**ТЕЛЕКОММУНИКАЦИИ**

**Понятие о сетях ЭВМ**

При физическом соединении двух или более компьютеров образуется *компьютерная сеть.* В общем случае, для создания компьютерных сетей необходимо специальное аппаратное обеспечение (*сетевое оборудование*) и специальное программное обеспечение (*сетевые программные средства*)*.* Простейшее соединение двух компьютеров для обмена данными называется *прямым соединением.* Для создания прямого соединения компьютеров, работающих в операционной системе Windows, не требуется ни специального аппаратного, ни программного обеспечения. В этом случае аппаратными средствами являются стандартные порты ввода/вывода (последовательный или параллельный), а в качестве программного обеспечения используется стандартное средство, имеющееся в составе операционной системы.

Компьютерные сети принято разделять на *локальные* (*LAN – Local Area Network*) и *глобальные* (*WAN – Wide Area Network*). Компьютеры локальной сети преимущественно используют единый комплект протоколов для всех участников. По территориальному признаку локальные сети отличаются компактностью. Они могут объединять компьютеры одного помещения, этажа, здания, группы компактно расположенных сооружений. Глобальные сети имеют, как правило, увеличенные географические размеры. Они могут объединять как отдельные компьютеры, так и отдельные локальные сети, в том числе и использующие различные протоколы.

**ЛОКАЛЬНЫЕ СЕТИ**

Используются для объединения близко расположенных компьютеров без использования телефонных линий. В свою очередь уже объединенные в ЛВС компьютеры могут быть подключены к Интернету.

**Типы локальных сетей**

Локальная вычислительная сеть (ЛВС) – это совокупность компьютеров и других средств вычислительной техники (активного сетевого оборудования, принтеров, сканеров и т. п.), объединенных с помощью кабелей и сетевых адаптеров и работающих под управлением сетевой операционной системы. Вычислительные сети создаются для того, чтобы группа пользователей могла совместно задействовать одни и те же ресурсы: файлы, принтеры, модемы, процессоры и т. п. Каждый компьютер в сети оснащается сетевым адаптером, адаптеры соединяются с помощью сетевых кабелей и тем самым связывают компьютеры в единую сеть. Компьютер, подключенный к вычислительной сети, называется рабочей станцией или сервером, в зависимости от выполняемых им функций. Эффективно эксплуатировать мощности ЛВС позволяет применение технологии "клиент/ сервер". В этом случае приложение делится на две части: клиентскую и серверную. Один или несколько наиболее мощных компьютеров сети конфигурируются как серверы приложений: на них выполняются серверные части приложений. Клиентские части выполняются на рабочих станциях; именно на рабочих станциях формируются запросы к серверам приложений и обрабатываются полученные результаты.

Различают сети с одним или несколькими выделенными серверами и сети без вы деленных серверов, называемые одноранговыми сетями. Рассмотрим сначала локальные сети с выделенным сервером. В сетях с выделенным сервером именно ресурсы сервера, чаще всего дисковая память (винчестер), доступны всем пользователям. Серверы, разделяемым ресурсом которых является дисковая память, называются файл-серверами. Можно сказать, что сервер обслуживает все рабочие станции. Файловый сервер обычно используется только администратором сети и не предназначен для решения прикладных задач. Поэтому он может быть оснащен недорогим, даже мо­нохромным дисплеем. Однако файловые серверы почти всегда содержат несколько быстродействующих накопителей. Сервер должен быть высоконадежным, поскольку выход его из строя приведет к остановке работы всей сети. На файловом сервере, как правило, устанавливается сетевая операционная система.

На рабочих станциях, как правило, устанавливается обычная операционная система, например Windows. Рабочая станция – это индивидуальное рабочее место пользователя. Полноправным владельцем всех ресурсов рабочей станции является пользователь. В то же время ресурсы файл сервера разделяются всеми пользователями. В качестве рабочей станции может использоваться компьютер практически любой конфигурации. Но в конечном счете, все зависит от тех приложений, которые этот компьютер использует.

Существует несколько признаков, по которым можно узнать, работает компьютер в составе сети или автономно. Если компьютер является сетевой рабочей станцией, то, во-первых после его включения появляются соответствующие сообщения, во-вторых, для входа в сеть необходимо пройти процедуру регистрации и, в-третьих, после регистрации в распоряжении оказываются новые дисковые накопители, принадлежащие файловому сереру.

Еще одной важной функцией файлового сервера является управление работой сетевого пойнтера. Сетевой принтер подключается к файл-серверу, но пользоваться им можно с любой рабочей станции. То есть каждый пользователь может отправить на сетевой принтер материалы, предназначенные для печати. Регулировать очередность доступа к сетевому принтеру будет файловый сервер.

**ЛВС с выделенным сервером**

При выборе компьютера на роль файлового сервера необходимо учитывать следующие факторы:

быстродействие процессора;

скорость доступа к файлам, размещенным на жестком диске;

емкость жесткого диска;

объем оперативной памяти;

уровень надежности сервера;

степень защищенности данных.

Высокое быстродействие серверу нужно для того, чтобы во время работы большой ЛВС файловый сервер мог обрабатывать огромное количество запросов на обслуживание файлов, а на это затрачивается значительное процессорное время. Для того чтобы ускорить обслуживание запросов и создать у пользователя впечатление, что именно он является единственным клиентом сети, необходим быстродействующий процессор.

Наиболее важным компонентом файлового сервера является дисковый накопитель На нем хранятся все файлы пользователей сети. Быстрота доступа, емкость и надежность накопителя во многом определяют, насколько эффективным будет использование сети

Сетевые операционные системы с выделенным файл-сервером обычно имеют более высокую производительность, поскольку они оптимизированы именно под выполнение операций с файлами. В принципе, никаких более важных действий на выделенном файл-сервере не выполняется. Значительного повышения производительности работы сервера можно добиться, увеличивая его оперативную память. В одноранговой сети 512 мегабайт памяти может быть вполне достаточно, в то время как для крупной сети с выделенным файл-сервером желательна память объемом 2048 и более мегабайт. Если файловый сервер снабжен оперативной памятью достаточного объема, то он имеет возможность именно в оперативной памяти хранить те области дискового пространства, к которым обращаются наиболее часто. Такой метод хорошо известен, часто применяется для ускорения доступа к данным на обычных ПК и называется методом кэширования. Ведь если идет обращение к файлу, данные которого в данный момент находятся в кэше, сервер может передать искомую информацию, не обращаясь к диску. В результате этого будет достигнут значительный временной выигрыш.

Сетевой адаптер, установленный на файловом сервере – это такое устройство, через которое проходят практически все данные, функционирующие в локальной сети. В связи с этим необходимо, чтобы этот адаптер работал быстро. Сетевой адаптер становится более быстродействующим в результате, во-первых, повышения его разрядности и, во-вторых, увеличения объема его собственного ОЗУ. На файл-сервере должен быть установлен сетевой адаптер для шины PCI, что позволяет поддерживать высокую скорость передачи данных.

**Одноранговые ЛВС**

В одноранговых сетях любой компьютер может быть и файловым сервером, и рабочей станцией одновременно. Преимущество одноранговых сетей заключается в том, что нет необходимости копировать все используемые сразу несколькими пользователями файлы на сервер. В принципе любой пользователь сети имеет возможность использовать все данные, хранящиеся на других компьютерах сети, и устройства, подключенные к ним. Основной недостаток работы одноранговой сети заключается в значительном увеличении времени решения прикладных задач. Это связано с тем, что каждый компьютер сети отрабатывает все запросы, идущие к нему со стороны других пользователей. Следовательно, в одноранговых сетях каждый компьютер работает значительно интенсивнее, чем в автономном режиме.

Затраты на организацию одноранговых вычислительны сетей относительно небольшие. Однако при увеличении числа рабочий станций эффективность их использования резко уменьшается. Пороговое значение числа рабочих станций составляет, по оценкам фирмы Novell, 25-30. Поэтому одноранговые сети используются только для относительно небольших рабочих групп.

**Архитектура ЛВС**

Различают три наиболее распространенные сетевые архитектуры, которые используют и для одноранговых сетей и для сетей с выделенным файл-сервером. Это так называемые шинная, кольцевая и звездообразная структуры.

В случае реализации *шинной структуры* все компьютеры связываются в цепочку. Причем на ее концах надо разместить так называемые терминаторы, служащие для гашения сигнала. Если же хотя бы один из компьютеров сети с шинной структурой оказывается неисправным, вся сеть в целом становится неработоспособной. В сетях с шинной архитектурой для объединения компьютеров используется тонкий и толстый кабель. Максимальная теоретически возможная пропускная способность таких сетей составляет 10 Мбит/с. Такой пропускной способности для современных приложений, использующих видео- и мультимедийные данные, явно недостаточно. Поэтому почти повсеместно применяются сети с звездообразной архитектурой.



Рис. 8. Шинная архитектура

Для построения сети со *звездообразной архитектурой* в центре сети необходимо поместить концентратор (рис. 9). Его основная функция – обеспечение связи между компьютерами, входящими в сеть. То есть все компьютеры, включая файл-сервер, не связываются непосредственно друг с другом, а присоединяются к концентратору. Такая структура надежнее, поскольку в случае выхода из строя одной из рабочих станций все остальные сохраняют работоспособность. В сетях же с шинной топологией в случае повреждения кабеля хотя бы в одном месте происходит разрыв единственного физического канала, необходимого для движения сигнала. Кроме того, сети с звездообразной топологией поддерживают технологии Fast Ethernet и Gigabit Ethernet, что позволяет увеличить пропускную способность сети в десятки и даже сотни раз (при использовании соответствующих сетевых адаптеров и кабелей).



Рис. 9. ЛВС со звездообразной архитектурой

Кольцевая структура (рис. 10) используется в в сетях Token Ring и мало чем отличается от шинной. Также в случае неисправности одного из сегментов сети вся сеть выходит из строя. Правда, отпадает необходимость в использовании терминаторов.



Рис. 4.3. ЛВС с кольцевой архитектурой

**Принципы работы сети**

В сети любой структуры в каждый момент времени обмен данными может происходить только между двумя компьютерами одного сегмента. В случае ЛВС с выделенным файл-сервером – это файл-сервер и произвольная рабочая станция; в случае одноранговой ЛВС – это любые две рабочие станции, одна из которых выполняет функции файл-сервера. Упрощенно диалог между файл-сервером и рабочей станцией выглядит так: открыть файл → подтвердить открытие файла; передать данные файла - пересылка данных; закрыть файл → подтверждение закрытия файла. Управляет диалогом сетевая операционная система, клиентские части которой должны быть установлены на рабочих станциях.

Связь между компьютерами ЛВС физически осуществляется на основе одной из двух схем – обнаружения коллизий и передачи маркера. Метод *обнаружения коллизий* используется стандартами Ethernet, Fast Ethernet и Gigabit Ethernet, а *передачи маркера* – стандартом Token Ring.

В сетях Ethernet адаптеры непрерывно находятся в состоянии прослушивания сети. Для передачи данных сервер или рабочая станция должны дождаться освобождения ЛВС и только после этого приступить к передаче. Однако не исключено, что передача может начаться несколькими узлами одного сегмента сети одновременно, что приведет к коллизии. В случае возникновения коллизии, узлы должны повторить свои сообщения. Повторная передача производится адаптером самостоятельно без вмешательства процессора компьютера. Время, затрачиваемое на преодоление коллизии, обычно не превышает одной микросекунды. Передача сообщений в сетях Ethernet производится пакетами со скоростью 10, 100 и 1000 Мбит/с. Естественно, реальная загрузка сети меньше, поскольку требуется время на подготовку пакетов. Все узлы сегмента сети принимают сообщение, передаваемое компьютером этого сегмента, но только тот узел, которому оно адресовано, посылает подтверждение о приеме. Основными поставщиками оборудования для сетей Ethernet являются фирмы 3Com, Bay Networks (недавно компания Nortel купила Bay Networks), CNet.

В ЛВС с *передачей маркера* сообщения передаются последовательно от одного узла к другому вне зависимости от того, какую архитектуру имеет сеть – кольцевую или звездообразную. Каждый узел сети получает пакет от соседнего. Если данный узел не является адресатом, то он передает тот же самый пакет следующему узлу. Передаваемый пакет может содержать либо данные, направляемые от одного узла другому, либо маркер. Маркер – это короткое сообщение, являющееся признаком незанятости сети. В том случае, когда рабочей станции необходимо передать сообщение, ее сетевой адаптер дожидается поступления маркера, захватывает его, а затем формирует пакет, содержащий данные, и передает этот пакет в сеть. Пакет распространяется по ЛВС от одного сетевого адаптера к другому до тех пор, пока не дойдет до компьютера-адресата, который произведет в нем стандартные изменения. Эти изменения являются подтверждением того, что данные достигли адресата. После этого пакет продолжает движение дальше по ЛВС, пока не возвратится в тот узел, который его сформировал. Узел-источник убеждается в правильности передачи пакета и возвращает в сеть маркер. Важно отметить, что в ЛВС с передачей маркера функционирование сети организовано так, что коллизии возникнуть не могут. Пропускная способность сетей Token Ring равна 16 Мбит/с. Оборудование для сетей Token Ring производит IBM, 3Com и некоторые другие фирмы.

**Сетевое оборудование**

В ПК для того, чтобы его можно было использовать в сети, необходимо установить сетевые адаптеры. Некоторые ПК имеют заранее установленный сетевой адаптер. Сетевой адаптер должен быть по скорости совместим с концентратором, к которому ПК подключается. Так, сетевой адаптер Ethernet соответствует концентратору Ethernet, а сетевой адаптер Fast Ethernet – концентратору Fast Ethernet.

*Концентратор* и *коммутатор* относятся к разным типам активного сетевого оборудования, которое используется для соединения устройств сети. Они различаются способом передачи в сеть поступающих данных (трафика).

*Концентраторы*. Термин "концентратор" иногда используется для обозначения любого сетевого устройства, которое служит для объединения ПК сети, но на самом деле концентратор – это многопортовый повторитель. Устройства подобного типа просто передают (повторяют) всю информацию, которую они получают – то есть все устройства, подключенные к портам кон­центратора, получают одну и ту же информацию.

Концентраторы используются для расширения сети. Однако чрезмерное увлечение концентраторами может привести к большому количеству ненужного трафика, который поступает на сетевые устройства. Ведь концентраторы передают трафик в сеть, не определяя реальный пункт назначения данных. ПК, которые получают пакеты данных, используют адреса назначения, имеющиеся в каждом пакете, для определения, предназначен ли пакет им или нет. В небольших сетях это не является проблемой, но даже в сетях среднего размера с интенсивным трафиком следует использовать коммутаторы, которые минимизируют количество необязательного трафика.

*Коммутаторы*. Коммутаторы контролируют сетевой трафик и управляют его движением, анализируя адреса назначения каждого пакета. Коммутатор знает, какие устройства соединены с его портами, и направляет пакеты только на необходимые порты. Это дает возможность одновременно работать с несколькими портами, расширяя тем самым полосу пропускания.

Таким образом, коммутация уменьшает количество лишнего трафика, что происходит в тех случаях, когда одна и та же информация передается всем портам.

Коммутаторы и концентраторы часто используются в одной и той же сети; концентраторы расширяют сеть, увеличивая число портов, а коммутаторы разбивают сеть на небольшие, менее перегруженные сегменты. Однако применение коммутатора оправдано лишь в крупных сетях, т. к. его стоимость на порядок выше стоимости концентратора.

*Когда следует использовать концентратор или коммутатор*. В небольшой сети (до 20 рабочих мест) концентратор или группа концентраторов вполне могут справиться с сетевым трафиком. В этом случае концентратор просто служит для соединения всех пользователей сети.

 В сетях большего размера (около 50 пользователей) может появиться необходимость использовать коммутаторы для разделения сети на сегменты, чтобы уменьшить количество необязательного трафикпа.

*Сетевые карты.* При выборе сетевой карты, нужно обратить внимание на то, с какой шиной – PCI или ISA – она работает. Сейчас большинство сетевых карт предназначено для размещения в PCI-слоты. Поскольку шина РСI более быстродействующая, ее предпочтительно использовать в сетях Fast Ethernet.

Обычно на сетевой карте имеется несколько индикаторов, представляющих собой обычные светодиоды. Индикаторы показывают, в каком режиме работает сетевая карта и передает она в данный момент данные или нет. Чаще всего используется три-четыре индикатора. Перечислим информацию, передаваемую индикаторами:

исправность сетевого соединения;

режим работы: полу или полнодуплексный;

скорость передачи данных 10 или 100 Мбит/с;

идет передача данных или нет.

Для отображения режима работы и скорости передачи могут использоваться не два индикатора, а один. Например, компания 3Com для демонстрации скорости передачи использует два индикатора, a SMC – один, цвет которого меняется в зависимости от значения скорости – 10 или 100 Мбит/с. Естественно, чем больше у сетевого адаптера индикаторов, тем больше информации о роботе сети у вас имеется.

Существует еще ряд характеристик, которые в ряде случаев следует учитывать при выборе сетевых карт. К ним относятся: наличие Boot ROM, то есть возможность загрузки с сетевой карты (а не, например, с винчестера); наличие режима Bus master, то есть возможность независимой работы с шиной; поддержка удаленного управления и администрирования. Кроме того, многие производители сетевого оборудования и ПО, разработали программные средства, позволяющие увеличить производительность работы сетевых адаптеров.

*Средства обеспечения надежности*. Большой вред работе сети может нанести отключение электропитании или значительное падение напряжения в сети. Ведь если сбой электропитания произойдет во время записи данных на диск, файл может оказаться испорченным. Для защиты данных в случае возникновения таких ситуаций в ЛВС применяются источники бесперебойного питания. ИБП – это устройство, основным элементом которого является аккумуляторная батарея. При отключении питания или при резком падении напряжения необходимый уровень напряжения поддерживается ИБП. Батареи ИБП непрерывно подзаряжаются от внешней электросети. Даже в случае отключения питания в сети ИБП способен сохранять работоспособность ком­пьютера в течение длительного периода времени. Этот период зависит от мощности, потребляемой компьютером, и от мощности ИБП, которая измеряется в вольт-амперах. Так, ИБП мощностью 600 ВА может автономно поддерживать работу 300 Вт компьютера примерно в течение двадцати минут.

Имеет смысл в сетях с выделенным файл-сервером снабжать ИБП по крайней мере файл-сервер. ИБП обычно поставляется вместе со специальными платами-адаптерами, которые устанавливаются в свободный слот сервера. Сетевая ОС взаимодействует с адаптером ИБП и в случае сбоя в системе электропитания оповещает об этом рабочие станции, закрывает все открытые файлы и выдает сообщение о необходимости отключения сервера.

**ГЛОБАЛЬНЫЕ СЕТИ**

**Основные компоненты глобальной сети**

По территориальному признаку локальные сети отличаются компактностью. Они могут объединять компьютеры одного помещения, этажа, здания, группы компактно расположенных сооружений. Глобальные сети имеют, как правило, увеличенные географические размеры. Они могут объединять как отдельные компьютеры, так и отдельные локальные сети, в том числе и использующие различные протоколы.

Создание локальных сетей характерно для отдельных предприятий или отдельных подразделений предприятий. Если предприятие (или отрасль) занимает обширную территорию, то отдельные локальные сети могут объединяться в глобальные сети. В этом случае локальные сети связывают между собой с помощью любых традиционных каналов связи (кабельных, спутниковых, радиорелейных и т. п.). При соблюдении специальных условий для этой цели могут быть использованы также телефонные каналы.

Для связи между собой нескольких локальных сетей, работающих по разным протоколам, служат специальные средства, называемые *шлюзами.* Шлюзы могут быть как аппаратными, так и программными. Например, это может быть специальный компьютер (*шлюзовой сервер*),а может быть и компьютерная программа. В последнем случае компьютер может выполнять не только функцию шлюза, но и какие-то иные функции, типичные для рабочих станций.

При подключении локальной сети предприятия к глобальной сети важную роль играет понятие *сетевой безопасности*.В частности, должен быть ограничен доступ в локальную сеть для посторонних лиц извне, а также ограничен выход за пределы локальной сети для сотрудников предприятия, не имеющих соответствующих прав. Для обеспечения сетевой безопасности между локальной и глобальной сетью устанавливают так называемые *брандмауэры.* Брандмауэром может быть специальный компьютер или компьютерная программа, препятствующая несанкционированному перемещению данных между сетями.

Для работы в Интернете необходимо:

* физически подключить компьютер к одному из узлов Всемирной сети;
* получить *IP*-адрес на постоянной или временной основе;
* установить и настроить программное обеспечение – программы-клиенты тех служб Интернета, услугами которых предполагается пользоваться.

Организации, предоставляющие возможность подключения к своему узлу и выделяющие *IP*-адреса, называются *поставщиками услуг Интернета* (используется также термин *провайдер).* Они оказывают подобную услугу на договорной основе.

Физическое подключение может быть *выделенным* или *коммутируемым.* Для выделенного соединения необходимо проложить новую или арендовать готовую физическую линию связи (кабельную, оптоволоконную, радиоканал, спутниковый канал и т. п.). Такое подключение используют организации и предприятия, нуждающиеся в передаче больших объемов данных.

**Принципы построения, архитектура глобальной сети**

Типичный пример структуры глобальной компьютерной сети приведен на рис. 11. Здесь используются следующие обозначения: S (switch) — коммутаторы, К – компьютеры, R (router) — маршрутизаторы, MUX (multiplexor) – мультиплексор, UNI (User-Network Interface) – интерфейс пользователь-сеть и NNI (Network-Network Interface) – интерфейс сеть-сеть. Кроме того, офисная АТС обозначена аббревиатурой РВХ, а маленькими черными квадратиками – устройства DCE.

Сеть строится на основе некоммутируемых (выделенных) каналов связи, которые соединяют коммутаторы глобальной сети между собой. Коммутаторы называют также *центрами коммутации пакетов*, то есть они являются коммутаторами пакетов, которые в разных технологиях глобальных сетей могут иметь и другие названия – кадры, ячейки (cell). Как и в технологиях локальных сетей принципиальной разницы между этими единицами данных нет, однако в некоторых технологиях есть традиционные названия.



Рис. 11. Пример структуры глобальной сети

Коммутаторы устанавливаются в тех географических пунктах, в которых требуется ответвление или слияние потоков данных конечных абонентов или магистральных каналов, переносящих данные многих абонентов. Естественно, выбор мест расположения коммутаторов определяется многими соображениями, в которые включается также возможность обслуживания коммутаторов квалифицированным персоналом, наличие выделенных каналов связи в данном пункте, надежность сети, определяемая избыточными связями между коммутаторами.

Абоненты сети подключаются к коммутаторам в общем случае также с помощью выделенных каналов связи. Эти каналы связи имеют более низкую пропускную способность, чем магистральные каналы, объединяющих коммутаторы, иначесеть бы не справилась с потоками данных своих многочисленных пользователей. Для подключения конечных пользователей допускается использование коммутируемых каналов, то есть каналов телефонных сетей, хотя в таком случае качество транспортных услуг обычно ухудшается.

Конечные узлы глобальной сети более разнообразны, чем конечные узлы локальной сети. На рис. 11 показаны основные типы конечных узлов глобальной сети: отдельные компьютеры К, локальные сети, маршрутизаторы R и мультиплексоры MUX, которые используются для одновременной передачи по компьютерной сети данных и голоса (или изображения). Все эти устройства вырабатывают данные для передачи в глобальной сети, поэтому являются для нее устройствами типа DTE (Data Terminal Equipment). Локальная сеть отделена от глобальной маршрутизатором или удаленным мостом (который на рисунке не показан), поэтому для глобальной сети она представлена единым устройством DTE – портом маршрутизатора или моста.

**Модели протоколов обмена информацией, семиуровневая модель**

Согласно рекомендациям Международного института стандартизации *ISO* системы компьютерной связи рекомендуется рассматривать на семи разных уровнях (рис. 12). Каждый новый уровень все больше и больше увеличивает функциональность системы связи. Чем выше уровень в модели связи, тем больше различных функциональных служб его используют. Рассмотрим, как в модели *ISO* происходит обмен данными между пользователями, находящимися на разных континентах.



Рис. 12. Простейшая модель службы передачи сообщений

1. На *прикладном уровне* с помощью специальных приложений пользователь создает документ (сообщение, рисунок и т. п.).

2. На *уровне представления* операционная система компьютера фиксирует, где находятся созданные данные (в оперативной памяти, в файле на жестком диске и т. п.) и обеспечивает взаимодействие со следующим уровнем. Здесь данные упаковываются в *блоки*.

3. На *сеансовом уровне* компьютер пользователя взаимодействует с локальной или глобальной сетью. Протоколы этого уровня проверяют права пользователя на «выход в эфир» и передают документ к протоколам транспортного уровня. Данные запаковываются во **фрагмент**.

4. На *транспортном уровне* документ преобразуется в ту форму, в которой положено передавать данные в используемой сети. Например, он может нарезаться на небольшие **пакеты** стандартного размера.

5. *Сетевой уровень* определяет маршрут движения данных в сети. Так, например, если на транспортном уровне данные были «нарезаны» на пакеты, то на сетевом уровне каждый пакет должен получить адрес, по которому он должен быть доставлен независимо от прочих пакетов. Здесь данные с 4 уровня запаковываются в **кадр**.

6. *Уровень соединения* необходим для того, чтобы промодулировать сигналы, циркулирующие на физическом уровне, в соответствии с данными, полученными с сетевого уровня. Например, в компьютере эти функции выполняет сетевая карта или модем.

7. Реальная передача данных происходит на *физическом уровне*. Здесь нет ни документов, ни пакетов, ни даже байтов – только биты, то есть, элементарные единицы представления данных. Восстановление документа из них произойдет постепенно, при переходе с нижнего на верхний уровень на компьютере клиента. Средства физического уровня лежат за пределами компьютера. В локальных сетях это оборудование самой сети. При удаленной связи с использованием телефонных модемов это линии телефонной связи, коммутационное оборудование телефонных станций и т. п.

На компьютере получателя информации происходит обратный процесс преобразования данных от битовых сигналов до документа.

Разные уровни протоколов сервера и клиента не взаимодействуют друг с другом напрямую, но они взаимодействуют через физический уровень. Постепенно переходя с верхнего уровня на нижний, данные непрерывно преобразуются, «обрастают» дополнительными данными, которые анализируются протоколами соответствующих уровней на сопредельной стороне. Это и создает эффект виртуального взаимодействия уровней между собой. Однако, несмотря на виртуальность, это все-таки соединения, через которые тоже проходят данные.

На использовании виртуальных соединений основаны такие позитивные свойства электронных систем связи, как возможность работать по одному физическому каналу сразу с несколькими серверами. Но на них же основаны и такие негативные средства, как «троянские программы». Троянская программа – разновидность «компьютерного вируса», создающая во время сеансов связи виртуальные соединения для передачи данных о компьютере, на котором установлена. Среди этих данных может быть парольная информация, информация о содержании жесткого диска и т. п. В отличие от обычных компьютерных вирусов троянские программы не про­изводят разрушительных действий на компьютере и потому лучше маскируются.

На виртуальных соединениях основаны все службы современного Интернета. Так, например, пересылка сообщения от сервера к клиенту может проходить через десятки различных компьютеров. Это совсем не означает, что на каждом компьютере сообщение должно пройти через все уровни – ему достаточно «подняться» до сетевого уровня, (определяющего адресацию) при приеме и вновь «опуститься» до физического уровня при передаче. В данном случае служба передачи сообщений основывается на виртуальном соединении сетевого уровня и соответствующих ему протоколах.

**Основные протоколы**

Ранние эксперименты по передаче и приему информации с помощью компьютеров начались еще в 50-х годах и имели лабораторный характер. Лишь в конце 60-х годов на средства Агентства Перспективных Разработок министерства обороны США (*DARPA – Defense Advanced Research Project Agency*) была создана первая сеть национального масштаба. По имени агентства она получила название *ARPANET.* Эта сеть связала несколько крупных научных, исследовательских и образовательных центров. Ее основной задачей стала координация групп коллективов, работающих над едиными научно-техническими проектами, а основным назначением стал обмен электронной почтой и файлами с научной и проектно-конструкторской документацией. Сеть *ARPANET* заработала в 1969 году. Немногочисленные узлы, входившие в нее в то время, были связаны *выделенными линиями.* Прием и передача информации обеспечивались программами, работающими на *узловых* компьютерах. Сеть постепенно расширялась за счет подключения новых узлов, а к началу 80-х годов на базе наиболее крупных узлов были созданы свои региональные сети, воссоздающие общую архитектуру *ARPANET* на более низком уровне (в региональном или локальном масштабе).

Пока глобальное расширение *ARPANET* происходило за счет механического подключения все новых и новых аппаратных средств (узлов и сетей), до Интернета в современном понимании этого слова было еще очень далеко. По-настоящему рождением Интернета принято считать 1983 год. В этом году произошли революционные изменения в программном обеспечении компьютерной связи. Днем рождения Интернета в современном понимании этого слова стала дата стандартизация протокола связи *TCP/IP,* лежащего в основе Всемирной сети по нынешний день.

Здесь требуется уточнить, что в современном понимании *TCP/IP* – это не один сетевой протокол, а два протокола, лежащих на разных уровнях (это так называемый *стек протоколов*). Протокол *TCP –* протокол *транспортного уровня.* Он управляет тем, *как происходит передача информации.* Протокол *IP* – *адресный.* Он принадлежит *сетевому уровню* и определяет, *куда происходит передача.*

*Протокол TCP.* Согласно протоколу *TCP,* отправляемые данные “нарезаются” на небольшие пакеты, после чего каждый пакет маркируется таким образом, чтобы в нем были данные, необходимые для правильной сборки документа на компьютере получателя.

Для понимания сути протокола *TCP* можно представить игру в шахматы по переписке, когда двое участников разыгрывают одновременно десяток партий. Каждый ход записывается на отдельной открытке с указанием номера партии и номера хода. В этом случае между двумя партнерами через один и тот же почтовый канал работает как бы десяток соединений (по одному на партию). Два компьютера, связанные между собой одним физическим соединением, могут точно так же поддерживать одновременно несколько TCP-соединений. Так, например, два промежуточных сетевых сервера могут одновременно по одной линии связи передавать друг другу в обе стороны множество TCP-пакетов от многочисленных клиентов.

*Протокол IP.* IP (*Internet Protocol*) – адресный протокол*.* Его суть состоит в том, что у каждого участника Всемирной сети должен быть свой уникальный адрес (*IP-адрес*)*.* Без этого нельзя говорить о точной доставке *ТСР-*пакетов на нужное рабочее место. Этот адрес выражается очень просто – четырьмя байтами, например: 195.38.46.11. Структуру IP-адреса организована так, что каждый компьютер, через который проходит какой-либо *ТСР*-пакет, может по этим четырем числам определить, кому из ближайших “соседей” надо переслать пакет, чтобы он оказался “ближе” к получателю. В результате конечного числа перебросок *ТСР*-пакет достигает адресата. "Близость" оценивается не географически – в расчет принимаются условия связи и пропускная способность линии. Два компьютера, находящиеся на разных континентах, но связанные высокопроизводительной линией космической связи, считаются более “близкими” друг к другу, чем два компьютера из соседних поселков, связанные простым телефонным проводом. Решением вопросов, что считать “ближе”, а что “дальше”, занимаются специальные средства – *маршрутизаторы.*

Поскольку один байт содержит до 256 различных значений, то теоретически с помощью четырех байтов можно выразить более четырех миллиардов уникальных *IP*-адресов (2564 за вычетом некоторого количества адресов, используемых в качестве служебных). На практике же из-за особенностей адресации к некоторым типам локальных сетей количество возможных адресов составляет порядка двух миллиардов, но и это по современным меркам достаточно большая величина.

**Линии связи**

*Физическая среда передачи данных* может представлять собой кабель, то есть набор проводов, изоляционных и защитных оболочек и соединительных разъемов, а также земную атмосферу или космическое пространство, через которые распространяются электромагнитные волны.

В зависимости от среды передачи данных линии связи разделяются на:

проводные (воздушные);

кабельные (медные и волоконно-оптические);

радиоканалы наземной и спутниковой связи.

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

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

Скрученная пара проводов называется *витой парой*. Витая пара существует в экранированном варианте, когда пара медных проводов обертывается в изоляционный экран, и неэкранированном, когда изоляционная обертка отсутствует. Скручивание проводов снижает влияние внешних помех на полезные сигналы, передаваемые по кабелю. *Коаксиальный кабель* имеет несимметричную конструкцию и состоит из внутренней медной жилы и оплетки, отделенной от жилы слоем изоляции. Существует несколько типов коаксиального кабеля, отличающихся характеристиками и областями применения – для локальных сетей, для глобальных сетей, для кабельного телевидения и т. п. *Волоконно-оптический кабель* состоит из тонких (5÷60 микрон) волокон, по которым распространяются световые сигналы. Это наиболее качественный тип кабеля – он обеспечивает передачу данных с очень высокой скоростью (до 10 Гбит/с и выше) и к тому же лучше других типов передающей среды обеспечивает защиту данных от внешних помех.

*Радиоканалы наземной и спутниковой связи* образуются с помощью передатчика и приемника радиоволн. Существует большое количество различных типов радиоканалов, отличающихся как используемым частотным диапазоном, так и дальностью канала. Диапазоны коротких, средних и длинных волн (KB, CB и ДВ), называемые также диапазонами амплитудной модуляции (Amplitude Modulation, AM) по типу используемого в них метода модуляции сигнала, обеспечивают дальнюю связь, но при невысокой скорости передачи данных. Более скоростными являются каналы, работающие на диапазонах ультракоротких волн (УКВ), для которых характерна частотная модуляция (Frequency Modulation, FM), а также диапазонах сверхвысоких частот (СВЧ или microwaves). В диапазоне СВЧ (свыше 4 ГГц) сигналы уже не отражаются ионосферой Земли, и для устойчивой связи требуется наличие прямой видимости между передатчиком и приемником. Поэтому такие частоты используют либо спутниковые каналы, либо радиорелейные каналы, где это условие выполняется.

В компьютерных сетях сегодня применяются практически все описанные типы физических сред передачи данных, но *наиболее перспективными являются волоконно-оптические*. На них сегодня строятся как магистрали крупных территориальных сетей, так и высокоскоростные линии связи локальных сетей. Популярной средой является также витая пара, которая характеризуется отличным соотношением качества к стоимости, а также простотой монтажа. С помощью витой пары обычно подключают конечных абонентов сетей на расстояниях до 100 метров от концентратора. Спутниковые каналы и радиосвязь используются чаще всего в тех случаях, когда кабельные связи применить нельзя – например, при прохождении канала через малонаселенную местность или же для связи с мобильным пользователем сети, таким как шофер грузовика, врач, совершающий обход, и т. п.

**Службы Интернета**

Когда говорят о работе в Интернете или об использовании Интернета, то на самом деле речь идет не об Интернете в целом, а только об одной или нескольких из его многочисленных служб. В зависимости от конкретных целей и задач клиенты Сети используют те службы, которые им необходимы.

Разные службы имеют разные протоколы. Они называются *прикладными протоколами.* Их соблюдение обеспечивается и поддерживается работой специальных программ. Таким образом, чтобы воспользоваться какой-то из служб Интернета, необходимо установить на компьютере программу, способную работать по протоколу данной службы. Такие программы называют *клиентскими* или просто *клиентами*. Так, например, для передачи файлов в Интернете используется специальный прикладной протокол *FTP* (*File Transfer Protocol*). Соответственно, чтобы получить из Интернета файл, необходимо:

– иметь на компьютере программу, являющуюся клиентом *FTP* (*РТР-клиент*);

– установить связь с сервером, предоставляющим услуги *FTP* (*FTP-сервером*).

Другой пример: чтобы воспользоваться электронной почтой, необходимо соблюсти протоколы отправки и получения сообщений. Для этого надо иметь программу (*почтовый клиент*) и установить связь с *почтовым сервером*. Так же обстоит дело и с другими службами.

***Терминальный режим****.* Исторически одной из ранних является служба удаленного управления компьютером *Telnet*. Подключившись к удаленному компьютеру по протоколу этой службы, можно управлять его работой. Такое управление еще называют *консольным* или *терминальным.* В прошлом эту службу широко использовали для проведения сложных математических расчетов на удаленных вычислительных центрах. Так, например, если для очень сложных вычислений на персональном компьютере требовались недели непрерывной работы, а на удаленной супер-ЭВМ всего несколько минут, то персональный компьютер применяли для удаленного ввода данных в ЭВМ и для приема полученных результатов.

В наши дни в связи с быстрым увеличением мощности персональных компьютеров необходимость в подобной услуге сократилась, но, тем не менее, службы *Telnet* в Интернете продолжают существовать. Часто протоколы *Telnet* применяют для дистанционного управления техническими объектами, например телескопами, видеокамерами, промышленными роботами.

Каждый сервер, предоставляющий *Telnet*-услуги, обычно предлагает свое клиентское приложение. Его надо получить по сети (например, по протоколу FTP), установить на своем компьютере, подключиться к серверу и работать с удаленным оборудованием.

***Электронная почта* (*E-Mail*)**. Эта служба также является одной из наиболее ранних. Ее обеспечением в Интернете занимаются специальные *почтовые серверы*. Здесь и далее под *сервером* может пониматься как специальный компьютер, так и программное обеспечение. Таким образом, один узловой компьютер Интернета может выполнять функции нескольких серверов и обеспечивать работу различных служб, оставаясь при этом универсальным компьютером, на котором можно выполнять и другие задачи, характерные для средств вычислительной техники. Почтовые серверы получают сообщения от клиентов и пересылают их по цепочке к почтовым серверам адресатов, где эти сообщения накапливаются. При установлении соединения между адресатом и его почтовым сервером происходит автоматическая передача поступивших сообщений на компьютер адресата. Почтовая служба основана на двух прикладных протоколах: *SMTP* и *РОР*З. По первому происходит отправка корреспонденции с компьютера на сервер, а по второму – прием поступивших сообщений. Существует большое разнообразие клиентских почтовых программ. К ним относится, например, программа *Microsoft* *Outlook* *Express*, входящая в состав операционной системы Windows как стандартная. Более мощная программа, интегрирующая в себе кроме поддержки электронной почты и другие средства делопроизводства, *Microsoft* *Outlook*, входит в состав известного пакета *Microsoft* *Office*. Из специализированных почтовых программ хорошую популярность имеют программы *The* *Bat*! и *Eudora* *Pro*.

***Списки рассылки* (*Mail list*)**. Обычная электронная почта предполагает наличие двух партнеров по переписке. Если же партнеров нет, то достаточно большой поток почтовой информации в свой адрес можно обеспечить, подписавшись на *списки рассылки*. Это специальные тематические серверы, собирающие информацию по определенным темам и переправляющие ее подписчикам в виде сообщений электронной почты. Темами списков рассылки может быть что угодно, например, научно-технические обзоры, презентация новых программных и аппаратных средств вычислительной техники и т.д. Большинство телекомпаний создают списки рассылки на своих узлах, через которые рассылают клиентам аннотированные обзоры телепрограмм. Списки рассылки позволяют эффективно решать вопросы регулярной доставки данных.

***Служба телеконференций* (*Usenet*).** Служба телеконференций похожа на циркулярную рассылку электронной почты, в ходе которой одно сообщение отправляется не одному корреспонденту, а большой группе (такие группы называются *телеконференциями* или *группами новостей).*

Обычное сообщение электронной почты пересылается по узкой цепочке серверов от отправителя к получателю. При этом не предполагается его хранение на промежуточных серверах. Сообщения, направленные на сервер группы новостей, отправляются с него на все серверы, с которыми он связан, если на них данного сообщения еще нет. Далее процесс повторяется.

На каждом из серверов поступившее сообщение хранится ограниченное время (обычно неделю), и все желающие могут в течение этого времени с ним ознакомиться. Распространяясь во все стороны, менее чем за сутки сообщения охватывают весь земной шар. Далее распространение затухает, поскольку на сервер, который уже имеет данное сообщение, повторная передача производиться не может. Ежедневно в мире создается порядка миллиона сообщений для групп новостей. Выбрать в этом массиве действительно полезную информацию практически невозможно. Поэтому вся система телеконференций разбита на тематические группы. Сегодня в мире насчитывают порядка 50 000 тематических групп новостей. Они охватывают большинство тем, интересующих массы. Особой популярностью пользуются группы, посвященные вычислительной технике. Основной прием использования групп новостей состоит в том, чтобы задать вопрос, обращаясь ко всему миру, и получить ответ или совет от тех, кто с этим вопросом уже разобрался. При этом важно следить за тем, чтобы содержание вопроса соответствовало теме данной телеконференции. Многие квалифицированные специалисты мира регулярно просматривают сообщения телеконференций, проходящие в группах, касающихся их сферы деятельности. Такой просмотр *называется мониторингом информации*. Регулярный мониторинг позволяет специалистам точно знать, что нового происходит в мире по их специальности, какие проблемы беспокоят большие массы людей и на что надо обратить особое внимание в своей работе.

В современных промышленных и проектно-конструкторских организациях считается хорошим тоном, если специалисты высшего эшелона периодически (Один-два раза в месяц) отвечают через систему телеконференций на типовые вопросы» пользователей своей продукции.

При отправке сообщений в телеконференции принято указывать свой адрес электронной почты для обратной связи. В тех случаях, когда есть угроза переполнения электронного «почтового ящика» корреспонденцией, не относящейся непосредственно к производственной деятельности, вместо основного адреса, используемого для деловой переписки, указывают дополнительный адрес. Как правило, такой адрес арендуют на сервере одной из бесплатных анонимных почтовых служб, например www.hotmail.com.

Огромный объем сообщений в группах новостей значительно затрудняет их целенаправленный мониторинг, поэтому в некоторых группах производится предварительный «отсев» бесполезной информации (в частности, рекламной), не относящейся к теме конференции. Такие конференции называют *модерируемыми*. В качестве *модератора* может выступать не только человек, но и программа, фильтрующая сообщения по определенным ключевым словам. В последнем случае говорят об *автоматической модерации*.

Для работы со службой телеконференций существуют специальные клиентские программы. Так, например, приложение *Microsoft* *Outlook* *Express*, указанное выше как почтовый клиент, позволяет работать также и со службой телеконференций. Для начала работы надо настроить программу на взаимодействие с сервером групп новостей, оформить «подписку» на определенные группы и периодически, как и электронную почту, получать все сообщения, проходящие по теме этой группы. В Данном случае слово «подписка» не предполагает со стороны клиента никаких обязательств или платежей – это просто указание серверу о том, что сообщения по указанным темам надо доставлять, а по прочим – нет. Отменить подписку или изменить ее состав можно в любой удобный момент.

***Служба WWW*.** World Wide Web («Всемирная паутина») – это *гипертекстовая* информационно-поисковая система в *Internet*. Блоки данных *WWW* («страницы») размещаются на отдельных ком­пьютерах, называемых *WWW*-*серверами* (или *Web*-серверами) и принадлежащих отдельным организациям или частным лицам. С помощью *гипертекстовых ссылок,* встроенных в до­кументы *WWW*, пользователь может переходить от одного документа к другому.

В основе WWW лежит протокол передачи гипертекстовых сообщений *HTTP* (*Hypertext Transfer Protocol*), а сами страницы форматируются с помощью специального гипертекстового языка описания документов *HTML* (*Hypertext Markup Language*).

Для работы с *WWW* используются специальные программы-клиенты, которые по-английски называются *browsers* (от глагола «*browse*» просматривать), а по-русски – браузерами, навигаторами, обозревателями. В нашей стране сейчас наиболее популярны обозреватели *Netscape Navigator* фирмы *Netscape* и *Microsoft Internet Explorer*.

*WWW* и ее программное обеспечение – это наиболее мощные и перспективные инструменты Сети. Они обеспечивают пользователям доступ практически ко всем ресурсам (*FTP*, *Gopher*, *WAIS* и др.).

*Служба имен доменов* (*DNS*). Адрес любого компьютера или любой локальной сети в Интернете может быть выражен четырьмя байтами, например,

195.28.132.97

Так как человеку неудобно работать с числовым представлением *IP*-адреса, то числовое имя может быть заменено символическим, например

www.abcdef.com

Это две разных формы записи адреса одного и того же *сетевого компьютера*. Кроме того, в символический адрес вкладывается некий смысл, например адрес www.microsoft.com является адресом Web-сервера компании *Microsoft*.

С другой стороны, автоматическая работа серверов сети организована с использованием четырехзначного числового адреса. Благодаря ему промежуточные серверы могут осуществлять передачу запросов и ответов в нужном направлении, не зная где конкретно находятся отправитель и получатель. Поэтому необходим перевод доменных имен в связанные с ними *IР*-адреса. Этим и занимаются серверы службы имен доменов *DNS*. Наш запрос на получение одной из страниц сервера www.abcdef.com сначала обрабатывается сервером *DNS*,и далее он направляется по *IP*-адресу, а не по доменному имени.

***Служба передачи файлов* (*FTP*)**. Прием и передача файлов составляют значительный процент от прочих Интернет-услуг. Необходимость в передаче файлов возникает, например, при приеме файлов программ, при пересылке крупных документов (например, книг), а также при передаче архивных файлов, в которых запакованы большие объемы информации.

Служба *FTP* имеет свои серверы в мировой сети, на которых хранятся архивы данных. Со стороны клиента для работы с серверами *FTP* может быть установлено специальное программное обеспечение, хотя в большинстве случаев браузеры *www* обладают встроенными возможностями для работы и по протоколу *FTP.* Протокол *FTP* работает одновременно с двумя *TCP*-соединениями между сервером и клиентом. По одному соединению идет передача данных, а второе соединение используется как управляющее. Протокол *FTP* также предоставляет серверу средства для идентификации обратившегося клиента. Этим часто пользуются коммерческие серверы и серверы ограниченного доступа, поставляющие информацию только зарегистрированным клиентам – они выдают запрос на ввод имени пользователя и связанного с ним пароля. Однако существуют и десятки тысяч *FTP*-серверов с *анонимным доступом* для всех желающих. В этом случае в качестве имени пользователя надо ввести слово: *anonymous*, а в качестве пароля задать адрес электронной почты. В большинстве случаев программы-клиенты *FTP* делают это автоматически.

***IRC*.** Служба *IRC* (*Internet Relay Chat*) предназначена для прямого общения нескольких человек в режиме реального времени. Иногда службу *IRC* называют *чат-конференциями* или просто *чатом.* В отличие от системы телеконференций, в которой общение между участниками обсуждения темы открыто всему миру, в системе *IRС* общение происходит только в пределах одного *канала*, в работе которого принимают участие обычно лишь несколько человек. Каждый пользователь может создать собственный канал и пригласить в него участников «беседы» или присоединиться одному из открытых в данный момент каналов.

Существует несколько популярных клиентских программ для работы с сервер и сетями, поддерживающими сервис *IRC.* Одна из наиболее популярных – грамма mlRC.exe.

***ICQ*.** Эта служба предназначена для поиска сетевого *IP-адреса* человека, подключенного в данный момент к Интернету. Необходимость в подобной услуге связана с тем что большинство пользователей не имеют постоянного *IP-адреса*. Для пользования этой службой надо зарегистрироваться на ее центральном сервере (http://www.icq.com) и получить персональный идентификационный номер *UIN (Universal Internet Number).* Данный номер можно сообщить партнерам по контактам, и тогда служб *ICQ* приобретает характер *Интернет-пейджера.* Зная номер *UIN* партнера, но не зная его текущий *IР*-адрес, можно через центральный сервер службы отправить ему сообщение с предложением установить соединение.

Как было указано выше, каждый компьютер, подключенный к Интернету, должен иметь четырехзначный *IР*-адрес. Этот адрес может быть *постоянным* или *динамическим* временным. Те компьютеры, которые включены в Интернет на постоянной основе, имеют постоянные *IP-адреса.* Большинство же пользователей подключаются к Интернету лишь на время сеанса. Им выдается динамический *IР*-адрес, действующий только в течение данного сеанса. Этот адрес выдает тот сервер, через который происходит подключение. В разных сеансах динамический *IР*-адрес может быть различным, причем заранее неизвестно каким.

При каждом подключении к Интернету программа *ICQ* установленная на нашем компьютере, определяет текущий *IР*-адрес и сообщает его центральной службе, которая, в свою очередь, оповещает наших партнеров по контактам. Далее партнеры (если они тоже являются клиентами данной службы) могут установить с нами прямую связь. Программа предоставляет возможность выбора режима связи («готов к контакту»; «прошу не беспокоить, но готов принять срочное сообщение»»; «закрыт для контакта» и т. п.). После установления контакта связь происходит в режиме, аналогичном сервису *IRC*.

**БЕСПРОВОДНЫЕ КОМПЬЮТЕРНЫЕ СЕТИ**

**Введение**

Беспроводные сети широко распространены в западных странах. Там они, как правило, применяются как корпоративные сети внутри зданий, на территории промышленного предприятия, а так же для связи удаленных отделений между собой.

В России большинство беспроводных сетей работает вне зданий, обеспечивая услугами скоростной передачи данных пользователей, разбросанных на расстоянии в несколько километров и даже десятков километров. Беспроводная локальная сеть зачастую является единственным экономически оправданным решением – когда кабельная система отсутствует или низкого качества.

Средства и системы беспроводной связи используются в сетях, включающих также и проводные (кабельные) средства, и дают возможность удобно, быстро и экономично решить проблемы, возникающие в процессе решения и модернизации чисто кабельных сетей. Беспроводные средства связи следует считать не полной альтернативой кабельным сетям, а лишь альтернативной технологией для реализации отдельных сегментов (или целых уровней) в проектируемой, расширяемой или модернизируемой локальной компьютерной сети.

**Что такое беспроводные вычислительные сети**

Беспроводные компьютерные сети – это технология, позволяющая создавать вычислительные сети, полностью соответствующие стандартам для обычных проводных сетей (например, Ethernet), без использования кабельной проводки. В качестве носителя информации в таких сетях выступают радиоволны СВЧ-диапазона.

Сеть, развернутая в соответствии со стандартом “RadioEthernet”, представляет собой аналог обычной кабельной сети Ethernet с коллизионным механизмом доступа к среде передачи данных. Разница состоит только в характере этой среды. Radio Ethernet полностью обеспечивает все потребности беспроводной передачи данных внутри помещений.

При наружном применении RadioEthernet очень удобно использовать сети на “последней миле” взамен кабельной, то есть – для соединения между абонентом и ближайшим узлом опорной сети. При этом реальная протяженность “последней мили” может быть от нескольких сотен метров до 20÷30 км и ограничена лишь наличием прямой видимости.

Беспроводные сети можно развертывать без разрешения Связьнадзора на использование частот, достаточно просто зарегистрировать такую сеть.

Беспроводная одноранговая локальная сеть предназначена для быстрого развертывания временных сетей на выставках, в процессе проведения различных семинаров и совещаний, а также в офисах малых компаний. Все компьютеры сети оснащаются беспроводными сетевыми адаптерами (внешними с интерфейсом USB, или внутренними с интерфейсом PCI), работающими в диапазоне 2,4 ГГц в соответствии со стандартом IEEE 802.11.

 Сеть проста в установке и работоспособна сразу после инсталляции драйверов. Дальность действия – от 30 до нескольких сот метров. Максимальная скорость передачи данных – 54 Мбит/сек. Сеть поддерживает мобильность абонентов в пределах зоны действия сети, а также защиту канала в соответствии с алгоритмом WEP (Wired Equivalent Privacy).

Если развертываемая сеть достаточно крупная, то оптимальным решением в этих ситуациях является развертывание многосотовой беспроводной сети инфраструктурной топологии.

 Сеть состоит из нескольких беспроводных сот, в центре которых находятся точки доступа, объединенные единственным проводным каналом. Такая сеть обеспечивает наивысшую производительность, свободное перемещение пользователей в пределах зон радиовидимости точек доступа и обеспечивает безопасность на уровне проводных каналов.

**Защита беспроводных сетей**

Вообще говоря, соответствующие стандарту IEEE 802.11 продукты для беспроводных сетей предлагают четыре уровня средств безопасности: физический, идентификатор набора служб (SSID – Service Set Identifier), идентификатор управления доступом к среде (MAC ID – Media Access Control ID) и шифрование.

 Поток требующих передачи данных "разворачивается" по каналу шириной 20 МГц с помощью схемы ключей дополнительного кода (Complementary Code Keying, CCK). Для декодирования принятых данных получатель должен установить правильный частотный канал и использовать ту же самую схему CCK. Таким образом, технология обеспечивает первую линию обороны от нежелательного доступа к передаваемым данным –практически все подслушивающие устройства будут отфильтровыватся.

 Идентификатор SSID позволяет различать отдельные беспроводные сети, которые могут действовать в одном и том же месте или области. Он представляет собой уникальное имя сети, включаемое в заголовок пакетов данных и управления IEEE 802.11. Беспроводные клиенты и точки доступа используют его, чтобы проводить фильтрацию и принимать только те запросы, которые относятся к их сети. Таким образом, пользователь не сможет обратиться к точке доступа, если только ему не предоставлен правильный номер сети.

 Возможность принятия или отклонения запроса к сети может зависеть также от значения идентификатора. MAC ID – это уникальное число, присваиваемое в процессе производства каждой сетевой карте. Когда клиентский ПК пытается получить доступ к беспроводной сети, точка доступа должна сначала проверить адрес MAC для клиента. Точно так же и клиентский ПК должен знать имя точки доступа.

 Механизм Wired Equivalency Privacy (WEP), определенный в стандарте IEEE 802.11, обеспечивает еще один уровень безопасности. Он опирается на алгоритм шифрования RC4 компании RSA Data Security с 40- или 128-разрядными ключами. Использование WEP несколько снижает пропускную способност сети. Дополнительные функции WEP затрагивают процессы сетевой аутентификации и шифрования данных. Процесс аутентификации с разделяемым ключом для получения доступа к беспроводной сети использует 64-разрядный ключ – 40-разрядный ключ WEP выступает как секретный, а 24-разрядный вектор инициализации (Initialization Vector) – как разделяемый. Если конфигурация точки доступа позволяет принимать только обращения с разделяемым ключом, она будет направлять клиенту случайную строку вызова длиной 128 октетов. Клиент должен зашифровать строку вызова и вернуть зашифрованное значение точке доступа. Далее точка доступа расшифровывает полученную от клиента строку и сравнивает ее с исходной строкой вызова. Наконец, право клиента на доступ к сети определяется в зависимости от того, прошел ли он проверку шифрованием. Процесс расшифровки данных, закодированных с помощью WEP, заключается в выполнении логической операции "исключающее ИЛИ" (XOR) над ключевым потоком и принятой информацией. Процесс аутентификации с разделяемым ключом не допускает передачи реального 40-разрядного ключа WEP, поэтому этот ключ практически нельзя получить путем контроля за сетевым трафиком. Ключ WEP рекомендуется периодически менять, чтобы гарантировать целостность системы безопасности.

 Еще одно преимущество беспроводной сети связано с тем, что физические характеристики сети делают ее локализованной. В результате дальность действия сети ограничивается лишь определенной зоной покрытия. Для подслушивания потенциальный злоумышленник должен будет находиться в непосредственной физической близости, а значит, привлекать к себе внимание. В этом преимущество беспроводных сетей с точки зрения безопасности. Беспроводные сети имеют также уникальную особенность: их можно отключить или модифицировать их параметры, если безопасность зоны вызывает сомнения.

 Благодаря средствам аутентификации и шифрования данных WEP злоумышленнику почти невозможно получить доступ к сети или перехватить передаваемые данные. В сочетании с мерами безопасности на сетевом уровне протокола (подключение к сети, парольный доступ и т.д.), а также функциями безопасности тех или иных конкретных приложений (шифрование, парольный доступ и т.д.) средства безопасности продуктов беспроводной связи открывают путь к безопасной сети.

**Несанкционированное вторжение в сеть**

Для вторжения в сеть необходимо к ней подключиться. В случае проводной сети требуется электрическое соединение, беспроводной – достаточно оказаться в зоне радиовидимости сети с оборудованием того же типа, на котором построена сеть.

 В проводных сетях основное средство защиты на физическом и MAC-уровнях – административный контроль доступа к оборудованию, недопущение злоумышленника к кабельной сети. В сетях, построенных на управляемых коммутаторах, доступ может дополнительно ограничиваться по MAC-адресам сетевых устройств.

 В беспроводных сетях для снижения вероятности несанкционированного доступа предусмотрен контроль доступа по MAC-адресам устройств и тот же самый WEP. Поскольку контроль доступа реализуется с помощью точки доступа, он возможен только при инфраструктурной топологии сети. Механизм контроля подразумевает заблаговременное составление таблицы MAC-адресов разрешенных пользователей в точке доступа и обеспечивает передачу только между зарегистрированными беспроводными адаптерами. В одноранговых беспроводных сетях контроль доступа на уровне радиосети не предусмотрен.

**Технические особенности беспроводных сетей**

Базовый стандарт 802.11 ориентирован на работу в диапазоне частот 2,4 ГГц. Здесь используется три типа протоколов физического уровня, соответствующим трем технологиям передачи сигналов (инфракрасное излучение, с помощью прямого расширения спектра и с использованием скачкообразной перестройки частоты). Передача данных возможна на скоростях 1 и 2 Мбит/с.

В стандарте 802.11 определена сотовая архитектура системы. Каждая сота управляется базовой станцией, называемой точкой доступа (Access Point, AP), которая обслуживает рабочие станции пользователей в пределах своего радиуса действия, образуя базовую зону обслуживания (Basic Service Set, BSS). Точки доступа многосотовой сети взаимодействуют между собой через распределительную систему (Distribution System, DS). Инфраструктура, включающая AP и DS, образует расширенную зону обслуживания (Extended Service Set, ESS). Стандарт предусматривает построение односотовой сети даже без точки доступа, отдельные функции которой выполняются в этом случае рабочими станциями. Оборудование для беспроводных сетей, ориентированное на диапазон частот 2,4 ГГц, способно обеспечить связь на расстоянии до 300 м. Допускаются любые варианты топологии сети: точка – точка, звезда, точка – много точек, каждый с каждым. Мобильность рабочих станций достигается за счет использования специальных процедур сканирования радиоканала и присоединения абонентов.

Наиболее "широкополосный" стандарт из семейства Radio Ethernet – это 802.11a, последняя редакция которого была утверждена в 1999 году. Предельная для него скорость передачи данных – 54 Mбит/с (в спецификациях определены три обязательные скорости - 6, 12 и 24 Mбит/с, а также пять необязательных – 9, 18, 36, 48 и 54 Mбит/с). Данный стандарт предусматривает работу в диапазоне 5 ГГц, возможность передавать полезные сигналы параллельно на нескольких частотах диапазона, что существенно повышает пропускную способность канала. Для оборудования, использующего диапазон частот 5 ГГц, характерна более высокая (чем для области 2,4 ГГц) потребляемая мощность передатчиков и меньший радиус действия – около 100 м.

 Стандарт 802.11b (его окончательная редакция, принятая в 1999 году, известна как Wi-Fi – Wireless Fidelity) ориентирован на радиочастотный диапазон 2,4 ГГц и по пропускной способности до 11 Мбит/с практически соответствует проводному Ethernet-каналу. Стандарт предусматривает автоматическое понижение скорости передачи информации при ухудшении качества сигнала.

 Не так давно официально принята новая версия стандарта – 802.11g, которая в итоге должна заменить 802.11b. Она работает в том же частотном диапазоне, что и предшественница (2,4 ГГц), но в пять раз быстрее (54 Мбит/с) и, разумеется, имеет обратную совместимость. С практической точки зрения это означает, что, если устройство с поддержкой 802.11g находит точку доступа 802.11b, оно автоматически переключается на работу в этом стандарте. Аналогично с точкой доступа стандарта 802.11g могут работать устройства, оснащенные поддержкой 802.11b.

**Способы построение беспроводных сетей**

Самым простым способом объединения рабочих мест в беспроводную сеть – это способ "каждый с каждым" (ad-hoc). В каждый компьютер устанавливается Network Adapter и обеспечиваются условия прямой радиовидимости с соседними точками. Данный способ может быть применён для быстрого развертывания сети на ограниченных территориях, где проводные сети по техническим причинам развернуть нельзя.

 Другим методом является объединение рабочих мест с использованием единых точек доступа. В системе может существовать несколько базовых станций и ретрансляторов, позволяющих увеличить радиус действия сети. Беспроводные абоненты могут быть подключены к любой базовой станции или ретранслятору.

 Инфраструктура позволяет строить территориально-распределенные сети на значительных расстояниях и выполнять соединения типа компьютер-компьютер, компьютер - ЛВС, ЛВС-ЛВС.

Как правило, базовая станция оператора подключена к сети Интернет. Таким образом, на каждом рабочем месте, имеющем доступ в беспроводную сеть, имеется возможность доступа к Всемирной сети. Аналогично может быть выполнено подключение к другим сетям и каналам связи операторов связи, действующих в регионе и России в целом.

Различают два базовых варианта построения беспроводных сетей – в пределах одного здания и между зданиями. В пределах одного здания максимальная дальность зависит от материала стен и перекрытий и составляет от 25 до 500 метров с использованием встроенной в сетевые карты антенны. Дальность связи в помещениях может быть увеличена путем применения комнатных всенаправленных и направленных антенн. При соединении компьютеров, расположенных в разных зданиях используются внешние антенны, устанавливаемые обычно за окном или на крыше. При применении направленных внешних антенн с высоким коэффициентом усиления дальность связи при наличии прямой видимости составляет 15÷20 км. Применение дополнительных усилителей позволяет получить устойчивую высококачественную связь на расстояниях 50 и более километров.

 Логическое построение беспроводных сетей осуществляется по двум схемам: точка-много точек и точка-точка. При построении системы "точка-много точек" существует так называемая базовая станция (точка доступа), имеющая выход в магистральный канал передачи данных (например, доступ к глобальной сети Internet) и набор абонентских станций, каждая из которых является шлюзом доступа для своей локальной сети.

При работе по схеме точка-точка каждая абонентская станция работает в жесткой паре с другой.

Коммутация пакетов осуществляется под управлением стека IP, протоколом доступа к сети является Ethernet-подобный протокол, а средой передачи – радиоканал. В нашей стране радиоканал обычно организуется на частотах диапазона 2.4 ГГц, разрешенных для передачи данных.