**Сети и телекоммуникации в КИС**

**Основы компьютерных сетей**

**Что такое компьютерная сеть**

Компьютеры имеют огромное значение в современном мире, а компьютерные вычислительные сети и телекоммуникации значительно дают новые возможности в работе и расширяют отдых. После появления вычислительных машин возникла естественная идея связать их между собой для более эффективного использования их программных и аппаратных ресурсов. Первые сети соединяли большие ЭВМ в государственных вычислительных центрах. Однако с течением времени сетевые технологии распространились на другие организации, а затем, с появлением персональных компьютеров (ПК), пришли практически в каждый дом. Компьютеры объединили в локальные вычислительные сети (ЛВС), а эти сети соединили друг с другом, подключив к региональным и глобальным сетям. В итоге за последние годы сотни миллионов компьютеров в мире были объединены в сети, и более миллиарда пользователей получили возможность взаимодействовать друг с другом.

Сегодня компьютерные сети стали неотъемлемой частью жизни, а область их применения охватывает все сферы человеческой деятельности.

Ранее, когда были отдельные, не связанные в сеть компьютеры, то, чтобы работать с одними и теми же данными, нужно с одного компьютера скопировать эти файлы на носитель (например, на дискету) и перенести эти файлы на другие компьютеры. Для распечатки документов надо было снабдить каждый из компьютеров отдельным принтером. Одновременная и совместная работа нескольких пользователей с одним и тем же документом в такой ситуации исключалось.

Теперь компьютеры соединены в сеть (рис. 4.1) и настроен общий доступ к общим ресурсам. Дискеты больше не нужны и принтер требуется лишь один.

Теперь дадим первые определения.

*Сеть*(*Network*) **-** группа компьютеров и/или других устройств, каким-либо способом соединенных для обмена информацией и совместного использования ресурсов.

*Ресурсы*(*Resourses*) **-** это программы, файлы данных, а также принтеры и другие, совместно используемые периферийные устройства в сети.

Возможно множество различных способов классификации компьютерных сетей. Рассмотрим основные из них.

В зависимости от *расстояния между узлами* сети можно разделить на три основных класса: *локальные, региональные* и *глобальные* (рис. 4.2).

*Локальной вычислительной сетью (ЛВС)*(*Local Area Network, LAN*) –называют небольшую группу компьютеров, связанных друг с другом и расположенных в пределах одного здания или организации. Более точно можно определить как ***локальную*** такую сеть, которая позволяет пользователям не замечать связи. По сути, компьютеры, связанные локальной сетью, объединяются в один виртуальный компьютер, ресурсы которого могут быть доступны всем пользователям, причем этот доступ не менее удобен, чем к ресурсам, входящим непосредственно в каждый отдельный компьютер.

*Региональная сеть*(*Metropolitan Area Network*) **-** сеть, соединяющая множество локальных сетей в рамках одного района, города или региона.

*Глобальная сеть*(*Wide Area Network*) - сеть, объединяющая компьютеры разных городов, регионов и государств.

Объединение глобальных, региональных и локальных вычислительных сетей позволяет создавать многоуровневые иерархии, которые предоставляют мощные средства для обработки огромных массивов данных и доступ к практически неограниченным информационным ресурсам.

На рис. 4.3 приведена одна из возможных иерархий вычислительных сетей. Локальные вычислительные сети (ЛВС) в качестве компонентов могут входить в состав региональной сети; региональные сети - объединяться в составе глобальной сети; наконец, глобальные сети могут образовывать еще более крупные структуры. Самым большим объединением компьютерных сетей на сегодня является «сеть сетей» - *Интернет*(*Internet*)*.*

Современным примером связи локальных и глобальных сетей является *виртуальная частная сеть (Virtual Private Network, VPN).* Так называется сеть организации, получающаяся в результате объединения нескольких территориально разделенных ЛВС с помощью общедоступных каналов глобальных сетей, например, через Интернет (рис. 4.4). *По типу среды передачи* сети делятся на *проводные* и *беспроводные* (рис. 4.5), а по *скорости передачи информации* - на *низко-, высоко-* и *сверхвысокоскоростные* (рис. 4.6). С точки зрения *распределения ролей между компьютерами* сети бывают *одноранговые* и *клиент-серверные* (рис. 4.7).

*Сервер*(*Server*) – это специально выделенный высокопроизводительный компьютер, оснащенный соответствующим программным обеспечением (ПО), централизованно управляющий работой сети и/или предоставляющий другим компьютерам сети свои ресурсы (файлы данных, накопители, принтер).

*Клиентский компьютер* (клиент**-** *Client***,** рабочая станция) **-** компьютер или программа пользователя сети, получающие доступ к ресурсам сервера (серверов).

Поскольку понятия одноранговых и клиент-серверных сетей очень важны, рассмотрим их подробнее.

В *одноранговой* сети (рис. 4.8) все компьютеры равноправны, каждый из них может выступать как в роли сервера, т. е. предоставлять файлы, ПО и аппаратные ресурсы (накопители, принтеры и пр.) другим компьютерам, так и в роли клиента, пользующегося ресурсами других компьютеров.

Преимущества и недостатки одноранговых сетей

|  |  |
| --- | --- |
| ***Преимущества*** | ***Недостатки*** |
| ● легкость в установке и настройке;  ● независимость отдельных компьютеров и их ресурсов друг от друга;  ● возможность для пользователя контролировать ресурсы своего собственного компьютера;  ● сравнительно низкая стоимость развертывания и поддержки;  ● отсутствие необходимости в дополнительном программном обеспечении (кроме операционной системы);  ● отсутствие необходимости в постоянном присутствии администратора сети | ●необходимость помнить столько паролей, сколько имеется разделенных ресурсов (для сетей на основе Windows 95/98), либо имен и паролей для входа (для сетей на основе Windows NT/2000 /XP);  ● необходимость производить резервное копирование отдельно на каждом компьютере, чтобы защитить все совместно используемые данные;  ● отсутствие возможности централизованного управления сетью и доступом к данным;  ● низкая общая защищенность сети и данных |

Число компьютеров в одноранговых сетях обычно не превышает десяти, отсюда их другое название - *рабочая группа (Work Group).* Типичными примерами рабочих групп являются домашние сети, сети небольших фирм и офисов.

*Сети с выделенным сервером* (сети типа «клиент-сервер»),как правило, создаются в учреждениях или крупных организациях. В таких сетях (рис. 4.9) выделяются один или несколько компьютеров, называемых *серверами,* задача которых состоит в быстрой и эффективной обработке большого числа запросов других компьютеров - *клиентов.* Обычно в роли серверов выступают мощные и надежные компьютеры. Они часто оснащают специализированным оборудованием, например емкими хранилищами данных («RAID-массивами»), накопителями на ленте для резервного копирования, высокоскоростными сетевыми адаптерами и т.д. Такие компьютеры работают постоянно, круглосуточно предоставляя пользователям свои ресурсы и обеспечивая доступ к своим *службам (services),* работающим на серверах программам, выполняющие действия по запросу клиента.

Преимущества и недостатки клиент-серверных сетей

|  |  |
| --- | --- |
| ***Преимущества*** | ***Недостатки*** |
| ● использование мощного серверного оборудования обеспечивает быстрый доступ к ресурсам и эффективную обработку запросов клиентов: один сервер может обслуживать тысячи пользователей;  ● централизация данных и ресурсов позволяет наладить четкое управление информацией и пользовательскими данными;  ● размещение данных на сервере существенно упрощает процедуры резервного копирования;  ● повышается общая защищенность сети и сохранность данных | ●неисправность сервера может сделать всю сеть практически неработопособной, а ресурсы - недоступными;  ●сложность развертывания и поддержки требует наличия квалифицированного персонала, что увеличивает стоимость сопровождения сети;  ●стоимость сопровождения сети также увеличивается из-за потребности в выделенном оборудовании и специализированном программном обеспечении;  ●требуется постоянное присутствие на рабочем месте администраторов |

**Взаимодействие компьютеров в сети (модель OSI)**

Для обеспечения взаимодействия компьютеров, сначала нужно каким-либо образом соединить между собой всех участников сети - серверы, персональные компьютеры (ПК, *PC*) - стационарные рабочие станции пользователей, ноутбуки, карманные компьютеры (КПК), а также принтеры, сетевые хранилища данных и пр.

Для этих целей применяются *сетевые кабели* различных типов, *телефонные* или *спутниковые каналы,* а в последнее время все более популярными становятся *беспроводные решения* (*Wireless LAN - WLAN, Wi-Fi, WiМАХ*).

Для подсоединения кабелей к компьютерам требуются специальные *коннекторы,* закрепленные на их концах. Затем кабель одним концом вставляется в *сетевой адаптер* - специальную плату, установленную в компьютер и позволяющую подключить его к сети, а другим - в какое-либо *устройство связи* (концентратор, мост, коммутатор, маршрутизатор, шлюз и т. д.). В большинстве современных компьютеров сетевой адаптер является встроенным (соответствующий разъем имеется непосредственно на материнской плате).

Если же на компьютере используется *беспроводной сетевой адаптер,* то взаимодействие с сетью происходит за счет передачи радиосигналов между этим адаптером и *точкой доступа,* соединенной с локальной сетью.

Однако соединить компьютеры друг с другом недостаточно - нужно организовать их взаимодействовие друг с другом. Для этого требуются *сетевые операционные системы,* поддерживающие один и тот же *набор протоколов (стек)*, с помощью которых компьютеры общаются по сети. И только после этого, запустив *сетевое приложение,* можно будет решать задачи в сети.

Рассмотрим принципы взаимодействия компьютеров в сети более подробно.

Способов непосредственного общения у них нет, поэтому, чтобы общаться, им приходится прибегать к целому ряду последовательно выполняемых процедур, называемых *сетевыми протоколами* (наборам правил и процедур, регулирующих порядок взаимодействия компьютеров в сети)*.* Чтобы протоколы работали надежно и согласованно, каждая операция в них строго регламентируется. Чтобы программы и оборудование разных производителей могли взаимодействовать друг с другом, протоколы должны соответствовать определенным *стандартам.*

Создано множество различных протоколов - как открытых (опубликованных для бесплатного применения), так и закрытых (разработанных коммерческими компаниями и требующих лицензирования).

Все эти протоколы принято соотносить с так называемой ***эталонной моделью взаимодействия открытых систем*** *(Open Systems Interconnection Reference Model),* или просто *моделью OSI.* Ее описание было опубликовано в 1984 г. Международной организацией по стандартизации (*International Standards Organization, ISO*), поэтому для нее часто используется другое название - ***модель ISO/OSI****.* Эта модель представляет собой набор спецификаций, описывающих сети с неоднородными устройствами, требования к ним, а также способы их взаимодействия.

Модель *OSI* имеет вертикальную структуру, в которой все сетевые функции распределены между семью *уровнями* (рис. 4.10). Каждому такому уровню соответствуют строго определенные операции, оборудование и протоколы. Реальное взаимодействие уровней, т. е. передача информации внутри одного ПК, возможно только по вертикали и только с соседними уровнями (выше- и нижележащими). Логическое взаимодействие(в соответствии с правилами того или иного протокола) между ПК осуществляется по горизонтали – формируется некая виртуальная связь с аналогичным уровнем другого компьютера на другом конце линии связи. Реальная физическая связь между ПК осуществляется лишь на нижнем (физическом) уровне.

Каждый более высокий уровень пользуется услугами нижележащего уровня, зная, в каком виде и каким способом (через какой *интерфейс)* нужно передать ему данные.Задача более низкого уровня - принять данные от верхнего уровня, добавить свою информацию (форматирующую или адресную, которая необходима для правильного взаимодействия с аналогичным уровнем на другом компьютере) и передать данные дальше вниз. Только дойдя до самого нижнего, физического уровня сетевой модели, информация попадает в среду передачи и отправляется компьютеру-получателю. В нем она проходит сквозь все те же слои снизу вверх в обратном порядке, пока не достигнет того же уровня, с которого была послана компьютером-отправителем.

Теперь познакомимся поближе с уровнями модели *OSI* и определим сетевые услуги, которые они предоставляют смежным уровням.

*Уровень 0*- не определен в общей схеме (на рис. 4.10), но весьма важен. Здесь представлены посредники, по которым собственно и происходит передача сигналов: кабели различных типов, радио-, ИК-сигналы и т.п. На этом уровне ничего не описывается, уровень 0 предоставляет физическому уровню 1только *среду передачи.*

*Уровень 1 - Физический* **(***Physical***).** Здесь осуществляется передача неструктурированного потока битов, полученных от вышележащего канального уровня 2, к физической среде - например, в виде электрических или световых сигналов. Физический уровень отвечает за поддержание связи *(link)* и детально описывает электрические, оптические, механические и функциональные интерфейсы со средой передачи: напряжения, частоты, длины волн, типы коннекторов, число и функциональность контактов, схемы кодирования сигналов и т.д.

*Уровень 2 - Канальный* **(***Data Link***) -** обеспечивает передачу данных*,* полученных от вышележащего сетевого уровня 3, через физический уровень 1 между компьютерами одного сегмента сети (соседними ПК).

Информация на этом уровне помещается в *кадры (frames),* где в начале *(заголовке кадра)* содержатся адреса получателя и отправителя, а также управляющая информация, а в конце - *контрольная сумма,* позволяющая выявить возникающие при передаче ошибки (рис. 4.11).

При получении данныхна канальном уровне определяются начало и конец кадра в потоке битов, сам кадр извлекается из потока и проверяется на наличие ошибок. Поврежденные при передаче кадры, а также кадры, для которых не получено подтверждение о приеме,пересылаются заново *(ретранслируются).* Это организуют, как правило, более высокие уровни стека протоколов. Наконец, на канальном уровне обеспечивается управление доступом к среде передачи.

Канальный уровень сложен, поэтому в соответствии со стандартами ***IEEE*** (*Institute of Electrical and Electronics Engineers*)его часто разбивают на 2 подуровня (рис. 4.12): *управления доступом к среде (Media Access Control,**MAC)* и *управления логической связью (Logical Link Control,**LLC).*

Подуровень *MAC* обеспечивает совместный доступ сетевых адаптеров к физическому уровню, определение границ кадров, распознавание *адресов назначения кадров* (эти адреса часто называют *физическими,* или *MAC адресами)*. Подуровень *LLC,* действующий над уровнем MAC, отвечает за установление канала связи и за безошибочную посылку и прием сообщений с данными.

*Уровень 3 - Сетевой* **(***Network***)** - отвечает за обеспечение связимежду любыми точками в сети. Этот уровень осуществляет проводку сообщений по сети*,* которая может состоять из множества отдельных сетей, соединенных множеством линий связи. Такая доставка требует *маршрутизации,* т.е. определения пути доставки сообщения*,* а также решения задач управления потоками данных и обработки ошибок передачи.

*Уровень 4 - Транспортный* **(***Transport***)** **-** *гарантирует* *доставку информации* от одного ПК другому. На этом уровне ПК-отправителя большие блоки данных разбиваются на мелкие *пакеты,* которые затем надежно доставляются ПК-получателю.На транспортном уровне ПК-получателя пакеты собираются в нужной последовательности в исходные блоки данных. Таким образом, транспортный уровень обеспечивает процесс передачи данных*,* скрывая от более высоких уровней все детали и проблемы, связанные с доставкой информации любого объемамежду любыми точкамиво всей сети.

*Уровень 5 - Сеансовый* **(***Session***)** - позволяет двум *сетевым приложениям* на разных компьютерах устанавливать, поддерживать и завершать соединение, называемое *сетевым сеансом.* Этот уровень отвечает также и за восстановление аварийно прерванных сеансов связи. Кроме того, на пятом уровне выполняется преобразование имен компьютеров в сетевые адреса *(распознавание имен),* а также реализуются функции *защиты сеанса.*

*Уровень 6 - Представительский* **(***Presentation***)** - определяет форматыпередаваемой между компьютерами информации. Здесь решаются такие задачи, как перекодировка(перевод информации в вид, понятный для всех участвующих в обмене компьютеров), сжатие и распаковка данных, шифрование и дешифровка, поддержка сетевых файловых систем и т.п.

*Уровень 7 - Прикладной или уровень приложений* **(***Application***) -** обеспечивает интерфейс взаимодействия программ, работающих на компьютерах в сети. С помощью именно этих программ пользователь получает доступ к таким сетевым услугам, как обмен файлами, передача электронной почты, удаленный терминальный доступ и т. д.

Представленная модель *OSI* в основном используется для обучения, а для реализации более подходят и используются другие, большинство из которых соответствуют этой модели лишь до определенной степени.

Например, к моменту появления модели *OSI* уже существовали и показали высокую эффективность другие наборы (стеки) протоколов, например, *стек* ***TCP/IP***. Поэтому построенный в полном соответствии с описанной выше моделью *набор протоколов OSI* так и не получил широкого распространения. Несмотря на это, сама модель *ISO/OSI* до сих пор широко используется для описания взаимодействия в сетевых средах.

**Сетевые топологии и способы доступа к среде передачи данных**

При организации компьютерной сети исключительно важным является выбор *топологии*, т.е. компоновки сетевых устройств и кабельной инфраструктуры.Надо определить такую топологию, которая обеспечила бы надежную и эффективную работу сети, удобное управление потоками сетевых данных. Необходимо также, чтобы стоимость создания и сопровождения сети получилась доступной и существовали бы возможности для ее расширения и для перехода к более высокоскоростным технологиям с минимальными затратами. Поэтому необходимо знать, какие бывают сетевые топологии, в чем их преимущества и какие у них недостатки. При этом следует различать понятия *физической топологии,* т.е. способа размещения ЭВМ, сетевого оборудования и их соединения с помощью среды передачи, и *логической топологии* - структуры взаимодействия ЭВМ и характера распространения сигналов по сети.

Существует три базовые топологии, на основе которых строится большинство сетей.

*«Шина»*(*Bus*).В этой топологии все компьютеры соединяются друг с другом в единую разделяемую среду, например, одним кабелем(рис. 4.13). Посланные в такую сеть данные передаются и доступны всем компьютерам*,* но обрабатывает их только тот, аппаратный МАС-адрес сетевого адаптера которого записан в адрес получателя пакета, идущего по сети. Эта топология проста в реализации и малозатратна (требует меньше всего кабеля), однако имеет ряд существенных недостатков.

Такие сети трудно расширять(увеличивать число компьютеров и количество *сегментов* - отдельных отрезков кабеля, их соединяющих).

Поскольку шина используется совместно, в каждый момент времени передачу может вести только один из компьютеров*.* Если передачу одновременно начинают два или больше компьютеров, возникает искажение сигнала *(столкновение* или *коллизия),* приводящее к повреждению переданных ими кадров. Тогда компьютеры вынуждены приостанавливать передачу, а затем по очереди повторять данные. Влияние столкновений будет тем заметнее, чем выше объем передаваемой по сети информации и больше в ней компьютеров. Эти факторы снижают производительность сети, замедляют ее работу.

«Шина» является пассивной топологией- компьютеры только «слушают» кабель и не могут восстанавливать затухающие при прохождении по сети сигналы. Чтобы удлинить сеть, нужно использовать *повторители (репитеры),* усиливающие сигнал перед его передачей в следующий сегмент.

Надежность сети с топологией «шина» невысока. Когда электрический сигнал достигает конца кабеля, он (если не приняты специальные меры) отражается*,* нарушая работу всего сегмента сети. Чтобы предотвратить такое отражение сигналов, на концах кабеля устанавливаются специальные *резисторы (терминаторы),* поглощающие сигналы. Если же в любом месте кабеля возникает обрыв (нарушение целостности кабеля или его отсоединение от коннектора), то возникают два сегмента, на концах которых сигналы начинают отражаться, и сеть перестает работать. Проблемы, характерные для топологии «шина», привели к тому, что такие сети, столь популярные еще десять лет назад, сейчас практически не используются.

*«Кольцо»*(*Ring*). В данной топологии каждый из компьютеров соединяется с двумя другими так, чтобы от одного он получал информацию, а второму - передавал ее (рис. 4.14). Последний компьютер подключается к первому и сетевое кольцо замыкается*.* Здесьнедостатки несколько перевешивают достоинства, и результате популярные ранее кольцевые сети теперь в ЛВС используются гораздо реже.

Преимущества и недостатки сетей «кольцо»

|  |  |
| --- | --- |
| ***Преимущества*** | ***Недостатки*** |
| ● поскольку у кабелей в этой сети нет свободных концов, терминаторы здесь не нужны;  ● каждый из компьютеров выступает в роли *повторителя,* усиливая сигнал, что позволяет строить сети большой протяженности;  ● из-за отсутствия *столкновений* топология обладает высокой устойчивостью к перегрузкам, обеспечивая эффективную работу с боль-шими потоками передаваемой по сети информации | ●сигнал в «кольце» должен пройти последовательно (и только в одном направлении) через все компьютеры, каждый из которых проверяет, не ему ли адресована информация, поэтому время передачи может быть достаточно большим;  ● выход из строя хотя бы одного из ПК или устройств может нарушить работу всей сети;  ●обрыв или короткое замыкание в любом из кабелей кольца делает работу всей сети невозможной;  ●чтобы избежать остановки работы сети при отказе ПК или обрыве кабеля, обычно прокладывают два кольца, что удорожает сеть |

Активная топология*«звезда»*(*Active Star*).Эта топология возникла, когда к мощному центральному компьютеру подключались все остальные абоненты сети. В такой конфигурации все потоки данных шли исключительно через центральный компьютер - он полностью отвечал за управление информационным обменом между всеми участниками сети. Конфликты при такой организации взаимодействия в сети были невозможны, однако нагрузка на центральный компьютер была так значительна, что ничем другим, кроме обслуживания сети, этот компьютер, как правило, не занимался. Выход его из строя приводил к отказу всей сети, тогда как отказ периферийного компьютера или обрыв связи с ним на работе остальной сети не сказывался. Сейчас такие сети встречаются довольно редко.

Гораздо более распространенной сегодня топологией является похожий вариант - *«звезда-шина»* (*Star Bus*), или **«***пассивная звезда»* (рис. 4.15). Здесь периферийные компьютеры подключаются не к компьютеру, а к пассивному *концентратору* (хабу*, hub).* Он, в отличие от центрального компьютера, никак не отвечает за управление обменом данными, а выполняет те же функции, что и повторитель, то есть восстанавливает приходящие сигналы и пересылает их всем остальным подключенным к нему компьютерам и устройствам. Именно поэтому данная топология, хотя физически выглядит как «звезда», логически является топологией «шина».

Несмотря на больший расход кабеля, характерный для сетей типа «звезда», эта топология имеет существенные преимущества перед остальными, что и обусловило ее широчайшее применение в современных сетях:

*надежность* - подключение к центральному концентратору и отключение компьютеров от него никак не отражается на работе остальной сети; обрывы кабеля влияют только на единичные компьютеры; терминаторы не требуются;

*легкость при обслуживании и устранении проблем* - все компьютеры и сетевые устройства подключаются к центральному устройству, что существенно упрощает диагностику, обслуживание и ремонт сети;

*защищенность* - концентрация точек подключения в одном месте позволяет легко ограничить доступ к жизненно важным объектам сети.

Если вместо концентраторов использовать более «интеллектуальные» сетевые устройства *(коммутатор* или *маршрутизатор*), то получается промежуточный тип топологии, когда устройство связи не только передает поступающие сигналы, но и производит управление их обменом.

Реальные компьютерные сети постоянно расширяются и модернизируются. Поэтому почти всегда такая сеть является *гибридной,* т. е. ее топология представляет собой комбинацию нескольких базовых топологий - «звезды» и «шины», либо «кольца» и «звезды».

Особо следует выделить топологию*«дерево»*(*tree*), которую можно рассматривать как объединение нескольких «звезд» (рис. 4.16). Эта топология сегодня является наиболее популярной при построении ЛВС.

Надо упомянуть о *сеточной*(*mesh*)топологии,в которой все, либо многие компьютеры и другие устройства соединены друг с другом напрямую (рис. 4.17). Такая топология очень надежна - при обрыве любого канала передача данных не прекращается, поскольку возможно несколько маршрутов доставки информации*.* Сеточные топологии (чаще всего не полные, а частичные) используются там, где требуется обеспечить максимальную отказоустойчивостьсети, например, при объединении нескольких участков сети крупного предприятия или при подключении к Интернету, хотя при этом существенно увеличивается расход кабеля, усложняется сетевое оборудование и его настройка.

С сетевой топологией тесно связано понятие *способа доступа к среде передачи,* под которым понимается набор правил, определяющих, как именно компьютеры должны отправлять и принимать данные по сети.

Таких способов возможно несколько. Основными из них являются:

множественный доступ с контролем несущей и обнаружением столкновений (*CSMA/CD)*;

множественный доступ с контролем несущей с предотвращением столкновений (*CSMA/CA)*;

передача маркера (*Token Passing*).

При *множественном доступе с контролем несущей и обнаружением столкновений* (*Carrier* *Sense Multiple Access with Collision Detection, CSMA/CD*) все компьютеры (множественный доступ)«слушают» кабель (контроль несущей),чтобы определить, передаются по нему данные или нет. Если кабель свободен, любой компьютер может начать передачу; тогда все остальные компьютеры должны ждать, пока кабель не освободится. Если компьютеры начали передачу одновременно и возникло столкновение, они приостанавливают передачу *(обнаружение столкновений),* каждый - на разные промежутки времени, после чего ретранслируют данные.

Серьезным недостатком этого способа доступа является то, что при большом количестве компьютеров и высокой нагрузке на сеть число столкновений возрастает, а пропускная способность падает, иногда очень существенно. Однако этот метод очень прост в технической реализации, поэтому именно он используется в наиболее популярной сегодня *технологии Ethernet.* А чтобы уменьшить количество столкновений, в сетях применяются такие устройства, как мосты, коммутаторы и маршрутизаторы.

Метод *множественного доступа с контролем несущей и предотвращением столкновений* (*Carrier Sense Multiple Access with Collision Avoidance, CSMA/CA*) отличается от предыдущего тем, что перед передачей данных компьютер посылает в сеть специальный небольшой пакет, сообщая остальным компьютерам о своем намерении начать трансляцию. Так другие компьютеры узнают о готовящейся передаче, что позволяет избежать столкновений. Конечно, эти уведомления увеличивают общую нагрузку на сеть и снижают ее пропускную способность (из-за чего метод *CSMA/CA* работает медленнее, чем *CSMA/CD*), однако они, безусловно, необходимы для работы, например, беспроводных сетей.

В сетях с *передачей маркера* (*Token Passing*) от одного компьютера к другому по кольцу постоянно курсирует небольшой блок данных, называемый *маркером.* Если у компьютера, получившего маркер, нет информации для передачи, он просто пересылает его следующему компьютеру. Если же такая информация имеется, компьютер «захватывает» маркер,дополняет его данными и отсылает все это следующему компьютеру по кольцу. Такой информационный пакет передается от компьютера к компьютеру, пока не достигает станции назначения. Поскольку в момент передачи данных маркер в сети «захвачен», другие компьютеры ничего передавать не могут. Поэтому в сетях с передачей маркера невозможны ни столкновения, ни временные задержки, что делает их весьма привлекательными для использования в системах автоматизации работы предприятий.

Таким образом, при выборе типа сети следует учитывать:

*имеющуюся кабельную систему и оборудование* - есть ли уже сеть, которую нужно расширить, или имеются только отдельные компьютеры;

*физическое* *месторасположение* – т.е., как расположены компьютеры, и где можно разместить сетевое оборудование. Объединить ПК в одной комнате просто, однако если они располагаются на разных этажах или в зданиях, конфигурацию сети и ее топологию надо тщательно продумать;

*размеры* *планируемой* *сети* - если имеется лишь несколько компьютеров, структура сети будет простой; если же компьютеров сотни или тысячи, то, скорее всего, придется остановить свой выбор на сложной гибридной топологии;

*объем и тип информации для совместного использования* - эти параметры надо обязательно учитываться при выборе типа сети: если между компьютерами передаются большие файлы - видео или графические, то потребуется высокоскоростная сеть, позволяющая быстро и без задержек передавать значительные объемы информации.

Подавляющее большинство современных сетей используют топологию *«звезда*» или *гибридную топологию,* представляющую собой объединение нескольких «звезд» (топологию типа «дерево») и метод доступа к среде передачи *CSMA/CD.*

**Линии связи**

Чтобы компьютеры могли взаимодействовать, необходима некоторая промежуточная среда, обеспечивающая возможность передачи сигналов на физическом уровне. *Среда передачи* может представлять собой *кабельную инфраструктуру* (набор проводов различных типов), соединительных *разъемов (коннекторов)* и *устройств связи.* Но она может быть атмосферой или даже безвоздушным пространством, - лишь бы имелась возможность каким-то образом передать сигналот одного компьютера к другому.

Наиболее часто в компьютерных сетях применяются *кабельные соединения*, выступающие в качестве среды передачи электрических или оптических сигналов между компьютерами и другими сетевыми устройствами. При этом используются следующие типы кабеля:

коаксиальный кабель (*coaxial cable*);

витая пара (*twisted* *pair*): неэкранированная (*unshielded, UTP*) или экранированная (*shielded, STP*);

волоконно-оптический или оптоволоконный кабель (*fiber optic*).

На начальном этапе становления ЛВС сетей в основном применялся *коаксиальный кабель,* состоящий из передающей сигнал медной или алюминиевой жилы, слоя изоляции, экранирующей оплетки из медных проводов или алюминиевой фольги и защитной внешней оболочки (рис. 4.18). Для передачи сигнала в коаксиальном кабеле использовалась центральная жила, а оплетка заземлялась, выступая в роли «электрического нуля».

Использовались два типа кабеля - «тонкий» и «толстый».

*Тонкий коаксиальный кабель* - гибкий, диаметром около 0,5 см, позволял передавать данные без затухания на расстояния до185 м (в реальности - до 300 м). Для подключения кабеля к сетевым устройствам применялись специальные *разъемы типа BNC* (*Bayonet* *Neill-Concelman* - от фамилий изобретателей разъема, или *Bayonet* *Navy* *Connector*, *British* *Naval* *Connector* или *Bayonet* *Nut* *Connector*).

На концах отрезков кабеля монтировались *BNC*-коннекторы. Сращивание этих отрезков производили с помощью *I*-коннекторов (или «баррел-коннекторов»), а для соединения с сетевыми адаптерами и устройствами использовались *Т*-коннекторы. Чтобы отраженный сигнал поглощался на концах кабеля, там устанавливали *BNC*-терминаторы, один из которых обязательно заземлялся (рис. 4.19).

*Толстый коаксиальный кабель* - жесткий, диаметром около 1 см. В нем медная жила толще, чем у тонкого коаксиального кабеля и ее электрическое сопротивление меньше. Поэтому толстый коаксиальный кабель позволял передавать сигнал на расстояния до 500 м. Для подключения к нему применялись специальные устройства - *трансиверы* (от «*transmitter-receiver*» - «приемопередатчик»). В качестве разъемов использовались *AUI*- или *DIX*-коннекторы.

Широкое распространение сетей, построенных на основе коаксиального кабеля, было вызвано двумя обстоятельствами: дешевизной и простотой - достаточно было проложить магистральный кабель, установить на его концах терминаторы и подключить к нему компьютеры. Тем не менее сейчас коаксиальный кабель в большинстве сетей заменен витой парой или оптическими кабелями.

*Витая пара –* два скрученных друг с другом изолированных медных провода. Подавляющее большинство кабелей на основе витой пары состоит из четырех пар, перевитых с разным шагом для уменьшения электрических наводок со стороны соседних пар и внешних источников и покрытых пластиковой оболочкой (рис. 4.20).

В *экранированной витой паре,* кроме того, используется одна или несколько оплеток из алюминиевой или медной фольги, существенно повышающих помехозащищенность кабеля.

Такие кабели выпускаются в соответствии со стандартом *EIA/TIA 568* (американский стандарт проводки в коммерческих зданиях) и подразделяются на *категории.* Кабели разной категории различаются, в первую очередь, шагом скрутки витых пар. Чем меньше шаг, тем выше категория и тем больших скоростей передачи данных можно достичь при его использовании (табл. 4.1).

Таблица 4.1Категории кабеля «витая пара»

|  |  |
| --- | --- |
| Категория | **Характеристика** |
| 1 | Телефонный кабель для передачи голоса или данных с помощью аналоговых модемов |
| 2 | Старый 2-х парный тип кабеля. Поддерживает передачу данных со скоростью **до 4 Мбит/с**. Использовался в сетях Token Ring и ARCNet. Сегодня иногда применяется в телефонных сетях |
| 3 | 2-х и 4-х парный кабель. Использовался в сетях Token Ring и 10BASE-T. Поддерживает передачу данных со скоростью только **до 10Мбит/с**. Применяется в телефонных сетях |
| 4 | 4-х парный кабель. Использовался в сетях Token Ring, 10BASE-T, 10BASE-T4 для скоростей **до 16 Мбит/с**. Сегодня практически не используется |
| 5 | Именно этот 4-х парный кабель имеют в виду под названием «витая пара». Способен передавать данные со скоростью **до 100 Мбит/с** при использовании двух пар (Fast Ethernet) и до **1000 Мбит/с** - при использовании всех четырех пар (Gigabit Ethernet). Наиболее распространен в современных локальных сетях, хотя при прокладке новых сетей чаще применяется кабель категории 5е, лучше пропускающий высокочастотные сигналы. Выпускается также в экранированном варианте |
| 6 | 4-х парный кабель (экранированный или неэкранированный). Способен передавать данные со скоростью **до 10000 Мбит/с** (10 Gigabit Ethernet) на частотах до 200 МГц. В кабелях категории 6е предельная частота передачи увеличена до 500 МГц. Более половины современных сетей строится с использованием кабеля этой категории |
| 7 | 4-х парный кабель, спецификация для которого еще окончательно не утверждена. Скорость передачи данных - **до 10000 Мбит/с**, частота пропускания - до 600-700 МГц. Все отдельные пары и сам кабель для этой категории экранированы |

Благодаря дешевизне, легкости в установке и универсальности, неэкранированная витая пара является сейчас самым распространенным в ЛВС типом кабеля. Экранированная витая пара, несмотря на большую помехозащищенность, не получила широкого распространения из-за сложностей в установке - требуется заботиться о заземлении, кабель более жесткий.

Витая пара подключается к компьютерам и другим устройствам с помощью восьми контактного разъема *RJ-45* (*Registered Jack 45*). Этот коннектор (рис. 4.21) похож на применяемый в телефонных линиях коннектор *RJ-11*, только немного больше него. В табл. 4.2 приведено описание способов заделки кабеля «витая пара» в коннектор *RJ-45* в соответствии со стандартами *EIA/TIA 568A* и *568В*; эта операция выполняется с помощью специального обжимного инструмента. (Если расположить разъем контактами вверх и от себя, то нумеровать их надо слева направо, от 1 до 8.)

Таблица 4.2 - Разводка проводников в *RJ-45*

|  |  |  |
| --- | --- | --- |
| Контакт | Цвет оплетки провода | |
| *568А* | *568В* |
| 1 | бело-зеленый | бело-оранжевый |
| 2 | зеленый | оранжевый |
| 3 | бело-оранжевый | бело-зеленый |
| 4 | голубой | голубой |
| 5 | бело-голубой | бело-голубой |
| 6 | оранжевый | зеленый |
| 7 | бело-коричневый | бело-коричневый |
| 8 | коричневый | коричневый |

Кабели для подключения ПК к концентраторам и коммутаторам, обжимаются с двух сторон одинаково. При этом получается так называемый *прямой кабель.* Однако для непосредственного соединения сетевых адаптеров ПК либо для связи между концентраторами используется *перекрестный кабель («кросс-кабелъ»).* С одной стороны такого кабеля витые пары при их заделке в разъем меняют местами: зеленый провод - на место оранжевого.

*Оптоволоконный кабель* (рис. 4.22) отличается от других видов сетевой проводки тем, что передает световые, а не электрические импульсы. Он похож на коаксиальный, но вместо металлической жилы используется стекловолокно. При этом могут применяться два вида оптоволоконных кабелей: *многомодовый* (*multi-mode*) или *одномодовый* (*single-mode*). В дешевом многомодовом кабеле центральное стекловолокно имеет диаметр 50 или 62,5 мкм, а оболочка - 125 мкм. Для передачи сигналов по нему применяют недорогие *светодиодные трансиверы* с длиной волны 850 нм. В высококачественном и дорогом одномодовом кабеле волокно тоньше - диаметр 9-10 мкм, а затухание светового сигнала в нем много меньше. Для передачи сигналов по нему используются *лазерные трансиверы* с длиной волны 1300 нм. В результате максимальное расстояние передачи светового сигнала при применении одномодовых кабелей и трансиверов гораздо больше, чем для многомодовых. Для подключения оптоволоконного кабеля используются специальные коннекторы (рис. 4.23). *Коннекторы FC* и *ST* сегодня считаются устаревшими, поэтому в новом оборудовании чаще всего применяются разъемы для *коннекторов SC****.***Монтаж коннекторов (заделка кабеля в коннектор) сложен и требует специального оборудования. По сравнению с электрическими кабелями оптоволокно обеспечивает намного лучшие параметры помехозащищенности и защиты передаваемого сигнала от перехвата. Кроме того, при его использовании данные удается передавать на существенно большие расстояния, да и теоретически возможные скорости передачи в оптоволокне намного выше.

Недостатки оптоволокна: большая стоимость кабеля, сложность заделки коннекторов и необходимость применения дополнительных трансиверов, преобразующих световые сигналы в электрические и обратно. Все это существенно повышает общую стоимость развертывания сети, поэтому до сих пор оптоволокно в локальных сетях применяется реже, чем витая пара.

Основные проблемы, характерные для всех проводных сетей, - их низкая мобильность*,* довольно большие капиталовложения в кабельную инфраструктуру и относительно малая дальность передачи сигнала. К беспроводным сетям это относится в меньшей степени, поэтому они все чаще входят в практику создания сетей. Хотя «кабель» в беспроводных сетях отсутствует, среда передачи в них существует.

Используют несколько способов:

при использовании *радиосвязи* данные пересылают на радиочастотах и практически не имеют ограничений по дальности, используются как в локальных сетях, так и для сетевых соединений на больших расстояниях. Поскольку радиосигналы легко перехватить, требуется обязательная защита данных кодированием и/или шифрованием;

передача *микроволновом диапазоне* использует более высокие частоты и применяется как на коротких расстояниях (объединение локальных сетей в разных зданиях), так и в глобальных коммуникациях - с помощью спутников и наземных спутниковых антенн. Главное ограничение такой связи: передатчик и приемник должны быть в зоне прямой видимости;

*инфракрасное излучение* (ИК)применяется для двусторонней или широковещательной передачи на близких расстояниях в помещениях и для взаимодействия с портативными (мобильными) устройствами. ИК-сигналы блокируются любыми предметами, а также подвержены помехам со стороны сильных источников света и тепла, которые есть практически в любом помещении;

применяют *световое излучение в видимом диапазоне*, хотя этот способ передачи используется редко. Этот способ соединения может быть удобен для связи между высотными зданиями.

**Локальные сети (Token Ring, Ethernet, Wi-Fi , WiMAX)**

Для выбора сети нужно определиться с *сетевой архитектурой* - набором стандартов, топологий и протоколов низкого уровня, необходимых для создания работоспособной сети. Рассмотрим основные сетевые архитектуры, их преимущества и недостатки и выберем из них наилучшую: высокоскоростную, надежно функционирующую и расширяемую.

За многие годы развития сетевых технологий было разработано множество различных архитектур. Большинство из них вышли из употребления, а лучшие активно используются по сей день и постоянно совершенствуются.

1). Технология ***Token Ring*** была разработана компанией IBM в 70-х гг., а затем стандартизована как спецификация *IEEE 802.5*.

Она имеет следующие основные характеристики:

- физическая топология - «звезда», логическая топология - «кольцо»;

- метод доступа - передача маркера;

- скорость передачи данных - 4 или 16 Мбит/с;

- максимальный размер кадра - до 16 Кбайт;

- среда передачи - витая пара (используется 2 пары);

- максимальная длина сегмента:

UTP - 150 м (для 4 Мбит/с) или 60 м (для 16 Мбит/с),

STP - 300 м (для 4 Мбит/с) или 100 м (для 16 Мбит/с);

- максимальная длина сегмента с репитерами:

UTP - 365 м, STP **-** 730 м;

- максимальное количество ПК на сегмент **-** 72 и 260 (от типа кабеля).

Для объединения компьютеров в сетях *Token Ring* (рис. 4.24) используются *концентраторы MSAU* (*Multi*-*Station Access Unit*), неэкранированная или экранированная витая пара (возможно и применение оптоволокна), в качестве разъемов используются специализированные соединители фирмы IBM либо стандартные коннекторы *RJ-45*.

К преимуществам архитектуры *Token* *Ring* можно отнести высокую дальность передачи, а также легкое определение максимальной задержки при передаче информации между любыми двумя устройствами - ведь в качестве метода доступа к среде используется передача маркера.

Недостатки архитектуры *Token Ring* - довольно высокая стоимость, низкая совместимость оборудования (например, в 16-мегабитных сетях *Token Ring* нельзя использовать 4-мегабитные устройства), а также довольно малая скорость передачи данных. Однако, в настоящее время имеются версии *Token*-*Ring* на скорость в 100Мбит/с (*High Speed Token-Ring, HSTR*) и на 1000 Мбит/с (*Gigabit Token-Ring*). Компании, поддерживающие *Token*-*Ring*, не намерены отказываться от своей сети, рассматривая ее как достойного конкурента *Ethernet*.

2). Технология ***Ethernet*** первоначально она была создана фирмой *Xerox* в середине 70-х гг. и тогда представляла собой систему передачи со скоростью 2,93 Мбит/с. После доработки с участием компаний *Intel* и *DEC* архитектура *Ethernet* послужила основой принятого в 1985г. стандарта *IEEE**802.3*, определившего следующие параметры:

- топология - «шина», метод доступа - *CSMA/CD*;

- скорость передачи - 10 Мбит/с;

- среда передачи – коаксиальный кабель;

- максимальная длина сегмента сети с толстым коаксиальным кабелем - до 500м, а сети **-** до 2,5 км;

- максимальное количество компьютеров в сегменте 100, в сети - 1024.

В исходной версии *Ethernet* предусматривалось применение коаксиального кабеля двух видов - «толстого» и «тонкого» (стандарты *10Base-5* и *10Bаse-2*, рис.4.13). Однако в начале 90-х гг. появились спецификации для построения сетей *Ethernet* с использованием витой пары (*10Base-T*) и оптоволокна (*10Base-FL*), рис. 4.15, 4.16.

Архитектура *Ethernet* фактически объединяет целый набор стандартов, имеющих как общие черты, так и отличия:

- в 1995 г., был опубликован стандарт архитектуры ***Fast Ethernet*** (*IEEE 802.3u*), обеспечивающей передачу на скоростях до 100 Мбит/с:

- в 1998 г. - стандарт ***Gigabit Ethernet*** (*IEEE 802.3z* и *802.3ab*);

- в 2002 г. - стандарт ***10 Gigabit Ethernet*** (*IEEE 802.3ае*).

Сравнение различных стандартов *Ethernet* представлено в табл. 4.4.

Заметим, что в современных версиях *Ethernet* использование физической топологии «шина» уже не предусмотрено, да и найти сейчас сети, построенные на коаксиальном кабеле, весьма затруднительно.

Основной недостаток сетей *Ethernet* связан с использованием в них метода доступа к среде *CSMA/CD*.

При увеличении количества компьютеров растет число столкновений, что снижает пропускную способность сети и увеличивает время доставки кадров. Поэтому рекомендуемой нагрузкой для сетей *Ethernet* считается уровень в 30-40 % от общей полосы пропускания.

В современных сетях этот недостаток легко устраняется путем замены *концентраторов* *- мостами* и *коммутаторами,* умеющими «изолировать» передачу данных между двумя компьютерами в сети от других.

Таблица 4.4Характеристики различных стандартов *Ethernet*

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Реализация | Скорость, Мбит/с | | Топология | | Среда передачи | | | Максимальная длина кабеля, м |
| ***Ethernet*** | | | | | | | | |
| *10Base-5* | 10 | | «шина» | | толстый коаксиальный кабель | | | 500 |
| *10Base-2* | 10 | | «шина» | | тонкий коаксиальный кабель | | | 185;  реально - до 300 |
| *10Base-T* | 10 | | «звезда» | | витая пара | | | 100 |
| *10Base-FL* | 10 | | «звезда» | | оптоволокно | | | 500 (ПК - концентратор);  2000 (между ПК) |
| ***Fast Ethernet*** | | | | | | | | |
| *100Base-TX* | 100 | | «звезда» | | витая пара категории 5 (2 пары) | | | 100 |
| *100Base-T4* | 100 | | «звезда» | | витая пара категории 3, 4 или 5 (4 пары) | | | 100 |
| *100Base-FX* | 100 | | «звезда» | | многомодовое или одномодовое оптоволокно | | | 2000 м (многомодовый),  15-40 км (одномодовый) |
| ***Gigabit Ethernet*** | | | | | | | | |
| *1000Base-T* | | 1000 | | «звезда» | | витая пара категории 5 и выше | 100 | |
| *1000Base-CX* | | 1000 | | «звезда» | | специальный кабель типа STP | 25 | |
| *1000Base-SX* | | 1000 | | «звезда» | | оптоволокно | 220-550 (многомодовый) | |
| *1000Base-LX* | | 1000 | | «звезда» | | оптоволокно | 550 (многомодовый);  5-80 км(одномодовый) | |
| ***10 Gigabit Ethernet*** | | | | | | | | |
| *10GBase-х* | | 10000 | | «звезда» | | оптоволокно | 0,3-40км (от типа кабеля и длины волны) | |
| *10GBase-Т* | | 10000 | | «звезда» | | ВП (STR) категории 7 | 100 | |

Преимуществ у архитектуры *Ethernet* много.

Прежде всего, сама эта технология довольно проста в реализации, а поэтому *Ethernet*-устройства (сетевые адаптеры, концентраторы, коммутаторы и т.д.) оказываются значительно дешевле аналогичных устройств других сетевых архитектур.

В *Ethernet* можно использовать практические любые виды кабеля, а применение оптоволокна позволяет объединять участки сетей далеко друг от друга.

Совместимость различных вариантов *Ethernet* очень высока, что позволяет не только наращивать мощности сети с использованием существующей кабельной инфраструктуры, но и легко расширять сеть, подключая к ней новые, более скоростные сегменты.

Сегодня архитектура *Ethernet* не только стала господствующей в локальных сетях, но и вытесняет другие технологии в региональных и глобальных сетях.

Перейдем теперь к беспроводным сетевым решениям, из которых в ЛВС сейчас наиболее часто применяются технологии *Wi-Fi* и *Bluetooth*.

3). Технология ***Wi-Fi*** («*Wireless Fidelity*», «беспроводная точность») - популярная технология, обеспечивающая беспроводное подключение мобильных пользователей к локальной сети и Интернету (рис. 4.25). Под именем *Wi-Fi* скрывается несколько стандартов, разработанных для беспроводных сетей на основе выпущенной еще в 1997 г. спецификации *IEEE 802.11* (табл. 4.5).

Важно отметить, что в стандарте *802.11* предусматривается использование только *полудуплексных приемопередатчиков,* которые не могут одновременно передавать и принимать информацию. Из-за этого в беспроводных сетях *802.11* станция в принципе не может обнаружить столкновение во время передачи (поскольку в это время не имеет возможности принимать данные). Поэтому в качестве метода доступа к среде во всех стандартах используется метод *CSMA/CA* (с предотвращением коллизий), позволяющий избегать столкновений. Это приводит к дополнительным сложностям при взаимодействии и, как следствие, к существенно меньшим скоростям передачи данных, чем, например, в технологии *Ethernet*.

Основным недостатком сетей *Wi-Fi* на сегодня является малая дальность передачи данных, не превышающая для большинства устройств 150 м (максимум 300 м) на открытом пространстве или всего нескольких десятков метров - в помещении.

4). Решением указанной проблемы может стать архитектура ***WiMAX*** (*Worldwide Interoperability for Microwave Access*, *IEEE 802.16*). Реализация этой технологии, также использующей радиосигналы в качестве среды передачи, позволит предоставить пользователям скоростной беспроводной доступ на расстояниях до нескольких десятков километров (рис. 4.26).

Таблица 4.5Наиболее важные стандарты *IEEE 802.11 х*

|  |  |  |  |
| --- | --- | --- | --- |
| Стандарт | Среда передачи | Скорости, Мбит/с | Примечание |
| *802.11* | Радиосигнал с частотой 2,4ГГц или ИК-сигнал | 1-2 | Базовый стандарт, определяющий взаимодействие на физическом и канальном уровнях модели *OSI* |
| *802.11а* | Радиосигнал с частотой ~ 5ГГц | до 54 (48, 36, 4,18, 12,9,6) | Несовместим на физическом уровне со стандартами *802.11b* и *g;* в России не используется |
| *802.11b* | Радиосигнал,  2,4-2,483 ГГц | до 11  (5,5, 2, 1) | Относительно низкая скорость и защищенность. Большая дальность передачи данных |
| *802.11g* | Радиосигнал,  2,4-2,483 ГГц | до 54 | Обеспечивает обратную совместимость со стандартом *802.11b*, но характеризуется большей скоростью и защищенностью |
| *802.11n* | Радиосигнал,  2,4-2,483 ГГц | до 150-300 | Большая скорость; обратно совместим с *802.11b* и *802.11g*. Основное отличие – добавление к физическому уровню поддержки протокола *MIMO* (*multiple-input multiple-output*). |

5). Наконец, стоит упомянуть еще об одной из популярных сегодня беспроводных архитектур - о технологии ***Bluetooth*** (стандарт *IEEE 802.15.1*). В ней, как и в *Wi-Fi* используется радиосигнал с частотой 2,4 ГГц, однако эти стандарты между собой несовместимы. *Bluetooth* характеризуется довольно низким энергопотреблением, что позволяет с успехом применять эту технологию в переносных устройствах - ноутбуках, КПК и мобильных телефонах (рис. 4.27). К тому же *Bluetooth* практически не требует настройки - этот стандарт позволяет устройствам устанавливать взаимодействие при минимальном участии пользователя. С другой стороны, у *Bluetooth* весьма низкие показатели по дальности передачи и пропускной способности - не более 10 м и 400-700 Кбит/с, что резко ограничивает возможности использования этой технологии в локальных сетях.

6). Новая технология ***Wireless USB*** является альтернативой *Bluetooth* и обеспечивает сверхвысокоскоростную до 480 Мбит/с, а в перспективе **-** до 1 Гбит/с передачу данных на короткие расстояния (до 10 м). Она позволяет реализовать беспроводное подключение устройств, аналогичное USB 2.0.

**Контрольные вопросы**

1. Дайте определение компьютерной сети.
2. Определите основные различия между локальными, региональными и глобальными сетями?
3. Дайте определение и определите основные особенности корпоративной сети?
4. Дайте определение и определите основные особенности виртуальной сети?
5. Определите основные классификационные признаки сетей.
6. Определите основное предназначение модели OSI
7. Назовите уровни модели OSI и их назначение.
8. Определите разницу между физической и логической топологией.
9. Назовите базовые топологии локальных сетей, их достоинства и недостатки.
10. Что такое метод доступа к среде передачи данных?
11. Назовите основные методы доступа к среде в локальных сетях, их достоинства, недостатки и технологии, где они реализованы.
12. Что такое среда передачи данных, приведите их классификацию и примеры.
13. Какие коннекторы применяются в известных Вам средах передачи, назовите их названия и обозначения.
14. Какие категории кабеля витая пара Вам известны. Какая категория используется в технологии Ethernet, Fast Ethernet? Gigabit Ethernet, 100VG-Any Lan, 100BASE-T4?
15. Что какое одно- и многомодовый кабель? Назовите их характеристики, достоинства и недостатки.
16. Назовите основные технологии локальных сетей, их достоинства и недостатки.
17. Какие основные характеристики у локальной сети 10BASE-T, 100BASE-TX, 100BASE-T4?
18. Какие основные характеристики у локальной сети
19. Какие технологии беспроводных сетей Вы знаете, их основные характеристики, достоинства и недостатки.

**Сетевое оборудование и протоколы**

* + 1. **Устройства связи (сетевые адаптеры, концентраторы, мосты, коммутаторы, маршрутизаторы, шлюзы)**

Для обеспечения связи между компьютерами, серверами, ноутбуками и КПК нужно выбрать устройства, которые объединят их в единую сеть.

Чтобы взаимодействовать с сетью, компьютеру требуется специальное устройство - *сетевой адаптер* (проводной или беспроводной). Большинство современных компьютеров имеют встроенные сетевые адаптеры *Ethernet* и *Wi-Fi*, интегрированные в материнскую плату. Если адаптера нет, или нужен другой, его легко приобрести и установить в слот расширения компьютера или в порт USB.

Кроме этого, необходимо установить *драйвер сетевого адаптера* - специальное программное обеспечение, позволяющее операционной системе (ОС) работать с этим устройством. Как правило, современная ОС сама его распознает и устанавливает для него требуемый драйвер. Если же этого не произошло, то надо установить драйвер вручную с носителя, входящей в комплект поставки адаптера.

Сетевой адаптер и драйвер работают на *физическом уровне* и *подуровне управления доступом к среде (MAC)* модели *OSI*, обеспечивая взаимодействие физического и сетевого уровней.

Адаптер должен иметь нужный разъем для подключения коннектора (обычно *RJ-45*), а также уникальный физический (или «*MAC*») адрес, используемый *для однозначной идентификации компьютера в данном сегменте сети.* Этот адрес назначается производителем адаптера при изготовлении, некоторые модели адаптеров допускают смену *МАС*-адреса через настройки *BIOS*адаптера или с помощью специальной программы.

Если на компьютере с операционной системой *Windows 2000* или *ХР* установлен протокол ***TCP/IP***, то *МАС*-адреса установленных в этом компьютере адаптеров можно легко определить с помощью целого ряда утилит: *IPCONFIG, NBTSTAT, ROUTE PRINT, NETSTAT, NET CONFIG.*

Например, в командной строке подать команду *IPCONFIG /ALL* и в выданном на экран тексте посмотреть на параметр «Физический адрес».

В операционной системе *Windows XP* это сделать еще проще - достаточно дважды щелкнуть мышью на значке подключения в окне **Сетевые подключения,** в открывшемся окне состояния адаптера выбрать вкладку **Поддержка** и на ней нажать кнопку **Подробности.**

Существует ряд специальных устройств, используемых для связи компьютеров в сетях.

Чтобы объединить сетью *только* *два* компьютера, устройства связи не нужны - достаточно наличия в них совместимых сетевых адаптеров.

При использовании *Ethernet* потребуется *перекрестный кабель*, который достаточно вставить в разъемы *RJ-45* сетевых адаптеров.

При использовании *Wi-Fi* следует переключить беспроводные адаптеры в специальный режим *Ad-Hoc,* обеспечивающий прямое взаимодействие компьютеров друг с другом. Таким способом можно соединить и несколько ПК с беспроводными адаптерами, однако скорость передачи данных будет уменьшаться с увеличением числа компьютеров в сети.

Простейшим устройством, обеспечивающим связь компьютеров друг с другом, является *концентратор* («хаб», *hub*)*.* В сетях, использующих коаксиальный кабель, концентраторы называют *повторителями* или *репитерами (repeater).*

Обычно концентратор имеет от 4 до 32 гнезд *(портов)* для подсоединения коннекторов различных типов. В большинстве случаев это гнезда для коннекторов *RJ-45*, однако существуют и *гибридные концентраторы* с портами *RJ-45* и *BNC*, позволяющие объединять сегменты *Ethernet* стандартов *10Base-T* и *10Base-2*. К портам можно подключать не только компьютеры, но и другие концентраторы, формируя *цепочки (каскады) концентраторов* или более сложные топологии типа «дерево».

В стандартах *10Base-5* и *10Base-2* на такое *каскадирование* концентраторов действовали жесткие ограничения, описываемые «правилом 5-4-3»: в сети не могло быть больше 5 сегментов, соединенных 4 репитерами, и только в 3 сегментах допускалось подключение компьютеров. В сетях стандарта *10Base-T* допускалось максимум 4 повторителя и 5 сегментов. В стандарте *100Base-T* все еще сложнее - *концентраторы класса I*, поддерживающие одновременную работу с устройствами *100Base-T4*, *100Base-TX* и *100Base-FX*, каскадировать было нельзя, а *концентраторы класса II* можно было объединять только в пару. Таким образом, первая проблема сетей на основе концентраторов состоит в том, что построить крупную сеть с помощью только концентраторов просто невозможно.

Концентраторы работают на физическом уровне модели OSI и являются простыми *активными устройствами* (требующими подключения к электрической сети). Их основная задача - принять, усилить и ретранслировать электрический сигнал,полученный от одного компьютера, во все остальные активные порты (рис. 5.1). Никакой другой обработке сигнал в концентраторе не подвергается, его буферизация не производится, а коллизии не обрабатываются. При этом пакет, отправленный одним компьютером другому компьютеру, будет передан **всем** рабочим станциям, серверу, принтеру и всем другим сетевым устройствам.

Отсюда вытекает вторая проблема сетей, применяющих только концентраторы, - очень большое количество столкновений, возрастающее с увеличением числа сегментов и компьютеров в сети. Существует термин, описывающий такое поведение сети: концентраторы *формируют «область столкновений»* (*Collision Domain*). Поэтому сегодня концентраторы в сетях практически редко используются - их вытеснили сначала *мосты,* а затем *коммутаторы.*

*Мосты (bridge),* а затем и *коммутаторы (switch)* были созданыдля объединения сетей и устранения проблемы возникновения большого числа коллизий. Существенным отличием этих устройств от концентраторов является то, что они умеют определять *МАС*-адреса источника и приемника сигналов, а также поддерживать *таблицу соответствия своих портов и используемых в сети МАС-адресов.*

Такую таблицу мост (или коммутатор) формирует сразу после включения по следующему принципу - как только порт получает пакет от устройства с определенным физическим адресом, в таблице появляется строчка соответствия: «*МАС*-адрес <-> порт». Таким образом, эти устройства работают не только на физическом уровне модели OSI, но и на канальном*,* - точнее, *на подуровне управления доступом к среде (MAC).*

Получив кадр и определив адрес назначения, мост (коммутатор) транслируют кадр только в тот порт, с которым этот *МАС*-адрес сопоставлен в таблице соответствий. Кадры, передаваемые между ПК одного сегмента, коммутатор получает, но никуда не транслирует (рис. 5.2). При этом обмен данными между одними компьютерами никак не влияет на взаимодействие других компьютеров с сервером и друг с другом.

Единственными сигналами, передаваемыми во все порты, являются кадры, предназначенные для адресов, не имеющих записей в таблице соответствий, и специальные *широковещательные сообщения,* предназначенные всем компьютерам локальной сети. Чтобы обозначить эту особенность работы мостов и коммутаторов, говорят, что они формируют *«область широковещания» (Broadcast Domain).*

Различие между мостами и коммутаторами заключается в том, что мост в каждый момент времени может передавать только один кадр, обслуживая передачу от одного компьютера к другому. Коммутатор умеет выстраивать большое число виртуальных каналов связи между портами, производя параллельную обработку кадров, поступающих с разных портов. Поэтому производительность сетей, построенных на базе коммутаторов, существенно выше. Подавляющее большинство современных сетей строится именно на коммутаторах.

*Маршрутизаторы* работают на еще более высоком уровне модели *OSI* - *сетевом.* В их задачу входит анализ адресов, используемых в протоколе такого уровня (*IP*-адресов), и определение наилучшего маршрута доставки пакета данныхпо назначению. Конечно, маршрутизаторы работают и на более низких уровнях модели *OSI* - они восстанавливают уровень и форму предаваемого сигнала (как концентраторы) и позволяют избежать столкновений (как мосты и коммутаторы). Однако, в отличие от этих устройств, маршрутизаторы изменяют передаваемые кадры *Ethernet* – они «разбирают» их до сетевого уровня, а затем формируют заново по определенным правилам. Без определенной настройки маршрутизаторы не передают в другие порты даже широковещательные пакеты, и, таким образом, служат в сетях границами областей столкновений и широковещании.

Кроме того, совместно с программами более высокого уровня модели *OSI*, маршрутизаторы умеют выполнять целый ряд сложных действий - обнаруживать проблемы в сети и сообщать о них, вести статистику полученных и переданных данных, фильтровать пакеты, проводить авторизацию пользователей при выходе в Интернет и т.д.

Маршрутизаторы являются сложными и дорогими программно-аппаратными комплексами, поэтому в современных сетях они чаще заменяются *коммутаторами 3-го уровня* - устройствами, занимающими промежуточную ступень между коммутаторами и маршрутизаторами. От обычных коммутаторов они отличаются тем, что могут выполнять простейшие функции маршрутизации, оставаясь при этом производительными и не очень дорогими.

Следует упомянуть о такой функции современных коммутаторов, как возможность строить *виртуальные локальные сети (Virtual LAN),* когда в один *логический* сегмент сети объединяются компьютеры, *физически* подключенные к разным коммутаторам. Критерии для такого объединения могут быть различными, начиная с *MAC*- или *IP*-адресов и заканчивая именами компьютеров.

*Шлюз* (*Gateway*) это устройство или программа, позволяющие объединять разные сетевые архитектуры(пример: шлюз из *Ethernet* в *Token* *Ring*). Он должен иметь физические порты для подключения разнородных сетей и «понимать» их протоколы, выступая для них в роли «переводчика».

Типичным примером *шлюзов* являются широко используемые в современных сетях интегрированные устройства, в которых объединены *ADSL-модем* для подключения к Интернету, *беспроводная точка доступа*, работающая по стандарту *IEEE 802.11b/g*/*n*, и *коммутатор* *Fast Ethernet*.

На рис. 5.3 представлена графическая иллюстрация уровней функционирования различных сетевых устройств.

Сформулируем несколько рекомендаций, которыми можно руководствоваться при выборе необходимых устройств связи.

Наиболее распространенными устройствами связи в сетях сегодня являются *коммутаторы* *Fast* и *Gigabit* *Ethernet*, а подключение беспроводных устройств к локальной сети осуществляется с помощью *шлюзов,* объединяющих функции *коммутатора* и *точки беспроводного доступа,* работающей по стандарту *802.11g*/*n*.

Для небольших сетей подойдут 8- и 16-портовые *коммутаторы* *Fast* *Ethernet* с функцией управления портами. Если передача больших объемов данных не планируется, можно остановиться на беспроводных точках доступа, хотя это решение обойдется дороже и будет менее скоростным.

В крупных сетях основу должны составлять мощные и надежные *коммутаторы* *Gigabit* или *10Gigabit* *Ethernet*, к которым подключаются *коммутаторы подразделений* (зданий), а к ним, в свою очередь, - *коммутаторы этажей* (офисов). Размещение точек доступа в таких сетях следует тщательно планировать, чтобы пользователь при перемещении по территории предприятия мог последовательно переключался с одной точки доступа на другую, сохраняя связь с локальной сетью.

Применение *маршрутизаторов* требуется только там, где нужно четко контролировать потоки *IP*-пакетов в сложной маршрутизируемой сети, а также обеспечивать резервные маршруты доставки пакетов, - например, при взаимодействии с удаленным офисом или Интернетом.

При выборе *сетевого адаптера* для компьютера следует обратить внимание на возможность поддержки стандартов *Ethernet* или *Wi-Fi*. Лучше всего выбрать современный сетевой адаптер, например *Gigabit* *Ethernet* или *Wi-Fi* стандарта *802.11g*/*n*. Поскольку эти стандарты *обратно совместимы* с предыдущими, такие адаптеры вполне смогут работать со старыми концентраторами *10Base-T* и точками доступа 802.11b, пока не будут заменены указанные устройства связи.

**Стеки протоколов (TCP/IP, NetBEUI, IPX/SPX, NWLink)**

Чтобы компьютеры могли взаимодействовать в сети необходимо, чтобы сетевые приложения могли обмениваться данными с помощью протоколов на уровнях, более высоких, чем канальный. Так, как этих уровней несколько, то потребуется не один, а несколько протоколов, объединенных в набор, или ***стек****.*

В сетях применяется целый ряд *стеков протоколов,* в том числе самый распространенный на сегодня набор протоколов - ***стек TCP/IP****.* Рассмотрим ретроспективу развития наиболее распространенных стеков протоколов.

1). ***NetBEUI*** (*NetBIOS Extended User Interface* - улучшенная версия протокола *NetBIOS*) - небольшой по объему протокол, реализующий поддержку *сетевого, транспортного и сеансового уровней* модели *OSI*. Он не требует настройки, работает быстро и эффективно в сетях масштабом до 200 компьютеров. Серьезными недостатками протокола *NetBEUI* являются ограничения при работе в сетях с большим количеством компьютеров и отсутствие поддержки маршрутизации. Поэтому его нельзя использовать в составных сетях с маршрутизаторами и при работе с Интернетом. Этот протокол поставлялся в составе всех операционных систем *Windows* вплоть до *Windows 2000*, однако в последних версиях его поддержка прекращена.

2). Стек протоколов ***IPX/SPX*** был разработан фирмой *Novell* в начале 80-х гг. для своей сетевой ОС *NetWare*. Основа стека - протоколы *IPX* (*Internetwork Packet eXchange*) и *SPX* (*Sequenced Packet eXchange*), реализующие функции сетевого и транспортного уровней модели *OSI*, соответственно.

Протокол *IPX/SPX* является небольшим (его код размещается на обычной дискете 1,44 Мб вместе с *DOS*) и быстрым. Кроме того, в стеке *IPX/SPX* поддерживается маршрутизация. Он был широко распространен в локальных сетях в 80-е и 90-е гг. К недостаткам этого стека протоколов следует отнести активное использование широковещательных сообщений, серьезно нагружающих сеть, что особенно плохо при работе по медленным глобальным каналам. Это, а также то, что стек *IPX/SPX* принадлежит фирме *Novell* и для его реализации другим производителям сетевых ОС необходимо покупать лицензию, привели к вытеснению *IPX/SPX* открытым стеком ***TCP/IP***. Важную роль здесь сыграло и то, что в Интернете использовался именно стек *TCP/IP*, а поддерживать в сети два стека - излишество.

***NWLink*** – это фирменная реализация стека *IPX/SPX* компанией *Microsoft*, поставляемая во всех версиях *Windows*.

3). История развития стека ***TCP/IP*** началась в конце 60-х гг. XX века с проекта *ARPANet* (*Advanced Research Project Agency Network*) - сети Агентства перспективных исследовательских проектов Министерства обороны США. Получившаяся в результате сеть и разработанный в 70-х гг. стек протоколов *TCP/IP* оказались удачными, продолжали жить и успешно развиваться, создав основы современного Интернета.

Основные преимущества стека *TCP/IP* перед другими – это более удобная система сетевой адресации, возможность фрагментации пакетови очень небольшое количество широковещательных сообщений. Эти преимущества оказались решающими не только при построении глобальных сетей, объединяющих сети с разнородными архитектурами, но и при создании крупных корпоративных сетей. В результате стек *TCP/IP* практически вытеснил все остальные - он используется и в небольших домашних сетях, и в глобальной сети Интернет.

Поскольку стек *TCP/IP* является *общедоступным,* его стандарты публикуются в Интернете в виде специальных документов под названием *RFC* (*Request* *for* *Comments*, запрос комментариев). Спецификация протокола *IP*, например, опубликована в *RFC* *791*, а протокола *HTTP* - в *RFC* *2616*. Стек *TCP/IP*, в отличие от семиуровневой модели *OSI*, принято описывать в рамках четырех уровней (рис. 5.4).

*На физическом уровн****е*** *TCP/IP* поддерживает работу с основными технологиями локальных сетей - *Ethernet, Token Ring, Wi-Fi, Bluetooth* и т.д.

*На сетевом уровне* располагаются несколько протоколов:

*-* протокол *ARP (Address Resolution Protocol)* является звеном, связывающим сетевой уровень с физическим. Он отвечает за преобразование сетевых IP-адресов в аппаратные *МАС*-адреса;

*-* протокол *ICMP (Internet Control Message Protocol)* - используется для передачи сообщений об ошибках, диагностики доступности сетевого узла и маршрута доставки пакетов (его используют такие утилиты, как *PING* и *TRACERT*);

*-* протокол *IGMP (Internet Group Management Protocol)* - используется для управления группами компьютеров, когда для снижения нагрузки на сеть пакет посылается по специальному адресу сразу нескольким компьютерам *(многоадресная рассылка);*

- протокол *IP (Internet Protocol)* - один из самых важных в стеке *TCP/IP*, он отвечает за доставку *IP-дейтаграмм* (так называются пакеты протокола *IP*), обеспечивая передачу пакета из одной сети в другую.

*На транспортном уровне* работают два протокола:

- протокол *TCP (Transmission Control Protocol,* протокол управления передачей*)* обеспечивает установку соединениямежду отправителем и получателем, разбиение крупного блока информации на небольшие *TCP*-пакеты и их гарантированную доставку получателю в нужном порядке и без ошибок. Поэтому он используется в тех приложениях, где важно обеспечить целостность при передаче данных;

- протокол *UDP (User Datagram Protocol),* в отличие от *TCP*, не устанавливает соединения перед передачей информации и не обеспечивает надежной доставки данных, работая при этом быстрее, чем *TCP*. Его используют там, где обеспечение доставки информации не особенно важно по сравнению со скоростью передачи.

Протокол *TCP* работает следующим образом:

- устанавливает соединение между ПК по определенным портам;

- на компьютере-отправителе разбивает информацию на пакеты, нумерует их и с помощью протокола *IP* передает получателю;

- на компьютере-получателе проверяет, все ли пакеты получены, а если пакет пропущен или поврежден, запрашивает у отправителя повторную пересылку;

- после получения всех пакетов закрывает соединение, собирает пакеты в нужном порядке и передает полученные данные приложению более высокого уровня.

При использовании протокола *UDP* никакого установления связи и подтверждения получения корреспонденции нет – пакеты просто отправляют в сеть.

*Порт* в *TCP* или *UDP* - это логический канал с определенным номером (от 0 до 65536), обеспечивающий текущее взаимодействие между отправителем и получателем. Порты позволяют компьютеру с одним *IP*-адресом параллельно обмениваться данными с множеством других компьютеров. Некоторые номера портов (порты с номерами от 0 до 1024) привязаны к определенным службам и приложениям, что позволяет клиентам легко обращаться к нужным им сетевым сервисам.

Наконец, самым богатым по набору протоколов является *прикладной уровень* стека *TCP/IP*. Ниже в табл. 5.1 приведены самые популярные протоколы, а также зарезервированные для них порты. Заметим, что в таблице приведены порты для наиболее часто применяемых протоколов транспортного уровня (*TCP* и *UDP*).

Таблица 5.1Протоколы прикладного уровня стека *TCP/IP*

|  |  |  |
| --- | --- | --- |
| Протокол | Назначение | № порта |
| *NTP (Network Time Protocol)* | Протокол сетевого времени, используется для синхронизации системных часов ПК в сетях | 123 (*UDP*) |
| *DNS (Domain Name System, или Service)* | Служба доменных имен, используется для преобразования понятных людям имен компьютеров в *IP*-адреса | 53 (*TCP*  и *UDP*) |
| *NetBIOS и WINS (Windows Internet Naming Service)* | Служба имен *NetBIOS* и служба межсетевых имен Windows, используются для преобразования *NetBIOS*-имен компьютеров (типа *SERVER*) в *IP*-адреса | 137 и 138 (*UDP*) |
| *NetBIOS session service* | Служба сеансов *NetBIOS*, используется для установления сеансов между компьютерами | 139 (*TCP*) |
| *LDAP (Lightweight Directory Access Protocol)* | Простой протокол доступа к каталогу, используется для работы с различными сетевыми каталогами (например, со службой *Active* *Directory* в доменах на основе *Windows* *Server* *2003*) | 389 (*TCP*) |
| *RPC (Remote Procedure Call)* | Вызов удаленной процедуры, используется для работы со многими сетевыми службами в сетях | 135 (*TCP*) |
| *Telnet* | Протокол для обеспечения терминального доступа к удаленным компьютерам | 23 (*TCP*) |
| *FTP (File Transfer Protocol)* | Протокол передачи файлов; используется для эффективной и надежной передачи файлов между клиентом и сервером *FTP* | 20 и 21 (*TCP*) |
| *TFTP*  *(Trivial File Transfer Protocol)* | Упрощенный вариант *FTP* (не имеет функций проверки пользователя при входе, просмотра каталогов и файлов сервера; используется только для записи/чтения файлов) | 69 (*UDP*) |
| *HTTP(HyperText Transfer Protocol)* | Протокол передачи гипертекста, самый популярный сегодня протокол, используемый в *WWW* | 80 (*TCP*) |
| *NNTP (Network News Transfer Protocol)* | Протокол передачи сетевых новостей, используется для обмена сообщениями в системах телеконференций | 119 (*TCP*) |
| *SMTP(Simple Mail Transfer Protocol)* | Простой протокол передачи, используется почтовыми серверами для обмена электронными сообщениями | 25 (*TCP*) |
| *POP3*  *(Post Office Protocol)* | «Протокол почтового отделения», простой протокол, используемый почтовым клиентом для подключения к своему почтовому ящику на сервере и считывания сообщений | 110 (*TCP*) |
| *IMAP4 (Internet Message Access Protocol)* | Протокол доступа к электронным сообщениям - клиентский протокол для доступа к почтовому серверу | 143 (*TCP*) |
| *SSL (Secure Sockets Layer)* | Протокол, обеспечивающий согласование алгоритмов и обмен ключами шифрования. Используется для защиты данных при их пересылке по сетям | 25 (*SMTP*) 443(*TCP*) |

* + 1. **Межсетевое взаимодействие**

Только небольшое количество сетей обладает однородностью (гомогенностью) программного и аппаратного обеспечения. Более частым и общим случаем являются **неоднородные** (**гетерогенные**) сети, состоящие из разнотипных рабочих станций, операционных систем и приложений, в которых для взаимодействия между компьютерами используется различное коммуникационное оборудование - коммутаторы и маршрутизаторы, а также разные коммуникационные протоколы.

При межсетевом взаимодействии под «сетью» понимается *совокупность компьютеров*, *общающихся друг с другом с помощью единого стека протоколов*. В однородной сети все компьютеры используют один и тот же стек. Проблема возникает, когда требуется организовать взаимодействие компьютеров, принадлежащих разным сетям, то есть организовать взаимодействие компьютеров, на которых поддерживаются отличающиеся стеки коммуникационных протоколов.

Например, если в одной сети на канальном уровне работает технология *Ethernet*, а в другой применяется протокол *PPP*, то непосредственно эти протоколы общаться и передавать между сетями кадры не могут. Именно для решения такого рода проблем и были в свое время созданы протоколы сетевого уровня (*IP, IPX*). Основная их функция состоит в организации взаимодействия канальных протоколов различных сетей. Однако использования протокола сетевого уровня недостаточно, когда в разных сетях на сетевом уровне работают разные протоколы (например, в одной сети - *IP*, а в другой – *IPX*).

Задачи устранения неоднородности имеют специфику и разные названия в зависимости от того, к какому уровню модели *OSI* они относятся. Задача объединения транспортных подсистем, отвечающих только за передачу сообщений, обычно называется задачей **межсетевого взаимодействия** (*internetworking*). Стандартным подходом для ее решения является использование единого сетевого протокола (либо *IP*, либо *IPX*).

Другая задача, называемая **операционной совместимостью** (*interoperability*), возникает при объединении сетей, использующих разные протоколы более высоких уровней - в основном прикладного и представительного. Она называется *согласованием сетевых служб операционных систем*, так как протоколы прикладного и представительного уровней реализуются этими сетевыми компонентами.

Решением проблемы межсетевого взаимодействия может стать повсеместное *использование единого стека протоколов*. В связи со стремительным ростом популярности Интернета практическим стандартом стал стек протоколов *TCP*/*IP*, который сегодня установлен практически на любом компьютере. В результате степень неоднородности сетей существенно снизилась. Помимо появления единого протокола сетевого уровня, этому способствовали еще две тенденции: доминирование на канальном уровне технологии *Ethernet* и сокращение перечня популярных сетевых ОС до двух семейств - *Windows* и *Unix* (*Linux*).

Для решения проблем *межсетевого взаимодействия* были разработаны несколько общих подходов, к которым относятся:

- трансляция;

- мультиплексирование;

- инкапсуляция (туннелирование).

*Трансляция*обеспечивает согласование стеков протоколов путем преобразования сообщений, поступающих от одной сети, в формат сообщений другой сети. Транслирующий элемент, в качестве которого могут выступать программный или аппаратный шлюз, мост, коммутатор или маршрутизатор, размещается между взаимодействующими сетями и служит посредником («переводчиком») в их «диалоге».

В зависимости от типа транслируемых протоколов процедура трансляции может иметь разную степень сложности. Так, преобразование протокола *Ethernet* в протокол *Token* *Ring* благодаря тому, что оба протокола ориентированы на единую схему адресации узлов, сводится к нескольким действиям. А, например, трансляция протоколов сетевого уровня *IP* в (из) *IPX* представляет собой гораздо более сложный процесс, включающий не только преобразование форматов сообщений, но и отображение (перевод) адресов сетей и узлов, по-разному применяемых в этих протоколах. Трансляция же протоколов еще более высокого, прикладного уровня включает отображение инструкций одного протокола на инструкции другого, что представляет собой сложную, логически неоднозначную интеллектуальную процедуру. На рис.5.5 показано размещение на компьютере *2* шлюз, который согласовывает протоколы компьютера *1* в сети ***А***с протоколами компьютера *3* в сети ***В****.*

Достоинство шлюзов состоит в том, что они сохраняют в неизменном виде программное обеспечение на клиентских компьютерах. Пользователи работают в привычной среде и могут даже не заметить, что получают доступ к ресурсам другой сети. Однако шлюз снижает надежность сети. Кроме того, при обработке запросов в нем возможны большие временные задержки, из-за затрат времени на собственно процедуру трансляции и задержек запросов в очереди к разделяемому всеми клиентами шлюзу, особенно если запросы поступают с большой интенсивностью. Это делает его плохо масштабируемым решением, однако в сети могут параллельно работать несколько шлюзов.

Другой подход к согласованию протоколов получил название *мультиплексирования стеков протоколов*. Он заключается в том, что в сетевое оборудование или в операционные системы серверов и рабочих станций встраиваются несколько стеков протоколов. Это позволяет клиентам и серверам выбирать для взаимодействия тот протокол, который является для них общим.

На рис. 5.6 показан пример взаимодействия клиентского компьютера сети ***В***с сервером в своей сети и сервером сети ***А***, работающей со стеком протоколов, полностью отличающимся от стека сети ***В***. В клиентском компьютере реализованы оба стека. Для того чтобы запрос от прикладного процесса был правильно обработан и направлен через соответствующий стек, необходимо наличие специального программного элемента – *мультиплексора (менеджера) протоколов.* Менеджер должен уметь определять, к какой сети направляется запрос клиента. Для этого может использоваться служба имен сети, в которой отмечается принадлежность ресурса определенной сети с соответствующим стеком протоколов.

При использовании мультиплексоров протоколов существует два варианта размещения дополнительного стека протоколов - на одном или на другом взаимодействующем компьютере. Если дополнительный стек устанавливается на сервере, то этот сервер становится доступным для всех клиентов с этим стеком. При этом нужно оценивать влияние этой установки на производительность сервера.

Аналогично, дополнительный стек на клиенте дает ему возможность устанавливать связи с другими серверами, использующими этот стек протоколов.

Важным преимуществом мультиплексирования является меньшее время выполнения запроса, чем при использовании шлюза. Это связано, во-первых, с отсутствием временных затрат на процедуру трансляции, а во-вторых, с тем, что при мультиплексировании на каждый запрос требуется только одна сетевая передача, в то время как при трансляции - две: запрос сначала передается в шлюз, а затем из шлюза на ресурсный сервер.

*Инкапсуляция*(*encapsulation*), или *туннелирование*(*tunneling*), - еще один метод решения задачи согласования сетей, который применим только для согласования транспортных протоколов и при некоторых ограничениях. Она может быть применена, когда две сети, построенные на одной транспортной технологии, необходимо соединить через транзитную сеть, построенную на базе другой технологии. В процессе инкапсуляции принимают участие три типа протоколов:

- протокол-«пассажир»;

- несущий протокол;

- протокол инкапсуляции.

Транспортный протокол объединяемых сетей является *протоколом-пассажиром,* а протокол транзитной сети - *несущим протоколом.* Пакеты протокола-пассажира помещаются в поле данных пакетов несущего протокола и извлекаются оттуда с помощью *протокола инкапсуляции.*

Пакеты протокола-пассажира не обрабатываются при транспортировке их по транзитной сети. Инкапсуляцию выполняет пограничное устройство (маршрутизатор или шлюз), которое располагается на границе между исходной и транзитной сетями. Извлечение пакетов-пассажиров из несущих пакетов выполняет второе пограничное устройство, которое находится на границе между транзитной сетью и сетью назначения. Пограничные устройства указывают в несущих пакетах свои адреса, а не адреса узлов назначения.

В связи с большой популярностью несущим протоколом транзитной сети обычно выступает протокол *IP*, а в качестве протоколов-пассажиров - протоколы локальных сетей. На рис. 5.7 представлен пример двух сетей, использующих протокол *IPX*, которые нужно соединить через транзитную сеть *TCP/IP*. Необходимо обеспечить только взаимодействие узлов двух сетей *IPX*, а взаимодействие между *IPX*-узлами и узлами сети *TCP/IP* не предусматривается, поэтому для соединения сетей *IPX* можно применить метод инкапсуляции.

Обычно инкапсуляция ведет к более простым и быстрым решениям по сравнению с трансляцией, так как решает более частную задачу, не обеспечивая взаимодействия с узлами транзитной сети. Помимо согласования транспортных технологий, инкапсуляция обеспечивает также секретность передаваемых данных. При этом исходные пакеты-пассажиры шифруются и передаются по транзитной сети с помощью пакетов ее несущего протокола.

**Адресация и маршрутизация**

Для корректной работы сети со стеком протоколов *TCP/IP* необходимо настроить *IP-адресацию* и *маршрутизацию,* т.е. задать *IP-адрес* и *маску подсети* для определения *локальных* или *удаленных IP-сетей.*

Первым обязательным параметром в свойствах протокола *TCP/IP* любого компьютера является его *IP-адрес*- это уникальная 32-разрядная последовательность двоичных цифр, с помощью которой ПК однозначно идентифицируетсяв *IP*-сети. Такой формат адреса используется в наиболее распространенной версии 4 протокола *IP* (*IPv4*)*.* Однако уже давно создана расширенная версия протокола - *IP версии 6* (*IPv6*)*,* в которой *IP*-адрес представляется в виде 128-битной последовательности двоичных цифр. Такая версия протокола IP пока еще не получила широкого распространения, хотя и поддерживается многими современными маршрутизаторами и операционными системами (*Windows XP* или *Windows Server 2003*).

Если 32-битовый стандарт обеспечивает количество *IP*-адресов, равное почти 4,3 млрд., то новая, 128-разрядная версия протокола *IP v.6* позволит увеличить количество *IP*-адресов до огромной величины - 3,4 х 1038. Для использования протокола *IPv6* в *Windows XP* имеется необходимое программное обеспечение, которое по умолчанию не активизировано. Чтобы задействовать новый протокол, надо в командной строке (меню **Пуск, Выполнить)** ввести команду *ipv6 install*. Получить справки по работе с протоколом *IPv6* можно командой *ipv6 /?.*

Для удобства работы с IP-адресами 32-разрядную последовательность обычно разделяют на 4 части по 8 битов (на *октеты),* каждый октет переводят в десятичное число и при записи разделяют эти числа точками. В таком виде *IP*-адреса занимают гораздо меньше места и намного легче запоминаются (табл. 5.2).

Таблица 5.2Различные представления *IP*-адреса

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| *IP*-адрес  в 32-разрядном виде | 11000000 10101000 00000101 11001000 | | | |
| *IP*-адрес,  разбитый на октеты | 11000000 | 10101000 | 00000101 | 11001000 |
| Октеты в десятичном представлении | 192 | 168 | 5 | 200 |
| *IP*-адрес в виде десятичных чисел,  разделенных точками | 192.168.5.200 | | | |

Однако только *IP*-адреса компьютеру для работы в сети *TCP/IP* недостаточно. Вторым обязательным параметром является *маска подсети* - 32-разрядное число, состоящее из идущих вначале единиц, а затем - нулей, например 255.255.255.0 (в десятичном представлении).

Маска подсети предназначена для определения, какие *IP*-адреса принадлежат *локальной* сети, а какие - *удаленным* сетям. С ее помощью производится разделение любого *IP-адpeca* на две части: *идентификатор сети (Net ID)* и *идентификатор узла (Host ID).* Такое разделение делается очень просто: там, где в маске подсети стоят единицы, находится идентификатор сети, а где нули - идентификатор узла.

Например, в представленном выше *IP*-адресе 192.168.5.200 при использовании маски 255.255.255.0 идентификатором сети будет 192.168.5.0, а узла - 200. Для маски 255.255.0.0 узел - 192.168.0.0 и сеть - 5.200.

Существует ряд обязательных правил, которые следует применять при назначении указанных параметров:

1. идентификатор сети не может содержать только двоичные нули или только единицы;
2. идентификатор узла также не может содержать только двоичные нули или единицы - такие адреса зарезервированы для специальных целей:

- все нули в идентификаторе узла означают, что этот адрес является *адресом сети.* Например, 192.168.5.0 является правильным адресом сети при использовании маски 255.255.255.0 и его нельзя использовать для адресации ПК,

- все единицы в идентификаторе узла означают, что этот адрес является *адресом широковещания* для данной сети. Например, 192.168.5.255 является адресом широковещания в сети 192.168.5.0 при использовании маски 255.255.255.0 и его нельзя использовать для адресации компьютеров;

1. идентификатор узла в пределах подсети должен быть уникальным;

- диапазон адресов от 127.0.0.1 до 127.255.255.254 нельзя использовать в качестве *IP*-адресов компьютеров - сеть 127.0.0.0 по маске 255.0.0.0 зарезервирована под *«адрес заглушки» (loopback),* используемый в *IP* для обращения компьютера к самому себе. Это легко проверить - выполнить команду *PING* 127.12.34.56 и компьютер будет отвечать на собственные запросы.

Первоначальная система *IP*-адресации выглядела так. Все пространство возможных *IP*-адресов было разбито на пять классов*,* причем принадлежность *IP*-адреса к определенному классу определялась по нескольким битам первого октета (табл. 5.3). При этом для адресации сетей и узлов использовались только классы ***А*, *В*** и ***С***. Кроме того, для этих сетей были определены *фиксированные маски подсети* по умолчаниюравные, соответственно, 255.0.0.0, 255.255.0.0 и 255.255.255.0, которые жестко определяли диапазон возможных *IP*-адресов узлов в таких сетях и механизм маршрутизации.

Таблица 5.3Классы адресов в первоначальной схеме *IP*-адресации

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| *Класс* | *Первые биты в октете* | *Возможные значения первого октета* | *Возможное число сетей* | *Возможное число узлов в сети* |
| ***А*** | 0 | 1-126 | 126 | 16777214 |
| ***В*** | 10 | 128-191 | 16384 | 65534 |
| ***С*** | 110 | 192-223 | 2097152 | 254 |
| ***D*** | 1110 | 224-239 | Используется для многоадресной рассылки (*multicast*) | |
| ***Е*** | 1111 | 240-254 | Зарезервирован для экспериментов | |

Чтобы рассчитать максимально возможное количество узлов в любой *IP*-сети, достаточно знать, сколько битов содержится в идентификаторе узла, или сколько нулей имеется в маске подсети. Это число используется в качестве показателя степени 2, а затем из результата вычитается два зарезервированных адреса (сети и широковещания). Аналогично вычисляются количество сетей классов *А, В, С,* если учесть, что первые биты в октете уже зарезервированы, а в классе *А* нельзя использовать *IP*-адреса 0.0.0.0 и 127.0.0.0 для адресации сети.

Распределением *IP*-адресов занимается частная некоммерческая организация *IANA* (*Internet Assigned Numbers Authority*). Для получения нужного диапазона *IP*-адресов организациям необходимо было заполнить регистрационную форму, в которой указать текущее число компьютеров и планируемый рост компьютеров в течение двух лет.

Первоначально эта схема хорошо работала, поскольку количество сетей было небольшим. Однако с развитием Интернета такой подход стал вызывать проблемы, особенно острые для сетей класса *В*.

Действительно, организациям, в которых число компьютеров не превышало нескольких сотен (например, 500), приходилось регистрировать для себя целую сеть класса *В*. Поэтому количество доступных сетей класса *В* стало на глазах «таять», но при этом громадные диапазоны *IP*-адресов пропадали зря.

Для решения проблемы была разработана *бесклассовая схема IP-адресации (Classless InterDomain Routing, CIDR),* в которой допускается применение *масок**подсети с переменной длиной (Variable Length Subnet Mask, VLSM).* Например, если при выделении сети для организации с 500 компьютерами вместо фиксированной маски 255.255.0.0 использовалась маска 255.255.254.0 и получившегося диапазона из 512 возможных *IP*-адресов будет достаточно. Этот подход позволил гораздо более эффективно выделять диапазоны *IP*-адресов, и проблема с нехваткой *IP*-сетей и адресов стала менее острой.

Все используемые в Интернете адреса должны регистрироваться в *IANA*, что гарантирует их уникальность в масштабе всей земли. Такие адреса называют *реальными,* или *публичными (public) IP-адресами.* Для локальных сетей, не подключенных к Интернету, регистрация *IP*-адресов не требуется, так что здесь можно использовать любые возможные адреса. Однако, чтобы не допускать возможных конфликтов при последующем подключении такой сети к Интернету, рекомендуется применять в локальных сетях только следующие диапазоны так называемых *частных (private) IP-адресов* (в Интернете эти адреса не существуют): 10.0.0.0-10.255.255.255; 172.16.0.0-172.31.255.255; 192.168.0.0-192.168.255.255.

Чтобы правильно взаимодействовать с другими компьютерами и сетями, каждый ПК определяет, какие *IP*-адреса принадлежат его локальной сети, а какие - удаленным сетям. Если выясняется, что *IP*-адрес компьютера назначения принадлежит локальной сети, пакет посылается непосредственно компьютеру назначения, если же это адрес удаленной сети, то пакет посылается по адресу основного шлюза.

Рассмотрим этот процесс подробнее. Возьмем, например, компьютер со следующими параметрами протокола *IP*:

*IP*-адрес - 192.168.5.200;

маска подсети - 255.255.255.0;

основной шлюз - 192.168.5.1.

При запуске протокола *IP* на компьютере выполняется *операция логического «И» между его собственными IP-адресом и маской подсети,* в результате которой все биты *IP*-адреса, соответствующие нулевым битам маски подсети, также становятся нулевыми:

*IP*-адрес в 32-разрядном виде - 11000000 10101000 00000101 11001000;

маска подсети - 11111111 11111111 11111111 00000000;

идентификатор сети - 11000000 10101000 00000101 00000000.

Эта простая операция позволяет компьютеру определить *идентификатор**собственной**сети* (в нашем примере - 192.168.5.0).

Пусть компьютеру надо отправить *IP*-пакет по адресу 192.168.5.15. Чтобы решить, как это нужно сделать, компьютер выполняет *операцию логического «И» с IP-адресом компьютера назначения и собственной маской подсети.* Полученный в результате *идентификатор сети назначения* будет совпадать с идентификатором собственной сети компьютера-отправителя. Так компьютер определит, что компьютер назначения находится в одной с ним сети, и выполнит следующие операции:

- с помощью протокола *ARP* будет определен физический *МАС*-адрес, соответствующий *IP*-адресу компьютера назначения;

- с помощью протоколов канального и физического уровня по этому *МАС*-адресу будет послана нужная информация.

Теперь посмотрим, что изменится, если пакет надо отправить по адресу 192.168.10.20. Компьютер выполнит аналогичную процедуру определения идентификатора сети назначения. В результате будет получен адрес 192.168.10.0, не совпадающий с идентификатором сети компьютера-отправителя. Так будет установлено, что ПК назначения находится в удаленной сети, и алгоритм действий компьютера-отправителя изменится: будет определен *МАС*-адрес не компьютера назначения, а маршрутизатора сети; с помощью протоколов канального и физического уровня по этому *МАС*-адресу на маршрутизатор будет послана информация.

Несмотря на то, что *IP*-пакет в этом случае не доставляется непосредственно по назначению, протокол *IP* на компьютере-отправителе считает свою задачу выполненной. Дальнейшая судьба *IP*-пакета зависит от правильной настройки маршрутизаторов, объединяющих сети 192.168.5.0 и 192.168.10.0.

Чтобы понять, как работают маршрутизаторы, проанализируем *таблицу**маршрутов,* которую выстраивает при загрузке протокола *IP* компьютер с операционной системой *Windows* *XP* (рис. 5.8). В таблице определено несколько маршрутов с разными параметрами. Читать каждую запись в таблице маршрутизации нужно следующим образом.

*Чтобы доставить пакет в сеть с адресом «Сетевой адрес» и маской «Маска**сети», нужно с интерфейса с IP-адресом «Интерфейс****»*** *послать пакет по IP-адресу «Адрес шлюза», а «стоимость» такой доставки будет равна числу «Метрика».*

Параметры *Сетевой**адрес*и *Маска**сети*задают диапазон всех разрешенных в данной сети *IP*-адресов. Например, 127.0.0.0 и 255.0.0.0 означают любой *IP*-адрес от 127.0.0.1 до 127.255.255.254. *IP*-адрес 127.0.0.1 называется «адресом заглушки» - посланные по этому адресу пакеты должны обрабатываться самим компьютером. Кроме того, маска 255.255.255.255 означает сеть из одного *IP*-адреса, а комбинация 0.0.0.0 - любой неопределенный адрес или маску подсети.

Первая строка в таблице маршрутизации означает то, что делает компьютер при необходимости послать пакет в удаленную, т.е. неизвестную ему из таблицы маршрутизации, сеть - со своего интерфейса пакет посылается на *IP*-адрес маршрутизатора.

Вторая строка таблицы заставляет компьютер посылать самому себе (и отвечать на них) все пакеты, отправленные по любому *IP*-адресу из диапазона 127.0.0.1 - 127.255.255.254.

В третьей строке определено, как посылать пакеты компьютерам ЛВС (по адресам из диапазона 192.168.5.1-192.168.5.254).Здесь видно, что делать это должен сам компьютер - адресом шлюза является его собственный *IP*-адрес 192.168.5.200.

Аналогично (5, 6 и 7 строки таблицы) нужно поступать и в случае, когда пакеты направляются по адресу рассылки подсети (192.168.5.255), по адресам многоадресной рассылки (224.0.0.0) или по адресу локальной широковещательной рассылки (255.255.255.255).

Четвертая строка означает, что пакеты, посланные по *IP*-адресу 192.168.5.200 должны обрабатываться самим компьютером.

Несколько сложнее будет выглядеть таблица маршрутизации компьютера с двумя сетевыми адаптерами, который используется в качестве маршрутизатора для объединения двух сегментов небольшой сети (рис. 5.9).

В этой таблице появилось несколько дополнительных строк, обозначающих маршруты в обе сети - 192.168.5.0 и 192.168.10.0. Заметим, что все такие маршруты будут выстроены компьютером автоматически.

Чтобы наладить *обмен IP-пакетами между этими сетями,* нужно выполнить следующие действия:

- включить маршрутизацию на компьютере *R1* - это можно сделать, например, настроив службу маршрутизации и удаленного доступа, входящую в состав операционной системы Windows Server 2003;

- на всех компьютерах в сети *N1* параметр *Основной шлюз* нужно установить равным *IP*-адресу интерфейса маршрутизатора, подключенного к этой сети, т.е. равным 192.168.5.1, а на компьютерах в сети *N2* - равным 192.168.10.1.

Таким образом, маршрутизатор - это программно-аппаратное устройство с несколькими сетевыми интерфейсами, на котором работает *служба маршрутизации.*

В крупных сетях, содержащих большое количество соединенных друг с другом подсетей, вручную прописывать маршруты доставки пакетов на всех маршрутизаторах нецелесообразно. К тому же такие маршруты являются *статическими,* значит, при каждом изменении конфигурации сети нужно будет проделывать большую работу по перестройке системы 1Р-маршрутизации.

Чтобы избежать этого, достаточно настроить маршрутизаторы так, чтобы они обменивались друг с другом информацией о маршрутах.Для этого в локальных сетях используют такие протоколы, как *RIP (Routing Information Protocol)* и *OSPF (Open Shortest Path First).* Протокол *RIP* проще в настройке, чем *OSPF*, однако для обмена информацией в нем применяются широковещательные сообщения, заметно нагружающие сеть. Поэтому *RIP* обычно используют в относительно небольших сетях. Протокол *OSPF* работает эффективнее, но сложнее настраивается, поэтому его использование рекомендуется для крупных корпоративных сетей.

Таким образом, правильная настройка протокола *IP* для взаимодействия компьютеров в сети *TCP/IP* является очень важной.

Самый простой способ настройки параметров протокола *IP* - назначить их вручную. Достоинством такого метода является то, что сетевые администраторы полностью контролируют все *IP*-адреса компьютеров в сети, что может быть важно с точки зрения защиты данных или взаимодействия с Интернетом. Однако у этого способа много недостатков. Во-первых, легко ошибиться и ввести неправильные параметры маски или шлюза или, что еще хуже, назначить повторяющийся в сети *IP*-адрес. Во-вторых, при изменениях параметров *IP*-адресации в сети (например, при смене IP-адреса маршрутизатора) придется перенастраивать все компьютеры. Но самое неприятное, что при таком способе настройки практически невозможно работать в крупных корпоративных сетях с мобильными устройствами типа ноутбуков или КПК, которые часто перемещаются из одного сегмента сети в другой.

Поэтому чаще применяют специальные серверы, поддерживающие *протокол динамической конфигурации узлов - DHCP (Dynamic Host Configuration Protocol),* задача которых состоит в обслуживании запросов клиентов на получение *IP*-адреса и другой информации, необходимой для правильной работы в сети. Именно поэтому компьютеры с ОС *Windows* по умолчанию настроены на автоматическое получение *IP*-адреса.

Если сервер *DHCP* недоступен, то компьютер самостоятельно назначают себе *IP*-адрес. При этом используется *механизм автоматической личной IP-адресации (Automatic Private IP Addressing, АРIPA),* для которого корпорацией *Microsoft* зарегистрирован диапазон адресов 169.254.0.0-169.254.255.255.

Для проверки параметров и работоспособности протокола IP нужно предпринять следующие шаги.

1. Выполните команду *IPCONFIG /ALL.*

Если в выданной на экран информации не содержится никаких параметров, значит нет активных интерфейсов.

Если в выданной информации есть диагностическое сообщение «Сеть отключена», значит, проблемы с физическим уровнем - проверьте подключение коннектора в разъеме сетевого адаптера и/или работоспособность коммутатора.

Если ваши параметры *IP*-адреса и маски подсети равны 0.0.0.0, значит, используется статический *IP*-адрес, конфликтующий с другим узлом в сети.

Если *IP*-адрес находится в диапазоне 169.254.х.х, значит, *DHCP*-сервер недоступен и работать можно только с теми компьютерами в сети, которые также самостоятельно назначили себе адрес.

В нормальной ситуации при получении *IP*-адреса от *DHCP*-сервера или правильной ручной настройке в выданной на экран информации будут такие параметры, как *IP*-адрес ПК, маска подсети, основной шлюз, *DNS*-сервер и *DHCP*-сервер.

2. Выполните команду *PING* 127.0.0.1.

Если ответ не получен, это свидетельствует о неправильной настройке стека протоколов *TCP/IP*; придется переустановить соответствующую программную поддержку. Если ответ получен, значит, стек протоколов *TCP/IP* работает правильно.

3. Выполните команду *PING* w.x.y.z*,* где w.x.y.z- *IP*-адрес соседнего ПК. Так проверяется работоспособность локальной сети.

4. Выполните команду *PING* w.x.y.z*,*где w.x.y.z - *IP*-адрес основного шлюза.Так проверяется доступность и работоспособность маршрутизатора.

5. Выполните команду *PING* w.x.y.z***,*** где w.x.y.z - *IP*-адрес удаленного ПК.Так проверяется работоспособность всей системы маршрутизации вашей корпоративной сети или соединения с Интернетом.

Во многих современных сетях пакеты протокола *ICMP*, с помощью которых утилита *PING* тестирует взаимодействие, запрещаются по требованию служб безопасности. ОС *Windows XP SP2* с включенным межсетевым экраном также блокирует *ICMP*-пакеты. Поэтому, если утилита *PING* не показывает ответов, не спешите искать причину сбоя на своем компьютере, а сначала выясните у сетевого администратора (или в настройках своей ОС *Windows XP*), разрешено ли в сети использование *ICMP*. В итоге - набор кратких правил, которые помогут не ошибиться при настройке IP-адресации и маршрутизации в сетях *TCP/IP*:

1. чтобы взаимодействовать в сети *TCP/IP*, все ПК должны иметь *IP*-адреса;
2. компьютеры, находящиеся в одном физическом сегменте сети (соединенные концентраторами или коммутаторами), должны принадлежать одной IP-сети, но иметь уникальные *IP*-адреса;
3. для определения идентификаторов локальной сети или удаленных сетей используется маска подсети;
4. чтобы взаимодействовать с удаленными сетями, компьютерам требуется адрес основного шлюза, который должен совпадать с адресом маршрутизатора, соединяющего сеть с другими;
5. маршрутизаторы - это компьютеры с несколькими сетевыми интерфейсами, умеющие передавать *IP*-пакеты из одной сети в другую в соответствии со своими таблицами маршрутизации;
6. маршрутизатор всегда имеет маршруты во все сети, подключенные к нему непосредственно;
7. маршруты в другие сети нужно настраивать;
8. таблицы маршрутизации можно настраивать вручную либо применять динамические протоколы обмена информацией о маршрутизации.

**Контрольные вопросы**

1. Назовите известные Вам сетевые устройства, различия между ними, достоинства и недостатки каждого.
2. Что такое «правило 5-4-3»?
3. Поясните, что такое «*«область столкновений»* (*Collision Domain*)? Какие сетевые устройства ее ограничивают*.*
4. Что такое MAC-адрес, какова его размерность и структура?
5. Что такое *«область широковещания» (Broadcast Domain).* Какие сетевые устройства ее ограничивают*.*
6. Что такое *виртуальные локальные сети?*
7. Что такое стеки протоколов? Какие стеки Вы знаете, их достоинства и недостатки?
8. Какие протоколы составляют стек протоколов сети Интернет?
9. Что такое порт в транспортном уровне стека протоколов сети Интернет?
10. В чем суть задачи межсетевого взаимодействия?
11. Что такое операционная совместимость?
12. В чем решение проблемы межсетевого взаимодействия?
13. Какие основные подходы к решению проблем межсетевого взаимодействия?
14. Что такое инкапсуляцияи туннелирование?
15. Что такое и какой формат IP-адреса?
16. Что такое классы сетей А, В и С?
17. Что такое и зачем нужна маска сети?
18. Что такое бесклассовая схема IP-адресации?
    1. **Технологии и стандарты компьютерных сетей**

**Сетевые службы, клиенты, серверы, ресурсы**

Для работы сети необходимы *сетевые операционные системы* (СОС), с помощью которых можно обмениваться информацией, совместно работать с данными, использовать общие ресурсы и пр. Сетевые ОС подразделяются на *клиентские* (*Windows* *XP* или *Windows* *Vista*) и *серверные* (*Windows Server 2003, 2008)*.

Основная функция клиентской сетевой ОС - предоставление пользователю удобного интерфейса для работы, обеспечение защиты компьютера и безопасности при доступе к данным и ресурсам. Функции серверных ОС - выполнять сервисные функции, предоставляя свои данные и ресурсы для совместного использования, а также обслуживая различные клиентские запросы. Операционными системами для работы в сети используются различные сервисы.

Клиентские операционные системы кроме протокола *TCP/IP*, обеспечивающего межсетевые и транспортные функции, используют еще два сервиса - *службу доступа к файлам и принтерам сетей Microsoft* и *Клиента для сетей Microsoft.* Эти две службы связаны друг с другом - одна используется для предоставления каталогов и принтеров в общий доступ, а другая - для подключения к ним по сети. В операционной системе *Windows XP* дополнительно предоставляется *Планировщик пакетов QoS* (*Quality of Service*) - служба обеспечения качества связи, позволяющая резервироватьнекоторую часть общей полосы пропускания сетевого подключения, а затем выделятьее для таких приложений, где задержки недопустимы (например, при передаче по сети аудио или видео).

Таким образом, в клиентской ОС по умолчанию предусмотрена серверная служба доступа к файлам и принтерам. Эта служба позволяет в небольших сетях обходиться без использования серверов. Такие сети называются *одноранговыми* или *рабочими группами.* Количество компьютеров в них не превышает 10. Компьютеры в одноранговых сетях обычно подключаются к одному концентратору или коммутатору, маршрутизаторы не используются. Чтобы обнаружить соседей, компьютеры применяют широковещательные сообщения, и никакие системы преобразования имен в *IP*-адреса при этом не требуются.

В крупных сетях без серверов не обойтись. Приходится постоянно повышать количество и функциональность серверов, расширять их аппаратные возможности. Многие серверы зачастую делают специализированными- предназначенными для поддержки конкретных служб или приложений. Другие, не очень сложные сервисы можно объединятьв рамках одного мощного аппаратного сервера. При этом под сервером в разных случаях может пониматься как собственно компьютер, так и установленное на нем специализированное программное обеспечение, либо весь этот программно-аппаратный комплекс в целом.

Рассмотрим основные типы серверов.

1). Серверы, обеспечивающие работу в сети *TCP/IP* (серверы сетевой инфраструктуры). К ним относятся *DHCP***-,** *DNS***-** и *WINS*-серверы и настройку работы в крупной сети начинают с них.

*- DHCP-серверы* необходимы, чтобы по запросу *DHCP-клиента* (компьютера, у которого в настройках протокола *TCP/IP*включен режим автоматического получения IP-адреса) выдать ему такие параметры, как уникальный *IP*-адрес и маска подсети. Кроме них, клиент может получать от *DHCP*-сервера ряд дополнительных параметров, важных для взаимодействия с другими сетями и удобной работы в сети: адрес основного шлюза, адреса *DNS*- и *WINS*-серверов, название домена, в который входит этот компьютер, и некоторые другие;

*- DNS-серверы* (*Domain* *Name* *System*) расшифровывается как «система (служба) доменных имен» и выполняют очень важную функцию преобразования (разрешения) имен узлов *(host names)* в соответствующие им *IP-*адреса. Служба *DNS* в Интернете с 1981 г., а с 2000 с выходом *Windows* *2000* стала основной службой преобразования имен в сетях *Microsoft*;

*- WINS-серверы* (*Windows* *Internet* *NameService,* служба межсетевых имен Windows) регистрируют в сети *NetBIOS*-имена компьютеров и их *IP*-адреса, а затем по запросу *WINS-*клиентовпреобразуют эти имена в *IP*-адреса. Эта служба была разработана, чтобы обеспечить поддержку работы *NetBIOS-*приложенийв маршрутизируемых сетях на базе протокола *TCP/IP*. Сейчас она используется для того, чтобы в сети корректно работали устаревшие ОС типа *Windows 9x* или *Windows NT*.

Поясним, что компьютеры для взаимодействия друг с другом используют *IP*-адреса. Пользователям числовыми *IP*-адресами работать неудобно, поэтому при работе в сетях обычно используются символьные имена компьютеров двух типов:

*имена узлов* - состоят из комбинаций букв, цифр и знака дефиса, разделенных точками. Это могут быть имена компьютеров как в Интернете (пример: *www.microsoft.com*), так и в локальной сети (*serverl.domain.local*);

*NetBIOS-имена* - имена компьютеров, содержащие не более 15 любых символов, кроме точек (например, *SERVER1*).

2). *Серверы файлов (файл-серверы)*нужны для хранения больших объемов данных и предоставления к ним доступа пользователей. Один файловый сервер может поддерживать одновременную работу сотен и даже тысяч пользователей. Чтобы обеспечить сохранность информации, файл-серверы оснащены отказоустойчивыми наборами (массивами) жестких дисков и системами резервного копирования на магнитную ленту или другой носитель.

3). *Серверы печати (принт-серверы)*предназначены для обеспечения доступа пользователей к одному или нескольким общим принтерам. Они принимают по сети задания на печать, поступающие от пользовательских приложений, и управляют очередями заданий на печать,обычно обслуживая несколько печатающих устройств.

4). Похожие функции выполняют и*факс-серверы,*обслуживающие клиентские задания на отправку факсов, но они, кроме того, отвечают за получение факсов и их доставку пользователям.

5). *Серверы приложений*выполняют задачи обслуживания запросов пользователей на выборку или обработку какой-либо информации; их часто объединяют с *серверами баз данных.*Важно, что с серверами приложений и баз данных одновременно может работать большое число пользователей, причем выполнение клиентских запросов на специализированном многопроцессорном сервере производится намного быстрее, чем на компьютерах пользователей.

6). *Серверы удаленного доступа и серверы VPN*(*Virtual Private Network* - виртуальная частная сеть) обеспечивают удаленное подключение к локальной сети по модему или через Интернет. Это дает пользователям возможность работать с ресурсами локальной сети предприятия, офиса или учебного заведения из дома или из любого места, где есть подключение к Интернету.

7). *Терминальные серверы*предоставляют возможность работы с другими серверами через специальные программы - *терминальные клиенты.* С помощью этих программ администраторы, находясь вдалеке от локальной сети, могут полностью управлять им, а пользователи могут удаленно работать с установленными на сервере приложениями.

8). *Брандмауэры (межсетевые экраны)*используются при подключении к Интернету для защиты внутренней сети от проникновения или атаки злоумышленников на корпоративные серверы.

9). *Прокси-серверы (серверы-посредники)*выполняют функции контроля доступа пользователей в Интернет и кэширования часто запрашиваемых веб-страниц (что позволяет снизить расходы на пользование Интернетом). Поскольку оба этих сервера предназначены для установки на компьютер, связывающий локальную сеть с Интернетом, их часто объединяют в единую программно-аппаратную систему.

10). *Серверы электронной почты (почтовые серверы, mail-серверы)*обслуживают почтовые ящики пользователей в данной организации, обеспечивая подключения к ним *почтовых клиентов,* а также обрабатывают все входящие и исходящие сообщения. Их также можно использовать для ведения адресных книг, общих папок и систем электронного документооборота.

11). *WWW и FTP-серверы*предоставляют для внешних (а часто - и для внутренних) пользователей доступ к *WWW* и *FTP*-ресурсам, размещенным в данной сети.

12). *Контроллеры домена*обеспечивают в сетях *Microsoft* работу служб я*активного каталога* (*Active Directory*) и поддерживают базу данных всех зарегистрированных в *домене* пользователей, компьютеров, групп и ресурсов. Наличие такой базы данных позволяет администраторам централизованно управлять всеми сетевыми объектами и ресурсами. Пользователи же получают возможность входить в сеть с любого принадлежащего домену компьютера, а затем «прозрачно» (без ввода имени и пароля) подключаться к другим ПК и работать с их ресурсами.

**Стандарты и технологии территориально распределенных сетей**

Решения по первым территориально распределенным (глобальным) сетям началось с решения простой задачи - обеспечения доступа к компьютеру с терминалов, удаленных от него на сотни и тысячи километров. Терминалы соединялись с компьютерами через телефонные сети с помощью модемов. Такие сети позволяли пользователям получать удаленный доступ к разделяемым ресурсам нескольких мощных компьютеров класса суперЭВМ. Затем появились системы, в которых наряду с удаленными соединениями типа терминал-компьютер были реализованы и удаленные связи типа компьютер-компьютер. Компьютеры получили возможность обмениваться данными в автоматическом режиме, что является признаком вычислительной сети. На основе подобного механизма в первых сетях были реализованы службы обмена файлами, синхронизации баз данных, электронной почты и другие, ставшие теперь традиционными сетевые службы.

Именно при построении глобальных сетей были впервые предложены и отработаны многие основные идеи, лежащие в основе современных вычислительных сетей. Такие, например, как многоуровневое построение коммуникационных про­токолов, концепции коммутации и маршрутизации пакетов.

Глобальные компьютерные сети многое унаследовали от старых и распространенных глобальных сетей — *телефонных*. Главное технологическое новшество глобальных компьютерных сетей - отказ от принципа коммутации каналов, на протяжении многих десятков лет успешно использовавшегося в телефонных сетях.

Выделяемый на все время сеанса связи составной телефонный канал, передаю­щий информацию с постоянной скоростью, не мог эффективно использоваться пульсирующим трафиком компьютерных данных, у которого периоды интенсивного обмена чередуются с продолжительными паузами. Эксперименты и математическое моделирование показали, что пульсирующий и малочувствительный к задержкам компьютерный трафик гораздо эффективней передается сетями, работающими по принципу коммутации пакетов, когда данные разделяются на небольшие порции - *пакеты*, - которые самостоятельно перемещаются по сети благодаря наличию адреса конечного узла в заголовке пакета.

Так как прокладка высококачественных линий связи на большие расстояния обходится очень дорого, то в первых глобальных сетях часто использовались уже существующие каналы связи, изначально предназначенные совсем для других целей Например, в течение многих лет глобальные сети строились на основе телефонных каналов тональной частоты, способных в каждый момент времени вести передачу только одного разговора в аналоговой форме. Поскольку скорость передачи дискретных компьютерных данных по таким каналам была очень низкой (десятки килобит в секунду), набор предоставляемых услуг в глобальных сетях такого типа обычно ограничивался передачей файлов, преимущественно в фоновом режиме, и электронной почтой Помимо низкой скорости такие каналы имеют и другой недостаток - они вносят значительные искажения в передаваемые сигналы Поэтому протоколы глобальных сетей, построенных с использованием каналов связи низкого качества, отличаются сложными процедурами контроля и восстановления данных Типичным примером таких сетей являются сети 70-х гг. - *X.25*.

Территориально распределенные сети реализованы в виде телекоммуникационной сети (ТКС), которая включает (рис. 6.1):

- сети доступа (*access* *network*), предназначенные для передачи информационных потоков, поступающих по каналам связи от оборудования пользователей, в узлах магистральной сети (магистрали);

- магистраль (*backbone*, *core network*) объединяет отдельные сети доступа, обеспечивая транзит трафика между ними по высокоскоростным каналам;

- информационные центры или центры управления сервисами (*data centers* или *services control point*) - это ресурсы сети, которые обслуживают пользователей.

Прогресс глобальных компьютерных сетей во многом определялся прогрессом  
телефонных сетей. Это привело к появлению высокоскоростных цифровых каналов, соединяющих автоматические телефонные станции (АТС) и позволяющих одновременно передавать десятки и сотни разговоров. Была разработана специальная технология для создания так называемых *первичных*, или *опорных*, сетей. Такие сети не предоставляют услуг конечным пользователям, они являются фундаментом, на котором строятся скоростные цифровые каналы «точка-точка», соединяющие оборудование других, так называемых *наложенных сетей*, которые уже работают на конечного пользователя.

Первичные сети предназначены для создания коммутируемой инфраструктуры, с помощью которой можно быстро и гибко организовать постоянный канал с двухточечной топологией между двумя устройствами, подключенными к такой сети. Используется техника *коммутации каналов*. На основе каналов, образованных первичными сетями, работают наложенные компьютерные и телефонные сети. Каналы, предоставляемые первичными сетями, отличаются пропускной способностью - от 2 Мбит/с до 10 Гбит/с.

Существует три поколения технологий первичных сетей:

* плезиосинхронная цифровая иерархия (*Plesiochronous Digital Hierarchy, PDH*);
* синхронная цифровая иерархия (*Synchronous Digital Hierarchy, SDH*), в США - *SONET*,
* уплотненное волновое мультиплексирование (*DWDM*).

Первые две технологии (*PDH* и *SDH*) для разделения высокоскоростного канала используют *временное мультиплексирование* (*TDM*) и передают данные в цифровой форме. Каждая из них поддерживает *иерархию скоростей*, так что пользователь может выбрать подходящую ему скорость для каналов, с помощью которых он будет строить наложенную сеть.

Технология *SDH* обеспечивает более высокие скорости, так что при построении крупной первичной сети ее магистраль строится на технологии *SDH*, а сеть доступа — на *PDH*.

Современные сети *DWDM* представляют собой последнее достижение в области создания высокоскоростных каналов. Они уже не являются цифровыми, так как предоставляют своим пользователям *выделенную волну* для передачи информации, которую можно задействовать по усмотрению - модулировать или кодировать. Технология *DWDM* вытесняет *SDH* из протяженных магистралей на периферию сети, превращая ее в технологию сетей доступа. Эти три технологии позволяют создать гибкую и масштабируемую первичную сеть, способную обслуживать большое количество компьютерных и телефонных сетей.

Начало технологии *PDH* было положено разработкой мультиплексора *T-1*, который позволял в цифровом виде мультиплексировать, передавать и коммутировать (на постоянной основе) голосовой трафик **24** абонентов. Так как абоненты по-прежнему пользовались обычными телефонными аппаратами, то есть передача голоса шла в аналоговой форме, то *Т-1* сами осуществляли оцифровывание голоса с частотой 8 КГц и кодировали голос методом импульсно-кодовой модуляции. В результате каждый абонентский канал образовывал цифровой поток данных 64 Кбит/с, а мультиплексор *Т-1* обеспечивал передачу 1,544 Мбит/с.

Для соединения крупных телефонных станций каналы *Т-1* представляли собой слабые и негибкие средства мультиплексирования, поэтому была реализована идея образования каналов с *иерархией скоростей:* **4** канала типа *Т-1* объединили в канал следующего уровня цифровой иерархии *Т-2*, передающий данные со скоростью 6,312 Мбит/с; канал *Т-3*, образованный путем объединения **7**-ми каналов *Т-2*, имеет скорость 44,736 Мбит/с; канал *Т-4*объединяет **6** каналов *Т-3*, в результате его скорость равна 274 Мбит/с. Вся эта технология получила название системы *Т*-каналов**.**

Технология систем *Т*-каналов была стандартизована Американским нацио-нальным институтом стандартов (*ANSI*), а позже – международным комитетом *CCITT* иполучила название *Plesiochrortous* *Digital* *Hierarchy* (*PDH*). В результате внесенных комитетом *CCITT* изменений возникла несовместимость американской и международной версий стандарта *PDH*. Аналогом систем Т-каналов в международном стандарте являются каналы *E-1*, *E-2* и *Е-3* со скоростями - 2,048, 8,488 и 34,368 Мбит/с. Несмотря на различия, в американской и международной версиях технологии цифровой иерархии принято использовать одни и те же обозначения для иерархии скоростей — *DSn* (*Digital* *Signal n*). Далее в таблице приводятся значения для всех введенных стандартами уровней скоростей обеих технологий (см. табл. 6.1).

**Первичные сети** *SDH/SONET*(*Synchronous Digital Hierarchy* — синхронная цифровая иерархия) реализуют технологию синхронных волоконно-оптических сетей. Это высокоскоростные сети цифровой связи, которые строятся на базе оптоволоконных кабельных линий или цифровых радиорелейных линий (рис. 6.2).

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Таблица 6.1 Иерархия цифровых скоростей *PDH* | | | | | | |
|  | **Америка** | | | *CCITT* **(Европа)** | | |
| Обозначение скорости | Количество голосовых каналов | Количество каналов предыдущего уровня | Скорость, Мбит/с | Количество голосовых каналов | Количество каналов предыдущего уровня | Скорость, Мбит/с |
| **DS-0** | 1 | 1 | 64  Кбит/с | 1 | 1 | 64  Кбит/с |
| **DS-1** | 24 T1 | 24 | 1,544 | 30 E1 | 30 | 2,048 |
| **DS-2** | 96 T2 | 4 | 6,312 | 120 E2 | 4 | 8,488 |
| **DS-3** | 672 T3 | 7 | 44,736 | 480 E3 | 4 | 34,368 |
| **DS-4** | 4032 T4 | 6 | 274,176 | 1920 E4 | 4 | 139,264 |

***При построении сетей SDH*** используются следующие модули:

• *мультиплексоры* *SDH* — это основные функциональные модули сетей *SDH*, предназначенные для сборки высокоскоростного потока информации из низкоскоростных потоков и разборки высокоскоростного потока на низкоскоростные;

• *коммутаторы* обеспечивают связь каналов, закрепленных за пользователями, путем полупостоянного перекрестного соединения между ними;

• *концентраторы* служат для объединения однотипных потоков нескольких удаленных узлов сети в одном распределенном узле;

• *регенераторы* - устройства мультиплексирования с одним оптическим каналом доступа и 1-2 выходами, используемыми для увеличения расстояния между узлами сети *SDH*.

Сети и технологии *SDH* отличаются высоким уровнем стандартизации, высокой надежностью (централизованное управление сетью обеспечивает полный мониторинг состояния узлов), наличием полного программного контроля (отслеживание и регистрация аварийных ситуаций, управление конфигурацией сети осуществляется программными средствами с единой консоли управления), возможностью оперативного предоставления услуг по требованию, сравнительно простой схемой развития сети. Благодаря этим преимуществам технология *SDH* стала основной при построении цифровых транспортных сетей самого различного масштаба.

Топология всей *SDH*-сети формируется из отдельных базовых топологий типа «кольцо», «линейная цепь», «звезда», «точка-точка», которые используются в качестве сегментов сети. Чаще применяется радиально-кольцевая архитектура *SDH*-сети, построенная на базе кольцевой и линейной топологий (рис.6.3).

Преимущества сетей *SDH*/*SONET*:

***- гибкая иерархическая схема мультиплексирования цифровых потоков*** разных скоростей (табл. 6.2), позволяющая вводить в магистральный канал и выводить из него пользовательскую информацию любого поддерживаемого уровня скорости, не деульсиплексируя поток;

***- отказоустойчивость сети.***Сети *SDH* обладают высокой степенью «живучести» - технология предусматривает автоматическую реакцию оборудования на такие типичные отказы, как обрыв кабеля, отказ порта, выход из строя мультиплексора или отдельной его карты, направляя трафик по резервному пути или переходя на резервный модуль. Переход на резервный путь происходит в течение ~50 мс;

***- мониторинг и управление сетью***осуществляется на основе информации, встроенной в заголовки кадров. Это обеспечивает обязательный уровень управляемости сети, не зависящий от производителя оборудования, и создает основу для наращивания функций менеджмента в фирменных системах управления;

***- высокое качество транспортного обслуживания***для трафика любого типа (голос, видео и данные). В основе *SDH* - техника временного мультиплексирования *TDM*, обеспечивая каждому абоненту гарантированную пропускную способность, а также низкий и фиксированный уровень задержек.

Сети *SDH* добились прочного положения в телекоммуникационном мире — сегодня они составляют фундамент практически всех крупных сетей — региональных, национальных и международных.

***Недостатки*** – неспособность динамически перераспределять пропускную способность между абонентами сети, т.е. то, что обеспечивается пакетными сетями.

Укрепляет это положение и то, что технология *SDH* может легко интегрироваться с технологией *DWDM*(*Dense Wave Division Multiplexing* – плотное волновое (спектральное) мультиплексирование), обеспечивающей передачу информации по оптическим магистралям с еще более высокими скоростями — сотни гигабит в секунду и выше — *за счет мультиплексирования с разделением по длине волны*.

Таблица 6.2 Иерархия скоростей *SDH / SONET*

|  |  |  |
| --- | --- | --- |
| *SDH* | *SONET* | Скорость, Мбит/с |
|  | *STS-1, OC-1* | 51,84 |
| *STM-1* | *STS-3, OC-3* | 155,52 |
| *STM-3* | *OC-9* | 466,56 |
| *STM-4* | *OC-12* | 622,08 |
| *STM-6* | *OC-18* | 933,12 |
| *STM-8* | *OC-24* | 1244 |
| *STM-12* | *OC-36* | 1866 |
| *STM-16* | *OC-48* | 2488 |
| *STM-64* | *OC-192* | 9953 |
| *STM-256* | *OC-768* | 39810 |

В магистральных сетях с ядром *DWDM* сети *SDH* играют роль сети доступа, то есть ту же роль, которую играют сети *PDH* по отношению к *SDH*.

Технология *DWDM*(*Dense Wave Division Multiplexing* – плотного волнового (спектральное) мультиплексирования) – предназначена для создания оптических магистралей, работающих на мультимегабитных и терабитных скоростях.

Такой качественный скачок происходит из-за принципиально иного, чем в *SDH*, метода мультиплексирования – информация в оптическом волокне передается одновременно большим количеством световых волн. Сети *DWDM* работают по принципу *коммутации каналов*, при этом каждая световая волна представляет собой отдельный *спектральный канал* и несет собственную информацию. При этом устройства *DWDM* занимаются только объединением различных волн в одном световом пучке, а также выделением из общего сигнала информации каждого спектрального канала (рис. 6.4).

К территориальным сетям и представляющих их технологиям обычно относят сети и технологии *X.25*, *Frame Relay* и *ATM*, которые значительно различаются функциональными характеристиками, но все используют технику виртуальных каналов, т.е. ориентированы на установление соединения. Эти сети являются исторически преемственными. Технология сетей *Х.25* появилась в середине 1970-х гг. В них виртуальные каналы использовались для надежной передачи данных, что в 1970-80 годы было очень востребовано, так как линии связи в основном были аналоговыми и не могли обеспечить надежную передачу цифровых данных. Поэтому была важна способность *Х.25* к восстановлению искаженных и потерянных пакетов.

Распространение высокоскоростных и надежных цифровых каналов к середине 1980-х годов привело к тому, что функции технологии *Х.25* по обеспечению надежной передачи данных стали избыточными. Результатом этого стало появление новой технологии глобальных сетей *Frame Relay* (*FR*), особенность которой состоит в том, что избавившись от ненужных в высоконадежных сетях функций проверки, она выполняет только то, что необходимо для доставки кадров адресату. Одновременно возможности *Frame* *Relay* были расширены – стала обеспечиваться поддержки параметров качества обслуживания (*Quality of Service*, *QoS*), необходимая, например, для передачи аудиоданных. В сетях *FR* возможна передача голоса с высоким качеством - для этого коммутаторы сети должны обеспечивать первоочередную передачу аудио трафика среди остальных данных.

В конце 1990-х появилась технология *ATM*, которая отличалась от предыдущих тем, что с самого начала разрабатывалась для предоставления комплекса высокоскоростных транспортных услуг различного уровня качества. *ATM* создавалась как технология для передачи трафика всех возможных типов: компьютерных данных, голоса, видео и пр. При этом был выбран фиксированный и небольшой размер ячейки (кадра), который позволил минимизировать задержки трафика реального времени. Однако это обернулось технической сложностью решения проблемы обработки ячеек на сверхвысоких скоростях (до 2,5 Гбит/с и выше) и значительной стоимостью сети. Остановимся на упомянутых технология подробнее.

Сети ***Х.25*** – первое поколение глобальных сетей с созданием виртуальных каналов и коммутацией пакетов - были стандартизированы в 1976 г. по рекомендациям Международного консультативного комитета по телефонии и телеграфии (CCITT). Стандарт определил синхронный пользовательский интерфейс между пользователем и сетью (*User-to-Network Interface, UNI*). Сама сеть состоит из территориально разнесенных коммутаторов, соединенных выделенными линиями связи, как цифровыми, так и аналоговыми. Устройство и структура сети может быть любой и определяется ее оператором. Взаимодействие между устройствами сети производится по протоколам, аналогичным *UNI*, а между различными сетями - по специальным интерфейсам (*Network-to-Network Interface, NNI*). Сети *Х.25* очень подходят для передачи данных малой интенсивности по ненадежным аналоговым сетям. В структуре сети предусматривалются специальные устройства *PAD* (*Packet Assembler Disassembler*) для сборки-разборки низкоскоростных потоков данных с цифровых терминалов в пакеты, передаваемые по сети. Это и сейчас важно для России, где до сих пор отсутствует развитая инфраструктура высокоскоростных каналов связи. При этом достоверная и упорядоченная передача данных по ненадежным линиям связи обеспечивается за счет тщательной проверки правильности полученных кадров и повторной передачи искаженных кадров между каждой парой соседних узлов сети (рис. 6.5). Рекомендации спецификации *Х.25* описывают три уровня протоколов (стек): физический, канальный и сетевой (рис. 6.6).

Физический уровень описывает сигналы и логику взаимодействия на уровне физического интерфейса - протоколы синхронного интерфейса *Х.21, Х.21bis* к устройствам передачи данных (если линия связи является цифровой), либо к синхронному модему (если линия аналоговая).

Канальный уровень отвечает за эффективную и надежную передачу данных в соединении «точка - точка», т.е. между соседними узлами сети (протокол *LAP-B*, *Link Access Protocol-Balanced*). На этом уровне осуществляется защита от ошибок при передаче между соседними узлами, управление потоком данных и получение оптимального по скорости передачи режима. Для реализации этого поток информации разбивается на кадры, т.е. специальную последовательность битов. Кадр обрамляется «флагами» со значением 0х7е (01111110) и состоит из служебных полей (адреса с максимальной длиной 16 байт, управления с номером кадра, поля проверочной последовательности кадра) и информационного поля. Стандартным размером данных в сетях *Х.25* является 128 байт, а длина пакета может лежать в пределах 64-4096 байт.

На сетевом уровне (в стандарте он называется пакетным) определен протокол *Х.25/3* для обмена пакетами между оконечным оборудованием и сетью. Сетевой уровень предназначен для работы только с одним протоколом канального уровня и не может соединять разнородные сети. Протокол выстаивает виртуальный маршрут между узлами сети, производя первоначальную маршрутизацию пакетов и доведение информации от «точки входа» в сеть до «точки выхода» из нее. В сетях *Х.25* реализуется метод виртуальной коммутации цепей. Перед передачей потока данных от одного абонента к другому между ними сначала устанавливается виртуальное (логическое) соединение, для чего производится провод первого кадра по маршруту сети и выстраивание виртуального канала.

В качестве адресов первоначального запроса используются формат *Х.121* международных номеров (*International Data Numbers, IDN*) комитета CCITT, который может иметь разную длину (до 14-ти десятичных знаков) и бывает трех типов:

полный (международный) сетевой адрес;

внутрисетевой адрес;

телефонный адрес.

Первые четыре десятичные цифры международного адреса – код идентификации (*Data Network Identification Code, DNIC*) сети поделен на две части:

три цифры определяют страну, где находится сеть (Россия – 250 и 251);

четвертая десятичная цифра определяет номер сети в стране.

Остальные цифры кода – это номер национального терминала (*National* *Terminal Number, NTN*), которые позволяют определить номер устройства в сети.

После установления виртуального канала узлы обмениваются пакетами данных, в которых вместо адресов получателя и отправителя указываются более короткие номера логических каналов. Такие виртуальные соединения могут быть как постоянными (*Permanent Virtual Circuit* (или *Channel* или *Connection*), *PVC*), что обеспечивалось на первом этапе развития сети, так и с 1984 г. - коммутируемыми (*Switched* *Virtual* *Circuit* (*Channel*, *Connection*), *SVC*), когда соединение устанавливается на каждый сеанс обмена информацией.

Основные преимущества сетей *Х.25* заключались в следующем:

сети *Х.25* позволяют в режиме реального времени разделять один и тот же физический канал между несколькими абонентами;

сети *Х.25* позволяют передавать данные по выделенным и коммутируемым каналам телефонной сети общего пользования оптимальным образом;

в сетях *Х.25* имеется механизм альтернативной маршрутизации, с помощью которого задается ряд резервных маршрутов, за счет чего значительно увеличивается надежность работы сети.

У сетей *Х.25* были серьезные ограничения:

невозможность передачи голосовой и видеоинформации;

малые скорости передачи, причиной чего являются развитые механизмы коррекции ошибок. Они требуют подтверждения информации между каждыми соседними узлами сети, что приводит к значительным задержкам распространения информации. Поэтому технология *Х.25* применяется в сетях, использующих каналы связи со скоростью передачи от 9,6 до 64 и максимум - 128 Кбит/с.

Указанные ограничения преодолены в технологии *Frame* *Relay* (рис. 6.7).

Сети и технологии *Frame* *Relay* (ретрансляция кадров) были стандартизированы в 1993 г. Они позволяют быстро (до 1,5…2 Мб/с) и эффективно передавать пакетами неравномерно распределенный во времени трафик вычислительных сетей дейтаграммным способом по виртуальному каналу.

Положительные особенности протокола *FR*: малое время задержки при передаче информации через сеть, высокие скорости передачи, эффективное использование полосы пропускания. По сетям *FR* возможна передача не только собственно данных, но и оцифрованного голоса.

Протокол *FR* выполняет функции первого, второго и частично третьего уровней модели OSI и позволяет устанавливать соединение между взаимодействующими узлами сети, что аналогично соединению по *Х.25* в случае, когда используется постоянное виртуальное соединение. Внутри каждого физического канала может быть создана совокупность логических каналов, что и объясняет высокую степень связности, обеспечиваемую протоколом *FR*. Что касается коммутируемых виртуальных соединений, то их использование в *FR*-сетях описывается специальными протоколами (отличия от *Х.25* – отсутствие проверок).

На рис. 6.8 показан стек протоколов *FR* как они описаны в стандарте. Протоколы слоя управления (внешние столбцы на рисунке) выполняют работу по установлению виртуального соединения. Для создания динамически коммутируемых каналов *SVC* коммутаторы сети поддерживают протокол слоя управления *LAP-D* (*Q.921*) для надежной передачи сигнальных кадров установки виртуального канала – на канальном уровне и протокол *Q.933* для адресации оконечных узлов в стандарте *E.164* – на сетевом. Адрес в *E.164* состоит из 15-ти десятичных цифр, которые включают код страны (1..3 цифры), а также код города и номер абонента. К адресу добавляется 40 цифр подадреса для нумерации терминальных устройств.

Быстрая синхронная передача данных обеспечивается на канальном уровне протоколом *LAP-F* (*Link Access Procedure for Frame mode bearer services*), упрощенная версия протокола *LAP-D* сети *X.25*, называемый в рекомендациях стандарта - *Q.922*. При этом высокая скорость передачи обеспечивается, в том числе, за счет исключения контроля ошибок в промежуточных узлах. Адресация, инкапсуляция и восстановление данных осуществляется только в оконечных пунктах средствами протоколов верхних уровней (*IP, IPX, SNA*).

На физическом уровне *FR* может использовать как первичные (опорные) сети *PDH/SDH*, так и цифровые сети *ISDN* (*Integrated Services Digital Network*).

Физическое подключение к сети производится через синхронный порт со скорости от 9,6-64 Кб/с и выше. Один физический канал может разбиваться на несколько постоянных виртуальных каналов (*PVC*), определяемые адресом интерфейса информационного канала (*Data Link Control Interface, DLCI*) в 10 бит. Формат кадра во многом совпадает с кадром сети Х.25 и также ограничен флагами 0х7е (01111110), отличия в размерах заголовка (2 байта, из них 10 бит - под *DLCI*, возможны также 3-х и 4-х байтные заголовки) и информационного поля (стандарт не ограничивает размер кадров, чаще всего минимальный размер 262 октета, а наиболее распространенные реализации употребляют кадры от 1600 до 4096 октетов. Максимальный размер кадра определяется провайдером услуг связи в зависимости от возможностей оборудования). Кадр также содержит проверочное поле, позволяющее определить искаженные кадры.

Сети *FR* могут выступать высокоскоростной альтернативой сетей *Х.25*. В отличие от сетей *Х.25*, где в случае искажения кадра при передаче между соседними узлами происходит его повторная передача, ошибочные кадры *FR* просто выбрасываются, их повторная передача средствами *FR* не происходит. Для обеспечения гарантированной и упорядоченной передачи кадров необходимо использовать протоколы более высокого уровня.

Долговременному использованию технологии *FR* способствует наличие стандартов, обеспечивающих совместимость сетей *FR* с другими сетями. Имеется стандарт *IETF 1294* для преобразования пакетов *TCP/IP* в кадры FR. Спецификация *RFC* *1490* определяет методы инкапсуляции в трафик *FR* трафика сетевых протоколов и протоколов ЛВС. Есть стандарты, обеспечивающие совместимость FR с современными высокоскоростными сетями *ATM*. При входе в сеть *ATM* длинные кадры *FR* разбиваются на короткие, размещаемые внутри *ATM*-ячеек, а при выходе из сети *ATM* из ячеек *ATM*-сети извлекаются фрагменты кадров *FR*, и из них собираются полные кадры *FR*.

Поддержка параметров качества обслуживания (*QoS*) осуществляется путем гарантии для каждого виртуального соединения следующих параметров:

согласованной скорости передачи данных (Committed Information Rate, CIR) - скорости, с которой сеть будет передавать пользовательские данные;

согласованной величины пульсации (*Committed Burst Size, Be*) - максимального количества байтов, которое сеть будет передавать от пользователя за интервал времени *Т* (время пульсации) со скоростью *CIR*;

дополнительной величины пульсации (*Excess Burst Size, Be*) – максимального количество байтов, которое сеть будет пытаться передать сверх установленного значения *Вс* за интервал времени *Т*.

Все эти данные могут задаваться для каждого направления виртуального канала отдельно, обеспечивая различные варианты качества доставки информации.

Наиболее распространенные способы доступа к сетям *FR*:

- использование выделенных линий;

- через сети *Х.25* по обычным коммутируемым телефонным линиям;

- через цифровую сеть *ISDN* для передачи данных и голоса.

Технология *FR* сохраняет свои преимущества и актуальность, т.к. она обеспечивает идеальный доступ к высокоскоростной магистральной сети по низкоскоростным каналам связи. Эта технология в настоящее время является эффективной для приложений, связанных с интеграцией неравномерного трафика локальных сетей, и чувствительной к задержке голосовой информации.

**ATM** (*Asynchronous Transfer Mode*, режим асинхронной передачи) - это сетевая технология, основанная на передаче небольших информационных блоков - ячеек (*cells*) - фиксированного размера, предназначенная для передачи разнородного трафика (звук, видео, данные). Применение малых ячеек фиксированного размера упрощает аппаратуру передачи данных, минимизирует задержки при обработке данных и обеспечивает более равномерную загрузку сети. Передатчик и приемник здесь не синхронизированы, а ячейки передаются в любое время.

Технология была предложена лабораторией AT&T (США) в 1980 г. В 1988 г. был принят стандарт МККТТ (CCITT) по использованию *ATM* в широкополосных цифровых сетях с интегрированным обслуживанием (***В-ISDN***). Заработала технология с середины 1990-х гг.

В основе режима асинхронной передачи лежит концепция двух оконечных систем (терминалов), осуществляющих связь друг с другом через совокупность промежуточных коммутаторов (*ATM Switch*), а каскадное соединение нескольких коммутаторов позволяет увеличить размеры сети.

Стандарт *ATM* определяет интерфейс пользователя с сетью (***UNI***, *User-to-Network Interface*) и интерфейс между сетями (***NNI***, *Network-to-Network Interface*), т.е. *UNI* соединяет устройство оконечного пользователя (абонентную систему - АС) с *АТМ*-коммутатором, a *NNI* представляет собой канал связи между двумя коммутаторами. На рис. 6.9 показана упрощенная структура сети *ATM*.

Процедура установки виртуального соединения между двумя узлами *ATM*-сети похожа на процедуру установления виртуального *TCP*-соединения (принцип трехшагового рукопожатия) – см. рис. 6.10.

Установка виртуального соединения начинается с выдачи *UNI*-интерфейсом узла 1 запроса на соединение (*setup*).Коммутатор (*Switch ATM* 1), получив запрос, транслирует его дальше по сети через интерфейс *NNI*, а в ответ на полученный запрос формирует в адрес узла 1 подтверждение выполнения запроса (*call proceeding*— запрос в процессе исполнения). Коммутатор 2 (*Switch* *ATM* 2), получив запрос на соединение, выполняет аналогичные действия: передает запрос на соединениеUNI-устройству узла 2 и выдает подтверждение исполнения запроса коммутатору *ATM* 1. *UNI*-устройство узла 2, получив запрос, формирует подтверждение «запрос принят» (*connect*),которое далее транслируется по тем же каналам к источнику запроса на соединение, т.е. *UNI*-устройству узла 1. Каждый промежуточный узел и *UNI*-устройство узла 1, получая этот ответ, формирует в адрес отправителя «подтверждение получения запроса» (*connect ACK*).

Аналогично происходит разрыв соединения. Узел 1 - инициатор завершения связи посредством *UNI*-интерфейса передает в сеть «сообщение о завершении» (*release*),в ответ на которое все устройства, задействованные в организации соединения, передают источнику сообщения «подтверждение получения сообщения *release*» (*release complete*).Получение этого сообщения *UNI*-устройством узла 1 является сигналом к завершению связи.

Адрес места назначения указывается в сообщении *setup*.

В *AIM* используется 3 вида адресов. Первый - имеет 20 байт и имеет структуру *OSI*-адреса. Первый байт указывает на вид адреса (один из трех). Байты 2и 3 указывают на принадлежность к стране, а байт 4 задает формат последующей части кода адреса, которая содержит 3 байта кода администрации (*authority*), 2 байта домена, 2 байта области и 6 байт собственно адреса (аналогично *MAC*-адресу). Во втором формате байты 2 и 3 выделены для международных организаций, а не стран. Остальная часть адреса имеет тот же формат, что и в варианте 1. Третий формат является старой формой МККТТ (*CCITT E.164*) в15-цифровых десятичных телефонных номеров *ISDN*.

*UNI*-устройства узлов обеспечивают правильную маршрутизацию ячеек, используя два поля заголовка *ATM*-ячейки - идентификаторы виртуальных пути (*Virtual Path Identifier, VPI*) и канала (*Virtual Circuit Identifier, VCI*).

Архитектура (модель) *ATM* описывает процедуры связи двух оконечных систем посредством *ATM*-коммутаторов и состоит из трех уровней (рис. 6.11): физического уровня, уровня ATM и уровня адаптации ATM. Прямого соответствия между уровнями протоколов технологии АТМ и уровнями модели OSI нет, примерное соотношение представлено на рисунке.

Протоколы ATM физического уровня определяют, как получать информационные сигналы из среды передачи, преобразовывать их в ячейки и передавать эти ячейки уровню *ATM*. Этот уровень условно разбит на два подуровня: преобразования передачи (*Transmission* *Convergence, ТС*) и адаптации к физической среде передачи (*Physical Medium Dependent, PMD*). Цель создания данных подуровней - обеспечить возможность использования разнообразных физических сред (табл. 6.3), для которых определены различные предельные скорости передачи данных. Стандартными значениями скорости передачи данных для сетей *ATM* являются 25, 155 и 622 Мбит/с, хотя потенциально *ATM* может обеспечить скорость до 2,5 Гбит/с.

Таблица 6.3 Скорости передачи в сетях АТМ в различных средах

|  |  |
| --- | --- |
| *Среда передачи данных* | *Скорость передачи данных, Мбит/с* |
| Неэкранированная витая пара (UTP) категории 3  UTP категории 3, экранированная витая пара (STP)  Оптоволоконный кабель | 25  155  25, 155, 622 и выше |

Подуровень *ТС*отвечает за прием ячеек с уровня *ATM* и упаковку их в соответствующий формат для передачи по подуровню *PMD*. На этом уровне осуществляется выделение ячеек из потока, их шифрование-дешифрование и вставка/подавление ячеек в потоке с целью обеспечения его непрерывности. Подуровень выполняет создание при передаче и проверку при приеме контрольной суммы заголовка (*Header Error Check, НЕС*).

Протоколы уровня *ATM* описывают механизмы получения ячеек, формирования заголовков и передачи ячеек уровню адаптации *ATM*, а также установки соединения с требуемым качеством сервиса (*QoS*).

Сети с установлением соединений могут гарантировать определенное качество сервиса (*Quality of Service, QoS*) для трафика, чувствительного к параметрам сети (например, звук, видео).

Уровень *ATM* выполняет следующие основные функции:

мультиплексирование и демультиплексирование ячеек разных соединений определяются идентификаторами виртуальных канала (*VCI*) и пути (VPI);

преобразование значений VCI и/или VPI на коммутаторах;

извлечение/вставку заголовка ячейки;

реализация механизма управления потоком данных в универсальном сетевом интерфейсе (*UNI*).

Ячейка состоит из заголовка (5 байт) и поля данных (48 байт). Ее формат представленна рис. 6.12, причем формат заголовка для связи «интерфейс пользователя - сеть» (*UNI*) и «сеть - сеть» (*NNI*) различаются.

Поле «общее управление потоком» (*GFC*) используется только в *UNI* для управления трафиком и предотвращения перегрузки, а для *NNI* оно не определено и его биты применяются для поля «идентификатора виртуального пути» (*VPI*).

Значения полей «идентификатор виртуального пути» (*VPI*) и «идентификатор виртуального канала» (*VCI*) полей *VPI* и *VCI* устанавливаются оконечными устройствами при запрашивании соединения.

Поле «идентификатор типа полезной нагрузки» (*Payload Type Identification, PTI*) и используется для обозначения типа полезной нагрузки ячейки, а также для обозначения управляющих процедур.

Поле «признак потери приоритета ячейки» (*Cell Loss Priority, CLP*) - это 1 бит, который определяет возможность потери ячейкой своего приоритета. Если ячейку можно отбросить из-за перегрузки, этот бит устанавливается в единицу, в этом случае если на коммутаторе возникает перегрузка, то он отбрасывает все ячейки, у которых этот бит установлен. Таким образом, при перегрузке сети можно отдать приоритет ячейкам, переносящим информацию определенного типа, например видео.

Поле «контрольная сумма заголовка» (*НЕС*) содержит код, который вычисляется по всем полям *ATM*-заголовка. Такой метод контроля ошибок позволяет выявить все 1-разрядные ошибки и часть многоразрядных.

Уровень адаптации *ATM* изначально состоял из пяти протоколов (*ATM* *adaptation* *layer, AAL*). Эти протоколы принимают ячейки с уровня *ATM*, формируют из них данные и передают эти данные на более высокий уровень. Когда протоколы *AAL* получают данные с более высокого уровня, они разбивают их на ячейки и передают их уровню *ATM*.

*ATM*-технология способна обрабатывать трафики 4 различных классов.

***Класс А*** - синхронный трафик с постоянной скоростью передачи и с предварительным установлением соединения. Протокол, обслуживающий трафик этого класса, предназначен для обеспечения потребностей в сетевых услугах при передаче информации с постоянной скоростью (примеры - несжатая речь, видеоинформация).

***Класс В*** - синхронный трафик с переменной скоростью передачи и с предварительным установлением соединения (сжатая речь, видеоинформация). Здесь также необходимы синхронизация аппаратуры отправителя и получателя и предварительное установление связи между ними, но допускается переменная скорость передачи. Информация передается через фиксированные промежутки времени, но ее объем в течение сеанса передачи может изменяться. Если объем передаваемой информации превышает фиксированный размер одной ячейки, эта информация разбивается на несколько ячеек, сборка которых осуществляется в пункте назначения.

***Класс С*** - асинхронный трафик с переменной скоростью передачи и с предварительным установлением соединения. Здесь синхронизации аппаратуры отправителей получателя не требуется. Такой способ передачи необходим в сетях с коммутацией пакетов (сети *Х.25*, Интернет, сети с ретрансляцией кадров).

***Класс D*** - асинхронный трафик с переменной скоростью передачи и без установления соединения. Протокол, управляющий доставкой трафика класса D, разработан для обеспечения коммутации данных без установления соединения. В этом протоколе предусматривается использование кадров переменной длины: с помощью передатчика каждый кадр делится на сегменты фиксированного размера, которые помещаются в *ATM*-ячейки; приемник собирает сегменты в исходный кадр, завершая таким образом процесс, который называется сегментацией и сборкой.

Уровень адаптации *ATM* определяет 4 категории сервиса - постоянную (*Constant Bit Rate, CBR*), переменную (*Variable Bit Rate, VBR*), неопределенную (*Unspecified Bit Rate, UBR*) и доступную скорости передачи (*Available Bit Rate, ABR*). Они используются для различного качества сервиса для разных типов трафика.

Категория*CBR*гарантирует самое высокое качество сервиса и применяется для чувствительного к задержкам трафика (аудио и видеоинформация). Данные передаются с постоянной скоростью и малыми задержками.

Категория*VBR*существует в двух видах, которые используются для различных типов трафика: реального времени(*Real-Time VBR, RT-VBR*), когда требуется жесткая синхронизация между ячейками и поддержка чувствительного к задержкам трафика и без требований реального времени(*Non-Real-Time VBR, NRT-VBR*), когда нет нужды в жесткой синхронизации между ячейками и допускаются задержки.

Категория*UBR*применяется для трафика, который допускает задержки. Подобно *VBR* здесьне резервирует полосу пропускания для виртуального канала. В результате один виртуальный канал может применяться для нескольких передач.

Категория*ABR*используется для передачи трафика, который допускает задержки и дает возможность многократно использовать виртуальные каналы. Однако если *UBR* не резервирует полосу пропускания и не предотвращает потерь ячеек, то *ABR* обеспечивает для соединения допустимые значения ширины полосы пропускания и коэффициента потерь.

Категории дифференцируются по значениям параметров, определяющих качество сервиса (*QoS*), примеры приведены в табл. 6.4:

коэффициент потерь ячеек (*Cell Loss Ratio*) определяет, какой процент высокоприоритетных ячеек может быть потерян за время передачи;

задержка передачи ячейки (*Cell Transfer Delay*) определяет время (или среднее время), требуемое для доставки ячейки адресату;

вариации задержек при передаче ячеек (*Cell Delay Variation, CDV*), большая величина *CDV* приводит к прерыванию аудио- и видеосигналов.

Способность *ATM* обеспечивать для приложений различный уровень качества сервиса является одним из важнейших достоинств этой технологии.

Таблица 6.4. Категории сервиса

|  |  |  |
| --- | --- | --- |
| *Класс* | *Описание* | *Пример* |
| *CBR* | Постоянная скорость передачи | Несжатый звук или видеоинформация |
| *RT-VBR* | Переменная скорость передачи (реальное время) | Пакетные аудио-, видеоконференции и *multimedia* |
| *NRT-VBR* | Переменная скорость передачи (не в режиме реального времени) | Мультимедиа по электронной почте, *Frame relay, X.25* |
| *ABR* | Доступная скорость передачи | Протоколы без организации соединений типа *IP*, просмотр *Web*-информации |
| *UBR* | Неспецифицированная скорость передачи | Пересылка файлов в фоновом режиме |

* + 1. **Защита компьютерных сетей**

Во времена, когда компьютеры не были объединены в сети или подключены к Интернету, о безопасности данных можно было особенно не заботиться. Достаточно было обеспечить *физическую защиту* компьютера и контролировать доступ посторонних пользователей к устройствам записи (например, к дисководам).

После объединения компьютеров в сети все изменилось - без серьезной защиты теперь уже не обойтись, иначе и операционная система, и хранящиеся на компьютере или передаваемые по сети данные могут стать легкой добычей, причем так, что работающие на этом компьютере пользователи ничего не заметят. Поэтому далее изучим основные принципы, используемые при построении современных сетевых ОС, обсудим главные угрозы, представляющие опасность для компьютеров, пользователей и их данных, а также укажем простейшие правила обеспечения безопасности, которые обязательно следует соблюдать при работе в сети.

Принципы построения защищенных ОС:

1) все современные ОС являются *многопользовательскими* - они рассчитаны на работу в системе (в том числе одновременную) нескольких пользователей;

2) чтобы отличить одного пользователя от другого, применяются *учетные**записи* (*accounts*) с уникальными *именами* и *паролями;*

3) учетные записи различаются *уровнем**полномочий (привилегий, прав)* - набором действий, которые обладатель данной учетной записи может выполнять в системе. Обычно учетные записи разделяют на *административные,* обладающие максимальными привилегиями, и *пользовательские,* набор полномочий для которых позволяет нормально работать в системе, но не разрешает выполнять какие-либо критичные с точки зрения безопасности данных операции, например форматировать разделы жесткого диска или менять настройки сети.

В версиях ОС *Windows* дополнительно существуют учетные записи с уровнем прав, средним между административным и пользовательским (участники группы «Опытные пользователи»), а также обладающие минимальными полномочиями *гостевые учетные записи* (участники группы «Гости», включая встроенную учетную запись «Гость»). Кроме того, существует два типа учетных записей - *локальные* из базы данных конкретного компьютера с ОС *Windows*, и *глобальные учетные записи в домене,* которые хранятся на контроллерах домена (подробнее о них будет сказано далее);

4) для входа в компьютер обязательно нужно указать имя и пароль учетной записи, зарегистрированной в системе. Следует подчеркнуть, что понятие «вход в систему» подразумевает не только непосредственный доступ, но и другие возможности работы с компьютером, например *сетевой* или *терминальный* вход, для которых также требуются пользовательские имя и пароль.

В операционных системах *Windows* допускается также сетевой вход без указания имени и пароля *(анонимный* вход); такие подключения используются при некоторых взаимодействиях в сетях *Microsoft*;

5) после входа в систему (интерактивного, сетевого и т. д.) пользователь получает доступ к ресурсам того компьютера, в который он вошел (например, доступ к локальным файлам или каталогам). Уровень доступа при этом определяется *списком разрешений,* т. е. возможных действий, которые данный пользователь может осуществлять с защищенным объектом. Например, один пользователь может изменить или удалить файл, другой - только прочитать его, а третьему вообще будет отказано в доступе к этому файлу.

Уже неоднократно упоминались *рабочие группы* и *домены.* Разберем, чем отличаются эти две модели сетевого взаимодействия в сетях *Microsoft*.

*Рабочая группа*- это логическая группировка компьютеров, объединенных общим именем для облегчения навигации в пределах сети. Принципиально важно, что каждый компьютер в рабочей группе равноправен(т. е. сеть получается одноранговой) и поддерживает собственную *локальную базу данных учетных записей пользователей (Security Accounts Manager, SAM).*

Отсюда вытекает основная проблема, которая не позволяет использовать рабочие группы в крупных корпоративных сетях. Действительно, если вспомнить, что вход в защищенную систему является обязательным, а непосредственный и сетевой входы принципиально различаются (непосредственный контролируется локальным компьютером, а сетевой - удаленным), то, например, пользователю, вошедшему на компьютер *Comp1* под локальной учетной записью *User1*, будет отказано в доступе к принтеру, установленному на компьютере *Соmр2*, поскольку в его локальной базе нет пользователя с именем *Userl* (рис. 6.13). Таким образом, для обеспечения «прозрачного» взаимодействия в рабочей группе нужно создавать одинаковые учетные записи с одинаковыми паролями на всех компьютерах,где работают пользователи и расположены ресурсы.

В ОС *Windows XP Professional* для рабочих групп предусмотрен специальный режим: «Использовать простой общий доступ к файлам», позволяющий обойти указанную проблему (режим включен по умолчанию).

В этом случае подключение к любому сетевому ПК осуществляется от имени его локальной гостевой учетной записи, которая включается с помощью *Мастера настройки сети* (по умолчанию она отключена) и для которой настраивается нужный уровень доступа. Для ОС *Windows XP Home Edition* этот способ сетевого взаимодействия является основным и отключить его нельзя (поэтому компьютеры с данной ОС невозможно сделать участниками домена). Понятно, что управлять учетными записями и ресурсами в рабочей группе можно только при небольшом количестве компьютеров и пользователей. В крупных сетях следует применять домены.

*Домен*- это логическая группировка компьютеров, объединенных общей базой данных пользователей и компьютеров, политикой безопасности и управления.

Домены создаются на основе сетевых ОС Windows, а база данных, как мы уже говорили, поддерживается *контроллерами домена.* Важным в доменах является то, что все компьютеры здесь не сами осуществляют проверку пользователей при входе, а передоверяют эту процедуру контроллерам (рис. 6.14). Такая организация доступа позволяет легко осуществить однократную проверку пользователя при входе в сеть, а затем без проверки предоставлять ему доступ к ресурсам всех ПК домена.

Угроз, поджидающих пользователей при подключении компьютера к сети, довольно много. Приведем только основные из них:

*- «взлом» компьютера* обычно производится с целью захвата контроля над операционной системой и получения доступа к данным;

*- повреждение системы* чаще всего организуется, чтобы нарушить работоспособность (вызвать отказ в обслуживании - «*Denial of Service*») каких-либо сервисов или компьютера (чаще сервера) целиком, а иногда - даже всей сетевой инфраструктуры организации;

*- кража данных* из-за неправильно установленных прав доступа, при передаче данных или «взломе» системы позволяет получить доступ к защищаемой, часто - конфиденциальной информации со всеми вытекающими отсюда неприятными для владельца этих данных последствиями;

*- уничтожение данных* имеет целью нарушить или даже парализовать работу систем, компьютеров, серверов или всей организации.

Атаки на компьютеры или серверы, вирусы, «черви», шпионские и «троянские» программы - все это злонамеренное ПО пишется для того, чтобы осуществить в той или иной степени перечисленные выше угрозы.

Типичная «троянская» программа обычно «маскируется» под какую-либо полезную утилиту (или может быть спрятана в какой-либо программе), а если пользователь по незнанию запустит ее на выполнение, такая программа начинает контролировать компьютер, открывая её создателю доступ к данным (так называемый «*backdoor*» - «черный ход»), похищая и пересылая ему набираемые с клавиатуры пароли и т. п.

«*Фишинг*» (*fishing*, рыбная ловля) - распространенный сегодня вид мошенничества в Интернете. Злоумышленники создают сайты, внешне похожие на сайты Интернет-магазинов, банков и пр., а затем «заманивают» на них посетителей (например, с помощью рекламных баннеров) и предлагают «подтвердить свои персональные данные». Иногда злоумышленники с той же целью рассылают электронные письма якобы от имени администрации почтового сервера с просьбой «подтвердить пароль доступа к почтовому ящику».

*Основные меры безопасности при работе в сети*довольно просты. Их можно сформулировать в виде следующего набора правил:

- отключайте компьютер, когда им не пользуются. Как говорят эксперты по компьютерной безопасности, «самым защищенным является выключенный компьютер, хранящийся в банковском сейфе»;

- своевременно обновляйте операционную систему. В любой ОС периодически обнаруживаются так называемые *«*уязвимости*»,* снижающие защищенность компьютера. Их наличие нужно внимательно отслеживать, чтобы вовремя предпринимать меры для их устранения.

Для ОС Windows корпорацией *Microsoft* создан специальный веб-узел *Windows Update*, обратившись к которому (например, с помощью программы *WUPDMGR.EXE* или команды ***Windows Update*** в меню **Пуск**), можно просмотреть и скачать список обновлений, рекомендуемых для компьютера;

- используйте ограниченный набор хорошо проверенных приложений, не устанавливайте на компьютер программы, взятые из непроверенных источников (особенно из Интернета). Если приложение больше не нужно, удалите его;

- без необходимости не предоставляйте ресурсы компьютера в общий доступ. Если же это все-таки потребовалось, обязательно настройте минимально необходимый уровень доступа к ресурсу только для зарегистрированных учетных записей;

- установите (или включите) на компьютере *персональный межсетевой экран (брандмауэр).* Если речь идет о корпоративных сетях, установите брандмауэры как на маршрутизаторах, соединяющих вашу локальную сеть с Интернетом, так и на всех компьютерах сети;

- обязательно установите на компьютер специализированное антивирусное и «антишпионское» программное обеспечение. Настройте его на автоматическое получение обновлений как минимум один раз в неделю;

- даже если вы единственный владелец компьютера, для обычной работы применяйте *пользовательскую учетную запись:* в этом случае повреждение системы, например, при заражении вирусом, будет неизмеримо меньше, чем если бы вы работали с правами администратора. Для всех учетных записей, особенно административных, установите и запомните сложные пароли.

Сложным является пароль, содержащий случайную комбинацию букв, цифр и специальных символов, например *jxglrg$N*. Он не должен совпадать с именем учетной записи. В операционных системах *Windows* сложный пароль можно сгенерировать автоматически, используя команду *NET USER* с ключом /*RANDOM*, например: *NET USER Имя\_Пользователя /RANDOM.* Пароль в виде случайной последовательности символов нелегко запомнить, поэтому часто используют следующую технику - пароль набирается в английской раскладке русскими буквами. Например, слово «Пароль» тогда будет выглядеть как «*Gfhjkm*». Однако этот способ следует применять с осторожностью - взломщики давно имеют целые словари подобным образом преобразованных слов, так что желательно вставлять в такие пароли специальные символы и цифры.

Пароли для доступа в различные системы должны быть разными. Недопустимо использовать один и тот же пароль для администрирования компьютера и для входа, например, на игровой веб-сайт;

- при работе с электронной почтой никогда сразу не открывайте вложения, особенно полученные от неизвестных отправителей. Сохраните вложение на диск, проверьте его антивирусной программой и только затем откройте. Если есть такая возможность, включите в вашей почтовой программе защиту от потенциально опасного содержимого и отключите поддержку *HTML*;

- при работе с веб-сайтами соблюдайте меры разумной предосторожности: старайтесь избегать регистрации, не передавайте никому персональные сведения о себе и внимательно работайте с Интернет-магазинами и другими службами, где применяются онлайновые способы оплаты с помощью кредитных карт или систем типа *WebMoney*, Яндекс-Деньги и т. д.

При проведении оплаты убедитесь, что соединение защищено шифрованием с помощью технологии *Secure Sockets Layer (SSL)* - в этом случае адресная строка обязательно должна начинаться с «*https://»;*

- перечисленные выше меры лишь повышают общую защищенность системы и данных, но не дают никакой гарантии от их повреждения или даже полной потери. Поэтому обязательно следует создавать *резервные копии* системы и данных на съемном жестком диске или на *DVD-RW* - это позволит вам легко восстановить их в случае утери. При этом одну копию имеет смысл хранить вне дома, например, в сейфе;

- исключительно важную роль играет обучение всех пользователей основам безопасной работы в сетях - как в домашних, так и в корпоративных, - ведь нарушение правил одним пользователем ставит под угрозу всю систему защиты.

При резервном копировании полезно использовать утилиты для создания «образов» жесткого диска (такие, как *Norton Ghost*). Резервную копию можно снять с «системного» жесткого диска после правильной установки на него всех требуемых программ и антивирусной проверки и хранить ее на другом жестком диске (сетевом или съемном), чтобы в случае повреждения системы быстро восстановить ее работоспособность.

Таким образом, для работы в сети нужны сетевые операционные системы, которые принято делить на клиентские и серверные:

- клиентские ОС отличаются небольшим набором служб, но включают в себя спектр сетевых приложений;

- серверные системы бывают различных типов и предназначены для обслуживания тех или иных запросов сетевых клиентов.

Для организации работы в сетях Microsoft применяются две модели:

- рабочие группы, используемые при небольшом числе компьютеров, и

- домены, позволяющие легко объединять большое число пользователей, рабочих станций и серверов.

Все сетевые ОС и хранящиеся на компьютерах данные должны быть надежно защищены, причем желательно, чтобы применяемая система безопасности была многоуровневой.

**Контрольные вопросы**

1. Какие клиентские сетевые ОС Вы знаете?
2. Какие серверные сетевые ОС Вы знаете?
3. Назовите известные Вам типы серверов и их основные функции.
4. Какое главное технологическое новшество глобальных компьютерных сетей перед сетями связи?