МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ
БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ
«САМАРСКИЙ ГОСУДАРСТВЕННЫЙ АЭРОКОСМИЧЕСКИЙ
УНИВЕРСИТЕТ ИМЕНИ АКАДЕМИКА С.П. КОРОЛЕВА
(НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ)» (СГАУ)

Безопасность сетей ЭВМ

Электронный учебно-методический комплекс

САМАРА
2012

УДК 004.7, 004.056

Автор-составитель: **Кузнецов Михаил Владимирович**

Безопасность сетей ЭВМ [Электронный ресурс] : электрон. Учеб.-метод. комплекс по дисциплине в LMS Moodle / Минобрнауки России, Самар. Гос. аэрокосм. Ун-т им. С. П. Королева (нац. исслед. ун-т); авт.-сост. М. В. Кузнецов. - Электрон. текстовые и граф. дан. - Самара, 2012. – 1 эл. опт. диск (CD-ROM).

В состав учебно-методического комплекса входят:
1. Учебное пособие «Курс лекций».
2. Темы для подготовки к экзамену
3. Рабочая программа.

УМДК «Безопасность сетей ЭВМ» предназначен для студентов факультета информатики, обучающихся по специальности 090303.65 «Информационная безопасность автоматизированных систем», в 7 семестре.

УМДК разработан на кафедре Геоинформатики и информационной безопасности.

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение
высшего профессионального образования
«Самарский государственный аэрокосмический университет
имени академика С.П. Королёва (национальный исследовательский
университет)» (СГАУ)

Факультет информатики
Кафедра геоинформатики и информационной безопасности

Кузнецов М.В.

Курс лекций «БЕЗОПАСНОСТЬ СЕТЕЙ ЭВМ»

Учебное пособие

для студентов, обучающихся по специальности
090303.65 «Информационная безопасность
автоматизированных систем»

Самара 2012

Содержание

Безопасность сетей ЭВМ

Раздел 1. ПРИНЦИПЫ ПОСТРОЕНИЯ ВЫЧИСЛИТЕЛЬНЫХ СЕТЕЙ

1.1. Классификация вычислительных сетей

Все многообразие компьютерных сетей можно классифицировать по группе признаков:

1.1.1. По территориальной распространенности сети могут быть:

- *Персональные* (*PAN*) – расположены в пределах одного помещения;
- *Локальные* (*LAN*) – расположены в пределах одного здания или кампуса.
  Городские (*MAN*) – расположены на территории города.
- *Региональные (RAN)* – расположены на территории области.
  Глобальные (*WAN*) – расположены на территории государства или группы государств, например, всемирная сеть Internet.

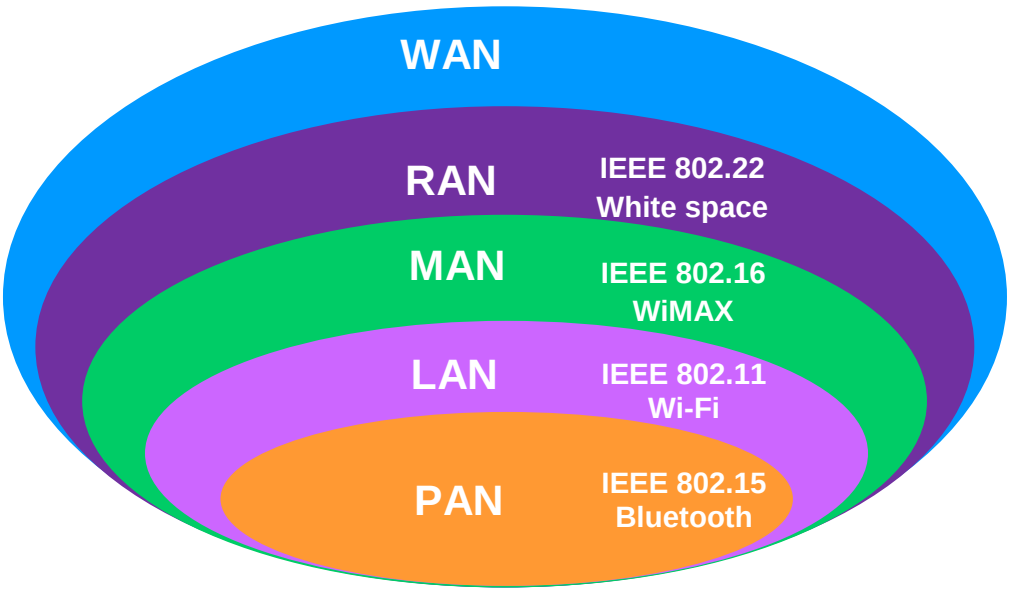


Рис. 1.1 Классификация беспроводных сетей и технологий по территориальному охвату.

Термин "корпоративная сеть" также используется в литературе для обозначения объединения нескольких сетей, каждая из которых может быть построена на различных технических, программных и информационных принципах.

Локальные и персональные сети являются сетями закрытого типа, доступ к ним разрешен только ограниченному кругу пользователей, для которых работа в такой сети непосредственно связана с их профессиональной деятельностью. Глобальные и региональные сети являются открытыми и ориентированы на обслуживание любых пользователей.

1.1.2. Ведомственная принадлежность

По принадлежности различают *ведомственные* и *государственные сети*. Ведомственные принадлежат одной организации и располагаются на ее территории. Государственные сети - сети, используемые в государственных структурах.

1.1.3. По скорости передачи

По скорости передачи информации компьютерные сети делятся на:

- низкоскоростные (до 10 Мбит/с),
- среднескоростные (до 100 Мбит/с),
- высокоскоростные (свыше 100 Мбит/с);

1.1.4. По типу среды передачи

По типу среды передачи сети разделяются на:

- проводные – на витой паре, коаксиальные, оптоволоконные;
- беспроводные - с передачей информации по радиоканалам, в инфракрасном диапазоне.

1.1.5. По способу коммутации компьютеров

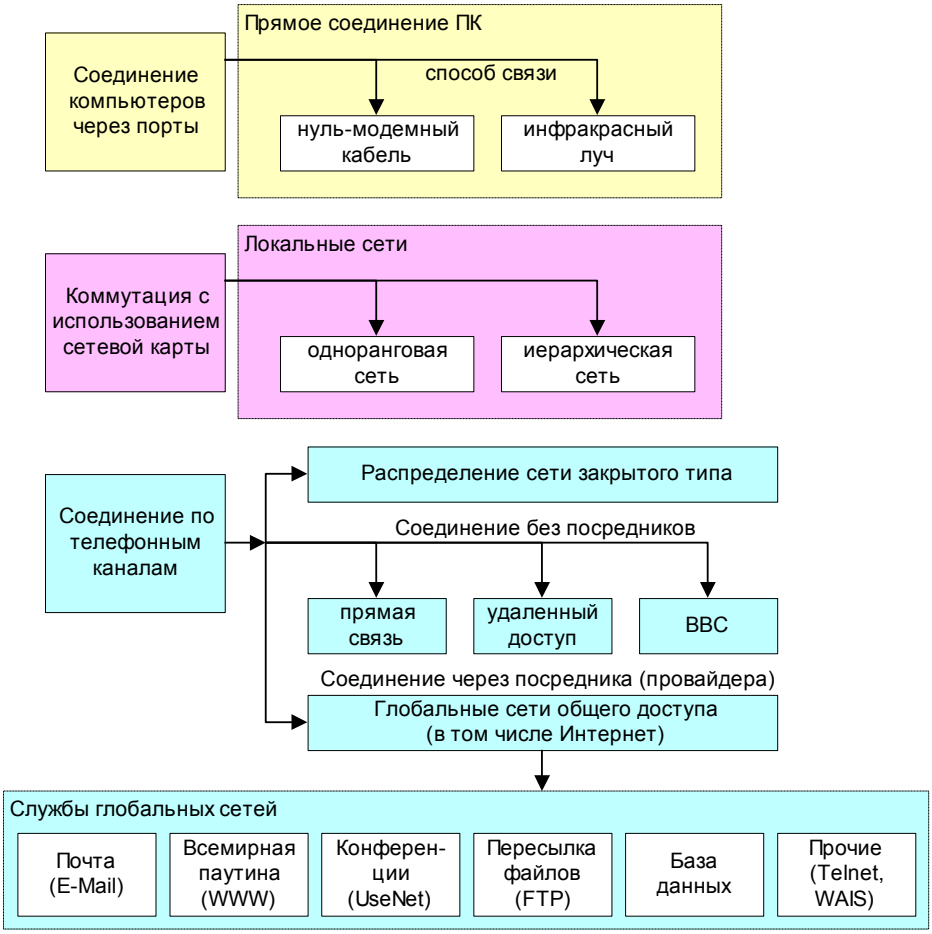


Рисунок 1.2 - Способы коммутации компьютеров и виды сетей.

1.1.6. Одноранговые и иерархические сети

С точки зрения организации взаимодействия компьютеров, сети делят на одноранговые (пиринговые) и с выделенным сервером (иерархические).

1.1.6.1. Одноранговые сети

Все компьютеры одноранговой сети равноправны. Любой пользователь сети может получить доступ к данным, хранящимся на любом компьютере.

Достоинства одноранговых сетей:

- Наиболее просты в установке и эксплуатации.
- Распространённые операционные системы обладают всеми необходимыми функциями, позволяющими строить одноранговую сеть.

Недостатки:

- В условиях одноранговых сетей затруднено решение вопросов защиты информации. Поэтому такой способ организации сети используется для сетей с небольшим количеством компьютеров и там, где вопрос защиты данных не является принципиальным.

1.1.6.2. Иерархические сети

В иерархической сети при установке сети заранее выделяются один или несколько компьютеров, управляющих обменом данных по сети и распределением ресурсов. Такой компьютер называют сервером.

Любой компьютер, имеющий доступ к услугам сервера называют клиентом сети или рабочей станцией.

Сервер в иерархических сетях - это постоянное хранилище разделяемых ресурсов. Сам сервер может быть клиентом только сервера более высокого уровня иерархии. Поэтому иерархические сети иногда называются сетями с выделенным сервером.

Серверы обычно представляют собой высокопроизводительные компьютеры, возможно, с несколькими параллельно работающими процессорами, с винчестерами большой емкости, с высокоскоростной сетевой картой (100 Мбит/с и более).

Иерархическая модель сети является наиболее предпочтительной, так как позволяет создать наиболее устойчивую структуру сети и более рационально распределить ресурсы. Также достоинством иерархической сети является более высокий уровень защиты данных.

К недостаткам иерархической сети, по сравнению с одноранговыми сетями, относятся:

- Необходимость дополнительной ОС для сервера.
- Более высокая сложность установки и модернизации сети.
- Необходимость выделения отдельного компьютера в качестве сервера

Различают две технологии использования сервера: технологию *файл-сервера* и архитектуру *клиент-сервер*.

В первой модели используется файловый сервер, на котором хранится большинство программ и данных. По требованию пользователя ему пересылаются необходимая программа и данные. Обработка информации выполняется на рабочей станции.

В системах с архитектурой клиент-сервер обмен данными осуществляется между приложением-клиентом и приложением-сервером. Хранение данных и их обработка производится на мощном сервере, который выполняет также контроль за доступом к ресурсам и данным. Рабочая станция получает только результаты запроса. Разработчики приложений по обработке информации обычно используют эту технологию.

1.2. Распределенные вычислительные системы

Компьютерные сети относятся к распределенным (или децентрализованным) вычислительным системам. Поскольку основным признаком распределенной вычислительной системы является наличие нескольких центров обработки данных, то наряду с компьютерными сетями к распределенным системам относят также мультипроцессорные компьютеры и многомашинные вычислительные комплексы.

1.2.1. Мультипроцессорные компьютеры.

В мультипроцессорных компьютерах имеется несколько процессоров, каждый из которых может относительно независимо от остальных выполнять свою программу. В мультипроцессоре существует общая для всех процессоров операционная система, которая оперативно распределяет вычислительную нагрузку между процессорами. Взаимодействие между отдельными процессорами организуется наиболее простым способом - через общую оперативную память.

Основное достоинство мультипроцессора - его высокая производительность, которая достигается за счет параллельной работы нескольких процессоров. Так как при наличии общей памяти взаимодействие процессоров происходит очень быстро, мультипроцессоры могут эффективно выполнять даже приложения с высокой степенью связи по данным.

Важным свойством мультипроцессорных систем является отказоустойчивость, то есть способность к продолжению работы при отказах некоторых элементов, например процессоров или блоков памяти. При этом производительность, естественно, снижается, но не до нуля, как в обычных системах, в которых отсутствует избыточность.

1.2.2. Многомашинные системы.

Многомашинная система - это вычислительный комплекс, включающий в себя несколько компьютеров (каждый из которых работает под управлением собственной операционной системы), а также программные и аппаратные

средства связи компьютеров, которые обеспечивают работу всех компьютеров комплекса как единого целого.

Работа любой многомашинной системы определяется двумя главными компонентами: высокоскоростным механизмом связи процессоров и системным программным обеспечением, которое предоставляет пользователям и приложениям прозрачный доступ к ресурсам всех компьютеров, входящих в комплекс. В состав средств связи входят программные модули, которые занимаются распределением вычислительной нагрузки, синхронизацией вычислений и реконфигурацией системы. Если происходит отказ одного из компьютеров комплекса, его задачи могут быть автоматически переназначены и выполнены на другом компьютере. Если в состав многомашинной системы входят несколько контроллеров внешних устройств, то в случае отказа одного из них, другие контроллеры автоматически подхватывают его работу. Таким образом, достигается высокая отказоустойчивость комплекса в целом.

Многомашинные системы позволяют достичь высокой производительности за счет организации параллельных вычислений. По сравнению с мультипроцессорными системами возможности параллельной обработки в многомашинных системах ограничены: эффективность распараллеливания резко снижается, если параллельно выполняемые задачи тесно связаны между собой по данным. Это объясняется тем, что связь между компьютерами многомашинной системы менее тесная, *чем между процессорами в мультипроцессорной системе*, так как основной обмен данными осуществляется через общие многовходовые периферийные устройства. В отличие от мультипроцессоров, где используются сильные программные и аппаратные связи, в многомашинных системах аппаратные и программные связи между обрабатывающими устройствами являются более слабыми. Территориальная распределенность в многомашинных комплексах не обеспечивается, так как расстояния между компьютерами определяются длиной связи между процессорным блоком и дисковой подсистемой.

1.2.3. Вычислительные сети

В вычислительных сетях программные и аппаратные связи являются еще более слабыми, а автономность обрабатывающих блоков проявляется в наибольшей степени - основными элементами сети являются стандартные компьютеры, не имеющие ни общих блоков памяти, ни общих периферийных устройств. Связь между компьютерами осуществляется с помощью специальных сетевых адаптеров, соединенных относительно протяженными каналами связи. Каждый компьютер работает под управлением собственной операционной системы, а какая-либо «общая» операционная система, распределяющая работу между компьютерами сети, отсутствует. Взаимодействие между компьютерами сети происходит за счет передачи сообщений через сетевые адаптеры и каналы связи. С помощью этих сообщений один компьютер обычно запрашивает доступ к локальным ресурсам другого компьютера. Такими ресурсами могут быть как данные, хранящиеся на

диске, так и разнообразные периферийные устройства - принтеры, модемы, сканеры и т. д. Основная цель создания вычислительной сети - разделение локальных ресурсов каждого компьютера между всеми пользователями сети.

На тех компьютерах, ресурсы которых должны быть доступны всем пользователям сети, необходимо добавить модули, которые постоянно будут находиться в режиме ожидания запросов, поступающих по сети от других компьютеров. Обычно такие модули называются программными серверами, так как их главная задача - обслуживать запросы на доступ к ресурсам своего компьютера. На компьютерах, пользователи которых хотят получать доступ к ресурсам других компьютеров, также нужно добавить к операционной системе некоторые специальные программные модули, которые должны вырабатывать запросы на доступ к удаленным ресурсам и передавать их по сети на нужный компьютер. Такие модули обычно называют программными клиентами. Собственно же сетевые адаптеры и каналы связи решают в сети достаточно простую задачу - они передают сообщения с запросами и ответами от одного компьютера к другому, а основную работу по организации совместного использования ресурсов выполняют клиентские и серверные части операционных систем.

Пара модулей «клиент-сервер» обеспечивает совместный доступ пользователей к определенному типу ресурсов, например к файлам. Обычно сетевая операционная система поддерживает несколько видов сетевых служб для своих пользователей - файловую службу, службу печати, службу электронной почты, службу удаленного доступа и т. п.

Термины «клиент» и «сервер» используются не только для обозначения программных модулей, но и компьютеров, подключенных к сети. Если компьютер предоставляет свои ресурсы другим компьютерам сети, то он называется сервером, а если он их потребляет - клиентом. Иногда один и тот же компьютер может одновременно играть роли и сервера, и клиента.

1.2.4. Распределенные программы.

Сетевые службы всегда представляют собой распределенные программы. Распределенная программа - это программа, которая состоит из нескольких взаимодействующих частей (в приведенном на рис.1.3 примере - из двух), причем каждая часть, как правило, выполняется на отдельном компьютере сети.

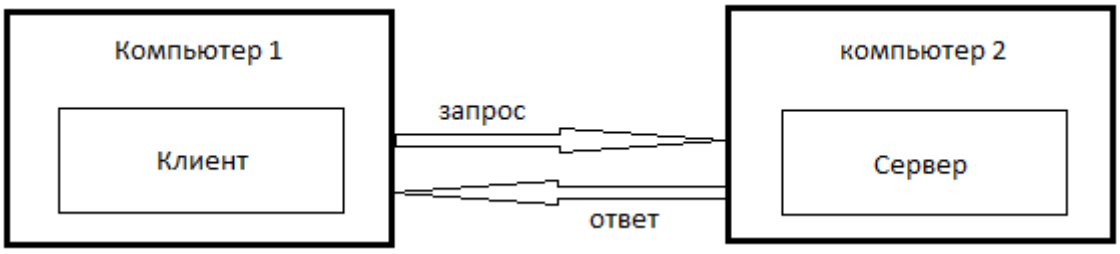


Рис. 1.3 Взаимодействие частей распределенного приложения

В сети могут выполняться и распределенные пользовательские программы - приложения. Распределенное приложение также состоит из нескольких частей, каждая из которых выполняет какую-то определенную законченную работу по решению прикладной задачи. Например, одна часть приложения, выполняющаяся на компьютере пользователя, может поддерживать специализированный графический интерфейс вторая - работать на мощном выделенном компьютере и заниматься статистической обработкой введенных пользователем данных, а третья - заносить полученные результаты в базу данных на компьютере с установленной стандартной СУБД. Распределенные приложения в полной мере используют потенциальные возможности распределенной обработки, предоставляемые вычислительной сетью, и поэтому часто называются сетевыми приложениями.

Следует подчеркнуть, что не всякое приложение, выполняемое в сети, является сетевым. Существует большое количество популярных приложений, которые не являются распределенными и целиком выполняются на одном компьютере сети. Такие приложения могут использовать преимущества сети за счет встроенных в операционную систему сетевых служб.

1.2.5. Прозрачность

Прозрачностью называется возможность доступа к ресурсам или услугам, не зная их местонахождения. Различают несколько разновидностей прозрачности, в частности:

- прозрачность доступа: к локальным или удаленным объектам можно обращаться посредством одинаковых операций;
- прозрачность местонахождения: объекты должны быть доступны без необходимости знать их физическое местоположение;
- прозрачность одновременности доступа: несколько пользователей должны иметь возможность одновременного доступа к данным, без нежелательных последствий;
- прозрачность копирования: должна существовать возможность копировать данные из файлов или из других объектов в целях повышения эффективности или обеспечения доступности незаметно для пользователей;
- прозрачность при неисправностях: пользователи или прикладные программы должны иметь возможность завершить свои задания, даже в случае неисправностей аппаратной или программной части;
- прозрачность при динамических изменениях конфигурации: система может динамически менять свою конфигурацию, в целях повышения эффективности и в зависимости от нагрузки.

С точки зрения прикладного программиста, речь идет о возможности использования одинаковых примитивов доступа, независимо от местонахождения службы или необходимого ресурса. У пользователя имеется только один прикладной интерфейс и он видит перед собой только один

компьютер. С более концептуальной точки зрения, прозрачность определяется как возможность видеть систему как единый организм, а не как собрание независимых друг от друга объектов.

1.3. Топологии компьютерных сетей

Вычислительные сети состоят из *узлов и ветвей сети. Узел* представляет собой компьютер, сетевой принтер или коммутирующее устройство. *Ветвь сети* - это путь, соединяющий два смежных узла.

Узлы сети бывают трёх типов:

- оконечный узел - расположен в конце только одной ветви;
- промежуточный узел - расположен внутри одной ветви;
- смежный узел - соседний узел соединённый одним путём, не содержащим никаких других узлов.

Способ соединения компьютеров в сеть называется её **топологией**. Различают топологии: «Общая шина», «Звезда», «Кольцо», «Древовидную», «Сетевую» и «Комбинированную».

1.3.1. Топология Шина (bus) — все компьютеры параллельно подключаются к одной линии связи. Информация от каждого компьютера одновременно передается всем остальным компьютерам (рис. 1.4)

Рисунок 1.4 Топология «общая шина»

Шина самой своей структурой предполагает идентичность сетевого оборудования компьютеров, а также равноправие всех абонентов по доступу к сети. Компьютеры в шине могут передавать только по очереди, так как линия связи в данном случае единственная. Если несколько компьютеров будут передавать информацию одновременно, она исказится в результате наложения (**коллизии**). В шине всегда реализуется режим **полудуплексного** (half duplex) обмена (в обоих направлениях, но по очереди, а не одновременно).

В топологии шина отсутствует явно выраженный центральный абонент, через который передается вся информация, это увеличивает ее надежность. Добавление новых абонентов в шину довольно просто и возможно даже во время работы сети. В большинстве случаев при использовании шины требуется минимальное количество соединительного кабеля по сравнению с другими топологиями.

Важное преимущество шины состоит в том, что при отказе любого из компьютеров сети, исправные машины смогут нормально продолжать обмен.

Рисунок 1.5 Обрыв кабеля в сети с топологией шина

Из-за особенностей распространения электрических сигналов по длинным линиям связи необходимо предусматривать включение на концах шины специальных согласующих устройств, **терминаторов**, показанных на рис.1.5 в виде прямоугольников. Без включения терминаторов сигнал отражается от конца линии и искажается так, что связь по сети становится невозможной. В случае разрыва или повреждения кабеля нарушается согласование линии связи, и прекращается обмен даже между теми компьютерами, которые остались соединенными между собой. Короткое замыкание в любой точке кабеля шины выводит из строя всю сеть.

Отказ сетевого оборудования любого абонента в шине может вывести из строя всю сеть. К тому же такой отказ довольно трудно локализовать, поскольку все абоненты включены параллельно, и понять, какой из них вышел из строя, невозможно.

При прохождении по линии связи сети с топологией шина информационные сигналы ослабляются и никак не восстанавливаются, что накладывает жесткие ограничения на суммарную длину линий связи. Для увеличения длины сети с топологией шина часто используют несколько **сегментов** (частей сети, каждый из которых представляет собой шину), соединенных между собой с помощью специальных усилителей и восстановителей сигналов — **репитеров** или **повторителей** (рис. 1.6).

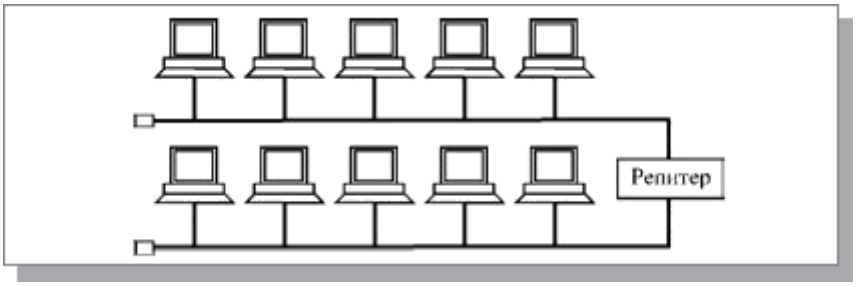


Рисунок 1.6 Соединение сегментов сети типа шина с помощью репитера

1.3.2. Топология звезда — это единственная топология сети с явно выделенным центром, к которому подключаются все остальные абоненты. Обмен информацией идет исключительно через центральный компьютер, на который ложится большая нагрузка, поэтому ничем другим, кроме сети, он, заниматься не может. Сетевое оборудование центрального абонента должно быть существенно более сложным, чем оборудование периферийных абонентов. Обычно центральный компьютер самый мощный, именно на него возлагаются все функции по управлению обменом. Никакие конфликты в сети с

топологией звезда в принципе невозможны, так как управление полностью централизовано.

Выход из строя периферийного компьютера или его сетевого оборудования никак не отражается на функционировании оставшейся части сети, зато любой отказ центрального компьютера делает сеть полностью неработоспособной. Обрыв кабеля или короткое замыкание в нем нарушает обмен только с одним компьютером, а все остальные компьютеры могут нормально продолжать работу.

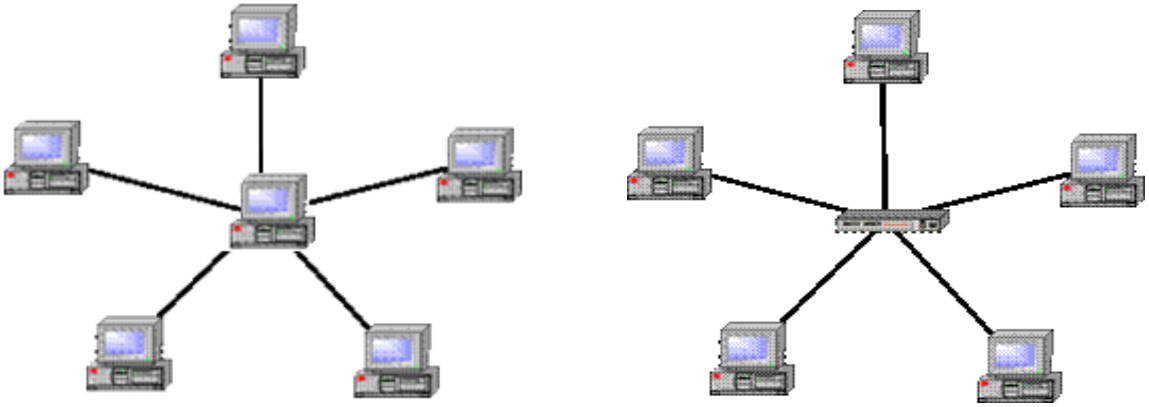


Рисунок 1.7 Топология «Активная звезда» и «Пассивная звезда»

В настоящее время пассивная звезда распространена гораздо более широко, чем активная. В центре сети с данной топологией помещается не компьютер, а специальное устройство - *коммутатор*, которое выполняет ту же функцию, что и *репитер*, то есть восстанавливает приходящие сигналы и пересылает их во все другие линии связи.

Серьезный недостаток топологии звезда состоит в жестком ограничении количества периферийных абонентов.

Проблема затухания сигналов в линии связи также решается в звезде проще, чем в случае шины, ведь каждый приемник всегда получает сигнал одного уровня. Предельная длина сети с топологией звезда может быть вдвое больше, чем в шине.

Общим недостатком для всех топологий типа звезда (как активной, так и пассивной) является значительно больший, чем при других топологиях, расход кабеля, что существенно влияет на стоимость сети в целом.

1.3.3. Топология кольцо — это топология, в которой каждый компьютер соединен линиями связи с двумя другими: от одного он получает информацию, а другому передает. На каждой линии связи, как и в случае звезды, работает только один передатчик и один приемник (связь типа точка-точка). Это позволяет отказаться от применения внешних терминаторов. Передача информации в кольце всегда производится только в одном направлении. Каждый из компьютеров передает информацию только одному компьютеру, следующему в цепочке за ним, а получает информацию только от предыдущего в цепочке компьютера (рис. 1.8). Поэтому выход из строя хотя бы одного из них нарушает работу сети в целом.

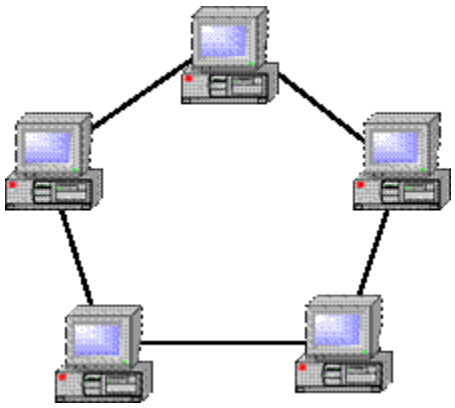


Рисунок 1.8 Сетевая топология кольцо

Важная особенность кольца состоит в том, что каждый компьютер ретранслирует (восстанавливает, усиливает) приходящий к нему сигнал, то есть выступает в роли репитера. Затухание сигнала во всем кольце не имеет никакого значения, важно только затухание между соседними компьютерами кольца. Размеры кольцевых сетей достигают десятков километров (например, в сети FDDI). Кольцо в этом отношении существенно превосходит любые другие топологии.

Компьютеры в кольце не являются полностью равноправными (в отличие, например, от шинной топологии). Ведь один из них обязательно получает информацию от компьютера, ведущего передачу в данный момент, раньше, а другие — позже. Подключение новых абонентов в кольцо выполняется достаточно просто, хотя и требует обязательной остановки работы всей сети на время подключения. Как и в случае шины, максимальное количество абонентов в кольце может быть довольно велико (до тысячи и больше). Кольцевая топология обычно обладает высокой устойчивостью к перегрузкам, обеспечивает уверенную работу с большими потоками передаваемой по сети информации, так как в ней, как правило, нет конфликтов (в отличие от шины), а также отсутствует центральный абонент (в отличие от звезды), который может быть перегружен большими потоками информации.

Иногда сеть с топологией кольцо выполняется на основе двух параллельных кольцевых линий связи, передающих информацию в противоположных направлениях. Цель подобного решения — увеличение вдвое скорости передачи информации по сети. К тому же при повреждении одного из кабелей сеть может работать с другим кабелем (правда, предельная скорость уменьшится).

1.3.4. Топология дерево (tree), которую можно рассматривать как комбинацию нескольких звезд. Причем, как и в случае звезды, дерево может быть *активным или истинным* (рис. 1.9) и *пассивным* (рис. 1.10). При активном дереве в центрах объединения нескольких линий связи находятся центральные компьютеры, а при пассивном — концентраторы (хабы).

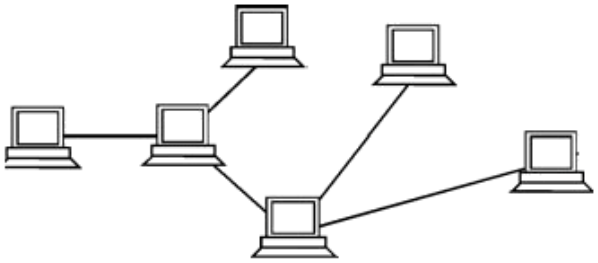


Рисунок 1.9
Топология активное дерево

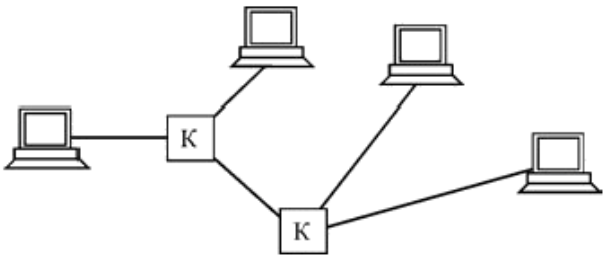


Рисунок 1.10
Топология пассивное дерево.
К — концентраторы

1.3.5. Комбинированные сетевые топологии, среди которых наиболее распространены **звездно-шинная** (рис. 1.11) и **звездно-кольцевая** (рис.1.12).

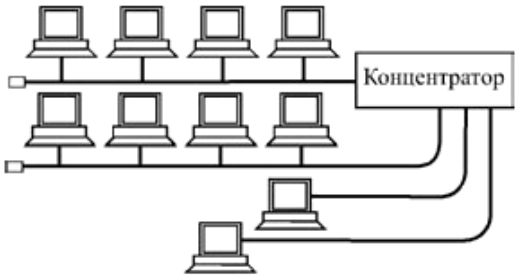


Рисунок 1.11 Пример звездно-шинной топологии

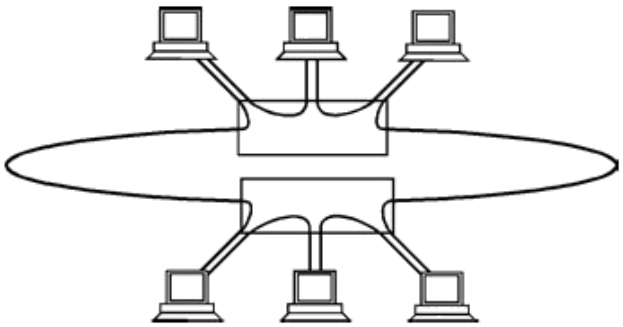


Рисунок 1.12 Пример звездно-кольцевой топологии

В звездно-шинной (star-bus) топологии используется комбинация шины и пассивной звезды. К концентратору подключаются как отдельные компьютеры, так и целые шинные сегменты. В данной топологии может использоваться и несколько концентраторов, соединенных между собой и образующих так называемую магистральную, опорную шину. К каждому из концентраторов при этом подключаются отдельные компьютеры или шинные сегменты. В результате получается звездно-шинное дерево. Таким образом, пользователь может гибко комбинировать преимущества шинной и звездной топологий, а также легко изменять количество компьютеров, подключенных к сети. С точки зрения распространения информации данная топология равноценна классической шине.

В случае звездно-кольцевой (star-ring) топологии в кольцо объединяются не сами компьютеры, а специальные концентраторы, к которым в свою очередь подключаются компьютеры с помощью звездообразных двойных линий связи. В действительности все компьютеры сети включаются в замкнутое кольцо, так как внутри концентраторов линии связи образуют замкнутый контур. Данная топология дает возможность комбинировать преимущества звездной и кольцевой топологий. Например, концентраторы позволяют собрать в одно место все точки подключения кабелей сети. Если говорить о распространении информации, данная топология равноценна классическому кольцу.

1.3.6. Сеточной топологии (mesh), при которой компьютеры связываются между собой не одной, а многими линиями связи, образующими сетку (рис. 1.13).

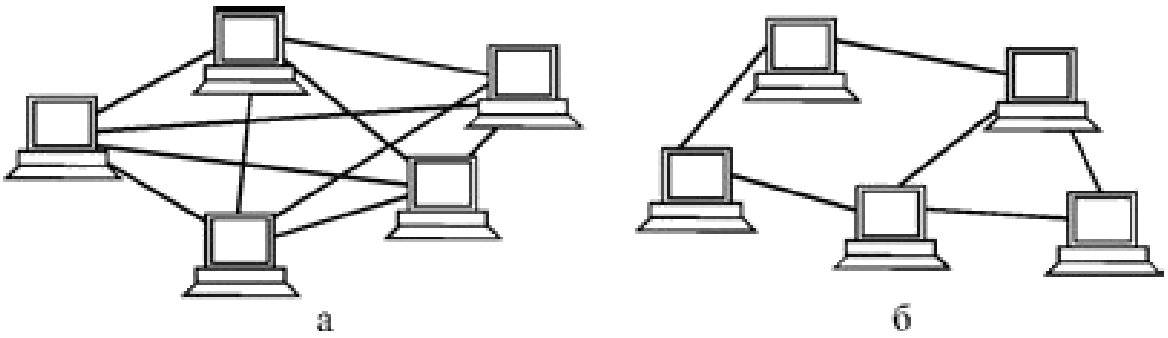


Рисунок 1.13 Сеточная топология: полная (а) и частичная (б)

В полной сеточной топологии каждый компьютер напрямую связан со всеми остальными компьютерами. В этом случае при увеличении числа компьютеров резко возрастает количество линий связи. Кроме того, любое изменение в конфигурации сети требует внесения изменений в сетевую аппаратуру всех компьютеров, поэтому полная сеточная топология не получила широкого распространения.

Частичная сеточная топология предполагает прямые связи только для самых активных компьютеров, передающих максимальные объемы информации. Остальные компьютеры соединяются через промежуточные узлы. Сеточная топология позволяет выбирать маршрут для доставки информации от абонента к абоненту, обходя неисправные участки. С одной стороны, это увеличивает надежность сети, с другой же – требует существенного усложнения сетевой аппаратуры, которая должна выбирать маршрут.

1.3.7. Многозначность понятия топологии

Топология сети указывает не только на физическое расположение компьютеров, но и на характер связей между ними, особенности распространения информации, сигналов по сети. Именно характер связей определяет степень отказоустойчивости сети, требуемую сложность сетевой аппаратуры, наиболее подходящий метод управления обменом, возможные типы сред передачи (каналов связи), допустимый размер сети (длина линий связи и количество абонентов) необходимость электрического согласования и многое другое.

Физическое расположение компьютеров, соединяемых сетью, почти не влияет на выбор топологии. Как бы ни были расположены компьютеры, их можно соединить с помощью любой заранее выбранной топологии (рис 2.11).

В том случае, если соединяемые компьютеры расположены по контуру круга, они могут соединяться, как звезда или шина. Когда компьютеры расположены вокруг некоего центра, их допустимо соединить с помощью

топологий шина или кольцо. Наконец когда компьютеры расположены в одну линию, они могут соединяться звездой или кольцом. Другое дело, какова будет требуемая длина кабеля.

Необходимо отметить, что топология все-таки не является основным фактором при выборе типа сети. Гораздо важнее, например, уровень стандартизации сети, скорость обмена, количество абонентов, стоимость оборудования, выбранное программное обеспечение. Но, с другой стороны, некоторые сети позволяют использовать разные топологии на разных уровнях. Этот выбор уже целиком ложится на пользователя, который должен учитывать все перечисленные факторы.

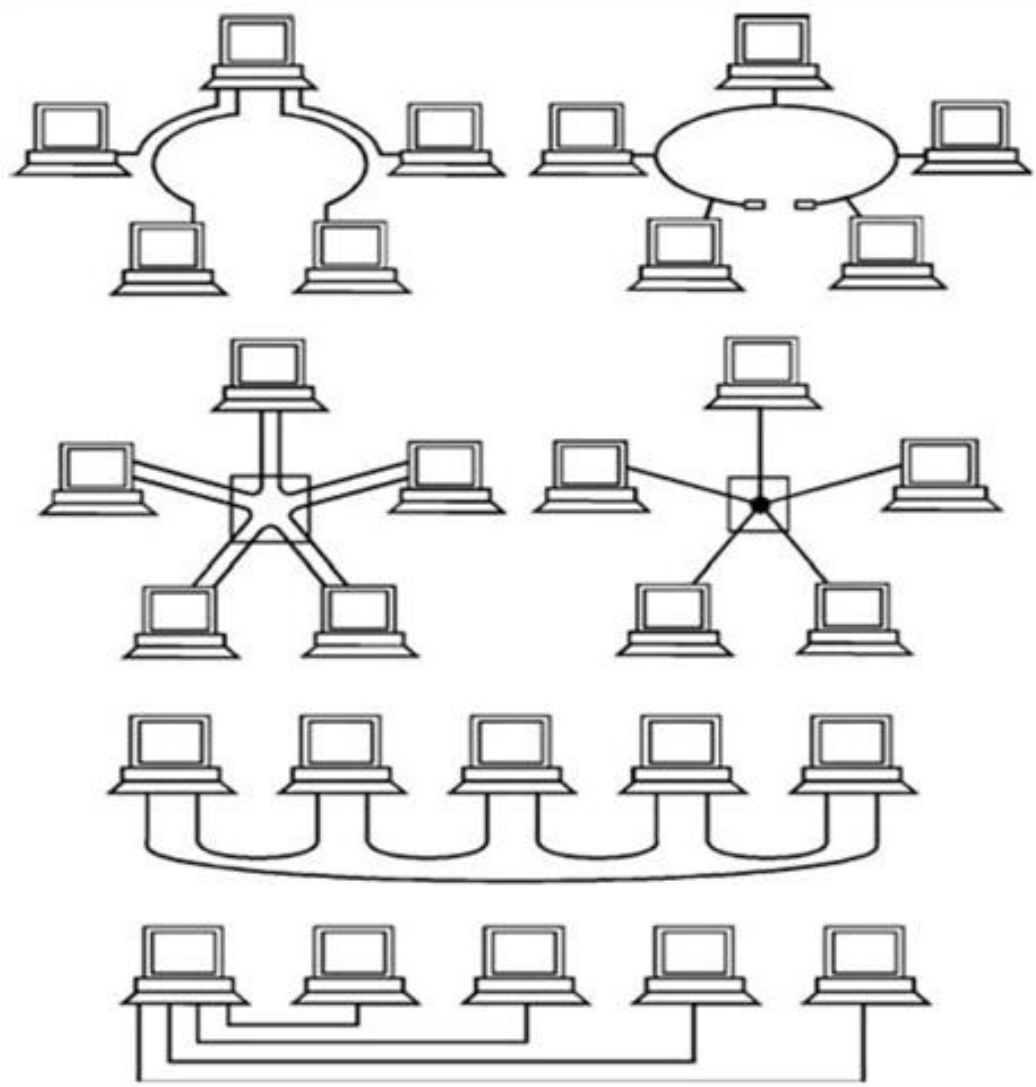


Рисунок 1.14 Примеры использования разных топологий

1.4. Семиуровневая модель взаимодействия открытых систем

Международная организация стандартов (International Standards Organization - **ISO**) создала эталонную модель взаимодействия **открытых систем** (Open System Interconnection reference model - **OSI**), которая определяет концепцию и методологию создания сетей передачи данных. Модель описывает стандартные правила функционирования устройств и программных средств при обмене данными между узлами (компьютерами) в открытой системе. Открытая система состоит из программно-аппаратных средств, способных взаимодействовать между собой, при использовании **стандартных правил и устройств сопряжения** – называемых интерфейсами.

Модель ISO/OSI включает семь уровней взаимодействия двух устройств: узла источника – source и узла назначения – destination. Правила, по которым происходит обмен данными между программно-аппаратными средствами, находящимися на одном уровне, называется **протоколом**. Набор взаимодействующих протоколов называется **стеком протоколов** и задается определенным стандартом.

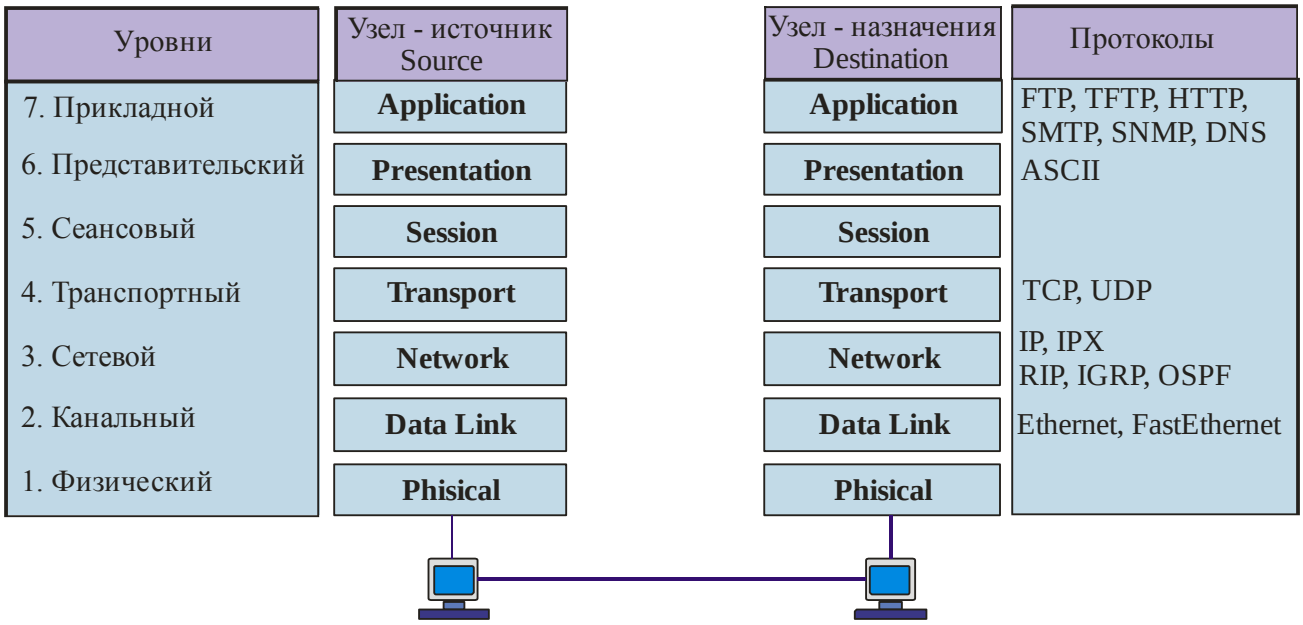


Рис.1.15. Семиуровневая модель ISO/OSI

Взаимодействие соответствующих уровней является **виртуальным**, за исключением физического уровня, на котором происходит обмен данными по линиям связи, соединяющим компьютеры. Взаимодействие уровней между собой происходит через межуровневый **интерфейс** и каждый нижележащий уровень предоставляет услуги вышележащему.

Виртуальный обмен между соответствующими уровнями узлов HostA и HostB происходит определенными единицами информации. На трех верхних уровнях – это сообщения или данные (Data). На транспортном уровне – сегменты (Segment), на сетевом уровне – пакеты (Packet), на канальном уровне – кадры (Frame) и на физическом передается поток битов.

Для каждой сетевой технологии существуют свои протоколы и свои технические средства, часть из которых имеет условные обозначения, приведенные на рисунке. Данные обозначения введены фирмой **Cisco** и стали общепринятыми.

Среди технических средств физического уровня следует отметить кабели, разъемы, повторители сигналов (repeater), многопортовые повторители или концентраторы (**hub**), преобразователи среды (transceiver), например, преобразователи электрических сигналов в оптические и наоборот.

На канальном уровне это мосты (bridge), коммутаторы (**switch**).

На сетевом уровне – маршрутизаторы (**router**). Сетевые адаптеры (Network Interface Card – NIC) функционируют как на канальном, так и на физическом уровне.

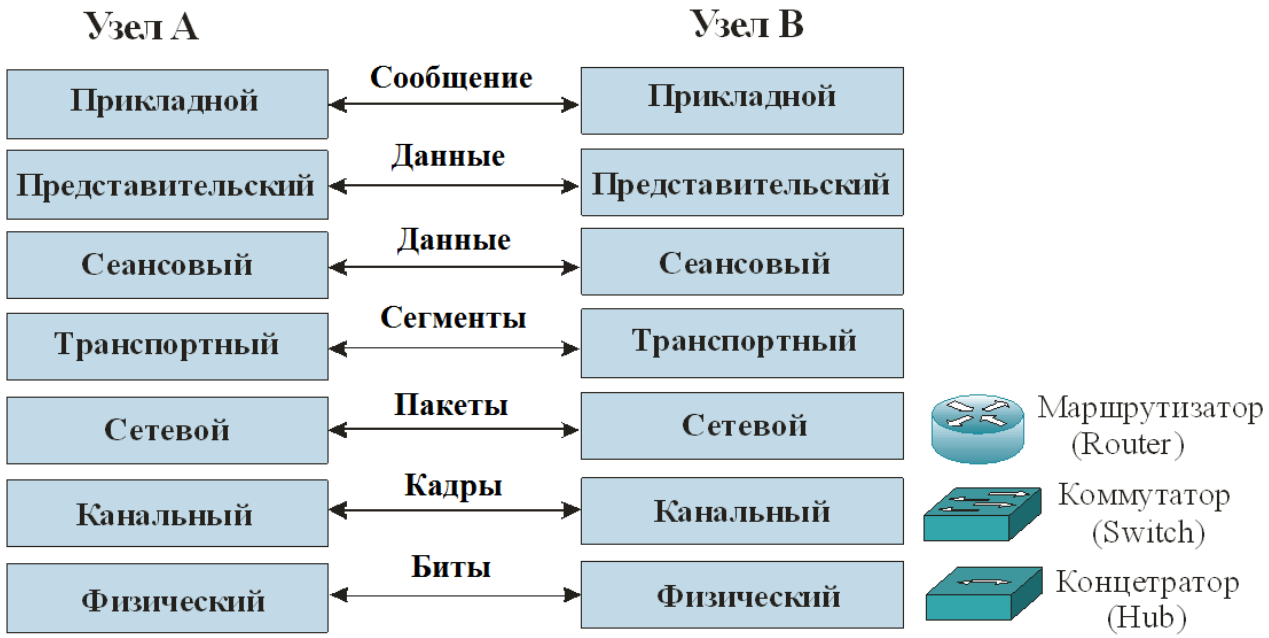


Рис.1.16. Устройства и единицы информации соответствующих уровней

При передаче данных от источника к узлу назначения, подготовленные на прикладном уровне передаваемые данные последовательно проходят от самого верхнего Прикладного уровня 7 узла источника информации до самого нижнего – Физического уровня 1, затем передаются по физической среде узлу назначения, где последовательно проходят от нижнего уровня 1 до уровня 7.

Прикладной самый верхний уровень (Application Layer) 7 оперирует наиболее общей единицей данных – сообщением. На этом уровне реализуется управление общим доступом к сети, потоком данных, сетевыми службами, такими как **FTP**, **TFTP**, **HTTP**, **SMTP**, **SNMP** и др.

Представительский уровень (Presentation Layer) 6 изменяет форму представления данных. Например, передаваемые с уровня 7 данные преобразуются в общепринятый формат **ASCII**. При приеме данных происходит обратный процесс. На уровне 6 также происходит шифрация и сжатие данных.

Сеансовый (Session Layer) уровень 5 устанавливает соединение двух компьютеров, определяет, какой компьютер является передатчиком, а какой приемником, задает для передающей стороны время передачи, а для приёмной – синхронизацию.

Транспортный уровень (Transport Layer) 4 из длинного сообщения узла источника информации формирует сегменты определенного объема, а короткие сообщения может объединять в один сегмент. В узле назначения происходит обратный процесс. Кроме того, транспортный уровень обеспечивает **надежную доставку пакетов**. При обнаружении потерь и ошибок на этом уровне формируется запрос повторной передачи, при этом используется протокол **TCP**. Когда необходимость проверки правильности доставленного сообщения отсутствует, то используется более простой протокол **UDP**.

Сетевой уровень (Network Layer) 3 адресует сообщение, задавая единице передаваемых данных (**пакету**) логический сетевой адрес, определяет **маршрут**, по которому будет отправлен **пакет данных**, транслирует логические сетевые адреса в физические, а на приемной стороне – физические адреса в логические.

Канальный уровень (Data Link) 2 формирует из пакетов **кадры** данных (**frames**). На этом уровне задаются **физические адреса** устройства-отправителя и устройства-получателя данных. На этом же уровне к передаваемым данным производится прибавление контрольной суммы, определяемой с помощью алгоритма циклического кода. На приемной стороне по контрольной сумме определяют и по возможности исправляют ошибки.

Физический уровень (Physical) 1 осуществляет передачу потока битов по соответствующей физической среде (электрический или оптический кабель, радиоканал) через соответствующий интерфейс. На этом уровне производится линейное кодирование данных, синхронизация передаваемых битов информации.

Протоколы трех верхних уровней являются сетенезависимыми, три нижних уровня являются сетезависимыми. Связь между тремя верхними и тремя нижними уровнями происходит на транспортном уровне.

Важным процессом при передаче данных является **инкапсуляция** (encapsulation) данных. Передаваемый поток данных, сформированный приложением, проходит три верхних сетенезависимых уровня и поступает на транспортный уровень, где формируются сегменты данных. В заголовке сегмента содержится номер протокола прикладного уровня, с помощью которого подготовлено сообщение и порядковый номер сегмента.

На сетевом уровне к сегменту добавляется заголовок (**header**), который содержит специфическую для данного уровня информацию, прежде всего, сетевые (логические) адреса отправителя информации (источника) – Source Address (**SA**) и адрес получателя (назначения) – Destination Address (**DA**). При этом формируется **пакет** данных.

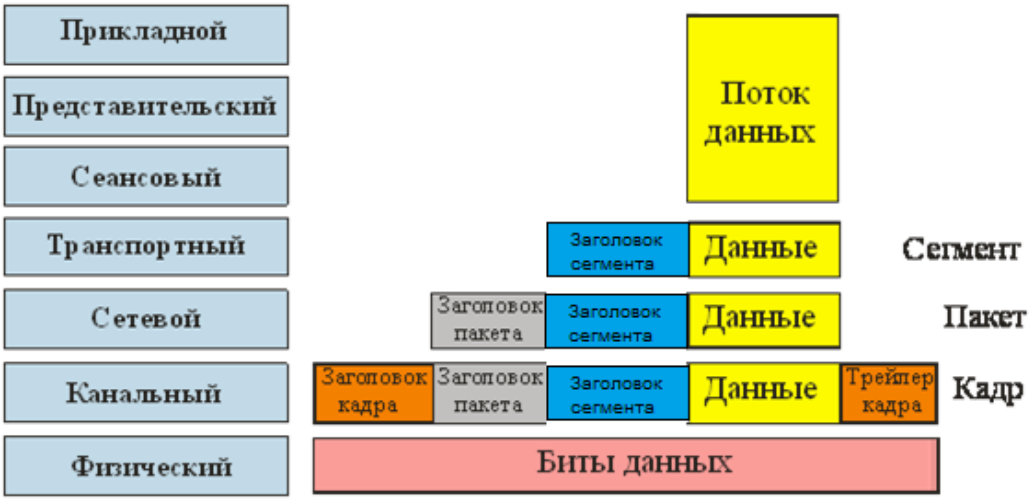


Рис.1.17. Инкапсуляция данных

На канальном уровне к пакету добавляется новый заголовок, содержащий физические адреса источника и следующего узла сети, через который пройдет сообщение, а также другую информацию. При этом формируется **кадр** или **фрейм** данных. Кроме того, на этом уровне добавляется **трейлер** (концевик) кадра, содержащий информацию, необходимую для проверки правильности принятой информации. Таким образом, происходит обрамление данных заголовками со служебной информацией, т.е. **инкапсуляция** данных.

Помимо семиуровневой OSI модели на практике применяется четырехуровневая модель TCP/IP.

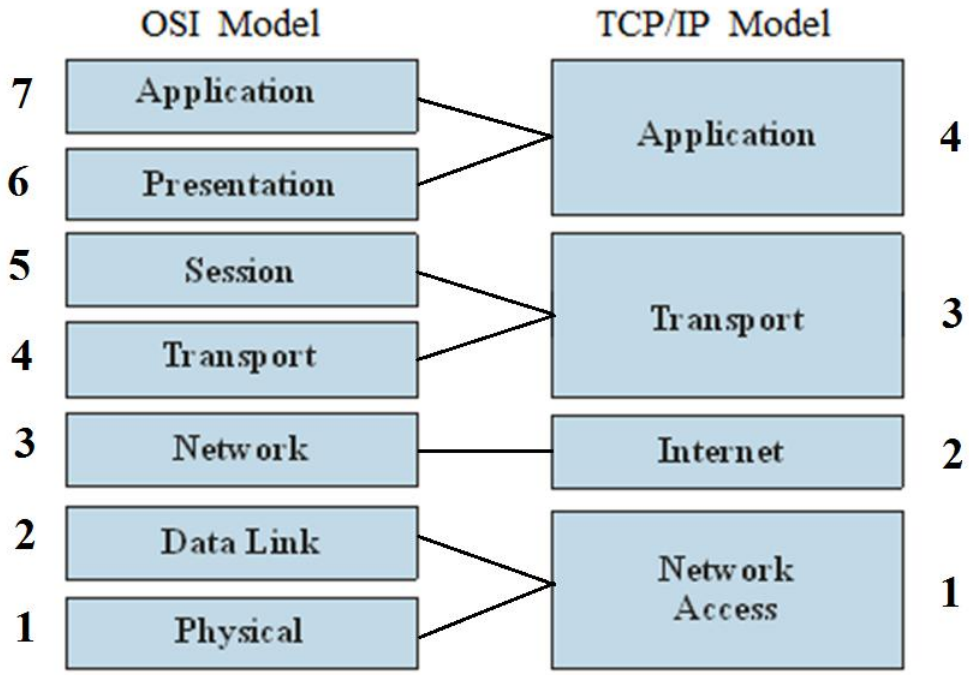


Рис.1.18. Модели OSI и TCP/IP

Прикладной уровень модели TCP/IP по названию совпадает с названием модели OSI, но по функциям гораздо шире, поскольку охватывает два верхних сетенезависимых уровня (прикладной и представительский). Транспортный уровень совпадает по названию с четвёртым, а по функциям объединяет в себе и сеансовый. Сетевой уровень модели OSI соответствует межсетевому (internet) уровню модели TCP/IP, а два нижних уровня (канальный и физический) представлены объединенным уровнем Network Access.

Основная информация, добавляемая в заголовках сообщений на разных уровнях OSI модели.

Физический уровень	Канальный уровень	Сетевой уровень	Транспортный уровень	Верхние уровни
Частотно-временные параметры и синхронизация	Физические адреса узлов источника и назначения	Логические адреса узлов источника и назначения	Номера порта узлов источника и назначения	Сопряжение пользователей с сетью

На транспортном уровне в заголовке сегмента задаются номера портов приложений источника и назначения. Номера портов адресуют приложения или сервисы прикладного уровня, которые создавали сообщение и будут его обрабатывать на приемной стороне. Например, сервер электронной почты с номерами портов 25 и 110 позволяет посылать e-mail сообщения и принимать их, № порта 80 адресует веб-сервер.

Для обмена сообщениями, помимо номеров портов, на сетевом уровне в заголовке пакета необходимо задать логические адреса источника и назначения. К логическим адресам относятся, например, IP-адреса пользователей. В документации IP-адреса используемой в настоящее время версии IPv4 отображаются в десятичной форме в виде четырех групп чисел. Каждая группа может содержать числа от 0 до 255. Группы разделены между собой точками, например, 192.168.10.21; 172.16.250.17; 10.1.10.122.

В дополнение к логическим адресам на канальном уровне в заголовке кадра задаются физические адреса устройства-источника и устройства-назначения. Наиболее широко распространенной сетевой технологией канального уровня в настоящее время является Ethernet или её модификации (Fast Ethernet, Gigabit Ethernet, 10Gigabit Ethernet). При этом в качестве физических адресов используются MAC-адреса (Media Access Control). В документации MAC-адреса представлены в виде 12 шестнадцатеричных чисел, например, 00-05-A8-69-CD-F1. Тот же адрес может быть представлен и в несколько другой форме 00:05:A8:69:CD:F1 или 0005.A869.CD-F1. MAC-адреса компьютеров прошиты в ПЗУ сетевой карты.

Таким образом, тройная система адресации позволяет адресовать устройства, пользователей и программное обеспечение приложений.

Раздел 2. ОБОРУДОВАНИЕ И ОРГАНИЗАЦИЯ ВЫЧИСЛИТЕЛЬНЫХ СЕТЕЙ

2.1. Аппаратура локальных сетей

Аппаратура локальных сетей обеспечивает реальную связь между абонентами. Выбор аппаратуры имеет важнейшее значение на этапе проектирования сети, так как стоимость аппаратуры составляет наиболее существенную часть от стоимости сети в целом, а замена аппаратуры связана не только с дополнительными расходами, но зачастую и с трудоемкими работами. К аппаратуре локальных сетей относятся: кабели для передачи информации; разъемы для присоединения кабелей; согласующие терминаторы; сетевые адаптеры; репитеры; трансиверы; концентраторы; мосты; маршрутизаторы; шлюзы.

2.1.1. Сетевые адаптеры (они же контроллеры, карты, платы, интерфейсы, NIC – Network Interface Card) – это основная часть аппаратуры локальной сети. Назначение сетевого адаптера – сопряжение компьютера (или другого абонента) с сетью, то есть обеспечение обмена информацией между компьютером и каналом связи в соответствии с принятыми правилами обмена. Именно они реализуют функции двух нижних уровней модели OSI. Как правило, сетевые адаптеры выполняются в виде платы, вставляемой в слоты расширения системной магистрали (шины) компьютера (чаще всего PCI, ISA или PC-Card). Плата сетевого адаптера обычно имеет также один или несколько внешних разъемов для подключения к ней кабеля сети.

Например, сетевые адаптеры Ethernet могут выпускаться со следующими наборами разъемов:

1. TPO – разъем RJ-45 (для кабеля на витых парах по стандарту 10BASE-T).
2. TPC – разъемы RJ-45 (для кабеля на витых парах 10BASE-T) и BNC (для коаксиального кабеля 10BASE2).
3. TP – разъем RJ-45 (10BASE-T) и трансиверный разъем AUI.
4. Combo – разъемы RJ-45 (10BASE-T), BNC (10BASE2), AUI.
5. Coax – разъемы BNC, AUI.
6. FL – разъем ST (для оптоволоконного кабеля 10BASE-FL).

Функции сетевого адаптера делятся на магистральные и сетевые. К магистральным относятся те функции, которые осуществляют взаимодействие адаптера с магистралью (системной шиной) компьютера (то есть опознание своего магистрального адреса, пересылка данных в компьютер и из компьютера, выработка сигнала прерывания компьютера и т.д.). Сетевые функции обеспечивают общение адаптера с сетью.

К основным сетевым функциям адаптеров относятся:

1. гальваническая развязка компьютера и кабеля локальной сети (для этого обычно используется передача сигналов через импульсные трансформаторы);
2. преобразование логических сигналов в сетевые (электрические или световые) и обратно;
3. кодирование и декодирование сетевых сигналов, то есть прямое и обратное преобразование линейных кодов передачи информации (например, манчестерский код);
4. опознание принимаемых пакетов (выбор из всех приходящих пакетов тех, которые адресованы данному абоненту или всем абонентам сети одновременно);
5. преобразование параллельного кода в последовательный при передаче и обратное преобразование при приеме;
6. буферизация передаваемой и принимаемой информации в буферной памяти адаптера;
7. организация доступа к сети в соответствии с принятым методом управления обменом;
8. подсчет контрольной суммы пакетов при передаче и приеме.

Типичный алгоритм взаимодействия компьютера с сетевым адаптером выглядит следующим образом.

Для передачи компьютер сначала формирует пакет в своей памяти, затем пересылает его в буферную память сетевого адаптера и дает команду адаптеру на передачу. Адаптер анализирует текущее состояние сети и при первой же возможности выдает пакет в сеть (выполняет управление доступом к сети). При этом он производит преобразование информации из буферной памяти в последовательный вид для побитной передачи по сети, подсчитывает контрольную сумму, кодирует биты пакета в сетевой код и через узел гальванической развязки выдает пакет в кабель сети. Буферная память в данном случае позволяет освободить компьютер от контроля состояния сети, а также обеспечить требуемый для сети темп выдачи информации.

Если по сети приходит пакет, то сетевой адаптер через узел гальванической развязки принимает биты пакета, производит их декодирование из сетевого кода и сравнивает сетевой MAC-адрес приемника из пакета со своим собственным MAC-адресом, который, как правило, устанавливается производителем адаптера. Если адрес совпадает, то сетевой адаптер записывает пришедший пакет в свою буферную память и сообщает компьютеру (обычно – сигналом аппаратного прерывания) о том, что пришел пакет и его надо читать. Одновременно с записью пакета производится подсчет контрольной суммы, что

позволяет к концу приема сделать вывод, о наличии ошибки в этом пакете. Буферная память в данном случае опять же позволяет освободить компьютер от контроля сети, а также обеспечить высокую степень готовности сетевого адаптера к приему пакетов.

Некоторые адаптеры позволяют реализовать функцию удаленной загрузки, то есть поддерживать работу в сети бездисковых компьютеров, загружающих свою операционную систему прямо из сети. Для этого в состав таких адаптеров включается постоянная память с соответствующей программой загрузки. Правда, не все сетевые программные средства поддерживают данный режим работы.

Сетевой адаптер выполняет функции первого и второго уровней модели OSI.

Все остальные аппаратные средства локальных сетей (кроме адаптеров) имеют вспомогательный характер, и без них часто можно обойтись. Это сетевые промежуточные устройства.

2.1.2. Трансиверы или приемопередатчики (от английского TRANsmitter + reCEIVER) служат для передачи информации между адаптером и кабелем сети или между двумя сегментами (частями) сети. Трансиверы усиливают сигналы, преобразуют их уровни или преобразуют сигналы в другую форму (например, из электрической в оптическую и обратно). Трансиверами также часто называют встроенные в адаптер приемопередатчики. Трансивер устанавливается непосредственно на кабеле и питается от сетевой карты компьютера. С сетевой картой трансивер соединяется интерфейсным кабелем AUI (Attachment Unit Interface).

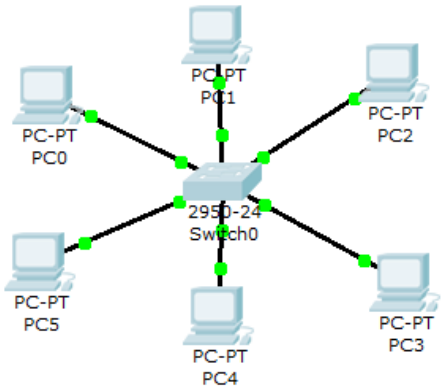
2.1.3. Репитеры или повторители (repeater) выполняют более простую функцию, чем трансиверы. Они не преобразуют ни уровни сигналов, ни их физическую природу, а только восстанавливают ослабленные сигналы (их амплитуду и форму), приводя их к исходному виду. Цель такой ретрансляции сигналов состоит исключительно в увеличении длины сети.

Однако часто репитеры выполняют и некоторые другие, вспомогательные функции, например, гальваническую развязку соединяемых сегментов и оконечное согласование. Репитеры так же как трансиверы не производят никакой информационной обработки проходящих через них сигналов.

2.1.4. Концентратор (хабы, hub), это повторитель, который имеет несколько портов и соединяет несколько физических линий связи. Концентраторы представляют собой несколько собранных в едином конструктиве репитеров, и

выполняют те же функции. Концентратор всегда изменяет физическую топологию сети, но при этом оставляет без изменения ее логическую топологию. Если на какой-либо его порт поступает сообщение, он пересылает его на все остальные. Преимущество концентраторов по сравнению репитерами в том, что все точки подключения собраны в одном месте, это упрощает реконфигурацию сети, контроль и поиск неисправностей.

2.1.5. Коммутатор (switch), как и концентратор, служат для соединения сегментов сети.



Они выполняют более сложные функции, производя сортировку поступающих на них пакетов.

Коммутаторы передают из одного сегмента сети в другой не все поступающие на них пакеты, а только те, которые адресованы компьютерам из другого сегмента. Пакеты, передаваемые между абонентами одного сегмента, через коммутатор не проходят. При этом сам пакет коммутатором не принимается, а только пересылается. Интенсивность обмена в сети снижается вследствие разделения нагрузки, поскольку каждый сегмент работает не только со своими пакетами, но и с пакетами, пришедшими из других сегментов.

2.1.6. Мост (bridge) – служит для объединения сетей с разными стандартами обмена, например, Ethernet и Arcnet, или нескольких сегментов (частей) одной и той же сети, например, Ethernet. Мост**,** как и коммутатор, только разделяет нагрузку сегментов, повышая тем самым производительность сети в целом. Мосты принимают поступающие пакеты целиком и в случае необходимости производят их простейшую обработку. Мосты, как и коммутаторы, работают на втором уровне модели OSI, но в отличие от них могут захватывать также и верхний подуровень LLC второго уровня (для связи разнородных сетей). В последнее время мосты быстро вытесняются коммутаторами, которые становятся более функциональными.

2.1.7. Маршрутизатор (router) осуществляет выбор оптимального маршрута для каждого пакета с целью предотвращения перегрузки отдельных участков сети и обхода поврежденных участков. Он применяется, как правило, в сложных разветвленных сетях, имеющих несколько маршрутов между отдельными абонентами, а также для разделения различных сетей.

Маршрутизаторы не преобразуют протоколы нижних уровней, поэтому они соединяют только сегменты сетей. Маршрутизаторы работают на третьем уровне модели OSI так как они анализируют не только MAC-адреса пакета, но и IP-адреса, то есть более глубоко проникают в инкапсулированный пакет.

Существуют также гибридные маршрутизаторы (brouter), представляющие собой гибрид моста и маршрутизатора. Они выделяют пакеты, которым нужна маршрутизация и обрабатывают их как маршрутизатор, а для остальных пакетов служат обычным мостом.

2.1.8. Шлюз (gateway) – это устройство для соединения сетей с сильно отличающимися протоколами, например, для соединения локальных сетей с большими компьютерами или с глобальными сетями. Это самые дорогие и редко применяемые сетевые устройства. Шлюзы реализуют связь между абонентами на верхних уровнях модели OSI (с четвертого по седьмой). Соответственно они должны выполнять и все функции нижестоящих уровней.

Маршрутизаторы, мосты и шлюзы служат для объединения в одну сеть несколько разнородных сетей с разными протоколами обмена нижнего уровня, в частности, с разными форматами пакетов, методами кодирования, скоростью передачи и т.д. В результате их применения сложная и неоднородная сеть, содержащая в себе различные сегменты, с точки зрения пользователя выглядит самой обычной сетью. Обеспечивается прозрачность сети для протоколов высокого уровня. Реализуются они обычно на базе компьютеров, подключенных к сети с помощью сетевых адаптеров. По сути, они являются специализированными абонентами (узлами) сети.

2.2. Стандарты кабелей вычислительных сетей

При построении сетей применяются линии связи, использующие различную физическую среду: телефонные и телеграфные провода, подвешенные в воздухе, медные коаксиальные кабели, медные витые пары, волоконно-оптические кабели, радиоволны.

Кабель - это сложное изделие, состоящее из проводников, слоев экрана и изоляции. В некоторых случаях в состав кабеля входят разъемы, с помощью которых кабели присоединяются к оборудованию. Кроме этого, для обеспечения быстрой перекоммутации кабелей и оборудования используются различные электромеханические устройства, называемые кроссовыми секциями, кроссовыми коробками или шкафами.

Линии связи могут использовать, кроме кабеля, промежуточную аппаратуру, прозрачную для пользователей. Промежуточная аппаратура выполняет две основные функции: усиливает сигналы и обеспечивает постоянную коммутацию между парой пользователей линии.

В зависимости от типа промежуточной аппаратуры линии связи делятся на аналоговые и цифровые. В аналоговых линиях связи для уплотнения низкоскоростных каналов абонентов в общий высокоскоростной канал используется метод разделения частот (FDMA), а в цифровых - метод разделения во времени (TDMA).

Для характеристики способности линии передавать сигналы произвольной формы без значительных искажений применяется ряд показателей, использующих в качестве тестового сигнала синусоиды различной частоты. К этим показателям относятся: амплитудно-частотная характеристика, полоса пропускания и затухание сигнала на определенной частоте.

В компьютерных сетях применяются кабели, удовлетворяющие определенным стандартам. Современные стандарты определяет характеристики не отдельного кабеля, а полного набора элементов, необходимого для создания кабельного соединения, например шнура от рабочей станции до розетки, самой розетки, основного кабеля, жесткого кроссового соединения и шнура до концентратора. Сегодня наиболее употребительными стандартами являются: американский стандарт EIA/TIA-568A, международный стандарт ISO/IEC 11801, европейский стандарт EN50173, а также фирменный стандарт компании IBM.

Стандарты определены для четырех типов кабеля: на основе **неэкранированной витой пары**, на основе **экранированной витой пары**, **коаксиального** и **волоконно-оптического кабелей**.

В стандартах кабелей оговаривается достаточно много характеристик, из которых наиболее важные перечислены ниже.

Затухание (Attenuation). Затухание измеряется в децибелах на метр для определенной частоты или диапазона частот сигнала.

Перекрестные наводки на ближнем конце (Near End Cross Talk, NEXT). Измеряются в децибелах для определенной частоты сигнала.

Импеданс (волновое сопротивление) - это полное (активное и реактивное) сопротивление в электрической цепи. Импеданс измеряется в Омах и является относительно постоянной величиной для кабельных систем (например, для

коаксиальных кабелей, используемых в стандартах Ethernet, импеданс кабеля должен составлять 50 Ом). Для неэкранированной витой пары наиболее часто используемые значения импеданса - 100 и 120 Ом. В области высоких частот (100-200 МГц) импеданс зависит от частоты.

Активное сопротивление - это сопротивление постоянному току в электрической цепи. В отличие от импеданса активное сопротивление не зависит от частоты и возрастает с увеличением длины кабеля.

Емкость - это свойство металлических проводников накапливать энергию. Два электрических проводника в кабеле, разделенные диэлектриком, представляют собой конденсатор, способный накапливать заряд. Емкость является нежелательной величиной, поэтому следует стремиться к тому, чтобы она была как можно меньше (иногда применяют термин «паразитная емкость»). Высокое значение емкости в кабеле приводит к искажению сигнала и ограничивает полосу пропускания линии.

Уровень внешнего электромагнитного излучения или электрический шум. Электрический шум - это нежелательное переменное напряжение в проводнике. Электрический шум бывает двух типов: фоновый и импульсный. Электрический шум можно также разделить на низко-, средне- и высокочастотный. Источниками фонового электрического шума в диапазоне до 150 кГц являются линии электропередачи, телефоны и лампы дневного света; в диапазоне от 150 кГц до 20 МГц - компьютеры, принтеры, ксероксы; в диапазоне от 20 МГц до 1 ГГц - телевизионные и радиопередатчики, микроволновые печи. Основными источниками импуль-сного электрического шума являются моторы, переключатели и сварочные агрегаты. Электрический шум измеряется в милливольтах.

Диаметр или площадь сечения проводника. Для медных проводников достаточно употребительной является американская система AWG (American Wire Gauge), которая вводит некоторые условные типы проводников, например 22 AWG, 24 AWG, 26 AWG. Чем больше номер типа проводника, тем меньше его диаметр. В вычислительных сетях наиболее употребительными являются типы проводников, приведенные выше в качестве примеров. В европейских и международных стандартах диаметр проводника указывается в миллиметрах. Естественно, приведенный перечень характеристик далеко не полон, причем в нем представлены только электромагнитные характеристики и его нужно дополнить механическими и конструктивными характеристиками, определяющими тип изоляции, конструкцию разъема и т. п. Помимо универсальных характеристик, таких, например, как затухание, которые

применимы для всех типов кабелей, существуют характеристики, которые применимы только к определенному типу кабеля. Например, параметр шаг скрутки проводов используется только для характеристики витой пары, а параметр NEXT применим только к многопарным кабелям на основе витой пары.

Основное внимание в современных стандартах уделяется кабелям на основе витой пары и волоконно-оптическим кабелям.

2.2.1. Кабели на основе неэкранированной витой пары

Медный неэкранированный кабель UTP в зависимости от электрических и механических характеристик разделяется на 5 категорий (Category 1 - Category 5). Кабели категорий 1 и 2 были определены в стандарте EIA/TIA-568, но в стандарт 568A уже не вошли, как устаревшие.

2.2.1.1. Кабели категории 1 применяются там, где требования к скорости передачи минимальны. Обычно это кабель для цифровой и аналоговой передачи голоса и низкоскоростной (до 20 Кбит/с) передачи данных. До 1983 года это был основной тип кабеля для телефонной разводки.

2.2.1.2. Кабели категории 2 были впервые применены фирмой IBM при построении собственной кабельной системы. Главное требование к кабелям этой категории - способность передавать сигналы со спектром до 1 МГц.

2.2.1.3. Кабели категории 3 были стандартизованы в 1991 году, когда был разработан Стандарт телекоммуникационных кабельных систем для коммерческих зданий (EIA-568), на основе которого затем был создан действующий стандарт EIA-568A. Стандарт EIA-568 определил электрические характеристики кабелей категории 3 для частот в диапазоне до 16 МГц, поддерживающих, таким образом, высокоскоростные сетевые приложения. Кабель категории 3 предназначен как для передачи данных, так и для передачи голоса. Шаг скрутки проводов равен примерно 3 витка на 1 фут (30,5 см). Кабели категории 3 сейчас составляют основу многих кабельных систем зданий, в которых они используются для передачи и голоса, и данных.

2.2.1.4. Кабели категории 4 представляют собой несколько улучшенный вариант кабелей категории 3. Кабели категории 4 обязаны выдерживать тесты на частоте передачи сигнала 20 МГц и обеспечивать повышенную помехоустойчивость и низкие потери сигнала. Кабели категории 4 хорошо подходят для применения в системах с увеличенными расстояниями (до 135

метров) и в сетях Token Ring с пропускной способностью 16 Мбит/с. На практике используются редко.

2.2.1.5. Кабели категории 5 были специально разработаны для поддержки высокоскоростных протоколов. Поэтому их характеристики определяются в диапазоне до 100 МГц. Большинство новых высокоскоростных стандартов ориентируются на использование витой пары 5 категории. На этом кабеле работают протоколы со скоростью передачи данных 100 Мбит/с - FDDI (с физическим стандартом TP-PMD), Fast Ethernet, l00VG-AnyLAN, а также более скоростные протоколы - ATM на скорости 155 Мбит/с, и Gigabit Ethernet на скорости 1000 Мбит/с (вариант Gigabit Ethernet на витой паре категории 5 стал стандартом в июне 1999 г.). Кабель категории 5 пришел на замену кабелю категории 3, и сегодня все новые кабельные системы крупных зданий строятся именно на этом типе кабеля (в сочетании с волоконно-оптическим).

Наиболее важные электромагнитные характеристики кабеля категории 5 имеют следующие значения:

- полное волновое сопротивление в диапазоне частот до 100 МГц равно 100 Ом (стандарт ISO 11801 допускает также кабель с волновым сопротивлением 120 Ом);
- величина перекрестных наводок NEXT в зависимости от частоты сигнала должна принимать значения не менее 74 дБ на частоте 150 кГц и не менее 32 дБ на частоте 100 МГц;
- затухание имеет предельные значения от 0,8 дБ (на частоте 64 кГц) до 22 дБ (на частоте 100 МГц);
- активное сопротивление не должно превышать 9,4 Ом на 100 м;
- емкость кабеля не должна превышать 5,6 нф на 100 м.

Все кабели UTP независимо от их категории выпускаются в 4-парном исполнении. Каждая из четырех пар кабеля имеет определенный цвет и шаг скрутки. Обычно две пары предназначены для передачи данных, а две - для передачи голоса.

Для соединения кабелей с оборудованием используются вилки и розетки RJ-45, представляющие 8-контактные разъемы, похожие на обычные телефонные разъемы. RJ-11.

2.2.1.6. Кабели категорий 6 и 7 занимают Особое место**,** которые промышленность начала выпускать сравнительно недавно. Для кабеля категории 6 характеристики определяются до частоты 200 МГц, а для кабелей

категории 7 - до 600 МГц. Кабели категории 7 обязательно экранируются, причем как каждая пара, так и весь кабель в целом. Кабель категории 6 может быть как экранированным, так и неэкранированным. Основное назначение этих кабелей - поддержка высокоскоростных протоколов на отрезках кабеля большей длины, чем кабель UTP категории 5. Некоторые специалисты сомневаются в необходимости применения кабелей категории 7, так как стоимость кабельной системы при их использовании получается соизмеримой по стоимости сети с использованием волоконно-оптических кабелей, а характеристики кабелей на основе оптических волокон выше.

2.2.2. Кабели на основе экранированной витой пары

Экранированная витая пара STP хорошо защищает передаваемые сигналы от внешних помех, а также меньше излучает электромагнитных колебаний наружу, что защищает, в свою очередь, пользователей сетей от вредного для здоровья излучения. Наличие экрана удорожает кабель и усложняет его прокладку, так как требует выполнения качественного заземления. Экранированный кабель применяется только для передачи данных, а голос по нему не передают.

Основным стандартом, определяющим параметры экранированной витой пары, является фирменный стандарт IBM. В этом стандарте кабели делятся не на категории, а на типы: Type 1, Type 2,..., Type 9.

Основным типом экранированного кабеля является кабель **Type 1** стандарта IBM. Он состоит из 2-х пар скрученных проводов, экранированных проводящей оплеткой, которая заземляется. Электрические параметры кабеля Type 1 примерно соответствуют параметрам кабеля UTP категории 5. Однако волновое сопротивление кабеля Type 1 равно 150 Ом (UTP категории 5 имеет волновое сопротивление 100 Ом), поэтому простое «улучшение» кабельной проводки сети путем замены неэкранированной пары UTP на STP Type 1 невозможно. Трансиверы, рассчитанные на работу с кабелем, имеющим волновое сопротивление 100 Ом, будут плохо работать на волновое сопротивление 150 Ом. Поэтому при использовании STP Type 1 необходимы соответствующие трансиверы. Такие трансиверы имеются в сетевых адаптерах Token Ring, так как эти сети разрабатывались для работы на экранированной витой паре. Некоторые другие стандарты также поддерживают кабель STP Type 1 - например, l00VG-AnyLAN, а также Fast Ethernet (хотя основным типом кабеля для Fast Ethernet является UTP категории 5). В случае если технология может использовать UTP и STP, нужно убедиться, на какой тип кабеля рассчитаны приобретаемые трансиверы. Сегодня кабель STP Type 1 включен в

стандарты EIA/TIA-568A, ISO 11801 и EN50173, то есть приобрел международный статус.

Экранированные витые пары используются также в кабеле **IBM Type 2**, который представляет кабель Type 1 с добавленными 2 парами неэкранированного провода для передачи голоса.

Для присоединения экранированных кабелей к оборудованию используются специальные разъемы конструкции IBM.

Не все типы кабелей стандарта IBM относятся к экранированным кабелям - некоторые определяют характеристики неэкранированного телефонного кабеля (Type 3) и оптоволоконного кабеля (Type 5).

2.2.3. Коаксиальные кабели

Существует большое количество типов коаксиальных кабелей, используемых в сетях различного типа - телефонных, телевизионных и компьютерных.

2.2.3.1. RG-8 и **RG-11** - «толстый» коаксиальный кабель, разработанный для сетей Ethernet l0Base-5. Имеет волновое сопротивление 50 Ом и внешний диаметр 0,5 дюйма (около 12 мм). Этот кабель имеет достаточно толстый внутренний проводник диаметром 2,17 мм, который обеспечивает хорошие механические и электрические характеристики (затухание на частоте 10 МГц - не хуже 18 дБ/км). Зато этот кабель сложно монтировать - он плохо гнется.

2.2.3.2. RG-58/U, RG-58A/U и **RG-58C/U** − разновидности «тонкого» коаксиального кабеля для сетей Ethernet l0Base-2. Кабель RG-58/U имеет сплошной внутренний проводник, а кабель RG-58A/U − многожильный. Кабель RG-58C/U проходит «военную приемку». Все эти разновидности кабеля имеют волновое сопротивление 50 Ом, но обладают худшими механическими и электрическими характеристиками по сравнению с «толстым» коаксиальным кабелем. Тонкий внутренний проводник 0,89 мм не так прочен, зато обладает гораздо большей гибкостью, удобной при монтаже. Затухание в этом типе кабеля выше, чем в «толстом» коаксиальном кабеле, что приводит к необходимости уменьшать длину кабеля для получения одинакового затухания в сегменте. Для соединения кабелей с оборудованием используется разъем типа BNC.

2.2.3.3. RG-59 − телевизионный кабель с волновым сопротивлением 75 Ом. Широко применяется в кабельном телевидении.

2.2.3.4. RG-62 − кабель с волновым сопротивлением 93 Ома, использовался в сетях ArcNet, оборудование которых сегодня практически не выпускается. Коаксиальные кабели с волновым сопротивлением 50 Ом (то есть «тонкий» и «толстый») описаны в стандарте EIA/TIA-568. Новый стандарт EIA/TIA-568A коаксиальные кабели не описывает, как морально устаревшие.

2.2.4. Волоконно-оптические кабели

Волоконно-оптические кабели состоят из центрального проводника света (сердцевины) - стеклянного волокна, окруженного другим слоем стекла - оболочкой, обладающей меньшим показателем преломления, чем сердцевина. Распространяясь по сердцевине, лучи света не выходят за ее пределы, отражаясь от покрывающего слоя оболочки. В зависимости от распределения показателя преломления и от величины диаметра сердечника различают:

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

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

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

В многомодовых кабелях во внутреннем проводнике одновременно существует несколько световых лучей, отражающихся от внешнего проводника под разными углами. Угол отражения луча называется модой луча. В

многомодовых кабелях с плавным изменением коэффициента преломления режим распространения каждой моды имеет более сложный характер.

Многомодовые кабели имеют более узкую полосу пропускания − 500 ÷ 800 МГц/км. Сужение полосы происходит из-за потерь световой энергии при отражениях, а также из-за интерференции лучей разных мод.

В качестве источников излучения света в волоконно-оптических кабелях применяются: светодиоды; полупроводниковые лазеры.

Для одномодовых кабелей применяются только полупроводниковые лазеры, так как при таком малом диаметре оптического волокна световой поток, создаваемый светодиодом, невозможно без больших потерь направить в волокно. Для многомодовых кабелей используются более дешевые светодиодные излучатели.

Для передачи информации применяется свет с длиной волны 1550 нм (1,55 мкм), 1300 нм (1,3 мкм) и 850 нм (0,85 мкм). Светодиоды могут излучать свет с длиной волны 850 нм и 1300 нм. Излучатели с длиной волны 850 нм существенно дешевле, чем излучатели с длиной волны 1300 нм, но полоса пропускания кабеля для волн 850 нм уже, например 200 МГц/км вместо 500 МГц/км.

Лазерные излучатели работают на длинах волн 1300 и 1550 нм. Быстродействие современных лазеров позволяет модулировать световой поток с частотами 10 ГГц и выше. Лазерные излучатели создают когерентный поток света, за счет чего потери в оптических волокнах становятся меньше, чем при использовании некогерентного потока светодиодов.

Использование только нескольких длин волн для передачи информации в оптических волокнах связанно с особенностью их амплитудно-частотной характеристики. Именно для этих дискретных длин волн наблюдаются ярко выраженные максимумы передачи мощности сигнала, а для других волн затухание в волокнах существенно выше.

Волоконно-оптические кабели присоединяют к оборудованию разъемами MIC, ST и SC.

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

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

2.3. Структурированная кабельная система

Кабельная система составляет фундамент любой компьютерной сети. От ее качества зависят все основные свойства сети.

Структурированная кабельная система (Structured Cabling System, SCS) представляет собой своего рода «конструктор», с помощью которого проектировщик сети строит нужную ему конфигурацию из стандартных кабелей, соединенных стандартными разъемами и коммутируемых на стандартных кроссовых панелях. При необходимости конфигурацию связей можно легко изменить, что позволяет создавать регулярные, легко расширяемые структуры связей в вычислительных сетях.

При построении структурированной кабельной системы подразумевается, что каждое рабочее место на предприятии должно быть оснащено розетками для подключения телефона и компьютера, даже если в данный момент этого не требуется. Хорошая структурированная кабельная система строится избыточной, что бы изменения в подключении новых устройств можно было производить за счет перекоммутации уже проложенных кабелей.

Структурированная кабельная система планируется и строится иерархически, с главной магистралью и многочисленными ответвлениями от нее.

Типичная иерархическая структура структурированной кабельной системы включает:

- горизонтальные подсистемы (в пределах одного этажа соединяют кроссовый шкаф с розетками пользователей);
- вертикальные подсистемы (внутри здания соединяют кроссовые шкафы каждого этажа с центральной аппаратной здания);
- подсистему кампуса (в пределах одной территории соединяет несколько зданий с главной аппаратной всего кампуса. Эта часть кабельной системы обычно называется магистралью).

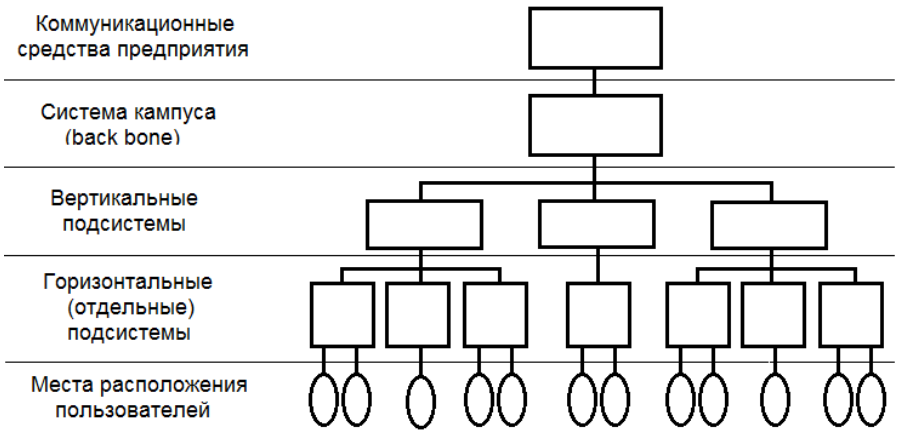


Рис.2.2. Иерархическая схема структурированной кабельной системы

Преимущества использования структурированной кабельной системы:

- **Универсальность.** Структурированная кабельная система при продуманной организации может стать единой средой для передачи компьютерных данных в локальной вычислительной сети, организации локальной телефонной сети, передачи видеоинформации и даже передачи сигналов от датчиков пожарной безопасности или охранных систем. Это позволяет автоматизировать многие процессы контроля, мониторинга и управления хозяйственными службами и системами жизнеобеспечения предприятия.

- **Увеличение срока службы**. Срок морального старения хорошо структурированной кабельной системы может составлять 10-15 лет.

- **Уменьшение стоимости добавления новых пользователей** и изменения их мест размещения. При таком подходе все работы по добавлению или перемещению пользователя сводятся к подключению компьютера к уже имеющейся прозапас розетке.

- **Возможность легкого расширения сети**. Структурированная кабельная система является модульной, поэтому ее легко расширять. Так, к магистрали можно добавить новую подсеть, не оказывая никакого влияния на уже существующие подсети. Можно заменить в отдельной подсети тип кабеля независимо от остальной части сети. Структурированная кабельная система является основой для деления сети на легко управляемые логические сегменты, так как она сама уже разделена на физические сегменты.

- **Обеспечение более эффективного обслуживания.** Структурированная кабельная система облегчает обслуживание и поиск неисправностей. Отказ одного сегмента не действует на другие, так как объединение сегментов осуществляется с помощью коммутаторов, которые локализуют неисправный участок.

- **Надежность.** Структурированная кабельная система имеет повышенную надежность, поскольку производитель такой системы гарантирует не только качество ее отдельных компонентов, но и их совместимость.

2.3.1. Выбор типа кабеля для горизонтальных подсистем

Разработка структурированной кабельной системы начинается с горизонтальных подсистем, так как именно к ним подключаются конечные пользователи. При этом есть выбор между экранированной витой парой, неэкранированной витой парой, коаксиальным кабелем и волоконно-оптическим кабелем. Возможно использование и беспроводных линий связи.

Горизонтальная подсистема характеризуется большим количеством ответвлений кабеля, так как его нужно провести к каждой пользовательской розетке, причем и в тех комнатах, где пока компьютеры в сеть не объединяются. Поэтому к кабелю, используемому в горизонтальной проводке, предъявляются повышенные требования к удобству выполнения ответвлений, а также удобству его прокладки в помещениях. На этаже обычно устанавливается кроссовая панель, которая позволяет с помощью коротких отрезков кабеля, оснащенного разъемами, провести переключение соединений между пользовательским оборудованием и коммутаторами.

При выборе кабеля принимаются во внимание следующие характеристики: полоса пропускания, расстояние, физическая защищенность, электромагнитная помехозащищенность, стоимость. Кроме того, при выборе кабеля нужно учитывать, какая кабельная система уже установлена на предприятии, а также какие тенденции и перспективы существуют на рынке в данный момент.

Преобладающим кабелем для горизонтальной подсистемы является неэкранированная витая пара категории 5.

2.3.2. Выбор типа кабеля для вертикальных подсистем

Кабель вертикальной (или магистральной) подсистемы, которая соединяет этажи здания, должен передавать данные на небольшие расстояния, но с большей скоростью по сравнению с кабелем горизонтальной подсистемы.

Для вертикальной подсистемы выбор кабеля в настоящее время ограничивается тремя вариантами:

- Оптоволокно - отличные характеристики пропускной способности, расстояния и защиты данных; устойчивость к электромагнитным помехам; может передавать голос, видеоизображение и данные. Но сравнительно дорого, сложно выполнять ответвления.

- Толстый коаксиал - хорошие характеристики пропускной способности, расстояния и защиты данных. Но с ним сложно работать.

- Широкополосный кабель, используемый в кабельном телевидении, - хорошие показатели пропускной способности и расстояния; может передавать голос, видео и данные. Но очень сложно работать и требуются большие затраты во время эксплуатации.

Применение волоконно-оптического кабеля в вертикальной подсистеме имеет рад преимуществ. Он передает данные на значительно большие расстояния без необходимости регенерации сигнала. Он имеет меньший диаметр, поэтому может быть проложен в более узких местах. Оптоволоконный кабель не чувствителен к электромагнитным и радиочастотным помехам, в отличие от медного коаксиального кабеля. Это делает оптоволоконный кабель идеальной средой передачи данных для промышленных сетей. Оптоволоконному кабелю не страшна молния, поэтому он хорош для внешней прокладки. Он обеспечивает более высокую степень защиты от несанкционированного доступа, так как ответвление гораздо легче обнаружить, чем в случае медного кабеля.

Недостатки - волоконно-оптический кабель дороже, чем медный кабель, дороже обходится и его прокладка. Оптоволоконный кабель менее прочный, чем коаксиальный. Инструменты, применяемые при прокладке и тестировании оптоволоконного кабеля, имеют высокую стоимость и сложны в работе. Присоединение коннекторов к оптоволоконному кабелю требует большого искусства и времени, а следовательно, дорого.

Для уменьшения стоимости построения межэтажной магистрали на оптоволокне некоторые компании, предлагают кабельную систему с одним коммутационным центром. При этом все оптические кабели расходятся из единого кроссового шкафа прямо к разъемам конечного оборудования - коммутаторов, концентраторов или сетевых адаптеров с оптоволоконными трансиверами.

2.3.2. Выбор типа кабеля для подсистемы кампуса

Как и для вертикальных подсистем, оптоволоконный кабель является наилучшим выбором для подсистем нескольких зданий, расположенных в радиусе нескольких километров. Для этих подсистем также подходит толстый коаксиальный кабель. При выборе кабеля для кампуса нужно учитывать воздействие среды на кабель вне помещения. Для предотвращения поражения молнией лучше выбрать для внешней проводки неметаллический оптоволоконный кабель. По многим причинам внешний кабель производится в полиэтиленовой защитной оболочке высокой плотности. При подземной прокладке кабель должен иметь специальную влагозащитную оболочку (от дождя и подземной влаги), а также металлический защитный слой от грызунов и вандалов. Влагозащитный кабель имеет прослойку из инертного газа между диэлектриком, экраном и внешней оболочкой. Кабель для внешней прокладки не подходит для прокладки внутри зданий, так как при сгорании он выделяет большое количество токсичных газов и дыма.

Раздел 3. СТАНДАРТЫ И ПРОТОКОЛЫ ВЫЧИСЛИТЕЛЬНЫХ СЕТЕЙ

3.1. Структура стандартов IEEE 802.X

Стандарты семейства IEEE 802.X охватывают только два нижних уровня семи-уровневой модели OSI - физический и канальный. Это связано с тем, что именно эти уровни в наибольшей степени отражают специфику локальных сетей. Старшие уровни, начиная с сетевого, в значительной степени имеют общие черты как для локальных, так и для глобальных сетей.

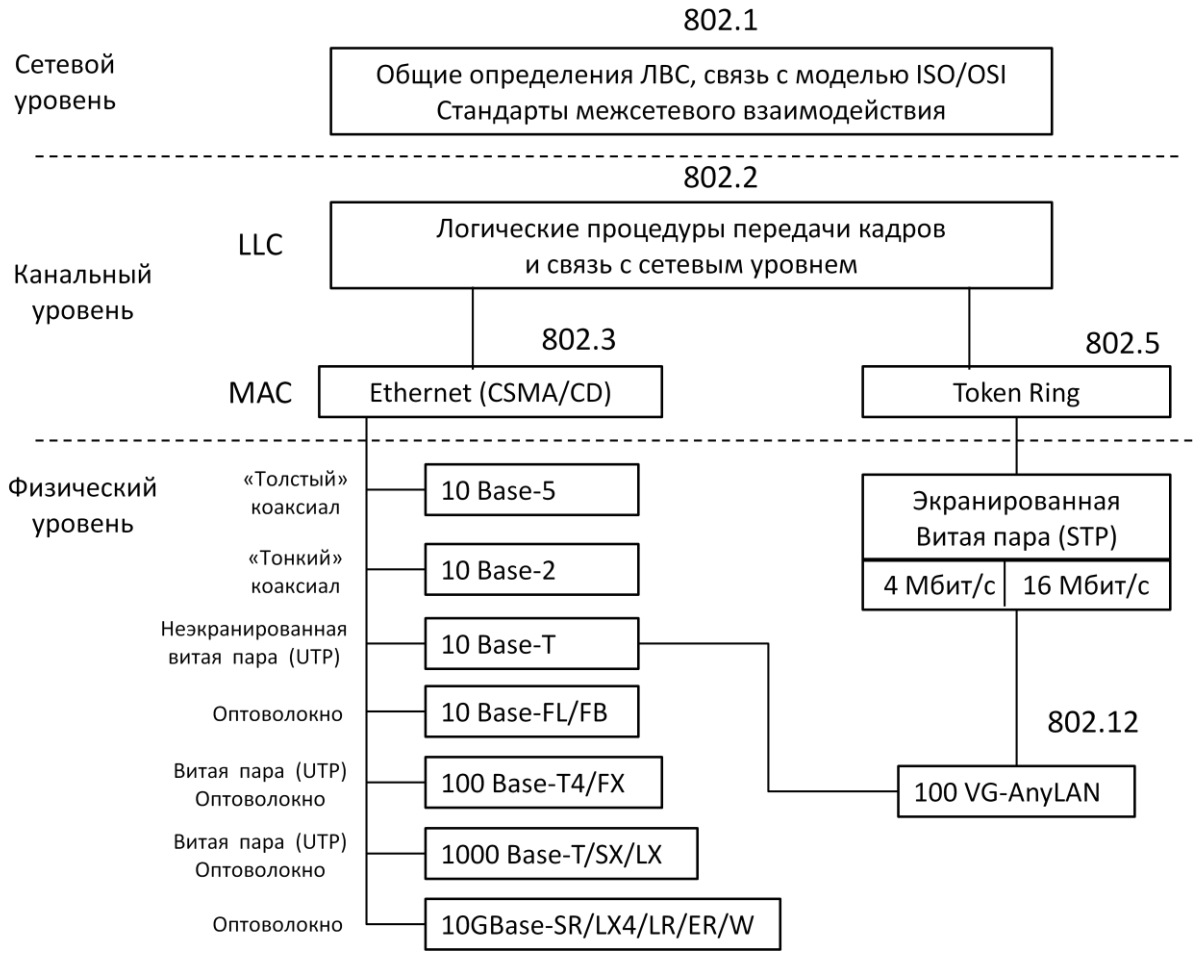


Рис.3.1 Стандарты вычислительных сетей

Описание каждой технологии разделено на две части: описание уровня MAC и описание физического уровня. Практически у каждой технологии единственному протоколу уровня MAC соответствует несколько вариантов протоколов физического уровня. Специфика локальных сетей заключается в разделении канального уровня (Data Link Layer) на два подуровня, которые часто называют также уровнями:

- логической передачи данных (Logical Link Control, LLC);
- управления доступом к среде (Media Access Control, MAC).

Уровень **MAC** появился из-за существования в локальных сетях разделяемой среды передачи данных. Именно этот уровень обеспечивает

корректное совместное использование общей среды, предоставляя ее в соответствии с определенным алгоритмом в распоряжение той или иной станции сети. После того как доступ к среде получен, ею может пользоваться более высокий уровень - уровень LLC, организующий передачу логических единиц данных, кадров информации, с различным уровнем качества транспортных услуг.

В современных локальных сетях получили распространение несколько протоколов уровня MAC, реализующих различные алгоритмы доступа к разделяемой среде. Эти протоколы полностью определяют специфику таких технологий, как Ethernet, Fast Ethernet, Gigabit Ethernet, Token Ring, FDDI, l00VG-AnyLAN.

Уровень **LLC** отвечает за передачу кадров данных между узлами с различной степенью надежности, а также реализует функции интерфейса с прилегающим к нему сетевым уровнем. Именно через уровень LLC сетевой протокол запрашивает у канального уровня нужную ему транспортную операцию с нужным качеством. На уровне LLC существует несколько режимов работы, отличающихся наличием или отсутствием на этом уровне процедур восстановления кадров в случае их потери или искажения, то есть отличающихся качеством транспортных услуг этого уровня.

Протоколы уровней MAC и LLC взаимно независимы - каждый протокол уровня MAC может применяться с любым протоколом уровня LLC, и наоборот.

Над канальным уровнем всех технологий изображен общий для них протокол LLC, поддерживающий несколько режимов работы, но независимый от выбора конкретной технологии. Стандарт LLC курирует подкомитет 802.2. Даже технологии, стандартизованные не в рамках комитета 802, ориентируются на использование протокола LLC, определенного стандартом 802.2, например протокол FDDI, стандартизованный ANSI.

Стандарты 802.1 носят общий для всех технологий характер. В подкомитете 802.1 были разработаны общие определения локальных сетей и их свойств, определена связь трех уровней модели IEEE 802 с моделью OSI. Наиболее практически важными являются стандарты, которые описывают взаимодействие между собой различных технологий, а также стандарты по построению более сложных сетей на основе базовых топологий. Эта группа стандартов носит общее название стандартов межсетевого взаимодействия (internetworking).

Сюда входят:

- стандарт 802.1D, описывающий логику работы моста/коммутатора;
- стандарт 802.1H, определяющий работу транслирующего моста, который может без маршрутизатора объединять сети Ethernet и FDDI, Ethernet и Token Ring и т. п.;

- стандарт 802.1Q, определяет способ построения виртуальных локальных сетей VLAN в сетях на основе коммутаторов.

Стандарты 802.3, 802.4, 802.5 и 802.12 описывают технологии локальных сетей, которые появились в результате улучшений фирменных технологий, легших в их основу. Так, основу стандарта 802.3 составила технология Ethernet, разработанная компаниями Digital, Intel и Xerox (или Ethernet DIX), стандарт 802.4 появился как обобщение технологии ArcNet компании Datapoint Corporation, а стандарт 802.5 в основном соответствует технологии Token Ring компании IBM.

Сегодня комитет 802 включает:

- 802.1 - Internetworking - объединение сетей;
- 802.2 - Logical Link Control, LLC - управление логической передачей данных;
- 802.3 – Ethernet с методом доступа CSMA/CD;
- 802.4 – Token Bus LAN - локальные сети с методом доступа Token Bus;
- 802.5 – Token Ring LAN - локальные сети с методом доступа Token Ring;
- 802.6 – Metropolitan Area Network, MAN - сети мегаполисов;
- 802.7 – Broadband Technical Advisory Group - техническая консультационная группа по широкополосной передаче;
- 802.8 – Fiber Optic Technical Advisory Group - техническая консультационная группа по волоконно-оптическим сетям;
- 802.9 – Integrated Voice and data Networks - интегрированные сети передачи голоса и данных;
- 802.10 – Network Security - сетевая безопасность;
- 802.11 – Wireless Networks - беспроводные сети Wi-Fi;
- 802.12 – Demand Priority Access LAN, l00VG-AnyLAN - локальные сети с методом доступа по требованию с приоритетами;
- 802.15 – Wireless Networks - беспроводные сети Bluetooth;
- 802.16 – Wireless Networks - беспроводные сети WiMAX;
- 802.17 – Адаптивные, кольцевые, высокоскоростные сети;
- 802.22 – Wireless Regional Area Network - беспроводные сети «White space».

При организации взаимодействия узлов в локальных сетях основная роль отводится классическим технологиям Ethernet, Token Ring, FDDI, основанным на использовании разделяемых сред. Разделяемые среды поддерживаются и новыми технологиями - Fast Ethernet, l00VG-AnyLAN, Gigabit Ethernet, 10GE.

Современной тенденцией является частичный или полный отказ от разделяемых сред: соединение узлов индивидуальными связями (например, в технологии ATM), широкое использование коммутируемых связей и микросегментации. Еще одна важная тенденция - появление полнодуплексного режима работы практически для всех технологий локальных сетей.

3.2. Стек протоколов TCP/IP

3.2.1. Многоуровневая структура стека TCP/IP

В настоящее время стек TCP/IP является самым популярным средством организации составных сетей. В отличие от модели OSI/ISO, в стеке TCP/IP определены 4 уровня. Каждый из этих уровней несет на себе некоторую нагрузку по решению основной задачи - организации надежной и производительной работы составной сети, части которой построены на основе разных сетевых технологий.

Уровень I	Прикладной уровень
Уровень II	Основной (транспортный) уровень
Уровень III	Уровень межсетевого взаимодействия
Уровень IV	Уровень сетевых интерфейсов

Рис.3.2. Уровни стека TCP/IP

3.2.1.1. Прикладной уровень

Прикладной уровень объединяет все службы, предоставляемые системой пользовательским приложениям, и реализуется программными системами, построенными в архитектуре клиент-сервер, базирующимися на протоколах нижних уровней. В отличие от протоколов остальных трех уровней, протоколы прикладного уровня занимаются деталями конкретного приложения и «не интересуются» способами передачи данных по сети. Этот уровень постоянно расширяется Telnet, FTP, TFTP, DNS, SNMP, HTTP.

3.2.1.2. Основной уровень

Обеспечение надежной информационной связи между двумя конечными узлами - решает основной уровень стека TCP/IP, называемый также транспортным. На этом уровне функционируют протокол управления передачей TCP (Transmission Control Protocol) и протокол дейтаграмм пользователя UDP (User Datagram Protocol).

Протокол TCP обеспечивает надежную передачу сообщений между удаленными прикладными процессами за счет образования логических соединений. Этот протокол позволяет равноранговым объектам на компьютере-отправителе и компьютере-получателе поддерживать обмен данными в дуплексном режиме. TCP позволяет без ошибок доставить сформированный на одном из компьютеров поток байт в любой другой компьютер, входящий в составную сеть. TCP делит поток байт на части - сегменты, и передает их ниже лежащему уровню межсетевого взаимодействия. После того как эти сегменты будут доставлены средствами уровня межсетевого взаимодействия в пункт назначения, протокол TCP снова соберет их в непрерывный поток байт.

Протокол UDP обеспечивает передачу прикладных пакетов дейтаграммным способом, как и главный протокол уровня межсетевого взаимодействия IP, и выполняет только функции связующего звена (мультиплексора) между сетевым протоколом и многочисленными службами прикладного уровня или пользовательскими процессами.

3.2.1.3. Уровень межсетевого взаимодействия

Стержнем всей архитектуры является уровень межсетевого взаимодействия, который реализует концепцию передачи пакетов в режиме без установления соединений, то есть дейтаграммным способом. Именно этот уровень обеспечивает возможность перемещения пакетов по сети, используя тот маршрут, который в данный момент является наиболее рациональным. Этот уровень также называют уровнем internet, указывая тем самым на основную его функцию - передачу данных через составную сеть.

Основным протоколом сетевого уровня (в терминах модели OSI) в стеке является протокол IP (Internet Protocol). Этот протокол изначально проектировался как протокол передачи пакетов в составных сетях, состоящих из большого количества локальных сетей, объединенных как локальными, так и глобальными связями.

К уровню межсетевого взаимодействия относятся и все протоколы, связанные с составлением и модификацией таблиц маршрутизации, такие как протоколы сбора маршрутной информации RIP (Routing Internet Protocol) и OSPF (Open Shortest Path First), а также протокол межсетевых управляющих сообщений ICMP (Internet Control Message Protocol), который предназначен для обмена информацией об ошибках между маршрутизаторами сети и узлом-источником пакета. С помощью специальных пакетов ICMP сообщает о невозможности доставки пакета, о превышении времени жизни или продолжительности сборки пакета из фрагментов, об аномальных величинах параметров, об изменении маршрута пересылки и типа обслуживания, о состоянии системы и т. п.

3.2.1.4. Уровень сетевых интерфейсов

Протоколы этого уровня должны обеспечивать интеграцию в составную сеть других сетей, то есть, сеть TCP/IP должна иметь средства включения в себя любой другой сети, какую бы внутреннюю технологию передачи данных эта сеть не использовала. Для каждой технологии, включаемой в составную сеть подсети, должны быть разработаны собственные интерфейсные средства. К таким интерфейсным средствам относятся протоколы инкапсуляции IP-пакетов уровня межсетевого взаимодействия в кадры локальных технологий.

Уровень сетевых интерфейсов в протоколах TCP/IP не регламентируется, но он поддерживает все популярные стандарты физического и канального уровней: для локальных сетей это Ethernet, Token Ring, FDDI, Fast Ethernet,

Gigabit Ethernet, 100VG-AnyLAN, для глобальных сетей - протоколы соединений «точка-точка» SLIP и PPP, протоколы территориальных сетей с коммутацией пакетов X.25, frame relay. Разработана также специальная спецификация, определяющая использование технологии ATM в качестве транспорта канального уровня.

3.2.2. Соответствие уровней стека TCP/IP семиуровневой модели ISO/OSI

Так как стек TCP/IP был разработан до появления модели взаимодействия открытых систем ISO/OSI, то, хотя он также имеет многоуровневую структуру, соответствие уровней стека TCP/IP уровням модели OSI достаточно условно. Рассматривая многоуровневую архитектуру TCP/IP, можно выделить в ней, подобно архитектуре OSI, уровни, функции которых зависят от конкретной технической реализации сети, и уровни, функции которых ориентированны на работу с приложениями.

<table>
<tr><td>7
6</td><td>WWW, Gopher, WAIS</td><td>SNMP</td><td>FTP</td><td>telnet</td><td>SMTP</td><td>TFTP</td><td>I</td></tr>
<tr><td>5
4</td><td colspan="5">TCP</td><td>UDP</td><td>II</td></tr>
<tr><td>3</td><td>IP</td><td>ICMP</td><td>RIP</td><td>OSPF</td><td colspan="2">ARP</td><td>III</td></tr>
<tr><td>2
1</td><td colspan="6">Не регламентируется Etemet, Token Ring, FDDI, X.25, SLIP, PPP</td><td>IV</td></tr>
</table>

OSI **TCP/IP**

Рис.3.3. Соответствие уровней стека TCP/IP семиуровневой модели OSI

Протоколы прикладного уровня стека TCP/IP работают на компьютерах, выполняющих приложения пользователей. Даже полная смена сетевого оборудования в общем случае не должна влиять на работу приложений, если они получают доступ к сетевым возможностям через протоколы прикладного уровня.

Протоколы транспортного уровня уже более зависят от сети, так как они реализуют интерфейс к уровням, непосредственно организующим передачу данных по сети. Однако, подобно протоколам прикладного уровня, программные модули, реализующие протоколы транспортного уровня, устанавливаются только на конечных узлах. Протоколы двух нижних уровней являются сетезависимыми, а следовательно, программные модули протоколов межсетевого уровня и уровня сетевых интерфейсов устанавливаются как на конечных узлах составной сети, так и на маршрутизаторах.

Каждый коммуникационный протокол оперирует с некоторой единицей передаваемых данных. Названия этих единиц иногда закрепляются стандартом, а чаще просто определяются традицией. В стеке TCP/IP за многие годы его существования образовалась устоявшаяся терминология в этой области.

Потоком называют данные, поступающие от приложений на вход протоколов транспортного уровня TCP и UDP.

Протокол TCP нарезает из потока данных *сегменты*.

Единицу данных протокола UDP часто называют *дейтаграммой* (или датаграммой). Дейтаграмма - это общее название для единиц данных, которыми оперируют протоколы без установления соединений. К таким протоколам относится и протокол межсетевого взаимодействия IP. Дейтаграмму протокола IP называют также пакетом.

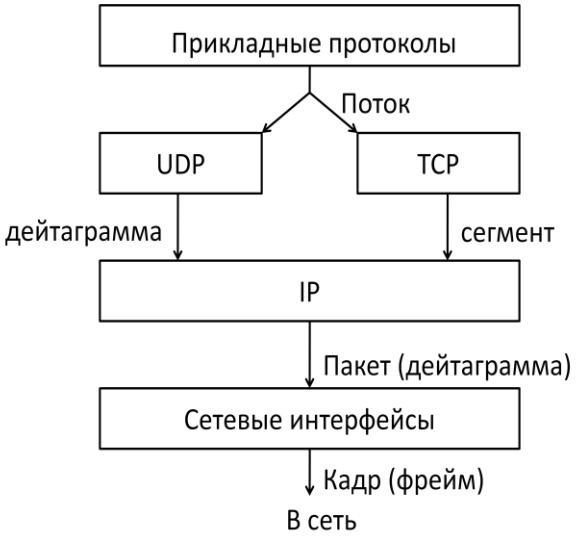


Рис. 3.4. Сегментация данных

В стеке TCP/IP принято называть кадрами (фреймами) единицы данных протоколов, на основе которых IP-пакеты переносятся через подсети составной сети. При этом не имеет значения, какое название используется для этой единицы данных в локальной технологии.

3.2.3. Установление соединения через TCP

Поскольку TCP является протоколом, ориентированным на предварительное соединение (connection-oriented), то сначала необходимо установить сессию между приложениями конечных устройств. Один узел инициализирует соединение, которое должно быть подтверждено другим. Модули программного обеспечения протокола двух операционных систем обмениваются сообщениями через сеть, чтобы проверить, что передача разрешена и что обе стороны готовы к ней.

Соединение между двумя устройствами производится в три этапа:

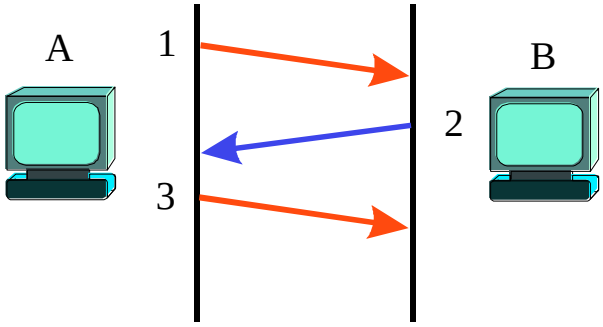


Рис.3.5. Установление соединения

Во-первых, инициализирующее устройство производит установление связи путем посылки устройству назначения запроса синхронизации SYN (1).

Во-вторых, принимающий узел подтверждает запрос синхронизации и задает свои параметры синхронизации в противоположном направлении ACK (2).

Третья часть – это подтверждение, посылаемое адресату назначения, что обе стороны согласны, чтобы соединение было установлено (3). После того, как соединение было установлено, начинается передача данных.

Такой механизм получил название трехэтапного установления связи (**Three-way handshake)**. Кроме того, оба узла должны согласовать начальную последовательность номеров передаваемых частей информации, что происходит через обмен сегментами, несущими служебный бит синхронизации (SYN) и начальные номера последовательности.

3.2.4. Структура заголовка пакета TCP

Контроль надежности реализуется путем задания ряда параметров в заголовке сегмента TCP, который содержит 20 байт.

<table>
<tr><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>10</td><td>11</td><td>12</td><td>13</td><td>14</td><td>15</td><td>16</td><td>17</td><td>18</td><td>19</td><td>20</td><td>21</td><td>22</td><td>23</td><td>24</td><td>25</td><td>26</td><td>27</td><td>28</td><td>29</td><td>30</td><td>31</td><td>32</td></tr>
<tr><td colspan="16">1. Source Port (номер порта источника)</td><td colspan="16">2. Destination Port (номер порта приёмника)</td></tr>
<tr><td colspan="32">3. Sequence number (порядок фрагментации и номер фрагмента)</td></tr>
<tr><td colspan="32">4. Acknowledgement Number (номера подтверждения принятых данных и ожидаемых) - 32</td></tr>
<tr><td colspan="4">5. H L</td><td colspan="6">6. Reserved</td><td colspan="6">7. Code Bits</td><td colspan="16">8. Window</td></tr>
<tr><td colspan="16">9. Checksum</td><td colspan="16">10. Urgent</td></tr>
<tr><td colspan="32">11. Options</td></tr>
<tr><td colspan="32">12. Data</td></tr>
</table>

Рис.3.6. Структура заголовка пакета TCP

Поля заголовка TCP сегмента определяют следующее:
1 - **Source Port** – номер порта, который посылает данные,
2 - **Destination Port** – номер порта, который принимает данные,
3 - **Sequence Number** – номер последовательности, используемый, чтобы гарантировать объединение (**reassemble**) частей (порций) данных в корректном порядке в устройстве назначения,
4 - **Acknowledgment Number** – 32 бита последовательного номера подтверждения принятых данных, следующая ожидаемая порция TCP,
5 - **HL** – число 32-разрядных слов в заголовке,
6 - **Reserved** – разряды поля, установленные в ноль,
7 - **Code bits** – 6 разрядов, выполняющих функции контроля, таких как установка и завершение сеанса,
8 - **Window** – число октетов в окне,
9 - **Checksum** – вычисленная контрольная сумма заголовка и поля данных,
10 - **Urgent pointer** – индицирует конец срочных данных,
11 - **Option** – Определяет максимальный размер TCP сегмента.
12 - **Data** – Данные протокола верхнего уровня.

3.2.5. Структура заголовка пакета UDP

Поскольку протокол UDP не обладает механизмами надежности, то она обеспечивается протоколами прикладного уровня. Однако небольшой размер заголовка UDP и отсутствие дополнительной обработки номера последовательности, окна и подтверждения получения данных повышают скорость передачи данных по сравнению с TCP.

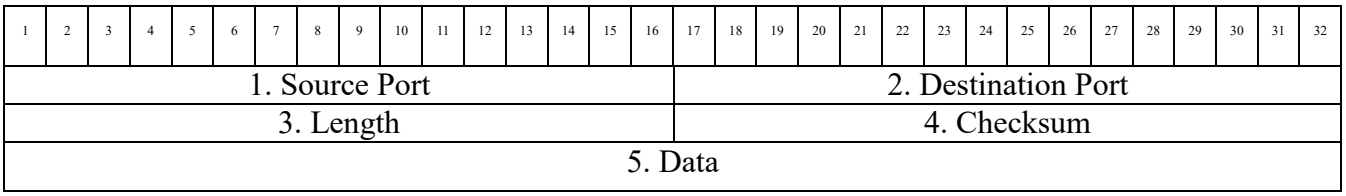


Рис.3.7. Структура заголовка пакета UDP

Поля UDP сегмента определяют следующее:

- **Source port** – номер порта, который посылает данные,
- **Destination port** – номер порта, который принимает данные,
- **Length** – число байт в заголовке и данных,
- **Checksum** –контрольная сумма заголовка и поля данных,
- **Data** – данные протокола верхнего уровня.

3.2.6. Структура заголовка пакета IP

Формат пакета сетевого протокола IP включает заголовок, состоящий из 12 полей общей длиной в 160 бит (20 байт), поля IP опции переменной длины и поля данных.

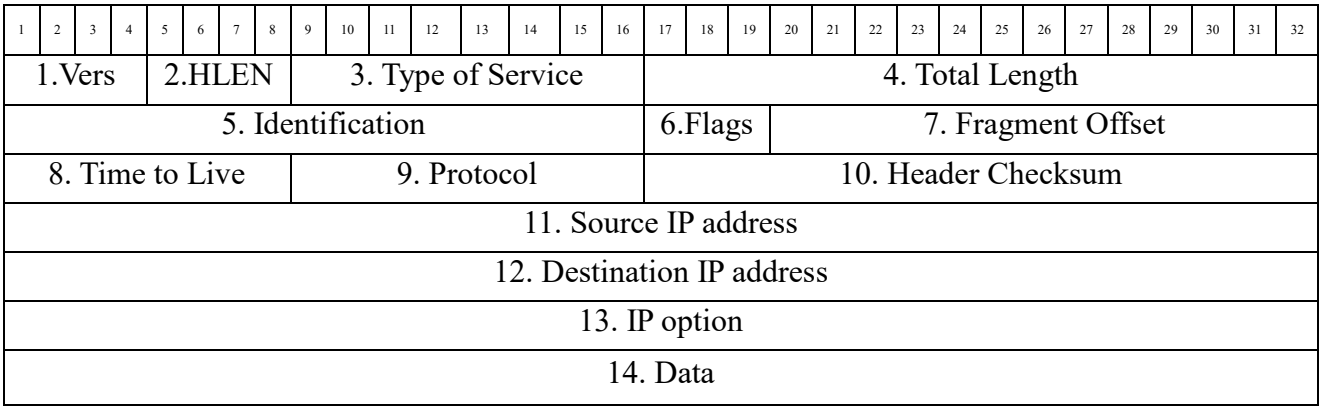


Рис.3.8. Структура заголовка пакета IP

1. Первое 4-х разрядное поле (Vers) задает номер версии протокола. В настоящее время действует версия 4 – IPv4, согласно которой длина адреса источника (Source IP address) и адреса назначения (Destination IP address) равна 32 разрядам (4 байтам).
2. HLEN – Длина заголовка – количество 32-разрядных слов в заголовке. Например, код в этом поле – 0101 означает, что заголовок содержит 5 слов по 32 разряда или 20 байт.
3. Поле типа сервиса (Type of Service – ToS) длиной 8 бит включает четыре идентификатора: трехразрядный идентификатор PR и одноразрядные D,

T, R. Идентификаторы определяют требования к метрике при прокладке маршрута. Идентификатор PR определяет тип пакета (нормальный, управляющий и др.) и в соответствие с этим задает приоритет. Установка 1 в разряде D означает требование минимизации задержки при передаче пакета; единица в разряде T означает требование максимальной пропускной способности; установка 1 в разряде R означает требование максимальной надежности.

4. Поле Total Length задает общую длину пакета, включая заголовок и поле данных. 16 разрядов поля позволяют задавать максимальную длину 64 Кбайт. Поскольку максимальная длина кадра в большинстве технологий локальных сетей меньше 64 Кбайт, например, в Ethernet она составляет 1500 байт, то большие пакеты разбивают на фрагменты. При **фрагментации** пакета используется информация 5, 6 и 7 полей, все фрагменты должны иметь: одинаковый идентификационный номер пакета; номер, определяющий порядок следования фрагмента при сборке пакета; дополнительную информацию.
5. Поле заголовка содержит идентификационный номер пакета.
6. Трехразрядное поле Flags содержит два одноразрядных флага фрагментации. Установка 1 в разряде DF запрещает маршрутизатору производить фрагментацию данного пакета. Единица в разряде MF указывает, что данный пакет не является последним.
7. 13-разрядное поле Fragment Offset помогает собрать фрагменты в единый пакет. Оно задает смещение в байтах поля данных этого пакета от начала общего поля данных исходного не фрагментированного пакета.
8. Из заданного значения Time to Live – время жизни (255 – максимум) при прохождении каждого маршрутизатора или каждую секунду вычитается 1. Таким образом ограничено число узлов, через которые может пройти пакет.
9. Поле Protocol указывает протокол верхнего уровня (TCP, UDP, OSPF и др.), которому будет передан принятый пакет после завершения IP процесса.
10. Поле контрольной суммы заголовка Header Checksum, пересчитывается в каждом маршрутизаторе заново.
11. Source IP address – адрес источника информации, длина 4 байта.
12. Destination IP address – адрес приемника информации, длина 4 байта.
13. Поле IP option позволяет поддерживать различные опции, например, опцию защиты информации. Поскольку это поле может иметь разную длину, то оно дополняется нулями до 32 разрядов.
14. Поле данных Data имеет длину более 64 разрядов.

3.2.7. Порты

Комбинация номера порта и IP-адреса образует комплексный адрес, так называемый сокет (**socket**), который определяет не только устройство, но и программное обеспечение, используемое для создания и обработки сообщения.

Номера портов делятся на несколько типов:

- известные номера (Well Known Ports), диапазон которых от 0 до 1023;
- зарегистрированные порты с номерами от 1024 до 49151;
- динамические частные порты с номерами от 49151 до 65535, которые обычно динамически присваиваются пользователям.

Номера известных портов заданы организацией Internet Assigned Numbers Authority (**IANA**). Номера известных портов назначаются службам сервиса, а затем закрепляются и опубликовываются в стандартах Internet (RFC 1700). Номера некоторых известных портов протокола TCP:

Таблица 3.1 Номера известных портов

Протоколы	FTP	Telnet	SMTP	HTTP	HTTPS	POP3
Порты	20, 21	23	25	80	443	110

В приложении протокола передачи файлов FTP используются два стандартных номера порта 20 и 21. Порт 20 используется для передачи данных, а порт 21 – для управления. Для передачи файлов в гипертекстовом формате HTTP кроме 80 порта в других протоколах так же широко используются порты 8080 и 8008.

Среди известных номеров протокола UDP наиболее распространенные: протокол TFTP – 69, RIP – 520.

Протоколы DNS с номером порта 53 и SNMP – 161 используются как протоколом TCP, так и UDP.

3.3. Протоколы маршрутизации

Маршрутизатор — это устройство, распределяющее пакеты по сети с помощью информации сетевого уровня. Маршрутизатор извлекает данные об адресации сетевого уровня из пакета данных. В маршрутизаторе также имеются алгоритмы, называемые протоколами маршрутизации, с помощью которых он строит таблицы. В соответствии с этими таблицами и определяется маршрут, по которому должен быть направлен пакет до пункта назначения. Если маршрутизатор является многопротокольным, т.е. понимает несколько форматов адресов сетевого уровня и может работать с несколькими протоколами маршрутизации, то он хранит отдельные таблицы маршрутизации для каждого из протоколов сетевого уровня.

Маршрутизируемый протокол — любой сетевой протокол, который обеспечивает в адресе сетевого уровня достаточно информации, чтобы позволить передать пакет от одного узла сети к другому на основе принятой схемы адресации. Маршрутизируемый протокол определяет формат и назначение полей внутри пакета. В общем случае пакеты переносятся от одной

конечной системы к другой. Примером маршрутизируемого протокола является межсетевой протокол IP.

Протокол маршрутизации — поддерживает маршрутизируемый протокол за счет предоставления механизмов коллективного использования маршрутной информации. Сообщения протокола маршрутизации циркулируют между маршрутизаторами. Протокол маршрутизации позволяет маршрутизаторам обмениваться информацией с другими маршрутизаторами с целью актуализации и ведения таблиц. Примерами протоколов маршрутизации являются протокол маршрутной информации (RIP), усовершенствованный протокол внутренней маршрутизации между шлюзами (EIGRP) и протокол маршрутизации с выбором кратчайшего пути (OSPF).

3.3.1. Статические и динамические маршруты

Статическая информация администрируется вручную. Сетевой администратор вводит ее в конфигурацию маршрутизатора. Если изменение в топологии сети требует актуализации статической информации, то администратор сети должен вручную обновить соответствующую запись о статическом маршруте. Статическая маршрутизация позволяет маршрутизаторам правильно направлять пакет от сети к сети. Маршрутизатор просматривает свою таблицу маршрутизации и, следуя содержащимся там статическим данным, ретранслирует пакет следующему маршрутизатору, который делает то же самое и ретранслирует пакет маршрутизатору, доставляющему пакет узлу получателя.

Маршрут по умолчанию — запись в таблице маршрутизации, которая используется для направления пакетов, которые не имеют в таблице маршрутизации явно указанного следующего перехода. Маршруты по умолчанию могут устанавливаться как результат статического конфигурирования, выполняемого администратором. Вместо сведений о каждой конкретной сети каждому маршрутизатору компании X сообщается маршрут по умолчанию, с помощью которого он может добраться до любого неизвестного пункта назначения, направляя пакет в сеть Internet.

Динамическая информация собирается после ввода администратором сети соответствующих команд, запускающих функцию динамической маршрутизации. Сведения о маршрутах обновляются процессом маршрутизации автоматически сразу после поступления из сети новой информации. Изменения в динамически получаемой информации распространяются между маршутизаторами как часть процесса актуализации данных. Динамическая маршрутизация обеспечивает более гибкое и автоматическое поведение. В соответствии с таблицей маршрутизации, генерируемой маршрутизатором, пакет может достичь своего пункта назначения по предпочтительному маршруту. Однако к пункту назначения возможен и другой путь. Протоколы динамической маршрутизации могут также перенаправлять трафик между различными путями в сети.

3.3.2. Операции динамической маршрутизации

Успех динамической маршрутизации зависит от двух основных функций маршрутизатора:

- Ведение таблицы маршрутизации.
- Своевременное распространение информации — в виде пакетов актуализации — среди других маршрутизаторов.

В обеспечении коллективного пользования информацией о маршрутах динамическая маршрутизация полагается на протокол маршрутизации. Протокол маршрутизации определяет набор правил, используемых маршрутизатором при его общении с соседними маршрутизаторами.

Например, протокол маршрутизации описывает следующее:

- как посылаются пакеты актуализации;
- какие сведения содержатся в таких пакетах актуализации;
- когда следует посылать эту информацию;
- как определять получателей этих пакетов актуализации.

3.3.3. Представление расстояния с помощью метрики

Когда алгоритм маршрутизации обновляет таблицу маршрутизации, его главной целью является определение наилучшей информации для включения в таблицу. Для каждого пути в сети алгоритм генерирует число, называемое метрикой. Как правило, чем меньше величина этого числа, тем лучше путь.

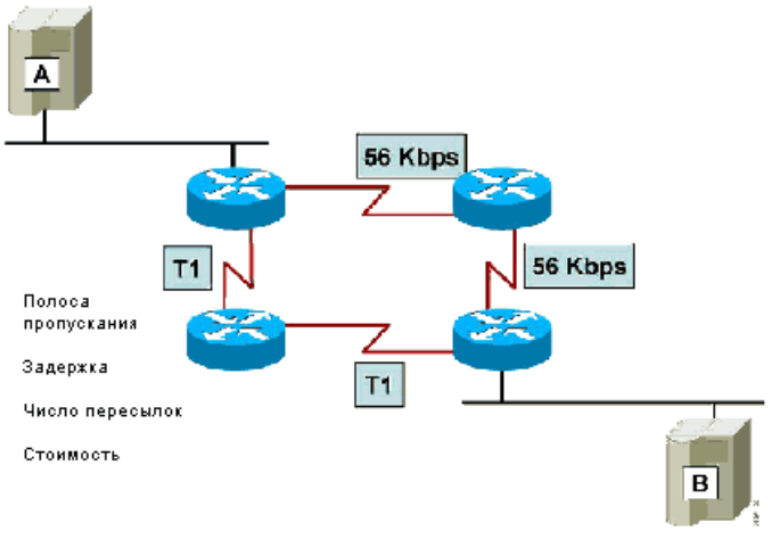


Рис. 3.9 Метрики маршрутизации

Метрики могут рассчитываться на основе одной характеристики пути. Объединяя несколько характеристик, можно рассчитывать и более сложные метрики. Наиболее общеупотребительными метриками, используемыми маршрутизаторами, являются следующие:

- Количество переходов — количество маршрутизаторов, которые должен пройти пакет, чтобы дойти до получателя. Чем меньше количество переходов, тем лучше путь. Для обозначения суммы переходов до пункта назначения используется термин длина пути.
- Полоса пропускания — пропускная способность канала передачи данных. Например, для арендуемой линии 64 Кбит/с обычно предпочтительным является канал типа E1 с полосой пропускания 2,048 Мбит/с.
- Задержка — продолжительность времени, требующегося для перемещения пакета от отправителя до получателю.
- Нагрузка — объем действий, выполняемый сетевым ресурсом, например маршрутизатором или каналом.
- Надежность — темп возникновения ошибок в каждом сетевом канале.
- Стоимость — произвольное значение, обычно основанное на величине полосы пропускания, денежной стоимости или результате других измерений, которое назначается сетевым администратором.

3.3.4. Протоколы динамической маршрутизации

Большинство алгоритмов маршрутизации можно свести к трем основным алгоритмам:

- Протокол на основе маршрутизации по вектору расстояния, в соответствии с которым определяются направление (вектор) и расстояние до каждого канала в сети.
- Протокол на основе оценки состояния канала (также называемый выбором наикратчайшего пути), при котором воссоздается точная топология всей сети (или по крайней мере той части, где размещается маршрутизатор).
- Гибридный подход, объединяющий алгоритмы с определением вектора расстояния и оценки состояния канала.

Алгоритм маршрутизации является основой динамической маршрутизации. Как только вследствие роста, реконфигурирования или отказа изменяется топология сети, база знаний о сети должна изменяться тоже; это прерывает маршрутизацию.

Необходимо, чтобы знания отражали точное и непротиворечивое представление о новой топологии. В том случае, когда все маршрутизаторы используют непротиворечивое представление топологии сети, имеет место сходимость. Сетевой комплекс сходится, когда все имеющиеся в нем маршрутизаторы работают с одной и той же информацией. Процесс и время, требующиеся для возобновления сходимости маршрутизаторов, меняются в зависимости от протокола маршрутизации. Для сети желательно обладать свойством быстрой сходимости, поскольку это уменьшает время, когда маршрутизаторы используют для принятия решений о выборе маршрута устаревшие знания, и эти решения могут быть неправильными, расточительными по времени или и теми и другими одновременно.

3.3.5. Алгоритмы маршрутизации по вектору расстояния

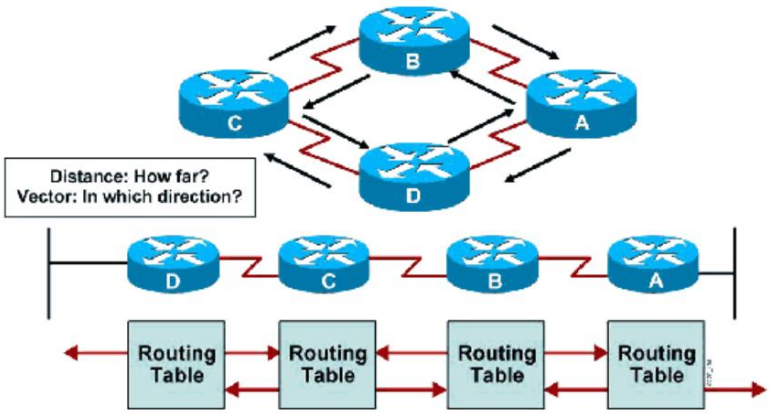


Рис. 3.10 Маршрутизации на основе вектора расстояния

Алгоритмы маршрутизации на основе вектора расстояния (также известные под названием алгоритмы Беллмана—Форда (Bellman-Ford algorithms)) предусматривают периодическую передачу копий таблицы маршрутизации от одного маршрутизатора другому. Регулярно посылаемые между маршрутизаторами пакеты актуализации сообщают обо всех изменениях топологии. Наиболее известные среди них RIP и RIP2.

Каждый маршрутизатор получает таблицу маршрутизации от своего соседа. Такой процесс выполняется пошагово между соседними маршрутизаторами во всех направлениях. Подобным образом алгоритм аккумулирует сетевые расстояния и поэтому способен поддерживать базу данных информации о топологии сети. Однако алгоритмы на основе вектора расстояния не позволяют маршрутизатору знать точную топологию всего сетевого комплекса.

3.3.6. Алгоритмы маршрутизации с учетом состояния канала связи

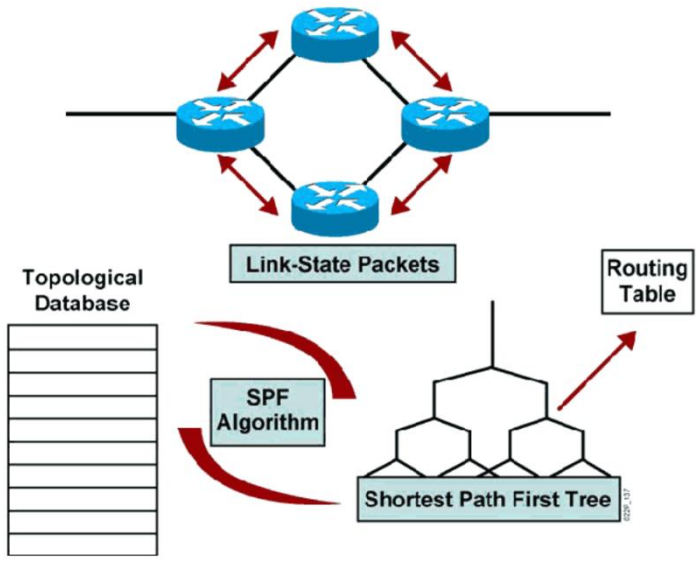


Рис. 3.11 Маршрутизация с учетом состояния канала связи

Алгоритмы маршрутизации с учетом состояния канала связи, также известные под названием алгоритмов выбора первого кратчайшего пути (shortest path first (SPF) algorithms), поддерживают сложную базу данных топологической информации. И если алгоритмы с маршрутизацией по вектору расстояния работают с неконкретной информацией о дальних сетях, то алгоритмы маршрутизации с учетом состояния канала собирают полные данные о дальних маршрутизаторах и о том, как они соединены друг с другом.

Для выполнения маршрутизации с учетом состояния канала связи используются сообщения объявлений о состоянии канала (link-state advertisements, LSA), база данных топологии, SPF-алгоритм, результирующее SPS-дерево и таблица маршрутизации, содержащая пути и порты к каждой сети.

3.3.7. Сравнение маршрутизации по вектору расстояния и маршрутизации с учетом состояния канала связи.

Маршрутизация по вектору расстояния	Маршрутизация с учётом состояния канала связи
Видит топологию сети глазами соседних маршрутизаторов	Получает общий вид топологии всей сети
Суммирует вектор расстояния от одного маршрутизатора к другому	Вычисляет кратчайший путь до других маршрутизаторов
Частые периодические обновления топологической информации, медленная сходимость	Обновления инициируются фактом изменения топологии, быстрая сходимость
Передаёт копии таблицы маршрутизации только соседним маршрутизаторам	Передаёт пакеты с информацией об актуальном состоянии канала связи всем другим маршрутизаторам

Сравнивать маршрутизацию по вектору расстояния и маршрутизацию с учетом стояния канала связи можно в нескольких ключевых областях:

- Процесс маршрутизации по вектору расстояния получает все топологические данные из информации, содержащейся в таблицах маршрутизации соседей. Процесс маршрутизации с учетом состояния канала связи получает широко представление обо всей топологии сетевого комплекса, собирая данные из всех необходимых LSA-пакетов.
- Процесс маршрутизации по вектору расстояния определяет лучший путь с помощью сложения получаемых метрик по мере того, как таблица движется от одного маршрутизатора к другому. При использовании маршрутизации с учетом состояния канала каждый маршрутизатор работает отдельно, вычисляя свой собственный кратчайший путь к пункту назначения.
- В большинстве протоколов маршрутизации по вектору расстояния пакеты актуализации, содержащие сведения об изменениях топологии, являются периодически посылаемыми пакетами актуализации таблиц маршрутизации. Эти таблицы передаются от одного маршрутизатора к другому, что обычно приводит к более медленной сходимости.

- В протоколах маршрутизации с учетом состояния канала связи пакеты актуализации обычно генерируются и рассылаются по факту возникновения изменения топологии.
- Относительно небольшие LSA-пакеты передаются всем другим маршрутизаторам, что, как правило, приводит к более быстрой сходимости при любом изменении топологии сетевого комплекса.

3.4. Технология Ethernet (IEEE 802.3)

В зависимости от типа физической среды стандарт IEEE 802.3 имеет различные модификации - l0Base-5, l0Base-2, l0Base-T, l0Base-FL, l0Base-FB.

Для передачи двоичной информации по кабелю для всех вариантов физического уровня технологии Ethernet, обеспечивающих пропускную способность 10 Мбит/с, используется манчестерский код. (1−10, 0−01)

Все виды стандартов Ethernet (в том числе Fast Ethernet и Gigabit Ethernet) используют один и тот же метод разделения среды передачи данных - метод коллективного доступа с опознаванием несущей и обнаружением коллизий (carrier-sense-multiply-access with collision detection, CSMA/CD).

3.4.1. Метод доступа CSMA/CD

Этот метод применяется исключительно в сетях с логической общей шиной, которая может быть использована для передачи данных между любыми двумя узлами сети. Одновременно все компьютеры сети имеют возможность немедленно (с учетом задержки распространения сигнала по физической среде) получить данные, которые любой из компьютеров начал передавать на общую шину. Кабель, к которому подключены все станции, работает в режиме коллективного доступа (Multiply Access, MA).

Все данные, передаваемые по сети, помещаются в кадры определенной структуры и снабжаются уникальным адресом станции назначения (MAC-адрес).

Чтобы получить возможность передавать кадр, станция должна убедиться, что разделяемая среда свободна. Это достигается прослушиванием основной гармоники сигнала, которая также называется несущей частотой (carrier-sense, CS). Признаком незанятости среды является отсутствие на ней несущей частоты, которая при манчестерском способе кодирования равна 5÷10 МГц, в зависимости от последовательности единиц и нулей, передаваемых в данный момент.

Если среда свободна, то узел имеет право начать передачу кадра. Кадр данных всегда сопровождается преамбулой (preamble), которая состоит из 7 байт, состоящих из значений 10101010, и 8-го байта, равного 10101011. Преамбула нужна для вхождения приемника в побитовый и побайтовый синхронизм с передатчиком.

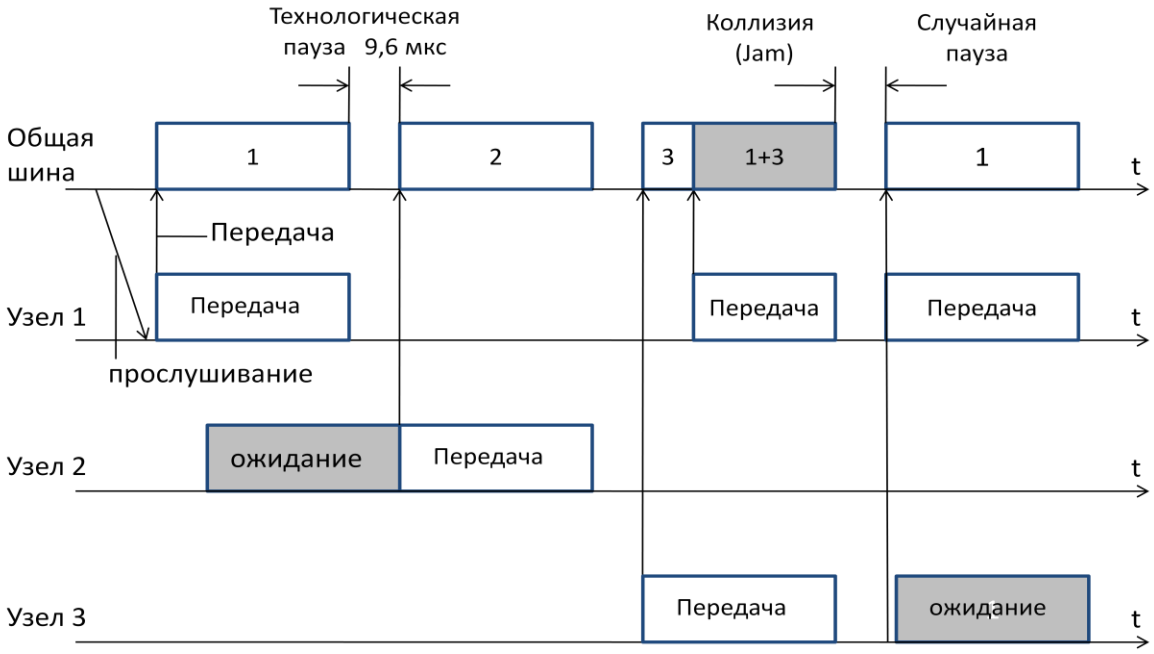


Рис.3.9. Метод доступа CSMA/CD

Все станции, подключенные к кабелю, могут распознать факт передачи кадра, и та станция, которая узнает собственный адрес в заголовках кадра, записывает его содержимое в свой внутренний буфер, обрабатывает полученные данные, передает их вверх по своему стеку, а затем посылает по кабелю кадр-ответ. Адрес станции источника содержится в исходном кадре, поэтому станция-получатель знает, кому нужно послать ответ.

После окончания передачи кадра все узлы сети обязаны выдержать технологическую паузу (Inter Packet Gap) в 9,6 мкс. Эта пауза, называемая также межкадровым интервалом, нужна для приведения сетевых адаптеров в исходное состояние, а также для предотвращения монопольного захвата среды одной станцией. После окончания технологической паузы узлы имеют право начать передачу своего кадра, так как среда свободна. Из-за задержек распространения сигнала по кабелю не все узлы строго одновременно фиксируют факт окончания передачи кадра узлом 1.

3.4.1.1. Домен коллизий

Домен коллизий (collision domain) - это часть сети Ethernet, все узлы которой распознают коллизию независимо от того, в какой части этой сети коллизия возникла. Сеть Ethernet, построенная на повторителях, всегда образует один домен коллизий. Домен коллизий соответствует одной разделяемой среде. Мосты, коммутаторы и маршрутизаторы делят сеть Ethernet на несколько доменов коллизий.

3.4.1.2. Возникновение коллизии

Механизм прослушивания среды и пауза между кадрами не гарантируют от возникновения такой ситуации, когда две или более станции одновременно решают, что среда свободна, и начинают передавать свои кадры. При этом

происходит коллизия (collision), так как содержимое обоих кадров сталкивается на общем кабеле и происходит искажение информации - методы кодирования, используемые в Ethernet, не позволяют выделять сигналы каждой станции из общего сигнала.

Коллизия - это нормальная ситуация в работе сетей Ethernet. Для возникновения коллизии не обязательно, чтобы несколько станций начали передачу абсолютно одновременно, такая ситуация маловероятна. Гораздо вероятней, что коллизия возникает из-за того, что один узел начинает передачу раньше другого, но до второго узла сигналы первого просто не успевают дойти к тому времени, когда второй узел решает начать передачу своего кадра. То есть коллизии - это следствие распределенного характера сети.

Чтобы корректно обработать коллизию, все станции одновременно наблюдают за возникающими на кабеле сигналами. Если передаваемые и наблюдаемые сигналы отличаются, то фиксируется обнаружение коллизии (collision detection, CD). Для увеличения вероятности скорейшего обнаружения коллизии всеми станциями сети станция, которая обнаружила коллизию, прерывает передачу своего кадра (в произвольном месте, возможно, и не на границе байта) и усиливает ситуацию коллизии посылкой в сеть специальной последовательности из 32 бит, называемой jam-последовательностью.

После этого обнаружившая коллизию передающая станция обязана прекратить передачу и сделать паузу в течение короткого случайного интервала времени. Затем она может снова предпринять попытку захвата среды и передачи кадра. Случайная пауза выбирается по определённому алгоритму и может принимать значения от 0 до 52,4 мс.

Если 16 последовательных попыток передачи кадра вызывают коллизию, то передатчик должен прекратить попытки и отбросить этот кадр.

Вероятность успешного получения в свое распоряжение общей среды зависит от загруженности сети, то есть от интенсивности возникновения в станциях потребности в передаче кадров.

Следует отметить, что метод доступа CSMA/CD вообще не гарантирует станции, что она когда-либо сможет получить доступ к среде. Конечно, при небольшой загрузке сети вероятность такого события невелика, но при коэффициенте использования сети, приближающемся к 1, такое событие становится очень вероятным. Этот недостаток метода случайного доступа - плата за его чрезвычайную простоту, которая сделала технологию Ethernet самой недорогой. Другие методы доступа - маркерный доступ сетей Token Ring и FDDI, метод Demand Priority сетей 100VG-AnyLAN - свободны от этого недостатка.

Все параметры протокола Ethernet подобраны таким образом, чтобы при нормальной работе узлов сети коллизии всегда четко распознавались. В

стандарте Ethernet принято, что минимальная длина поля данных кадра составляет 46 байт (что вместе со служебными полями дает минимальную длину кадра 64 байт, а вместе с преамбулой - 72 байт или 576 бит). Отсюда может быть определено ограничение на расстояние между станциями.

В 10-мегабитном Ethernet время передачи кадра минимальной длины равно 575 битовых интервалов, следовательно, время двойного оборота должно быть меньше 57,5 мкс. Расстояние, которое сигнал может пройти за это время, зависит от типа кабеля и для толстого коаксиального кабеля равно примерно 13 280 м. Учитывая, что за это время сигнал должен пройти по линии связи дважды, расстояние между двумя узлами не должно быть больше 6 635 м. В стандарте величина этого расстояния выбрана существенно меньше, с учетом других, более строгих ограничений.

С увеличением скорости передачи кадров, что имеет место в новых стандартах, базирующихся на том же методе доступа CSMA/CD, например Fast Ethernet, максимальное расстояние между станциями сети уменьшается пропорционально увеличению скорости передачи. В стандарте Fast Ethernet оно составляет около 210 м, а в стандарте Gigabit Ethernet оно было бы ограничено 25 метрами, если бы разработчики стандарта не предприняли некоторых мер по увеличению минимального размера пакета.

3.4.2. Параметры уровня MAC Ethernet

В табл. 3.1 приведены значения основных параметров процедуры передачи кадра стандарта 802.3, которые не зависят от реализации физической среды. Важно отметить, что каждый вариант физической среды технологии Ethernet добавляет к этим ограничениям свои, часто более строгие ограничения, которые также должны выполняться.

Таблица 3.2

Параметры	**Значения**
Битовая скорость	10 Мбит/с
Интервал отсрочки	512 битовых интервала
Межкадровый интервал	9,6 мкс
Максимальное число попыток передачи	16
Максимальное число возрастания диапазона паузы	10
Длина jam-последовательности	32 бита
Максимальная длина кадра (без преамбулы)	1518 байт
Минимальная длина кадра (без преамбулы)	64 байт (512 бит)
Длина преамбулы	64 бит
Минимальная длина случайной паузы после коллизии	0 битовых интервалов
Максимальная длина случайной паузы после коллизии	524 000 битовых интервалов
Максимальное расстояние между станциями сети	2500 м
Максимальное число станций в сети	1024

3.5. Технологии «Fast Ethernet» и «100VG-AnyLAN»

В связи с необходимостью увеличить скорость обмена данными в вычислительных сетях назрела необходимость в разработке «нового» Ethernet, то есть технологии, которая была бы такой же эффективной по соотношению цена/качество при производительности 100 Мбит/с. В результате поисков и исследований специалисты разделились на два лагеря, что привело к появлению двух новых технологий - Fast Ethernet и l00VG-AnyLAN. Они отличаются степенью преемственности с классическим Ethernet.

В центре дискуссий была проблема сохранения случайного метода доступа CSMA/CD. Предложение Fast Ethernet Alliance сохраняло этот метод и тем самым обеспечивало преемственность и согласованность сетей 10 Мбит/с и 100 Мбит/с. Коалиция HP и AT&T, которая имела поддержку значительно меньшего числа производителей в сетевой индустрии, чем Fast Ethernet Alliance, предложила совершенно новый метод доступа, названный Demand Priority - приоритетный доступ по требованию. Он существенно менял картину поведения узлов в сети, поэтому не смог вписаться в технологию Ethernet и стандарт 802.3, и для его стандартизации был организован новый комитет IEEE 802.12.

Осенью 1995 года обе технологии стали стандартами IEEE. Комитет IEEE 802.3 принял спецификацию Fast Ethernet в качестве стандарта 802.3u, который не является самостоятельным стандартом, а представляет собой дополнение к существующему стандарту 802.3 в виде глав с 21 по 30. Комитет 802.12 принял технологию l00VG-AnyLAN, которая использует новый метод доступа Demand Priority и поддерживает кадры двух форматов - Ethernet и Token Ring.

3.5.1. Физический уровень технологии Fast Ethernet

Все отличия технологии Fast Ethernet от Ethernet сосредоточены на физическом уровне. Уровни MAC и LLC в Fast Ethernet остались абсолютно теми же.

Официальный стандарт 802.3u установил три различных спецификации для физического уровня Fast Ethernet:

- 100Base-TX для двухпарного кабеля на неэкранированной витой паре UTP категории 5 или экранированной витой паре STP Type 1;
- 100Base-T4 для четырехпарного кабеля на неэкранированной витой паре UTP категории 3, 4 или 5;
- 100Base-FX для многомодового оптоволоконного кабеля, используются два волокна.

Форматы кадров технологии Fast Ethernetee отличаются от форматов кадров технологий 10-мегабитного Ethernet.

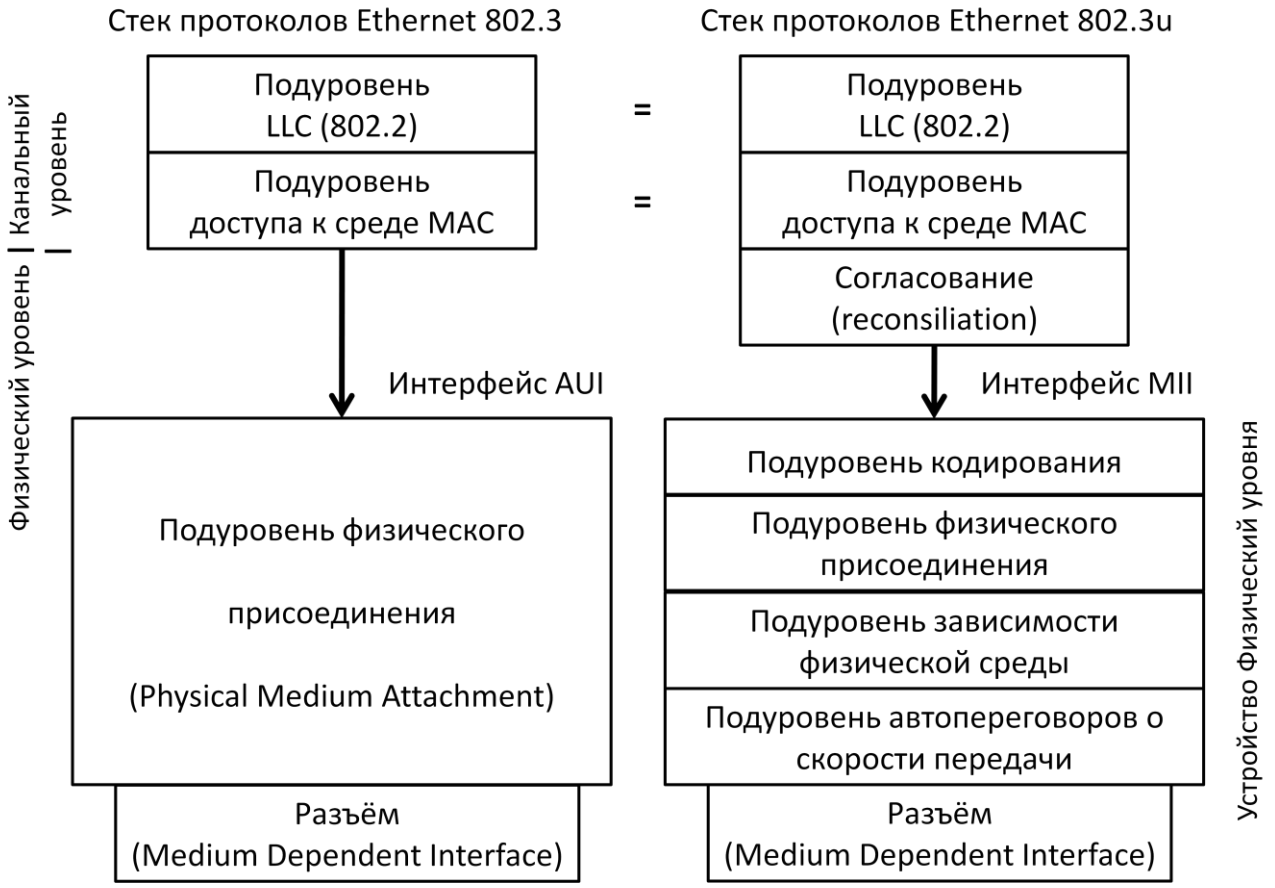


Рис.3.10. Сравнение физических уровней 802.3 и 802.3u

Межкадровый интервал равен 0,96 мкс, а битовый интервал равен 10 нс. Все временные параметры алгоритма доступа (интервал отсрочки, время передачи кадра минимальной длины и т. п.), измеренные в битовых интервалах, остались прежними, поэтому изменения в разделы стандарта, касающиеся уровня MAC, не вносились.

Признаком свободного состояния среды является передача по ней символа Idle соответствующего избыточного кода (а не отсутствие сигналов, как в стандартах Ethernet 10 Мбит/с). Физический уровень включает три элемента:

1. Уровень согласования (reconciliation sublayer) нужен для того, чтобы уровень MAC, рассчитанный на интерфейс AUI, смог работать с физическим уровнем через интерфейс MII;
2. Независимый от среды интерфейс (Media Independent Interface, MII);
3. Устройство физического уровня (Physical layer device, PHY), которое состоит, из нескольких подуровней:
   - подуровня логического кодирование данных, преобразующего поступающие от уровня MAC байты в символы кода 4B/5B или 8B/6T (оба кода используются в технологии Fast Ethernet);
   - подуровней физического присоединения и подуровня зависимости от физической среды (PMD), которые обеспечивают формирование

сигналов в соответствии с методом физического кодирования, например NRZI или MLT-3;

- подуровня автопереговоров, который позволяет двум взаимодействующим портам автоматически выбрать наиболее эффективный режим работы, например, полудуплексный или полнодуплексный (этот подуровень является факультативным).

Интерфейс MII поддерживает независимый от физической среды способ обмена данными между подуровнем MAC и подуровнем PHY. Этот интерфейс аналогичен по назначению интерфейсу AUI классического Ethernet за исключением того, что интерфейс AUI располагался между подуровнем физического кодирования сигнала (для любых вариантов кабеля использовался одинаковый метод физического кодирования - манчестерский код) и подуровнем физического присоединения к среде, а интерфейс MII располагается между подуровнем MAC и подуровнями кодирования сигнала, которых в стандарте Fast Ethernet три - FX, TX и T4.

Разъем MII в отличие от разъема AUI имеет 40 контактов, максимальная длина кабеля MII составляет один метр. Сигналы, передаваемые по интерфейсу MII, имеют амплитуду 5 В.

3.5.2 Физический уровень 100Base-FX - многомодовое оптоволокно, два волокна

Эта спецификация определяет работу протокола Fast Ethernet по многомодовому оптоволокну в полудуплексном и полнодуплексном режимах на основе схемы кодирования FDDI. Как и в стандарте FDDI, каждый узел соединяется с сетью двумя оптическими волокнами, идущими от приемника (Rx) и от передатчика (Tx).

Между спецификациями l00Base-FX и l00Base-TX есть много общего, поэтому общие для двух спецификаций свойства будут даваться под обобщенным названием l00Base-FX/TX.

В стандарте Fast Ethernet определен метод кодирования - 4B/5B. Этот метод уже показал свою эффективность в стандарте FDDI и без изменений перенесен в спецификацию l00Base-FX/TX. При этом методе каждые 4 бита данных подуровня MAC (называемых символами) представляются 5 битами. Избыточный бит позволяет применить потенциальные коды при представлении каждого из пяти бит в виде электрических или оптических импульсов. Существование запрещенных комбинаций символов позволяет отбраковывать ошибочные символы, что повышает устойчивость работы сетей с l00Base-FX/TX.

Для отделения кадра Ethernet от символов Idle используется комбинация символов Start Delimiter (пара символов J (11000) и K (10001) кода 4B/5B, а после завершения кадра перед первым символом Idle вставляется символ T.

Рис.3.11. Непрерывный поток данных спецификаций 100Base-FX/TX

После преобразования 4-битовых порций кодов MAC в 5-битовые порции физического уровня их необходимо представить в виде оптических или электрических сигналов в кабеле, соединяющем узлы сети. Спецификации l00Base-FX и l00Base-TX используют для этого различные методы физического кодирования - NRZI и MLT-3 соответственно (как и в технологии FDDI при работе через оптоволокно и витую пару).

3.5.3 Физический уровень 100Base-TX - витая пара DTP Cat 5 или STP Type 1, две пары

В качестве среды передачи данных спецификация l00Base-TX использует кабель UTP категории 5 или кабель STP Type 1. Максимальная длина кабеля в обоих случаях - 100 м.

Основные отличия от спецификации l00Base-FX - использование метода MLT-3 для передачи сигналов 5-битовых порций кода 4B/5B по витой паре, а также наличие функции автопереговоров (Auto-negotiation) для выбора режима работы порта. Схема автопереговоров позволяет двум соединенным физически устройствам, которые поддерживают несколько стандартов физического уровня, отличающихся битовой скоростью и количеством витых пар, выбрать наиболее выгодный режим работы. Обычно процедура автопереговоров происходит при подсоединении сетевого адаптера, который может работать на скоростях 10 и 100 Мбит/с, к концентратору или коммутатору.

Описанная ниже схема Auto-negotiation сегодня является стандартом технологии l00Base-T. До этого производители применяли различные собственные схемы автоматического определения скорости работы взаимодействующих портов, которые не были совместимы. Принятую в качестве стандарта схему Auto-negotiation предложила первоначально компания National Semiconductor под названием NWay.

Всего в настоящее время определено 5 различных режимов работы, которые могут поддерживать устройства l00Base-TX или 100Base-T4 на витых парах:

- l0Base-T - 2 пары категории 3;
- l0Base-T full-duplex - 2 пары категории 3;
- l00Base-TX - 2 пары категории 5 (или Type 1ASTP);
- 100Base-T4 - 4 пары категории 3;
- 100Base-TX full-duplex - 2 пары категории 5 (или Type 1A STP).

Режим l0Base-T имеет самый низкий приоритет при переговорном процессе, а полнодуплексный режим 100Base-T4 - самый высокий. Переговорный процесс происходит при включении питания устройства, а также может быть инициирован в любой момент модулем управления устройства.

Устройство, начавшее процесс auto-negotiation, посылает своему партнеру пачку специальных импульсов Fast Link Pulse burst (FLP), в котором содержится 8-битное слово, кодирующее предлагаемый режим взаимодействия, начиная с самого приоритетного, поддерживаемого данным узлом.

Если узел-партнер поддерживает функцию auto-negotuiation и также может поддерживать предложенный режим, он отвечает пачкой импульсов FLP, в которой подтверждает данный режим, и на этом переговоры заканчиваются. Если же узел-партнер может поддерживать менее приоритетный режим, то он указывает его в ответе, и этот режим выбирается в качестве рабочего. Таким образом, всегда выбирается наиболее приоритетный общий режим узлов.

Узел, который поддерживает только технологию l0Base-T, каждые 16 мс посылает манчестерские импульсы для проверки целостности линии, связывающей его с соседним узлом. Такой узел не понимает запрос FLP, который делает ему узел с функцией Auto-negotiation, и продолжает посылать свои импульсы. Узел, получивший в ответ на запрос FLP только импульсы проверки целостности линии, понимает, что его партнер может работать только по стандарту l0Base-T, и устанавливает этот режим работы и для себя.

3.5.4 Физический уровень 100Base-T4 - витая пара UTP Cat 3, четыре пары

Спецификация 100Base-T4 была разработана для того, чтобы можно было использовать для высокоскоростного Ethernet имеющуюся проводку на витой паре категории 3. Эта спецификация позволяет повысить общую пропускную способность за счет одновременной передачи потоков бит по всем 4 парам кабеля.

Спецификация 100Base-T4 появилась позже других спецификаций физического уровня Fast Ethernet. Разработчики этой технологии в первую очередь хотели создать физические спецификации, наиболее близкие к спецификациям l0Base-T и l0Base-F, которые работали на двух линиях передачи данных: двух парах или двух волокнах. Для реализации работы по двум витым парам пришлось перейти на более качественный кабель категории 5.

Вместо кодирования 4B/5B в этом методе используется кодирование 8B/6T, которое обладает более узким спектром сигнала и при скорости 33 Мбит/с укладывается в полосу 16 МГц витой пары категории 3 (при кодировании 4B/5B спектр сигнала в эту полосу не укладывается). Каждые 8 бит информации уровня MAC кодируются 6-ю троичными цифрами (ternary symbols), то есть цифрами, имеющими три состояния. Каждая троичная цифра

имеет длительность 40 нс. Группа из 6-ти троичных цифр затем передается на одну из трех передающих витых пар, независимо и последовательно.

Четвертая пара всегда используется для прослушивания несущей частоты в целях обнаружения коллизии. Скорость передачи данных по каждой из трех передающих пар равна 33,3 Мбит/с, поэтому общая скорость протокола 100Base-T4 составляет 100 Мбит/с. В то же время из-за принятого способа кодирования скорость изменения сигнала на каждой паре равна всего 25 Мбод, что и позволяет использовать витую пару категории 3.

На рис. 3.8 показано соединение порта MDI сетевого адаптера 100Base-T4 с портом MDI-X концентратора (приставка X говорит о том, что у этого разъема присоединения приемника и передатчика меняются парами кабеля по сравнению с разъемом сетевого адаптера, что позволяет проще соединять пары проводов в кабеле - без перекрещивания). Пара 1-2 всегда требуется для передачи данных от порта MDI к порту MDI-X, пара 3-6 -для приема данных портом MDI от порта MDI-X, а пары 4-5 и 7-8 являются двунаправленными и используются как для приема, так и для передачи, в зависимости от потребности.

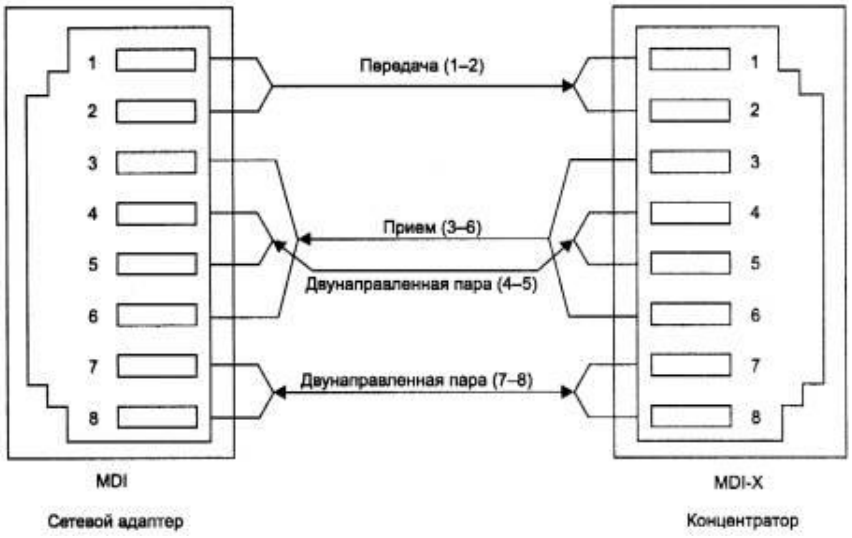


Рис.3.12. Соединение узлов по спецификации 100Base-T4

3.5.5 Особенности технологии 100VG-AnyLAN

В технологии 100VG-AnyLAN используется метод доступа Demand Priority, который обеспечивает более справедливое распределение пропускной способности сети по сравнению с методом CSMA/CD, Кроме того, этот метод поддерживает приоритетный доступ для синхронных приложений.

Кадры передаются не всем станциям сети, а только станции назначения.

В сети есть выделенный арбитр доступа - концентратор, и это заметно отличает данную технологию от других, в которых применяется распределенный между станциями сети алгоритм доступа.

Поддерживаются кадры двух технологий - Ethernet и Token Ring (именно это обстоятельство дало добавку AnyLAN в названии технологии).

Данные передаются одновременно по 4 парам кабеля UTP категории 3. По каждой паре данные передаются со скоростью 25 Мбит/с, что в сумме дает 100 Мбит/с. В отличие от Fast Ethernet в сетях 100VG-AnyLAN нет коллизий, поэтому удалось использовать для передачи все четыре пары стандартного кабеля категории 3. Для кодирования данных применяется код 5B/6B, который обеспечивает спектр сигнала в диапазоне до 16 МГц (полоса пропускания UTP категории 3) при скорости передачи данных 25 Мбит/с. Метод доступа Demand Priority основан на передаче концентратору функций арбитра, решающего проблему доступа к разделяемой среде. Сеть 100VG-AnyLAN состоит из центрального концентратора, называемого также корневым, и соединенных с ним конечных узлов и других концентраторов.

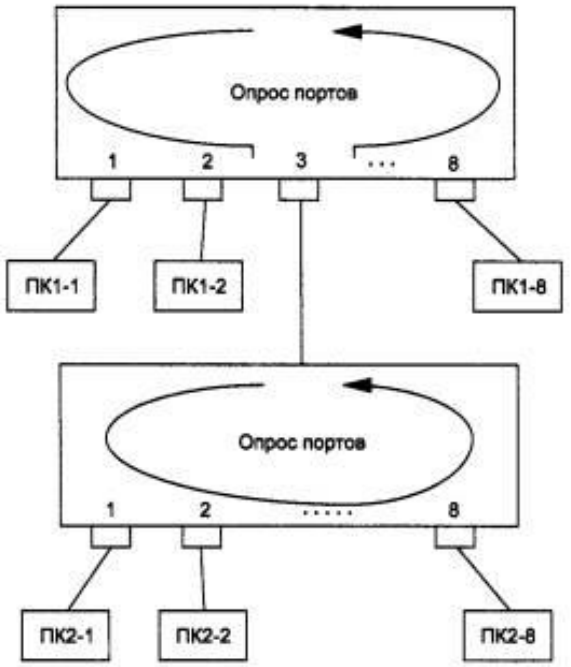


Рис. 3.13 Каскадирование 100VG-AnyLAN

Допускаются три уровня каскадирования. Каждый концентратор и сетевой адаптер l00VG-AnyLAN должен быть настроен либо на работу с кадрами Ethernet, либо с кадрами Token Ring, причем одновременно циркуляция обоих типов кадров не допускается.

Концентратор циклически выполняет опрос портов. Станция, желающая передать пакет, посылает специальный низкочастотный сигнал концентратору, запрашивая передачу кадра и указывая его приоритет. В сети l00VG-AnyLAN используются два уровня приоритетов - низкий и высокий. Низкий уровень приоритета соответствует обычным данным (файловая служба, служба печати и т. п.), а высокий приоритет соответствует данным, чувствительным к временным задержкам (например, мультимедиа). Приоритеты запросов имеют статическую и динамическую составляющие, то есть станция с низким уровнем приоритета, долго не имеющая доступа к сети, получает высокий приоритет.

Если сеть свободна, то концентратор разрешает передачу пакета. После анализа адреса получателя в принятом пакете концентратор автоматически отправляет пакет станции назначения. Если сеть занята, концентратор ставит полученный запрос в очередь, которая обрабатывается в соответствии с порядком поступления запросов и с учетом приоритетов. Если к порту подключен другой концентратор, то опрос приостанавливается до завершения опроса концентратором нижнего уровня. Станции, подключенные к концентраторам различного уровня иерархии, не имеют преимуществ по доступу к разделяемой среде, так как решение о предоставлении доступа

принимается после проведения опроса всеми концентраторами опроса всех своих портов.

Во всех других технологиях кадр просто передавался всем станциям сети, а станция назначения, распознав свой адрес, копировала кадр в буфер. Для решения этой задачи концентратор узнает адрес MAC станции в момент физического присоединения ее к сети кабелем. Если в других технологиях процедура физического соединения выясняет связность кабеля (link test в технологии l0Base-T), тип порта (технология FDDI), скорость работы порта (процедура auto-negotiation в Fast Ethernet), то в технологии l00VG-AnyLAN концентратор при установлении физического соединения выясняет адрес MAC станции. И запоминает его в таблице адресов MAC, аналогичной таблице моста/коммутатора. Отличие концентратора l00VG-AnyLAN от моста/коммутатора в том, что у него нет внутреннего буфера для хранения кадров. Поэтому он принимает от станций сети только один кадр, отправляет его на порт назначения и, пока этот кадр не будет полностью принят станцией назначения, новые кадры концентратор не принимает. Так что эффект разделяемой среды сохраняется. Улучшается только безопасность сети - кадры не попадают на чужие порты, и их труднее перехватить.

Технология l00VG-AnyLAN поддерживает несколько спецификаций физического уровня. Первоначальный вариант был рассчитан на четыре неэкранированные витые пары категорий 3,4,5. Позже появились варианты физического уровня, рассчитанные на две неэкранированные витые пары категории 5, две экранированные витые пары типа 1 или же два оптических многомодовых оптоволокна.

Важная особенность технологии l00VG-AnyLAN - сохранение форматов кадров Ethernet и Token Ring. Сторонники l00VG-AnyLAN утверждают, что этот подход облегчит межсетевое взаимодействие через мосты и маршрутизаторы, а также обеспечит совместимость с существующими средствами сетевого управления, в частности с анализаторами протоколов.

Технология l00VG-AnyLAN не нашла большого количества сторонников и значительно уступает по популярности технологии Fast Ethernet. Возможно, это произошло из-за того, что технические возможности поддержки разных типов трафика у технологии ATM существенно шире, чем у l00VG-AnyLAN. Поэтому при необходимости тонкого обеспечения качества обслуживания применяют (или собираются применять) технологию ATM. А для сетей, в которых нет необходимости поддерживать качество обслуживания на уровне разделяемых сегментов, более привычной оказалась технология Fast Ethernet. Тем более что для поддержки очень требовательных к скорости передачи данных приложений имеется технология Gigabit Ethernet, которая, сохраняя преемственность с Ethernet и Fast Ethernet, обеспечивает скорость передачи данных 1000 Мбит/с.

3.6 Высокоскоростная технология Gigabit Ethernet (802.3z)

3.6.1. Общая характеристика стандарта

Первая версия стандарта была рассмотрена в январе 1997 года, а окончательно стандарт 802.3z был принят 29 июня 1998 года на заседании комитета IEEE 802.3. Работы по реализации Gigabit Ethernet на витой паре категории 5 были переданы специальному комитету 802.3ab. Окончательно стандарт 802.3ab принят в сентябре 1999 года.

Основная идея разработчиков стандарта Gigabit Ethernet состоит в максимальном сохранении классической технологии Ethernet при достижении битовой скорости в 1000 Мбит/с. Сохраняются все форматы кадров Ethernet.

Существуют полудуплексная версия протокола, поддерживающая метод доступа CSMA/CD, и полнодуплексная версия, работающая с коммутаторами. Сохранение недорогого решения для разделяемых сред позволит применить Gigabit Ethernet в небольших рабочих группах, имеющих быстрые серверы и рабочие станции.

Поддерживаются все основные виды кабелей, используемых в Ethernet и Fast Ethernet: волоконно-оптический, витая пара категории 5, коаксиал.

3.6.2 Спецификации физической среды стандарта 802.3z

В стандарте 802.3z определены следующие типы физической среды:

- одномодовый волоконно-оптический кабель;
- многомодовый волоконно-оптический кабель 62,5/125;
- многомодовый волоконно-оптический кабель 50/125;
- двойной коаксиал с волновым сопротивлением 75 Ом.

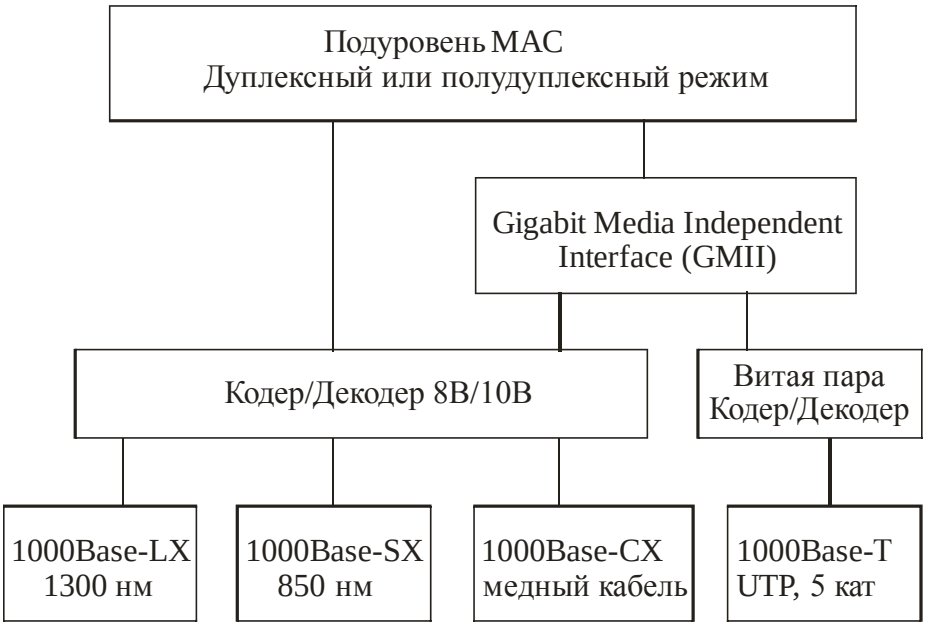


Рис.3.14. Спецификации технологии Gigabit Ethernet

3.6.3 Многомодовый кабель

Для передачи данных по традиционному для компьютерных сетей многомодовому волоконно-оптическому кабелю стандарт определяет применение излучателей, работающих на двух длинах волн: 1300 и 850 нм. Применение светодиодов с длиной волны 850 нм объясняется тем, что они намного дешевле, чем светодиоды, работающие на волне 1300 нм, хотя при этом максимальная длина кабеля уменьшается, так как затухание многомодового оптоволокна на волне 850 м более чем в два раза выше, чем на волне 1300 нм.

Для многомодового оптоволокна стандарт 802.3z определил спецификации l000Base-SX и l000Base-LX.

В первом случае используется длина волны 850 нм (S означает Short Wavelength, короткая волна), а во втором - 1300 нм (L - от Long Wavelength, длинная волна).

Для спецификации l000Base-SX предельная длина оптоволоконного сегмента для кабеля 62,5/125 оставляет 220 м, а для кабеля 50/125 - 500 м. Приведенные расстояния рассчитаны для худшего по стандарту случая полосы пропускания многомодового кабеля, находящегося в пределах от 160 до 500 МГц/км. Реальные кабели обычно обладают значительно лучшими характеристиками, находящимися между 600 и 1000 МГц/км. В этом случае можно увеличить длину кабеля до примерно 800 м.

Для спецификации l000Base-LX в качестве источника излучения всегда применяется полупроводниковый лазер с длиной волны 1300 нм.

Основная область применения стандарта l000Base-LX - это одномодовое оптоволокно. Максимальная длина кабеля для одномодового волокна равна 5 км.

Спецификация l000Base-LX может работать и на многомодовом кабеле. В этом случае предельное расстояние получается небольшим - 550 м. Это связано с особенностями распространения когерентного света в широком канале многомодового кабеля. Для присоединения лазерного трансивера к многомодовому кабелю необходимо использовать специальный адаптер.

3.6.4 Твинаксиальный кабель

В качестве среды передачи данных используется высококачественный твинаксиальный кабель (Twinax) с волновым сопротивлением 150 Ом (2x75 Ом). Данные посылаются одновременно по паре проводников, каждый из которых окружен экранирующей оплеткой. При этом получается режим полудуплексной передачи. Для обеспечения полнодуплексной передачи необходимы еще две пары коаксиальных проводников. Начал выпускаться специальный кабель, который содержит четыре коаксиальных проводника - так

называемый Quad-кабель. Он внешне напоминает кабель категории 5 и имеет близкий к нему внешний диаметр и гибкость. Максимальная длина твинаксиального сегмента составляет всего 25 метров, поэтому это решение подходит для оборудования, расположенного в одной комнате.

3.6.5 Gigabit Ethernet на витой паре категории 5

Для использования уже имеющихся симметричных кабелей UTP категории 5 был разработан стандарт 802.3ab. Поскольку в технологии Gigabit Ethernet данные должны передаваться со скоростью 1000 Мбит/с, а витая пара 5 категории имеет полосу пропускания 100 МГц, то было решено передавать данные параллельно по 4 витым парам и использовать UTP категории 5 или 5e с шириной полосы 125 МГц. Таким образом, по каждой витой паре необходимо передавать данные со скоростью 250 Мбит/с, что в 2 раза превышает возможности UTP категории 5e. Для устранения этого противоречия используется код 4D-PAM5 с пятью уровнями потенциала (-2, -1, 0, +1, +2). По каждой паре проводов одновременно производится передача и прием данных со скоростью 125 Мбит/с в каждую сторону. При этом происходят коллизии, при которых формируются сигналы сложной формы пяти уровней. Разделение входного и выходного потоков производится за счет использования схем гибридной развязки **Н** (рис.2.11). В качестве таких схем используются сигнальные процессоры. Для выделения принимаемого сигнала приемник вычитает из суммарного (передаваемого и принимаемого) сигнала собственный передаваемый сигнал.

Таким образом, технология Gigabit Ethernet обеспечивает высокоскоростной обмен данными и применяется, главным образом, для передачи данных между подсетями, а также для обмена мультимедийной информацией.

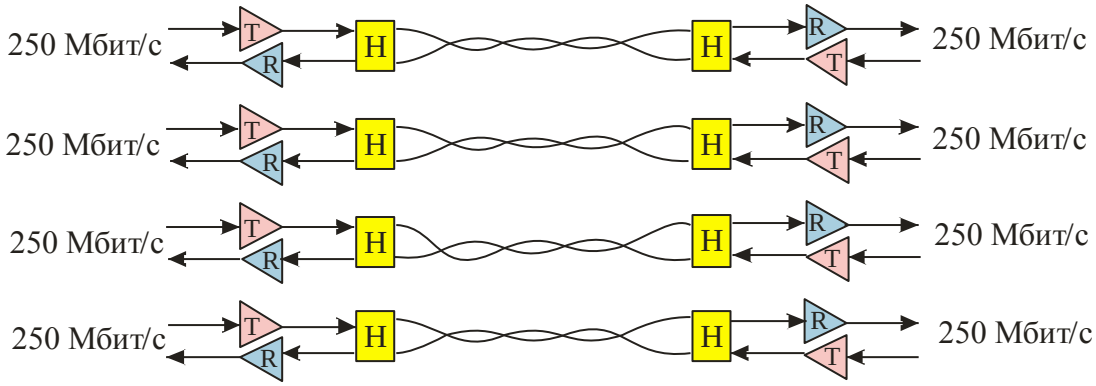


Рис. 3.15. Передача данных по 4 парам UTP категории 5

3.6.6 Диаметр сети Gigabit Ethernet

Стандарт IEEE 802.3 рекомендует, что технология Gigabit Ethernet с передачей данных по волокну должна быть магистральной (backbone). Временные интервалы, формат кадра и передача являются общими для всех

версий 1000Мбит/с. Физический уровень определяют две схемы кодирования сигнала. Схема 8В/10В используется для оптического волокна и медных экранированных кабелей. Для симметричных кабелей UTP используется модуляция амплитуды импульсов (код PAM5). Технология 1000Base-X использует логическое кодирование 8В/10В и линейное кодирование (NRZ).

Сигналы **NRZ** передаются по волокну, используя либо коротковолновые (**short-wavelength**), либо длинноволновые (**long-wavelength**) источники света. В качестве коротковолновых источников используются светодиоды с длиной волны **850** нм для передачи по многомодовому оптическому волокну (1000Base-SX). Этот менее дорогостоящий вариант используется для передачи на короткие расстояния. Длинноволновые лазерные источники (**1310** нм) используют одномодовое или многомодовое оптическое волокно (1000Base-LX). Лазерные источники с одномодовым волокном способны передавать информацию на расстояние до **5000** м.

В соединениях точка – точка (**point-to-point**) для передачи (**Tx**) и приема (**Rx**) используются раздельные волокна, поэтому реализуется **полнодуплексная** связь. Технология Gigabit Ethernet позволяет устанавливать только **единственный ретранслятор** между двумя станциями. Ниже приведено сравнение технологий 1000Base (табл. 3.3).

Таблица 3.3

Сравнительные характеристики спецификаций Gigabit Ethernet

	Спецификация	**Среда**	**Расстояние**
1	1000Base-LX	Волокно 10 мкм	5000 м
2		Волокно 50 мкм	500 м
3		Волокно 62,5 мкм	500 м
4	1000Base-SX	Волокно 50 мкм	500 м
5		Волокно 62,5 мкм	300 м
6	1000Base-T	Витая пара UTP, 5e	100 м
7	1000Base-CX	Экранир. кабель	25 м

Сети Gigabit Ethernet строятся на основе коммутаторов, когда расстояние полнодуплексных соединений ограничено только средой, а не временем двойного оборота. При этом, как правило, используются топология «звезда» или «расширенная звезда», а проблемы определяются логической топологией и потоком данных.

Стандарт 1000Base-T предусматривает использование практически такого же кабеля UTP, как и стандарты 100Base-T, и 10Base-T. Кабель UTP технологии 1000Base-T такой же, как кабель 10Base-T и 100Base-TX, за исключением того, что рекомендовано использовать кабель категории 5e. При длине кабеля 100м аппаратура 1000Base-T работает на пределе своих возможностей.

3.7 Технология 10-Gigabit Ethernet

Технология 10-Gigabit Ethernet (10GbE) описывается стандартом IEEE 802.3ae, который определяет полнодуплексную передачу данных со скоростью 10 Гбит/с по волокну оптического кабеля. 10-Gbps Ethernet был стандартизирован в июне 2002. Максимальные расстояния передачи зависят от типа используемого волокна. Используя одномодовое волокно как среду передачи, максимальное расстояние передачи - 40 километров. Обсуждается возможность стандартов для 40, 80, и даже 100-Gbps Ethernet.

Стандарт 10GbE на физическом уровне позволяет увеличить расстояние связи до 40 км по одномодовому волокну и обеспечить совместимость с сетями синхронной цифровой иерархии (SDH). Функционирование на 40-километровом расстоянии, скорость передачи до 10 Gbps и совместимость с системами SDH делает технологию 10GbE не только технологией локальных, но и технологией глобальных сетей. Таким образом, стандарт развивается не только для LAN, но также для MAN и WAN. Сети 10GbE могут также конкурировать с ATM в определенных приложениях. Поскольку в технологии 10GbE используются волокна только в режиме полнодуплексной связи, в режиме CSMA/CD нет необходимости.

Стандарт 802.3ae управляет семейством 10GbE, которое включает новые технологии:

- **10GBase-SR** –для коротких расстояний по уже установленному многомодовому волокну, поддерживает связь на расстоянии от 26м до 82м.
- **10GBase-LX4** – использует технологию уплотнения по длины волне (**WDM**), поддерживает связь на расстоянии от 240 м до 300 м по уже установленному многомодовому волокну и 10 км по одномодовому волокну.
- **10GBase- LR и 10GBase-ER** – поддерживает связь до 10 км и 40 км по одномодовому волокну
- **10GBase-SW, 10GBase-LW и 10GBase-EW** – технологии с общим названием **10GBase-W**, предназначенны, чтобы обеспечить работу **WAN** оборудования с модулями SONET/SDH

Вследствие высокой скорости передачи данных в технологии 10 GbE существуют проблемы синхронизации, полосы пропускания и отношения Сигнал/Шум. Поэтому 10-Gigabit Ethernet использует два отдельных этапа кодирования. При использовании кодирования для представления данных пользователя, передача будет более эффективной. Закодированные данные обеспечивают синхронизацию, эффективное использование полосы пропускания и улучшенные характеристики отношения Сигнал/Шум.

Сложные последовательные потоки битов используются для всех версий 10GbE, за исключением 10GBase-LX4, которая использует Wide Wavelength Division Multiplex (WWDM), чтобы мультиплексировать четыре потока бит при использовании четырех длин волн света в волокне одновременно.

Для 10-Gigabit Ethernet не предусмотрены повторители, поскольку полудуплексный режим явно не поддерживается.

Таблица 3.4
Параметры спецификаций технологии 10GbE

Спецификация	Длина волны	Волокно	Расстояние
10GBase-LX4	1310 нм	62,5 мкм	2 – 300 м
		50 мкм	2 – 240 м
		50 мкм	2 – 300 м
		10 мкм	2 – 10 км
10GBase-S	850 нм	62,5 мкм	2 – 26 м
		62,5 мкм	2 – 33 м
		50 мкм	2 – 66 м
		50 мкм	2 – 82 м
		50 мкм	2 – 300 м
10GBase-L	1310 нм	10 мкм	2 – 10 км
10GBase-E	1550 нм	10 мкм	2 – 30 км

В заключение следует отметить, что в настоящее время технологии Ethernet является стандартом для различных соединений: горизонтальных, вертикальных и связи между зданиями. Новые версии Ethernet стирают различие между локальными и глобальными сетями. Передача информации производится по трем составляющим сетевой среды:

1. Медь примерно 1000 Мбит/с и возможно больше
2. Беспроводная (радиоканалы) – примерно 100 Мбит/с и больше
3. Оптическая– примерно 10000 Мбит/с и возможно больше

Медная и беспроводная среда имеют определенные физические и практические ограничения на высокочастотные сигналы. В волоконно-оптических системах ограничивающим фактором является электронная технология (emitters and detectors) и производственные процессы волокна.

Когда Ethernet был медленным, полудуплексным, с возникновением коллизий, не рассматривался вопрос качества обслуживания (QoS), необходимый при передаче определенных видов трафика, например, IP телефония и видео. Полнодуплексные быстродействующие технологии Ethernet обеспечивают достаточную поддержку разнообразных приложений. Это делает потенциальные приложения Ethernet еще шире.

Раздел 4. МОНИТОРИНГ И УПРАВЛЕНИЕ СЕТЯМИ

4.1. Средства анализа и управления сетями

4.1.1. Функции и архитектура систем управления сетями

Независимо от объекта управления система управления должна выполнять ряд функций, которые определены международными стандартами, обобщающими опыт применения систем управления в различных областях. Существуют рекомендации ITU-T X.700 и близкий к ним стандарт ISO 7498-4, которые делят задачи системы управления на пять функциональных групп:

1. Управление конфигурацией сети и именованием (Configuration Management). Эти задачи заключаются в конфигурировании параметров как элементов сети (*Network Element, NE*), так и сети в целом. Для элементов сети, таких как маршрутизаторы, мультиплексоры и т. п., с помощью этой группы задач определяются сетевые адреса, идентификаторы (имена), географическое положение и пр.

Для сети в целом управление конфигурацией обычно начинается с построения карты сети, то есть отображении реальных связей между элементами сети и изменении связей между элементами сети - образование новых физических или логических каналов, изменение таблиц коммутации и маршрутизации.

Управление конфигурацией (как и другие задачи системы управления) могут выполняться в автоматическом, ручном или полуавтоматическом режимах. Например, карта сети может составляться автоматически, на основании зондирования реальной сети пакетами-исследователями, а может быть введена оператором системы управления вручную. Чаще всего применяются полуавтоматические методы, когда автоматически полученную карту оператор подправляет вручную. Методы автоматического построения топологической карты, как правило, являются фирменными разработками.

Более сложной задачей является настройка коммутаторов и маршрутизаторов на поддержку маршрутов и виртуальных путей между пользователями сети. Согласованная ручная настройка таблиц маршрутизации при полном или частичном отказе от использования протокола маршрутизации (а в некоторых глобальных сетях, например X.25, такого протокола просто не существует) представляет собой сложную задачу. Многие системы управления сетью общего назначения ее не выполняют, но существуют специализированные системы конкретных производителей, например система *NetSys* компании *Cisco Systems*, которая решает ее для маршрутизаторов этой же компании.

2. Обработка ошибок (Fault Management). Эта группа задач включает выявление, определение и устранение последствий сбоев и отказов в работе сети. На этом уровне выполняется не только регистрация сообщений об

ошибках, но и их фильтрация, маршрутизация и анализ на основе некоторой корреляционной модели. Фильтрация позволяет выделить из весьма интенсивного потока сообщений об ошибках, только важные сообщения. Маршрутизация обеспечивает их доставку нужному элементу системы управления, а корреляционный анализ позволяет найти причину, породившую поток взаимосвязанных сообщений (например, обрыв кабеля может быть причиной большого количества сообщений о недоступности сетей и серверов).

Устранение ошибок может быть как автоматическим, так и полуавтоматическим. В первом случае система непосредственно управляет оборудованием или программными комплексами и обходит отказавший элемент за счет резервных каналов. В полуавтоматическом режиме основные решения и действия по устранению неисправности выполняют люди, а система управления только помогает в организации этого процесса - оформляет квитанции на выполнение работ и отслеживает их поэтапное выполнение.

В этой группе задач иногда выделяют подгруппу задач управления проблемами, подразумевая под проблемой сложную ситуацию, требующую для разрешения обязательного привлечения специалистов по обслуживанию сети.

3. Анализ производительности и надежности (Performance Management). Задачи этой группы связаны с оценкой на основе накопленной статистической информации таких параметров, как время реакции системы, пропускная способность реального или виртуального канала связи между двумя конечными абонентами сети, интенсивность трафика в отдельных сегментах и каналах сети, вероятность искажения данных при их передаче через сеть, а также коэффициент готовности сети или ее определенной транспортной службы. Функции анализа производительности и надежности сети нужны как для оперативного управления сетью, так и для планирования развития сети.

Результаты анализа производительности и надежности позволяют контролировать соглашение об уровне обслуживания (*Service Level Agreement, SLA*), заключаемое между пользователем сети и ее администраторами (или компанией, продающей услуги). Обычно в соглашении оговариваются такие параметры надежности, как коэффициент готовности службы в течение года и месяца, максимальное время устранения отказа, а также параметры производительности, например, средняя и максимальная пропускная способности при соединении двух точек подключения пользовательского оборудования, время реакции сети (если информационная служба, для которой определяется время реакции, поддерживается внутри сети), максимальная задержка пакетов при передаче через сеть (если сеть используется только как транзитный транспорт). Без средств анализа производительности и надежности поставщик услуг публичной сети или отдел информационных технологий предприятия не сможет ни проконтролировать, ни тем более обеспечить нужный уровень обслуживания для конечных пользователей сети.

4. Управление безопасностью (Security Management). Задачи этой группы включают в себя контроль доступа к ресурсам сети (данным и оборудованию) и сохранение целостности данных при их хранении и передаче через сеть. Базовыми элементами управления безопасностью являются процедуры аутентификации пользователей, назначение и проверка прав доступа к ресурсам сети, распределение и поддержка ключей шифрования, управления полномочиями и т. п. Часто функции этой группы не включаются в системы управления сетями, а реализуются либо в виде специальных продуктов (например, системы аутентификации и авторизации, различных защитных экранов, систем шифрования данных), либо входят в состав операционных систем и системных приложений.

5. Учет работы сети (Accounting Management). Задачи этой группы занимаются регистрацией времени использования различных ресурсов сети - устройств, каналов и транспортных служб. Эти задачи имеют дело с такими понятиями, как время использования службы и плата за ресурсы - *billing*. Ввиду специфического характера оплаты услуг у различных поставщиков и различными формами соглашения об уровне услуг, эта группа функций обычно не включается в коммерческие системы и платформы управления типа HP Open View, а реализуется в заказных системах, разрабатываемых для конкретного заказчика.

Модель управления OSI не делает различий между управляемыми объектами - каналами, сегментами локальных сетей, мостами, коммутаторами и маршрутизаторами, модемами и мультиплексорами, аппаратным и программным обеспечением компьютеров, СУБД. Все эти объекты управления входят в общее понятие «система», и управляемая система взаимодействует с управляющей системой по открытым протоколам OSI.

Однако на практике деление систем управления по типам управляемых объектов широко распространено. Ставшими классическими системы управления сетями, такие как ***SunNet Manager, HP Open View*** или ***Cabletron Spectrum***, управляют только коммуникационными объектами корпоративных сетей, то есть концентраторами и коммутаторами локальных сетей, а также маршрутизаторами и удаленными мостами, как устройствами доступа к глобальным сетям. Оборудованием территориальных сетей обычно управляют системы производителей телекоммуникационного оборудования, такие как ***RADView*** компании ***RAD Data Communications, MainStreetXpress 46020*** компании ***Newbridge*** и т. п.

Рассмотрим, как преломляются общие функциональные задачи системы управления, определенные в стандартах X.700/ISO 7498-4, в задачи такого конкретного класса систем управления, как системы управления компьютерами и их системным и прикладным программным обеспечением. Их называют ***системами управления системой (System Management System)***.

Обычно система управления системой выполняет следующие функции:

- *Учет используемых аппаратных и программных средств (Configuration Management).* Система автоматически собирает информацию об установленных в сети компьютерах и создает записи в специальной базе данных об аппаратных и программных ресурсах. После этого администратор может быстро выяснить, какими ресурсами он располагает и где тот или иной ресурс находится, например, узнать о том, на каких компьютерах нужно обновить драйверы принтеров, какие компьютеры обладают достаточным количеством памяти, дискового пространства и т. п.
- *Распределение и установка программного обеспечения (Configuration Management).* После завершения обследования администратор может создать пакеты рассылки нового программного обеспечения, которое нужно инсталлировать на всех компьютерах сети или на какой-либо группе компьютеров. В большой сети, где проявляются преимущества системы управления, такой способ инсталляции может существенно уменьшить трудоемкость этой процедуры. Система может также позволять централизованно устанавливать и администрировать приложения, которые запускаются с файловых серверов, а также дать возможность конечным пользователям запускать такие приложения с любой рабочей станции сети.
- *Удаленный анализ производительности и возникающих проблем (Fault Management and Performance Management).* Эта группа функций позволяет удаленно измерять наиболее важные параметры компьютера, операционной системы, СУБД и т. д. (например, коэффициент использования процессора, интенсивность страничных прерываний, коэффициент использования физической памяти, интенсивность выполнения транзакций). Для разрешения проблем эта группа функций может давать администратору возможность брать на себя удаленное управление компьютером в режиме эмуляции графического интерфейса популярных операционных систем. База данных системы управления обычно хранит детальную информацию о конфигурации всех компьютеров в сети для того, чтобы можно было выполнять удаленный анализ возникающих проблем.

Примерами систем управления системами являются Microsoft System Management Server (SMS), CA Unicenter, HP Operationscenter и многие другие.

Функции системы управления системами, повторяют функции системы управления сетью, но только для других объектов. Действительно, функция учета используемых аппаратных и программных средств соответствует функции построения карты сети, функция распределения и установки программного обеспечения - функции управления конфигурацией коммутаторов и маршрутизаторов, а функция анализа производительности и возникающих проблем - функции производительности.

На практике уже несколько лет также заметна отчетливая тенденция интеграции систем управления сетями и системами в единые интегрированные продукты управления корпоративными сетями, например CA Unicenter TNG или TME-10 IBM/Tivoli. Наблюдается также интеграция систем управления телекоммуникационными сетями с системами управления корпоративными сетями.

4.2. Архитектура и функции систем управления вычислительными сетями

4.2.1. Многоуровневое представление задач управления

Для построения интегрированной системы управления разнородными элементами сети применяется многоуровневый иерархический подход. Наиболее проработанным и эффективным является стандарт Telecommunication Management Network (TMN), разработанный совместными усилиями ITU-T, ISO, ANSI и ETSI. Стандарты TMN состоят из большого количества рекомендаций ITU-T, но основные принципы модели TMN описаны в рекомендации M.3010.

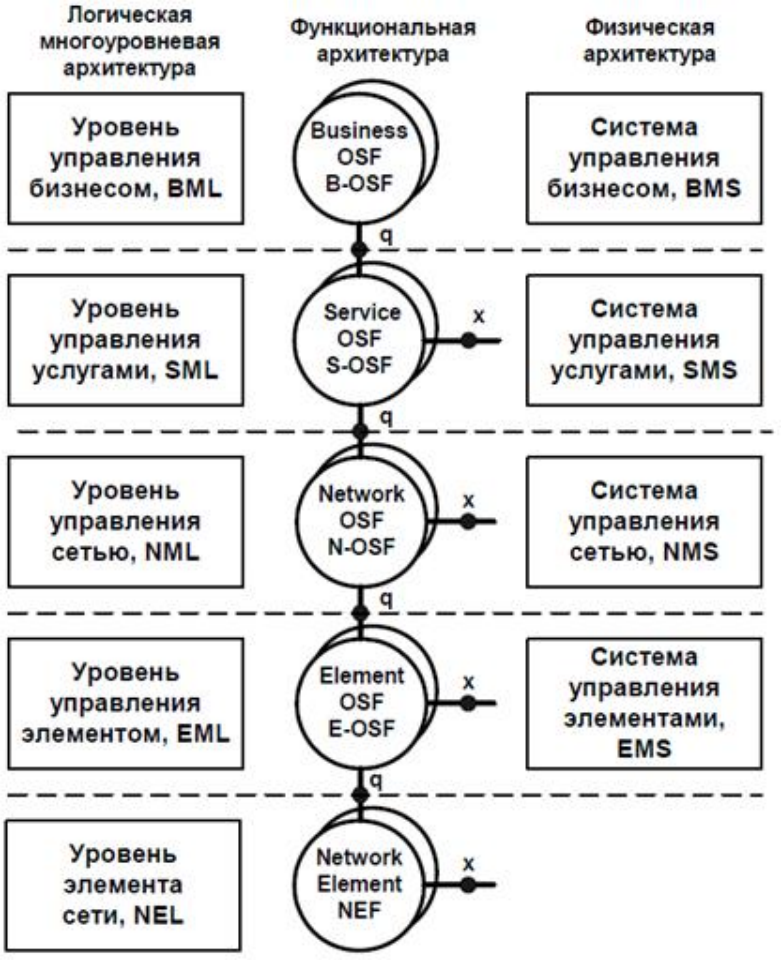


Рис.4.1. Иерархия систем управления

1). ***Уровень элемента сети (Network Element layer, NE)*** - состоит из отдельных устройств сети: каналов, усилителей, оконечной аппаратуры, мультиплексоров,

коммутаторов и т. п. Современные технологии обычно имеют встроенные функции управления, которые позволяют выполнять хотя бы минимальные операции контроля за состоянием устройства и за передаваемым трафиком. Подобные функции встроены в технологии FDDI, ISDN, Frame Relay, SDH. В этом случае устройство всегда можно охватить системой управления, даже если оно не имеет специального блока управления, так как протокол технологии обязывает устройство поддерживать некоторые функции управления. Устройства, которые работают по протоколам, не имеющим встроенных функций контроля и управления, снабжаются отдельным блоком управления, который поддерживает один из двух наиболее распространенных протоколов управления - SNMP или CMIP. Эти протоколы относятся к прикладному уровню модели OSI.

2). ***Уровень управления элементом сети (network element management layer)*** - представляет собой элементарные системы управления, которые автономно управляют отдельными элементами сети - контролируют канал связи SDH, управляют коммутатором или мультиплексором. Уровень управления элементами изолирует верхние слои системы управления от деталей и особенностей управления конкретным оборудованием. Этот уровень ответственен за моделирование поведения оборудования и функциональных ресурсов нижележащей сети. Обычно элементарные системы управления разрабатываются и поставляются производителями оборудования. Примерами таких систем могут служить системы управления CiscoView от Cisco Systems, Optivity от Bay Networks, RADView от RAD Data Communications и т. д.

3). ***Уровень управления сетью (Network management layer)***. Этот уровень координирует работу элементарных систем управления, позволяя контролировать конфигурацию составных каналов, согласовывать работу транспортных подсетей разных технологий и т. п. С помощью этого уровня сеть начинает работать как единое целое, передавая данные между своими абонентами.

4). ***Уровень управления услугами (Service management layer)*** - занимается контролем и управлением за транспортными и информационными услугами, которые предоставляются конечным пользователям сети. В задачу этого уровня входит подготовка сети к предоставлению определенной услуги, ее активизация, обработка вызовов клиентов. Формирование услуги (service provisioning) заключается в фиксации в базе данных значений параметров услуги, например, требуемой средней пропускной способности, максимальных величин задержек пакетов, коэффициента готовности и т. п. В функции этого уровня входит также выдача уровню управления сетью задания на конфигурирование виртуального или физического канала связи для поддержания услуги. После формирования услуги данный уровень занимается контролем за качеством ее реализации, то есть за соблюдением сетью всех принятых на себя обязательств в отношении производительности и надежности

транспортных услуг. Результаты контроля качества обслуживания нужны, в частности, для подсчета оплаты за пользование услугами клиентами сети.

5). ***Уровень бизнес-управления (Business management layer)*** занимается вопросами долговременного планирования сети с учетом финансовых аспектов деятельности организации, владеющей сетью. На этом уровне помесячно и поквартально подсчитываются доходы от эксплуатации сети и ее отдельных составляющих, учитываются расходы на эксплуатацию и модернизацию сети, принимаются решения о развитии сети с учетом финансовых возможностей. Этот уровень является частным случаем уровня автоматизированной системы управления предприятием (АСУП), в то время как все нижележащие уровни соответствуют уровням автоматизированной системы управления технологическими процессами (АСУТП), для такого специфического типа предприятия, как телекоммуникационная, вычислительная или корпоративная сеть.

4.2.2. Архитектуры систем управления сетями

В основе любой системы управления сетью лежит элементарная схема взаимодействия агента с менеджером. На основе этой схемы могут быть построены системы практически любой сложности с большим количеством агентов и менеджеров разного типа.

Агент является посредником между управляемым ресурсом и основной управляющей программой-менеджером. Чтобы один и тот же менеджер мог управлять различными реальными ресурсами, создается некоторая модель управляемого ресурса, которая отражает только те характеристики ресурса, которые нужны для его контроля и управления. Например, модель маршрутизатора обычно включает такие характеристики, как количество портов, их тип, таблицу маршрутизации, количество кадров и пакетов протоколов канального, сетевого и транспортного уровней, прошедших через эти порты.

Менеджер получает от агента только те данные, которые описываются моделью ресурса. Агент же является некоторым экраном, освобождающим менеджера от ненужной информации о деталях реализации ресурса. Агент поставляет менеджеру обработанную и представленную в нормализованном виде информацию. На основе этой информации менеджер принимает решения по управлению, а также выполняет дальнейшее обобщение данных о состоянии управляемого ресурса, например, строит зависимость загрузки порта от времени.

Менеджер и агент должны располагать одной и той же моделью управляемого ресурса, иначе они не смогут понять друг друга. При этом агент наполняет модель управляемого ресурса текущими значениями характеристик данного ресурса, и в связи с этим модель агента называют базой данных управляющей информации - Management Information Base, MIB. Менеджер

использует модель, чтобы знать о том, чем характеризуется ресурс, какие характеристики он может запросить у агента и какими параметрами можно управлять.

Обычно менеджер работает с несколькими агентами, обрабатывая получаемые от них данные и выдавая на них управляющие воздействия. Агенты могут встраиваться в управляемое оборудование, ии работать на отдельном компьютере, связанном с управляемым оборудованием по какому-либо интерфейсу. Менеджер обычно работает на отдельном компьютере, который выполняет также роль консоли управления для оператора или администратора системы.

Модель менеджер - агент лежит в основе таких популярных стандартов управления, как стандарты Internet на основе протокола SNMP и стандарты управления ISO/OSI на основе протокола CMIP.

4.2.3. Структуры распределенных систем управления

Схема «менеджер - агент» позволяет строить достаточно сложные в структурном отношении распределенные системы управления.

Обычно распределенная система управления включает большое количество связок менеджер - агент, которые дополняются рабочими станциями операторов сети, с помощью которых они получают доступ к менеджерам.

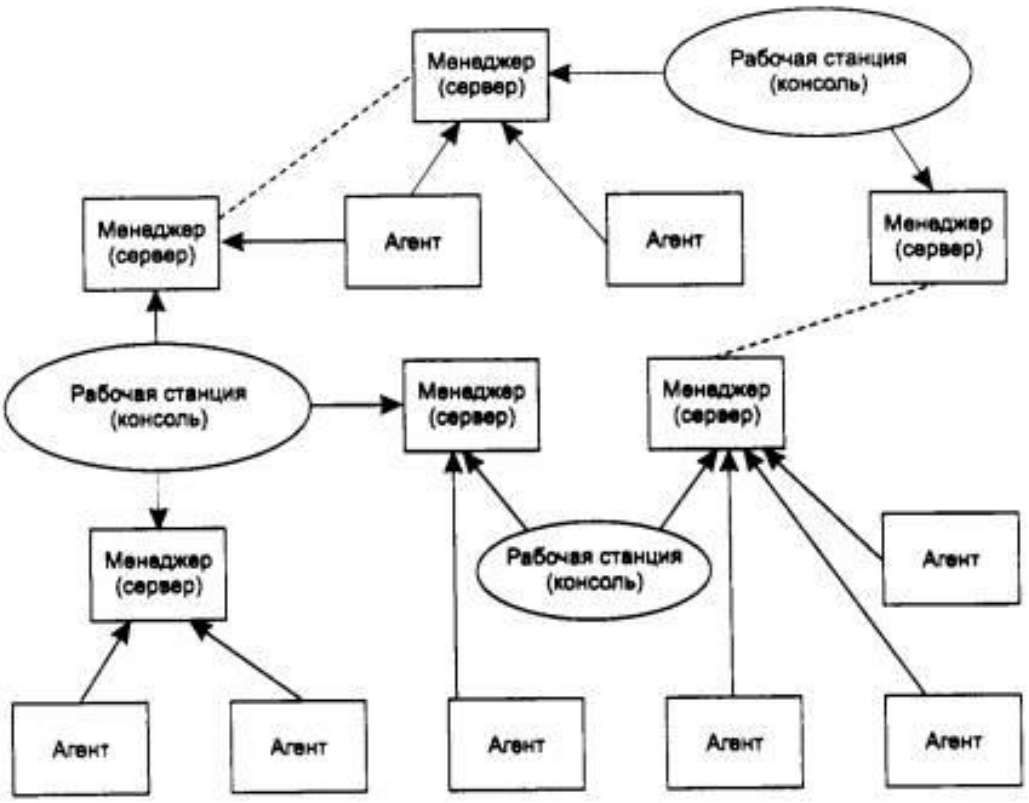


Рис.4.2. Распределенная система управления на основе нескольких менеджеров и рабочих станций

Каждый агент собирает данные и управляет определенным элементом сети. Менеджеры, иногда также называемые серверами системы управления, собирают данные от своих агентов, обобщают их и хранят в базе данных. Операторы, работающие за рабочими станциями, могут соединиться с любым из менеджеров и с помощью графического интерфейса просмотреть данные об управляемой сети, а также выдать менеджеру некоторые директивы по управлению сетью или ее элементами.Наличие нескольких менеджеров позволяет распределить между ними нагрузку по обработке данных управления, обеспечивая масштабируемость системы.

Как правило, связи между агентами и менеджерами носят более упорядочен-ный характер. Чаще всего используются два подхода к их соединению - одноранговый и иерархический.

Рис.4.3. Одноранговые связи между менеджерами

В случае одноранговых связей каждый менеджер управляет своей частью сети на основе информации, получаемой от нижележащих агентов. Центральный менеджер отсутствует. Координация работы менеджеров достигается за счет обмена информацией между базами данных каждого менеджера.

Гораздо более гибким является иерархическое построение связей между менеджерами. Каждый менеджер нижнего уровня выполняет также функции агента для менеджера верхнего уровня. Такой агент работает уже с гораздо более укрупненной моделью (MIB) своей части сети, в которой собирается именно та информация, которая нужна менеджеру верхнего уровня для управления сетью в целом. Обычно для разработки моделей сети на разных уровнях проектирование начинают с верхнего уровня, на котором определяется состав информации, требуемой от менеджеров-агентов более низкого уровня, поэтому такой подход назван подходом «сверху вниз». Он сокращает объемы информации, циркулирующей между уровнями системы управления, и приводит к гораздо более эффективной системе управления.

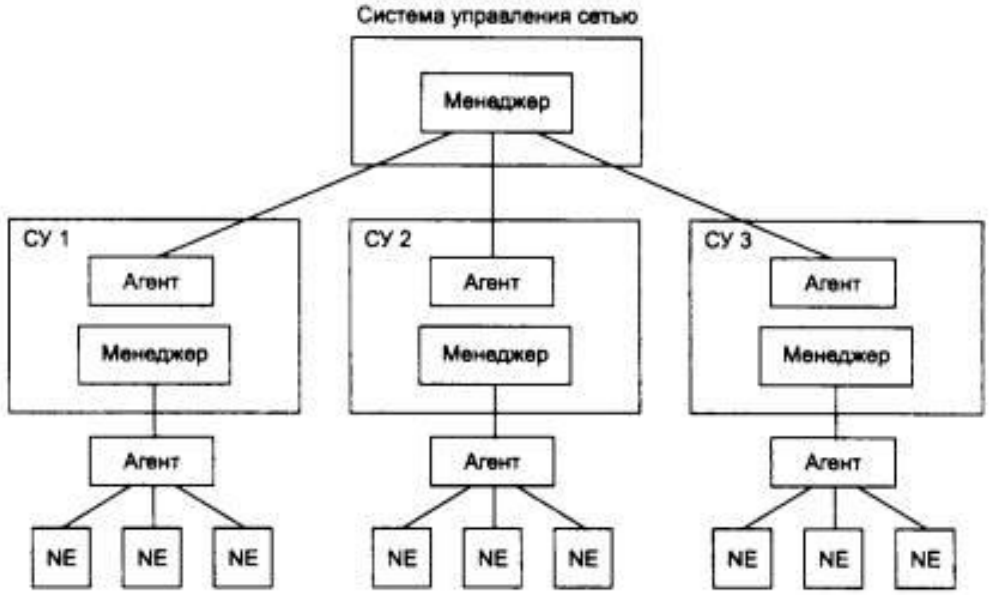


Рис.4.4. Иерархическая система управления сетью

Модель TMN в наибольшей степени соответствует иерархической архитектуре связей между менеджерами, хотя известны реализации принципов TMN и в одноуровневых архитектурах.

4.2.4. Платформенный подход

При построении систем управления крупными локальными и корпоративными сетями обычно используется платформенный подход, когда индивидуальные программы управления разрабатываются не «с нуля», а используют службы и примитивы, предоставляемые специально разработанным для этих целей программным продуктом - платформой. Примерами платформ для систем управления являются такие известные продукты, как HP OpenView, SunNet Manager и Sun Soltice, Cdbletron Spectrum, IMB/Tivoli TMN10.

Эти платформы создают общую операционную среду для приложений системы управления точно так же, как универсальные операционные системы, такие как Unix или Windows NT, создают операционную среду для приложений любого типа, таких как MS Word, Oracle и т. п. Платформа обычно включает поддержку протоколов взаимодействия менеджера с агентами - SNMP и реже CMIP, набор базовых средств для построения менеджеров и агентов, а также средства графического интерфейса для создания консоли управления. В набор базовых средств обычно входят функции, необходимые для построения карты сети, средства фильтрации сообщений от агентов, средства ведения базы данных. Набор интерфейсных функций платформы образует интерфейс прикладного программирования (API) системы управления. Пользуясь этим API, разработчики из третьих фирм создают законченные системы управления, которые могут управлять специфическим оборудованием в соответствии с пятью основными группами функций.

Обычно платформа управления поставляется с каким-либо универсальным менеджером, который может выполнять некоторые базовые функции управления без программирования. Чаще всего к этим функциям относятся функции построения карты сети (группа Configuration Management), а также функции отображения состояния управляемых устройств и функции фильтрации сообщений об ошибках (группа Fault Management). Например, одна из наиболее популярных платформ HP OpenView поставляется с менеджером Network Node Manager, который выполняет перечисленные функции.

Чем больше функций выполняет платформа, тем лучше. В том числе и таких, которые нужны для разработки любых аспектов работы приложений, прямо не связанных со спецификой управления. В конце концов, приложения системы управления - это прежде всего приложения, а потом уже приложения системы управления. Поэтому полезны любые средства, предоставляемые платформой, которые ускоряют разработку приложений вообще и распределенных приложений в частности.

Компании, которые производят коммуникационное оборудование, разрабатывают дополнительные менеджеры для популярных платформ, которые выполняют функции управления оборудованием данного производителя более полно. Примерами таких менеджеров могут служить менеджеры системы Optivity компании Bay Networks и менеджеры системы Trancsend компании 3Com, которые могут работать в среде платформ HP OpenView и SunNet Manager.

Раздел 5. ЗАЩИТА ВЫЧИСЛИТЕЛЬНЫХ СЕТЕЙ

5.1. Способы и средства защиты информации в сетях

Под защитой информации в компьютерных системах принято понимать создание и поддержание организованной совокупности средств, способов, методов и мероприятий, предназначенных для предупреждения искажения, уничтожения и несанкционированного использования информации, хранимой и обрабатываемой в электронном виде.

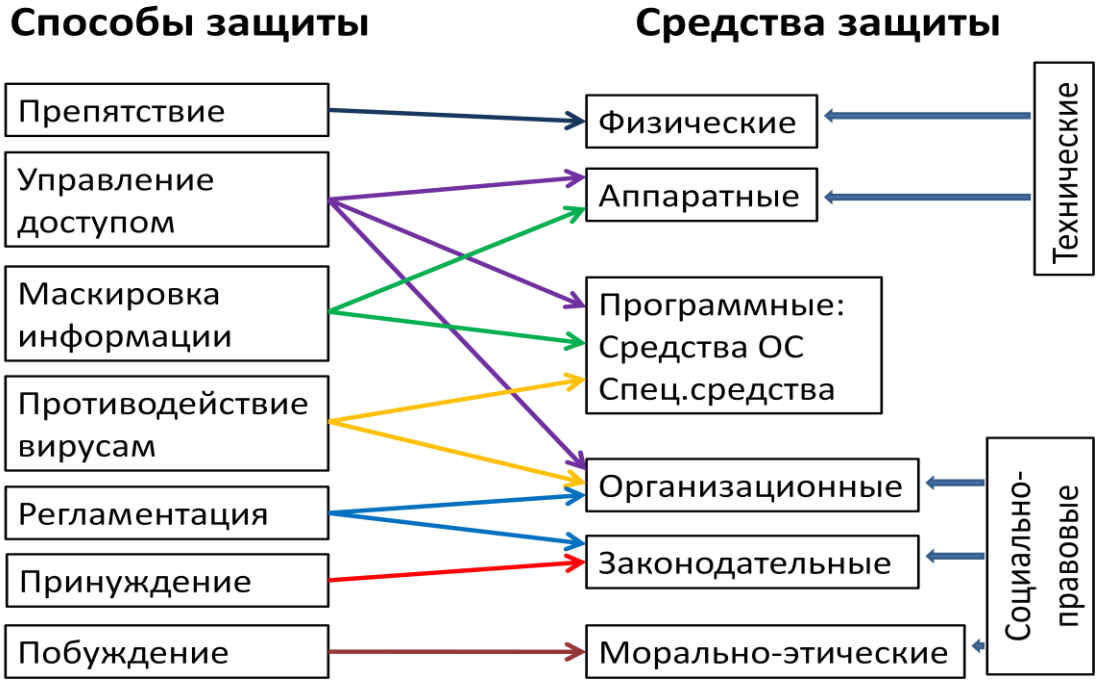


Рис.5.1. Соответствие средств способам защиты информации

5.1.1. Способы защиты информации можно разделить на 7 групп:

Препятствие - способ физического преграждения пути злоумышленнику к защищаемой информации (к аппаратуре, носителям информации и т.д.).

Управление доступом - способ защиты информации за счет регулирования использования всех ресурсов системы (технических, программных, временных и др.). Эти методы должны противостоять всем возможным путям НСД к информации. Управление доступом включает следующие функции защиты:

- идентификацию пользователей, персонала и ресурсов системы (присвоение каждому объекту персонального идентификатора);
- установление подлинности объекта или субъекта по предъявленному им идентификатору;
- проверку полномочий;
- разрешение и создание условий работы в пределах установленного регламента;

- регистрацию (протоколирование) обращений к защищаемым ресурсам;
- реагирование (сигнализация, отключение, задержка работ, отказ в запросе и т.п.) при попытках несанкционированных действий.

Маскировка информации, как правило, осуществляется путем ее криптографического закрытия или стеганографии. При передаче информации по каналам связи большой протяженности эти методы являются достаточно надежными. Механизмы шифрования все шире применяются как при обработке, так и при хранении информации на магнитных носителях и CD.

Противодействие вирусам (или атакам различных вредоносных программ) предполагает использование антивирусных программ, а так же комплекс разнообразных мер организационного характера. Цели принимаемых мер - это уменьшение вероятности инфицирования ИС; выявление фактов заражения системы; уменьшение последствий информационных инфекций, локализация или уничтожение вирусов; восстановление информации в ИС.

Регламентация заключается в реализации чёткой системы организационных мероприятий, определяющих все стороны процесса обработки информации.

Принуждение - способ защиты, при котором пользователи и персонал ИС вынуждены соблюдать определенные правила работы с информацией (обработки, передачи и использования защищаемой информации) под угрозой материальной, административной или уголовной ответственности.

Побуждение - способ защиты, побуждающий пользователей и персонал ИС не нарушать установленные порядки за счет соблюдения сложившихся моральных и этических норм.

5.1.2. Средства защиты информации, хранимой и обрабатываемой в электронном виде, разделяют на три самостоятельные группы: ***технические, программные и социально-правовые***. В свою очередь вся совокупность технических средств подразделяется на аппаратные и физические. Социально-правовые средства включают в себя организационные, законодательные и морально-этические.

Физические средства включают различные инженерные устройства и сооружения, препятствующие физическому проникновению злоумышленников на объекты защиты и осуществляющие защиту персонала (личные средства безопасности), материальных средств и финансов, информации от противоправных действий. Примеры физических средств: замки на дверях, решетки на окнах, турникеты, средства электронной охранной сигнализации и т.п.

Аппаратные средства - устройства, встраиваемые непосредственно в вычислительную технику, или устройства, которые сопрягаются с ней по стандартному интерфейсу. Такие средства принадлежат к наиболее защищенной

части системы. С их помощью могут быть реализованы любые концепции защиты, но стоимость реализации оказывается на порядок выше по сравнению с аналогичными по назначению программными средствами. При наличии выбора предпочтение следует отдавать аппаратным средствам защиты, так как они исключают любое вмешательство в их работу непосредственно из сети. Изучение уязвимостей работы этих средств возможно только при наличии непосредственного физического доступа к ним. Другим преимуществом аппаратных средств является их большая производительность по сравнению с программными средствами защиты (особенно в случае их использования в устройствах криптографической защиты).

Программные средства - это специальные программы и программные комплексы, предназначенные для защиты информации в ИС. Они являются наиболее распространенными средствами, так как с их помощью могут быть реализованы практически все идеи и методы защиты, и, кроме того, по сравнению с аппаратными средствами они имеют невысокую стоимость. С помощью программных методов обеспечения безопасности реализованы почти все межсетевые экраны и большинство средств криптографической защиты. Основным их недостатком является доступность для хакеров, особенно это касается широко распространенных на рынке средств защиты. По целевому назначению их можно разделить на несколько классов:

- программы идентификации и аутентификации пользователей;
- программы определения прав (полномочий) пользователей;
- программы регистрации работы технических средств и пользователей (ведение так называемого системного журнала);
- программы уничтожения (затирания) информации после решения соответствующих задач или при нарушении пользователем определенных правил обработки информации.

Программные средства защиты информации часто делят на средства, реализуемые в стандартных операционных системах (ОС), и средства защиты в специализированных информационных системах.

Криптографические программы основаны на использовании методов шифрования или кодирования информации. Данные методы являются достаточно надежными средствами защиты, значительно повышающими безопасность передачи информации в сетях.

Аппаратно-программные средства защиты основаны на использовании технологических устройств, допускающих некоторую настройку параметров их работы программными методами. Они представляют собой компромисс между предыдущими двумя средствами и совмещают высокую производительность аппаратно реализованных систем и гибкость настройки программных. Типичными представителями такого рода устройств является аппаратно реализованные маршрутизаторы фирмы Cisco, которые допускают их настройку в качестве пакетных фильтров (межсетевых экранов).

Организационные и законодательные средства защиты информации предусматривают создание системы нормативно-правовых документов, регламентирующих порядок разработки, внедрения и эксплуатации ИС, а также ответственность должностных и юридических лиц за нарушение установленных правил, законов, приказов, стандартов и т.п.

Организационные средства осуществляют регламентацию производственной деятельности и использования компьютеров в сети и взаимоотношений исполнителей на нормативно-правовой основе таким образом, что разглашение, утечка и несанкционированный доступ к конфиденциальной информации становятся невозможными или существенно затрудняются за счет проведения организационных мероприятий. Комплекс этих мер реализуется группой информационной безопасности, но должен находиться под контролем первого руководителя. Организационные меры должны охватывать этапы проектирования, внедрения и эксплуатации информационных систем. Они обеспечивают объединение всех используемых средств защиты в единый механизм.

Законодательные средства защиты определяются законодательными актами страны, которыми регламентируются правила пользования, обработки и передачи информации ограниченного доступа и устанавливаются меры ответственности за нарушение этих правил. Основной целью законодательных средств является предупреждение и сдерживание потенциальных нарушителей.

Морально-этические средства защиты информации основаны на использовании моральных и этических норм, господствующих в обществе. Они включают всевозможные нормы поведения, которые традиционно сложились ранее, складываются по мере распространения информационных технологий в стране и в мире или специально разрабатываются. Морально-этические нормы могут быть неписаные (например, честность), либо оформленные в некий свод (устав) правил или предписаний. Эти нормы, как правило, не являются законодательно утвержденными, но поскольку их несоблюдение приводит к падению престижа организации, они считаются обязательными для исполнения.

5.2. Классификация удаленных атак на распределенные вычислительные системы

Основной особенностью любой распределенной системы является то, что ее компоненты распределены в пространстве и связь между ними физически осуществляется при помощи сетевых соединений и программно при помощи механизма сообщений. При этом все управляющие сообщения и данные, пересылаемые между объектами распределенной ВС, передаются по сетевым соединениям в виде пакетов обмена. Эта особенность и является основной для удаленных атак на инфраструктуру и протоколы IP-сетей.

Удаленные атаки можно классифицировать по следующим признакам:

Рис.5.2. Классификация удалённых атак на РВС

5.2.1. По характеру воздействия:

1. ***Пассивное воздействие*** на распределенную вычислительную систему не оказывает непосредственного влияния на работу системы, но может нарушать ее политику безопасности. Примером пассивного типового удаленного воздействия в РВС служит прослушивание канала связи в сети. Именно отсутствие непосредственного влияния на работу распределенной ВС приводит к тому, что пассивное удаленное воздействие практически невозможно обнаружить.
2. ***Активное воздействие*** оказывает непосредственное влияние на работу системы (изменение конфигурации РВС, нарушение работоспособности и т. д.) и нарушает принятую в ней политику безопасности. Практически все типы удаленных атак являются активными воздействиями.

5.2.2. По цели воздействия

- нарушение конфиденциальности информации либо ресурсов системы
- нарушение целостности информации
- нарушение работоспособности (доступности) системы

Угрозы нарушения конфиденциальности направлены на разглашение конфиденциальной или секретной информации. При реализации этих угроз

информация становится известной лицам, которые не должны иметь к ней доступ.

Угрозы нарушения целостности информации, хранящейся в компьютерной системе или передаваемой по каналу связи, направлены на её изменение или искажение, приводящее к нарушению её качества или полному уничтожению. Целостность информации может быть нарушена умышленно злоумышленником, а также в результате объективных воздействий со стороны среды, окружающей систему. Эта угроза особенно актуальна для систем передачи информации - компьютерных сетей и систем телекоммуникации.

Угрозы нарушения работоспособности (отказ в обслуживании) направлены на создание таких ситуаций, когда определённые преднамеренные действия либо снижают работоспособность системы, либо блокируют доступ к некоторым её ресурсам. Его основная цель - добиться, чтобы операционная система на атакуемом объекте вышла из строя и для всех остальных объектов системы доступ к ресурсам атакованного объекта был бы невозможен. Примером удаленной атаки, целью которой является нарушение работоспособности системы, может служить "Отказ в обслуживании".

Этот классификационный признак является прямой проекцией трех основных типов угроз - раскрытия, целостности и отказа в обслуживании.

Основная цель практически любой атаки - получить несанкционированный доступ к информации. Существуют две принципиальные возможности доступа к информации:

- перехват
- искажение.

Возможность перехвата информации означает получение к ней доступа, но невозможность ее модификации. Следовательно, перехват информации ведет к нарушению ее конфиденциальности. Примером перехвата информации может служить анализ сетевого трафика в сети. В этом случае имеется несанкционированный доступ к информации без возможности ее искажения. Очевидно также, что нарушение конфиденциальности информации является пассивным воздействием.

Возможность искажения информации означает либо полный контроль над информационным потоком между объектами системы, либо возможность передачи сообщений от имени другого объекта. Таким образом, очевидно, что искажение информации ведет к нарушению ее целостности. Данное информационное разрушающее воздействие представляет собой яркий пример активного воздействия. Примером удаленной атаки, цель которой нарушение целостности информации, может служить типовая удаленная атака (УА) "Ложный объект РВС".

Опасные воздействия можно разделить на: случайные и преднамеренные

Причины случайных воздействий:

- аварийные ситуации из-за стихийных бедствий и отключения электроэнергии;
- отказы и сбои аппаратуры;
- ошибки в программном обеспечении;
- ошибки в работе обслуживающего персонала и пользователей;
- помехи в линии связи из-за воздействия внешней среды.

5.2.3. По условию начала осуществления воздействия

Удаленное воздействие, также как и любое другое, может начать осуществляться только при определенных условиях. В распределенных ВС существуют три вида условий начала осуществления удаленной атаки:

- Атака по запросу от атакуемого объекта. При этом атакующий ожидает передачи от потенциальной цели атаки запроса определенного типа, который и будет условием начала осуществления воздействия. Примером подобных запросов в ОС Novell NetWare[1] может служить SAP[2]-запрос, а в сети Internet - DNS[3]- и ARP-запросы[4]. Важно отметить, что данный тип удаленных атак наиболее характерен для распределенных ВС.
- Атака по наступлению ожидаемого события на атакуемом объекте. При этом атакующий осуществляет постоянное наблюдение за состоянием операционной системы удаленной цели атаки и при возникновении определенного события в этой системе начинает воздействие. Как и в предыдущем случае, инициатором осуществления начала атаки выступает сам атакуемый объект. Примером такого события может быть прерывание сеанса работы пользователя с сервером в ОС Novell NetWare без выдачи команды LOGOUT.
- Безусловная атака. При этом начало осуществления атаки безусловно по отношению к цели атаки, то есть атака осуществляется немедленно и безотносительно к состоянию системы и атакуемого объекта. Следовательно, в этом случае атакующий является инициатором начала осуществления атаки.

[1] ОС Novell NetWare - семейство сетевых операционных систем, созданных фирмой Novell

[2] SAP - [Service Advertising Protocol] протокол извещения об услугах; протокол рекламы сервиса (в сетях IPX используется файловыми серверами для передачи информации о своей доступности и имени клиентам)

[3] DNS - [Domain Name System] служба имен доменов (механизм, используемый в сети Internet и устанавливающий соответствие между числовыми IP-адресами и текстовыми именами)

[4] ARP[Address Resolution Protocol] протокол разрешения адресов (протокол из семейства TCP/IP, обеспечивающий преобразование IP-адреса в MAC-адрес (MAC address) для пакетов IP)

5.2.4. По наличию обратной связи с атакуемым объектом

- с обратной связью
- без обратной связи (однонаправленная атака)

Удаленная атака, осуществляемая при наличии обратной связи с атакуемым объектом, характеризуется тем, что на некоторые запросы, переданные на атакуемый объект, атакующему требуется получить ответ, а, следовательно, между атакующим и целью атаки существует обратная связь, которая позволяет атакующему адекватно реагировать на все изменения, происходящие на атакуемом объекте. Подобные удаленные атаки наиболее характерны для распределенных ВС.

Атаки без обратной связи обычно осуществляются передачей на атакуемый объект одиночных запросов, ответы на которые атакующему не нужны. Подобную угрозу можно называть однонаправленной удаленной атакой. Примером однонаправленных атак является "Отказ в обслуживании".

5.2.5. По расположению субъекта атаки относительно атакуемого объекта

В случае внутрисегментной атаки, субъект и объект атаки находятся в одном сегменте. При межсегментной атаке субъект и объект атаки находятся в разных сегментах.

Данный классификационный признак позволяет судить о так называемой "степени удаленности" атаки.

На практике межсегментную атаку осуществить значительно труднее, чем внутрисегментную, однако межсегментная удаленная атака представляет гораздо большую опасность, чем внутрисегментная. Это связано с тем, что в случае межсегментной атаки объект её и непосредственно атакующий могут находиться на расстоянии многих тысяч километров друг от друга, что может существенно воспрепятствовать мерам по отражению атаки.

В общем виде все атаки делятся на:

- внутренние атаки
- внешние атаки

Внутренние атаки инициируются персоналом объекта, на котором установлена система, содержащая КИ.

Внешние атаки возникают благодаря непосредственной деятельности недобросовестных конкурентов, преступных элементов, иностранных разведывательных служб, из-за неумелой постановки взаимоотношений с

представителями государственных структур, общественных организаций, средств массовой информации. Действия извне могут быть направлены на пассивные носители информации следующими способами:

1. похищение или снятие копий с различных носителей информации;
2. снятие информации в процессе коммуникации;
3. снятие информации в процессе её передачи по сети связи;
4. уничтожение информации или повреждение ее носителей;
5. случайное или преднамеренное доведение до сведения конкурентов документов и материалов, содержащих секретную информацию.

Внешние угрозы (в случае коммерческой информации), как правило, выступают в форме промышленного шпионажа. В ходе конкурентной борьбы использование промышленного шпионажа нельзя отнести к этическим видам деловых взаимоотношений предпринимателей. Однако любая предпринимательская деятельность, как показывает зарубежная практика, без него немыслима. Самый благоприятный общественно-экономический климат для развития предпринимательства не сможет предотвратить банкротства, если в результате удачной шпионской акции будут похищены секретные для фирмы сведения.

5.2.6. По уровню эталонной модели ISO/OSI, на котором осуществляется воздействие

Международная Организация по Стандартизации (ISO) приняла стандарт ISO 7498, описывающий взаимодействие открытых систем (OSI). Распределенные ВС также являются открытыми системами. Любой сетевой протокол обмена, как и любую сетевую программу, можно с той или иной степенью точности спроецировать на эталонную семиуровневую модель OSI. Такая многоуровневая проекция позволит описать в терминах модели OSI функции, заложенные в сетевой протокол или программу. Удаленная атака также является сетевой программой. В связи с этим представляется логичным рассматривать удаленные атаки на распределенные ВС, проецируя их на эталонную модель ISO/OSI.

5.3. Принципы создания защищенных систем связи в распределенных вычислительных системах

При построении защищенных систем следует бороться не с угрозами, являющимися следствием недостатков системы, а с причинами возможного успеха атак.

5.3.1. Выделенный канал связи между объектами распределенной ВС

Использование в РВС для связи между объектами широковещательной среды передачи означает, что все объекты распределенной ВС подключаются к одной общей шине, это приводит к тому, что сообщение, предназначенное

(адресованное) только одному объекту системы, будет получено всеми ее объектами. Однако только объект, адрес которого указан в заголовке сообщения как адрес назначения, будет считаться тем объектом, кому это сообщение непосредственно направлялось. Очевидно, что в РВС с топологией "общая шина" необходимо использовать специальные методы идентификации объектов, так как идентификация на канальном уровне возможна только в случае использования сетевых криптокарт.

Идеальным с точки зрения безопасности будет взаимодействие объектов распределенной ВС по выделенным каналам. Существуют два возможных способа организации топологии распределенной ВС с выделенными каналами. В первом случае каждый объект связывается физическими линиями связи со всеми объектами системы. Во втором случае в системе может использоваться сетевой концентратор, через который осуществляется связь между объектами (топология "звезда").

Достоинства:

- передача сообщений осуществляется напрямую между источником и приемником, минуя остальные объекты системы. В такой системе в случае отсутствия доступа к объектам, через которые осуществляется передача сообщения, не существует программной возможности для анализа сетевого трафика;
- имеется возможность идентифицировать объекты распределенной системы на канальном уровне по их адресам без использования специальных криптоалгоритмов шифрования трафика, поскольку система построена так, что по данному выделенному каналу осуществима связь только с одним определенным объектом. Появление в такой распределенной системе ложного объекта невозможно без аппаратного вмешательства (подключение дополнительного устройства к каналу связи);
- система с выделенными каналами связи - это система, в которой отсутствует неопределенность с информацией о ее объектах. Каждый объект в такой системе изначально однозначно идентифицируется и обладает полной информацией о других объектах системы.

Недостатки:

- сложность реализации и высокие затраты на создание системы;
- ограниченное число объектов системы (зависит от числа входов у концентратора);
- сложность внесения в систему нового объекта.

Наилучшее с точки зрения безопасности взаимодействие объектов в РВС возможно только по физически выделенному каналу.

5.3.2. Виртуальный канал как средство обеспечения дополнительной идентификации/аутентификации объектов в распределенной ВС

На практике обеспечить взаимодействие всех объектов по выделенному каналу достаточно сложно и, нельзя не предусмотреть вариант физического подключения к каналу. Следовательно, разработчик защищенной системы связи в распределенной ВС должен исходить из следующего принципа:

При построении защищенной системы связи в РВС необходимо учитывать, что все сообщения, передаваемые по каналу связи, могут быть перехвачены, но это не должно повлечь за собой нарушения безопасности системы в целом. Следовательно: необходимо ввести дополнительные средства идентификации объектов в РВС и криптозащиту сообщений передаваемых по каналу связи.

Идентификация объектов РВС, в отсутствие статической ключевой информации, возможна только при взаимодействии объектов с использованием виртуального канала. Поэтому, для того, чтобы ликвидировать причину успеха удаленных атак, необходимо руководствоваться следующим правилом:

Любое взаимодействие двух объектов в распределенной ВС должно проходить по виртуальному каналу связи.

Для этого при создании ВК могут использоваться криптоалгоритмы с открытым ключом (например Secret Socket Layer - SSL). Данные криптоалгоритмы основаны на результатах исследований, полученных в 70-х годах У. Диффи. Он ввел понятие односторонней функции с потайным входом. Это не просто вычисляемая в одну сторону функция, обращение которой невозможно, она содержит потайной вход (trapdoor), который позволяет вычислять обратную функцию лицу, знающему секретный ключ. Сущность криптографии с открытым ключом (или двухключевой криптографии) в том, что ключи, имеющиеся в криптосистеме, входят в нее парами и каждая пара удовлетворяет следующим двум свойствам:

- текст, зашифрованный на одном ключе, может быть дешифрован на другом;
- знание одного ключа не позволяет вычислить другой.

Поэтому один из ключей может быть опубликован. При опубликованном (открытом) ключе шифрования и секретном ключе дешифрования получается система шифрования с открытым ключом. Каждый пользователь сети связи может зашифровать сообщение при помощи открытого ключа, а расшифровать его сможет только владелец секретного ключа. При опубликовании ключа дешифрования получается система цифровой подписи. Здесь только владелец секретного ключа создания подписи может правильно зашифровать текст (т.е. подписать его), а проверить подпись (дешифровать текст) может любой на основании опубликованного ключа проверки подписи.

Для обеспечения надежной идентификации объектов распределенной ВС при создании виртуального канала необходимо использовать криптоалгоритмы с открытым ключом.

5.3.3. Контроль за маршрутом сообщения в распределенной ВС

Каждый объект распределенной ВС должен обладать адресом, уникально его идентифицирующим. Для того, чтобы сообщение от одного объекта было передано на другой объект системы, оно должно пройти через цепь маршрутизаторов, маршрут до объекта определяется цепочкой узлов, пройденных сообщением, который может являться информацией, аутентифицирующей с точностью до подсети подлинность адреса субъекта, отославшего сообщение. Очевидно, что перед любой системой связи объектов в РВС встает стандартная проблема проверки подлинности адреса сообщения, пришедшего на объект. Эту задачу, с одной стороны, можно решить, введя дополнительную идентификацию сообщений на другом, более высоком уровне OSI. Так, адресация осуществляется на сетевом уровне, а дополнительная идентификация, например, на транспортном. Однако подобное решение не позволит избежать проблемы контроля за созданием соединений, так как дополнительная идентификация абонентов будет возможна только после создания соединения.

Функцию проверки подлинности адреса отправителя можно возложить на маршрутизатор, так как он может отследить, откуда к нему пришел пакет и проверить соответствие адреса отправителя с адресом соответствующей подсети, откуда пришло сообщение. В случае совпадения сообщение пересылается далее, а в противном случае - отфильтровывается. Этот способ позволит на начальной стадии отбросить пакеты с неверными адресами отправителя.

Другой вариант решения может состоять в создании в заголовке пакета специальных полей, куда каждый маршрутизатор, через который проходит пакет, заносит маршрутную информацию (часть своего адреса, например). При этом первый маршрутизатор, на который поступил пакет, заносит также информацию о классе сети (A, B, C), откуда пришел пакет. Тем не менее, внесение в пакет адресов всех пройденных по пути маршрутизаторов будет неоптимальным решением, так как в этом случае сложно заранее определить максимальный размер заголовка пакета.

Когда сообщение дойдет до конечного адресата, в его заголовке будет полностью отмечен пройденный маршрут. По этому маршруту, вне зависимости от указанного в пакете сетевого адреса отправителя, можно, во-первых, с точностью до подсети идентифицировать подлинность адреса и, во-вторых, определить с точностью до подсети истинный адрес отправителя. Итак, получив подобное сообщение с указанным маршрутом, сетевая операционная система анализирует маршрут и проверяет подлинность адреса отправителя. В случае его недостоверности пакет отбрасывается.

В распределенной ВС необходимо обеспечить на сетевом уровне контроль за маршрутом сообщений для аутентификации адреса отправителя.

5.3.4. Контроль за виртуальными соединениями в распределенной ВС

Если в системе связи удаленных объектов РВС не предусмотреть использование надежных алгоритмов контроля за соединением, то, избавившись от одного типа удаленных атак на соединение ("Подмена доверенного объекта"), можно подставить систему под другую типовую УА - "Отказ в обслуживании". Поэтому для обеспечения надежного функционирования и работоспособности (доступности) каждого объекта распределенной ВС необходимо прежде всего контролировать процесс создания соединения. Задача контроля за ВК распадается на две подзадачи:

- контроль за созданием соединения;
- контроль за использованием соединения.

Решение второй задачи лежит на поверхности: так как сетевая операционная система не может одновременно иметь бесконечное число открытых ВК, то в том случае, если ВК простаивает в течение определенного системой тайм-аута, происходит его закрытие.

Основная задача контроля за созданием соединения в РВС состоит в том, чтобы не позволить одному субъекту взаимодействия занять все виртуальные каналы системы. При создании ВК полученный системой запрос на создание соединения ставится в очередь запросов, и, когда до него дойдет время, система выработает ответ на запрос и отошлет его обратно отправителю запроса. Задача контроля за созданием соединения заключается как раз в том, чтобы определить те правила, исходя из которых система могла бы либо поставить запрос в очередь, либо нет. Если все пришедшие запросы автоматически ставятся системой в очередь (так построены все сетевые ОС, поддерживающие протокол TCP/IP), то это в случае атаки ведет к переполнению очереди и к отказу в обслуживании всех остальных легальных запросов. Это происходит, когда атакующий посылает в секунду столько запросов, сколько позволит трафик (тысячи запросов в секунду), а обычный пользователь с легальным запросом на подключение может послать лишь несколько запросов в минуту! Поэтому необходимо ввести ограничение на число обрабатываемых в секунду запросов из одной подсети. Вводимое ограничение не позволит атакующему переполнить очередь, так как только первые несколько его запросов будут поставлены в очередь на обслуживание, а остальные будут игнорироваться. Первый же запрос легального пользователя из другой подсети будет также сразу поставлен в очередь.

К минусам этого способа решения проблемы контроля за созданием соединения можно отнести тот факт, что, так как адрес отправителя можно аутентифицировать с точностью только до подсети, то атакующий может посылать запросы от имени любого объекта данной подсети. Следовательно, в случае атаки все остальные объекты из подсети атакующего будут лишены

возможности подключения к атакуемому объекту. Однако, так как, во-первых, атакующего по указанному в пакете маршруту можно будет вычислить с точностью до его подсети и, во-вторых, не произойдет нарушения работоспособности цели атаки, то такая атака вряд ли будет иметь смысл.

Необходимо обеспечить контроль за созданием соединения, введя ограничение на число обрабатываемых в секунду запросов из одной подсети.

Необходимо обеспечить контроль за использованием соединения, разрывая его по тайм-ауту в случае отсутствия сообщений.

5.3.5. Проектирование РВС с полностью определенной информацией о ее объектах с целью исключения алгоритмов удаленного поиска

Одной из особенностей распределенной ВС является возможное отсутствие информации, необходимой для доступа к ее удаленным объектам. Поэтому в РВС возникает необходимость использования потенциально опасных с точки зрения безопасности алгоритмов удаленного поиска. Следовательно, для того, чтобы в РВС не возникало необходимости в использовании данных алгоритмов, требуется на начальном этапе спроектировать систему так, чтобы информация о ее объектах была изначально полностью определена.

Однако в РВС с неопределенным и достаточно большим числом объектов (например, Internet) спроектировать систему с отсутствием неопределенности практически невозможно. В этом случае отказаться от алгоритмов удаленного поиска не представляется возможным.

Существуют два типа данных алгоритмов. Первый типовой алгоритм удаленного поиска − с использованием информационно-поискового сервера, второй − с использованием широковещательных запросов. Применение в РВС алгоритма удаленного поиска с использованием широковещательных запросов в принципе не позволяет защитить систему от внедрения в нее ложного объекта, а, следовательно, использование данного алгоритма в защищенной системе недопустимо. Применение в распределенной ВС алгоритма удаленного поиска с использованием информационно-поискового сервера позволяет обезопасить систему от внедрения в нее ложного объекта только в том случае, если, во-первых, взаимодействие объектов системы с сервером происходит только с созданием виртуального канала и, во-вторых, у объектов, подключенных к данному серверу, и у сервера существует заранее определенная статическая ключевая информация, используемая при создании виртуального канала. Выполнение этих условий сделает невозможным в распределенной ВС передачу в ответ на запрос с объекта ложного ответа и, следовательно, внедрения в систему ложного объекта.

В том случае, если виртуальный канал с информационно-поисковым сервером создается с использованием только динамически вырабатываемой ключевой информации, например, по схеме открытого распределения ключей,

то ничто не мешает атакующему (в том случае, если он может перехватить первоначальный запрос на создание ВК с объекта системы) послать ложный ответ и создать виртуальный канал от имени настоящего сервера. Именно поэтому на всех объектах системы необходима начальная ключевая информация для создания ВК с информационно-поисковым сервером.

Наиболее безопасной распределенной ВС является та система, в которой информация о её объектах изначально полностью определена и в которой не используются алгоритмы удаленного поиска. В том случае, если выполнить это требование невозможно, необходимо в распределенной ВС использовать только алгоритм удаленного поиска с выделенным информационно-поисковым сервером, и при этом взаимодействие объектов системы с данным сервером должно осуществляться только по виртуальному каналу с применением надежных алгоритмов защиты соединения с обязательным использованием статической ключевой информации. В распределенной ВС для обеспечения безопасности необходимо отказаться от алгоритмов удаленного поиска с использованием широковещательных запросов.

В сети Internet в стандарте IPv4 практически ни одно из сформулированных требований к построению безопасных систем связи между удаленными объектами распределенных ВС не выполняется. Поэтому группы разработчиков уже заканчивают проект создания нового более защищенного стандарта сети Internet - IPv6, где будут, по-видимому, учтены некоторые из вышеизложенных требований. Однако разговор о том, насколько будет безопасна сеть Internet в новом стандарте, несколько преждевременен, и его необходимо отложить до окончательного выхода стандарта в свет.

Вопросы к экзамену по дисциплине

«Безопасность сетей ЭВМ»

1. Классификация компьютерных сетей.
2. Топологии компьютерных сетей.
3. Топология «Общая шина».
4. Топология «Звезда».
5. Топология «Кольцо».
6. Древовидная топология.
7. Сетевые топологии.
8. Стандарты кабелей вычислительных сетей.
9. Кабели на основе неэкранированной витой пары UTP.
10. Кабели на основе экранированной витой пары STP.
11. Коаксиальные кабели.
12. Волоконно-оптические кабели.
13. Структурированная кабельная система. Преимущества использования СКС.
14. Выбор типа кабеля для горизонтальных подсистем.
15. Выбор типа кабеля для вертикальных подсистем.
16. Выбор типа кабеля для подсистемы кампуса.
17. Распределённые вычислительные системы
18. Мультипроцессорные компьютеры.
19. Многомашинные системы.
20. Вычислительные сети.
21. Распределенные программы.
22. Прозрачность ресурсов сети.
23. Аппаратура локальных сетей.
24. Сетевые адаптеры.
25. Трансиверы и Репитеры.
26. Концентраторы и коммутаторы.
27. Маршрутизаторы, мосты и шлюзы.
28. Структура стандартов IEEE 802.X.
29. Общая характеристика протоколов локальных сетей.
30. Многоуровневая структура стека TCP/IP.
31. Соответствие уровней стека TCP/IP семиуровневой модели ISO/OSI.
32. Технология Ethernet (IEEE 802.3).
33. Метод доступа CSMA/CD.
34. Технология Fast Ethernet (IEEE 802.3u).
35. Технология 100VG-AnyLAN (IEEE 802.12).
36. Технология Gigabit Ethernet (IEEE 802.3z).
37. Gigabit Ethernet на витой паре категории 5 (IEEE 802.3ab).
38. Технология 10Gigabit Ethernet (IEEE 802.3ae).
39. Функции и архитектура систем управления сетями.
40. Многоуровневое представление задач управления.
41. Архитектуры систем управления сетями.
42. Структуры распределенных систем управления.
43. Способы и средства защиты информации в сетях.
44. Способы защиты информации в сетях.
45. Средства защиты информации в сетях.
46. Классификация удаленных атак на распределенные вычислительные системы.
47. Принципы создания защищенных систем связи в распределенных вычислительных системах.
48. Выделенный канал связи между объектами распределенной ВС.
49. Виртуальный канал как средство обеспечения дополнительной идентификации/аутентификации объектов в распределенной ВС.
50. Контроль за маршрутом сообщения в распределенной ВС.
51. Контроль за виртуальными соединениями в распределенной ВС.
52. Проектирование РВС с полностью определенной информацией о ее объектах с целью исключения алгоритмов удаленного поиска.

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное бюджетное государственное образовательное учреждение высшего профессионального образования «САМАРСКИЙ ГОСУДАРСТВЕННЫЙ АЭРОКОСМИЧЕСКИЙ УНИВЕРСИТЕТ имени академика С.П.КОРОЛЕВА (национальный исследовательский университет)»

«СОГЛАСОВАНО»
Управление образовательных программ

_____

«_____»_____2012г.

«УТВЕРЖДАЮ»
Проректор по учебной работе

_____

«_____»_____2012г.

РАБОЧАЯ ПРОГРАММА

По **Безопасность сетей ЭВМ**
(наименование дисциплины или практики по учебному плану)

федерального, национально-регионального компонента, по выбору студента, факультативная дисциплина специализации для специальности (специализации)
(нужное подчеркнуть)

090105.65 Комплексное Обеспечение Информационной Безопасности Автоматизированных Систем (специалист)
(коды и наименования специальностей и направлений подготовки, специализации, формы обучения)

Цикл: Общенаучный
Часть цикла: Базовая
Код учебного плана: (ОПД.Ф.07)

Факультеты №: **6**
Кафедра **геоинформатики и информационной безопасности**

Курс **4**

Семестр **7**

Лекции **36** (часов) Экзамен **7** (семестр)
Лабораторные занятия **36** (часов) Зачет **-** (семестр)
Практические занятия **-** (часов)
Курсовой проект (работа) **-** (часов)
Самост. и индивидуальная. работа **130** (часов)
Самост. подготовка и сдача экз-ов **14** (часов)
Всего часов **216**

2012 г.

Рабочая программа составлена на основании:

Федерального государственного образовательного стандарта высшего профессионального образования по направлению подготовки 090105.65 «Комплексное обеспечение информационной безопасности автоматизированных систем»

(наименование государственных образовательных стандартов специальностей и направлений, учебных планов, типовых программ)

Соответствие содержания рабочей программы, условий ее реализации, материально-технической и учебно-методической обеспеченности учебного процесса по дисциплине всем требованиям государственных образовательных стандартов подтверждаем.

Составители: Кузнецов М.В., к.т.н., доцент кафедры ГИиИБ

(Ф.И.О., ученое звание, степень место работы, подпись)

Заведующий кафедрой ГИиИБ _____ д.т.н., проф. Сергеев В.В.

(Ф.И.О., подпись)

Рабочая программа обсуждена на заседании кафедры ГИиИБ
Протокол № _____ от «_____» _____2012г.

1 Цели и задачи дисциплины, её место в учебном плане, требования к уровню освоения содержания дисциплины

1.0 Перечень развиваемых компетенций

ПК – профессиональная компетенция

(ПК-3) способностью использовать языки, системы и инструментальные средства программирования в профессиональной деятельности;

(ПК-5) способностью применять методологию научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами;

(ПК-8) способностью к освоению новых образцов программных, технических средств и информационных технологий;

(ПК-11) способностью разрабатывать и исследовать модели автоматизированных систем;

(ПК-15) способностью проводить анализ, предлагать и обосновывать выбор решений по обеспечению требуемого уровня эффективности применения автоматизированных систем;

(ПК-19) способностью участвовать в разработке компонентов автоматизированных систем в сфере профессиональной деятельности;

(ПК-30) способностью организовать эксплуатацию автоматизированной системы с учетом требований информационной безопасности;

(ПК-40) способностью обеспечить восстановление работоспособности систем защиты информации при возникновении нештатных ситуаций.

(ПСК-7.1) способностью разрабатывать и исследовать модели информационно-технологических ресурсов в распределенных информационных системах;

1.1.Цели и задачи изучения дисциплины

Цели дисциплины:

Дисциплина «Безопасность сетей ЭВМ» имеет целью обучить студентов основам построения и эксплуатации вычислительных сетей, принципам и методам защиты информации в компьтерных сетях, навыкам комплексного проектирования, построения, обслуживания и анализа защищенных вычислительных сетей. Дисциплина является базовой для изучения дисциплин по комплексному и организационному обеспечению информационной безопасности. Знания и практические навыки, полученные из курса «Безопасность сетей ЭВМ», используются обучаемыми при проектировании дипломных работ.

Задачи дисциплины - дать основы:

- архитектуры вычислительных сетей;
- программно-аппаратных и технических средств создания сетей;
- принципов построения сетей и управления ими;
- использования программных и аппаратных технологий защиты сетей;

- методологии проектирования, развертывания и сопровождения безопасных сетей;
- обследования и анализа защищенных вычислительных сетей.

1.2. Требования к уровню подготовки студента, завершившего изучение данной дисциплины

В результате изучения дисциплины студенты (слушатели) должны
иметь представление:

- о перспективных направлениях развития технологий обеспечения безопасности в сетях;
- о современных проблемах науки информационной безопасности и роли и месте защиты информации в сетях при решении задач, связанных с обеспечением комплексной информационной безопасности.

знать:

- методологические и технологические основы обеспечения информационной безопасности сетевых автоматизированных систем;
- угрозы и методы нарушения информационной безопасности сетевых автоматизированных систем;
- типовые модели атак, направленных на преодоление защиты сетевых автоматизированных систем, условия их осуществимости, возможные последствия, способы предотвращения;
- роль человеческого фактора в обеспечении безопасности сетей;
- возможности, способы и правила применения основных программных и аппаратных средств защиты информации в сетях;
- принципы функционирования основных защищенных сетевых протоколов;
- основы применения межсетевых экранов для защиты сетей;
- правила определение политики сетевой безопасности;
- стандарты по оценке защищенных сетевых систем и их теоретические основы;
- методы и средства проектирования, реализации и оценки защищенных сетевых систем.

уметь:

- проводить анализ сетевых автоматизированных систем с точки зрения обеспечения информационной безопасности;
- разрабатывать модели и политику сетевой безопасности, используя известные подходы, методы, средства и теоретические основы;
- применять стандарты по оценке защищенных сетевых систем при анализе и проектировании систем защиты информации в автоматизированных системах;

- применять защищенные протоколы и межсетевые экраны, необходимые для реализации систем защиты информации в сетях;
- реализовывать меры противодействия выявленным угрозам сетевой безопасности с использованием различных программных и аппатарных средств защиты в соответствии с правилами их применения;
- реализовывать системы защиты информации в автоматизированных системах в соответствии со стандартами по оценке защищенных систем.

иметь навыки:

- построения и эксплуатации вычислительных сетей;
- проектирования защищенных сетей;
- комплексного анализа и оценки сетевой безопасности.

1.3.Связь с предшествующими дисциплинами

Для успешного усвоения курса студенты должны изучить следующие дисциплины:

1) Теоретические основы компьютерной безопасности;
2) Системы и сети передачи информации;
3) Основы информационной безопасности.

1.4.Связь с последующими дисциплинами

Курс совместно с курсами: Системы и сети передачи информации, Безопасность сетей ЭВМ, Безопасность систем баз данных, Информационная безопасность распределенных информационных систем, Методы проектирования защищенных распределенных информационных систем, он составляет основу теоретической подготовки инженеров и играет роль прикладной базы, без которой невозможна успешная деятельность инженера информационной безопасности.

2 Содержание аудиторных занятий

Наименование дисциплин и разделов, используемых в данном разделе изучаемой дисциплины	ЛЕКЦИОННЫЕ ЗАНЯТИЯ		ПРАКТИЧЕСКИЕ, СЕМИНАРСКИЕ, ЛАБОРАТОРНЫЕ И ДР. ВИДЫ АУДИТОРНЫХ ЗАНЯТИЙ				Дисциплины, использующие данный раздел
	Номер, наименование темы и раздела. Содержание раздела.	Объем в часах	Практические занятия	Объем в часах	Лабораторные работы	Объем в часах	
1	2	3	4а	5а	4б	5б	6
Семестр 1							
Теоретические основы компьютерной безопасности; Системы и сети передачи информации; Основы информационной безопасности. Теория информации	1 . Классификация вычислительных сетей. (интерактивное) 2. Сетевая архитектура и топология вычислительных сетей. (интерактивное) 3 . Типовые угрозы сетевой безопасности. (интерактивное) 4. Распределённые вычислительные системы. (интерактивное) 5. Аппаратура локальных вычислительных сетей. (интерактивное) 6. Структурированная кабельная система. (интерактивное) 7. Протоколы и стандарты локальных сетей. (интерактивное) 8. Технология Ethernet (IEEE 802.3). (интерактивное) 9. Физический уровень технологии Fast Ethernet. (интерактивное) 10. Высокоскоростная технология Gigabit Ethernet. (интерактивное) 11. Средства анализа и управления сетями. (интерактивное) 12. Архитектуры систем управления	2 2 2 2 2 2 2 2 2 2 2 2			№ 1. Основы конфигурирования маршрутизаторов. Уровни доступа, пароли. (активное) № 2. Конфигурирование стандартных списков доступа. (активное) № 3. Межсетевые экраны. Создание расширенных списков доступа. (активное) № 4. Основы конфигурирования коммутаторов. (активное) № 5. Конфигурирование виртуальных частных сетей. (активное) № 6. Динамическая IP-адресация, Конфигурирование DHCP-сервера. (активное) № 7. Моделирование защищённой вычислительной сети. (активное) № 8, 9. Отчетные занятия. (интерактивное)	4 4 4 4 4 4 8	Безопасность систем баз данных. Информационная безопасность распределенных информационных систем. Методы проектирования защищенных распределенных информационных систем.

	сетями. (интерактивное) 13. Способы и средства защиты информации в сетях. (интерактивное) 14. Классификация удаленных атак на распределенные вычислительные системы. (интерактивное) 15. Принципы создания защищенных систем связи в распределенных вычислительных системах. (интерактивное) 16. Защита рабочего места пользователя сети Интернет (интерактивное) 17. Защита каналов связи в Интернет. (интерактивное) 18. Комплексная защита подключения к Интернет. (интерактивное)	2 2 2 2 2 2					
Итого на всю дисциплину		**36**		**0**		**36**	

3 Самостоятельная работа студентов[1]

Объем часов, отводимый на самостоятельную работу студентов по рабочей программе (в соответствии с учебными планами):

7 семестр: 144

Характеристика целей и форм самостоятельной работы по данной рабочей программе.

Самостоятельная работа по дисциплине направлена на:

- Поиск и изучение дополнительной литературы и современных статей по темам изученного материала, включая электронные издания, их систематизации и подготовки обобщающего итогового реферата.
- Решение задач для подготовки к выполнению лабораторных работ и закрепления пройденного материала.
- Подготовка к отчетным занятиям.

Перечень разделов и тем, выносящихся на самостоятельное изучение, с отводимым объемом часов:

7 семестр.

1.1. Типовые угрозы сетевой безопасности: 20 (изучение теории).
1.2. Аппаратура локальных вычислительных сетей: 20 (изучение теории).
1.3. Протоколы и стандарты локальных сетей: 20 (изучение теории).
1.4. Технологии Ethernet (IEEE 802.3): 15 (изучение теории).
1.5. Способы и средства защиты информации в сетях: 25 (изучение теории).
1.6. Архитектуры систем управления сетями: 15 (изучение теории).
1.7. Комплексная защита подключения к Интернет: 15 (изучение теории).
1.8. Подготовка к экзамену: 14.

4 Текущий и промежуточный контроль знаний студентов

Наименование контрольного мероприятия	Наименование раздела (темы) дисциплины	Срок проведения (неделя семестра или номер занятия)	Форма оценивания результата и дополнительные сведения (балльная оценка, допуск/ недопуск, % выполнения и т.п.)
1	2	3	4
Отчет по лабораторным работам	Все разделы	Каждое лабораторное занятие; отчетные занятия, 16 и 17 недели	Зачет / незачет % выполнения
экзамен	Все разделы	Согласно расписанию	Бальная оценка

5 Инновационные методы обучения[2]

5.1 Выполнение лабораторных работ с элементами исследования;

[1] - Подробное распределение часов по разделам и темам самостоятельной работы указывается по усмотрению составителей программы и заведующего кафедрой.

[2] В случае использования традиционных методов и средств обучения это необходимо отметить явно.

5.2 Компьютерное имитационное моделирование вычислительных сетей в лабораторных работах.

5.3 Решение прикладных задач исследовательского характера.

5.3 Прием отчётов по лабораторным работам в форме «круглого стола» для групп из 2-3 студентов.

6 Технические средства и материальное обеспечение учебного процесса[3]

6.1 Компьютерный класс, используемый при проведении лабораторного практикума и практических занятий.

6.2 Обучающие компьютерные программы, для демонстрации и изучения принципов построения и защиты вычислительных сетей.

7 Учебно-методическое обеспечение

7.1 Основная литература[4]:

7.1.1 Родичев Ю.А. КОМПЬЮТЕРНЫЕ СЕТИ: архитектура, технологии, защита: учеб. пособие для вузов. – Самара: изд-во «Универс-групп», 2006. – 468с.

7.1.2 Олифер В. Г., Олифер Н. А. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. 3-е изд. — СПб.: Питер, 2006. — 958 с: ил.

7.1.3 Крук Б.И., Попантонопуло В.Н., Шувалов В.П. Телекоммуникационные системы и сети – современные технологии. Т.1, – М.: Горячая линия – Телеком, 2003. – 647с.

7.2 Дополнительная литература[5]:

7.2.1 Уэнделл Одом Компьютерные сети. Первый шаг = Computer Networking First-step. — М.: «Вильямс», 2005. — С. 432. — ISBN 1-58720-101-1

7.2.2 Ершов В.А., Кузнецов В.А. Мультисервисные телекоммуникационные сети. М.: МГТУ им. Н.Э. Баумана, 2003, 432 с.: ил.

7.2.3 Cisco Systems, Inc. Программа сетевой академии Cisco CCNA 3 и 4. Вспомогательное руководство = Cisco Networking Academy Program CCNA 3 and 4 Companion Guide. — М.: «Вильямс», 2006. — С. 944. — ISBN 1-58713-113-7

7.2.4 Шмалько А.В. Цифровые сети связи: основы проектирования и построения. – М.: Эко-Трендз, 2001. – 282с.

7.2.5 Ломовицкий В.В., Михайлов А.И., Шестак К.В., Шекотихин К.В. Основы построения систем и сетей передачи информации. Уч. пособие. М.: Горячая линия-Телеком, 2005, 382 с.: ил.

7.3Электронные источники и интернет-ресурсы[6]

[3] Приводятся только самые основные технические средства, используемые в учебном процессе. По усмотрению составителей программы и заведующего кафедрой раздел может быть раскрыт с подробной детализацией.

[4] Указывается не более трех наименований. Информация о количестве экземпляров указывается составителями по решению кафедры.

[5] Приводится не более пяти наименований.

7.4 Методические указания и рекомендации

Текущий контроль знаний студентов в каждом семестре завершается на отчетном занятии, результатом которого является допуск или недопуск студента к экзамену по дисциплине. Основанием для допуска к экзамену является выполнение и отчет студента по всем лабораторным работам, и прием индивидуального задания. Неудовлетворительная оценка по контрольной работе не лишает студента права сдавать экзамен, но может быть основанием для дополнительного вопроса (задания) на экзамене.

Промежуточный контроль знаний студентов проводят в виде отчёта, который проводится согласно положению о текущем и промежуточном контроле знаний студентов, утвержденному ректором университета. Экзамен ставится на основании письменного и устного ответов студента по билету, который включает два теоретических вопроса и задачу.

Приложение. Распределение типов занятий[7]

Распределение типов занятий. Семестр 1

Вид занятия	Тип занятия (в часах)		
	активные	интерактивные	традиционные
Лекция	0	36	0
Практика			
Лабораторная работа	28	8	0
Курсовая работа			
Самостоятельная работа студента	50	50	44
ИТОГО (в часах):	78	94	44
ИТОГО (в %):	36	44	20

[6] Приводятся апробированные интернет-ресурсы и электронные курсы.

[7] См. Федеральный стандарт, глава 7 («Требования…»)