Федеральное государственное бюджетное образовательное
учреждение высшего профессионального образования
«Вятский государственный гуманитарный университет»

Дополнительная подготовка школьников по дисциплине «Информатика и информационные технологии»

Учебный модуль
Основы компьютерных сетей

Е. В. Котельников

Киров
2011

СОДЕРЖАНИЕ

1. Введение в компьютерные сети

1.1. Основные понятия

Компьютерная сеть (computer network) – объединение связанных между собой компьютеров, которые могут обмениваться информацией.

Компьютеры объединяют в сеть ради *трех главных* целей: совместное использование ресурсов сети, общение между пользователями и предоставление услуг.

Цель 1: совместное использование ресурсов сети.

Ресурсами сети могут быть:

- данные и программы (файлы на дисках);
- устройства (принтеры, сканеры, модемы и т. д.);
- вычислительная мощность процессоров.

Пример. Если требуется решить сложную задачу, связанную с длительными вычислениями, например, решить большую систему линейных уравнений, вполне вероятно, что такую задачу можно распараллелить и разделить между несколькими компьютерами в сети. В этом случае используется ресурс сети – вычислительная мощность процессоров.

Ресурсы, доступные в сети, называют *разделяемыми ресурсами* (shared resources).

Цель 2: общение между пользователями.

Общение между пользователями сети может происходить посредством специальных сайтов (социальные сети, блоги, форумы и т. д.), электронной почты (e-mail), чатов, видеоконференций, IP-телефонии и т. д.

Цель 3: предоставление услуг (сервисов) пользователям.

Этот способ использования компьютерных сетей стал очень востребованным в последние 10-15 лет в связи с повсеместным распространением глобальной сети – Интернета. Сюда можно отнести покупку-продажу всевозможных товаров (книг, подарков, ж/д и авиабилетов, электронной аппаратуры и т. п.), электронные платежные системы (PayPal, WebMoney, Яндекс.Деньги и т. д.), интернет-радио и телевидение, реклама, онлайн-игры и др.

Все компьютеры в сети делятся на два вида – серверы и клиенты.

Сервер (server, от англ. *to serve* – служить) – компьютер или программа, предоставляющие ресурсы или услуги.

Клиент (client) – компьютер или программа, использующие ресурсы или услуги.

Иногда используется термин *peer*[1] – компьютер или программа, предоставляющие и использующие ресурсы.

Подчеркнем, что термины сервер и клиент могут использоваться по отношению и к компьютерам, и к программам. Например, *сервер базы данных* – мощный компьютер и/или специальная программа, управляющие доступом к базе данных.

Компьютеры, объединенные в сеть (как серверы, так и клиенты), а также другие сетевые устройства (концентраторы, коммутаторы, маршрутизаторы и т. д.) называются *узлами* (nodes) сети.

Канал связи, соединяющий узлы сети, называется *средой передачи данных* (media). Среда передачи может быть *проводной* (wire) и *беспроводной* (wireless).

Степень загруженности сети, определяемая потоком данных в ней, называется *трафиком* (traffic).

Виды передачи данных:

– *симплексная* (simplex) – передача может идти только в одну сторону (пример: телевидение, радиовещание);

– *полудуплексная* (half-duplex) – передача может идти в обе стороны, но попеременно (пример: две рации);

– *полнодуплексная* (full-duplex) – передача может идти в обе стороны одновременно (пример: телефония).

1.2. Классификация компьютерных сетей

Существует несколько способов классификации компьютерных сетей: по размеру, по способу взаимодействия, по топологии, по типу среды передачи и т. д. Рассмотрим некоторые из них.

[1] От этого термина, например, произошло понятие *пиринговые файлообменные сети* – это сети, в которых каждый компьютер может как предоставлять свои файлы в общий доступ, так и скачивать файлы с других узлов сети.

1.2.1. Классификация по размеру

Компьютерные сети различаются по размеру (или занимаемой территории). Выделяют персональные, локальные, городские и глобальные сети.

Персональная сеть (PAN – Personal Area Network) – сеть одного человека. Назначение такой сети – объединение всех электронных устройств пользователя (настольный компьютер, ноутбук, принтер, коммуникатор, сотовый телефон и т. п.). Реализуются персональные сети на основе технологий Wi-Fi, Bluetooth, USB и иногда IrDA[1].

Локальная сеть (LAN – Local Area Network) расположена в пределах одного или нескольких близких зданий и ее размер не превышает 1–2 километров. В LAN обычно используются ограниченный набор сетевых протоколов, например Ethernet + TCP/IP. Примеры: домашняя сеть, сеть факультета, университета, небольшого предприятия.

Недавно в связи с развитием беспроводных сетей появился термин *WLAN – Wireless LAN* (беспроводная локальная сеть).

Городская или *муниципальная сеть* (MAN – Metropolitan Area Network) является промежуточной между локальной и глобальной сетями как по размеру, так и по скорости передачи данных. Занимает территорию до нескольких десятков км и расположена в пределах города. Набор используемых сетевых протоколов и оборудования обычно шире, чем в LAN. Примером является сеть провайдера, предоставляющего жителям одного города доступ в Интернет.

Глобальная сеть (WAN – Wide Area Network) – это сеть, которая связывает отдельные компьютеры, локальные и городские сети, находящиеся на очень большом расстоянии, например в разных городах или на разных континентах. В связи с этим спектр применяемых протоколов и оборудования наиболее велик. Самым известным примером глобальной сети является *Интернет*.

1.2.2. Классификация по типу взаимодействия

Компьютерные сети по типу взаимодействия можно разделить на два вида:

- *одноранговые* (peer-to-peer); в сетях Microsoft Windows называются *рабочими группами* (workgroup);

[1] IrDA (Infrared Data Association) – стандарт связи по инфракрасному порту.

• *на основе сервера* (server based); в сетях Microsoft Windows называются *доменами*[1] (domain).

Компьютеры *одноранговой сети* могут быть и клиентами и серверами одновременно (*peer*). Ни один компьютер не имеет ни приоритета доступа, ни обязанности предоставлять ресурсы в совместное использование. Чаще всего в таких сетях находятся не более нескольких десятков компьютеров.

Управление доступом к ресурсам определенного компьютера должно осуществляться непосредственно на этом компьютере[2]. Чтобы получить доступ к ресурсам компьютера, необходимо знать имя и пароль пользователя, учетная запись которого создана на этом компьютере (рис. 1). Таким образом, чтобы иметь доступ ко всем ресурсам сети, нужно создать свои учетные записи на каждом компьютере и знать пароли к ним.

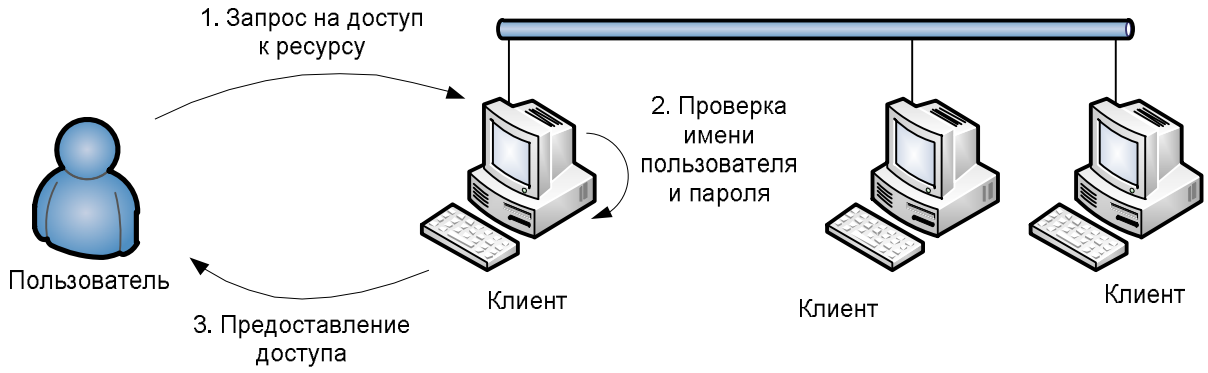


Рис. 1. Получение доступа к ресурсам в одноранговой сети

В *сетях на основе сервера* (*доменах*) существует один или несколько выделенных серверов (мощных компьютеров с серверной операционной системой и со специальным программным обеспечением), которые предоставляют ресурсы. Кроме того имеется один или несколько серверов, управляющих сетью[3] (в сетях Microsoft они называются *контроллерами домена, domain controller)*.

Важное отличие от одноранговых сетей состоит в повышении уровня безопасности. Здесь существует централизованная проверка учетных записей пользователей, их прав и паролей. Прежде чем получить доступ к любому ресурсу, пользователь должен *войти в сеть* – на любом компьютере сети ввести свои имя и пароль, которые будут автоматически переданы

[1] Термин *домен* может использоваться в разных контекстах (например, домен в Интернете). В любом случае под доменом понимают группу компьютеров, объединенных по какому-либо признаку.
[2] Конечно если не используются специальные утилиты удаленного администрирования.
[3] Один и тот же сервер может и предоставлять ресурсы, и управлять сетью.

контроллеру домена. Контроллер домена проверит пароль пользователя, и, в зависимости от прав пользователя, разрешит или запретит доступ к ресурсу (рис. 2). При этом, выполнив однажды вход в сеть, пользователь может пользоваться всеми ресурсами сети, не вводя имя и пароль повторно (до завершения сеанса работы, т. е. до выхода из сети).

Рис. 2. Получение доступа к ресурсам в сети на основе сервера

В таблице 1 приведена сравнительная характеристика рассмотренных видов сетей.

Таблица 1. Сравнительная характеристика одноранговых сетей и сетей на основе сервера

Характеристика	**Одноранговые сети**	**Сети на основе сервера**
Стоимость	Низкая, т. к. не нужно дополнительных ресурсов (выделенного сервера, администратора, специального ПО)	Высокая, т. к. требуется специальное оборудование, ПО и персонал
Установка и настройка	Простая	Сложная
Администрирование (управление)	Раздельное, на каждом компьютере отдельно	Централизованное, на контроллере домена

Характеристика	Одноранговые сети	Сети на основе сервера
Производительность	Низкая, поскольку нет выделенных серверов	Высокая, т. к. имеются выделенные серверы
Резервирование данных	Раздельное, на каждом компьютере отдельно	Централизованное, на серверах
Отказоустойчивость	Высокая – при отказе одного или нескольких компьютеров работоспособность сети сохраняется	При отказе контроллера домена вся сеть не работает; проблема решается дублированием контроллеров домена

В целом, одноранговую модель можно использовать для небольших недорогих сетей, включающих не более 20–30 компьютеров, в которых вопросы безопасности не являются приоритетными. В остальных случаях следует предпочесть модель на основе сервера.

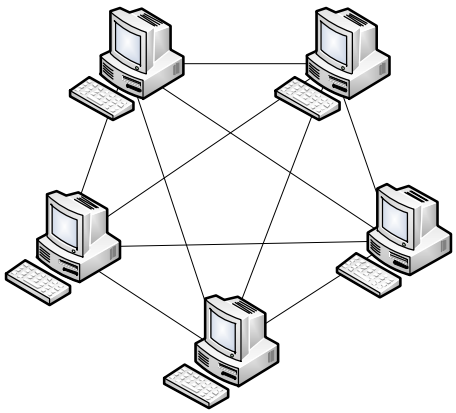
1.2.3. Классификация по топологии

Топология компьютерной сети – это способ организации связей между узлами сети.

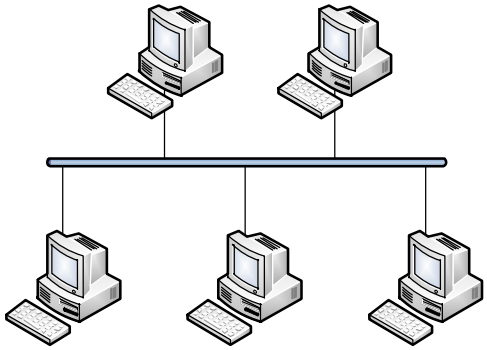
Существуют следующие основные виды топологий: ячеистая, общая шина, кольцо, звезда, иерархическая звезда (или дерево), сотовая (см. рис. 3).

Можно выделить два подвида *ячеистой топологии – полносвязная* (full mesh), когда каждый узел связан со всеми другими и *неполносвязная* (partial mesh), в которой между некоторыми узлами могут отсутствовать связи. Такая топология применяется редко, только если нужно обеспечить высокую надежность при малом числе узлов сети.

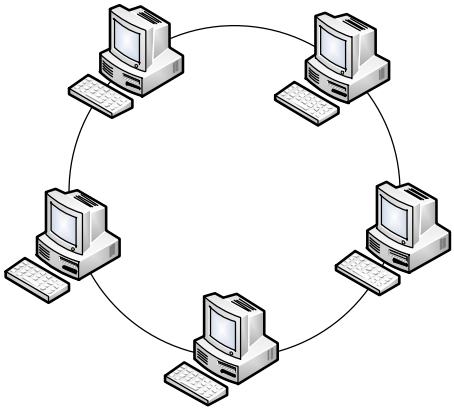
Топология *общая шина* (bus) позволяет создать сеть, используя кабель наименьшей длины. Особенностью шинной топологии является простота установки и изменения конфигурации сети. В качестве недостатков можно отметить то, что при повреждении шины отказывает вся сеть, причем достаточно сложно найти место разрыва; а также использование одного канала для всего трафика сети, что может стать узким местом при большом объеме трафика.



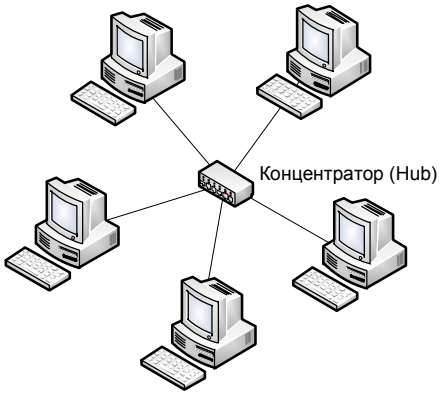
Ячеистая (Mesh)



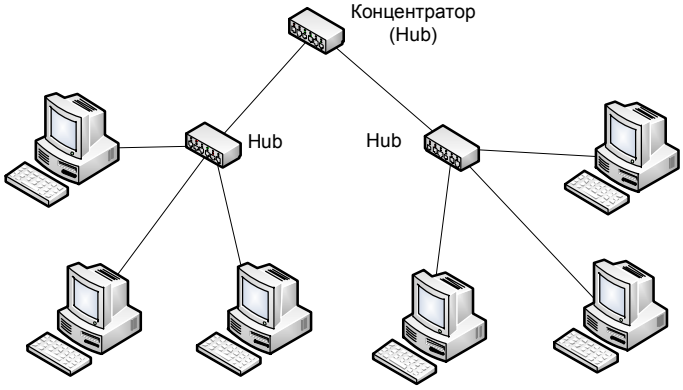
Общая шина (Bus)



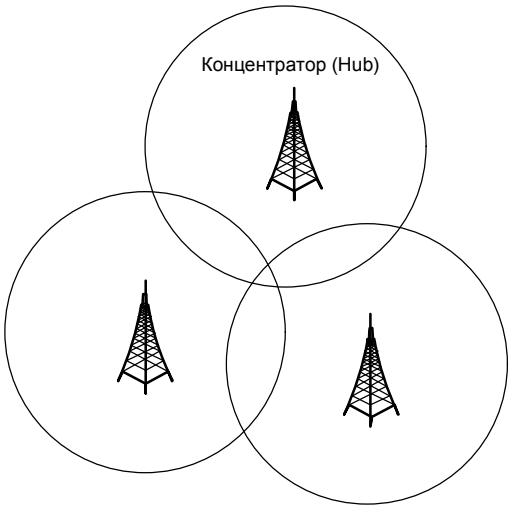
Кольцо (Ring)



Звезда (Star)



Дерево (Tree)
или Иерархическая
звезда



Сотовая (Cellular)

Рис. 3. Виды топологий

Кольцевая топология (ring) имеет существенное преимущество – наличие обратной связи. Это означает, что если один компьютер посылает сообщение другому, получатель может включить в сообщение информацию об успешном (или неуспешном) приеме и отправить его дальше по кольцу источнику сообщения. С другой стороны, так же как в общей шине, при разрыве кабеля вся сеть перестает работать и бывает сложно определить место повреждения. Для повышения надежности сети часто используют *двойное кольцо*: в штатном режиме постоянно работает первое кольцо, а при его разрыве вступает в действие второе, резервное кольцо.

В топологии *звезда* (star) обязательно наличие центрального устройства, которое называется *концентратор* (hub). Каждый узел подключается к сети через отдельный кабель, таким образом, при разрыве линии связи от сети оказывается отрезанным только один компьютер, остальные работают как обычно. Только в случае неисправности концентратора вся сеть перестает работать.

Топология *дерево* (tree) или *иерархическая звезда* является объединением нескольких звезд и позволяет строить достаточно большие сети. На сегодняшний день топологии звезда и дерево – самые распространенные в локальных сетях.

Сотовая топология (cellular) применяется в беспроводных сетях мобильной связи. Территория, охватываемая одним приемопередатчиком, называется *сотой* (cell). Информация может передаваться как в рамках одной соты, так и между несколькими сотами. Такая топология позволяет создавать огромные по размеру сети.

При выборе той или иной топологии необходимо оценивать сложность операций установки и нахождения неисправностей, а также принимать во внимание свойство отказоустойчивости сети. В общем, эти характеристики зависят от количества связей между узлами сети. Чем больше связей, тем сложнее установка, но тем проще находить поврежденный участок сети и тем сеть надежнее.

Например, ячеистая топология имеет наибольшее число связей и поэтому является самой надежной, но и очень сложна в установке. С другой стороны, шинная и кольцевая топологии обладают наименьшим количеством связей и, следовательно, просты в установке, но ненадежны и сложны в диагностике неисправностей.

1.3. Основные характеристики сети

Ключевые сетевые характеристики приведены на рис. 4.

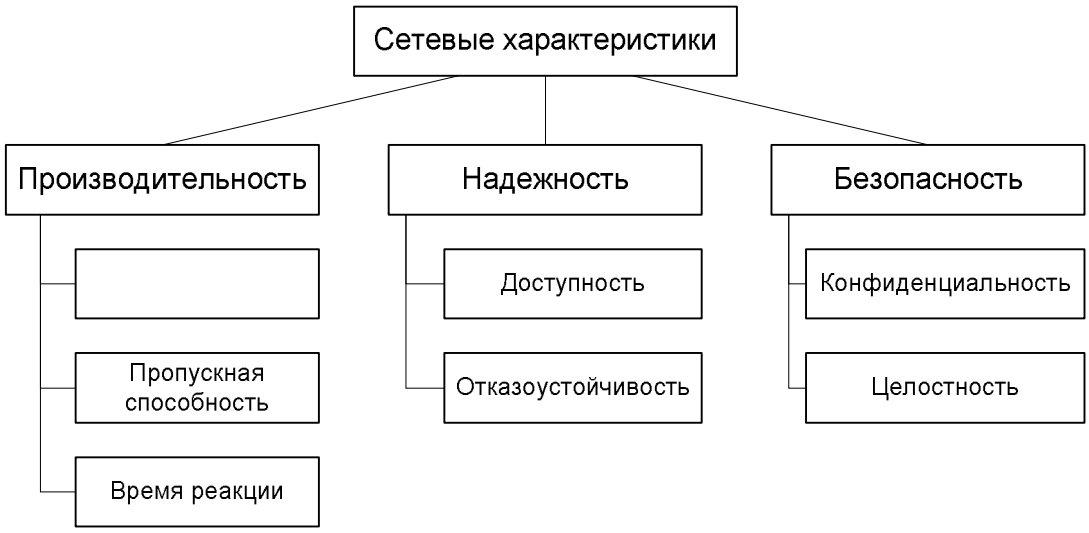


Рис. 4. Сетевые характеристики

Можно выделить три группы сетевых характеристик: производительность, надежность и безопасность.

Производительность (productivity) сети описывается тремя основными характеристиками – скоростью передачи данных, пропускной способностью и временем реакции.

Скорость передачи данных (data transfer rate) – количество информации, переданной за единицу времени. Измеряется в битах в секунду (бит/с). Чтобы найти скорость передачи данных, нужно разделить объем переданной информации на интервал времени, за который произошла передача.

Пропускная способность (throughput) – максимально возможная скорость передачи данных по линии связи. Измеряется также в бит/с.

Скорость передачи данных отражает реальное состояние сети в текущий момент времени и может изменяться. Это зависит от состояния канала связи, типа передаваемых данных, внешних факторов (помех). Пропускная способность является теоретической характеристикой линии связи или сетевой технологии и не изменяется. Она устанавливает верхний предел для скорости передачи данных. Чаще всего скорость передачи составляет величину, меньшую пропускной способности; связано это с тем, что помимо полезных данных по сети передается служебная информация, кроме того часть времени занимают процедуры доступа к сети.

Например, в локальных сетях Fast Ethernet пропускная способность равна 100 Мбит/с, то есть теоретически за 1 секунду можно передать 100

Мбит данных (или 12,5 Мбайт). Однако на практике за 1 секунду передается файл размером 4 Мбайт, т. е. реальная скорость передачи данных оказывается 32 Мбит/с или 32% от пропускной способности сети.

Ещё одной характеристикой производительности является *время реакции* (response time) – интервал времени между запросом пользователя к ресурсу сети и получением ответа на запрос. Время реакции складывается из интервалов времени выполнения следующих операций:

1) подготовка запроса на компьютере-клиенте;
2) передача запроса по сети;
3) подготовка ответа компьютером-сервером;
4) передача ответа по сети;
5) обработка ответа на компьютере-клиенте.

Как видно, время реакции является характеристикой не только сети, но и программного и аппаратного обеспечения, установленного на компьютерах.

Характеристика *надежности* (reliability) включает свойства доступности и отказоустойчивости.

Доступность (availability) – доля времени, в течение которого сеть готова к работе. Доступность является вероятностной величиной и измеряется на достаточно большом интервале времени (день, месяц, год). Обычное значение, например, 0,999 – означает, что, вероятно, сеть будет недоступна только около 8 с половиной часов в год.

Отказоустойчивость (fault tolerance) – это способность сети сохранять работоспособность при отказе отдельных элементов.

Например, ячеистая топология является отказоустойчивой, потому что при обрыве одной связи между узлами, остается ещё несколько путей передачи сообщений, так что сеть остается работоспособной. А вот шинная топология не обладает этим свойством, поскольку при повреждении кабеля сеть перестает правильно работать.

Общим принципом, обеспечивающим высокую надежность, является *внесение избыточных связей в сетевую структуру* (сравните ячеистую и шинную топологии по этому критерию).

Безопасность (safety) сети определяется конфиденциальностью и целостностью её ресурсов.

Конфиденциальность (privacy) – способность сети обеспечивать доступ к ресурсам только тем пользователям, которые имеют на это право.

Целостность (integrity) – способность сети обеспечивать сохранность ресурсов.

2. Модель сетевого взаимодействия

На рынке сетевого оборудования и программного обеспечения существует множество фирм и одной из важнейших является проблема совместимости, т. е. соответствия характеристик продукции разных производителей. Для того чтобы сетевые устройства правильно взаимодействовали между собой, требуется наличие общих для всех стандартов. К настоящему времени одним из наиболее распространенных сетевых стандартов, охватывающих весь процесс сетевого взаимодействия, является модель OSI[1].

2.1. Модель OSI

Модель взаимодействия открытых систем (OSI, Open Systems Interconnection model) разработана Международной организацией по стандартизации ISO[2] и Международным союзом электросвязи ITU[3] в 1977–1984 годах и принята в качестве стандарта ISO 7498.

Процесс сетевого взаимодействия весьма сложен. Как его описать и реализовать? В модели OSI используется фундаментальный для информатики принцип борьбы со сложностью – «Разделяй и властвуй». Сетевое взаимодействие рассматривается на семи уровнях, организованных в иерархию[4] (см. рис. 5). Каждый уровень имеет определенные функции и должен быть реализован на всех сетевых узлах.

Уровень модели OSI может взаимодействовать с соседними уровнями в иерархии, причем нижележащий уровень предоставляет набор услуг вышележащему уровню в соответствии со своим интерфейсом.

Интерфейс (interface) – это правила, определяющие формат сообщений, которыми обмениваются сетевые компоненты, находящиеся на соседних уровнях в одном узле.

Между одноименными уровнями, реализованными на разных узлах, также осуществляется взаимодействие по соответствующему протоколу.

[1] Также распространена модель DoD (Department of Defense – Министерство обороны США), в соответствие с которой построен стек протоколов TCP/IP, лежащий в основе Интернета.
[2] ISO – International Organization for Standardization.
[3] ITU – International Telecommunications Union.
[4] Иерархия – система уровней, в которой строго определено подчинение нижележащего уровня вышележащему.

Протокол (protocol) – это правила, определяющие формат сообщений, которыми обмениваются сетевые компоненты, лежащие на одном уровне, но в разных узлах.

Стек протоколов – это иерархически организованный набор протоколов, достаточный для организации взаимодействия узлов в сети.

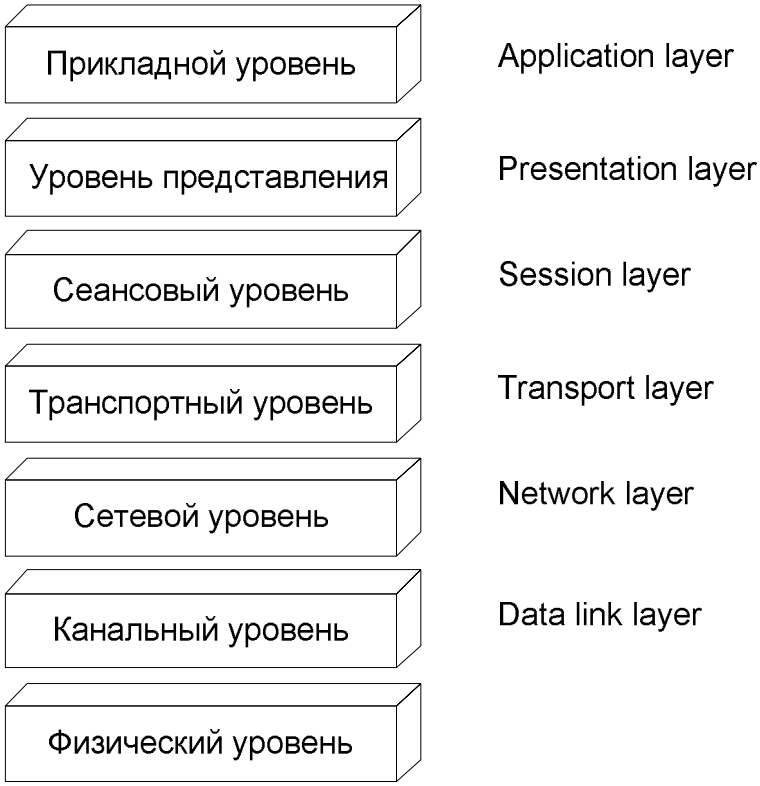


Рис. 5. Уровни модели OSI

В процессе коммуникации узлы обмениваются *сообщениями* (*message*). Передачу сообщения начинает сетевое приложение (программа, которой нужны услуги сети). При передаче сообщения сверху вниз каждый уровень добавляет к нему свой заголовок, содержащий информацию для одноименного уровня на другом узле. Непосредственно по каналам связи сообщение передается на узел-получатель в соответствии с протоколом физического уровня. Затем сообщение поднимается по иерархии снизу вверх и каждый уровень считывает «свой» заголовок. Иллюстрация этого процесса приведена на рис. 6.

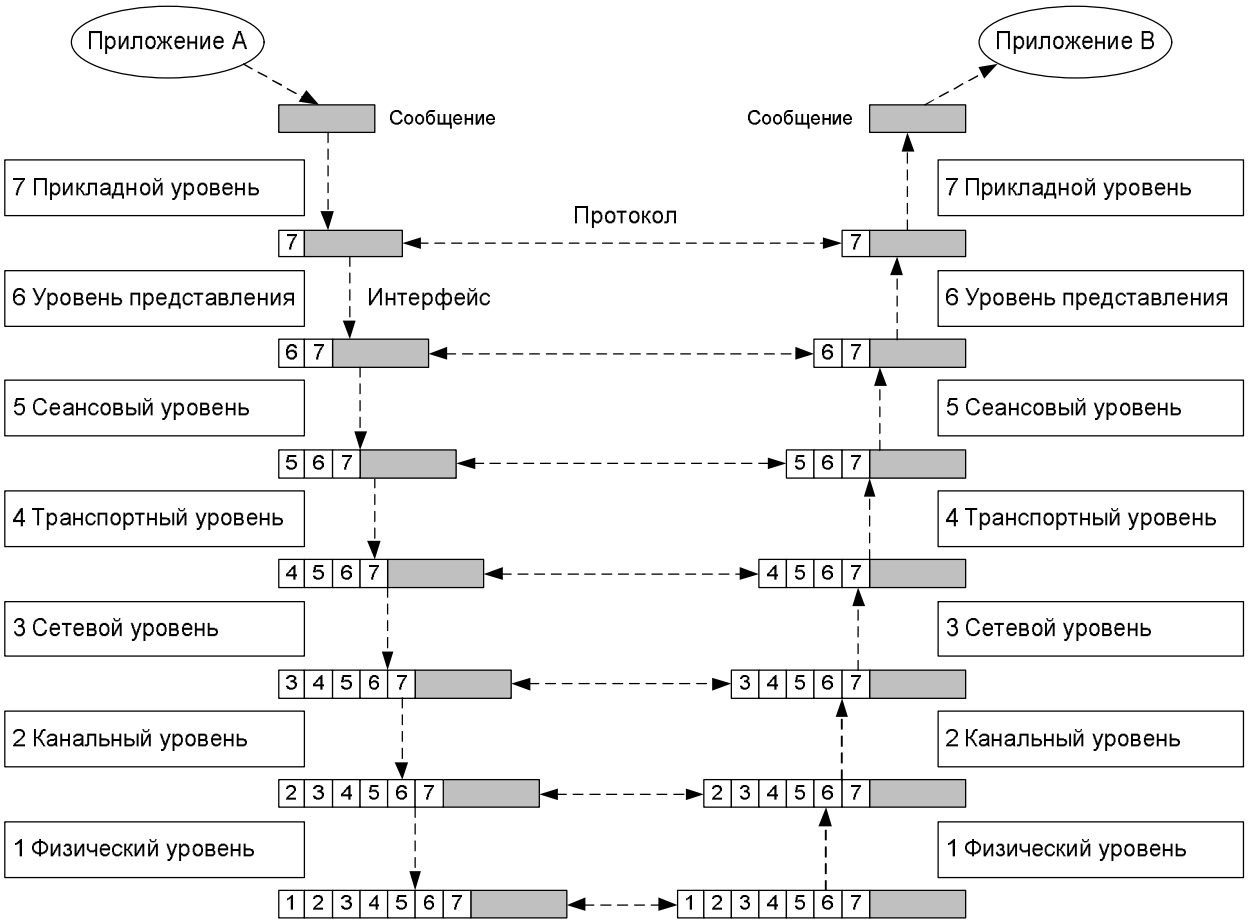


Рис. 6. Схема процесса взаимодействия в модели OSI

Чтобы лучше понять принцип работы модели OSI, можно воспользоваться следующим примером. Представим себе президентов двух стран и попробуем смоделировать процесс их общения как иерархическую систему (рис. 7).

В этой системе три уровня – уровень президента, уровень секретаря и уровень почты. Секретарь предоставляет президенту услуги по передаче сообщений (интерфейс). Интерфейс может быть реализован, например, посредством телефонной связи или непосредственного общения (директор вызывает секретаря и передает ему все необходимую информацию). В системе существуют три протокола – между президентами, между секретарями и почтовый протокол: стиль общения президентов отличается от стиля общения секретарей, а почта работает по своим особым правилам.

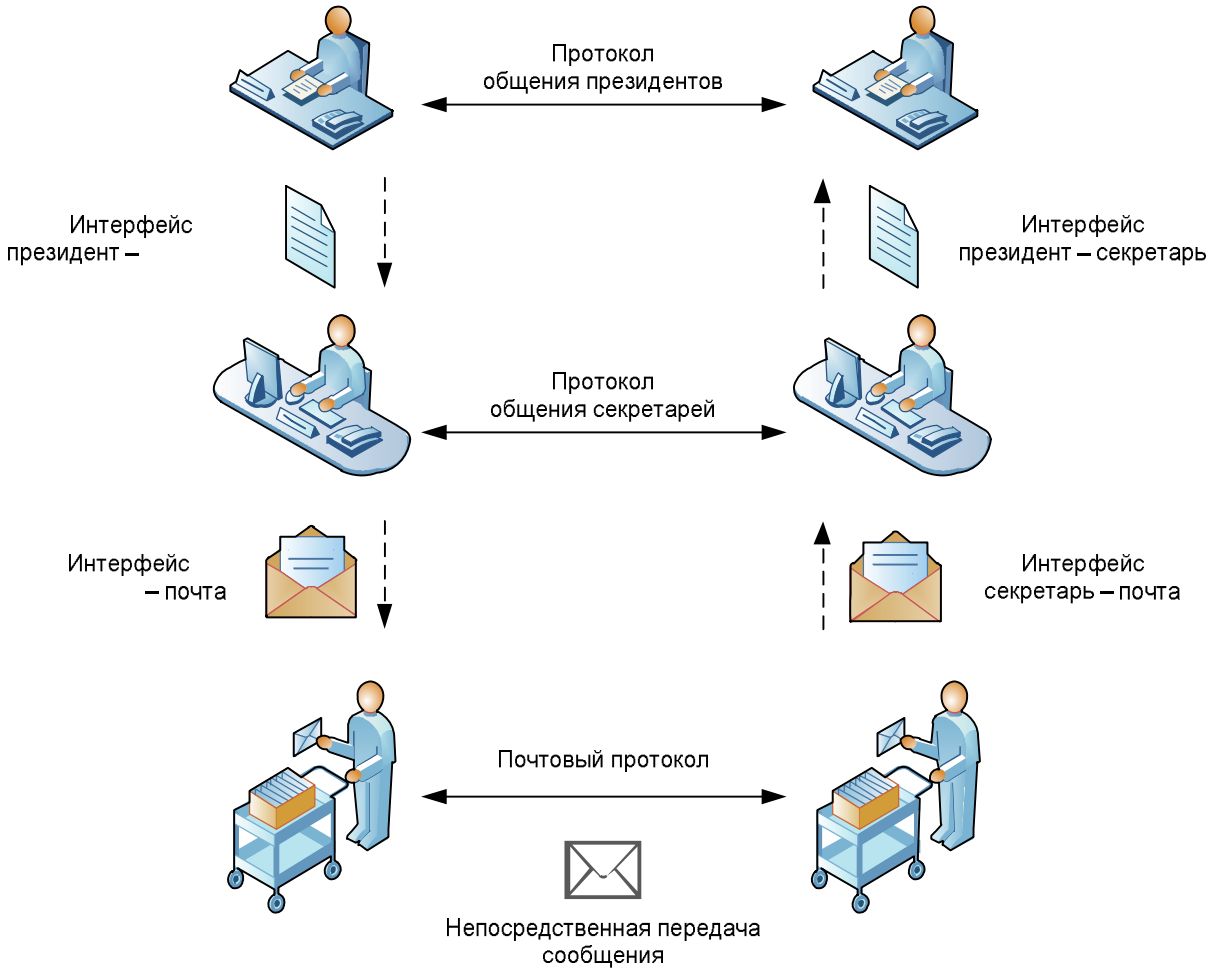


Рис. 7. Пример иерархической системы

Процесс передачи сообщения в такой системе происходит следующим образом. Одному президенту требуется передать сообщение другому президенту. Для этого он вызывает своего секретаря и передает ему сообщение, допустим на листе бумаги (работает интерфейс президент-секретарь). Секретарь переводит сообщение на иностранный язык, вкладывает сообщение в конверт и пишет на нем адрес и лицо, кому предназначено сообщение (добавляет свой заголовок), и отправляет его по почте (передача сообщения по каналам связи). Секретарь другого президента, получив письмо, читает информацию на конверте (считывает свой заголовок) и отправляет сообщение президенту (работает интерфейс президент-секретарь).

2.2. Функции уровней модели OSI

2.2.1. Физический уровень

Физический уровень должен передать по линии связи данные, приходящие от канального уровня. Данные передаются в виде потока бит.

Функции физического уровня:

1) представить последовательность бит данных в виде электрических сигналов – описать форму сигналов, их величину и продолжительность;

2) передать получившиеся электрические сигналы по определенным каналам связи – описать характеристики используемых кабелей, разъемов, беспроводных сред;

3) принять электрические сигналы и декодировать их в исходную последовательность бит.

Перечисленные функции реализуются с помощью аппаратных средств узлов сети – микросхем, проводников, транзисторов, конденсаторов и др.

2.2.2. Канальный уровень

Канальный уровень предназначен для передачи данных сетевого уровня в рамках простой сети с определенной топологией. Данные пересылаются уже не битами, а наборами бит, которые называются *кадры* (frame). В кадр может входить от нескольких десятков до нескольких тысяч байт.

Функции канального уровня:

1) проверка доступности среды передачи – в случае, если несколько сетевых узлов используют один канал связи, для предотвращения конфликтов требуются правила, определяющие порядок доступа узлов к среде;

2) адресация в простых сетях с определенной топологией – чтобы кадр дошел до нужного узла сети, в нем должна быть информация о том, кому он предназначен. Адресация в сложных составных сетях с разными топологиями возлагается на сетевой уровень;

3) обнаружение и коррекция ошибок – для решения этой задачи в кадр добавляется служебная информация, называемая *контрольной суммой*. Отметим, что проблема надежной передачи может решаться на всех уровнях, от физического до прикладного.

Канальный уровень реализуется совместно аппаратными средствами и программными компонентами (драйверами). Устройства, работающие на

канальном уровне, – сетевые карты, повторители, концентраторы, мосты, коммутаторы.

2.2.3. Сетевой уровень

Сетевой уровень используется для объединения простых сетей в единую составную сеть. Простые сети в этом случае называются *подсетями* (*subnet*) и могут иметь разные топологии, типы сред передачи, технологии реализации. На сетевом уровне данные, приходящие от транспортного уровня, пересылаются в виде *пакетов* (*packet*).

Функции сетевого уровня:

1) *маршрутизация* (routing) – выбор оптимального пути передачи сообщений. Термин «оптимальность» подразумевает определенный *критерий оптимальности*. В данном случае критериями могут быть время передачи, надежность и безопасность (см. параграф 1.3. Основные характеристики сети);

2) *адресация* в составных сетях – способ адресации должен включать адрес подсети и адрес узла в данной подсети, в отличие от канального уровня, где может быть только адрес узла.

Сетевой уровень реализуется на узлах сети с помощью программных компонентов операционных систем.

Подсети объединяются в единую сеть при помощи специальных устройств – *маршрутизаторов* (router). Маршрутизаторы решают задачу выбора оптимального пути на основании информации о текущем состоянии сети. Пример построения составной сети приведен на рис. 8.

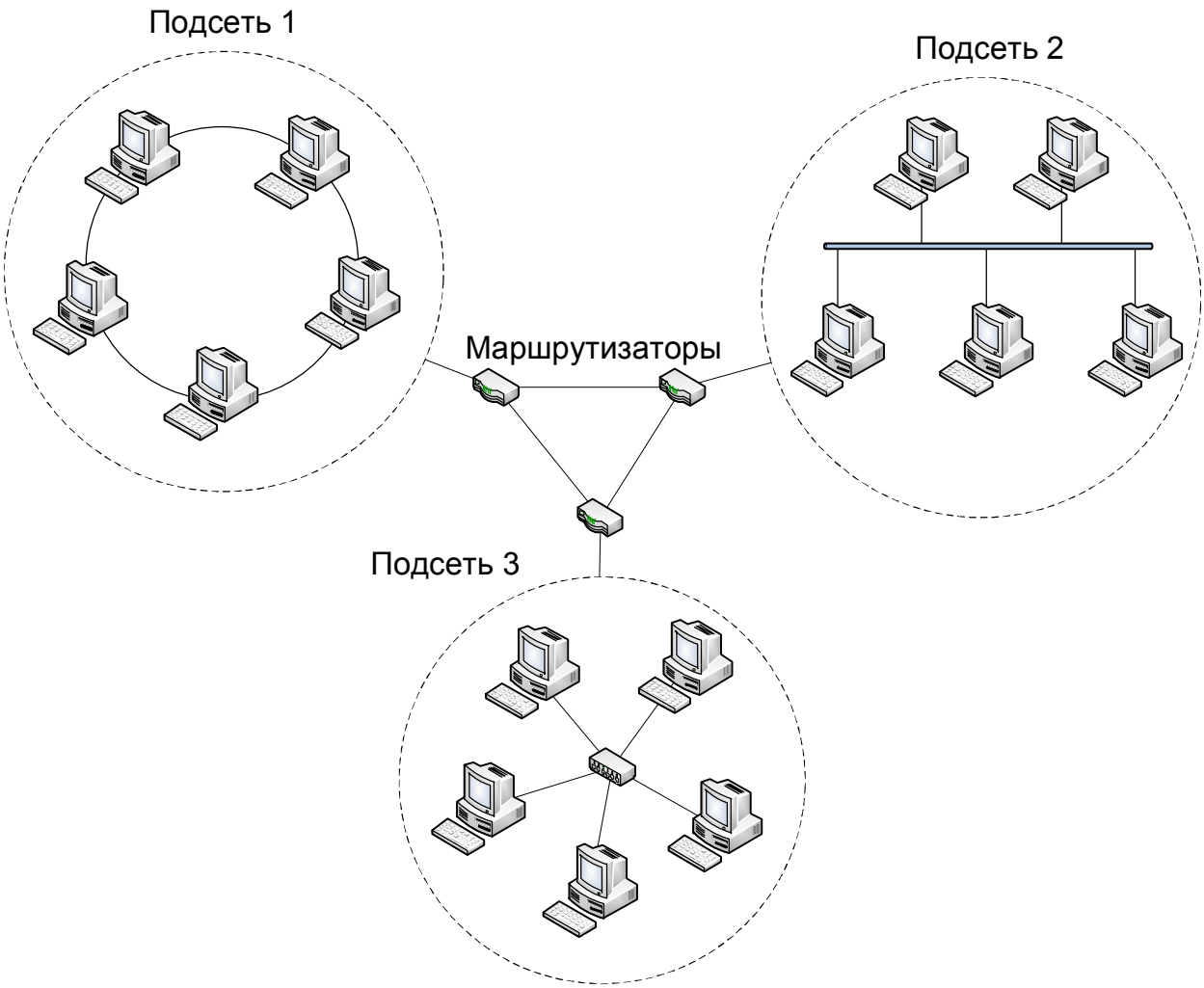


Рис. 8. Пример составной сети

2.2.4. Транспортный уровень

Транспортный уровень обеспечивает передачу данных прикладного уровня с необходимой степенью надежности и с учетом требований сетевого уровня к размеру пакетов.

Функции транспортного уровня:

1) передача данных верхних уровней с той степенью надежности, которая им требуется – существуют два основных уровня надежности: *гарантированная доставка* и *негарантированная* (рассмотрены ниже);

2) разбивка сообщений верхних уровней на части – размеры пакетов и кадров обычно не превышают нескольких килобайт; в то же время сообщения прикладного уровня могут быть намного больше. Для решения проблемы несоответствия размеров, сообщения разбиваются на части,

которые в случае гарантированной доставки называются *сегменты* (*segment*), а в случае негарантированной – *дейтаграммы* (*datagram*);

3) сборка переданных сегментов или дейтаграмм в исходное сообщение – части сообщения могут приходить получателю не в том порядке, в каком они были отправлены, так как состояние сети меняется и маршрутизаторы могут выбирать для пакетов разные пути. Чтобы на узле-приемнике собрать сегменты в исходное сообщение, каждому сегменту (дейтаграмме) присваивается идентификатор сообщения и номер сегмента в этом сообщении. На основе этой информации исходное сообщение собирается из отдельных сегментов (дейтаграмм).

В случае *гарантированной доставки* между отправителем и получателем устанавливается *соединение* (*виртуальный канал*), по которому они могут обмениваться информацией о ходе доставки сообщения. Сообщение на транспортном уровне разбивается на сегменты, которые передаются на нижележащий уровень. Каждый сегмент на сетевом уровне помещается в пакет и отправляется по сети с помощью канального и физического уровней. В процессе передачи получатель обязан на каждый полученный сегмент отправить подтверждение (положительную квитанцию) о доставке. В случае отсутствия подтверждения или отрицательной квитанции отправитель заново посылает тот же сегмент.

При *негарантированной доставке* соединение не устанавливается, сообщение разбивается на дейтаграммы, получение которых приемником не сопровождается отправлением подтверждающих квитанций.

Таким образом, гарантированная доставка обеспечивает надежную передачу сообщений, но является более медленной за счет обмена служебной информацией (установление соединения и квитанции). Напротив, негарантированная доставка является быстрой, но ненадежной.

Функции транспортного уровня, как и сетевого, реализуются программными компонентами операционных систем.

2.2.5. Сеансовый уровень

Сеансовый уровень позволяет организовать сеанс связи между узлами сети. В рамках сеанса можно управлять последовательностью передачи сообщений и в случае возникновения ошибки после её устранения продолжать передачу с прерванного места.

2.2.6. Уровень представления

Уровень представления занимается преобразованием данных из одного формата в другой для обеспечения совместимости узлов, работающих с разными формами представления, например преобразование между различными кодировками символов. К функциям этого уровня относится также шифрование и дешифрование передаваемых данных.

2.2.7. Прикладной уровень

Прикладной уровень отвечает за непосредственную реализацию основных целей создания компьютерной сети (см. параграф 1.1. Основные понятия), т. е. за предоставление пользователю доступа к ресурсам и услугам сети. На прикладном уровне работает самое большое число протоколов, что объясняется большим спектром ресурсов и услуг.

Перечислим некоторые важнейшие функции прикладного уровня:

1) передача файлов;
2) доступ к сетевым устройствам (принтерам, сканерам, модемам, …);
3) доступ к веб-сайтам;
4) электронная почта;
5) телеконференции;
6) IP-телефония;
7) организация чатов и т. д.

Единица данных прикладного уровня называется *сообщением* (*message*).

В таблицу 2 сведены основные функции, устройства и единицы данных уровней модели OSI.

Таблица 2. Функции, устройства и единицы данных уровней модели OSI

Уровень	**Функции**	**Устройства**	**Единица данных**
Прикладной	– передача файлов; – доступ к сетевым устройствам; – электронная почта; – …		– сообщение (message)
Транспортный	– надежная передача данных; – разбиение и сборка сообщений		– сегмент (segment) – дейтаграмма (datagram)
Сетевой	– маршрутизация; – адресация	– маршрутизатор (router); – шлюз (gateway)	– пакет (packet)
Канальный	– доступ к среде передачи; – адресация; – обнаружение и коррекция ошибок	– мост (bridge) – коммутатор (switch)	– кадр (frame)
Физический	– кодирование и декодирование бит в сигналы; – характеристики каналов связи	– повторитель (repeater) – концентратор (hub)	– бит (bit)

3. Линии связи

3.1. Классификация линий связи

Рассмотрим два способа классификации линий связи – по типу используемой среды передачи данных и по виду передаваемых сигналов.

Классификация по типу используемой среды передачи данных (рис. 9).

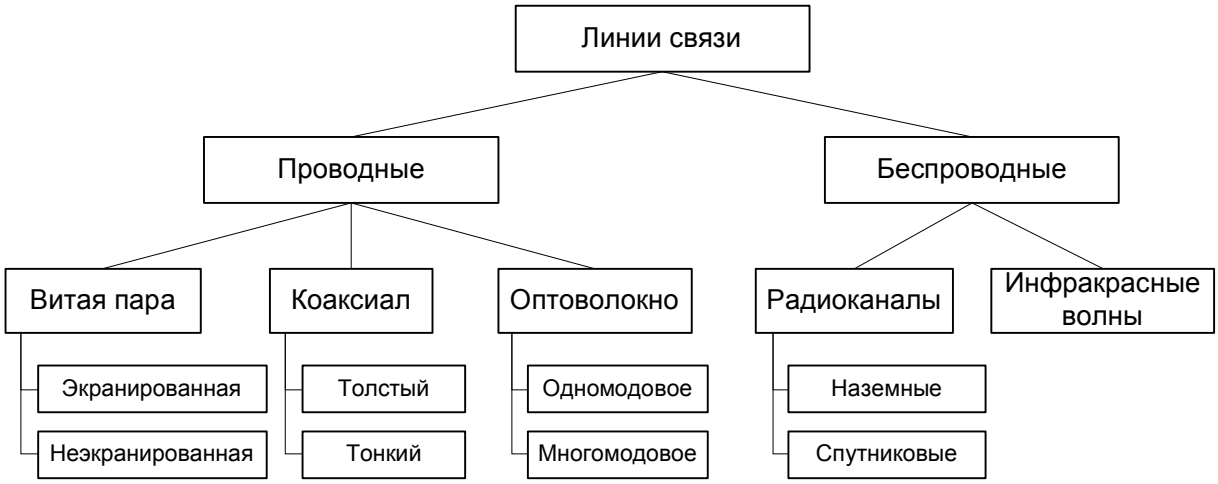


Рис. 9. Классификация по типу используемой среды передачи данных

Информация в компьютерных сетях передается с применением *электромагнитных волн*. Электрический ток, свет, радиосигналы, инфракрасное излучение – все это виды электромагнитных волн. Они могут распространяться по проводам или без проводов, отсюда две основные группы линий связи.

Классификация по виду передаваемых сигналов (рис. 10).

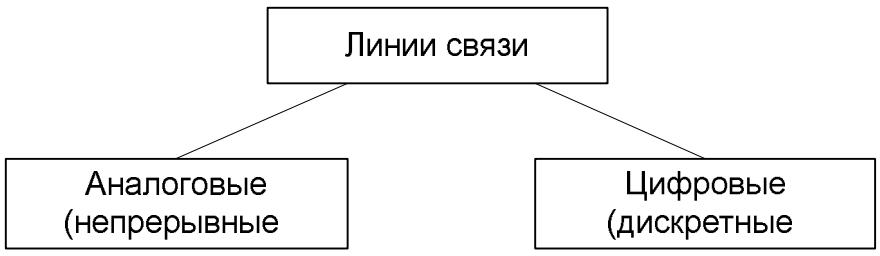


Рис. 10. Классификация по виду передаваемых сигналов

Аналоговый (непрерывный) сигнал – это сигнал, принимающий бесконечное число значений за конечный интервал времени.

Цифровой (дискретный) сигнал – это сигнал, принимающий конечное число значений за конечный интервал времени.

Различие этих видов сигналов иллюстрируется на рис. 11.

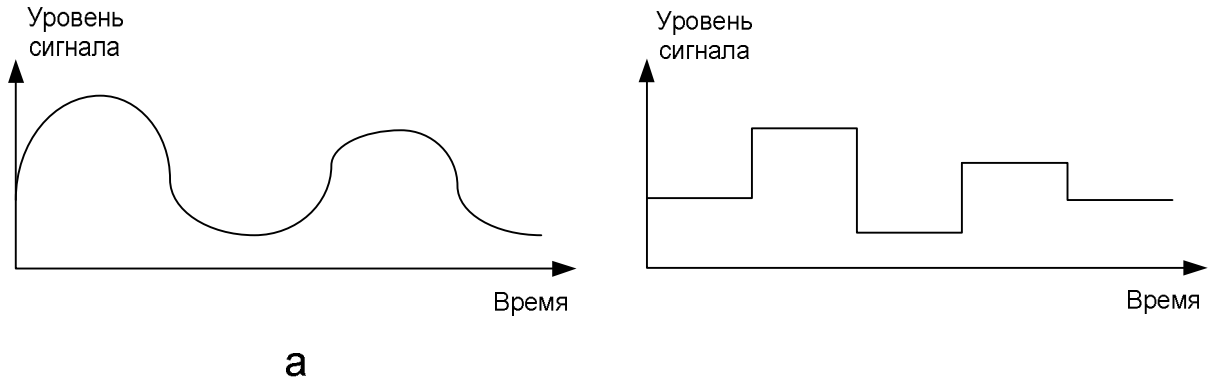


Рис. 11. Аналоговые и дискретные сигналы:
а – пример аналогового сигнала; б – пример дискретного сигнала

3.2. Коаксиальный кабель

Название «*коаксиальный*» (coaxial) произошло от латинских слов co – «совместно» и axis – «ось», что означает два проводника с общей осью (рис. 12).

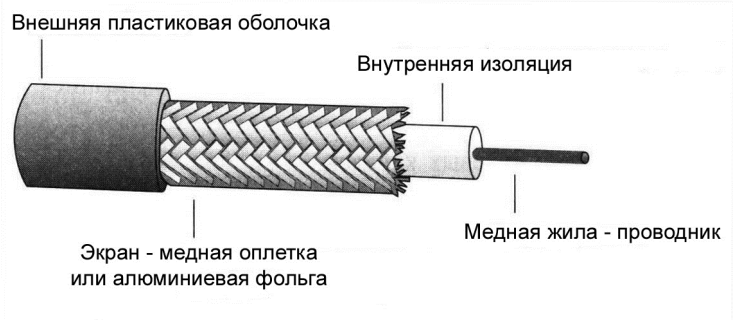


Рис. 12. Структура коаксиального кабеля

Одним из этих проводников является *медная жила*, находящаяся в центре кабеля; именно по ней проходят информационные сигналы. Другой проводник – так называемый *экран* (shield), который представляет собой оплетку из тонких медных проводников или алюминиевую фольгу. Назначение экрана – защита информационных сигналов от внешних электромагнитных помех. Чтобы проводники не замыкались, между ними прокладывается слой внутренней пластиковой изоляции. Вся эта

конструкция помещается в прочную пластиковую оболочку, которая предотвращает механическое повреждение кабеля (например, при сгибе или кручении), а также изолирует экран снаружи.

Некоторые виды коаксиального кабеля:

- RG-8 – «толстый» коаксиальный кабель (thick coaxial cable) для сетей Ethernet 10Base-5, диаметром примерно 9,5 мм. Максимальная длина сегмента[1] до 500 м, сопротивление кабеля – 50 Ом. Сложен в установке (плохо гнется);
- RG-58 – «тонкий» коаксиальный кабель (thin coaxial cable) для сетей Ethernet 10Base-2, диаметром около 5 мм. Максимальная длина сегмента до 185 м, сопротивление кабеля – 50 Ом. Установка проще, чем толстого коаксиала;
- RG-6, RG-59 – применяются в кабельном телевидении, сопротивление 75 Ом.

В настоящее время компьютерные сети на основе коаксиала (Ethernet 10Base-5 и 10Base-2) практически не применяются; в то же время коаксиальный кабель широко используется в кабельном телевидении и спутниковых системах.

3.3. Витая пара

В кабеле *витая пара* (twisted pair) для передачи данных используется пара медных проводников перевитых между собой. Обычно в один кабель помещают четыре такие пары. Перевивают проводники для уменьшения внешних и перекрестных[2] помех.

Существуют два основных вида витой пары:

- *экранированная* (shielded twisted pair, STP) – у каждой пары имеется собственный экран; применяется этот вид редко, в тех случаях, когда кабелю требуется дополнительная защита от помех;
- *неэкранированная* (unshielded twisted pair, UTP) – применяется в большинстве случаев.

Оба вида кабеля могут обладать общим внешним экраном; в этом случае используется аббревиатура S/STP (Screened STP) или S/UTP (Screened UTP).

[1] *Сегмент* – участок сети без повторителей – устройств, усиливающих сигнал.
[2] Перекрестные помехи – помехи в паре проводников, возникающие в одном проводнике от создаваемого другим проводником электромагнитного поля и наоборот.

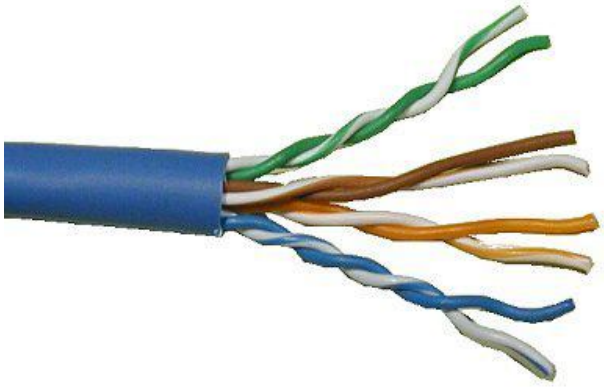


Рис. 13. Кабель UTP

Существуют несколько категорий неэкранированной витой пары. Они описаны в стандарте EIA/TIA 568[1] и обозначаются от CAT1 до CAT7 (табл. 3). Чем выше категория кабеля, тем шире у него полоса пропускания[2] и больше количество витков на единицу длины.

Таблица 3. Категории неэкранированной витой пары UTP

Категория	**Полоса пропускания, МГц**	**Кол-во пар**	**Сетевая технология**	**Примечание**
CAT-1	0,1	1	–	Телефонный кабель
CAT-2	1	2	Token Ring, ARCNet	Может встречаться в телефонных сетях
CAT-3	16	4	10BASE-T, 100BASE-T4, Token Ring	Может встречаться в телефонных сетях
CAT-4	20	4	10BASE-T, 100BASE-T4, Token Ring	В настоящее время не применяется
CAT-5	100	4	100BASE-TX	
CAT-5e	100	4	100BASE-TX, 1000BASE-T	Усовершенствованная CAT5

[1] EIA – Electronics Industries Alliance – Альянс отраслей электронной промышленности;
TIA – Telecommunication Industry Association – Ассоциация телекоммуникационной промышленности.
[2] Полоса пропускания – диапазон частот, которые линия связи передает без искажений. Чем шире полоса пропускания, тем больше теоретически достижимая пропускная способность линии связи.

Категория	Полоса пропускания, МГц	Кол-во пар	Сетевая технология	Примечание
CAT-6	250	4	100BASE-TX, 1000BASE-T, 10GBASE-T	
CAT-6A (Augmented)	500	4	100BASE-TX, 1000BASE-T, 10GBASE-T	Дополненная CAT6
CAT-7	600-700	4	Ethernet 10G, 40G, 100G	Основа будущих сетей

В настоящее время наиболее распространенными видами витой пары являются кабели категорий 5e, 6 и 6A, причем эти кабели могут быть как без общего экран, так и с экраном (т. е. S/UTP).

Для соединения кабелей с оборудованием используются вилки и розетки RJ-45[1], представляющие собой 8-контактные разъемы, похожие на обычные телефонные розетки RJ-11, только шире. При использовании кабеля UTP компьютер подключается к розетке через специальный короткий кабель (1–1,5 м), называемый *патч-корд* (patch cord).

3.4. Оптоволоконный кабель

В *оптоволоконном кабеле* (fiber-optic cable) информация передается при помощи световых сигналов. Средой передачи служит специальное стеклянное волокно. Структура оптоволоконного кабеля показана на рис. 14.

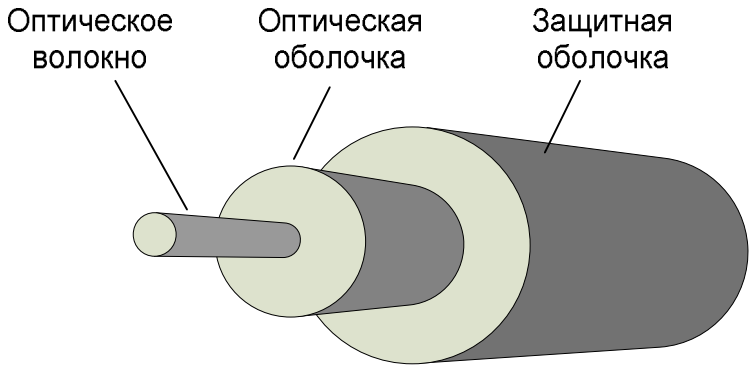


Рис. 14. Структура оптоволоконного кабеля

[1] RJ-45 (Registered jack – зарегистрированный разъем) – это ошибочное, но широко распространенное название разъема 8P8C (8 Position 8 Contact).

Информационные световые сигналы проходят по оптическому волокну, выполненному из стекла или пластика. В оптоволоконном кабеле может быть до нескольких сот волокон, но не менее двух – для передачи данных одновременно в противоположных направлениях.

Большинство волоконно-оптических систем используют инфракрасный свет[1] с длиной волны между 800 нм и 1600 нм (нм – *нанометр*, 1 нм = 10^{-9} м), поскольку стекло является более прозрачным для инфракрасного излучения, чем для видимого света.

Оптическая оболочка также изготавливается либо из стекла, либо из пластика и имеет коэффициент преломления, немного меньший, чем у оптического волокна (например, волокно – 1,47, оболочка – 1,46). Такая разность коэффициентов преломления обеспечивает эффект полного отражения света, проходящего по волокну, от оптической оболочки, так, что свет не рассеивается.

Пластиковая защитная оболочка предназначена для защиты от механических воздействий на кабель (изгиб, кручение).

Существуют стандартные диаметры стекловолокна и оптической оболочки, приведенные в таблице 4. Размер указывается в *микронах*[2] (обозначается *мкм*, 1 мкм = 10^{-6} м).

Таблица 4. Стандартные диаметры стекловолокна и оптической оболочки

Диаметр оптического волокна, мкм	Диаметр оптической оболочки, мкм
8	125
50	125
62,5	125
100	140

Диаметры оболочек кабеля обозначаются следующим образом: 8/125.

Различают два основных вида оптоволоконных кабелей: многомодовые и одномодовые (рис. 15). *Мода* – это вид траектории, по которой движется свет.

[1] *Инфракрасным светом* называют световые волны с длиной волны больше, чем у видимого света. Видимый свет имеет длину волны от 380 нм (темно-фиолетовый) до 750 нм (темно-красный).
[2] Для сравнения, диаметр человеческого волоса примерно 100 мкм.

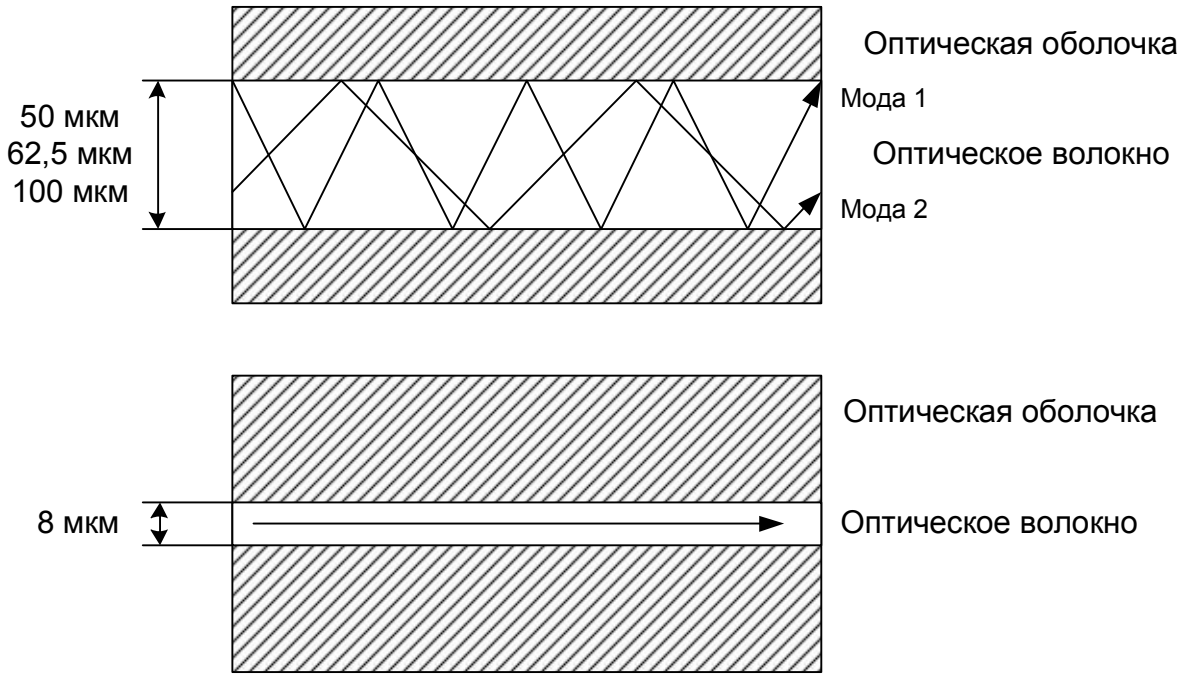


Рис. 15. Многомодовые и одномодовые оптоволоконные кабели

В *многомодовых кабелях* диаметр оптоволокна настолько велик, что свет распространяется по нескольким траекториям (модам), что приводит к искажениям и затуханию передаваемого сигнала. *Одномодовые кабели* имеют очень малый диаметр оптоволокна, поэтому свет проходит только по одному пути, за счет чего устраняются искажения сигнала, а затухание существенно уменьшается.

Таким образом, одномодовые кабели вследствие малого диаметра волокна сложнее изготавливать и устанавливать, но максимальная длина сегмента и пропускная способность у них выше, чем у многомодовых кабелей.

Сравнительная характеристика проводных линий связи приведена в таблице 5.

Таблица 5. Сравнительная характеристика проводных линий связи

Вид кабеля	**Стоимость**	**Сложность установки**	**Пропускная способность**	**Затухание сигнала**	**Максимальная длина сегмента, м**	**Защита от внешних помех и прослушивания**
Толстый коаксиал RG-8, RG-11	Низкая	Средняя	Низкая	Среднее	500 (10 Мбит/с)	Средняя
Тонкий коаксиал RG-58	Низкая	Низкая	Низкая	Высокое	185 (10 Мбит/с)	Средняя
Неэкранированная витая пара UTP-5, UTP-5e	Низкая	Низкая	Низкая	Высокое	100 (1 Гбит/с)	Низкая, но при наличии экрана – средняя
Неэкранированная витая пара UTP-6A	Средняя	Низкая	Средняя	Высокое	100 (1 Гбит/с)	Низкая, но при наличии экрана – средняя
Многомодовый оптоволоконный 50/125, 62,5/125	Средняя	Высокая	Высокая	Среднее	550 (1 Гбит/с)	Высокая
Одномодовый оптоволоконный 8/125	Высокая	Высокая	Очень высокая	Низкое	Несколько десятков км	Высокая

4. Технология Ethernet

Самая распространенная на сегодняшний день технология локальных сетей называется *Ethernet*. В соответствии с моделью OSI Ethernet отвечает за физический и канальный уровни.

4.1. История Ethernet

Технология Ethernet появилась в 1973 году – первый документ датируется 22 мая 1973 года. Это докладная записка, которую Роберт Меткалф (Robert Metcalfe) подал главе исследовательского центра Xerox в калифорнийском городке Пало-Альто (Xerox Palo Alto Research Center).

Название Ethernet произошло от двух слов: *ether* (эфир) и *net* (сеть), т. е. дословный перевод – «эфирная сеть». Дело в том, что эта технология основана на разработках в области компьютерных радиосетей (сеть ALOHAnet).

В 1975 году был получен патент, а в 1980 году усилиями трех фирм – DEC, Intel и Xerox, был создан первый стандарт Ethernet, который получил название DIX (по первым буквам названий фирм-разработчиков). В 1983 году международная ассоциация IEEE[1] публикует стандарт IEEE 802.3, разработанный на основе Ethernet DIX, в котором устанавливалась пропускная способность 10 Мбит/с.

80-е гг. прошли под знаком соперничества Ethernet с другими распространенными технологиями локальных сетей: Token Ring (IBM) и ARCNET. В 1995 году появляется стандарт IEEE 802.3u Fast Ethernet («быстрый Ethernet») со скоростью передачи 100 Мбит/с, а в 1998 году – стандарт IEEE 802.3z Gigabit Ethernet (1 Гбит/с). Эти новые стандарты, а также простота, надежность и низкая стоимость сетей, позволили Ethernet победить конкурентов и занять лидирующее положение на рынке LAN.

В 2003 году опубликован стандарт IEEE 802.3ae с пропускной способностью 10 Гбит/с, а в 2010 году – стандарт IEEE 802.3ba с пропускными способностями 40 и 100 Гбит/с.

4.2. Формат кадра

Чтобы сетевые узлы могли обмениваться информацией, должны быть согласованы форматы единиц передачи данных. Ethernet отвечает за

[1] IEEE (Institute of Electrical and Electronics Engineers) – Институт инженеров по электронике и электротехнике, некоммерческая международная ассоциация, одной из функцией которой является разработка стандартов в области информатики.

физический и канальный уровни, следовательно, в стандартах Ethernet должны быть определены способы кодирования бит и представления кадров. Рассмотрим формат кадров Ethernet. Считаем, что кадр передается от *узла-источника кадра* (source) к *узлу-приемнику* (destination).

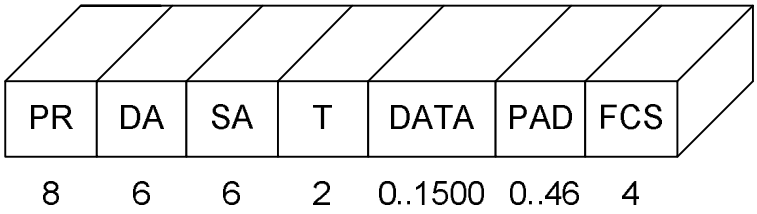


Рис. 16. Формат кадров Ethernet

Кадр состоит из набора полей, размер которых указан на рис. 16.

1) PR – *Preamble* (преамбула): последовательность восьми байтов вида 10101010, которая служит для синхронизации приемника и источника.

2) DA – *Destination Address* (адрес приемника).

3) SA – *Source Address* (адрес источника).

На канальном уровне для идентификации узлов сети используются MAC-адреса[1], состоящие из 6 байт. MAC-адрес записывается в виде последовательности шестнадцатеричных цифр, разделенных дефисами:

01–98–E5–67–DA–F0.

MAC-адреса являются атрибутом сетевой карты, поэтому называются ещё *физическими* (physical address) или *аппаратными* адресами (hardware address).

4) T – *Type* (тип): указывает протокол верхнего (сетевого) уровня, которому следует передать данный кадр (см. рис. 6).

5) DATA – данные: полезная информация, которую нужно передать. Чаще всего это пакет, пришедший от сетевого уровня. Размер данных может быть от 0 до 1500 байт.

6) PAD – *Padding* (заполнение): если данных в кадре менее 46 байт, используется поле *Padding* для дополнения до 46 байт. Заполнение требуется

[1] MAC – Media Access Control – управление доступом к среде передачи данных.

для обеспечения минимального размера кадра в 72 байта. Если кадр будет меньшего размера, существует вероятность его неправильной передачи.

7) FCS – *Frame Check Sequence* (контрольная сумма): источник, перед отправкой кадра, вычисляет значение определенной функции[1] от передаваемых данных и записывает это значение (которое называется *контрольная сумма*) в поле FCS. Приемник, получив кадр, вычисляет значение той же самой функции от полученных данных и сравнивает его со значением в поле FCS. Если они равны, значит кадр передан без искажений, иначе делается вывод об ошибке передачи.

4.3. Fast Ethernet

Рассмотрим один из стандартов Ethernet – Fast Ethernet с пропускной способностью 100 Мбит/с. В этом стандарте используется топология *звезда* и существует несколько спецификаций[2], которые обозначаются по формуле, общей для всех стандартов Ethernet:

<*Пропускная способность*> BASE – <*Тип среды передачи*>.

Например, 10BASE-T обозначает спецификацию Ethernet с пропускной способностью 10 Мбит/с и витой парой в качестве среды передачи данных (T – Twisted). Слово BASE (*базовый*) обозначает, что передача данных ведется на одной, базовой, частоте, в отличие от сетей, где информация по одному кабелю может передаваться с разными частотами.

Спецификации Fast Ethernet и их характеристики приведены в таблице 6.

Таблица 6. Спецификации Fast Ethernet

Спецификация	Среда передачи	Длина сегмента	Примечание
100BASE-TX	2 витые пары UTP категории 5 или выше	100 м	Самая распространенная в LAN спецификация
100BASE-T4	4 витые пары UTP категории 3 или выше	100 м	Не используется
100BASE-T2	2 витые пары UTP категории 3 или выше	100 м	Не используется

[1] Например, в качестве FCS используется остаток от деления по модулю 2 двоичной строки данных на определенное число. Деление по модулю 2 осуществляется с помощью логической операции XOR и происходит очень быстро.

[2] Спецификация – подробный перечень технических характеристик какого-либо продукта.

Спецификация	Среда передачи	Длина сегмента	Примечание
100BASE-FX	многомодовое оптоволокно, длина волны 1300 нм	2 км	
100BASE-SX	многомодовое оптоволокно, длина волны 850 нм	300 м	Дешевый вариант оптоволоконной сети
100BASE-LX	двухжильное одномодовое оптоволокно	10 км	
100BASE-BX	одножильное одномодовое оптоволокно	40 км	

5. Сетевые устройства

В современных сетях присутствует большое количество оборудования всевозможных типов и производителей. Рассмотрим самые распространенные виды сетевых устройств: сетевые карты, модемы, концентраторы, коммутаторы, маршрутизаторы.

5.1. Сетевые карты

Сетевая карта, сетевая плата, сетевой адаптер (Network Interface Card, NIC) – периферийное устройство, позволяющее подключать компьютер к компьютерной сети. Выпускаются в виде отдельных плат (рис. 17) или встраиваются в материнскую плату.

Рис. 17. Сетевая карта

Сетевая карта под управлением своего драйвера реализует физический и канальный уровни модели OSI и выполняет две основные функции – передача и прием кадра.

При передаче кадра сетевая карта принимает от вышележащего сетевого уровня модели OSI пакет, оформляет его в кадр соответствующей технологии, например Ethernet (см. рис. 16), т. е. вставляет MAC-адреса источника и приемника, вычисляет контрольную сумму. После этого в кабель, подключенный к разъему карты, выдается последовательность электрических сигналов, обозначающих двоичные нули и единицы.

Прием кадра происходит следующим образом: карта считывает пришедшие по кабелю сигналы, преобразует их в двоичные нули и единицы, определяет MAC-адрес приемника и сравнивает его со своим. Если MAC-

адреса не совпадают, кадр просто отбрасывается. Иначе вычисляется контрольная сумма и сравнивается с полученной в кадре. Если контрольные суммы не совпадают, на сетевой уровень выдается сообщение об ошибке передачи. Если все в порядке, из кадра извлекается поле данных (пакет) и передается на сетевой уровень.

5.2. Концентраторы

Концентратор, хаб, повторитель (hub) – сетевое устройство, которое объединяет несколько сегментов сети и повторяет сигналы, полученные из одного сегмента на все другие сегменты. Для подключения каждого сегмента используются разъемы, которые называются *портами*. Портов может быть от 4 до 48 и более.

Концентраторы работают на физическом уровне модели OSI, т. е. обрабатывают электрические сигналы, но не MAC-адреса. При использовании концентраторов возникают проблемы низкой производительности и безопасности – каждый кадр, отправленный в сеть, попадает всем узлам сети, даже тем, которым кадр не предназначен.

В настоящее время концентраторы вытеснены более совершенными устройствами – коммутаторами.

5.3. Коммутаторы

Коммутатор, *свитч* (switch) – сетевое устройство, объединяющее сегменты сети и передающее кадры только в необходимые сегменты.

Таким образом, кадр, попавший на один из портов коммутатора, будет передан только на тот порт, к которому присоединен сегмент сети с находящимся в нем узлом-приемником данного кадра. В этом заключается основное отличие коммутаторов от концентраторов.

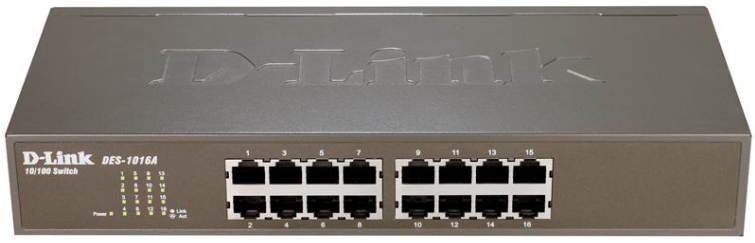


Рис. 18. 16-портовый коммутатор

Коммутатор работает на физическом и канальном уровнях модели OSI и умеет считывать MAC-адреса кадров. Коммутатор не нужно отдельно настраивать и сообщать ему, в каком сегменте какой компьютер находится, обнаружение узлов происходит автоматически.

Каким образом коммутатор узнает о расположении компьютеров сети? В нем хранится таблица соответствия «порт – MAC-адрес» и работает т. н. «алгоритм прозрачного моста»: коммутатор отслеживает прохождение всех кадров через свои порты и считывает MAC-адреса источников кадров. Если на какой-то порт пришел кадр с определенным MAC-адресом, значит этот MAC-адрес записывается в таблице как принадлежащий данному порту.

5.4. Маршрутизаторы

Маршрутизатор (router) – сетевое устройство, объединяющее подсети составной сети и решающее задачу маршрутизации на сетевом уровне модели OSI (см. параграф 2.2.3 Сетевой уровень).

У маршрутизатора также есть таблица соответствия «порт–адрес», которая называется *таблицей маршрутизации*, но используются не MAC-адреса, а IP-адреса.

IP-адрес[1] представляет собой 4-байтовое двоичное число, которое обычно записывается в виде 4-х десятичных чисел разделенных точками, например:

в десятичном виде: 192.168.0.1,
в двоичном виде: 11000000.10101000.00000000.00000001.

В отличие от MAC-адреса у IP-адреса можно выделить два уровня адресации – адрес подсети и адрес узла в этой подсети. Для этого в паре с IP-адресом часто указывают *маску подсети* – также 4-байтовое двоичное число, в определенном количестве старших разрядах которого (слева) находятся всегда единицы, а в остальных младших разрядах (справа) находятся нули. Единицы в двоичной записи маски означают, что соответствующий разряд в IP-адресе должен интерпретироваться как адрес подсети, а остальные разряды – как адрес узла в этой подсети.

Пример. Даны IP-адрес 192.168.0.1 и маска подсети 255.255.255.0. Требуется адрес подсети и адрес узла в подсети.

[1] IP – Internet Protocol (межсетевой протокол) – один из основных протоколов стека TCP/IP, на котором основана работа Интернета.

Запишем IP-адрес и маску подсети в двоичном виде:

IP-адрес: 11000000.10101000.00000000.00000001,
маска подсети: 11111111.11111111.11111111.00000000.

Единицы в маске содержатся в первых 24-х битах, следовательно, в IP-адресе соответствующие биты будут отвечать за адрес подсети (в остальные биты ставим нули):

адрес подсети:
двоичный 11000000.10101000.00000000.00000000,
десятичный 192.168.0.0.

Нули в маске находятся в младших 8 битах, соответствующие биты в IP-адресе обозначают адрес узла:

адрес узла:
двоичный 00000000.00000000.00000000.00000001,
десятичный 0.0.0.1.

Таблица маршрутизации может заполняться вручную администратором сети или автоматически самим маршрутизатором, который при этом не следит за проходящим трафиком, а рассылает запросы другим маршрутизаторам об имеющейся у них информации о конфигурации сети.

6. Стек протоколов TCP/IP

Стек TCP/IP – это набор иерархически упорядоченных сетевых протоколов. Название стек получил по двум важнейшим протоколам – TCP (Transmission Control Protocol) и IP (Internet Protocol). Помимо них в стек входят ещё несколько десятков различных протоколов. В настоящее время протоколы TCP/IP являются основными для Интернета, а также для большинства корпоративных и локальных сетей.

Стек протоколов TCP/IP обладает двумя важными свойствами:

- *платформонезависимостью*, т. е. возможностью его реализации на самых разных операционных системах и процессорах;
- *открытостью*, т. е. доступностью стандартов, по которым строится стек TCP/IP, любому желающему.

6.1. История создания TCP/IP

В 1967 году Агентство по перспективным исследовательским проектам министерства обороны США (ARPA – Advanced Research Projects Agency) инициировало разработку компьютерной сети, которая должна была связать ряд университетов и научно-исследовательских центров, выполнявших заказы Агентства. Проект получил название ARPANET. К 1972 году сеть соединяла 30 узлов.

В рамках проекта ARPANET были разработаны и в 1980–1981 годах опубликованы основные протоколы стека TCP/IP – IP, TCP и UDP. Важным фактором распространения TCP/IP стала реализация этого стека в операционной системе UNIX 4.2 BSD (1983).

К концу 80-х годов значительно расширившаяся сеть ARPANET стала называться Интернет (Interconnected networks – связанные сети) и объединяла университеты и научные центры США, Канады и Европы.

В 1992 году появился новый сервис Интернет – WWW (World Wide Web – всемирная паутина), основанный на протоколе HTTP. Во многом благодаря WWW Интернет, а с ним и протоколы TCP/IP, получил в 90-е годы бурное развитие.

В начале XXI века стек TCP/IP приобретает ведущую роль в средствах коммуникации не только глобальных, но и локальных сетей.

6.2. Структура TCP/IP

В основе TCP/IP лежит не модель OSI, а собственная модель, называемая по-разному: *DoD* (Department of Defense – Министерство обороны США), *DARPA* (Defense ARPA – новое название Агентства по перспективным исследовательским проектам) или просто *модель TCP/IP*. В этой модели всего четыре уровня. Соответствие модели OSI модели DoD, а также основным протоколам стека TCP/IP показано на рис. 19.

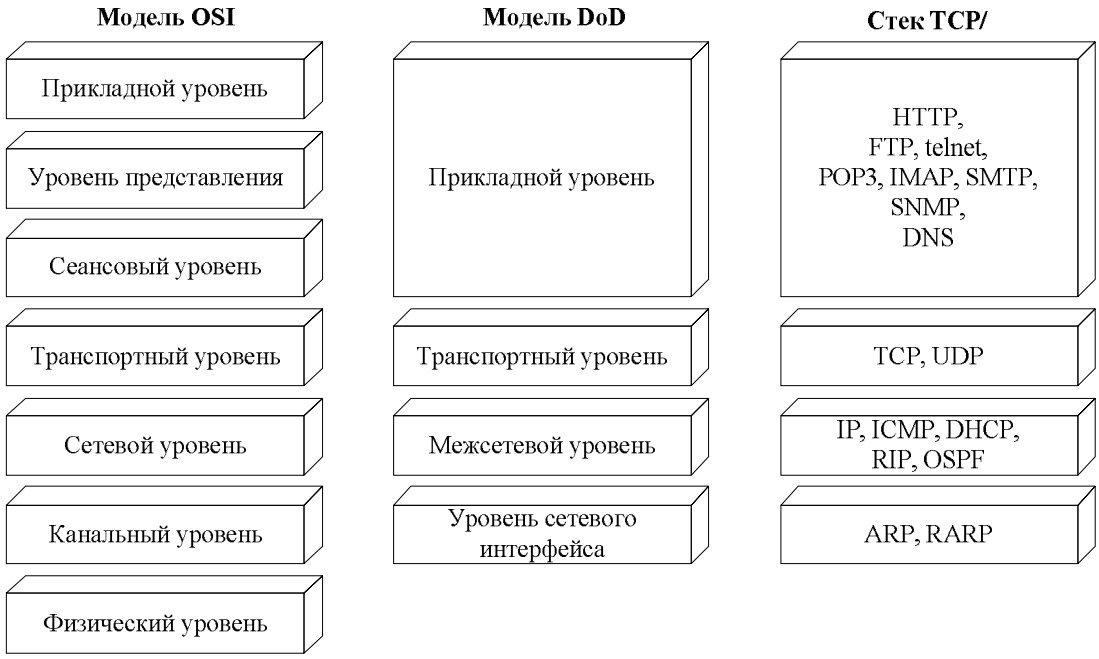


Рис. 19. Соответствие протоколов TCP/IP моделям OSI и DoD

Следует заметить, что нижний уровень модели DoD – уровень сетевого интерфейса – строго говоря, не выполняет всех функций канального уровня, а лишь обеспечивает связь (интерфейс) верхних уровней DoD с технологиями сетей, входящих в составную сеть (например, Ethernet, FDDI, ATM).

Все протоколы, входящие в стек TCP/IP, стандартизованы в документах RFC.

6.3. Документы RFC

Утвержденные официальные стандарты Интернета и TCP/IP публикуются в виде документов RFC (Request for Comments – рабочее предложение). Стандарты разрабатываются всем сообществом ISOC (Internet

Society – Сообщество Интернет, международная общественная организация). Любой член ISOC может представить на рассмотрение документ для его публикации в RFC. Далее документ рассматривается техническими экспертами, группами разработчиков и редактором RFC и проходит в соответствии с RFC 2026 следующие этапы, называемые *уровнями готовности* (maturity levels):

1) *черновик* (Internet Draft) – на этом этапе с документом знакомятся эксперты, вносятся дополнения и изменения;

2) *предложенный стандарт* (Proposed Standard) – документу присваивается номер RFC, эксперты подтвердили жизнеспособность предлагаемых решений, документ считается перспективным, желательно, чтобы он был опробован на практике;

3) *черновой стандарт* (Draft Standard) – документ становится черновым стандартом, если не менее двух независимых разработчиков реализовали и успешно применили предлагаемые спецификации. На этом этапе ещё допускаются незначительные исправления и усовершенствования;

4) *стандарт Интернета* (Internet Standard) – наивысший этап утверждения стандарта, спецификации документа получили широкое распространение и хорошо зарекомендовали себя на практике. Список стандартов Интернета приведен в RFC 5000. Из тысяч RFC только несколько десятков являются документами в статусе «стандарт Интернета».

Кроме стандартов документами RFC могут быть также описания новых сетевых концепций и идей, руководства, результаты экспериментальных исследований, представленных для информации и т. д. Таким документам RFC может быть присвоен один из следующих статусов:

- *экспериментальный* (Experimental) – документ, содержащий сведения о научных исследованиях и разработках, которые могут заинтересовать членов ISOC;
- *информационный* (Informational) – документ, опубликованный для предоставления информации и не требующий одобрения сообщества ISOC;
- *лучший современный опыт* (Best Current Practice) – документ, предназначенный для передачи опыта конкретных разработок, например реализаций протоколов.

Статус указывается в заголовке документа RFC после слова *Category* (категория). Для документов в статусе стандартов (Proposed Standard, Draft

Standard, Internet Standard) указывается название *Standards Track*, так как уровень готовности может меняться.

Номера RFC присваиваются последовательно и никогда не выдаются повторно. Первоначальный вариант RFC никогда не обновляется. Обновленная версия публикуется под новым номером. Устаревший и замененный документ RFC получает статус *исторический* (Historic).

Все существующие на сегодня документы RFC можно посмотреть, например, на сайте http://www.rfc-editor.org. В октябре 2011 года их насчитывалось около шести с половиной тысяч.

6.4. Обзор основных протоколов

Протокол IP (Internet Protocol) – это основной протокол сетевого уровня, отвечающий за адресацию в составных сетях и передачу пакета между сетями. Протокол IP является *дейтаграммным* протоколом, т. е. не гарантирует доставку пакетов до узла назначения. Обеспечением гарантий занимается протокол транспортного уровня TCP.

Протоколы RIP (Routing Information Protocol – протокол маршрутной информации*) и OSPF* (Open Shortest Path First – «первыми открываются кратчайшие маршруты») – протоколы маршрутизации в IP-сетях.

Протокол ICMP (Internet Control Message Protocol – протокол управляющих сообщений в составных сетях) предназначен для обмена информацией об ошибках между маршрутизаторами сети и узлом-источником пакета. С помощью специальных пакетов сообщает о невозможности доставки пакета, о продолжительности сборки пакета из фрагментов, об аномальных величинах параметров, об изменении маршрута пересылки и типа обслуживания, о состоянии системы и т. п.

Протокол ARP (Address Resolution Protocol – протокол преобразования адресов) преобразует IP-адреса в аппаратные MAC-адреса. Обратное преобразование осуществляется с помощью протокола *RAPR* (Reverse ARP).

Протокол TCP (Transmission Control Protocol – протокол управления передачей) обеспечивает надежную передачу сообщений между удаленными узлами сети за счет образования логических соединений. TCP позволяет без ошибок доставить сформированный на одном из компьютеров поток байт на любой другой компьютер, входящий в составную сеть. TCP делит поток байт на части – *сегменты* и передает их сетевому уровню. После того как эти сегменты будут доставлены в пункт назначения, протокол TCP снова соберет их в непрерывный поток байт.

Протокол UDP (User Datagram Protocol – протокол дейтаграмм пользователя) обеспечивает передачу данных дейтаграммным способом.

Далее рассматриваются протоколы прикладного уровня.

Протокол HTTP (HyperText Transfer Protocol – протокол передачи гипертекста) – протокол доставки web-документов, основной протокол службы WWW.

Протокол FTP (File Transfer Protocol – протокол передачи файлов) – протокол для пересылки информации, хранящейся в файлах.

Протоколы POP3 (Post Office Protocol version 3 – протокол почтового офиса), *IMAP* (Internet Message Access Protocol – протокол для доступа к электронной почте) и *SMTP* (Simple Mail Transfer Protocol – простой протокол пересылки почты) – протоколы для доставки входящей электронной почты (POP3 и IMAP) и отправки исходящей (SMTP).

Протоколы Telnet и *SSH* (Secure Shell – безопасная оболочка) – протоколы эмуляции терминала[1], позволяющие пользователю подключаться к другим удалённым станциям и работать с ними со своей машины, как если бы она была их удалённым терминалом. Протокол SSH, в отличие от Telnet, обеспечивает безопасное соединение за счет шифрования.

Протокол SNMP (Simple Network Management Protocol – простой протокол управления сетью) предназначен для диагностики работоспособности различных устройств сети.

6.5. Утилиты диагностики TCP/IP

В состав операционных систем семейства Windows входит ряд утилит (небольших служебных программ), предназначенных для диагностики функционирования стека TCP/IP (аналогичные утилиты есть и UNIX/Linux-системах).

Для запуска этих утилит следует в меню *Пуск* выбрать пункт *Выполнить*, в появившемся окне набрать *cmd* и нажать *Enter*[2]. Появится интерфейс командной строки с приглашением для ввода команд (рис. 20).

Информацию о любой утилите можно вывести, набрав в командной строке имя утилиты с ключом «/?», например: IPconfig /?

Hostname

Это самая простая утилита – она выводит на экран имя компьютера.

[1] Терминал – это сочетание устройства ввода и устройства вывода, например клавиатура и дисплей.

[2] В Windows 7 нужно в меню *Пуск* в текстовом окне «*Найти программы и файлы*» набрать *cmd* и нажать *Enter*.

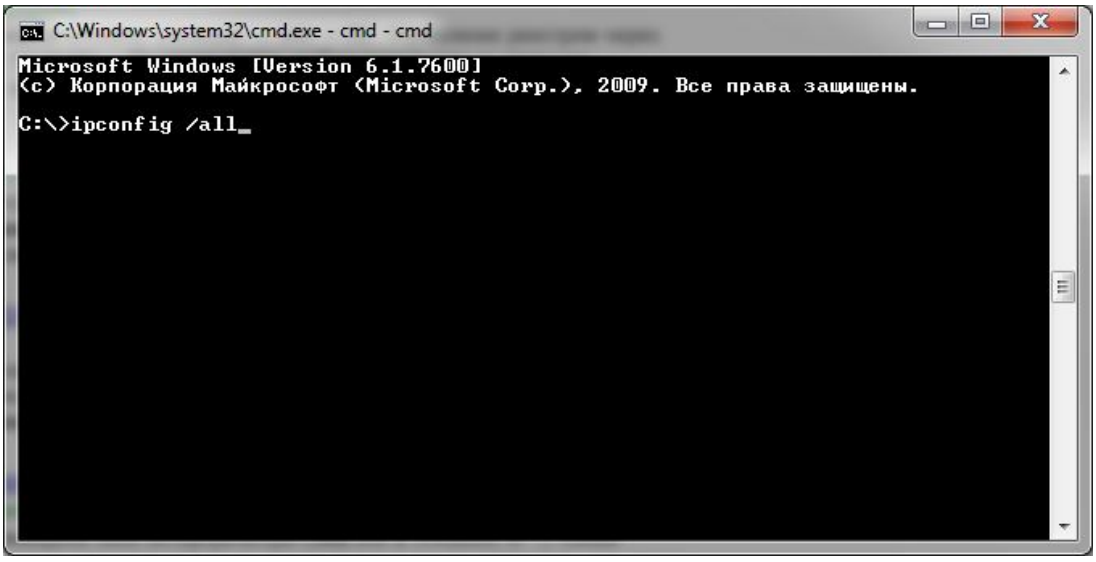


Рис. 20. Интерфейс командной строки

IPconfig

Утилита предназначена, во-первых, для вывода информации о конфигурации стека TCP/IP, во-вторых, для выполнения некоторых действий по настройке стека.

При вводе названия утилиты в командной строке без параметров на экране отобразится информация об основных настройках TCP/IP, например, IP-адрес (IP Address) и маска подсети (Subnet Mask).

Использование утилиты с ключом **/all** позволит узнать полную информацию о настройке стека TCP/IP на данном компьютере. Следует отметить, что при наличии нескольких сетевых карт выводятся данные по каждой карте отдельно, например, можно узнать MAC-адрес сетевой карты (физический адрес).

Ping

Основная цель этой утилиты – выяснение возможности установления соединения с удаленным узлом.

Принцип работы: утилита отправляет на удаленный узел несколько пакетов (число пакетов определяется ключом **–n**, по умолчанию четыре) по протоколу ICMP. Такие пакеты называются *эхо-пакетами*, т. е. требуют ответа. Если удаленный узел доступен, он отвечает на каждый эхо-пакет своим пакетом, а утилита измеряет интервал между отправкой эхо-пакета и приходом ответа.

Нужно отметить, что отсутствие ответа может быть связано не с физической недоступностью удаленного компьютера, а с тем, что на нем установлена специальная программа для обеспечения сетевой безопасности –

брандмауэр (другое название *firewall*), запрещающее отправку ответов на эхо-пакеты.

Tracert

Название утилиты произошло от Trace Route – отслеживание маршрута. Утилита позволяет решить следующие задачи:

– проследить путь прохождения пакета от данного компьютера до удаленного узла (отображаются промежуточные узлы-маршрутизаторы);

– выявить участки задержки пакетов;

– выявить места потери пакетов.

Принцип работы: утилита отправляет эхо-пакеты на заданный удаленный узел. Отличие между эхо-пакетами заключается в параметре, который называется *время жизни* (TTL – Time To Live). Этот параметр обозначает количество маршрутизаторов (процесс перехода пакета через маршрутизатор называется *hop* – прыжок), которое может пройти пакет, прежде чем попадет на заданный узел. Каждый маршрутизатор уменьшает время жизни на единицу. Если на каком-то маршрутизаторе TTL станет равным нулю, тот отбрасывает пакет и отправляет служебное сообщение на узел-источник.

Первый эхо-пакет посылается с временем жизни, равным единице. Первый маршрутизатор отбрасывает эхо-пакет и отправляет служебное сообщение, в котором содержится информации об имени и адресе маршрутизатора. Следующий эхо-пакет имеет TTL = 2 и отбрасывается уже на втором маршрутизаторе. Таким образом, эхо-пакеты отправляются с увеличением времени жизни на единицу, пока не придет ответ от заданного удаленного узла или время ожидания не будет превышено.

Arp

Эта утилита работает с протоколами преобразования IP-адресов в MAC-адреса и обратно ARP и RARP. С её помощью можно выводить на экран таблицу соответствия IP-адресов и MAC-адресов (ARP-кэш), добавлять и удалять записи в ней.

Основные ключи:

- **/a** – отображение таблицы ARP или, если указан IP-адрес, запись только для этого адреса;
- **/s** – добавление записи в таблицу;
- **/d** – удаление записи из таблицы.

7. Задания для самостоятельного выполнения

1. Перечислите цели объединения компьютеров в сеть и придумайте примеры, иллюстрирующие каждую цель.
2. Дайте определения терминов: *server*, *client*, *peer*, *node*, *media*, *wireless*, *traffic*, *simplex*, *duplex*.
3. Составьте таблицу, в которой перечислите достоинства и недостатки рассмотренных в лекции топологий.
4. Сравните известные топологии с точки зрения наличия избыточности.
5. Каким образом скорость передачи данных влияет на время реакции сети?
6. Классифицируйте известные Вам сети в Вашем населенном пункте по размеру, типу взаимодействия, топологии.
7. Опишите характеристики известной Вам сеть (например, школьную или домашнюю): производительность, надежность, безопасность.
8. Вам предложили создать локальную сеть школы. Составьте проект такой сети, включающий обоснование выбранных топологии, типа взаимодействия компьютеров, среды передачи данных.
9. Перечислите уровни модели OSI и кратко опишите функции каждого уровня.
10. Приведите свой пример иерархической системы.
11. Какая задача сложнее: обнаружение ошибок или коррекция ошибок?
12. В модуле рассмотрены два вида сетевых адресов – MAC-адреса и IP адреса. Существует ещё третий вид, который называется символьные доменные имена. За преобразование IP-адреса в доменное имя и обратно отвечает служба DNS (Domain Name System). Самостоятельно найдите информацию о доменных именах – из каких частей они состоят, примеры.
13. Сколько всего MAC-адресов?
14. Сколько всего IP-адресов?
15. Назовите виды линий связи, которые используются в Вашем доме (школе).
16. Как Вы думаете, почему поле DA (Destination Address) в кадре Ethernet идет раньше поля SA (Source Address)?
17. Какая технология Ethernet (10 Мбит/с, Fast Ethernet или Gigabit Ethernet) используется в известных вам локальных сетях (домашней, школьной)?

18. Перечислите сетевые устройства, которые присутствуют в известных вам сетях.

19. Дан IP-адрес 172.16.235.57, маска подсети 255.255.0.0. Укажите адрес подсети и адрес узла.

20. Зайдите на сайт http://www.rfc-editor.org и посмотрите там несколько документов RFC, например:

- самый первый RFC – RFC1,
- описание протокола IP – RFC791,
- описание доменных имен – RFC1034 и RFC1035,
- почтовый протокол POP3 – RFC1939,
- список стандартов – RFC5000.

21. При помощи утилиты *hostname* узнайте имя своего компьютера.

22. Определите свой IP-адрес, маску подсети и MAC-адрес с помощью утилиты *IPconfig*.

23. Узнайте, достижимы ли с Вашего компьютера узлы www.google.ru, www.yandex.ru, а также узлов локальной сети (если она есть), используя утилиту *ping*.

24. Определите маршрут до узлов www.google.ru, www.yandex.ru при помощи утилиты *tracert*.

25. Выведите на дисплей таблицу соответствия IP адресов и MAC адресов (ARP кэш) при помощи утилиты *arp*.

Литература

1. Иртегов Д. В. Введение в сетевые технологии. – СПб.: БХВ-Петербург, 2004.

2. Котельников Е. В., Кротова Н. А., Иванов С. Ю. Сетевое администрирование на основе Microsoft Windows Server 2003. – Киров: Изд-во ВятГГУ, 2009.

3. Олифер В. Г., Олифер Н. А. Компьютерные сети. Принципы, технологии, протоколы. – 4-е изд. – СПб.: Питер, 2011.

4. Олифер В. Г., Олифер Н. А. Основы компьютерных сетей. – СПб.: Питер, 2009.

5. Столлингс В. Компьютерные сети, протоколы и технологии Интернета. – СПб.: БХВ-Петербург, 2005.

6. Таненбаум Э. Компьютерные сети. – СПб: Питер, 2007.