эти функции в состав каждого приложения, у пользователей которого может возникнуть потребность в доступе к удаленным файлам, не рационально. Выгоднее создать специальный программный модуль, который будет выполнять функции формирования сообщений-запросов к удаленной машине и приема результатов для всех приложений. Такой служебный модуль называют клиентом. На стороне компьютера В должна работать другая специализированная программа — сервер. Сервер постоянно ожидает поступление запросов на удаленный доступ к файлам. После получения такого запроса из сети сервер обращается к локальному файлу при помощи локальной ОС. Необходимой функцией клиента является способность отличить запрос к удаленному файлу от запроса к локальному. Иногда такие функции выделяют в отдельный программный модуль.

Задача физической передачи данных по линиям связи

При передачи данных по линиям связи используют кодирование данных. Кодирование осуществляется также как и в вычислительной технике. Могут использовать либо потенциальный способ, либо импульсный. Кроме того, существует особый способ — модуляция. При модуляции дискретная информация представляется синусоидальным сигналом той частоты, которую хорошо передает имеющаяся линия связи.
Потенциальное или импульсное кодирование применяется на каналах высокого качества. А модуляция на всех остальных.
В сетевых линиях связи используется последовательная побитная передача данных, которая требует всего одной пары проводов. Еще одна проблема — взаимная синхронизация передатчика одного компьютера с приемником другого. Эта проблема решается двумя способами:

- Путем обмена специальными тактовыми синхроимпульсами по отдельной линии.
- Путем периодической синхронизации импульсами формы, отличной от формы импульсов данных.

Несмотря на эти меры, существует вероятность искажения мета-данных. Для повышения надежности передачи данных используют стационарный приемник. Подсчет контрольной суммы и передача ее после каждого байта или блока байтов.
Кроме того, в протокол обмена данными может включаться сигнал-квитанция, который подтверждает правильность приема данных и посылается от получателя отправителю.
Для обмена данными с внешними устройствами в компьютере предусмотрены интерфейсы или порты, те наборы проводов, соединяющих компьютер с устройствами, а также наборы правил обмена информацией по этим проводам. Логикой передачи сигналов на внешний интерфейс управляют аппаратное устройство компьютера (контроллер) и программный модуль (драйвер).

Топология физических связей

Как только компьютеров становится больше двух, появляется проблема выбора конфигурации физических связей или топологии. Под топологией сети понимается конфигурация графа, вершинам которого соответствует конечные узлы сети, например,

компьютеры, и коммуникационное оборудование, например, маршрутизаторы, а ребрам соответствуют электрические и информационные связи между ними. При увеличении числа связываемых устройств резко возрастает число возможных вариантов конфигураций. Среди множества конфигураций различают: полносвязные и неполносвязные. Полносвязная топология соответствует сети, в которой каждый компьютер непосредственно связан со всеми остальными. Несмотря на логическую простоту этот вариант является громоздким и неэффективным. Все другие варианты основаны на неполносвязных топологиях. В этом случае для обмена данными между двумя узлами может потребоваться промежуточная передача данных через другие узлы сети.
Ячеистая топология получается из полносвязной путем удаления некоторых возможных связей. ЯТ допускает соединение большого количества компьютеров и характерна для крупных сетей. В сетях с кольцевой топологией данные передаются по кольцу от одного компьютера к другому. Данные, сделав полный круг, возвращаются к узлу-источнику. Поэтому отправитель может контролировать процесс доставки данных адресату. Но при такой топологии необходимо предпринимать меры, чтобы в случае выхода из строя или отключения какой-либо станции не прерывался канал связи между остальными станциям кольца.
Топология звезда. Образуется в случае, когда каждый компьютер подключается отдельным кабелем у общему центральному устройству — концентратору. Концентратором может быть компьютер, либо коммутатор, маршрутизатор, повторитель. При выходе из строя центрального устройства сеть перестает работать. Возможность по наращиванию количества узлов в сети ограничено числом портов концентратора. Иногда строят сеть из нескольких концентраторов, соединенных связями типа звезда. Получаемую структуру называют деревом. Особым случаем звезды является конфигурация общая шина. Здесь в качестве центрального элемента выступает общая шина. К этому кабелю подключаются несколько компьютеров. Передаваемая информация распространяются по кабелю и доступна сразу всем узлам, присоединенным к кабелю. Достоинства заключаются в низкой стоимости, и простоте присоединения новых узлов к сети. Недостаток — низкая надежность. Любой дефект кабеля или какого-то из многочисленных разъемов полностью парализует всю сеть. Второй недостаток — пропускная способность канала всегда делится между всеми узлами сети. Для крупных сетей характерно наличие произвольных связей между компьютерами. В таких сетях можно выделить отдельные произвольно связанные фрагменты, имеющие типовую топологию. Поэтому большая сеть получила название сетью со смешанной топологией.

Адресация узлов сети

При объединении трех и более компьютеров возникает проблема их адресации. Один компьютер может иметь несколько сетевых интерфейсов. Адреса могут быть числовыми и символьными. Для числовой записи используется десятично-точечная нотация. 128.48.45.1. Этот же адрес может быть записан в 16й форме, либо в двоичной. У каждого сетевого интерфейса есть и числовой, и символьный адресат. В больших сетях применяется иерархическая схема адресации. Эта схема позволяет до определенного

момента пользоваться только старшей составляющей адреса. Затем для дальнейшей локализации адресата используют следующую по старшинству часть и тд, и в конечном счете пользуются младшей частью.
Вторая схема адресации — плоская схема или линейная. В этом случае множество адресов никак не структурированы.

К адресу сетевого интерфейса и схеме его назначения предъявляют следующие требования:
1. Адрес должен уникально идентифицировать сетевой интерфейс в сети любого масштаба
2. Схема назначения адресов должна сводить к минимуму ручной труд администратора и вероятность дублирования адресов
3. Желательно чтобы адрес имел иерархическую структуру
4. Адрес должен быть удобен для пользователей сети, поэтому он должен допускать символьное представление
5. Адрес должен быть компактным, чтобы не перегружать память коммуникационной аппаратуры.
Эти требования достаточно противоречивы. Например, адрес, имеющий иерархическую структуру будет менее компактным, чем плоский адрес. Все перечисленные требования трудно совместить в рамках одной схемы адресации, поэтому на практике используют сразу несколько схем и сетевой интерфейс компьютера одновременно может иметь несколько имен. Каждый адрес задействуется в той ситуации, когда это наиболее удобно. Для преобразования адресов из одного вида в другой используются специальные протоколы — протоколы разрешения адресов. Примером плоского числового адреса является MAC-адрес. Он предназначен для однозначной идентификации сетевых интерфейсов в локальных сетях. MAC-адрес обычно назначается компанией изготовителем. Второе название — аппаратный адрес.
К иерархическим адресам относятся: ip и ipx адреса. Здесь поддерживается двухуровневая иерархия. Адрес делится на старшую часть — номер сети, и младшую — номер узла сети. Такое деление позволяет передавать сообщения между сетями только на основании номера сети. Номер узла используется после доставки сообщения в нужную сеть. Символьные адреса предназначены для запоминания людьми и поэтому обычно несут смысловую нагрузку. В крупных сетях символьное имя может иметь иерархическую структуру. В современных сетях для адресации узлов как правило применяют одновременно все три эти схемы. Пользователи адресует компьютеры символьными именами, которые автоматически заменяются при передаче по сети числовыми именами, далее с помощью этих числовых номеров сообщения передаются из одной сети в другую и после доставки сообщения в нужную сеть вместо числового номера используется аппаратный адрес компьютера. Сегодня такая схема характерна даже для небольших автономных сетей. Проблема установления соответствия между адресами различных типов, которыми занимаются протоколы разрешения адресов, может решаться как централизованными, так и распределенными средствами. В случае централизованного подхода в сети выделяются один или несколько компьютеров, серверов, имен, в которых

хранится таблица соответствия друг другу имен различных типов. Все остальные компьютеры обращаются к серверу имен, чтобы по символьному имени найти числовой номер компьютера, и затем обменяться с ним данными. При распределённом подходе каждый компьютер сам решает эту задачу путем рассылки всем компьютерам сети широковещательных сообщений, и дальнейшего опознавания своего числового имени одним из компьютеров.
Распределённый подход хорош тем, что не предполагает выделение специального компьютера. Недостатком является необходимость рассылки широковещательных сообщений. Такие сообщения перегружают сеть, тк требуют обязательной обработки всеми узлами. Поэтому распределённый подход используется в небольших локальных сетях.
В крупных сетях распространение широковещательных сообщений по всем сегментам сети практически нереально. Поэтому применяют централизованный подход. Наиболее известной службой централизованного разрешения адресов является система доменных имен. В адресе назначения наряду с информацией, идентифицирующей порт устройства, должен указываться адрес процесса, которому предназначены данные. После того, как эти данные достигнут указанного сетевого интерфейса, программное обеспечение компьютера должно их направить соответствующему процессу. Адрес процесса должен быть уникальным в пределах компьютера.

Коммутация и мультиплексирование

Обобщенная задача коммутации

Если топология сети неполносвязная, то обмен данными между произвольной парой узлов в общем случае должен идти через транзитные узлы. Последовательность транзитных узлов на пути от отправителя к получателю называется маршрутом. В самом общем виде задача соединения конечных узлов через сеть транзитных узлов называется задачей коммутации. Она может быть представлена в виде нескольких взаимосвязанных частных задач.
1. Определение информационных потоков, для которых требуется прокладывать маршрут.
2. Определение маршрутов для потоков.
3. Сообщение о найденных маршрутах узлам сети.
4. Продвижение потоков, те распознавание потоков и их локальная коммутация.
5. Мультиплексирование и демультиплексирование потоков.

Определение информационных потоков

Через один транзитный узел может проходить несколько маршрутов. Транзитный узел должен уметь распознавать потоки данных, которые на него поступают. Для того, чтобы передавать их именно на тот свой интерфейс, который ведет к нужному узлу.
Информационным потоком или потоком данных называют непрерывную последовательность байтов, объединенных набором общих признаков, выделяющих его из общего сетевого трафика. Все данные, поступающие от одного компьютера можно определить как единый поток, а можно представить в виде нескольких подпотоков,

каждый из которых имеет адрес назначения. Каждый из этих подпотоков можно разделить на потоки данных, относящихся к разным сетевым приложениям. В качестве обязательного признака при коммутации выступает адрес назначения данных. Поэтому весь поток входящих в транзитный узел данных должен разделяться на подпотоки, имеющие различные адреса назначения. Те каждой паре конечных узлов будет соответствовать один поток и один маршрут. Однако поток данных между двумя конечными узлами в общем случае может быть представлен несколькими разными потоками, причем для каждого из них может быть проложен свой особый маршрут. В таком случае выбор маршрута должен осуществляться с учетом характера передаваемых данных. Для файлового сервера важно, чтобы его данные направлялись по каналам, обладающим высокой пропускной способностью. Для прогаммной системы управления, которая посылает в сеть короткие сообщения, требующие немедленной и обязательной обработки, при выборе маршрута более важна надежность линии связи и минимальный уровень задержек на маршруте. Кроме того одновременно могут прокладываться несколько маршрутов, чтобы засчет распараллеливания добиться одновременного использования различных каналов и тем самым ускорить передачу данных. Признаки потока могут иметь глобальное или локальное значение. В первом случае они однозначно определяют поток в пределах всей сети, а во втором в пределах одного транзитного узла. Кроме того существует особый тип признака — метка потока. Метка может иметь глобальное значение, также могут использоваться локальные метки потока, динамически меняющие свое значение. Т.о. при распознавании потоков должны учитываться не только адреса назначения данных, но и другие признаки, влияющие на маршрут.

Определение маршрутов

Выбрать маршрут передачи данных значит определить последовательность транзитных узлов и их интерфейсов, через которые нужно передавать данные, чтобы доставить их адресату. Задача определения маршрутов состоит в выборе из множества альтернативных путей одного или нескольких. Чаще всего этот выбор останавливают на одном оптимальном по некоторому критерию маршруте. Критериями оптимальности могут быть:

1. Номинальная пропускная способность
2. Загруженность каналов связи
3. Задержки, вносимые каналом
4. Количество промежуточных транзитных узлов
5. Надежность каналов и транзитных узлов

Маршрут может определяться вручную администратором сети, который, основываясь на личном опыте, анализирует топологию сети и определяет последовательность интерфейсов, которую должны пройти данные. Для больших сетей со сложной топологией эта задача решается автоматически. Для этого конечные узлы и другие устройства сети оснащают специальными программными средствами, которые организуют взаимный обмен служебными сообщениями, позволяющий каждому узлу составить свое представление по топологии сети. Затем на основе этого исследования и математических алгоритмов определяют рациональные маршруты.

Оповещение сети о выбранном маршруте

После того, как маршрут определен, нужно сообщить о нем всем устройствам сети. Сообщение о маршруте обрабатывается устройством и в результате создается новая запись в таблице коммутации. В этой таблице локальному или глобальному признакам потока ставится в соответствие номер интерфейса, на который устройство должно передавать данные, относящиеся к этому потоку. Передача информации о выбранных маршрутах может осуществляться и вручную, и автоматически. Администратор сети может зафиксировать маршрут, выполнив в ручном режиме конфигурирование устройства. Также он может по собственной инициативе внести запись о маршруте в таблицу коммутации. Однако, поскольку топология сети и информационных потоков могут меняться, то решение задач определения и задания маршрутов предполагает постоянный анализ состояния сети и обновления маршрутов. Это целесообразно реализовывать автоматически.

Продвижение потоков

Когда задачи определения и задания маршрута решены, должно произойти соединение абонентов. Для каждой пары абонентов эта операция может быть представлена совокупностью нескольких локальных операций коммутации. Отправитель должен выставить данные на тот свой порт, из которого выходит найденный маршрут, а все транзитные узлы должны соответствующим образом выполнить переброску данных с одного своего порта на другой, то есть выполнить коммутацию. Устройство, функциональным назначением которого является выполнение коммутации, называется коммутатором. Коммутатор производит коммутацию входящих в его порты информационных потоков, направляя их в соответствующие выходные порты. Однако, прежде чем выполнить коммутацию, коммутатор должен опознать поток. Для этого поступившие данные анализируются на предмет наличия в них признаков какого-либо из потоков, заданных в таблице коммутации. Если произошло совпадение, то эти данные направляются на интерфейс, который был определен для них в маршруте. Коммутатором может быть либо специализированное устройство, либо компьютер со встроенным программным механизмом коммутации. Компьютер может совмещать функции коммутации со своими обычными задачами. Но более целесообразным является выделение в сети некоторых узлов специально для выполнения коммутации. Эти узлы образуют коммутационную сеть, к которой подключаются все остальные.

Мультиплексирование и демультиплексирование

Обычно операцию коммутации сопровождает обратная операция МС. При этой операции из нескольких отдельных потоков данных образуется общий агрегированный поток, который можно передавать по одному физическому каналу связи.
Агрегирование это объединение нескольких элементов в единое целое. МС является способом обеспечения доступности имеющихся физических каналов одновременно для нескольких сеансов связи между абонентами сети. Прежде чем выполнить переброску данных на определенные для них интерфейсы коммутатор должен понять к какому потоку

они относятся. Эта задача должна решаться независимо от того, поступает ли на вход коммутатора только один поток в чистом виде или агрегированный поток. В случае агрегированного потока к задаче распознавания добавляется задача ДМС, то есть разделение суммарного агрегированного потока на несколько составляющих потоков. Операции МС и ДМС имеют такое же важное значение, как и операции коммутации, потому что без них пришлось бы все коммутаторы связывать большим количеством параллельных каналов, что свело бы на нет все преимущества неполносвязной сети. Существует множество способов МС потоков в одном физическом канале. Важнейшим из них является разделение времени. При этом способе каждый поток время от времени получает в свое распоряжение физический канал и передает в это время по нему свои данные. Также очень распространено частотное разделение каналов. Каждый поток передает данные в выделенном ему частотном диапазоне. Технология МС должна позволять получателю такого суммарного потока выполнять обратную операцию: разделение данных на составные потоки. В общем случае на каждом интерфейсе могут одновременно выполняться обе задачи: МС и ДМС.

1) Переменная величина задержки пакетов данных, которые могут достигать больших величин в моменты мгновенных перегрузок сети
2) Возможны потери данных из-за переполнения буфера

В настоящее время активно развиваются методы возможные победить указанные недостатки. Эти методы называются методами обеспечения качества обслуживания. Сети с коммутацией пакетов в которых реализованы эти методы позволяют одновременно передавать различные виды трафика.

Коммутация сообщений

По своим принципам близка к коммутации пакетов. Под коммутацией сообщений понимается передача единого блока данных между транзитными компьютерами сети с временной буферизацией этого блока на диске этого компьютера. Сообщение в отличии от пакета имеет произвольную длину, которая определяется не технологическими соображениями, а содержанием сообщения.

Транзитные компьютеры могут соединяться между собой как сетью с коммутацией каналов, так и пакетов. Передача с промежуточным хранением на диске используется для передачи сообщений не требующих немедленного ответа. Режим коммутации сообщений разгружает сеть для передачи трафика требующего быстрого ответа. Количество транзитных компьютеров по возможности стараются уменьшить. Если компьютеры подключены к сети с коммутацией пакетов, то число промежуточных компьютеров обычно два.

В настоящее время коммутация сообщений работает только для некоторых неоперативных служб, причем чаще всего с … коммутацией пакетов как служба прикладного уровня.

Постоянная и динамическая коммутация

В случае с динамической коммутацией сеть разрешает устанавливать соединение по инициативе пользователя сети. Коммутация выполняется на время сеанса связи, а затем опять же по инициативе одного из пользователей связь разрывается.

В случае постоянной коммутации сеть не предоставляет пользователю возможность выполнить динамическую коммутацию с другим произвольным пользователем сети. Вместо этого сеть разрешает паре пользователей заказать соединение на длительный период времени. Соединение устанавливается не пользователями, а персоналом обслуживающим сеть. Время, на которое устанавливается постоянная коммутация обычно составляет несколько месяцев. Режим постоянной коммутации в сетях с коммутацией каналов называется сервисом выделенных или арендуемых каналов. В том случае, когда постоянное соединение через сеть коммутаторов устанавливается с помощью автоматических процедур, его часто называют полупостоянным соединением.

Наиболее популярными сетями поддерживающими режим динамической коммутации являются телефонные сети, локальные сети, сети TCP/IP. К сетям работающим в режиме постоянной коммутации относятся сети технологии SDH. На основе этих сетей строятся выделенные каналы связи пропускной способностью несколько Гбит/с. Некоторые типы сетей поддерживают оба режима работы, например сеть X.25 или ITM могут предоставлять пользователю возможность динамически связаться с любым другим пользователем сети и в тоже время отправлять данные по постоянному соединению одному определенному абоненту.

31.03.2015

Многослойная модель сети

Весь комплекс программно-аппаратных средств сети может быть описан многослойной моделью. В основе любой сети лежит аппаратный слой стандартизированных компьютерных платформ. В настоящее время в сетях применяются компьютеры различных классов: от обычных ПК до супер ЭВМ. Набор компьютеров в сети должен соответствовать набору разнообразных задач, решаемых сетью.
Второй слой: коммуникационное оборудование. К нему относятся кабельные системы, повторители, мосты, коммутаторы, маршрутизаторы, модульные концентраторы. По стоимости оборудование может быть сопоставимо с компьютерами. Коммуникационное устройство может представлять собой сложный специализированный мультипроцессор, который нужно конфигурировать, оптимизировать и адмиристрировать. Третьим слоем являются операционные системы.
В зависимости от того, какие концепции положены в основу сетевой ОС зависит эффективность работы всей сети. При проектировании сети важно учитывать насколько просто данная ОС может взаимодействовать с другими ОС сети, насколько она

обеспечивает безопасность, как она позволяет наращивать число пользователей, можно ли перенести её на компьютер другого типа.
Самым верхним слоем являются различные сетевые приложения: сетевые бд, почтовые системы, средства архивирования данных, системы автоматизации коллективной работы. Очень важно представлять диапазон возможностей приложений, а также знать насколько они совместимы с другими сетевыми приложениями и ОС.

Сетевые службы и ОС

Для конечного пользователя сеть это тот набор сетевых служб, с помощью которых он получает возможность просмотреть список имеющихся в сети компьютеров, прочитать удаленный файл, распечатать документ на чужом принтере, или отправить почтовое сообщение. Именно совокупность предоставляемых возможностей определяет для пользователя облик той или иной сети. Кроме обмена данными сетевые службы должны решать другие более специфические задачи. Например задач, порождаемые распределённой обработки данных. К таким задачам относятся: обеспечение непротиворечивости нескольких копий данных, размещенных на разных машинах. Этим занимается служба репликации. Или организация выполнения одной задачи параллельно на нескольких машинах сети — служба вызова удаленных процедур. Среди сетевых служб можно выделить административную службу, те это службы, которые ориентированы не на простого пользователя, а на администратора. И они служат для организации правильной работы сети в целом.
К административным службам относятся:
1. Служба администрирования учетных записей пользователя — эта служба позволяет администратору вести общую базу данных о пользователях сети
2. Служба мониторинга сети — позволяет захватывать и анализировать сетевой трафик
3. Служба безопасности — реализация сетевых служб осуществляется программными средствами
Основные службы обычно предоставляются операционной системой, а вспомогательные — системными сетевыми приложениями.
При разработке сетевых служб приходится решать следующие проблемы:
1. Определение протокола взаимодействия между клиентской и серверной частями
2. Распределение между ними функций
3. Определение схемы адресации приложения
Одним из главных показателей качества сетевой службы является её удобство. Для одного и того де ресурса может быть разработано несколько служб, по-разному решающих одну и ту же задачу. Отличия могут заключаться в производительности или уровнем удобства предоставляемых услуг. Качество сетевой службы зависит и от качества пользовательского интерфейса. При определении степени удобства разделяемого ресурсом часто определяют термин прозрачность. Прозрачный доступ — такой доступ, при котором пользователь не знает где расположен нужный ему ресурс на собственном или удаленном компьютере. После того, как он смонтирует удаленную файловую систему в свое дерево каталогов, доступ к удаленным файлам становится для него совершенно прозрачным. Сама операция монтирования может иметь разную

степень прозрачности. Для обеспечения прозрачности важен способ адресации разделяемых сетевых ресурсов. Имена этих ресурсов не должны зависеть от их физического расположения на том или ином компьютере. В идеале пользователь ничего не должен менять в своей работе. В случае если администратор переместил каталог с одного компьютера на другой, сам администратор и сетевая ОС имеют информацию о расположении файловых систем, но от пользователя она скрыта. Такая степень прозрачности пока редко встречается в сетях. Обычно для получения доступа к ресурсам определенного компьютера сначала приходится устанавливать с ним логическое соединение.

Общая структура телекоммуникационной сети

В общем случае телекоммуникационная сеть состоит из:

1. Сети доступа
2. Магистральная сеть
3. Информационные центры

Сеть доступа и магистральная сеть строятся на основе коммутаторов. Каждый коммутатор оснащен некоторым количеством портов, которые соединяются с портами других коммутаторов каналами связи. Сеть доступа составляет нижний уровень иерархии телекоммуникационной сети. К этой сети подключаются конечные терминальные узлы. То есть оборудование, установленное у пользователей. Основное назначение сети доступа состоит в концентрации информационных потоков, которые поступают по многочисленным каналам связи от оборудования пользователей в сравнительно небольшом количестве узлов магистральной сети. Сеть доступа может состоять из нескольких уровней. Коммутаторы установленные в узлах нижнего уровня мультиплексируют информацию, поступающую по многочисленным абонентским каналам и передают её коммутаторам верхнего уровня, чтобы те в свою очередь передали её коммутаторам магистрали. Количество уровней сети доступа зависит от её размера. Небольшая сеть доступа может состоять из одного уровня, а крупная из двух-трех. Следующие уровни осуществляют дальнейшую концентрацию трафика, собирая его и мультиплексируя более скоростные каналы. Магистральная сеть объединяет отдельные сети доступа, выполняя функцию транзита траффика между ними по высокоскоростным каналам. Коммутаторы магистрали могут оперировать не только с информационными соединениями между отдельными пользователями, но и с аггрегированными информационными потоками. В результате информация с помощью магистрали попадает в сеть доступа получателей, демультиплексируется там и коммутирутся таким образом, что на входной порт оборудование пользователя поступает только та информация, которая ему адресована.

В том случае, когда абонент получатель подключен к тому же коммутатору доступа, что и абонент отправитель, отправитель самостоятельно выполняет необходимую операцию коммутации.

Информационные центры или центры управления сервисом — это собственные информационные ресурсы сети, на основе которых осуществляется обслуживание пользователей. В таких центрах может храниться информация двух типов:

1. Пользовательские информация, те та, которая непосредственно интересует конечных пользователей сети
2. Вспомогательная служебная информация — помогает предоставлять некоторые услуги пользователю.
К первому типу можно отнести веб-порталы, на которых расположено разнообразная справочная и новостная информация. Ресурсами второго типа являются: различные системы аутентификации и авторизации пользователей; системы биллинга, которые подсчитывают плату за полученные услуги; бд учетной информации; централизованные системы управления сетью.
У сетей каждого конкретного типа имеется много особенностей. Тем не менее их структура в целом соответствует описанной выше. В то же время в зависимости от назначения и размера сети в ней могут отсутствовать некоторые составляющие. В небольшой локальной сети нет ярко выраженных сетей доступа и магистралей. Они сливаются в общую структуру. В корпоративной сети как правило отсутствуют системы биллинга. Могут отсутствовать информационные центры.

Требования к компьютерным сетям

Главным требованием, предъявляемым к сетям, является выполнение сетью того набора услуг, для указания которых она предназначена. Все остальные требования: производительность, надежность, совместимость, управляемость, защищенность, расширяемость и масштабируемость связаны с качеством выполнения основной задачи. Две самые важные характеристики сети: производительность и надежность.

Производительность

Производительность — это характеристика сети, позволяющая оценить несколько быстро информация дойдёт от передающей станции до принимающей. На производительность влияют следующие характеристики:

1. Конфигурация сети
2. Скорость передачи данных
3. Метод доступа к каналу
4. Топология сети
5. Технология

Если производительность сети перестаёт отвечать предъявляемым к ней требованиям, то единства сети может сделать следующее:

1. Изменить конфигурацию сети таким образом, чтобы структура сети более соответствовала структуре информационных потоков.
2. Перейти к другой модели построения распределённых приложений, которая позволила бы уменьшить сетевой трафик.
3. Заменить мосты более скоростными коммутаторами.
4. Перейти на более скоростную технологию.

С ростом масштаба сетей возникла необходимость в повышении их производительности. Одним из способов достижения этого стала микросегментация. Она позволяет уменьшить число пользователей на один сегмент и снизить объем широковещательного трафика, что значительно повышает производительность сети.

Первоначально для микросегментации использовались маршрутизаторы, но оказалось, что они не очень приспособлены для этих целей. Решения на их основе были достаточно дорогостоящими, отличались большой временной задержкой и невысокой пропускной способностью. Более подходящими устройствами стали коммутаторы. Они имеют достаточно низкую стоимость, высокую производительность и просты в использовании. Таким образом сети стали строить на базе коммутаторов и маршрутизаторов.

Коммутаторы обеспечивают высокоскоростную пересылку трафика между сегментами, входящими в одну подсеть.

Маршрутизаторы передают данные между подсетями, ограничивают распространение трафика, решают вопросы безопасности. Потенциально высокая производительность — это одно из преимуществ распределённых систем. Это свойство обеспечивается принципиальной, но не всегда реализуемой возможностью распараллеливания работ между несколькими компьютерами. Существует несколько характеристик производительности сети:

1. Время реакции
2. Скорость передачи данных
3. Задержка передачи и вариация задержки передачи

Время реакции определяется как интервал времени между возникновением запроса пользователя к какой-либо сетевой службе и получением ответа на этот запрос. Значение этого показателя зависит от типа этой службы и от того, какой пользователь к какому серверу обращается. От загруженности элемента сети. Также используют средневзвешенную оценку времени реакции сети. Время реакции сети обычно складывается из нескольких составляющих. Обычно в него входит:

- Время подготовки запроса на клиентском компьютере.
- Время передачи запроса между клиентом и сервером.
- Время обработки запросов на сервере.
- Время передачи ответов от сервера клиенту.
- Время обработки полученных от сервера ответов на клиентском компьютере.

Значение сетевых составляющих времени реакции даёт возможность оценить производительность отдельных элементов сети, выявить узкие места и в случае необходимости выполнить модернизацию сети.

Свелось передачи данных отражает объем данных переданных сетью или её частью за единицу времени.

Пропускная способность говорит о скорости выполнения внутренних операций сети -- передачи пакетов данных через различные коммуникационные устройства. Она непосредственно характеризует качество выполнения основной функции сети -- транспортировки сообщений.

Скорость передачи данных изменяется либо в битах в секунду, либо в пакетах в секунду.

Пропускная способность может быть мгновенной, максимальной и средней. При проектировании, настройке и оптимизации сети используются средняя и максимальная пропускные способности. Средняя позволяет оценить работу на большом промежутке времени, на котором пики и спады трафика компенсируют друг друга. Пропускная способность позволяет оценить возможность сети справляться с пиковыми нагрузками. Пропускную способность можно измерять между любыми двумя узлами сети. Для анализа и настройки сети полезно знать информацию о пропускной способности.

Задержки передачи данных определяется как задержка между моментом получения данных на вход устройства и моментом появления их на выходе. Этот параметр характеризует только сетевые этапы обработки данных. Обычно качество сети характеризуют величинами максимальной задержки передачи и вариации задержки.

Пропускная способность и задержки передачи не зависят друг от друга. Сеть может обладать высокой пропускной способностью, но нести значительные задержки при передаче каждого пакета.

Надёжность и безопасность

Различают несколько аспектов надёжности. Для технических устройств используют такие показатели надёжности, как: среднее время наработки на отказ, вероятность отказа, интенсивность отказов. Этим показатели пригодны для оценки простых элементов, которые могут находиться только в двух состояниях: работает или нет. Сложные кроме этих двух имеют промежуточные, поэтому для оценки сложных систем применяется другой набор характеристик.

Готовность -- означает долю времени, в течение которого система может быть использована. Может быть улучшена путём ведения избыточности в структуру системы.

Ключевые элементы системы должны существовать в нескольких экземплярах, чтобы при отказе одного из них функционирование системы обеспечивали другие. Чтобы компьютерную систему можно было отнести к высоконадёжным, она помимо высокой готовности должна обеспечивать сохранность данных и их защиту от искажений. Кроме того, должна поддерживаться непротиворечивость данных.

Безопасность — это способность системы защитить данные от несанкционированного доступа. В распределённых системах это сделать гораздо сложнее, чем в централизованных. В сетях сообщения передаются по линиям связи часто подходящим через общедоступные помещения, в которых могут быть установлены прослушивающие устройства. Другим уязвимым местом могут быть оставленные без присмотра компьютеры. Кроме того, всегда существует потенциальная угроза взлома защиты сети от несанкционированных пользователей. Особенно если имеется выход в глобальные сети общего пользования.

Под отказоустойчивостью понимается способность системы скрывать от пользователя отказ отдельных её элементов. В отказоустойчивой системе отказ одного из её элементов приводит к некоторому снижению качества её работы, но не к полному отказу.

Расширяемость и масштабируемость

Расширяемость означает возможность сравнительно лёгкого добавления отдельных элементов сети, наращивания длины сегмента сети и замены существующей аппаратуры на более мощную. При этом принципиально важно, что лёгкость расширения системы иногда может обеспечиваться в весьма ограниченных пределах. Масштабируемость означает, что сеть позволяет наращивать количество узлов и протяжённость связей в очень широких пределах. При этом производительность сети не ухудшается. Для обеспечения масштабируемости сети применяют дополнительное коммуникационное оборудование и специальным образом структурируют сеть. Хорошей масштабируемостью обладает многосегментная сеть, построенная с помощью коммутаторов и маршрутизаторов и имеющую иерархическую структуру связей. Такая сеть может содержать несколько тысяч компьютеров и при этом обеспечивать каждому пользователю нужное качество обслуживания.

Прозрачность

Прозрачность сети достигается в том случае, когда сеть представляется пользователям, не как множество отдельных компьютеров, связанных кабелем, а как единая традиционная вычислительная машина с системой распределения времени. Прозрачность может быть достигнута на двух различных уровнях: на уровне пользователя и на уровне программиста.

На уровне пользователя прозрачность означает, что для ...ой, всё!.. он использует тот же набор команд и процедур, что и для работы с локальными.

На программном уровне прозрачность заключается в том, что приложениям для доступа к удалённым ресурсам требуются те же вызовы, что и для доступа к локальным.

Прозрачность расположения означает, что от пользователя не требуется знаний по месте расположения программных и аппаратных ресурсов.

Прозрачность перемещения означает, что ресурсы должны свободно перемещаться из одного компьютера в другой без изменения своих имён.

Прозрачность параллелизма заключается в том, что процесс распараллеливания вычислений происходит автоматически, без участия программиста. При том программа сама.. Блять, проебал..

Поддержка различных видов трафика

****

21.04

Открытые системы и модель OSI

Многоуровневый подход, декомпозиция задачи сетевого взаимодействия

Организация взаимодействия между устройствами сети является сложной задачей. Для решения сложных задач используют универсальный прием — декомпозицию. Т.е. разбиение одной сложной задачи на несколько более простых задач-модулей. Декомпозиция состоит в четком определении функции каждого модуля, а также порядка их взаимодействия. В результате достигается логическое упрощение задачи, и появляется возможность модификации отдельных модулей без изменения остальных частей системы. При декомпозиции часто используют многоуровневый подход. Все множество модулей, решающих частные задачи, разбивают на группы и сортируют по уровням, образующим иерархию. В соответствии с принципом иерархии для каждого промежуточного уровня можно указать непосредственно примыкающие к нему соседние вышележащие и нижележащие уровни. Группа модулей, составляющих каждый уровень, должна быть сформирована таким образом, чтобы все модули этой группы для выполнения своих задач обращались с запросами только к модулям соседнего нижележащего уровня. С другой стороны, результаты работы всех модулей, отнесенных к некоторому уровню, могут быть переданы только модулям соседнего вышележащего уровня. Такая иерархическая декомпозиция предполагает четкое определение функций каждого уровня и взаимодействие между ними. Интерфейс определяет набор функций, в которых нижележащий уровень предоставляет вышележащий. В результате

иерархической декомпозиции достигается относительная независимость уровней и появляется возможность их автономной разработки и модификации.
Средства решения задачи организации сетевого взаимодействия также представляются в виде иерархически организованного множества модулей. Решение задачи порученное вышележащему уровню может быть получено путем многократных обращений нижележащему уровню.

Протокол, интерфейс, стек протоколов

Многоуровневое представление средств сетевого взаимодействия имеет свою специфику, связанную с тем, что в процессе обмена сообщениями участвуют две стороны, то есть в данном случае необходимо организовать согласованную работу двух иерархий, работающих на разных компьютерах. Оба участника сетевого обмена должны принять множество соглашений. Они должны согласовать уровни и форму электрических сигналов, способ определения размера сообщений, договориться о методах контроля достоверности и тд.
Соглашения должны быть приняты для всех уровней начиная от самого низкого уровня передачи битов и до самого высокого, который реализует сервис для пользователей сети. Протокол определяет правила взаимодействия модулей одного уровня в разных узлах, а интерфейс определяет правила взаимодействия модулей соседних уровней в одном узле. Средства каждого уровня должны отрабатывать, во-первых, свой собственный протокол, а во-вторых, интерфейсы с соседними уровнями. Иерархически организованный набор протоколов, достаточный для организации взаимодействия узлов в сети называется стеком коммуникационных протоколов. Коммуникационные протоколы могут быть реализованы как программно, так и аппаратно. Протоколы нижних уровней часто реализуются комбинацией программных и аппаратных средств, а протоколы верхних уровней, как правило, чисто программными средствами. Программный модуль, реализующий некоторый протокол, также называют протоколом.

Общая характеристика модели OSI

В начале 80х годов была разработана модель, которая сыграла значительную роль в развитии сетей. Эта модель называется моделью взаимодействия открытых систем. Она определяет различные уровни взаимодействия систем в сетях с коммутацией пакетов, дает им стандартные имена и указывает какие функции должен выполнять каждый уровень. В Модели взаимодействия существует 7 уровней(сверху вниз):
Прикладной
Представительный
Сеансовый
Транспортный
Сетевой
Канальный
Физический
Каждый уровень имеет дело с одним определенным аспектом взаимодействия сетевых устройств.

Пусть приложение обращается с запросом к прикладному уровню, например, к файловой службе. На основании этого запроса программное обеспечение прикладного уровня формирует сообщение стандартного формата, которое состоит из заголовка и поля данных. Заголовок содержит служебную информацию, которую необходимо передать через сеть прикладному уровню машины адресата, чтобы сообщить ему какую работу нужно выполнить. В нашем случае заголовок должен содержать информацию о местонахождения файла и о типе операции, которую необходимо над ним выполнить. Поле данных сообщения может быть пустым или содержать какие-либо данные, которые, например, нужно записать в файл. После формирования сообщений 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 добавляет свой заголовок и тд. Наконец сообщение достигает нижнего физического уровня, который и передает сообщение по линиям связи. К этому моменту сообщение обрастает заголовками всех уровней. Когда сообщение по сети поступает на машину-адресат, оно принимается её физическим уровнем и последовательно перемещается вверх с уровня на уровень. Каждый уровень анализирует и обрабатывает заголовок своего уровня. Выполняет соответствующие функции, удаляет этот заголовок, и передает сообщение вышележащему уровню.

Физический уровень

Этот уровень имеет дело с передачей битов по физическим каналам связи. К этому уровню имеют отношение характеристики физических средств передачи данных: полоса пропускания, волновое сопротивление. На этом уровне определяются характеристики электрических сигналов, уровень напряжения сигнала, тип кодирования. Кроме того, здесь стандартизируются типы разъемов и назначение каждого контакта. Функции физического уровня реализуются во всех устройствах, подключенных к сети. Со стороны компьютера функции физического уровня выполняются сетевым адаптером или последовательным портом.

Канальный уровень

На физическом уровне просто пересылаются биты. При этом не учитывается, что в некоторых сетях, в которых линии связи используются (разделяются) попеременно несколькими парами взаимодействующих компьютеров, физическая среда передачи может быть занята. Поэтому одной из задач канального уровня (Data Link Layer) является проверка доступности среды передачи. Другой задачей канального уровня является реализация механизмов обнаружения и коррекции ошибок. Для этого на канальном уровне биты группируются в наборы, называемые кадрами (frames). Канальный уровень обеспечивает корректность передачи каждого кадра, помещая специальную

последовательность битов в начало и конец каждого кадра для его выделения, а также вычисляет контрольную сумму, обрабатывая все байты кадра определенным способом и добавляя контрольную сумму к кадру. Когда кадр приходит по сети, получатель снова вычисляет контрольную сумму полученных данных и сравнивает результат с контрольной суммой из кадра. Если они совпадают, кадр считается правильным и принимается. Если же контрольные суммы не совпадают, то фиксируется ошибка. Канальный уровень может не только обнаруживать ошибки, но и исправлять их за счет повторной передачи поврежденных кадров. Функция исправления ошибок не является обязательной для канального уровня.

В протоколах канального уровня, используемых в локальных сетях, заложена определенная структура связей между компьютерами и способы их адресации. Хотя канальный уровень и обеспечивает доставку кадра между любыми двумя узлами локальной сети, он это делает только в сети с совершенно определенной топологией связей, именно той топологией, для которой он был разработан. К таким типовым топологиям, поддерживаемым протоколами канального уровня локальных сетей, относятся общая шина, кольцо и звезда, а также структуры, полученные из них с помощью мостов и коммутаторов. Примерами протоколов канального уровня являются протоколы Ethernet, Token Ring, FDDI.

В локальных сетях протоколы канального уровня используются компьютерами, мостами, коммутаторами и маршрутизаторами. В компьютерах функции канального уровня реализуются совместными усилиями сетевых адаптеров и их драйверов.

В глобальных сетях, которые редко обладают регулярной топологией, канальный уровень часто обеспечивает обмен сообщениями только между двумя соседними компьютерами, соединенными индивидуальной линией связи. Примерами протоколов «точка-точка» могут служить широко распространенные протоколы PPP и LAP-B. Для доставки сообщений между конечными узлами через всю сеть используются средства более высокого сетевого уровня.

Для обеспечения качественной транспортировки сообщений в сетях любых топологий и технологий функций канального уровня оказывается недостаточно, поэтому в модели OSI решение этой задачи возлагается на два следующих уровня — сетевой и транспортный.

2.4. Сетевой уровень

Сетевой уровень (Network layer) служит для образования единой транспортной системы, объединяющей несколько сетей, причем эти сети могут использовать совершенно разные принципы передачи сообщений между конечными узлами и обладать произвольной структурой связей. Функции сетевого уровня достаточно разнообразны. Начнем их рассмотрение на примере объединения локальных сетей.

На сетевом уровне сам термин сеть наделяют специфическим значением. В данном случае под сетью понимается совокупность компьютеров, соединенных между собой в соответствии с одной из стандартных типовых топологий и использующих для передачи данных один из протоколов канального уровня, определенный для этой топологии.

Внутри сети доставка данных обеспечивается соответствующим канальным уровнем, а вот доставкой данных между сетями занимается сетевой уровень, который и поддерживает возможность правильного выбора маршрута передачи сообщения даже в том случае, когда характер структуры связей между составляющими сетями отличается от принятого в протоколах канального уровня.

Сети соединяются между собой специальными устройствами, называемыми маршрутизаторами. Маршрутизатор — это устройство, которое собирает информацию о топологии межсетевых соединений и на ее основании пересылает пакеты сетевого уровня в сеть назначения. Чтобы передать сообщение от отправителя, находящегося в одной сети, получателю, находящемуся в другой сети, нужно совершить некоторое количество транзитных передач между сетями, или хопов (hop — прыжок), каждый раз выбирая подходящий маршрут. Таким образом, маршрут представляет собой последовательность маршрутизаторов, через которые проходит пакет.

Проблема выбора наилучшего пути называется маршрутизацией, и ее решение является одной из главных задач сетевого уровня. Эта проблема осложняется тем, что самый короткий путь не всегда самый лучший. Часто критерием при выборе маршрута является время передачи данных по этому маршруту; оно зависит от пропускной способности каналов связи и интенсивности трафика, которая может изменяться с течением времени. Выбор маршрута может осуществляться и по другим критериям, например надежности передачи.

Сетевой уровень может также решать задачи согласования разных технологий, упрощения адресации в крупных сетях и создания надежных и гибких барьеров на пути нежелательного трафика между сетями.

Сообщения сетевого уровня принято называть пакетами (packet). При организации доставки пакетов на сетевом уровне используется понятие «номер сети». В этом случае адрес получателя состоит из старшей части — номера сети и младшей — номера узла в этой сети.

На сетевом уровне определяются два вида протоколов. Первый вид — сетевые протоколы (muted protocols) — реализуют продвижение пакетов через сеть. Однако часто к сетевому уровню относят и другой вид протоколов, называемых протоколами обмена маршрутной информацией или просто протоколами маршрутизации (routing protocols). С помощью этих протоколов маршрутизаторы собирают информацию о топологии межсетевых соединений. Протоколы сетевого уровня реализуются программными модулями операционной системы, а также программными и аппаратными средствами маршрутизаторов.

На сетевом уровне работают протоколы еще одного типа, которые отвечают за отображение адреса узла, используемого на сетевом уровне, в локальный адрес сети. Такие протоколы часто называют протоколами разрешения адресов (Address Resolution Protocol, ARP). Иногда их относят не к сетевому уровню, а к канальному, хотя тонкости классификации не изменяют их сути.

Примерами протоколов сетевого уровня являются протокол межсетевого взаимодействия IP стека TCP/IP и протокол межсетевого обмена пакетами IPX стека Novell.

2.5. Транспортный уровень

На пути от отправителя к получателю пакеты могут быть искажены или утеряны. Хотя некоторые приложения имеют собственные средства обработки ошибок, существуют и такие, которые предпочитают сразу иметь дело с надежным соединением. Транспортный уровень (Transport layer) обеспечивает приложениям или верхним уровням стека — прикладному и сеансовому — передачу данных с той степенью надежности, которая им требуется. Модель OSI определяет пять классов сервиса, предоставляемых транспортным уровнем. Эти виды сервиса отличаются качеством предоставляемых услуг: срочностью, возможностью восстановления прерванной связи, наличием средств мультиплексирования нескольких соединений между различными прикладными протоколами через общий транспортный протокол, а главное — способностью к обнаружению и исправлению ошибок передачи, таких как искажение, потеря и дублирование пакетов.

Выбор класса сервиса транспортного уровня определяется, с одной стороны, тем, в какой степени задача обеспечения надежности решается самими приложениями и протоколами более высоких, чем транспортный, уровней. С другой стороны, этот выбор зависит от того, насколько надежной является система транспортировки данных в сети, обеспечиваемая уровнями, расположенными ниже транспортного — сетевым, канальным и физическим.

Как правило, все протоколы, начиная с транспортного уровня и выше, реализуются программными средствами конечных узлов сети — компонентами их сетевых операционных систем. В качестве примера транспортных протоколов можно привести протоколы TCP и UDP стека TCP/IP и протокол SPX стека Novell.

Протоколы нижних четырех уровней обобщенно называют сетевым транспортом или транспортной подсистемой, так как они полностью решают задачу транспортировки сообщений с заданным уровнем качества в составных сетях с произвольной топологией и различными технологиями. Оставшиеся три верхних уровня решают задачи предоставления прикладных сервисов на основании имеющейся транспортной подсистемы.

2.6. Сеансовый уровень

Сеансовый уровень (Session layer) обеспечивает управление взаимодействием: фиксирует, какая из сторон является активной в настоящий момент, предоставляет средства синхронизации. Последние позволяют вставлять контрольные точки в длинные передачи, чтобы в случае отказа можно было вернуться назад к последней контрольной точке, а не начинать все с начала. На практике немногие приложения используют сеансовый уровень, и он редко реализуется в виде отдельных протоколов, хотя функции этого уровня часто объединяют с функциями прикладного уровня и реализуют в одном протоколе.

2.7. Представительный уровень

Представительный уровень (Presentation layer) имеет дело с формой представления передаваемой по сети информации, не меняя при этом ее содержания. За счет уровня представления информация, передаваемая прикладным уровнем одной системы, всегда понятна прикладному уровню другой системы. С помощью средств данного уровня протоколы прикладных уровней могут преодолеть синтаксические различия в представлении данных или же различия в кодах символов, например кодов ASCII и EBCDIC. На этом уровне может выполняться шифрование и дешифрование данных, благодаря которым секретность обмена данными обеспечивается сразу для всех прикладных служб. Примером такого протокола является протокол Secure Socket Layer (SSL), который обеспечивает секретный обмен сообщениями для протоколов прикладного уровня стека TCP/IP.

2.8. Прикладной уровень

Прикладной уровень (Application layer) — это в действительности просто набор разнообразных протоколов, с помощью которых пользователи сети получают доступ к разделяемым ресурсам, таким как файлы, принтеры или гипертекстовые web-страницы, а также организуют свою совместную работу, например, по протоколу электронной почты. Единица данных, которой оперирует прикладной уровень, обычно называется сообщением (message).

Существует очень большое разнообразие служб прикладного уровня. Приведем в качестве примера хотя бы несколько наиболее распространенных реализаций файловых служб: NCP в операционной системе Novell NetWare, SMB в Microsoft Windows NT, NFS, FTP и TFTP, входящие в стек TCP/IP.

2.9. Сетезависимые и сетенезависимые уровни

Функции всех уровней модели OSI могут быть отнесены к одной из двух групп: либо к функциям, зависящим от конкретной технической реализации сети, либо к функциям, ориентированным на работу с приложениями.

Три нижних уровня — физический, канальный и сетевой — являются сетезави-симыми, то есть протоколы этих уровней тесно связаны с технической реализацией сети и используемым коммуникационным оборудованием. Например, переход с оборудования Ethernet на оборудование FDDI означает полную смену протоколов физического и канального уровней во всех узлах сети.

Три верхних уровня — прикладной, представительный и сеансовый — ориентированы на приложения и мало зависят от технических особенностей построения сети. На протоколы этих уровней не влияют какие бы то ни было изменения в топологии сети, замена оборудования или переход на другую сетевую технологию. Так, переход от Ethernet на более скоростную технологию Fast Ethernet не требует никаких изменений в программных средствах, реализующих функции прикладного, представительного и сеансового уровней.

Транспортный уровень является промежуточным, он скрывает детали функционирования нижних уровней от верхних. Это позволяет разрабатывать приложения, не зависящие от технических средств непосредственной транспортировки сообщений.
Компьютер с установленной на нем сетевой ОС взаимодействует с другим компьютером по протоколам всех семи уровней. Это взаимодействие компьютеры осуществляют через различные коммуникационные устройства: концентраторы, модемы, мосты, коммутаторы, маршрутизаторы, мультиплексоры. В зависимости от типа коммуникационное устройство может работать либо только на физическом уровне (повторитель), либо на физическом и канальном (мост), либо на физическом, канальном и сетевом, иногда захватывая и транспортный уровень (маршрутизатор).

3. Стандартизация сетей

3.1. Понятие «открытая система»

Модель OSI, как это следует из ее названия (Open System Interconnection), описывает взаимосвязи открытых систем.
В широком смысле открытой системой может быть названа любая система (компьютер, вычислительная сеть, ОС, программный пакет, другие аппаратные и программные продукты), которая построена в соответствии с открытыми спецификациями. Под термином «спецификация» в вычислительной технике понимают формализованное описание аппаратных или программных компонентов, способов их функционирования, взаимодействия с другими компонентами, условий эксплуатации, ограничений и особых характеристик. Понятно, что не всякая спецификация является стандартом. В свою очередь, под открытыми спецификациями понимаются опубликованные, общедоступные спецификации, соответствующие стандартам и принятые в результате достижения согласия после всестороннего обсуждения всеми заинтересованными сторонами.
Модель OSI касается только одного аспекта открытости, а именно открытости средств взаимодействия устройств, связанных в вычислительную сеть. Здесь под открытой системой понимается сетевое устройство, готовое взаимодействовать с другими сетевыми устройствами с использованием стандартных правил, определяющих формат, содержание и значение принимаемых и отправляемых сообщений.
Соблюдение принципов открытости при построении сетей дает следующие преимущества:

- q возможность построения сети из аппаратных и программных средств различных производителей, придерживающихся одного и того же стандарта;
- q возможность безболезненной замены отдельных компонентов сети другими, более совершенными, что позволяет сети развиваться с минимальными затратами;
- q возможность легкого сопряжения одной сети с другой;
- q простоту освоения и обслуживания сети.

Ярким примером открытой системы является международная сеть Интернет. Само название стандартов, определяющих работу сети Интернет — Request For Comments

(RFC), что можно перевести как «запрос на комментарии», — показывает гласный и открытый характер принимаемых стандартов.

3.2. Модульность и стандартизация

Модульность — это одно из неотъемлемых и естественных свойств вычислительных сетей. Сеть состоит из огромного числа различных модулей — компьютеров, сетевых адаптеров, мостов, маршрутизаторов, модемов, операционных систем и модулей приложений. Разнообразные требования, предъявляемые предприятиями к компьютерным сетям, привели к такому же разнообразию выпускаемых для построения сети устройств и программ. В результате совершенно необходимым оказалось принятие многочисленных стандартов, которые гарантировали бы совместимость оборудования и программ различных фирм-изготовителей. Модульный подход только тогда дает преимущества, когда он сопровождается следованием стандартам. Большинство стандартов, принимаемых сегодня, носят открытый характер.

Сегодня в секторе сетевого оборудования и программ с совместимостью продуктов разных производителей сложилась следующая ситуация. Практически все продукты, как программные, так и аппаратные, совместимы по функциям и свойствам, которые были внедрены в практику уже достаточно давно и стандарты на которые уже разработаны и приняты по крайней мере 3-4 года назад. В то же время очень часто принципиально новые устройства, протоколы и свойства оказываются несовместимыми даже у ведущих производителей.

3.3. Источники стандартов

Работы по стандартизации вычислительных сетей ведутся большим количеством организаций. В зависимости от статуса организаций различают следующие виды стандартов:

- q стандарты отдельных фирм (например, графический интерфейс OPEN LOOK для UNIX-систем фирмы Sun);
- q стандарты специальных комитетов и объединений, создаваемых несколькими фирмами, например, стандарты союза Fast Ethernet Alliance по разработке стандартов 100 Мбит Ethernet;
- q национальные стандарты, например, стандарты безопасности для операционных систем, разработанные Национальным центром компьютерной безопасности (NCSC) Министерства обороны США;
- q международные стандарты, например, модель и стек коммуникационных протоколов OSI Международной организации по стандартизации (ISO).

Некоторые стандарты, непрерывно развиваясь, могут переходить из одной категории в другую. В частности, фирменные стандарты на продукцию, получившую широкое распространение, обычно становятся международными стандартами «де-факто», так как

вынуждают производителей из разных стран следовать фирменным стандартам, чтобы обеспечить совместимость своих изделий с этими популярными продуктами. Например, из-за феноменального успеха персонального компьютера компании IBM фирменный стандарт на архитектуру IBM PC стал международным стандартом де-факто.
Более того, ввиду широкого распространения некоторые фирменные стандарты становятся основой для национальных и международных стандартов «де-юре». Например, стандарт Ethernet, первоначально разработанный компаниями Digital Equipment, Intel и Xerox, через некоторое время и в несколько измененном виде был принят как национальный стандарт IEEE 802.3, а затем организация ISO утвердила его в качестве международного стандарта ISO 8802.3.
Далее приводятся краткие сведения об организациях, наиболее активно и успешно занимающихся разработкой стандартов в области вычислительных сетей.

- q Международная организация по стандартизации (International Organization for Standardization, ISO), часто называемая также International Standards Organization, представляет собой ассоциацию ведущих национальных организаций по стандартизации разных стран. Главным достижением ISO явилась модель взаимодействия открытых систем OSI, которая в настоящее время является концептуальной основой стандартизации в области вычислительных сетей.
- q Международный союз электросвязи (International Telecommunications Union, ITU) — организация, являющаяся в настоящее время специализированным органом Организации Объединенных Наций. Наиболее значительную роль в стандартизации вычислительных сетей играет постоянно действующий в рамках этой организации сектор телекоммуникационной стандартизации (ITU Telecommunication Standardization Sector, ITU-T). ITU-T разрабатывает международные стандарты в области телефонии, телематических служб (электронной почты, факсимильной связи, телетекста, телекса и т. д.), передачи данных, аудио- и видеосигналов. Раз в четыре года издаются труды ITU-T в виде так называемой «Книги», которая на самом деле представляет собой целый набор обычных книг, сгруппированных в выпуски, которые, в свою очередь, объединяются в тома. Каждый том и выпуск содержат логически взаимосвязанные рекомендации. Например, том III Синей книги содержит рекомендации для цифровых сетей с интеграцией услуг (ISDN).
- q Институт инженеров по электротехнике и радиоэлектронике (Institute of Electrical and Electronics Engineers, IEEE) — национальная организация США, определяющая сетевые стандарты. В 1981 году рабочая группа 802 этого института сформулировала основные требования, которым должны удовлетворять локальные вычислительные сети. Группа 802 определила множество стандартов, из них самыми известными являются стандарты 802.1, 802.2, 802.3 и 802.5, которые описывают общие понятия, используемые в области локальных сетей, а также стандарты на два нижних уровня сетей Ethernet и Token Ring.
- q Европейская ассоциация производителей компьютеров (European Computer Manufacturers Association, ECMA) — некоммерческая организация, активно сотрудничающая с ITU-T и ISO, занимается разработкой стандартов и технических

обзоров, относящихся к компьютерной и коммуникационной технологиям. Известна своим стандартом ECMA-101, используемым при передаче отформатированного текста и графических изображений с сохранением оригинального формата.

- q Ассоциация производителей компьютеров и оргтехники (Computer and Business Equipment Manufacturers Association, CBEMA) — организация американских фирм-произво-дителей аппаратного обеспечения; аналогична европейской ассоциации ЕКМА; участвует в разработке стандартов на обработку информации и соответствующее оборудование.
- q Ассоциация электронной промышленности (Electronic Industries Association, EIA) — промышленно-торговая группа производителей электронного и сетевого оборудования; является национальной коммерческой ассоциацией США; проявляет значительную активность в разработке стандартов для проводов, коннекторов и других сетевых компонентов. Ее наиболее известный стандарт - RS-232C.
- q Министерство обороны США (Department of Defense, DoD) имеет многочисленные подразделения, занимающиеся созданием стандартов для компьютерных систем. Одной из самых известных разработок DoD является стек транспортных протоколов TCP/IP.
- q Американский национальный институт стандартов (American National Standards Institute, ANSI) — эта организация представляет США в Международной организации по стандартизации ISO. Комитеты ANSI ведут работу по разработке стандартов в различных областях вычислительной техники. В области микрокомпьютеров ANSI разрабатывает стандарты на языки программирования, интерфейс SCSI.
- Особую роль в выработке международных открытых стандартов играют стандарты Интернета.

Основным их разработчиком является Internet Society (ISOC) — профессиональное сообщество, которое занимается общими вопросами эволюции и роста Интернета как глобальной коммуникационной инфраструктуры. Под управлением ISOC работает Internet Architecture Board (IAB) — организация, в ведении которой находится технический контроль и координация работ для Интернета. IAB координирует направление исследований и новых разработок для стека TCP/IP и является конечной инстанцией при определении новых стандартов Интернета.

В IAB входят две основные группы: Internet Engineering Task Force (IETF) и Internet Research Task Force (IRTF). IETF — это инженерная группа, которая занимается решением ближайших технических проблем Интернета. Именно IETF определяет спецификации, которые затем становятся стандартами Интернета. В свою очередь, IRTF координирует долгосрочные исследовательские проекты по протоколам TCP/IP.

В любой организации, занимающейся стандартизацией, процесс выработки и принятия стандарта состоит из ряда обязательных этапов, которые, собственно, и составляют процедуру стандартизации. Рассмотрим эту процедуру на примере разработки стандартов Интернета.

1. Сначала в IETF представляется так называемый рабочий проект (draft) в виде, доступном для комментариев. Он публикуется в Интернете, после чего широкий круг заинтересованных лиц включается в обсуждение этого документа, в него вносятся исправления, и наконец наступает момент, когда можно зафиксировать содержание документа. На этом этапе проекту присваивается номер RFC (возможен и другой вариант развития событий — после обсуждения рабочий проект отвергается и удаляется из Интернета).
2. После присвоения номера проект приобретает статус предлагаемого стандарта. В течение 6 месяцев этот предлагаемый стандарт проходит проверку практикой, в результате в него вносятся изменения.
3. Если результаты практических исследований показывают эффективность предлагаемого стандарта, то ему со всеми внесенными изменениями присваивается статус проекта стандарта. Затем в течение не менее 4 месяцев проходят его дальнейшие испытания «на прочность», в число которых входит создание по крайней мере двух программных реализаций.
4. Если во время пребывания в ранге проекта стандарта в документ не было внесено никаких исправлений, то ему может быть присвоен статус официального стандарта Интернета. Список утвержденных официальных стандартов Интернета публикуется в виде документа RFC и доступен в Интернете.

Следует заметить, что все стандарты Интернета носят название RFC с соответствующим порядковым номером, но далеко не все RFC являются стандартами Интернета — часто эти документы представляют собой комментарии к какому-либо стандарту или просто описания некоторой проблемы Интернета.

3.4. Стандартные стеки коммуникационных протоколов

Важнейшим направлением стандартизации в области вычислительных сетей является стандартизация коммуникационных протоколов. В настоящее время в сетях используется большое количество стеков коммуникационных протоколов. Наиболее популярными являются стеки: TCP/IP, IPX/SPX, NetBIOS/SMB, DECnet, SNA и OSI. Все эти стеки, кроме SNA, на нижних уровнях (физическом и канальном), используют одни и те же хорошо стандартизованные протоколы Ethernet, Token Ring, FDDI и некоторые другие, которые позволяют использовать во всех сетях одну и ту же аппаратуру. Зато на верхних уровнях все стеки работают по своим собственным протоколам. Эти протоколы часто не соответствуют рекомендуемому моделью OSI разбиению на уровни. В частности, функции сеансового и представительного уровня, как правило, объединены с прикладным уровнем. Такое несоответствие связано с тем, что модель OSI появилась как результат обобщения уже существующих и реально используемых стеков, а не наоборот.

3.4.1. Стек OSI

Следует четко различать модель OSI и стек OSI. В то время как модель OSI является концептуальной схемой взаимодействия открытых систем, стек OSI представляет собой набор вполне конкретных спецификаций протоколов. В отличие от других стеков протоколов, стек OSI полностью соответствует модели OSI, он включает спецификации протоколов для всех семи уровней взаимодействия, определенных в этой модели. На нижних уровнях стек OSI поддерживает Ethernet, Token Ring, FDDI, протоколы глобальных сетей, X.25 и ISDN, — то есть использует разработанные вне стека протоколы нижних уровней, как и все другие стеки. Протоколы сетевого, транспортного и сеансового уровней стека OSI специфицированы и реализованы различными производителями, но распространены пока мало. Наиболее популярными протоколами стека OSI являются прикладные протоколы. К ним относятся: протокол передачи файлов FTAM, протокол эмуляции терминала VTP, протоколы справочной службы X.500, электронной почты X.400 и ряд других.

Протоколы стека OSI отличает большая сложность и неоднозначность спецификаций. Эти свойства явились результатом общей политики разработчиков стека, стремившихся учесть в своих протоколах все случаи жизни и все существующие и появляющиеся технологии. К этому нужно еще добавить и последствия большого количества политических компромиссов, неизбежных при принятии международных стандартов по такому злободневному вопросу, как построение открытых вычислительных сетей.

Из-за своей сложности протоколы OSI требуют больших затрат вычислительной мощности центрального процессора, что делает их более подходящими для мощных машин, а не для сетей персональных компьютеров.

3.4.2. Стек TCP/IP

Стек TCP/IP был разработан по инициативе Министерства обороны США более 20 лет назад для связи экспериментальной сети ARPAnet с другими сетями как набор общих протоколов для разнородной вычислительной среды. Большой вклад в развитие стека TCP/IP, который получил свое название по популярным протоколам IP и TCP, внес университет Беркли, реализовав протоколы стека в своей версии ОС UNIX. Популярность этой операционной системы привела к широкому распространению протоколов TCP, IP и других протоколов стека. Сегодня этот стек используется для связи компьютеров всемирной информационной сети Интернет, а также в огромном числе корпоративных сетей.

Стек TCP/IP на нижнем уровне поддерживает все популярные стандарты физического и канального уровней. Для локальных сетей — это Ethernet, Token Ring, FDDI, для глобальных — протоколы работы на аналоговых коммутируемых и выделенных линиях SLIP, PPP, протоколы территориальных сетей X.25 и ISDN.

Основными протоколами стека, давшими ему название, являются протоколы IP и TCP. Эти протоколы в терминологии модели OSI относятся к сетевому и транспортному

уровням соответственно. IP обеспечивает продвижение пакета по составной сети, а TCP гарантирует надежность его доставки.
За долгие годы использования в сетях различных стран и организаций стек TCP/IP вобрал в себя большое количество протоколов прикладного уровня. К ним относятся такие популярные протоколы, как протокол пересылки файлов FTP, протокол эмуляции терминала telnet, почтовый протокол SMTP, используемый в электронной почте сети Интернет, гипертекстовые сервисы службы WWW и многие другие.
Стремительный рост популярности Интернета привел к тому, что сегодня в мире подавляющее большинство компьютеров использует стек TCP/IP. Сейчас любая промышленная операционная система обязательно включает программную реализацию этого стека в своем комплекте поставки.
Хотя протоколы TCP/IP неразрывно связаны с Интернетом, существует большое количество локальных, корпоративных и территориальных сетей, непосредственно не являющихся частями Интернета, в которых также используют протоколы TCP/IP. Чтобы отличать их от Интернета, эти сети называют сетями TCP/IP или просто IP-сетями.
Очень полезным свойством этого протокола является его способность фрагментировать пакеты, что позволяет передавать информацию в больших разнородных сетях, в каждой из частей которых может быть установлена собственная величина максимальной длины единицы передаваемых данных (кадра).
Другим преимуществом технологии TCP/IP является гибкая система адресации, позволяющая проще включать в интерсеть сети разных технологий.
Однако, как и всегда, за получаемые преимущества надо платить, и платой здесь оказываются высокие требования к ресурсам и сложность администрирования IP-сетей.

3.4.3. Стек IPX/SPX

Стек IPX/SPX является оригинальным стеком протоколов фирмы Novell, разработанным для сетевой операционной системы NetWare еще в начале 80-х годов. Протоколы сетевого и сеансового уровней Internetwork Packet Exchange (IPX) и Sequenced Packet Exchange (SPX), которые дали название стеку, являются прямой адаптацией протоколов XNS фирмы Xerox, распространенных в гораздо меньшей степени, чем стек IPX/SPX.
Популярность стека IPX/SPX непосредственно связана с операционной системой Novell NetWare, популярность которой сейчас значительно уступает операционным системам Microsoft.
Сейчас стек IPX/SPX реализован не только в NetWare, но и в нескольких других популярных сетевых ОС, например SCO UNIX, Sun Solaris, Microsoft Windows NT/2000.

3.4.4. Стек NetBIOS/SMB

Стек NetBIOS/SMB широко используется в продуктах компаний IBM и Microsoft. На физическом и канальном уровнях этого стека задействованы все наиболее распространенные протоколы Ethernet, Token Ring, FDDI и др. На верхних уровнях работают протоколы NetBEUI и SMB.

Протокол NetBIOS (Network Basic Input/Output System) появился в 1984 году. В дальнейшем этот протокол был заменен так называемым протоколом расширенного пользовательского интерфейса NetBEUI — NetBIOS Extended User Interface. Для обеспечения совместимости приложений в качестве интерфейса к протоколу NetBEUI был сохранен интерфейс NetBIOS. Этот протокол содержит много полезных сетевых функций, которые можно отнести к сетевому, транспортному и сеансовому уровням модели OSI, однако с его помощью невозможна маршрутизация пакетов. Это ограничивает применение протокола NetBEUI локальными сетями, не разделенными на подсети, и делает невозможным его использование в составных сетях. Некоторые ограничения NetBEUI снимаются реализацией этого протокола NBF (NetBEUI Frame), которая включена в операционную систему Microsoft Windows NT.
Протокол SMB (Server Message Block) выполняет функции сеансового, представительного и прикладного уровней. На основе SMB реализуется файловая служба, а также службы печати и передачи сообщений между приложениями.
Стеки протоколов SNA фирмы IBM, DECnet корпорации Digital Equipment и AppleTalk/AFP фирмы Apple применяются в основном в операционных системах и сетевом оборудовании этих фирм.
В табл. 1 показано соответствие некоторых, наиболее популярных протоколов уровням модели OSI. Часто это соответствие весьма условно, так как модель OSI — это только руководство к действию, причем достаточно общее, а конкретные протоколы разрабатывались для решения специфических задач, причем многие из них появились до разработки модели OSI. В большинстве случаев разработчики стеков отдавали предпочтение скорости работы сети в ущерб модульности — ни один стек, кроме стека OSI, не разбит на семь уровней. Чаще всего в стеке явно выделяются 3-4 уровня: уровень сетевых адаптеров, в котором реализуются протоколы физического и канального уровней, сетевой уровень, транспортный уровень и уровень служб, вбирающий в себя функции сеансового, представительного и прикладного уровней.

Таблица 1.

Модель OSI	IBM/Microsoft	TCP/IP	Novell	Стек OSI
Прикладной	SMB	Telnet, FTP, SNMP, SMTP, WWW	NCP, SAP	X.400, X.500, FTAM
Представительный				Представительный протокол OSI
Сеансовый	NetBIOS	TCP		Сеансовый протокол OSI
Транспортный			SPX	Транспортный протокол OSI

Сетевой		IP, RIP, OSPF		IPX, RIP, NLSP		ES-ES, IS-IS
Канальный		802.3 (Ethernet), 802.5 (Token Ring), FDDI, Fast Ethernet, SLIP, 100VG-AnyLAN, X.25, ATM, LAP-B, LAP-D, PPP				
Физический		Коаксиал, экранированная и неэкранированная витая пара, оптоволокно, радиоволны				

Лекция 5. Линии связи, кодирование данных

При построении сетей применяются линии связи, использующие различную физическую среду: телефонные и телеграфные провода, подвешенные в воздухе, медные коаксиальные кабели, медные витые пары, волоконно-оптические кабели, радиоволны. При выборе того или иного типа линий связи разработчики прежде всего учитывают их технические характеристики, стоимость, а также простоту монтажа. Сегодня наиболее перспективными являются волоконно-оптические кабели. На них строятся как магистрали крупных территориальных и городских сетей, так и высокоскоростные линии связи локальных сетей. Популярной средой является также витая пара, которая характеризуется отличным отношением качество/стоимость.

1. Типы линий связи

1.1. Среда передачи информации

Линия связи (рис. 5.1) состоит в общем случае из физической среды, по которой передаются информационные сигналы, аппаратуры передачи данных и промежуточной аппаратуры. Синонимом термина *линия связи (line)* является термин *канал связи (channel).*

Аппаратура передачи

Рис. 5.1. Состав линии связи

Физическая среда передачи данных (medium) может представлять собой кабель, то есть набор проводов, изоляционных и защитных оболочек, соединительных разъемов, а также земную атмосферу или космическое пространство, через которые распространяются информационные сигналы. В современных телекоммуникационных системах информация передается с помощью электрического тока или напряжения, радиосигналов или световых сигналов — все эти физические процессы представляют собой колебания электромагнитного поля различной частоты и природы.

В зависимости от среды передачи данных линии связи разделяются на:

- проводные (воздушные);
- кабельные (медные и волоконно-оптические);
- радиоканалы наземной и спутниковой связи.

Проводные (воздушные) линии связи представляют собой провода без каких-либо изолирующих или экранирующих оплеток, проложенные между столбами и висящие в воздухе. По таким линиям связи традиционно передаются телефонные или телеграфные сигналы, но при отсутствии других возможностей эти линии используются и для передачи компьютерных данных. Скоростные качества и помехозащищенность этих линий оставляют желать много лучшего. Сегодня проводные линии связи быстро вытесняются кабельными.

Кабельные линии имеют достаточно сложную конструкцию. Кабель состоит из проводников, заключенных в несколько слоев изоляции: электрической, электромагнитной, механической, а также, возможно, климатической. Кроме того, кабель может быть оснащен разъемами, позволяющими быстро выполнять присоединение к нему различного оборудования. В компьютерных (и телекоммуникационных) сетях применяются три основных типа кабеля: кабели на основе скрученных пар медных проводов, коаксиальные кабели с медной жилой, а также волоконно-оптические кабели (первые два типа кабелей называют также медными кабелями).

В зависимости от условий прокладки и эксплуатации кабели делятся на внутренние кабели (кабели зданий) и внешние кабели, которые, в свою очередь, подразделяются на подземные, подводные и кабели воздушной проводки.

Скрученная пара проводов называется *витой парой (twisted pair).* Скручивание проводов снижает влияние внешних и взаимных помех на полезные сигналы, передаваемые по кабелю. Для неответственных применений внутри здания иногда используются симметричные кабели из нескрученных пар — так называемая «лапша».

Основные особенности конструкции кабелей схематично показаны на рис. 5.2.

Рис. 5.2. Устройство кабелей

Кабели на основе витой пары называются *симметричными кабелями* из-за того, что они состоят из двух одинаковых в конструктивном отношении проводников. Симметричный кабель может быть как экранированным — на основе *экранированной витой пары (Shielded Twisted Pair, STP),* так и неэкранированным — на основе *неэкранированной витой пары (Unshielded Twisted Pair, UTP).*

Нужно отличать электрическую изоляцию проводящих жил, которая имеется в любом кабеле, от электромагнитной изоляции. Первая состоит из непроводящего диэлектрического слоя — бумаги или полимера, например поливинилхлорида или полистирола. Во втором случае кроме электрической изоляции проводящие жилы помещаются также внутрь электромагнитного экрана, в качестве которого чаще всего применяется проводящая медная оплетка. Симметричный кабель может состоять из нескольких витых пар. В настоящее время кабельные системы зданий чаще всего строятся на основе неэкранированной витой пары, при этом наиболее часто используется витая пара так называемой *категории 5* — в соответствии с классификацией американского национального стандарта для кабелей такого назначения.

Коаксиальный кабель (coaxial) состоит из несимметричных пар проводников. Каждая пара представляет собой внутреннюю медную жилу и соосную с ней внешнюю жилу, которая может быть полой медной трубой или оплеткой, отделенной от внутренней жилы диэлектрической изоляцией. Внешняя жила играет двоякую роль — по ней передаются информационные сигналы, также она является экраном, защищающим внутреннюю жилу от внешних

электромагнитных полей. Существует несколько типов коаксиального кабеля, отличающихся характеристиками и областями применения — для локальных компьютерных сетей, для глобальных телекоммуникационных сетей, для кабельного телевидения и т. п.

Волоконно-оптический кабель (optical fiber) состоит из тонких (5-60 микрон) гибких стеклянных волокон (волоконных световодов), по которым распространяются световые сигналы. Это наиболее качественный тип кабеля — он обеспечивает передачу данных с очень высокой скоростью (до 10 Гбит/с и выше) и к тому же лучше других типов передающей среды обеспечивает защиту данных от внешних помех (в силу особенностей распространения света такие сигналы легко экранировать).

Каждый световод состоит из центрального проводника света (сердцевины) — стеклянного волокна, и стеклянной оболочки, обладающей меньшим показателем преломления, чем сердцевина. Распространяясь по сердцевине, лучи света не выходят за ее пределы, отражаясь от покрывающего слоя оболочки. В зависимости от распределения показателя преломления и от величины диаметра сердечника различают:

- многомодовое волокно со ступенчатым изменением показателя преломления;
- многомодовое волокно с плавным изменением показателя преломления;
- одномодовое волокно.

Понятие «мода» описывает режим распространения световых лучей во внутреннем сердечнике кабеля. В *одномодовом кабеле (Single Mode Fiber, SMF)* используется центральный проводник очень малого диаметра, соизмеримого с длиной волны света — от 5 до 10 мкм. При этом практически все лучи света распространяются вдоль оптической оси световода, не отражаясь от внешнего проводника. Изготовление сверхтонких качественных волокон для одномодового кабеля представляет сложный технологический процесс, что делает одномодовый кабель достаточно дорогим. Кроме того, в волокно такого маленького диаметра достаточно сложно направить пучок света, не потеряв при этом значительную часть его энергии.

В *многомодовых кабелях (Multi Mode Fiber, MMF)* используются более широкие внутренние сердечники, которые легче изготовить технологически. В стандартах определены два наиболее употребительных многомодовых кабеля: 62,5/125 мкм и 50/125 мкм, где 62,5 мкм или 50 мкм — диаметр центрального проводника, а 125 мкм — диаметр внешнего проводника.

В многомодовых кабелях во внутреннем проводнике одновременно существует несколько световых лучей, отражающихся от внешнего проводника

под разными углами. Угол отражения луча называется модой луча. Многомодовые кабели проще изготавливать, поэтому они дешевле одномодовых, но и их характеристики существенно хуже, чем одномодовых. В результате многомодовые кабели используются в основном для передачи данных на небольшие расстояния (до 300-2000 м) на скоростях не более 1 Гбит/с, а одномодовые — для передачи данных со сверхвысокими скоростями в несколько десятков гигабит в секунду (а при использовании технологии DWDM — до нескольких терабит в секунду), на расстояниях от нескольких километров (локальные и городские сети) до нескольких десятков и даже сотен километров (дальняя связь).

В качестве источников излучения света в волоконно-оптических кабелях применяются:

- светодиоды, или светоизлучающие диоды (Light Emmited Diode, LED) для многомодовых кабелей;
- полупроводниковые лазеры, или лазерные диоды (Laser Diode) для одномодовых кабелей.

Волоконно-оптические кабели обладают отличными характеристиками всех типов: электромагнитными, механическими (хорошо гнутся, а в соответствующей изоляции обладают хорошей механической прочностью). Однако у них есть один серьезный недостаток — сложность соединения волокон с разъемами и между собой при необходимости наращивания (увеличения длины) кабеля.

Сама стоимость волоконно-оптических кабелей ненамного превышает стоимость кабелей на витой паре, однако проведение монтажных работ с оптоволокном обходится намного дороже из-за трудоемкости операций и высокой стоимости применяемого монтажного оборудования. Так, присоединение оптического волокна к разъему требует проведения высокоточной обрезки волокна в плоскости строго перпендикулярной оси волокна, а также выполнения соединения путем сложной операции склеивания, а не обжатия, как это делается для витой пары. В случае же некачественных соединений резко сужается полоса пропускания волоконно-оптических кабелей и линий.

Радиоканалы наземной и спутниковой связи образуются с помощью передатчика и приемника радиоволн. Существует большое разнообразие типов радиоканалов, отличающихся как используемым частотным диапазоном, так и дальностью канала. Диапазоны коротких, средних и длинных волн (КВ, СВ и ДВ), называемые также диапазонами амплитудной модуляции (Amplitude Modulation, AM) по типу используемого в них метода модуляции сигнала, обеспечивают дальнюю связь, но при невысокой скорости передачи данных. Более скоростными являются каналы, работающие на диапазонах ультракоротких волн (УКВ), для которых характерна частотная модуляция (Frequency Modulation, FM), а также диапазонах сверхвысоких частот (СВЧ, или microwaves). В диапазоне СВЧ (свыше

4 ГГц) сигналы уже не отражаются ионосферой Земли, и для устойчивой связи требуется наличие прямой видимости между передатчиком и приемником. Поэтому такие частоты используют либо спутниковые каналы, либо радиорелейные каналы, где это условие выполняется.

В компьютерных сетях сегодня применяются практически все описанные типы физических сред передачи данных, но наиболее перспективными являются волоконно-оптические кабели. На них сегодня строятся как магистрали крупных территориальных и городских сетей, так и высокоскоростные линии связи локальных сетей. Популярной средой является также витая пара, которая характеризуется отличным отношением качества к стоимости, а также простотой монтажа. Спутниковые каналы и радиосвязь используются чаще всего в тех случаях, когда кабельные линии связи применить нельзя — например, при прохождении канала через малонаселенную местность или же для связи с мобильными пользователями сети. Пока наиболее популярными являются мобильные телефонные сети, а мобильные компьютерные сети представлены сетями радио-Ethernet, имеющими несравнимо меньшее распространение. В мобильных сетях нового, так называемого третьего поколения (3d generation, 3G) предусматривается одновременная передача голоса и компьютерных данных, при этом каждый вид трафика считается одинаково важным.

1.2. Аппаратура линий связи

Аппаратура передачи данных, или *АПД (Data Circuit Equipment, DCE)* в компьютерных сетях непосредственно присоединяет компьютеры или локальные сети пользователя к линии связи и является, таким образом, пограничным оборудованием. Традиционно аппаратуру передачи данных включают в состав линии связи. Примерами DCE являются модемы, терминальные адаптеры сетей ISDN, устройства подключения к цифровым каналам. Обычно DCE работает на физическом уровне, отвечая за передачу информации в физическую среду (в линию) и прием из нее сигналов нужной формы и мощности.

Аппаратура пользователя линии связи, вырабатывающая данные для передачи по линии связи и подключаемая непосредственно к аппаратуре передачи данных, носит обобщенное название *оконечное оборудование данных,* или *ООД (Data Terminal Equipment, DTE).* Примером DTE могут служить компьютеры, коммутаторы или маршрутизаторы. Эту аппаратуру не включают в состав линии связи.

Промежуточная аппаратура обычно используется на линиях связи большой протяженности. Она решает две основные задачи:

- улучшение качества сигнала;

- создание постоянного составного канала связи между двумя абонентами сети.

В локальных сетях промежуточная аппаратура может совсем не использоваться, если протяженность физической среды — кабелей или радиоэфира — позволяет одному сетевому адаптеру принимать сигналы непосредственно от другого сетевого адаптера без промежуточного усиления. В противном случае применяются устройства типа повторителей и концентраторов.

В глобальных сетях необходимо обеспечить качественную передачу сигналов на расстояния в сотни и тысячи километров. Поэтому без усилителей (повышающих мощность сигналов) и регенераторов (наряду с повышением мощности восстанавливающих форму импульсных сигналов, исказившихся при передаче на большое расстояние), установленных через определенные расстояния, построить территориальную линию связи невозможно. В глобальной сети необходима также и промежуточная аппаратура другого рода — мультиплексоры, демультиплексоры и коммутаторы. Эта аппаратура решает вторую указанную задачу, то есть создает между двумя абонентами сети непрерывный составной канал из отрезков физической среды — кабелей с усилителями. Причем некоторые из этих отрезков, обладающие широкой полосой пропускания, например отрезки волоконно-оптического или коаксиального кабеля, одновременно участвуют в образовании сразу нескольких составных каналов. Такой высокоскоростной канал, по которому передаются одновременно данные от большого числа сравнительно низкоскоростных абонентских линий, обычно называют уплотненным каналом. Наличие промежуточной коммутационной аппаратуры избавляет создателей глобальной сети от необходимости прокладывать отдельную кабельную линию для каждой пары соединяемых узлов сети.

Промежуточная аппаратура канала связи прозрачна для пользователя, он ее не замечает и не учитывает в своей работе. Для него важны только качество полученного канала в целом, влияющее на скорость и надежность передачи дискретных данных. В действительности же невидимая пользователями промежуточная аппаратура образует сложную сеть. Эту сеть называют *первичной сетью,* так как сама по себе она никаких высокоуровневых служб (например, файловой или передачи голоса) не поддерживает, а только служит основой для построения компьютерных, телефонных или иных сетей, которые иногда называют *наложенными,* или *вторичными,* сетями.

В зависимости от типа промежуточной аппаратуры все линии связи делятся на аналоговые и цифровые. В *аналоговых линиях* промежуточная аппаратура предназначена для усиления аналоговых сигналов, то есть сигналов, которые имеют непрерывный диапазон значений. Такие линии связи традиционно

применялись в телефонных сетях для связи АТС между собой. Для создания высокоскоростных каналов, которые мультиплексируют несколько низкоскоростных аналоговых абонентских каналов, при аналоговом подходе обычно используется техника частотного мультиплексирования (Frequency Division Multiplexing, FDM).

В *цифровых линиях связи* передаваемые сигналы имеют конечное число состояний. Как правило, элементарный сигнал, то есть сигнал, передаваемый за один такт работы передающей аппаратуры, имеет 2, 3 или 4 состояния, которые передаются в линиях связи импульсами или потенциалами прямоугольной формы. С помощью таких сигналов передаются как компьютерные данные, так и оцифрованные речь и изображение (именно из-за общего вида представления информации современными компьютерными, телефонными и телевизионными сетями стали возможны общие первичные сети). В цифровых каналах связи используется специальная промежуточная аппаратура — регенераторы, которые улучшают форму импульсов и обеспечивает их ресинхронизацию, то есть восстанавливают период их следования. Промежуточная аппаратура мультиплексирования и коммутации первичных сетей работает по принципу временного мультиплексирования каналов (Time Division Multiplexing, TDM), когда каждому низкоскоростному каналу выделяется определенная доля времени (тайм-слот, или квант) высокоскоростного канала.

В настоящее время аналоговые каналы стали применяться в первичных сетях нового типа, использующих метод мультиплексирования по длине волны (Wavelength Division Multiplexing, WDM). В первичных сетях WDM каждый канал передает свою информацию с помощью световой волны определенной длины (и, соответственно, частоты). Такой канал также называется спектральным каналом, так как ему выделяется определенная полоса спектра светового излучения. Аппаратура передачи дискретных компьютерных данных по аналоговым линиям связи существенно отличается от аппаратуры такого же назначения, предназначенной для работы с цифровыми линиями. Аналоговая линия связи предназначена для передачи сигналов произвольной формы и не предъявляет никаких требований к способу представления единиц и нулей аппаратурой передачи данных (это справедливо для сетей FDM и WDM/DWDM), а в цифровой — все параметры передаваемых линией импульсов стандартизованы. Другими словами, на цифровых линиях связи протокол физического уровня определен, а на аналоговых линиях — нет (есть и исключения из этого правила, некоторые сети DWDM для передачи информации по спектральному каналу требуют цифрового кодирования определенного вида).

2. Характеристики линий связи

2.1. Группы характеристик линий связи

К основным характеристикам линий связи относятся *параметры распространения* и *параметры влияния.* Первые характеризуют процесс распространения полезного сигнала в зависимости от внутренних параметров линии, например погонной индуктивности медного кабеля. Вторые описывают степень влияния на полезный сигнал других сигналов — внешних помех, помех от других пар проводников в медном кабеле. Те и другие характеристики важны, так как сигнал на выходе линии связи всегда является результатом воздействия на исходный сигнал как внутренних, так и внешних факторов.

В каждой из этих групп можно выделить первичные и вторичные параметры. Первичные параметры описывают физическую природу линии связи, например погонное активное сопротивление, погонную индуктивность, погонную емкость и погонную проводимость изоляции медного кабеля, или же зависимость коэффициента преломления оптического волокна от расстояния от оптической оси. Вторичные параметры выражают некоторый обобщенный результат процесса распространения сигнала по линии связи и не зависят от ее природы. Например, важным вторичным параметром распространения любой линии связи является степень ослабления мощности сигнала при прохождении им определенного расстояния вдоль линии связи — так называемое затухание сигнала. Для медных кабелей не менее важен и такой вторичный параметр влияния, как степень ослабления помехи от соседней витой пары, — он позволяет оценить, не будут ли вызывать передаваемые по одной паре сигналы ложное срабатывание приемника, подключенного к соседней паре.

При описании вторичных параметров, подходя к линии связи как к кибернетическому «черному ящику», мы не строим внутреннюю модель этой физической системы, а подаем на нее некоторые эталонные воздействия и по отклику строим нужную вторичную характеристику.

2.2. Спектральный анализ сигналов на линиях связи

Из теории гармонического анализа известно, что любой периодический процесс можно представить в виде суммы синусоидальных колебаний различных частот и различных амплитуд. Каждая составляющая синусоида называется также

гармоникой, а набор всех гармоник называют спектральным разложением исходного сигнала.

Искажение передающим каналом синусоиды какой-либо частоты приводит в конечном счете к искажению амплитуды и формы передаваемого сигнала любого вида. Искажения формы проявляются в том случае, когда синусоиды различных частот искажаются неодинаково. Если это аналоговый сигнал, передающий речь, то изменяется тембр голоса за счет искажения обертонов — боковых частот. При передаче импульсных сигналов, характерных для компьютерных сетей, искажаются низкочастотные и высокочастотные гармоники, в результате фронты импульсов теряют свою прямоугольную форму. Вследствие этого на приемном конце линии сигналы могут плохо распознаваться.

Линия связи искажает передаваемые сигналы из-за того, что ее физические параметры отличаются от идеальных. Так, например, медные провода всегда представляют собой некоторую распределенную по длине комбинацию активного сопротивления, емкостной и индуктивной нагрузок. В результате для синусоид различных частот линия будет обладать разным полным сопротивлением, а значит, и передаваться они будут по-разному. Волоконно-оптический кабель также имеет отклонения от идеальной среды передачи света — вакуума. Если линия связи включает промежуточную аппаратуру, то последняя также может вносить дополнительные искажения, так как невозможно создать устройства, которые бы одинаково хорошо передавали весь спектр синусоид, от нуля до бесконечности.

Кроме искажений сигналов, вносимых внутренними физическими параметрами линии связи, существуют и внешние помехи, которые вносят свой вклад в искажение формы сигналов на выходе линии. Эти помехи создают различные электрические двигатели, электронные устройства, атмосферные явления и т. д.

Качество исходных сигналов (крутизна фронтов, общая форма импульсов) зависит от качества передатчика, генерирующего сигналы в линию связи. Одной из важных характеристик передатчика является спектральная характеристика, то есть спектральное разложение генерируемых им сигналов. Для генерации качественных прямоугольных импульсов необходимо, чтобы спектральная характеристика передатчика представляла собой как можно более узкую полосу.

2.3. Затухание и волновое сопротивление

Степень искажения синусоидальных сигналов линиями связи оценивается по таким характеристикам, как затухание и полоса пропускания.

Затухание показывает, насколько уменьшается мощность эталонного синусоидального сигнала на выходе линии связи по отношению к мощности сигнала на входе этой линии. Затухание *A* обычно измеряется в децибелах, дБ (decibel, dB) и вычисляется по следующей формуле:

$A = 10 \log_{10} P_{вых}/P_{вх}$.

Здесь $P_{вых}$ — мощность сигнала на выходе линии, $P_{вх}$ — мощность сигнала на входе линии.

Так как мощность выходного сигнала кабеля без промежуточных усилителей всегда меньше, чем мощность входного сигнала, затухание кабеля всегда является отрицательной величиной.

На практике затухание чаще используется в качестве характеристики линий связи, в частности, в стандартах на такую важную составляющую линии связи, как кабель, затухание является одной из основных характеристик.

Чаще всего при описании параметров линии связи приводятся значения затухания всего в нескольких точках общей зависимости, при этом каждая из этих точек соответствует определенной частоте, на которой измеряется затухание. Отдельное значение затухания называют *коэффициентом затухания.* Обычно затуханием характеризуют пассивные участки линии связи, состоящие из кабелей и кроссовых секций, без усилителей и регенераторов.

В качестве характеристики мощности передатчика часто используется абсолютный *уровень мощности сигнала.* Уровень мощности, как и затухание, измеряется в децибелах. При этом в качестве базового значения мощности сигнала, относительно которого измеряется текущая мощность, принимается значение в 1 мВт. Таким образом, уровень мощности *p* вычисляется по следующей формуле:

$p = 10 \lg P/1$ мВт [дБм].

Здесь P — мощность сигнала в милливаттах, а дБм (dBm) — единица измерения уровня мощности (децибел на 1 мВт).

Важным вторичным параметром распространения медной линии связи является ее *волновое сопротивление.* Этот параметр представляет собой полное (комплексное) сопротивление, которое встречает электромагнитная волна определенной частоты при распространении вдоль однородной цепи. Волновое сопротивление измеряется в омах и зависит от таких первичных параметров линии связи, как активное сопротивление, погонная индуктивность и погонная емкость, а также от частоты самого сигнала. Выходное сопротивление передатчика должно быть согласовано с волновым сопротивлением линии, иначе затухание сигнала будет чрезмерно большим.

2.4. Помехоустойчивость и достоверность

Помехоустойчивость линии определяет ее способность уменьшать уровень помех, создаваемых во внешней среде или на внутренних проводниках самого кабеля. Помехоустойчивость линии зависит от типа используемой физической среды, а также от экранирующих и подавляющих помехи средств самой линии. Наименее помехоустойчивыми являются радиолинии, хорошей устойчивостью обладают кабельные линии и отличной — волоконно-оптические линии, малочувствительные к внешнему электромагнитному излучению. Обычно для уменьшения помех, появляющихся из-за внешних электромагнитных полей, проводники экранируют и/или скручивают. Параметры, характеризующие помехоустойчивость, относятся к параметрам влияния линии связи.

Первичными параметрами влияния медного кабеля являются электрическая и магнитная связь. Электрическая связь определяется отношением наведенного тока в цепи, подверженной влиянию, к напряжению, действующему во влияющей цепи. Магнитная связь — это отношение электродвижущей силы, наведенной в цепи, подверженной влиянию, к току во влияющей цепи. Результатом электрической и магнитной связи являются наведенные сигналы (наводки) в цепи, подверженной влиянию. Существует несколько различных параметров, характеризующих устойчивость кабеля к наводкам.

Перекрестные наводки на ближнем конце (Near End Cross Talk, NEXT) определяют устойчивость кабеля в том случае, когда наводка образуется в результате действия сигнала, генерируемого передатчиком, подключенным к одной из соседних пар на том же конце кабеля, на котором работает подключенный к подверженной влиянию паре приемник (рис. 5.2). Показатель NEXT, выраженный в децибелах, равен 10 lg

$P_{вых}/P_{нав}$, где $P_{вых}$ – мощность выходного сигнала, $P_{нав}$ — мощность наведенного сигнала.

Перекрестные наводки на дальнем конце (Far End Cross Talk, FEXT) позволяют оценить устойчивость кабеля к наводкам для случая, когда передатчик и приемник подключены к разным концам кабеля. Очевидно, что этот показатель должен быть лучше, чем NEXT, так как до дальнего конца кабеля сигнал приходит ослабленный затуханием каждой пары.

Рис. 5.3. Переходное затухание

Показатели NEXT и FEXT обычно используются применительно к кабелю, состоящему из нескольких витых пар, так как в этом случае взаимные наводки одной пары на другую могут достигать значительных величин. Для одинарного коаксиального кабеля (то есть состоящего из одной экранированной жилы) этот показатель не имеет смысла, а для двойного коаксиального кабеля он также не применяется вследствие высокой степени защищенности каждой жилы. Оптические волокна также не создают сколько-нибудь заметных помех друг для друга.

В связи с тем, что в некоторых новых технологиях используется передача данных одновременно по нескольким витым парам, в последнее время стали применяться также показатели перекрестных наводок с приставкой PS *(PowerSUM),* такие как PS NEXT и PS FEXT. Эти показатели отражают устойчивость кабеля к суммарной мощности перекрестных наводок на одну из пар кабеля от всех остальных передающих пар.

Применяется также такой практически важный показатель, как защищенность кабеля (ACR). Защищенность определяется как разность между уровнями полезного сигнала и помех. Чем больше значение защищенности кабеля, тем в соответствии с формулой Шеннона с потенциально более высокой скоростью можно передавать данные по этому кабелю.

Достоверность передачи данных характеризует вероятность искажения для каждого передаваемого бита данных. Иногда этот же показатель называют *интенсивностью битовых ошибок (Bit Error Rate, BER).* Величина BER для каналов связи без дополнительных средств защиты от ошибок (например, самокорректирующихся кодов или протоколов с повторной передачей искаженных кадров) составляет, как правило, 10^{-4} – 10^{-6}, в оптоволоконных линиях связи — 10^{-9}. Значение достоверности передачи данных, например, в 10^{-4} говорит о том, что в среднем из 10 000 бит искажается значение одного бита.

Искажения бит происходят как из-за наличия помех на линии, так и по причине искажений формы сигнала ограниченной полосой пропускания линии.

Поэтому для повышения достоверности передаваемых данных нужно повышать степень помехозащищенности линии, снижать уровень перекрестных наводок в кабеле, а также использовать более широкополосные линии связи.

3. Полоса пропускания

Полоса пропускания — это еще одна вторичная характеристика, которая, с одной стороны, непосредственно зависит от затухания, а с другой стороны, прямо влияет на такой важнейший показатель линии связи, как максимально возможная скорость передачи информации.

Полоса пропускания (bandwidth) — это непрерывный диапазон частот, для которого затухание не превышает некоторый заранее заданный предел. То есть полоса пропускания определяет диапазон частот синусоидального сигнала, при которых этот сигнал передается по линии связи без значительных искажений (часто граничными частотами считаются частоты, на которых мощность выходного сигнала уменьшается в два раза по отношению к входному, что соответствует затуханию в -3 дБ).

Ширина полосы пропускания в наибольшей степени влияет на максимально возможную скорость передачи информации по линии связи. Именно этот факт нашел отражение в английском эквиваленте рассматриваемого термина (width — ширина).

Таким образом, амплитудно-частотная характеристика, полоса пропускания и затухание являются универсальными характеристиками, и их знание позволяет сделать вывод о том, как через линию связи будут передаваться сигналы любой формы.

q Полоса пропускания зависит от типа линии и ее протяженности.

4. Пропускная способность

4.1. Определение пропускной способности

Пропускная способность (количество бит информации, передаваемое в единицу времени) и достоверность передачи данных (вероятность доставки неискаженного бита или же вероятность искажения бита) интересуют разработчика компьютерной сети в первую очередь, поскольку эти характеристики прямо влияют на производительность и надежность создаваемой сети.

Пропускная способность и достоверность передачи данных зависят, с одной стороны, от характеристик физической среды, а с другой — определяются характеристиками способа передачи данных. Следовательно, нельзя говорить о пропускной способности линии связи, до того как для нее определен протокол

физического уровня. Например, поскольку для цифровых линий всегда определен протокол физического уровня, задающий битовую скорость передачи данных, то для них всегда известна и пропускная способность — 64 кбит/с, 2 Мбит/с и т. п.

В тех же случаях, когда только предстоит определить, какой из множества существующих протоколов можно использовать на данной линии, очень важными являются остальные характеристики линии, такие как полоса пропускания, перекрестные наводки, помехоустойчивость и другие характеристики.

Пропускная способность (throughput) линии характеризует максимально возможную скорость передачи данных по линии связи. Пропускная способность измеряется в битах в секунду (бит/с), а также в производных единицах, таких как килобит в секунду (кбит/с), мегабит в секунду (Мбит/с), гигабит в секунду (Гбит/с) и т. д.

Пропускная способность линии связи зависит не только от ее характеристик, таких как затухание и полоса пропускания, но и от спектра передаваемых сигналов. Если значимые гармоники сигнала (то есть те гармоники, амплитуды которых вносят основной вклад в результирующий сигнал) попадают в полосу пропускания линии, то такой сигнал будет хорошо передаваться данной линией связи и приемник сможет правильно распознать информацию, отправленную по линии передатчиком (рис. 5.4, а). Если же значимые гармоники выходят за границы полосы пропускания линии связи, то сигнал будет значительно искажаться, приемник будет ошибаться при распознавании информации, а значит, информация не сможет передаваться с заданной пропускной способностью (рис. 5.4, *б).*

Рис. 5.4. Соответствие между полосой пропускания линии связи и спектром сигнала

Выбор способа представления дискретной информации в виде сигналов, подаваемых на линию связи, называется *физическим,* или *линейным, кодированием.* От выбранного способа кодирования зависит спектр сигналов и, соответственно, пропускная способность линии. Таким образом, для одного способа кодирования линия может обладать одной пропускной способностью, а для другого — другой. Например, витая пара категории 3 может передавать данные с пропускной способностью 10 Мбит/с при способе кодирования стандарта физического уровня 10Base-T и 33 Мбит/с при способе кодирования стандарта 100Base-T4. В примере, приведенном на рис. 5.4, принят следующий способ кодирования: логическая 1 представлена на линии положительным потенциалом, а логический 0 — отрицательным.

Теория информации говорит, что любое различимое и непредсказуемое изменение принимаемого сигнала несет в себе информацию. В соответствии с этим прием синусоиды, у которой амплитуда, фаза и частота остаются неизменными, информации не несет, так как изменение сигнала хотя и

происходит, но является хорошо предсказуемым. Аналогично, не несут в себе информации импульсы на тактовой шине компьютера, так как их изменения также постоянны во времени. А вот импульсы на шине данных предсказать заранее нельзя, поэтому они переносят информацию между отдельными блоками или устройствами компьютера.

Большинство способов кодирования используют изменение какого-либо параметра периодического сигнала — частоты, амплитуды и фазы синусоиды или же знак потенциала последовательности импульсов. Периодический сигнал, параметры которого изменяются, называют *несущим сигналом* или *несущей частотой,* если в качестве такого сигнала используется синусоида.

Если сигнал изменяется так, что можно различить только два его состояния, то любое его изменение будет соответствовать наименьшей единице информации — биту. Если же сигнал может иметь более двух различимых состояний, то любое его изменение будет нести несколько битов информации.

Количество изменений информационного параметра несущего периодического сигнала в секунду измеряется в *бодах (baud).* Период времени между соседними изменениями информационного сигнала называется тактом работы передатчика.

Пропускная способность линии в битах в секунду в общем случае не совпадает с числом бод. Она может быть как выше, так и ниже числа бод, и это соотношение зависит от способа кодирования.

Если сигнал имеет более двух различимых состояний, то пропускная способность в битах в секунду будет выше, чем число бод. Например, если информационными параметрами являются фаза и амплитуда синусоиды, *причем различаются* 4 состояния фазы в 0, 90, 180 и 270° и два значения амплитуды сигнала, то информационный сигнал может иметь 8 различимых состояний. В этом случае модем, работающий со скоростью 2400 бод (с тактовой частотой 2400 Гц), передает информацию со скоростью 7200 бит/с, так как при одном изменении сигнала передается три бита информации.

При использовании сигналов с двумя различимыми состояниями может наблюдаться обратная картина. Это часто происходит потому, что для надежного распознавания приемником пользовательской информации каждый бит в последовательности кодируется путем нескольких изменений информационного параметра несущего сигнала. Например, при кодировании единичного значения бита импульсом положительной полярности, а нулевого значения бита импульсом отрицательной полярности физический сигнал дважды изменяет свое состояние при передаче каждого бита. При таком кодировании пропускная способность линии в два раза ниже, чем число бод, передаваемое по линии.

На пропускную способность линии оказывает влияние не только физическое, но и логическое кодирование. *Логическое кодирование* выполняется до физического кодирования и подразумевает замену битов исходной информации новой последовательностью битов, несущей ту же информацию, но обладающей, кроме этого, дополнительными свойствами, например возможностью для приемной стороны обнаруживать ошибки в принятых данных. Сопровождение каждого байта исходной информации одним битом четности — это пример очень часто применяемого способа логического кодирования при передаче данных с помощью модемов. Другим примером логического кодирования может служить шифрование данных, обеспечивающее их конфиденциальность при передаче через общественные каналы связи. При логическом кодировании чаще всего исходная последовательность бит заменяется более длинной последовательностью, поэтому пропускная способность канала по отношению к полезной информации при этом уменьшается.

4.2. Связь между пропускной способностью и полосой пропускания линии

Чем выше частота несущего периодического сигнала, тем больше информации в единицу времени передается по линии и тем выше пропускная способность линии при фиксированном способе физического кодирования. Однако, с другой стороны, с увеличением частоты периодического несущего сигнала увеличивается и ширина спектра этого сигнала, то есть разность между максимальной и минимальной частотами того набора синусоид, которые в сумме дадут выбранную для физического кодирования последовательность сигналов. Линия передает этот спектр синусоид с теми искажениями, которые определяются ее полосой пропускания. Чем больше несоответствие между полосой пропускания линии и шириной спектра передаваемых информационных сигналов, тем больше сигналы искажаются и тем вероятнее ошибки в распознавании информации принимающей стороной, а значит, скорость передачи информации на самом деле оказывается меньше, чем можно было предположить.

Связь между полосой пропускания линии и ее *максимально возможной пропускной способностью,* вне зависимости от принятого способа физического кодирования, установил Клод Шеннон:

$$C = F \log_2 (1+P_c/P_ш).$$

Здесь C — максимальная пропускная способность линии в битах в секунду, F — ширина полосы пропускания линии в герцах, $P_с$ — мощность сигнала, $P_ш$ — мощность шума.

Из этого соотношения видно, что хотя теоретического предела пропускной способности линии с фиксированной полосой пропускания не существует, на практике такой предел имеется. Действительно, повысить пропускную способность линии можно за счет увеличения мощности передатчика или же уменьшения мощности шума (помех) на линии связи. Обе эти составляющие поддаются изменению с большим трудом. Повышение мощности передатчика ведет к значительному увеличению его габаритов и стоимости. Снижение уровня шума требует применения специальных кабелей с хорошими защитными экранами, что весьма дорого, а также снижения шума в передатчике и промежуточной аппаратуре, чего достичь весьма не просто. К тому же влияние мощностей полезного сигнала и шума на пропускную способность ограничено логарифмической зависимостью, которая растет далеко не так быстро, как прямопропорциональная. Так, при достаточно типичном исходном отношении мощности сигнала к мощности шума в 100 раз повышение мощности передатчика в два раза даст только 15 % увеличения пропускной способности линии.

Близким по сути к формуле Шеннона является другое соотношение, полученное Найквистом, которое также определяет максимально возможную пропускную способность линии связи, но без учета шума на линии:

$C = 2F \log_2 M$.

Здесь *M* — количество различимых состояний информационного параметра.

Если сигнал имеет два различимых состояния, то пропускная способность равна удвоенному значению ширины полосы пропускания линии связи (рис. 5.5, *а).* Если же передатчик использует более двух устойчивых состояний сигнала для кодирования данных, то пропускная способность линии повышается, так как за один такт работы передатчик передает несколько битов исходных данных, например два бита при наличии четырех различимых состояний сигнала (рис. 5.5, *б).*

Рис. 5.5. Повышение скорости передачи за счет дополнительных состояний сигнала

Хотя формула Найквиста явно не учитывает наличие шума, косвенно его влияние отражается в выборе количества состояний информационного сигнала. Для повышения пропускной способности канала хотелось бы увеличить это количество до значительных величин, но на практике мы не можем этого сделать из-за шума на линии.

Приведенные соотношения дают предельное значение пропускной способности линии, а степень приближения к этому пределу зависит от конкретных методов физического кодирования, рассматриваемых ниже, а также мощности шума, то есть различного рода помех.

Передача сигнала по кабелю. Методы доступа.

Метод доступа -это набор правил, которые определяют, как компьютер должен отправлять и принимать данные по сетевому кабелю.
В сети несколько компьютеров должны иметь совместный доступ к кабелю. Однако, если два компьютера попытаются одновременно передавать данные, их сигналы будут мешать©друг другу и данные будут испорчены. Это называется «коллизия».
Чтобы передать данные по сети от одного пользователя к другому или получит с сервера, должен быть способ поместить данные в кабель без столкновения©с уже передаваемыми по нему данными, принять данные с достаточной степенью уверенности в том, что при передаче он были повреждены в результате коллизии.
Все сетевые компьютеры должны использовать один и тот же метод доступа, иначе произойдет сбой сети. Отдельные компьютеры, чьи методы будут доминировать, не дадут остальным осуществить передачу. Методы доступа служат для предотвращения одновременного доступа к кабе нескольких компьютеров, упорядочивая передачу и прием данных по сети и гарантируя, что в каждый момент времени только один компьютер может работать на передачу.
Существует три способа предотвратить одновременную попытку использовать кабель:

- Множественный доступ с контролем несущей:
    - с обнаружением коллизий;
    - с предотвращением коллизий.
- Доступ с передачей маркера. Только компьютер, получивший маркер, может передавать данные.
- Доступ по приоритету запроса.

Множественный доступ с контролем несущей и обнаружением коллизий
При множественном доступе с контролем несущей и обнаружением коллизий (сокращенно CSMA/CD) все компьютеры в сети - и клиенты, и серверы © «прослушивают» кабель,стремясь обнаружить передаваемые данные (т.е. трафик).

1. Компьютер «понимает», что кабель свободен (т.е. трафик отсутствует).

2. Компьютер может начать передачу данных.
3. Пока кабель не освободится (в течение передачи данных), ни один из сетевых компьютеров не может вести передачу.

В случае коллизии компьютеры приостанавливают передачу на случайный интервал времени, а затем вновь стараются отправить пакеты.
В то же время способность обнаружить коллизии - причина, которая ограничивает область действия метода. Из-за ослабления сигнала при расстояниях свыше 2500 м (1,5 мили) механизм обнаружения коллизий не эффективен. Если расстояние до передающего компьютера превышает это ограничение, некоторые компьютеры могут не «услышать»©его и начнут передачу данных, что приведет к коллизии и разрушению пакетов данных.
CSMA/CD известен как состязательный метод, поскольку сетевые компьютеры конкурируют между собой за право передавать данные. Он кажется достаточно громоздким, но современные реализации CSMA/CD настолько быстры, что пользователи даже не задумываются над тем, что применяют состязательный метод доступа.
Чем больше компьютеров в сети, тем интенсивнее сетевой трафик. При интенсивном трафике число коллизий возрастает, а это приводит к замедлению сети (уменьшению ее пропускной способности). Поэтому в некоторых ситуациях метод CSMA/CD может оказаться недостаточно быстрым. После каждой коллизии обоим компьютерам приходится возобновлять передачу, Если сеть очень загружена, повторные попытки опять могут привести к коллизиям, но уже с другими компьютерами. Теперь уже четыре компьютера (два от первой неудачной попытки и два от второй неудачной попытки первых) будут возобновлять передачу. Результат может оказаться тем же, что и в предыдущем случае, только пострадавших компьютеров станет еще больше. Такое лавинообразное нарастание вторных передач может парализовать работу всей сети. Вероятность возникновения подобной ситуации зависит от числа пользователе пытающихся получить доступ к сети, и приложений, с которыми они работают.
Сеть с методом доступа CSMA/CD, обслуживающая многих пользователей, которые работают с несколькими системами управления базами данных (критическое числоло пользователей зависит от аппаратных компонентов, кабельной системы и сетев программного обеспечения), может практически остановиться из-за чрезмерного сетвого трафика.

Множественный доступ с контролем несущей и предотвращением коллизий
Множественный доступ с контролем несущей и предотвращением коллизий (сок щенно CSMA/CA) основан на том, что каждый компьютер перед передачей данных в сеть сигнализирует о своем намерении, поэтому остальные компьютеры узнают о готовящейся передаче и могут избежать коллизий. Однако широковещательное оповещение увеличивает общий трафик сети уменьшает ее пропускную способность. Поэтому CSMA/CA работает медленнее, чем CSMA/CD.

Доступ с передачей маркера

Суть доступа с передачей маркера заключается в следующем: пакет особого типа, ма кер (token), циркулирует по кольцу от компьютера к компьютеру. Чтобы послать данные в сеть, любой из компьютеров сначала должен дождаться прихода свободного маркера и захватить его.
Когда какой-либо компьютер «наполнит» маркер своей информацией и пошлет его по сетевому кабелю, другие компьютеры уже не могут передавать данные. Поскольку в каждый момент времени только один компьютер будет использовать маркер, то в сети не возникнет ни состязания, ни коллизий, ни временных пауз.

Доступ по приоритету запроса

Доступ по приоритету запроса - относительно новый метод доступа, разработана для стандарта сети Ethernet со скоростью передачи данных 100 Мбит/с 1OOVG-AnyLAN. Он стандартизован IEEE в категории 802.12. Этот метод доступа основан на том, что все сети 1OOVG-AnyLAN строятся только из концентраторов и оконечных узлов. Концентраторы управляют доступом к кабелю последовательно опрашивая все узлы в сети и выявляя запросы на передачу. Концентратор, должен знать все адреса, связи и узлы и проверять их работоспособность. Оконечным узлом, в соответствии со спецификацией 1OOVG-AnyLAN, может быть компьютер, мост, маршрутизатор или коммутатор.
Как и при CSMA/CD, при доступе по приоритету запроса два компьютера могут бороться за право передать данные. Однако только последний метод реализует схему, по которой определенные типы данных - если возникло состязание, - имеют соответствующий приоритет. Получив одновременно два запроса, концентратор вначале отдаст предпочтение запросу с более высоким приоритетом. Если запросы имеют одинаковый приоритет, они будут обслужены в произвольном порядке. В сетях с использованием доступа по приоритету запроса каждый компьютер может одновременно передавать и принимать данные, поскольку для этих сетей разработана специальная схема кабеля. В них применяется восьмипроводной кабель, по каждой паре проводов сигналы передаются с частотой 25 МГц.
В сетях, где реализован доступ по приоритету запроса, связь устанавливается только между компьютером-отправителем, концентратором и компьютером-получателем. Такой вариант более эффективен, чем CSMA/CD, где передача осуществляется для всей сети. В среде с доступом по приоритету запроса каждый концентратор ©«знает»©только те оконечные узлы и репитеры, которые непосредственно подключены к нему, тогда как в среде с CSMA/CD каждый концентратор «знает» адреса всех узлов сети.

Лекция 12. Адресация в IP-сетях

Принятый в IP-сетях способ адресации узлов обеспечивает хорошую масштабируемость, которая позволяет однозначно идентифицировать множество сетевых интерфейсов.

1. Типы адресов стека TCP/IP

В стеке TCP/IP используются три типа адресов:

- q локальные, или аппаратные, адреса, используемые для адресации узлов в пределах подсети;
- q сетевые, или IP-адреса, используемые для однозначной идентификации узлов в пределах всей составной сети;
- q доменные имена — символьные идентификаторы узлов, к которым часто обращаются пользователи.

В общем случае сетевой интерфейс может иметь одновременно один или несколько локальных адресов и один или несколько сетевых адресов, а также одно или несколько доменных имен.

Если подсеть использует одну из базовых технологий LAN — Ethernet, FDDI, Token Ring, — то аппаратным адресом является MAC-адрес. Если в составную сеть TCP/IP входят подсети, построенные на основе более сложных технологий, например, Novell Netware, такими адресами являются IPX-адреса.

IP-адреса состоят из 4 байт и назначаются администратором при конфигурировании компьютеров и маршрутизаторов. IP-адрес состоит из двух частей: номера сети и номера узла. Номер сети может быть выбран администратором произвольно либо назначен по рекомендации специального подразделения Интернета (Internet Network Information Center, InterNIC), если сеть должна работать как составная часть Интернета. Номер узла в протоколе IP назначается независимо от локального адреса узла. Каждый порт маршрутизатора имеет собственный IP-адрес. Конечный узел также может входить в несколько IP-сетей, в этом случае он тоже имеет несколько IP-адресов.

Символьные имена в IP-сетях называются доменными и строятся по иерархическому признаку. Составляющие полного символьного имени в IP-сетях разделяются точкой и перечисляются «снизу вверх», например, base2.zil.ru. В сетях TCP/IP используется специальная распределенная служба доменных имен (Domain Name System, DNS), которая устанавливает соответствие символьных и IP-адресов на основании создаваемых администраторами сети таблиц.

1.1. Формы записи IP-адреса

Наиболее употребляемой формой представления IP-адреса является запись в виде четырех чисел, представляющих значения каждого байта в десятичной форме и разделенных точками, например 128.10.2.30 . Этот же адрес может быть представлен в двоичном формате 10000000 00001010 00000010 00011110 , а также в шестнадцатеричном формате 80.0A.02.1D .

Для выделения из адреса назначения номера сети используются 2 подхода. Первый состоит в том, что всё 32-битовое поле адреса заранее делится на две части, в одной из которых размещается номер сети, а в другой — номер узла.

Второй подход основан на использовании маски, т. е. числа, которое используется в паре с IP-адресом. Двоичная запись маски содержит последовательность единиц в тех

разрядах, которые в IP-адресе интерпретируются как номер сети, и нулей – для номера узла.
Используется и смешанный подход, когда вводится несколько классов сетей и для каждого класса определены свои размеры.

1.2. Классы IP-адресов

Принадлежность IP-адреса к классу определяется значениями первых битов адреса.

Если адрес начинается с 0, то этот адрес относится к классу A, в котором под номер сети отводится один байт, а остальные три байта интерпретируются как номер узла в сети. Сети класса A имеют номера в диапазоне от 1 (00000001) до 126 (01111110). Номер 0 не используется, а номер 127 зарезервирован для специальных целей. Сетей класса A немного, зато количество узлов в них может достигать 2^{24}, то есть 16 777 216 узлов.
Если первые два бита адреса равны 1 и 0, то адрес относится к классу B. В адресах класса B под номер сети и под номер узла отводится по два байта. Сети, имеющие номера в диапазоне от 128.0 (10000000 00000000) до 191.255 (10111111 11111111), называются сетями класса B. Сетей класса B больше, чем сетей класса A, но размеры их меньше, максимальное количество узлов в них составляет 2^{16} (65 536).
Если адрес начинается с последовательности битов 110, то это адрес класса C. В этом случае под номер сети отводится 24 бита, а под номер узла — 8 бит. Сети класса C наиболее распространены, но число узлов в них ограничено значением 2^8 (256) узлов.

Если адрес начинается с последовательности 1110, то он является адресом класса D и обозначает особый, групповой адрес (multicast), который идентифицирует группу узлов. Интерфейс, входящий в группу, получает наряду с индивидуальным IP-адресом еще один групповой адрес. Если при отправке пакета в качестве адреса назначения указан адрес класса D, то такой пакет должен быть доставлен всем узлам, которые входят в группу. Если адрес начинается с последовательности 11110, то это значит, что данный адрес относится к классу E. Адреса этого класса зарезервированы для будущих применений.

Класс	Первые биты	Наименьший номер сети	Наибольший номер сети	Максимальное число узлов в сети
A	0	1.0.0.0	126.0.0.0	2^{24}
B	10	128.0.0.0	191.255.0.0	2^{16}
C	110	192.0.1.0	223.255.255.0	2^{8}
D	1110	224.0.0.0	239.255.255.255	Multicast
E	11110	240.0.0.0	247.255.255.255	Зарезервирован

Большие сети получают адреса класса A, средние — класса B, а небольшие — класса C.

1.3. Особые IP-адреса

В протоколе IP существует несколько соглашений об особой интерпретации IP-адресов.

- q Если весь IP-адрес состоит только из двоичных нулей, то он обозначает адрес того узла, который сгенерировал этот пакет (этот режим используется только в некоторых сообщениях ICMP).
- q Если в поле номера сети стоят только нули, то по умолчанию считается, что узел назначения принадлежит той же самой сети, что и узел, который отправил пакет.
- q Если все двоичные разряды IP-адреса равны 1, то пакет с таким адресом назначения должен рассылаться всем узлам, находящимся в той же сети, что и источник этого пакета. Такая рассылка называется ограниченным широковещательным сообщением (limited broadcast). Ограниченность в данном случае означает, что пакет не выйдет за границы маршрутизатора ни при каких условиях.
- q Если в поле номера узла назначения стоят только единицы, то пакет, имеющий такой адрес, рассылается всем узлам сети с заданным номером сети. Например, пакет с адресом 192.190.21.255 доставляется всем узлам сети класса C с номером 192.190.21.0. Такая рассылка называется широковещательным сообщением (broadcast).

Специальные адреса, состоящие из последовательностей нулей, могут быть использованы только в качестве адреса отправителя, а адреса, состоящие из последовательностей единиц, — только в качестве адреса получателя.
При назначении адресов конечным узлам и маршрутизаторам необходимо учитывать ограничения, которые вносятся особым назначением некоторых IP-адресов. Так, ни номер сети, ни номер узла не может состоять только из одних двоичных единиц или только из одних двоичных нулей. Отсюда следует, что максимальное количество узлов, приведенное в таблице для сетей каждого класса, на практике должно быть уменьшено на 2. Например, в адресах класса C под номер узла отводится 8 бит, которые позволяют задать 256 номеров: от 0 до 255. Однако на практике максимальное число узлов в сети класса C не может превышать 254, так как адреса 0 и 255 имеют специальное назначение. Из этих же соображений следует, что конечный узел не может иметь адрес типа 98.255.255.255, поскольку номер узла в этом адресе класса A состоит из одних двоичных единиц.
Особый смысл имеет IP-адрес, первый октет которого равен 127. Он используется для тестирования программ и взаимодействия процессов в пределах одной машины. Когда программа посылает данные по IP-адресу 127.0.0.1, то образуется как бы «петля». Данные не передаются по сети, а возвращаются модулям верхнего уровня, как только что принятые. Поэтому в IP-сети запрещается присваивать сетевым интерфейсам IP-адреса, начинающиеся с числа 127. Этот адрес имеет название loopback.
В протоколе IP нет понятия широковещательности в том смысле, в котором оно используется в протоколах канального уровня локальных сетей, когда данные должны быть доставлены абсолютно всем узлам. Как ограниченный широковещательный IP-адрес, так и широковещательный IP-адрес имеют пределы распространения в интерсети — они ограничены либо сетью, к которой принадлежит узел-источник пакета, либо сетью, номер которой указан в адресе назначения. Поэтому деление сети с помощью маршрутизаторов на части локализует широковещательный шторм пределами одной из подсетей просто потому, что нет способа адресовать пакет одновременно всем узлам всех сетей составной сети.
Уже упоминавшаяся форма группового IP-адреса — multicast — означает, что данный пакет должен быть доставлен сразу нескольким узлам, которые образуют группу с номером, указанным в поле адреса. Один и тот же узел может входить в несколько групп. Члены какой-либо группы multicast не обязательно должны принадлежать одной сети. В общем случае они могут распределяться по различным сетям, расстояние между которыми измеряется произвольным количеством хопов. Групповой адрес не делится на поля номера сети и узла и обрабатывается маршрутизатором особым образом. Основное назначение адресов multicast — распространение информации по схеме «один ко многим». Хост, желающий передать одну и ту же информацию многим абонентам, использует для этого специальный протокол IGMP (Internet Group Management Protocol). Чтобы маршрутизаторы могли автоматически распространять пакеты с адресом multicast по составной сети, необходимо использовать в конечных маршрутизаторах модифицированные протоколы обмена маршрутной информацией, такие как, например, MOSPF (Multicast OSPF), multicast-аналог OSPF.

1.4. Использование масок при IP-адресации

Снабжая каждый IP-адрес маской, можно отказаться от понятий классов адресов и сделать систему адресации более гибкой. Например, если адрес 185.23.44.206 ассоциировать с маской 255.255.255.0, то номером сети будет 185.23.44.0 (адрес класса C), а не 185.23.0.0 (адрес класса B), как это определено системой классов.
В масках количество единиц в последовательности, определяющей границу номера сети, не обязательно должно быть кратным 8, чтобы повторять деление адреса на байты.
Для стандартных классов сетей маски имеют следующие значения:

- q класс B - 11111111. 11111111. 00000000. 00000000 (255.255.0.0);
- q класс C - 11111111. 11111111. 11111111. 00000000 (255.255.255.0).
- q класс A - 11111111. 00000000. 00000000. 00000000 (255.0.0.0);

Для записи масок могут использоваться и другие форматы, например, шестнадцатеричный код FF.FF.00.00 — маска для адресов класса B или обозначение 185.23.44.206/16 — эта запись говорит о том, что маска для этого адреса содержит 16 единиц или что в указанном IP-адресе под номер сети отведено 16 двоичных разрядов (185.23.0.0).
Механизм масок широко распространен в IP-маршрутизации, причем маски могут использоваться для самых разных целей. С их помощью администратор может разбивать свою сеть на несколько других, не требуя от поставщика услуг дополнительных номеров сетей (операция subnetting). На основе этого же механизма поставщики услуг могут объединять адресные пространства нескольких сетей путем введения так называемых «префиксов» с целью уменьшения объема таблиц маршрутизации и повышения за счет этого производительности маршрутизаторов — такая операция называется supernetting.

2. Порядок назначения IP-адресов

У каждой подсети в пределах составной сети должен быть собственный уникальный номер, следовательно, процедура распределения номеров должна быть централизованной. Аналогично централизованный характер должна иметь и процедура распределения номеров узлов в пределах каждой подсети.

2.1. Централизованное распределение адресов

Главным органом регистрации глобальных адресов в Интернете с 1998 года является ICANN (Internet Corporation for Assigned Names and Numbers). Региональные отделы этой организации выделяют блоки адресов сетей крупным поставщикам услуг, те, в свою очередь присваивают их своим клиентам, среди которых могут быть и более мелкие поставщики услуг.
В автономной сети могут использоваться произвольные IP-адреса, уникальные в пределах этой сети. В стандартах Интернета определено несколько адресов,

рекомендуемых для автономного использования: в классе A — это сеть 10.0.0.0, в классе B — это диапазон из 16 номеров сетей 172.16.0.0-172.31.0.0, в классе C — это диапазон из 255 сетей 192.168.0.0-192.168.255.0.
Уже сравнительно давно наблюдается дефицит IP-адресов, связанный не только с ростом сетей, но и нерациональным использованием адресного пространства. Для смягчения проблемы дефицита адресов применяются разные меры:

- q переход на новую версию IPv6, в которой резко расширяется адресное пространство за счет использования 6-байтных адресов;
- q в текущей версии IPv4 применяется технология бесклассовой междомеипой маршрутизации (Classless Inter-Domain Routing, CIDR), основанная на масках.

2.2. Автоматизация процесса назначения IP-адресов

выполняется с помощью протокола Dynamic Host Configuration Protocol (DHCP).
DHCP может поддерживать автоматическое динамическое распределение адресов, а также более простые способы ручного и автоматического статического назначения адресов. Протокол DHCP работает в соответствии с моделью клиент-сервер. Предполагается, что DHCP-клиент и DHCP-сервер находятся в одной IP-сети.
При ручной процедуре назначения статических адресов администратор сообщает DHCP-серверу информацию о жестком соответствии IP-адресов физическим адресам или другим идентификаторам клиентов. DHCP-сервер, пользуясь этой информацией, всегда выдает определенному клиенту один и тот же назначенный ему администратором адрес.
При автоматическом статическом способе DHCP-сервер самостоятельно выбирает клиенту произвольный IP-адрес из пула наличных IP-адресов. Границы пула задает администратор при конфигурировании DHCP-сервера. Постоянное соответствие между идентификатором клиента и его IP-адресом устанавливается в момент первого назначения сервером адреса клиенту.
При динамическом распределении адресов DHCP-сервер выдает адрес клиенту на ограниченное время, называемое временем аренды (lease duration), что дает возможность впоследствии повторно использовать этот IP-адрес для назначения другому компьютеру.
DHCP-сервер может назначить клиенту не только IP-адрес, но и другие параметры стека TCP/IP, необходимые для его эффективной работы, например, маску, IP-адрес маршрутизатора по умолчанию, IP-адрес сервера DNS, доменное имя компьютера и т. п.
Динамическое задание IP-адресов, кроме очевидных преимуществ, влечет за собой и проблемы:

- Снижается надежность системы из-за наличия центрального элемента — сервера DHCP.
- Возникают сложности при преобразовании символьного доменного имени в IP-адрес.
- Трудно осуществлять удаленное управление и автоматический мониторинг интерфейса, если в качестве его идентификатора выступает динамически изменяемый IP-адрес.

- При динамическом назначении адресов усложняется фильтрация пакетов по IP-адресам.

Все эти проблемы в той или иной степени находят решение. Так, для снижения риска выхода сети из строя из-за отказа сервера DHCP в сети ставят резервный сервер DHCP. А для серверов, к которым пользователи часто обращаются по символьному имени, назначают статические IP-адреса, оставляя динамические только для клиентских компьютеров. Есть примеры успешных подходов и к решению остальных задач.

3. Протоколы разрешения адресов

3.1. Отображение IP-адресов на локальные адреса

Для определения локального адреса по IP-адресу используется протокол разрешения адресов (Address Resolution Protocol, ARP).

При конфигурирования сети каждый интерфейс получает свои IP-адрес и MAC-адрес и на нём поддерживается отдельная ARP-таблица, определяющая соответствие между IP-адресами и MAC-адресами других узлов данной подсети. Первоначально, при включении компьютера или маршрутизатора в сеть все его ARP-таблицы пусты.

Работа ARP начинается с просмотра ARP-таблицы интерфейса, на который поступил IP-пакет. Исходящий IP-пакет, для которого нет локального адреса в ARP-таблице, запоминается в буфере, а протокол ARP формирует ARP-запрос и рассылает широковещательно.

Все интерфейсы подсети получают ARP-запрос и сравнивают указанный там IP-адрес с собственным. Интерфейс, в котором произошло совпадение, формирует ARP-ответ, указывая в нем свой IP-адрес и свой локальный адрес, а затем отправляет его уже направленно на интерфейс, пославший запрос.

Если в сети нет машины с искомым IP-адресом, то ARP-ответа не будет. Протокол IP уничтожает IP-пакеты, направляемые по этому адресу.

При получении ответа найденный MAC-адрес помещается в заголовок кадра Ethernet, ожидавшего отправления IP-пакета.

Найденное соответствие между IP-адресом и MAC-адресом записывается в ARP-таблицу соответствующего интерфейса. Теперь при повторной отправке пакета по тому же IP-адресу вместо широковещательного запроса сначала будет анализироваться ARP-таблица.

Записи могут быть динамическими или статическими. Статические записи создаются вручную с помощью утилиты arp и не имеют срока устаревания.

Динамические записи должны периодически обновляться. Если запись не обновлялась в течение определенного времени (порядка нескольких минут), то она исключается из таблицы. Таким образом, в ARP-таблице содержатся записи не обо всех узлах сети, а только о тех, которые активно участвуют в сетевых операциях. Поскольку такой способ хранения информации называют кэшированием, ARP-таблицы иногда называют ARP-кэшем.

Совсем другой способ разрешения адресов используется в глобальных сетях, в которых не поддерживаются широковещательные сообщения. Здесь администратору сети чаще всего приходится вручную формировать и помещать на какой-либо сервер ARP-таблицы.
В то же время наметилась тенденция автоматизации работы протокола ARP и в глобальных сетях. Для этой цели среди всех маршрутизаторов глобальной сети выделяется специальный маршрутизатор, который ведет ARP-таблицу для всех остальных узлов и маршрутизаторов этой сети. При таком централизованном подходе для всех узлов и маршрутизаторов вручную нужно задать только IP-адрес и локальный адрес выделенного маршрутизатора, называемого ARP-сервером.
В некоторых случаях возникает обратная задача — нахождение IP-адреса по известному локальному адресу. Тогда в действие вступает реверсивный протокол ARP (Reverse Address Resolution Protocol, RARP).

3.2. Организация доменов и доменных имен

Для обращения к любому компьютеру в составной сети можно использовать его IP-адрес. Однако пользователи обычно предпочитают работать с символьными именами компьютеров.
В небольших локальных сетях могут использоваться плоские символьные имена. Для именования компьютеров в больших сетях применяются иерархические составные имена.
В стеке TCP/IP применяется доменная система имен, которая имеет иерархическую древовидную структуру.
Иерархия доменных имен аналогична иерархии имен файлов, принятой в файловых системах. В отличие от имен файлов запись доменного имени начинается с самой младшей составляющей, а заканчивается самой старшей. Составные части доменного имени отделяются друг от друга точкой.
Разделение имени на части позволяет разделить административную ответственность за назначение уникальных имен между различными людьми или организациями в пределах своего уровня иерархии. Разделение административной ответственности позволяет решить проблему образования уникальных имен без взаимных консультаций между организациями, отвечающими за имена одного уровня иерархии. Очевидно, что должна существовать одна организация, отвечающая за назначение имен верхнего уровня иерархии.
Совокупность имен, у которых несколько старших составных частей совпадают, образуют домен (domain) имен.
Если один домен входит в другой домен как его составная часть, то такой домен могут называть поддоменом (subdomain). Обычно поддомен называют по имени той его старшей составляющей, которая отличает его от других поддоменов. Имя поддомену назначает администратор вышестоящего домена. Хорошей аналогией домена является каталог файловой системы.
По аналогии с файловой системой в доменной системе имен различают краткие имена, относительные имена и полные доменные имена. Краткое имя — это имя конечного узла

сети. Относительное имя — это составное имя, начинающееся с некоторого уровня иерархии, но не самого верхнего. Например, wwwl.zil — это относительное имя. Полное доменное имя (fully qualified domain name, FQDN) включает составляющие всех уровней иерархии, начиная от краткого имени и кончая корневой точкой.
Корневой домен управляется центральными органами Интернета: IANA и InterNIC. Домены верхнего уровня назначаются для каждой страны, а также на организационной основе. Имена этих доменов должны следовать международному стандарту ISO 3166. Для обозначения стран используются трехбуквенные и двухбуквенные аббревиатуры, например, ru (Россия), uk (Великобритания), fin (Финляндия), us (Соединенные Штаты), а для различных типов организаций — следующие обозначения:

- com — коммерческие организации (например, microsoft.com);
- edu — образовательные организации (например, mit.edu);
- gov — правительственные организации (например, nsf.gov);
- org — некоммерческие организации (например, fidonet.org);
- net — организации поддержки сетей (например, nsf.net).

Каждый домен администрируется отдельной организацией, которая обычно разбивает свой домен на поддомены и передает функции администрирования этих поддоменов другим организациям. Чтобы получить доменное имя, необходимо зарегистрироваться в какой-либо организации, которой организация InterNIC делегировала свои полномочия по распределению имен доменов. В России такой организацией является РосНИИРОС, которая отвечает за делегирование имен поддоменов в домене ru.
Доменная система имен реализована в Интернете, но она может работать и как автономная система имен в любой крупной корпоративной сети, которая также использует стек TCP/IP, но не связана с Интернетом.

3.3. Система доменных имен DNS

Соответствие между доменными именами и IP-адресами может устанавливаться как средствами локального хоста, так и средствами централизованной службы. На раннем этапе развития Интернета на каждом хосте вручную создавался текстовый файл с известным именем hosts.txt. Этот файл состоял из некоторого количества строк, каждая из которых содержала одну пару «IP-адрес — доменное имя».
В настоящее время используется масштабируемая служба для разрешения имен — система доменных имен (Domain Name System, DNS). Служба DNS использует в своей работе протокол типа «клиент-сервер». В нем определены DNS-серверы и DNS-клиенты. DNS-серверы поддерживают распределенную базу отображений, а DNS-клиенты обращаются к серверам с запросами о разрешении доменного имени в IP-адрес. Служба DNS использует текстовые файлы, которые администратор подготавливает вручную. Однако служба DNS опирается на иерархию доменов, и каждый сервер службы DNS хранит только часть имен сети, а не все имена. При росте количества узлов в сети проблема масштабирования решается созданием новых доменов и поддоменов имен и добавлением в службу DNS новых серверов.

Для каждого домена имен создается свой DNS-сервер. Обычно сервер домена хранит только имена, которые заканчиваются на следующем ниже уровне иерархии по сравнению с именем домена. (Аналогично каталогу файловой системы, который содержит записи о файлах и подкаталогах, непосредственно в него «входящих».) Именно при такой организации службы DNS нагрузка по разрешению имен распределяется более-менее равномерно между всеми DNS-серверами сети. Каждый DNS-сервер кроме таблицы отображений имен содержит ссылки на DNS-серверы своих поддоменов. Эти ссылки связывают отдельные DNS-серверы в единую службу DNS. Ссылки представляют собой IP-адреса соответствующих серверов. Для обслуживания корневого домена выделено несколько дублирующих друг друга DNS-серверов, IP-адреса которых являются широко известными (их можно узнать, например, в InterNIC).

Процедура разрешения DNS-имени во многом аналогична процедуре поиска файловой системой адреса файла по его символьному имени. Для определения IP-адреса по доменному имени необходимо просмотреть все DNS-серверы, обслуживающие цепочку поддоменов, входящих в имя хоста, начиная с корневого домена. Существенным отличием является то, что файловая система расположена на одном компьютере, а служба DNS по своей природе является распределенной.

Существует две основные схемы разрешения DNS-имен.

В первом варианте работу по поиску IP-адреса координирует DNS-клиент, последовательно обращаясь к DNS-серверам, начиная с корневого. Такая схема взаимодействия называется нерекурсивной, или итеративной. Так как эта схема загружает клиента достаточно сложной работой, то она применяется редко.

Во втором варианте DNS-клиент запрашивает локальный DNS-сервер, обслуживающий поддомен, к которому принадлежит имя клиента. Если локальный DNS-сервер знает ответ, то он сразу же возвращает его клиенту. Это может соответствовать случаю, когда запрошенное имя входит в тот же поддомен, что и имя клиента, а также случаю, когда сервер уже узнавал данное соответствие для другого клиента и сохранил его в своем кэше. Если локальный сервер не знает ответ, то он выполняет итеративные запросы к корневому серверу и к нижним по иерархии. Получив ответ, он передает его клиенту. Такая схема называется косвенной, или рекурсивной.

Для ускорения поиска IP-адресов DNS-серверы широко применяют процедуру кэширования проходящих через них ответов. Чтобы служба DNS могла оперативно отрабатывать изменения, происходящие в сети, ответы кэшируются на определенное время — обычно от нескольких часов до нескольких дней.