10.02.15

Компьютерные сети: преимущества и недостатки.

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

Преимущества:

- Возможность совместного использования периферийных устройств.
- Повышение эффективности и скорости обработки информации группой сотрудников.
- Обеспечение совместного доступа к сети Интернет.
- Быстрое получение доступа к корпоративным хранилищам информации.

Недостатки:

- Всегда существует потенциальная угроза безопасности данных передаваемых по сетям.
- 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 БИС и основанные на них мини компьютеры. Необходимость их объединения для совместной работы привела к появлению первых локальных вычислительных сетей.

Локальные сети – объединения 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 не стандартные программно-аппаратные средства. Они могли соединять только те конкретные модели компьютеров для которых были разработаны. К середине 80-х годов постепенно сложились стандартные технологии объединения компьютеров в сеть. Это Ethernet, Arc Net, Token Ring, Token Bas и FDDI. Мощным стимулом для их внедрения послужили ПК. С одной стороны, они были достаточно мощными для работы сетевого ПО, а с другой 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, причём 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 семейству Ethernet относятся: классическая технология Ethernet 10 Мбит/с, а также Fast Ethernet 100 Мбит/с и Gigabit Ethernet 1000 Мбит/с.

Простые алгоритмы работы предопределили низкую стоимость оборудования Ethernet. Широкий диапазон иерархии 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, удалённых от него на большие расстояния. Терминалы соединялись с компьютерами через телефонные сети с помощью модемов. Затем появились системы, в которых на ряду с соединением типа «терминал-компьютер» были реализованы удалённые связи типа «компьютер-компьютер».

Глобальные сети – сети, которые объединяют территориально рассредоточенные компьютеры, находящиеся в разных городах и странах. Именно при построении глобальных сетей был впервые предложены и отработаны многие основные идеи и концепции современных сетей. Глобальные компьютерные сети очень много унаследовали от других более старых и распространённых 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. В конце 60-х годов в телефонных сетях стала применяться передача голоса в цифровой форме. Была разработана специальная технология презиохронной цифровой иерархии, которая предназначена для первичных сетей. Такие сети не предоставляют услуг конечным пользователям. Они – фундамент, на котором строятся скоростные цифровые каналы «точка-тире-точка». В конце 80-х годов появилась технология синхронно цифровой иерархии. Она расширила диапазон скоростей до 10Гбит/с, а следующая технология спектрального мультиплексирования до 100Гбит/с и даже нескольких Тбит/с.

Сближение локальных и глобальных сетей.

В конце 80-х появились отличия между локальными и глобальными сетями:

- Протяженность и качество линий связи.
- Сложность методов передачи данных.
- Скорость обмена данными.
- Разнообразие услуг и масштабируемость.

Постепенно различия между локальными и глобальными технологиями 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 надёжности вышли процедуры обеспечения гарантированной средней скорости доставки. Большой вклад в сближении локальных и глобальных сетей внесло доминирование протокола IP. Компьютерные глобальные сети существенно расширили набор своих услуг и догнали в этом отношении локальные сети. 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 (Ethernet 10G).

Сближение компьютерных и телекоммуникационных сетей.

К телекоммуникационным сетям относятся:

- Компьютерные сети
- Телефонные сети
- Радио сети
- Телевизионные сети

Во всех этих сетях в качестве ресурса, предоставляемого клиенту, выступает информация. Сближение компьютерных и телекоммуникационных сетей происходит по многим направлениям. Прежде всего наблюдается сближение видов услуг, предоставляемых клиентам. Первая попытка создания универсальной, так называемой мульти сервисной сети, способной оказывать различные услуги привела к появлению технологии цифровых сетей с интегральными услугами (ISDN). В настоящее время на роль глобальной мульти сервисной сети нового поколения претендует Интернет. В конечном результате он должен с одинаковым успехом поддерживать услуги: WWW, телефонии, архивов данных, видео данных, аудио и видео новостей и мультимедийной почты. Технологическое сближение сетей происходит на основе цифровой передачи информации различного типа, метода коммутации пакетов и программирования услуг. Дополнительные услуги телефонных сетей, такие как переадресация вызовов, телеголосование, могут создаваться с помощью интеллектуальных сетей, которые по своей сути являются компьютерной сетью и сервером, на котором программируется логика услуг. Пакетные методы коммутации постепенно вытесняют традиционные для телефонных сетей методы коммутации каналов даже при передаче голоса. Использование коммутации пакетов для одновременной передачи разнородного трафика сделало актуальной разработку новых методов обеспечения требуемого качества обслуживания. Эти методы призваны минимизировать для чувствительного трафика и одновременно гарантировать среднюю скорость и динамическую передачу трафика данных. Компьютерные сети используют транспортную инфраструктуру, созданную в рамках тех или иных телекоммуникационных сетей.

17.02.15

Особенности сетевых операционных систем.

В вычислительных сетях, связь между компьютерами осуществляется с помощью специальных периферийных устройств (сетевых адаптеров), которые соединяются каналами связи. Каждый компьютер работает под управлением собственной операционной системы. Взаимодействие между компьютерами сети происходит путём передачи сообщений через сетевые адаптеры и каналы связи. В качестве совместно используемых ресурсов выступают данные на дисках, а также 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 операционным системам. 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 удалённым ресурсам и передавать их по сети на нужный компьютер. Такие модули называют программами клиентами. Пара модулей «клиент – сервер» обеспечивает совместный доступ пользователей к определённому типу ресурсов. Обычно сетевая операционная система поддерживает несколько видов сетевых служб для своих пользователей: файловая, печати, электронной почты, удалённого доступа. Термины «клиент» и «сервер» используются и для обозначения соответствующих компьютеров сети.

Распределённые программы.

Это программы, которые состоят из нескольких взаимодействующих частей. Причём каждая часть, как правило, выполняется на отдельном компьютере сети. Сетевые службы относятся к системным распределённым программам. Кроме того, в сети могут выполняться распределённые пользовательские программы – приложения. Распределённое предложение также состоит из нескольких частей. Каждая из этих частей выполняет какую-то определённую законченную работу по решению прикладной задачи. Распределённые 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 распределёнными и целиком выполняются на одном компьютере сети. Тем не менее такие приложения могут использовать преимущество сети за счёт встроенных в операционную систему сетевых служб. Создание распределённых приложений имеет много преимуществ, но является делом сложным. Нужно решить множество проблем:

- На сколько частей разбить приложение.
- Какие функции возложить на каждую часть.
- Как организовать взаимодействие этих частей и так далее.

Поэтому до сих пор не все приложения являются распределёнными.

Простейшая логическая схема взаимодействия двух компьютеров.

Здесь происходит взаимодействие двух программ, выполняемых на каждом их компьютеров. Программа, работающая на одном, не может получить непосредственный доступ к ресурсам другого. 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 файла, расположенного на диске компьютера Б. Функции побайтовой передачи данных между компьютерами по линии связи выполняют сетевые адаптеры и их драйверы. Приложение А формирует сообщение запрос для приложения Б. В запросе указывается имя файла, тип операции, смещение и размер области файла, содержащей нужные данные. Приложение Б, получив сообщение обращается к периферийному устройству (диску). Считанные с диска данные приложение Б помещает в буферную область оперативной памяти и затем передаёт их по каналу связи компьютеру 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 удалённым файлам не рационально. Выгоднее создать специальный программный модуль, который будет выполнять функции формирования сообщения запросов к удалённой машине и приема результатов для всех приложений. Такой служебный модуль называют клиентом. На стороне компьютера Б должна работать другая специальная программа – сервер. Сервер постоянно ожидает поступление запросов на удалённый доступ к файлам. После получения такого запроса из сети сервер обращается к локальному файлу при помощи локальной операционной системы. Необходимой функцией клиента является способность отличить запрос к удалённому файлу от запроса к локальному. Иногда такие функции выделяют в отдельный программный модуль.

Задачи физической передачи данных по линиям связи.

При передаче данных по линиям связи используют кодирование данных. Кодирование осуществляется также и в вычислительной технике. Используют потенциальный или импульсный способ. Также существует особый способ – модуляция. При ней дискретная информация представляется синусоидальным сигналом той частоты, которую хорошо передаёт имеющаяся линия связи. Потенциальное или импульсное кодирование применяется на каналах высокого качества, а модуляция в остальных.

В сетевых линиях связи используется последовательная побитовая передача данных, которая требует всего одной пары проводов. Ещё одна проблема – это проблема взаимной синхронизации передатчика одного компьютера с приемником другого. Эта проблема решается двумя способами:

1) Путём обмена специальными синхроимпульсами по отдельной линии.
2) Путём периодической синхронизации импульсами формы отличной от формы импульса данных.

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

24.02.15

Топология физических связей.

Как только компьютеров становится больше двух, становится проблема выбора конфигурации физических связей или топология. Под топологией сети понимается конфигурация графа, вершинам которого соответствуют конечные узлы сети, например, компьютеры, и коммуникационное оборудование, например, маршрутизаторы, а рёбрам 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 путём удаления некоторых возможных связей. Ячеистая топология 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 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 станциями кольца.

Топология «звезда». Образуется в случае, когда каждый компьютер подключается отдельным кабелем к общему центральному устройству концентратору. Концентратором может быть компьютер либо коммутатор, маршрутизатор, повторитель. При выходе из строя центрального устройства сеть перестаёт работать. Возможность по наращиванию количества узлов в сети ограниченна

числом портов концентратора. Иногда строят сеть из нескольких концентраторов, соединёнными 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 подключается несколько компьютеров. Передаваемая информация распространяется по кабелю и доступна сразу всем узлам присоединённым кабелем. Достоинства заключаются в низкой стоимости и простоте присоединения новых узлов к сети. Недостаток – низкая надёжность. Любой дефект кабеля или какого-то из многочисленных разъёмов 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 «сети со смешанной топологией».

Адресация узлов сети.

При объединении трёх 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: 192.168.1.1. Этот же адрес может быть записан в шестнадцатеричной системе, либо двоичной. У каждого сетевого интерфейса есть и числовой и символьный адреса. В больших сетях применяется иерархическая система адресации. Эта схема позволяет до определённого момента пользоваться только старшей составляющей адреса. Затем для дальнейшей локализации адресата используют следующую по старшинству часть и так далее до младшей части. Вторая схема адресации – плоская (линейная) схема. В этом случае множество адресов никак не структурированно.

03.03.15

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 пользователя сети, поэтому он должен допускать символьное представление.
5) Адрес должен быть компактным чтобы не перегружать память коммуникационной аппаратуры.

Эти требования 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 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 часть (номер узла в сети). Такое деление позволяет передавать сообщение между сетями только на основании номера сети, номер узла используется после доставки сообщения в нужную сеть.

Символьные адреса предназначены для запоминания людьми, поэтому несут обычно смысловую нагрузку. В крупных сетях символьное имя может иметь иерархическую структуру.

В современных сетях для адресации узлов как правило применяют все три эти схемы. Пользователи адресуют компьютеры символьными именами, которые автоматически заменяются при передаче по сети числовыми номерами. Далее с помощью этих номеров сообщения передаются из одной сети в другу 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, которые занимаются протоколами разрешения адресов, может решаться как централизованными, так и распределёнными средствами. В случае централизованного подхода в сети выделяются один или несколько компьютеров (серверов имён), в которых хранится таблица соответствия друг другу имён различных типов. Все остальные компьютеры обращаются к серверу имён 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 опознания своего числового имени одни из компьютеров. Распределённый подход хорош тем, что не предполагает выделение специального компьютера. Недостаток: необходимость рассылки широковещательных сообщений. Они перегружают сеть, так как требуют обязательной обработки всеми узлами. Поэтому такой подход используется в небольших локальных сетях. В крупных сетях распространение широковещательных сообщений по всем сегментам сети почти нереально, поэтому применяют централизованный подход. Известная служба централизованного разрешения адресов – система доменных имён (DNS). В адресе назначения наряду с информацией, идентифицирующей порт устройства, должен указываться адрес процессора, 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.

10.03.15

Обобщённая задача коммутации.

Если топология сети не полно-связная, 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:

- Определение информационных потоков, для которых требуется прокладывать маршруты.
- Определение маршрутов для потоков.
- Сообщение о найденных маршрутах узлам сети.
- Продвижение потоков (распознавание потоков и их локальная коммутация).
- 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 интерфейс, который ведёт к нужному узлу. Информационным потоком называют непрерывную последовательность байтов, объединённых 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. То есть 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, причём для каждого из них может быть проложен свой особый маршрут. В таком случае выбор маршрута должен осуществляться с учётом характера передаваемых данных. Для файлового сервера важно, чтобы его данные направлялись по каналам, обладающим высокой пропускной способностью. Для программной системы управления, которая посылает в сеть короткие сообщения, требующие немедленной и обязательной обработки, при выборе маршрута более важна надёжность линии связи и минимальный уровень задержек на маршруте. Кроме того, одновременно могут прокладываться несколько маршрутов, чтобы за счёт 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 своё значение. Таким образом, при распознавании потоков должны учитываться не только адреса назначения данных, но и другие признаки, влияющие на маршрут.

Определение маршрута.

Выбрать маршрут передачи данных – значит определить последовательность транзитных узлов и их интерфейсов через которые нужно передавать данные, чтобы доставить их адресату. Множество альтернативных путей между двумя конечными узлами – это лишь множество потенциальных возможностей. Задача определения маршрута состоит в выборе из всего этого множества одного или нескольких путей. Чаще всего выбор останавливают на одном, оптимальном по некоторому критерию, маршруте. В качестве критериев оптимальности выбранного маршрута могут выступать:

- Номинальная пропускная способность.
- Загруженность каналов связи.
- Задержки, вносимые каналами.
- Количество промежуточных транзитных узлов.
- Надёжность каналов и транзитных узлов.

Маршрут может определяться вручную администратором сети, который, используя различные, часто не формализованные соображения, анализирует топологию сети и определяет последовательность интерфейсов, которую должны пройти данные, чтобы достичь получателя. Среди мотивов выбора того или иного пути могут быть:

- Особые требования сети со стороны различных типов приложений.
- Решение передавать трафик через сеть определённого поставщика услуг.
- Предположения о пиковых нагрузках на некоторые каналы сети.
- Из соображений безопасности.

Для больших сетей со сложной топологией задача определения маршрутов решается, как правило, автоматически. Для этого конечные узлы и другие устройства сети оснащаются специальными программными средствами, которые позволяют каждому узлу составить своё представление о топологии сети. Затем на основе этого исследования и математических алгоритмов определяют рациональные маршруты.

17.03.15

Оповещение сети о выбранном маршруте.

После того, как маршрут определён, нужно сообщить о нём всем устройствам сети. Сообщение о маршруте обрабатывается устройством и в результате создаётся новая запись в таблице коммутации. В этой таблице локальному или глобальному признакам потоку 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. Так же 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 обновление 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 таблицей коммутации. Если произошло совпадение, то эти данные направляются на интерфейс, который был определён 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 мультиплексирования. 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. Мультиплексирование является способом обеспечения доступности имеющихся физических каналов, одновременно для нескольких сеансов связи между абонентами сети. Прежде чем выполнить переброску данных на определённые 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 демультиплексирования, то есть разделения суммарного агрегированного потока на несколько составляющих потока. Операции

мультиплексирования и демультиплексирования 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 не полно связной сети. Существует множество способов мультиплексирования потоков в одном физическом канале. Важнейшим из них является разделение времени. При этом способе каждый поток время от времени получает в своё распоряжение физический канал и передаёт в это время по нему свои данные. Так же очень распространено частотное разделение каналов. Каждый поток передаёт данные в выделенном ему частотном диапазоне. Технология мультиплексирования 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, мультиплексирование и демультиплексирование.

Разделяемая среда передачи данных.

Ещё одним параметром разделяемого канала связи является количество узлов, подключенных к такому каналу. В телекоммуникационных сетях как правило используется вид подключения, когда к одному каналу подключается несколько интерфейсов. Такое множественное подключение интерфейсов порождает уже рассматривавшуюся выше топологию «общая шина», иногда называемую так же «шлейфовое подключение». При этом возникает проблема согласованного использования канала связи. Совместно используемый несколькими интерфейсами физический канал называют разделяемым (shared). Часто используется также термин разделяемая среда передачи данных (shared media). Разделяемые каналы связи используются не только для связи типа коммутатор-коммутатор, но и для связи компьютер-коммутатор и компьютер-компьютер. Существуют различные способы решения задачи организации совместного доступа к разделяемым линиям связи. Одни из них используют централизованный подход, когда доступом управляет специальное устройство – арбитр. Другие децентрализованный. Внутри компьютера проблема разделения линий связи между различными модулями так же существует. Примером является доступ к системной шине, которым управляет либо процессор, либо специальный арбитр шины. В сетях организация совместного доступа к линиям связи имеет свою специфику из-за существенно большего времени распространения сигналов по линиям связи. Поэтому процедуры согласования доступа к линиям связи могут занимать слишком большой промежуток времени и приводить к значительным потерям производительности сети. Не смотря на все эти сложности в локальных сетях разделяемые среды используются очень часто. Этот подход в частности реализован в широко распространённых классических технологиях (Ethernet, Token Ring, FDDI). В глобальных сетях разделяемые между интерфейсами среды практически не используются. Это объясняется тем что большие временные задержки распространения сигналов вдоль протяжённых каналов связи приводят к слишком длительным переговорным процедурам доступа к разделяемой среде, сокращая до неприемлемого уровня долю полезного использования канала связи на передачу данных абонентов. Однако в последние годы наметилась тенденция отказа от разделяемых сред передачи данных в локальных сетях. Это связано с тем, что за достигаемое таким образом удешевление сети приходится

расплачиваться производительностью. Сеть с разделяемой средой при большом количестве узлов будет работать всегда медленнее, чем аналогичная сеть с индивидуальными линиями связи, так как пропуская способность индивидуальной линии связи достаётся одному компьютеру. А при её совместном использовании делится между всеми компьютерами сети. Часто с такой потерей производительности мирятся ради увеличения экономической эффективности сети. Не только в классических, но и в совсем новых технологиях, разработанных для локальных сетей сохраняется режим разделения локальных линий связи.

24.03.15

Коммутация каналов.

В случае коммутации каналов, коммутационная сеть образует между конечными узлами непрерывный составной физический канал из последовательно соединённых промежуточных канальных участков. Условием того, что несколько физических каналов при последовательном соединении образуют единый физический канал, является равенство скоростей передачи данных в каждом из составляющих физических каналов. Равенство скоростей означает, что коммутаторы такой сети не должны буферизировать передаваемые данные. Перед передачей данных всегда необходимо выполнить процедуру установления соединения. В процессе этой процедуры и создаётся составной канал. Только после этого можно начинать передачу данных. Основные достоинства коммутации каналов:

- Постоянная и известная скорость передачи данных по установленному каналу. Это позволяет на основе заранее произведенной оценки установить в сети канал нужной скорости.
- Низкий и постоянный уровень задержки передачи данных через сеть. Это позволяет качественно передавать данные чувствительные к задержкам.

Недостатки:

- Может произойти отказ сети в обслуживании запроса на установление соединения. Это может случиться из-за того, что на некотором участке сети соединение нужно установить вдоль физического канала, через который уже проходит максимальное количество информационных потоков. Отказ может случиться и на конечном участке составного канала, если абонент поддерживает только одно соединение.
- Нерациональное использование пропускной способности физических каналов. После установления соединения, часть пропускной способности отводится составному каналу, на все время соединения, то есть до тех пор, пока соединение не будет разорвано. В тоже время, во многих случаях абонентам не нужна пропускная способность канала на все время соединения, так как в любом трафике присутствуют паузы. Невозможность динамического перераспределения пропускной способности физического канала является принципиальным ограничением сети с коммутацией каналов.

- Необходима обязательная задержка перед передачей данных из-за фазы установления соединения.

Коммутация пакетов.

Техника коммутации пакетов была специально разработана, для эффективной передачи компьютерного трафика. При коммутации пакетов все передаваемые пользователем сети сообщения разбиваются в исходном узле на сравнительно небольшие части – пакеты. Сообщением называется логически завершенная порция данных. Сообщения могут иметь произвольную длину. Пакеты так же могут иметь переменную длину, но в более узких пределах от 46 до 1500 байт. Каждый пакет снабжается заголовком, в котором указывается адресная информация, а также номер пакета. Номер пакета используется для сборки сообщения. Пакеты транспортируются в сети, как независимые информационные блоки. Коммутаторы сети принимают пакеты от конечных узлов и на основании адресной информации передают их. Коммутаторы пакетной сети имеют внутреннюю буферную память для временного хранения пакетов. Если выходной порт коммутатора в момент принятия пакета занят передачей другого пакета, то пакет будет некоторое время находиться в буферной памяти выходного порта. Когда до него дойдёт очередь, то он передаётся следующему коммутатору. Такая схема передачи данных позволяет сглаживать пульсации трафика между коммутаторами и тем самым использовать их наиболее эффективным способом для повышения пропускной способности сети в целом. Для пары абонентов наиболее эффективным было бы предоставление им в единичное пользование скоммутированного канала связи, как это делается в сетях с коммутацией каналов. Сеть с коммутацией пакетов замедляет процесс взаимодействия конкретной пары абонентов, так как их пакеты могут ожидать своей очереди в коммутаторах. Тем не менее общий объём передаваемых сетью компьютерных данных в единицу времени при коммутации пакетов выше чем при коммутации каналов. Это происходит потому, что пульсации трафика распределяются во времени так что их пики не совпадают. Поэтому коммутаторы постоянно и достаточно равномерно загружены работой.

Достоинства сети с коммутацией пакетов:

- Высокая общая пропускная способность сети при передаче пульсирующего трафика.
- Возможность динамически перераспределять пропускную способность физических каналов связи в соответствии с реальными потребностями.

Недостатки:

- Неопределенность скорости передачи данных, обусловленная зависимостью задержек в очередях буферов коммутаторов сети от общей загрузки сети.
- Переменная величина задержки пакетов данных, которые могут достигать значительных величин в моменты мгновенных перегрузок сети.
- Возможные потери данных из-за переполнения буфера.

В настоящее время активно разрабатываются и внедряются методы, позволяющие преодолеть 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 каждого компьютера. Сообщение в отличии от пакета имеет произвольную длину, которая определяется не технологическими соображениями, а содержанием информации сообщения. Транзитные компьютеры могут соединяться между собой как сетью с коммутацией каналов, так и пакетов. Режим передачи с промежуточным хранением на диске используется для передачи сообщений не требующих немедленного ответа. Как пример, электронная почта. 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 не оперативных служб, причем чаще всего поверх сети с коммутацией пакетов, как служба прикладного уровня.

Постоянная и динамическая коммутация.

В случае динамической коммутации 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 с пропускной способностью несколько гигабит в секунду. Некоторые типы сетей поддерживают оба режима работы. Например, сети X.25 или ATM могут предоставлять пользователю возможность динамически связаться с любым другим

пользователем сети и в тоже время отправлять данные по постоянному соединению одному определенному абоненту.

31.03.15

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 – это коммуникационное оборудование. К нему относятся кабельные системы, повторители, мосты, коммутаторы, маршрутизаторы, модульные концентраторы. По стоимости оборудования может быть сопоставима с компьютерами. Коммуникационное устройство может представлять собой сложный специализированный мультипроцессор, который нужно конфигурировать, оптимизировать и администрировать. Третьим слоем является операционная система. В зависимости от того какие концепции положены в основы 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 или нет. Самым верхним слоем являются различные сетевые приложения, такие как сетевые базы данных, почтовые системы, средства архивирования данных, системы автоматизации коллективной работы. Очень важно представлять диапазон возможностей приложений, а также знать на сколько они совместимы с другими сетевыми приложениями и другими операционными системами.

Сетевые службы и операционная система.

Для конечного пользователя сеть — это тот набор сетевых служб, с помощью которых он получает возможность просмотреть список имеющихся в сети компьютеров, прочитать удалённый 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, задачи, порождаемые распределённой обработкой 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 в сети. Служба вызова удалённых процедур. Среди сетевых служб можно выделить административные, то есть 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 учётных 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 же ресурса может быть разработано несколько служб, по-разному решающих одну и ту же задачу. Отличия могут заключаться в производительности или уровне удобства предоставляемых услуг. Качество сетевой службы зависит и от качества сетевого интерфейса. При определении степени удобства разделяемого ресурса часто употребляют термин прозрачность. Прозрачный доступ — это такой доступ, при котором пользователь не знает где расположен нужный ему ресурс, на собственном или удалённом компьютере. После того, как он смонтирует удалённую файловую систему в своё дерево каталогов, доступ к удалённым 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 операционная система имеют информацию о расположении файловых систем, но от пользователя она скрыта. Такая степень прозрачности редко встречается в сетях. Обычно, для получения доступа к ресурсам определённого компьютера, с начала приходиться устанавливать с ним логическое соединение.

Общая структура телекоммуникационной сети.

В общем случае, телекоммуникационная сеть состоит из следующих компонентов:

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 другим 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 в сети доступа зависит от её размера. Не большая сеть доступа может состоять из одного уровня, а крупная из двух трёх. Следующие уровни осуществляют дальнейшую концентрацию трафика собирая его и мультиплексируя более скоростные каналы. Магистральная сеть объединяет отдельные сети доступа, выполняя функции транзита трафика между ними по высокоскоростным каналам. Коммутаторы магистрали могут оперировать не только с информационными соединениями между отдельными пользователями, но и с агрегированными информационными потоками. В результате информация с помощью магистрали попадает в сеть доступа получателей, демультиплексируется там и коммутируется таким образом, что на входной порт оборудования 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 сервисами – это собственные информационные ресурсы сети, на основе которых осуществляется обслуживание пользователей. В таких центрах может храниться информация двух типов:

1. Пользовательская информация. То есть та, которая непосредственно интересует конечных пользователей сети.
2. Вспомогательная служебная информация. Она помогает предоставлять некоторые услуги пользователям.

К первому типу можно отнести web-порталы, на которых расположена разнообразная справочная и новостная информация. Ресурсами второго типа являются:

1. Различные системы аутентификации и авторизации пользователя.
2. Системы биллинга, которые подсчитывают плату за полученные услуги.
3. Базы данных учётной информации.
4. Централизованные системы управления сетью.

У сетей каждого конкретного типа имеется много особенностей. Тем не менее их структура в целом соответствует описанной выше. В тоже 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 оказания 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.

07.04.15

Производительность.

Производительность – это характеристика сети, позволяющая оценить, на сколько быстро информация достигнет от передающей станции 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 администратор 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 повышения их производительности. Одним из способов достижения этого стала микро-сегментация. Она позволяет уменьшить число пользователей на один сегмент и снизить объём широковещательного трафика, что значительно повышает производительность сети. Первоначально для микро-сегментации использовались маршрутизаторы. Но оказалось, что они не очень приспособлены для этих целей. Решения на их основе были достаточно дорогостоящими, отличались большой временной задержкой и не высокой 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 широковещательного трафика, решают задачи 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 в какой-либо сетевой службе и получением ответа на этот сетевой запрос. Значение этого показателя зависит от типа этой службы и от того, какой пользователь к какому серверу обращается, от загруженности элементов сети. Так же используют средне взвешенную оценку времени реакции сети. Время реакции сети обычно складывается из нескольких составляющих. Обычно в него входит:

1. Время подготовки запроса на клиентском компьютере.
2. Время передачи запросов между клиентом и сервером.
3. Время обработки запросов на сервере.
4. Время передачи ответов от сервера клиенту.
5. Время обработки полученных от сервера ответов на клиентском компьютере.

Знание сетевых составляющих времени реакции даёт возможность оценить производительность отдельных элементов сети выявить узкие места и в случае необходимости выполнить модернизацию сети. Скорость передачи данных отражает объём данных переданных сетью или её частью в 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 измеряется либо в битах в секунду, либо в пакетах в секунду. Пропускная способность может быть мгновенной, максимальной и средней. При проектировании, настройке и оптимизации сети чаще всего используется средняя и максимальная пропускные способности. Средняя пропускная способность позволяет оценить работу сети на большом промежутке времени, в течении которого пики и спады интенсивности трафика компенсируют друг друга. Пропускная способность позволяет оценить возможности сети справляться с пиковыми нагрузками. Пропускную способность можно измерять между любыми двумя узлами сети. Для анализа и настройки сети полезно знать данные о пропускной способности отдельных элементов сети. Задержка передачи определяется как задержка между моментом поступления 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 вариацией задержки. Пропускная способность и задержки передачи не зависят друг от друга. Сеть может обладать высокой пропускной способностью, но вносить значительные задержки при передаче каждого пакета.

Надёжность и безопасность.

Различают несколько аспектов надежности: для технических устройств используют такие показатели надёжности как среднее время наработки на отказ, вероятность отказа, интенсивность отказов. Эти показатели пригодны для оценки надёжности простых элементов, которые могут находиться только в двух состояниях: работает или не работает. Сложные системы кроме двух этих состояний имеют промежуточные состояния, поэтому для оценки надёжности сложных систем применяется другой набор характеристик. Готовность или коэффициент готовности – означает долю времени, в течении которого система может быть использована. Готовность может быть улучшена путём введения 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 высоконадежной она помимо высокой готовности должна обеспечивать сохранность данных и их защиту от искажений. Кроме того, должна поддерживаться не противоречивость 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 проходящим 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 легкого добавления отдельных элементов сети, наращивание длины сегмента сети и замены существующей аппаратуры на более мощную. При этом принципиально важно, что легкость расширения системы иногда может обеспечиваться в весьма ограниченных приделах. Масштабируемость означает, что сеть позволяет наращивать количество узлов и протяженность 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 много сегментная сеть, построенная с использованием коммуникаторов и маршрутизаторов и имеющая иерархическую структуру связи. 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 сложной

системой кабелей, а как единая традиционная вычислительная машина с системой разделения времени. Прозрачность может быть достигнута на двух различных уровнях: на уровне пользователя и на уровне программиста. На уровне пользователя прозрачность означает, что для работы с удалёнными ресурсами он использует тот же набор команд и процедур, что и для работы с локальными. На программном уровне прозрачность заключается в том, что приложению для доступа к удалённым ресурсам требуются те же вызовы что и для доступа к локальным. Прозрачность расположения означает, что от пользователя не требуется знаний о 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 вычисления происходит автоматически без участия программиста. При этом система сама распределяет параллельные ветви приложения по процессорам и компьютерам сети.

14.04.15

Поддержка различных видов трафика.

См. рисунок ниже.

2.5. Поддержка разных видов трафика

Компьютерные сети изначально предназначены для совместного доступа пользователей к ресурсам компьютеров: файлам, принтерам и т. п. Трафик, создаваемый этими традиционными службами компьютерных сетей, имеет свои особенности и существенно отличается от трафика сообщений в телефонных сетях или, например, в сетях кабельного телевидения. Однако 90-е годы стали годами проникновения в компьютерные сети трафика мультимедийных данных, представляющих в цифровой форме речь и видеоизображение. Естественно, что для динамической передачи мультимедийного трафика требуются иные алгоритмы и протоколы и, соответственно, другое оборудование.

Главной особенностью трафика, образующегося при динамической передаче голоса или изображения, является наличие жестких требований к синхронности передаваемых сообщений. Для качественного воспроизведения непрерывных процессов, которыми являются звуковые колебания или изменения интенсивности света в видеоизображении, необходимо получение измеренных и закодированных амплитуд сигналов с той же частотой, с которой они были измерены на передающей стороне. При запаздывании сообщений будут наблюдаться искажения.

В то же время трафик компьютерных данных характеризуется крайне неравномерной интенсивностью поступления сообщений в сеть при отсутствии жестких требований к синхронности доставки этих сообщений. Например, доступ пользователя, работающего с текстом на удаленном диске, порождает случайный поток сообщений между удаленным и локальным компьютерами, зависящий от действий пользователя, причем задержки при доставке мало влияют на качество обслуживания пользователя сети. Сегодня практически все новые протоколы в той или иной степени предоставляют поддержку мультимедийного трафика.

Особую сложность представляет *совмещение* в одной сети традиционного *компьютерного* и *мультимедийного трафика.* Обычно протоколы и оборудование компьютерных сетей относят мультимедийный трафик к факультативному, поэтому качество его обслуживания оставляет желать лучшего. Сегодня затрачиваются большие усилия по созданию сетей, не ущемляющих интересы каждого из типов трафика. Наиболее близки к этой цели сети на основе технологии ATM, разработчики которой изначально учитывали случай сосуществования разных типов трафика в одной сети.

2.6. Управляемость

Управляемость сети подразумевает возможность централизованно контролировать состояние основных элементов сети, а также выявлять и разрешать проблемы, возникающие при работе сети, выполнять анализ производительности и планировать развитие сети. В идеале средства управления сетями представляют собой систему, которая осуществляет наблюдение, контроль и управление каждым элементом сети — от простейших до самых сложных устройств, при этом такая система рассматривает сеть как единое целое, а не как разрозненный набор отдельных устройств.

Хорошая система управления наблюдает за сетью и, обнаружив проблему, активизирует определенное действие, исправляет ситуацию и уведомляет администратора о том, что произошло и какие действия предприняты. Одновременно с этим система управления должна накапливать данные, на основании которых можно планировать развитие сети. Наконец, система управления должна быть независима от производителя и обладать удобным интерфейсом, позволяющим выполнять все действия с одной консоли.

Решая тактические задачи, администраторы и технический персонал сталкиваются с ежедневными проблемами обеспечения работоспособности сети. Эти задачи требуют быстрого решения, обслуживающий сеть персонал должен оперативно реагировать на сообщения о неисправностях, поступающих от пользователей или автоматических средств управления сетью. Постепенно становятся заметны общие проблемы производительности, конфигурирования сети, обработки сбоев и безопасности данных, требующие стратегического подхода, то

есть *планирования* сети. Планирование, кроме этого, включает прогноз изменений требований пользователей к сети, вопросы применения новых приложений, новых сетевых технологий и т. п.

Полезность системы управления особенно ярко проявляется в больших сетях: корпоративных или публичных глобальных.

В настоящее время в области систем управления сетями много нерешенных проблем. Большинство существующих средств вовсе не управляют сетью, а всего лишь осуществляют *наблюдение* за ее работой. Они следят за сетью, но не выполняют активных действий, если с сетью что-то произошло или может произойти. Мало масштабируемых систем, способных обслуживать как сети масштаба отдела, так и сети масштаба предприятия.

2.7. Совместимость

Совместимость, или *интегрируемость*, означает, что сеть способна включать в себя самое разнообразное программное и аппаратное обеспечение, то есть в ней могут сосуществовать различные операционные системы, поддерживающие разные стеки коммуникационных протоколов, а также аппаратные средства и приложения от разных производителей. Сеть, состоящая из разнотипных элементов, называется *неоднородной*, или *гетерогенной*, а если гетерогенная сеть работает без проблем, то она является интегрированной. Основной путь построения интегрированных сетей состоит в использовании модулей, выполненных в соответствии с открытыми стандартами и спецификациями.

2.8. Качество обслуживания

Качество обслуживания (Quality of Service, QoS) определяет вероятностные оценки выполнения тех или иных требований, предъявляемых к сети приложениями или пользователями. Например, при передаче голосового трафика через сеть под качеством обслуживания чаще всего понимают гарантии того, что голосовые пакеты будут доставляться сетью с задержкой не более *X* мс, при этом вариация задержки не превысит Y мс, и эти характеристики станут выдерживаться сетью с вероятностью 0,95 на определенном временном интервале. Файловому сервису нужны гарантии средней полосы пропускания и расширения ее на небольших интервалах времени до некоторого максимального уровня для быстрой передачи пульсаций. В идеале сеть должна гарантировать особые параметры качества обслуживания, сформулированные для каждого отдельного приложения. Однако по понятным причинам разрабатываемые и уже существующие механизмы QoS ограничиваются решением более простой задачи — гарантированием неких усредненных требований, заданных для основных типов приложений.

Чаще всего параметры, фигурирующие в разнообразных определениях качества обслуживания, регламентируют следующие показатели работы сети:

1. скорость передачи данных;
2. задержки передачи пакетов;
3. уровень потерь и искажений пакетов.

Качество обслуживания гарантируется для некоторого потока данных. Напомним, что поток данных — это последовательность пакетов, имеющих некоторые общие признаки, например адрес узла-источника, информация, идентифицирующая тип приложения (номер порта TCP/UDP) и т. п.

Механизмы поддержки качества обслуживания сами по себе не создают пропускной способности. Сеть не может дать больше того, что имеет. Так что фактическая пропускная способность каналов связи и транзитного коммуникационного оборудования — это ресурсы сети, являющиеся отправной точкой для работы механизмов QoS. Механизмы QoS только управляют распределением имеющейся пропускной способности в соответствии с требованиями приложений и настройками сети. Самый очевидный способ перераспределения пропускной способности сети состоит в управлении очередями пакетов.

Поскольку данные, которыми обмениваются два конечных узла, проходят через некоторое количество промежуточных сетевых устройств, таких как концентраторы, коммутаторы и маршрутизаторы, то поддержка QoS требует взаимодействия всех сетевых элементов на пути трафика, то есть «из конца в конец» («end-to-end», e2e). Любые гарантии QoS настолько хороши, насколько их обеспечивает наиболее «слабый» элемент в цепочке между отправителем и получателем. Поэтому нужно хорошо понимать, что поддержка QoS только в одном сетевом устройстве, пусть даже и магистральном, может весьма незначительно улучшить качество обслуживания или же совсем не повлиять на параметры QoS.

Реализация в компьютерных сетях механизмов поддержки QoS является сравнительно новой тенденцией. Долгое время компьютерные сети существовали без таких механизмов, и это объясняется в основном двумя причинами. Во-первых, большинство приложений, выполняемых в сети, были нетребовательными. Для таких приложений задержки пакетов или отклонения средней пропускной способности в достаточно широком диапазоне не приводили к значительной потере функциональности. Примерами нетребовательных приложений являются наиболее распространенные в сетях 80-х годов приложения электронной почты или удаленного копирования файлов.

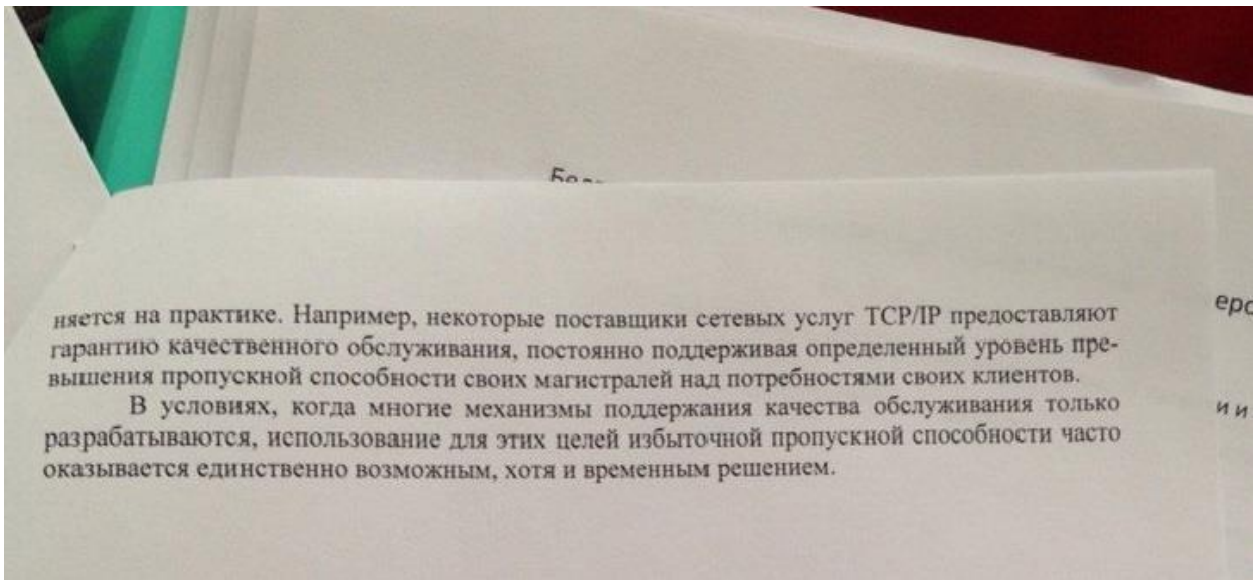
Во-вторых, сама пропускная способность 10-мегабитных сетей Ethernet во многих случаях не являлась дефицитом. Так, разделяемый сегмент Ethernet, к которому было подключено 10-20 компьютеров, изредка копирующих небольшие текстовые файлы, не превышающие несколько сотен килобайт, позволял трафику каждой пары взаимодействующих компьютеров пересекать сеть так быстро, как это требовалось породившим этот трафик приложениям.

В результате большинство сетей работало с тем качеством транспортного обслуживания, которое обеспечивало потребности приложений. Правда, никаких гарантий относительно нахождения задержек пакетов или пропускной способности, с которой пакеты передаются между узлами, в определенных пределах эти сети не давали. Более того, при временных перегрузках сети, когда значительная часть компьютеров одновременно начинала передавать данные с максимальной скоростью, задержки и пропускная способность становились такими, что работа приложений давала сбой — шла слишком медленно, с прерываниями сеансов и т. п.

Транспортный сервис, который предоставляли такие сети, получил название *best effort,* то есть сервис «с максимальными усилиями». Сеть старается обработать поступающий трафик как можно быстрее, но при этом никаких гарантий относительно результата своих усилий не дает. Примерами являются большинство популярных технологий, разработанных в 80-е годы: Ethernet, Token Ring, IP, X.25. Сервис «с максимальными усилиями» основан на некотором справедливом алгоритме обработки очередей, возникающих при перегрузках сети, когда в течение некоторого времени скорость поступления пакетов в сеть превышает скорость продвижения этих пакетов. В простейшем случае алгоритм обработки очереди рассматривает пакеты всех потоков как равноправные и продвигает их в порядке поступления *(First Input First Output, FIFO).* В том случае, когда очередь становится слишком большой (не умещается в буфере), проблема решается простым отбрасыванием вновь поступающих пакетов.

Очевидно, что сервис «с максимальными усилиями» обеспечивает приемлемое качество обслуживания только в тех случаях, когда производительность сети намного превышает средние потребности, то есть является избыточной. В такой сети пропускная способность достаточна даже для поддержания трафика пиковых периодов нагрузки. Также очевидно, что такое решение не экономично — по крайней мере, по отношению к пропускным способностям сегодняшних технологий и инфраструктур, особенно для глобальных сетей. Так как пиковые нагрузки и области, где они возникают, трудно предсказать, то такой путь не дает долговременного решения.

Тем не менее построение сетей с избыточной пропускной способностью, будучи самым простым способом обеспечения нужного уровня качества обслуживания, иногда приме-



няется на практике. Например, некоторые поставщики сетевых услуг TCP/IP предоставляют гарантию качественного обслуживания, постоянно поддерживая определенный уровень превышения пропускной способности своих магистралей над потребностями своих клиентов.

В условиях, когда многие механизмы поддержания качества обслуживания только разрабатываются, использование для этих целей избыточной пропускной способности часто оказывается единственно возможным, хотя и временным решением.

21.04.15

Открытые сети и модель OSI.

Многоуровневый подход – декомпозиция задачи сетевого обмена. Организация взаимодействия между устройствами сети является сложной задачей. Для решения сложных задач используют универсальный приём – декомпозицию, то есть разбиение одной сложной задачи на несколько более простых задач – модулей. Декомпозиция состоит в чётком 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. Всё множество модулей решающих частные задачи разбивают на группы и сортируют по уровням, образующим иерархии. 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, отнесённых к некоторому уровню, могут быть переданы только модулям соседнего вышележащего уровня. Такая иерархическая декомпозиция предполагает чёткое определение функций каждого уровня и взаимодействие между ними. Интерфейс определяет набор функций, которые нижележащий уровень предоставляет вышележащему. В результате иерархической декомпозиции достигается относительная независимость уровней и появляется возможность их автономной модификации. Средства решения задачи организации сетевого взаимодействия также представляется в виде иерархически организованного множества модулей. Решение задачи, порученное вышележащему уровню, может быть получено путём многократных обращений к 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 иерархию, работающую 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 так далее. Соглашения должны быть приняты для всех уровней, начиная от самого низкого уровня передачи битов и до самого высокого, который организует сервис для пользователей сети.

Протокол определяет правила взаимодействия модулей одного уровня в разных узлах, а интерфейс определяет правила взаимодействия модулей соседних уровней. Средства каждого уровня должны отрабатывать, во-первых, свой собственный протокол, а во-вторых, интерфейсы соседних уровней. 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 80-х годов была разработана модель, которая сыграла значительную роль в развитии сети. Эта модель называется «Моделью взаимодействия открытых систем». Она определяет различные уровни взаимодействия систем в сетях с коммутацией пакетов, даёт им стандартные имена и указывает, какие функции должен выполнять каждый уровень. В модели взаимодействия существует 7 уровней:

1. Прикладной
2. Представительный
3. Сеансовый
4. Транспортный
5. Сетевой
6. Канальный
7. Физический

Каждый уровень имеет дело с определённым аспектом взаимодействия сетевых устройств. Пусть приложение обращается с сетевым запросом к прикладному уровню, например, файловая служба. На основании этого запроса, программное обеспечение прикладного уровня формирует сообщения 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 месте нахождения 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 сообщения, прикладной уровень направляет его вниз по стеку представительному уровню. Протокол представительного уровня на основании информации, полученной из заголовка прикладного уровня, выполняет требуемые действия и добавляет в сообщение собственную служебную информацию – заголовок представительного уровня, в котором содержатся указания для протокола представительного уровня машины адресата. Полученное в результате сообщение передаётся вниз – сеансовому уровню, который добавляет свой заголовок и так далее. Наконец, сообщение достигает нижнего, физического уровня, который и передаёт его 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 передаёт 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, такие как: полоса пропускания; волновое сопротивление. На этом уровне определяются характеристики электрических сигналов, уровень напряжения сигнала, тип кодирования. Кроме того, здесь стандартизируются типы разъёмов и назначения каждого контакта. Функции физического уровня реализуются во всех устройствах, подключенных к сети. Со стороны компьютера функции физического уровня выполняются сетевым адаптером или последовательным портом.

28.04.15

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 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. 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 определённым 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 контрольные суммы не совпадают, то фиксируется ошибка. Канальный уровень может не только обнаруживать ошибки, но и исправлять их за счёт повторной передачи

повреждённых кадров. Функция исправления ошибок не является обязательной для канального уровня.

В протоколах канального уровня, используемых в локальных сетях, заложена определённая структура связей между компьютерами и способы их адресации. Хотя канальный уровень и обеспечивает доставку кадра между любыми двумя узлами сети, он это делает только в сети с совершенно определённой топологией связи. Именно той топологией, для которой он был разработан. К таким типовым топологиям, поддерживаемым протоколом канального уровня, 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, соединёнными индивидуальной линией связи. Примерами протоколов точка-точка могут служить широко распространённые протоколы PPP и Lab-bin. 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:

1. Сетевой.
2. Транспортный.

Сетевой уровень.

Сетевой уровень 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 связи. Функции сетевого уровня достаточно разнообразны. Начнём их рассмотрение на примере объединения локальных сетей.

На сетевом уровне сам термин «сеть» наделяют специфическим значением. В данном случае под сетью понимается совокупность компьютеров, соединённых между собой в соответствии с одной из стандартных типовых топологий и использующих для передачи данных один из протоколов канального уровня, определённый 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 её 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 (хоп – прыжок), каждый раз выбирая подходящий маршрут. Таким образом, маршрут представляет собой последовательность маршрутизаторов, через которую проходит пакет.

Проблема выбора наилучшего пути называется маршрутизацией, и её 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 скорость передачи данных по этому маршруту. Она зависит от пропускной способности канала связи и интенсивности трафика, которая может изменяться с течением времени. Выбор маршрута может осуществляться и по другим критериям, например, надёжность передачи.

Сетевой уровень может так же решать задачи согласования разных технологий, упрощение адресации в крупных сетях и создание надёжных и гибких барьеров на пути нежелательного трафика между сетями.

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

На сетевом уровне определяется два вида протоколов. Первый вид - сетевые протоколы. Реализуют продвижение пакетов через сеть. Однако часто к сетевому уровню относят и другой вид протоколов, называемых протоколами обмена маршрутной информации или просто протоколами маршрутизации. 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 ещё одного типа, которые отвечают за отображение адреса узла, используемого на сетевом уровне в локальный адрес сети. Такие протоколы часто называют протоколами разрешения адреса(ARP). Иногда их относят не к сетевому уровню, а к канальному.

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

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 надёжным соединением. Транспортный уровень обеспечивает приложениям или верхним уровням стека, прикладному и сеансовому, передачу данных с той степенью надёжности, которая им требуется. Модель OSI определяет пять классов сервиса, предоставляемых транспортным уровнем. Эти виды сервисов 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 устранению ошибок передачи. Выбор класса сервиса транспортного уровня определяется с одной стороны тем, в какой степени задача обеспечения надёжности 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, а также SPX.

Протоколы нижних четырёх уровней обобщённо 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. Оставшихся три верхних уровня решают задачу предоставления прикладных сервисов на основании имеющейся транспортной системы.

Сеансовый уровень.

Сеансовый уровень обеспечивает управление взаимодействием, фиксирует, какая из сторон является активной в настоящий момент, предоставляет средство синхронизации. Последнее позволяет 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 не многие 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.

05.05.15

Представительный уровень.

Представительный уровень 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.

Прикладной уровень

Прикладной уровень — 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.

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.

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 сетезависимыми, 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).

Стандартизация сетей. 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:

1) возможность построения сети из аппаратных и программных средств различных производителей, придерживающихся одного и того же стандарта;
2) возможность безболезненной замены отдельных компонентов сети другими, более совершенными, что позволяет сети развиваться с минимальными затратами;
3) возможность легкого сопряжения одной сети с другой;
4) 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.

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.

Источники стандартов.

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

1) стандарты отдельных фирм (например, графический интерфейс OPEN LOOK для UNIX-систем фирмы Sun);
2) стандарты специальных комитетов и объединений, создаваемых несколькими фирмами, например, стандарты союза Fast Ethernet Alliance по разработке стандартов 100 Мбит Ethernet;
3) национальные стандарты, например, стандарты безопасности для операционных систем, разработанные Национальным центром компьютерной безопасности (NCSC) Министерства обороны США;
4) 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.

1) 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.
2) 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).
3) 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.
4) 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.
5) Ассоциация производителей компьютеров и оргтехники (Computer and Business Equipment Manufacturers Association, CBEMA) — организация американских фирм-производителей аппаратного обеспечения; аналогична

европейской ассоциации ECMA; участвует в разработке стандартов на обработку информации и соответствующее оборудование.

6) 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.
7) 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.
8) 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.

12.05.15

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.

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.

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.

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.

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**	**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			

19.05.15

Типы линий связи. 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).

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.

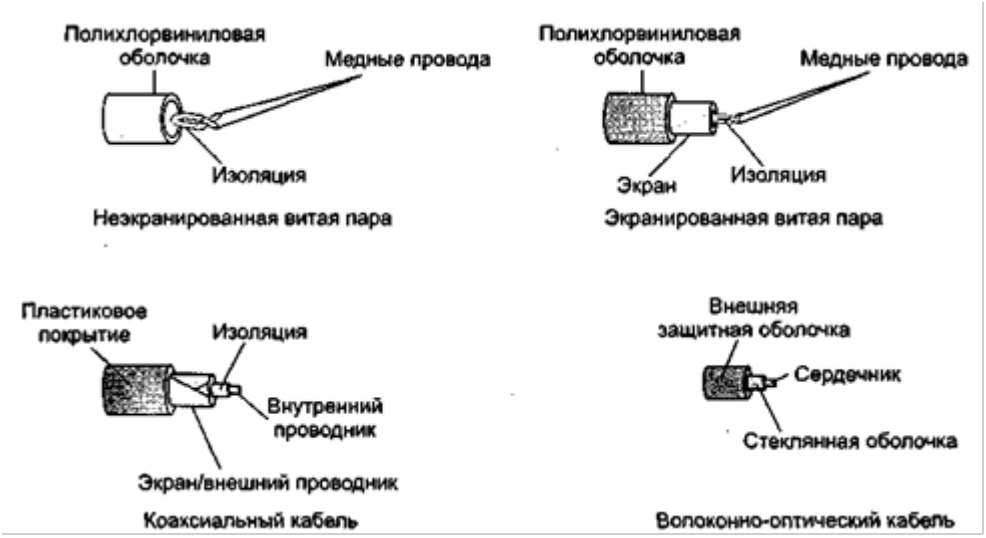


Рис. 5.2. Устройство кабелей

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 мно-гомодовых кабелей;
- полупроводниковые лазеры, или лазерные диоды (Laser Diode) для одномодо-вых 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.

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:

1) улучшение качества сигнала;
2) 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).

26.05.15

Адресация в IP-сетях.

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

В стеке TCP/IP используются три типа адресов:

1) локальные, или аппаратные, адреса, используемые для адресации узлов в пределах подсети;
2) сетевые, или IP-адреса, используемые для однозначной идентификации узлов в пределах всей составной сети;
3) 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.

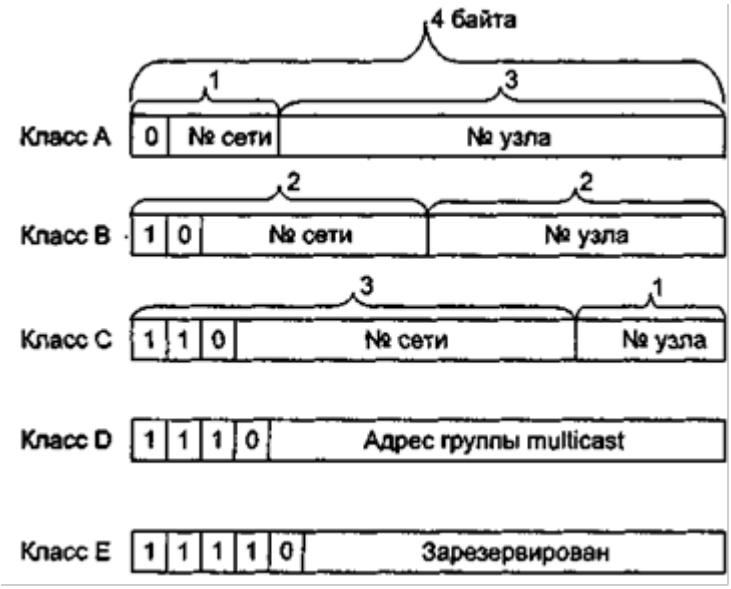
Наиболее употребляемой формой представления IP-адреса является запись в виде четырех чисел, представляющих значения каждого байта в десятичной форме и разделенных точками, например, 128.10.2.30. Этот же адрес может быть представлен в двоичном формате 10000000 00001010 00000010 00011110, а также в шестнадцатеричном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

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 224, 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 216 (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 28 (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.

Особые IP-адреса.

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

- 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).
- 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.
- 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.

- 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.

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:

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

Шлюз.

Сетевой шлюз (англ. gateway) — аппаратный маршрутизатор или программное обеспечение для сопряжения компьютерных сетей, использующих разные протоколы (например, локальной и глобальной).

Сетевой шлюз конвертирует протоколы одного типа физической среды в протоколы другой физической среды (сети). Например, при соединении локального компьютера с сетью Интернет обычно используется сетевой шлюз.

Маршрутизатор (он же — роутер) является одним из примеров аппаратных сетевых шлюзов.

Сетевые шлюзы работают на всех известных операционных системах. Основная задача сетевого шлюза — конвертировать протокол между сетями. Роутер сам по себе принимает, проводит и отправляет пакеты только среди сетей, использующих одинаковые протоколы. Сетевой шлюз может с одной стороны принять пакет, сформатированный под один протокол (например, Apple Talk) и конвертировать в пакет другого протокола (например, TCP/IP) перед отправкой в другой сегмент сети. Сетевые шлюзы могут быть аппаратным решением, программным обеспечением или тем и другим вместе, но обычно это программное обеспечение, установленное на роутер или компьютер. Сетевой шлюз должен понимать все протоколы, используемые роутером. Обычно сетевые шлюзы работают медленнее, чем сетевые мосты, коммутаторы и обычные маршрутизаторы. Сетевой шлюз — это точка сети, которая служит выходом в другую сеть. В сети Интернет узлом или конечной точкой может быть или сетевой шлюз, или хост. Интернет-пользователи и компьютеры, которые доставляют веб-страницы пользователям — это хосты, а узлы между различными сетями — это сетевые шлюзы. Например, сервер, контролирующий трафик между локальной сетью компании и сетью Интернет — это сетевой шлюз.

В крупных сетях сервер, работающий как сетевой шлюз, обычно интегрирован с прокси-сервером и межсетевым экраном. Сетевой шлюз часто объединен с роутером, который управляет распределением и конвертацией пакетов в сети.

Сетевой шлюз может быть специальным аппаратным роутером или программным обеспечением, установленным на обычный сервер или персональный компьютер. Большинство компьютерных операционных систем использует термины, описанные выше. Компьютеры под Windows обычно используют встроенный мастер подключения к сети, который по указанным параметрам сам устанавливает соединение с локальной или глобальной сетью. Такие системы могут также использовать DHCP-протокол. Dynamic Host Configuration Protocol (DHCP) — это протокол, который обычно используется сетевым оборудованием, чтобы получить различные данные, необходимые клиенту для работы с протоколом IP. С использованием этого протокола добавление новых устройств и сетей становится простым и практически автоматическим.

Интернет-шлюз — как правило, это программное обеспечение, призванное организовать передачу трафика между разными сетями. Программа является рабочим инструментом системного администратора, позволяя ему контролировать трафик и действия сотрудников.

Обычно Интернет-шлюз позволяет распределять доступ среди пользователей, вести учёт трафика, ограничивать доступ отдельным пользователям или группам пользователей к ресурсам в Интернет. Интернет-шлюз может содержать в себе прокси-сервер, межсетевой экран, почтовый сервер, шейпер, антивирус и другие

сетевые утилиты. Интернет-шлюз может работать как на одном из компьютеров сети, так и на отдельном сервере. Шлюз устанавливается как программное обеспечение на машину с операционной системой, либо на пустой компьютер с развертыванием встроенной операционной системы.

Также под шлюзом часто понимается IP-адрес машины, через которую организован доступ в интернет.

02.06.15

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, www.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.

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.

Протоколы разрешения адресов. Отображение IP-адресов на локальные адреса.

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

При конфигурировании 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).

09.06.15

Передача данных 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).

- Компьютер «понимает», что кабель свободен (т.е. трафик отсутствует).
- Компьютер может начать передачу данных.
- 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 повторных 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 число пользователей зависит от аппаратных компонентов, кабельной системы и сетевого программного обеспечения), может практически остановиться из-за чрезмерного сетевого трафика.

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.

Суть доступа с передачей маркера заключается в следующем: пакет особого типа, маркер (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 - 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.

Разбиение IP-сетей на подсети и создание надсетей.

Маски подсети позволяют настраивать адресное пространство в соответствии с требованиями к сети. Разбиение на подсети позволяет организовать иерархическую структуру сетей, а надсети и CIDR позволяют объединить разные сети в едином адресном пространстве.

Разбиение на подсети.

Маски подсети помогают определить, как IP-адрес разбивается на идентификаторы сети и узла. В адресах классов A, B и C применяются стандартные маски подсети, занимающие соответственно первые 8, 16 и 24 бита 32-битового адреса. Подсетью называется логическая сеть, определяемая маской подсети.

Стандартные маски годятся для сетей, которые не предполагается разбивать. Например, в сети из 100 компьютеров, соединенных с помощью карт гигабитного Ethernet, кабелей и коммутаторов, все узлы могут обмениваться информацией по локальной сети. Сеть не нуждается в маршрутизаторах для защиты от чрезмерного широковещания или для связи с узлами, расположенными в отдельных физических сегментах. В таком простом случае вполне достаточно идентификатора сети класса C.

Механизм разбиения на подсети.

Разбиение на подсети (subnetting) — это логическое разделение адресного пространства сети путем установки в 1 дополнительных битов маски подсети. Такое расширение позволяет создавать многие подсети в адресном пространстве сети.

Например, если маска подсети по умолчанию 255.255.0.0 используется для узлов сети класса B 131.107.0.0, IP-адреса 131.107.1.11 и 131.107.2.11 находятся в одной подсети и поддерживают взаимодействие посредством широковещания. Но если расширить маску подсети до 255.255.255.0, то эти адреса окажутся в разных подсетях и для обмена данными соответствующим узлам придется пересылать пакеты на основной шлюз, который перенаправит дейтаграммы в нужную подсеть. Внешние по отношению к сети узлы по-прежнему используют маску подсети по умолчанию для взаимодействия с узлами внутри сети. Обе версии показаны на рис. 2-7 и 2-8.

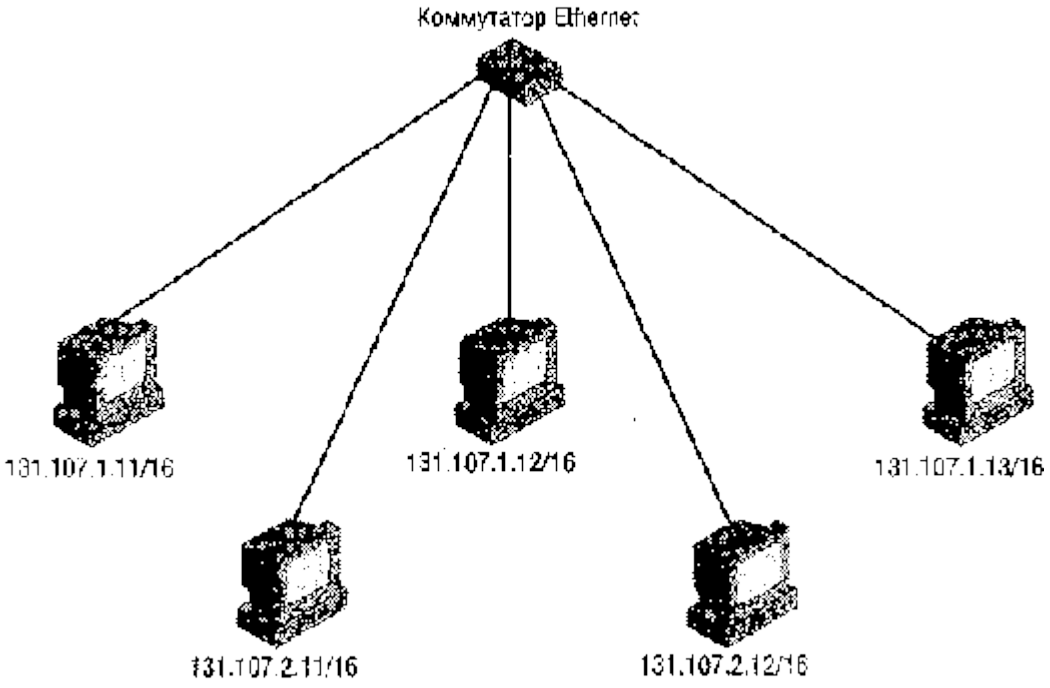


Рис. 2-7. Неразбитое на подсети адресное пространство класса B

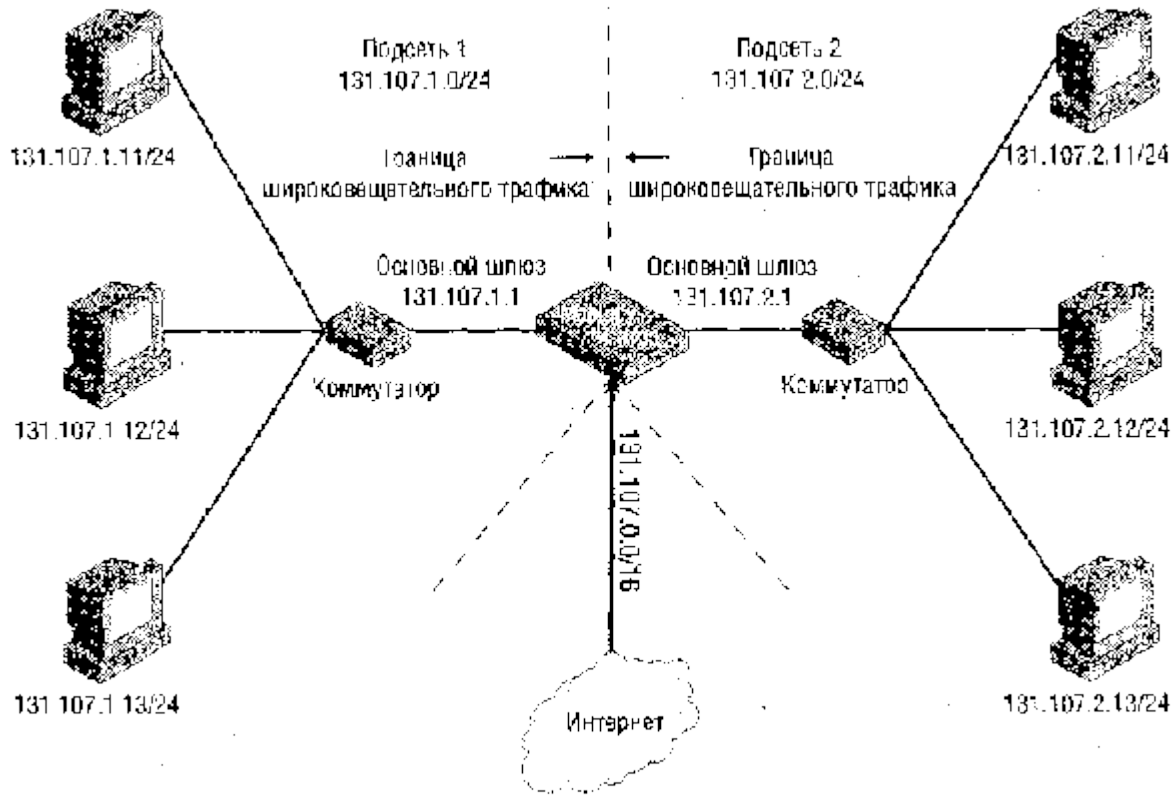


Рис. 2-7. Разбитое на подсети адресное пространство класса B

Показанное на рис. 2-7 исходное адресное пространство класса B, состоящее из единственной подсети, может содержать максимум 65 534 узлов, а новая маска подсети (рис. 2-8) позволяет разделить адресное пространство на 256 подсетей, в каждой из которых можно разместить до 254 узлов.

Преимущества разбиения на подсети.

Разбиение на подсети часто используют для обеспечения соответствия физической и логической топологии сети или для ограничения широковещательного трафика. Другие несомненные преимущества: более высокий уровень защиты (благодаря ограничению неавторизованного трафика маршрутизаторами) и упрощение администрирования (благодаря передаче управления подсетями другим отделам или администраторам).

Определение диапазонов адресов подсети

Десятично-точечная форма маски подсети позволяет определить диапазоны IP-адресов в каждой подсети простым вычитанием из 256 числа в соответствующем октете маски.

Например, в сети класса C с адресом 207.209.68.0 с маской подсети 255.255.255.192 вычитание 192 из 256 даст 64. Таким образом, новый диапазон начинается после каждого 64 адреса: 207.209.68.0-207.209.68.63, 207.209.68.64-207.209.68.127 и т.д. В сети класса B 131.107.0.0 с маской подсети 255.255.240.0

вычитание 240 из 256 дает 16. Следовательно, диапазоны адресов подсетей группируются по 16 в третьем октете, а четвертый октет принимает значения из диапазона 0—255: 131.107.0.0—131.107.15.255, 131.107.16.0— 131.107.31.255 и т.д.

Помните, что узлам нельзя назначать идентификаторы из одних нулей или единиц, так что исключаются первый и последний адрес каждого диапазона.

Использование бесклассовой междоменной маршрутизации

CIDR — это эффективный метод поддержки надсетей с помощью таблиц маршрутизации. Не будь CIDR, в таблицах маршрутизации следовало бы размещать отдельные записи для каждой сети в надсети, а так вся надсеть представляется одной записью (рис. 2-16).

Выделенные региональными регистраторами Интернета или интернет-провайдерами блоки адресов надсети часто называют CIDR-блоками, а термин CIDR часто используется для обозначения самих надсетей.

CIDR не совместим с устаревшим протоколом RIP (Routing Information Protocol) версии 1, который применялся в старых маршрутизаторах, и требует, чтобы маршрутизатор использовал бесклассовый протокол маршрутизации, такой как RIP версии 2 или OSPF(OpenShortestPathFirst).

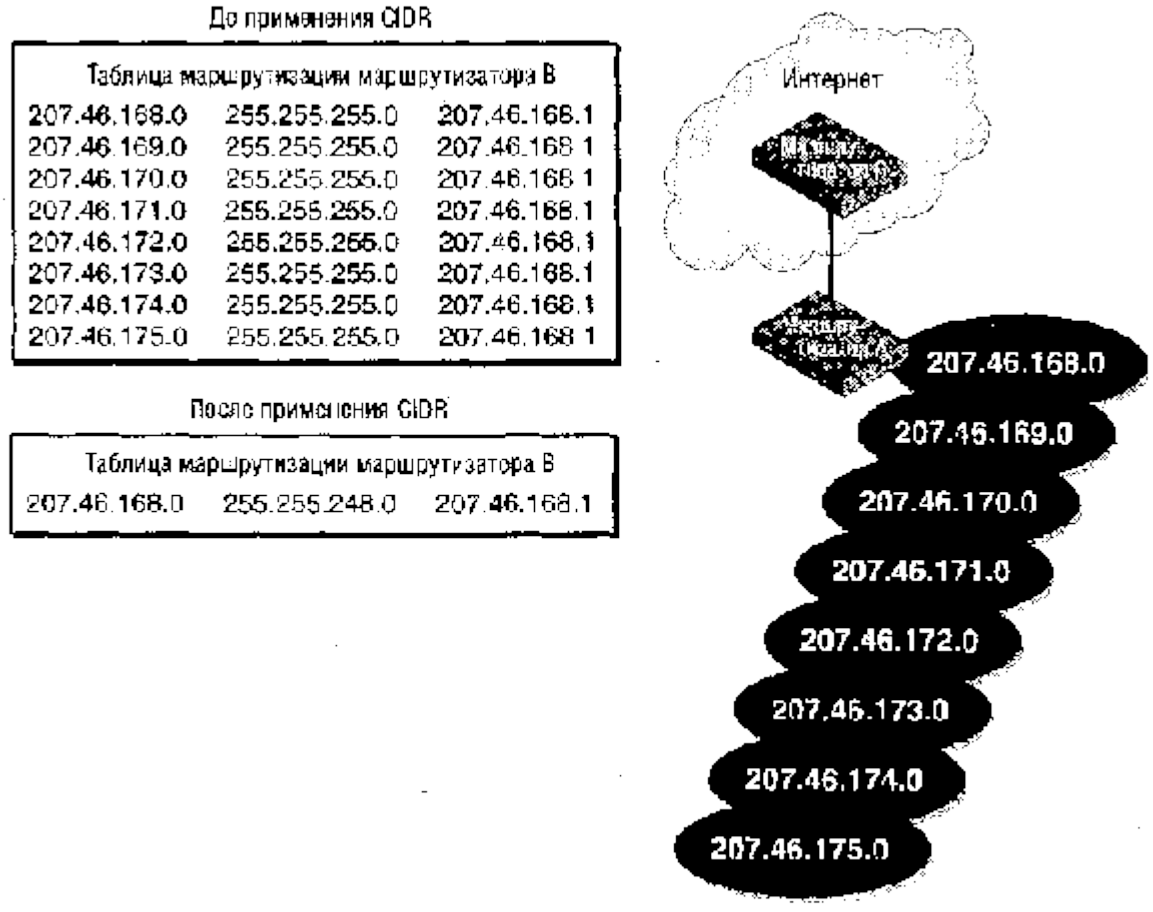


Рис. 2-16. Использование CIDR для упрощения создания надсетей

Маски подсети переменной длины

Традиционно все узлы и маршрутизаторы организации используют одну маску подсети. В этом случае сеть может разбиваться на подсети, в которых максимальное количество идентификаторов узлов одинаковое.

Однако поддержка масок подсети переменной длины (variable-length subnet mask, VLSM) позволяет маршрутизаторам обслуживать разные маски. Чаще всего VLSM применяют для разбиения на подсети самих подсетей. Допустим, большой организации принадлежит большое адресное пространство 131.107.0.0/16. Внешние маршрутизаторы для определения идентификатора сети используют первые 16 бит адреса и в соответствии с этим осуществляют маршрутизацию. При получении данных из Интернета маршрутизаторы организации используют маску подсети /22 для перенаправления трафика в любой из 64 региональных отделений организации. А маршрутизаторы региональных офисов в свою очередь используют маску подсети /25 для маршрутизации трафика в 8 отделов в рамках отделения.

Как и CIDR, работа масок подсетей переменной длины основана на бесклассовых протоколах маршрутизации, таких как RIP версии 2 и OSPF. VRLM несовместим с более старыми протоколами маршрутизации (например, с RIP версии 1).

Использование VLSM для поддержки подсетей разного размера

VLSM также позволяет разбивать сеть на подсети разных размеров на одном уровне иерархии и более эффективно использовать адресное пространство.

Например, если одна подсеть должна объединять 100 компьютеров, вторая — 50, а третья — 20, то не удастся обойтись традиционной маской по умолчанию для единственного идентификатора сети класса C. Как видно из табл. 2-5, никакая из масок подсети по умолчанию не обеспечивает одновременно достаточное число подсетей и узлов в подсети.

Табл. 2-5. Параметры маски подсети класса C (статические)

Сетевой адрес	Число подсетей	Число узлов в подсети
208.147.66.0/24	1	254
208.147.66.0/25	2	126
208.147.66.0/26	4	62
208.147.66.0/27	8	30

В таких ситуациях проблему решает VLSM. При этом не надо обращаться к Интернет-провайдеру за новым диапазоном адресов.

При разбиении на подсети различного размера нужно использовать специальный шаблон с завершающими нулями; сеть класса C поддерживает до семи подсетей. Завершающие нули нужны для предотвращения пересечения адресных пространств подсетей.

Если идентификатор подсети с маской переменной длины соответствует шаблону из табл. 2-6, подсети не пересекутся, и адреса будут интерпретироваться однозначно.

Табл. 2-6. Идентификаторы подсети на основе VLSM

Номер подсети	Идентификатор подсети (двоичный)	Маска подсети	Количество узлов	Пример адреса подсети
1	0	255.255.255.128	126	208.147.66.0.0/25
2	10	255.255.255.192	62	208.147.66.0.128/26
3	110	255.255.255.224	30	208.147.66.0.192/27
4	1110	255.255.255.240	14	208.147.66.0.224/28
5	11110	255.255.255.248	6	208.147.66.0.240/29
6	111110	255.255.255.252	2	208.147.66.0.248/30
7	НИИ	255.255.255.252	2	208.147.66.0.252/30

На рис. 2-17 показано, как с помощью VLSM построить 3 сети с 100, 50 и 20 узлами соответственно.

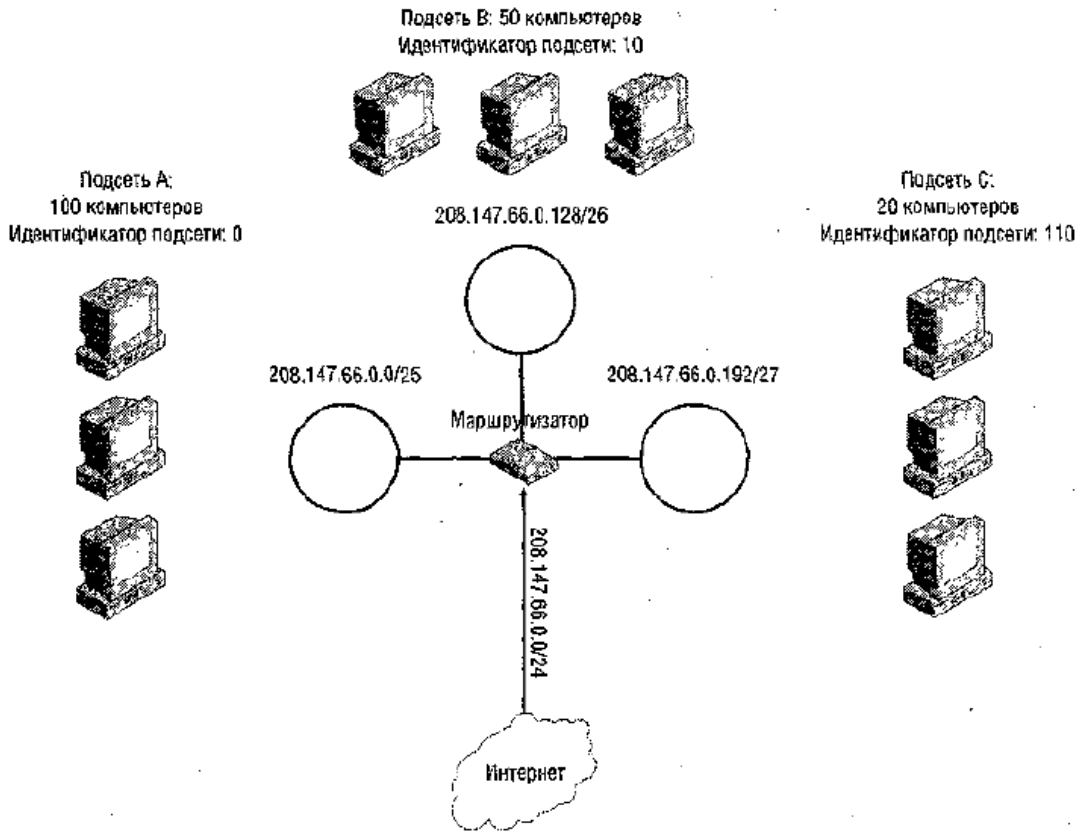


Рис. 2-17. VLSM дает дополнительную гибкость при разбиении на подсети.

Увеличение количества доступных узлов средствами VLSM.

Обратите внимание, что в табл. 2-6 седьмая (и последняя) подсеть имеет такое же количество узлов, как и шестая, отличаются только идентификаторы подсети, да и то всего одним битом (в идентификаторе 7-й сети в отличие от остальных

отсутствует завершающий нуль). Можно не использовать все семь подсетей — достаточно определить состоящий из одних единиц идентификатор подсети на любом уровне, который заменит все перечисленные в следующих строках таблицы подсети. Например, определить идентификатор подсети 1111, который заменит подсети 5—7 (см. табл. 2-6). Благодаря этому вы получите еще одну подсеть с 14 узлами вместо 3 подсетей, вместе содержащих только 10 узлов. Это позволит максимизировать количество узлов, которые вмещает сеть, состоящая из 5 подсетей.

Если сеть класса C разбита на 3, 5, 6 или 7 подсетей, VLSM позволяет максимизировать количество доступных узлов.